Configure Centralized Deployment

Centralized Deployment Overview

The IM and Presence centralized deployment allows you to deploy your IM and Presence deployment and your telephony deployment in separate clusters. The central IM and Presence cluster handles IM and Presence for the enterprise, while the remote Cisco Unified Communications Manager telephony cluster handles voice and video calls for the enterprise.

The Centralized Deployment option provides the following benefits when compared to standard deployments:

- The Centralized Deployment option does not require a 1x1 ratio of telephony clusters to IM and Presence Service clusters–you can scale your IM and Presence deployment and your telephony deployment separately, to the unique needs of each.
- Full mesh topology is not required for the IM and Presence Service
- Version independent from telephony–your IM and Presence central cluster can be running a different version than your Cisco Unified Communications Manager telephony clusters.
- Can manage IM and Presence upgrades and settings from the central cluster.
- Lower cost option, particularly for large deployments with many Cisco Unified Communications Manager clusters
- Easy XMPP Federation with third parties.
- Supports calendar integration with Microsoft Outlook. For configuration details, refer to the document *Microsoft Outlook Calendar Integration for the IM and Presence Service*.

OVA Requirements

For Centralized Deployments, we recommend the 25,000 user IM and Presence OVA with a minimum OVA of 15,000 users. The 15,000 user OVA can grow to 25,000 users. With a 25K OVA template, and a six-node cluster with High Availability enabled, the IM and Presence Service central deployment supports up to 75,000 clients. To support 75K users with 25K OVA, default trace level for XCP router needs to be changed from **Info** to **Error**. For the Unified Communications Manager publisher node in the central cluster, the following requirements apply:

- A 25,000 IM and Presence OVA (maximum 75,000 users) can be deployed with a 10,000 user OVA installed on the central cluster's Unified Communications Manager publisher node
- A 15,000 IM and Presence OVA (maximum 45,000 users) can be deployed with a 7,500 user OVA installed on the central cluster's Unified Communications Manager publisher node

Note If you plan to enable Multiple Device Messaging, measure deployments by the number of clients instead of the number of users as each user may have multiple Jabber clients. For example, if you have 25,000 users, and each user has two Jabber clients, your deployment requires the capacity of 50,000 users.

Interclustering for Centralized Deployment

Interclustering is supported between two centralized clusters. Intercluster peering is tested with one cluster with 25K (with 25K OVA) and another with 15K (with 15K OVA) devices and no performance issues were observed.

Centralized Deployment Setup vs Standard (Decentralized) Deployments

The following table discusses some of the differences in setting up an IM and Presence Centralized Cluster Deployment as opposed to standard deployments of the IM and Presence Service.

Setup Phase	Differences with Standard Deployments
Installation Phase	The installation process for an IM and Presence central deployment is the same as for the standard deployment. However, with central deployments, the IM and Presence central cluster is installed separately from your telephony cluster, and may be located on separate hardware servers. Depending on how you plan your topology, the IM and Presence central cluster may be installed on separate physical hardware from your telephony cluster. For the IM and Presence central cluster, you must still install Cisco Unified Communications Manager and then install the IM and Presence Service on the same servers. However, the Cisco Unified Communications Manager instance of the IM and Presence central cluster is for database and user provisioning primarily, and does not handle voice or video calls.

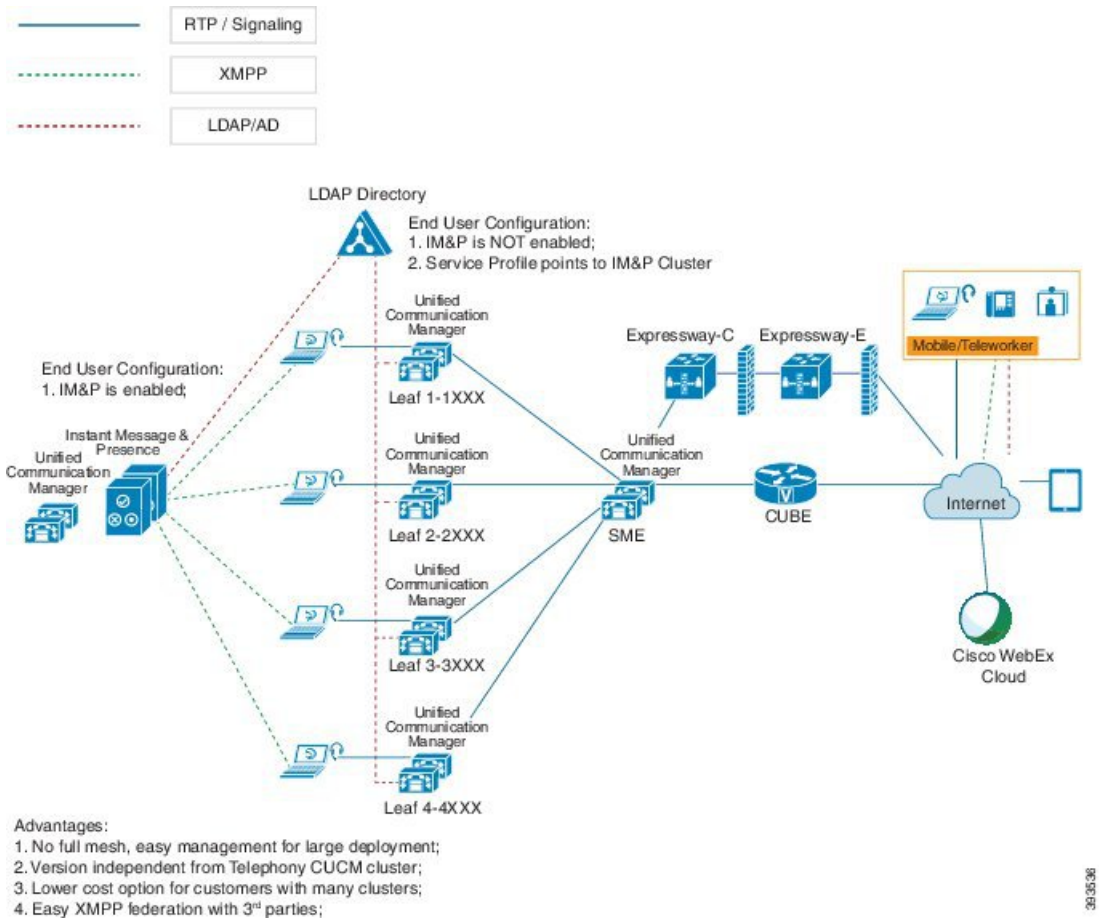
Setup Phase	Differences with Standard Deployments
Configuration Phase	Compared to standard (decentralized) deployments, the following extra configurations are required to set up the IM and Presence Service Central Deployment: • Users must be synced into both the telephony cluster and the IM and Presence Service central cluster so that they exist in both databases. • In your telephony clusters, end users should not be enabled for IM and Presence. • In your telephony clusters, the Service Profile must include the IM and Presence Service and must point to the IM and Presence central cluster. • In the IM and Presence central cluster, users must be enabled for the IM and Presence Service. • In the IM and Presence central cluster's database publisher node, add your remote Cisco Unified Communications Manager telephony cluster peers. The following configurations, which are used with Standard Deployments of the IM and Presence Service, but are not required with Central Deployments: • A Presence Gateway is not required. • A SIP Publish trunk is not required. • A Service Profile is not required on the IM and Presence central cluster—the Service Profile is configured on the telephony cluster to which the central cluster connects.

Centralized Cluster Deployment Architecture

The following diagram highlights the cluster architecture for this deployment option. Cisco Jabber clients connect to multiple Cisco Unified Communications Manager clusters for voice and video calling. In this example, the Cisco Unified Communications Manager telephony clusters are leaf clusters in a Session Management Edition deployment. For Rich Presence, Cisco Jabber clients connect to the IM and Presence Service central cluster. The IM and Presence central cluster manages instant messaging and presence for the Jabber clients.

Note Your IM and Presence cluster still contains an instance for Cisco Unified Communications Manager. However, this instance is for handling shared features such as database and user provisioning–it does not handle telephony.

Figure 1: IM and Presence Service Centralized Cluster Architecture

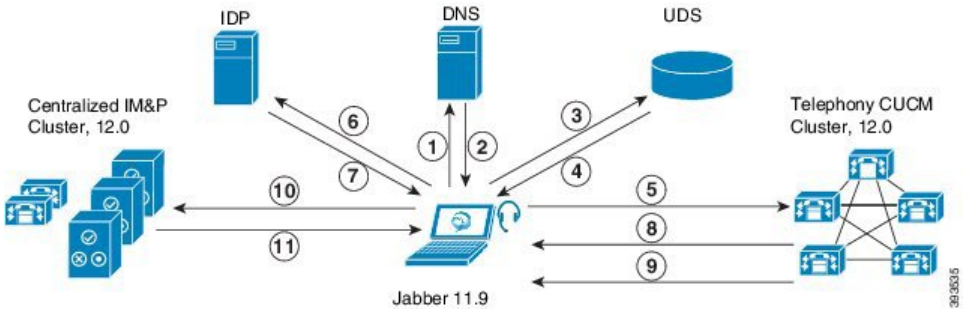


Centralized Cluster Use Case

To connect your telephony and IM and Presence clusters, a new system for exchanging access keys is introduced. This diagram shows the flow for SSO logins:

- [1]-[2]: Query DNS to get SRV record.
- [3]-[4]: Query UDS to get the Home Cisco Unified Communications Manager cluster.
- [5]-[8]: Get Access Token and Refresh Token from Cisco Unified Communications Manager cluster through SAML SSO.
- [9]: Read UC Service Profile. The service profile contains an IM and Presence profile and points to the IM and Presence central cluster.
- [10]: Client registers to the IM and Presence cluster using the same Access Token through SOAP and XMPP interfaces.
- [11]: The token is validated and a response is sent back to Jabber client.

Figure 2: IM and Presence Service Centralized Cluster Use Case



Centralized Deployment Prerequisites

The following requirements apply for the IM and Presence Service centralized deployment:

- The IM and Presence Service central cluster must be running Release 11.5(1)SU4 or higher.
- The local Cisco Unified Communications Manager instance that runs with the IM and Presence central cluster must be running the same release as the IM and Presence central cluster.
- The remote Cisco Unified Communications Manager telephony cluster must be running Release 10.5(2) or higher.
- Cisco Jabber must be running Release 11.9 or higher.
- For Push Notifications instant messaging support, the IM and Presence Service must be running at least 11.5(1)SU4.
- You need to enable Cisco Cloud Onboarding on the CUCM Publisher node of the centralised IM and Presence cluster so that all instant messages for iOS devices can also use the Apple Push Notification service (APNs) solution.

  Additionally, you also need to enable Cisco Cloud Onboarding option on the leaf CUCM clusters so that the TCT devices that normally register to those clusters, can have calls routed via the APNs when the Jabber for iOS devices have been suspended or killed by the iOS.

  For more information about how to enable Cisco Cloud Onboarding in the IM and Presence Service cluster, see the *Enable Cisco Cloud Onboarding* chapter in Push Notifications Deployment Guide.
- Cisco Unified Communications Manager functionality is based on the Cisco Unified Communications Manager version that is running on your remote telephony clusters rather than on the local instance that runs with the IM and Presence central cluster. For example:
  - For Push Notifications call support, the remote telephony cluster must be running at least 11.5(1)SU4.
  - For OAuth Refresh Logins support, the remote Cisco Unified Communications Manager telephony cluster must be running at least 11.5(1)SU4.
  - For SAML SSO support, the remote telephony cluster must be running at least 11.5(1)SU4.
- The **Cisco AXL Web Service** feature service must be running in all clusters. This service is enabled by default, but you can confirm that it is activated from the **Service Activation** window of Cisco Unified Serviceability.

- With Centralized Deployments, rich presence is handled by Cisco Jabber. The user's phone presence displays only if the user is logged in to Cisco Jabber.

DNS Requirements

The IM and Presence central cluster must have a DNS SRV record that points to the publisher node of the Cisco Unified Communications Manager telephony cluster. If your telephony deployment includes an ILS network, the DNS SRV must point to the hub cluster. This DNS SRV record should be referring to "_cisco-uds".

The SRV record is a Domain Name System (DNS) resource record that is used to identify computers that host specific services. SRV resource records are used to locate domain controllers for Active Directory. To verify SRV locator resource records for a domain controller, use the following method:

Active Directory creates its SRV records in the following folders, where Domain Name indicates the name of the installed domain:

- Forward Lookup Zones/Domain_Name/_msdcs/dc/_sites/Default-First-Site-Name/_tcp
- Forward Lookup Zones/Domain_Name/_msdcs/dc/_tcp

In these locations, an SRV record should appear for the following services:

- _kerberos
- _ldap
- _cisco_uds : indicates the SRV record

The below mentioned parameters has to be set during the SRV record creation .

- Service :_cisco_uds
- Protocol : _tcp
- weight : starts from 0 (0 is the highest priority)
- port no : 8443
- host : fqdn name of the server

An example of a DNS SRV record from a computer running a Jabber client is:

```
nslookup -type=all _cisco-uds._tcp.dcloud.example.com
Server: ad1.dcloud.example.com
Address: x.x.x.x
_cisco-uds._tcp.dcloud.example.com SRV service location:
priority = 10
weight = 10
port = 8443
svr hostname = cucm2.dcloud.example.com
cucm2.dcloud.example.com internet address = x.x.x.y
```

Centralized Deployment Configuration Task Flow

Complete these tasks if you want to configure a new IM and Presence Service deployment to use the centralized deployment option.

Note Use this task flow for new IM and Presence Service deployments only.

Table 1: Centralized Cluster Configuration Task Flow

	IM and Presence Central Cluster	Remote Telephony Clusters	Purpose
Step 1	Enable IM and Presence via Feature Group Template, on page 8		In your IM and Presence central cluster, configure a template that enables the IM and Presence Service.
Step 2	Complete LDAP Sync on IM and Presence Central Cluster, on page 9		Complete an LDAP sync to propagate settings to LDAP-synced users in your IM and Presence central cluster.
Step 3	Enable Users for IM and Presence via Bulk Admin, on page 10		Optional. If you have already completed an LDAP sync, use Bulk Administration to enable IM and Presence for users.
Step 4	Add Remote Telephony Clusters, on page 10		Add your remote telephony clusters to the IM and Presence central cluster.
Step 5		Configure an IM and Presence UC Service, on page 11	In your telephony clusters, add a UC service that points to the IM and Presence central cluster.
Step 6		Create Service Profile for IM and Presence, on page 12	Add your IM and Presence UC service to a service profile. Cisco Jabber clients use this profile to find the IM and Presence central cluster.
Step 7		Disable Presence Users in Telephony Cluster, on page 12	In the telephony cluster, edit Presence user settings to point to the IM and Presence central cluster.
Step 8		Configure OAuth Refresh Logins , on page 14	Configuring OAuth in the telephony cluster will enable the feature for the central cluster.
Step 9		Configure an ILS Network, on page 14	If more than one telephony cluster exists, you must configure ILS.

	IM and Presence Central Cluster	Remote Telephony Clusters	Purpose
Step 10		Mobile and Remote Access Configuration	Configuration of Mobile and Remote Access in case of centralized deployment.

What to do Next

- If you want to connect your central cluster to other IM and Presence clusters as part of an intercluster network, configure intercluster peering.
- You must restart the Cisco XCP Authentication Service when you make a new entry to the centralized deployment in the IM and Presence administrator console.

Enable IM and Presence via Feature Group Template

Use this procedure to configure a feature group template with IM and Presence settings for the central cluster. You can add the feature group template to an LDAP Directory configuration to configure IM and Presence for synced users.

Note You can apply a feature group template only to an LDAP directory configuration where the initial sync has not yet occurred. Once you've synced your LDAP configuration from the central cluster, you cannot apply edits to the LDAP configuration in Cisco Unified Communications Manager. If you have already synced your directory, you will need to use Bulk Administration to configure IM and Presence for users. For details, see Enable Users for IM and Presence via Bulk Admin, on page 10.

Procedure

Step 1 Log into the Cisco Unified CM Administration interface of the IM and Presence centralized cluster. This server should have no telephony configured.

Step 2 Choose **User Management** > **User Phone/Add** > **Feature Group Template**.

Step 3 Do one of the following:

- Click **Find** and select an existing template
- Click **Add New** to create a new template

Step 4 Check both of the following check boxes:

- **Home Cluster**
- **Enable User for Unified CM IM and Presence**

Step 5 Complete the remaining fields in the **Feature Group Template Configuration** window. For help with the fields and their settings, refer to the online help.

Step 6 Click **Save**.

What to do next

To propagate the setting to users, you must add the Feature Group Template to an LDAP directory configuration where the initial sync has not yet occurred, and then complete the initial sync.

Complete LDAP Sync on IM and Presence Central Cluster, on page 9

Complete LDAP Sync on IM and Presence Central Cluster

Complete an LDAP sync on your IM and Presence Service central cluster to configure users with IM and Presence services via the feature group template.

Note You cannot apply edits to an LDAP sync configuration after the initial sync has occured. If the initial sync has already occurred, use Bulk Administration instead. For additional detail on how to set up an LDAP Directory sync, see the "Configure End Users" part of the *System Configuration Guide for Cisco Unified Communications Manager*.

Before you begin

Enable IM and Presence via Feature Group Template, on page 8

Procedure

Step 1 Log into the Cisco Unified CM Administration interface of the IM and Presence centralized cluster. This server should have no telephony configured.

Step 2 Choose **System** > **LDAP** > **LDAP Directory**.

Step 3 Do either of the following:

a) Click **Find** and select an existing LDAP Directory sync.

b) Click **Add New** to create a new LDAP Directory.

Step 4 From the **Feature Group Template** drop-down list box, select the IM and Presence-enabled feature group template that you created in the previous task.

Step 5 Complete the remaining fields in the **LDAP Directory** window. For help with the fields and their settings, refer to the online help.

Step 6 Click **Save**.

Step 7 Click **Perform Full Sync**.

Cisco Unified Communications Manager synchronizes the database with the external LDAP directory. End users are configured with IM and Presence services.

What to do next

Add Remote Telephony Clusters, on page 10

Enable Users for IM and Presence via Bulk Admin

If you have already synced users into the central cluster, and those users were not enabled for the IM and Presence Service, use Bulk Administration's Update Users feature to enable those users for the IM and Presence Service.

Note You can also use Bulk Administration's Import Users or Insert Users feature to import new users via a csv file. For procedures, see the *Bulk Administration Guide for Cisco Unified Communications Manager*. Make sure that the imported users have the below options selected:

- Home Cluster
- Enable User for Unified CM IM and Presence

Procedure

Step 1 From Cisco Unified CM Administration, choose **Bulk Administration** > **Users** > **Update Users** > **Query**.

Step 2 From the **Filter**, select **Has Home Cluster Enabled** and click **Find**. The window displays all of the end users for whom this is their Home Cluster

Step 3 Click **Next**.
In the **Update Users Configuration** window, the check boxes on the far left indicate whether you want to edit this setting with this query. If you don't check the left check box, the query will not update that field. The field on the right indicates the new setting for this field. If two check boxes appear, you must check the check box on the left to update the field, and in the right check box, enter the new setting.

Step 4 Under **Service Settings**, check the left check box for each of the following fields to indicate that you want to update these fields, and then edit the adjacent field setting as follows:

- **Home Cluster**—Check the right check box to enable this cluster as the home cluster.
- **Enable User for Unified CM IM and Presence**—Check the right check box. This setting enables the central cluster as the provider of IM and Presence Service for these users.

Step 5 Complete any remaining fields that you want to update. For help with the fields and their settings, see the online help:

Step 6 Under **Job Information**, select **Run Immediately**.

Step 7 Click **Submit**.

Add Remote Telephony Clusters

Use this procedure to add your remote telephony clusters to the centralized IM and Presence Service cluster.

Note If you have more than one telephony cluster, you must deploy ILS. In this case, the telephony cluster to which the IM and Presence central cluster connects must be a hub cluster.

Procedure

Step 1 Log in to database publisher node on the IM and Presence Service centralized cluster.

Step 2 From Cisco Unified CM IM and Presence Administration, choose **System** > **Centralized Deployment**.

Step 3 Click **Find** to view the list of current remote Cisco Unified Communications Manager clusters. If you want to edit the details of a cluster, select the cluster and click **Edit Selected**.

Step 4 Click **Add New** to add a new remote Cisco Unified Communications Manager telephony cluster.

Step 5 Complete the following fields for each telephony cluster that you want to add:

- **Peer Address**—The FQDN, hostname, IPv4 address, or IPv6 address of the publisher node on the remote Cisco Unified Communications Manager telephony cluster.
- **AXL Username**—The login username for the AXL account on the remote cluster.
- **AXL Password**—The password for the AXL account on the remote cluster.

Step 6 Click the **Save and Synchronize** button.
The IM and Presence Service synchronizes keys with the remote cluster.

What to do next

Configure an IM and Presence UC Service, on page 11

Configure an IM and Presence UC Service

Use this procedure in your remote telephony clusters to configure a UC service that points to the IM and Presence Service central cluster. Users in the telephony cluster will get IM and Presence services from the IM and Presence central cluster.

Procedure

Step 1 Log in to the Cisco Unified CM Administration interface on your telephony cluster.

Step 2 Choose **User Management** > **User Settings** > **UC Service**.

Step 3 Do either of the following:

a) Click **Find** and select an existing service to edit.
b) Click **Add New** to create a new UC service.

Step 4 From the **UC Service Type** drop-down list box, select **IM and Presence** and click **Next**.

Step 5 From the **Product type** drop-down list box, select **IM and Presence Service**.

Step 6 Enter a unique **Name** for the cluster. This does not have to be a hostname.

Step 7 From **HostName/IP Address**, enter the hostname, IPv4 address, or IPv6 address of the IM and Presence central cluster database publisher node.

Step 8 Click **Save**.

Step 9 Recommended. Repeat this procedure to create a second IM and Presence service where the **HostName/IP Address** field points to a subscriber node in the central cluster.

What to do next

Create Service Profile for IM and Presence, on page 12.

Create Service Profile for IM and Presence

Use this procedure in your remote telephony clusters to create a service profile that points to the IM and Presence central cluster. Users in the telephony cluster will use this service profile to get IM and Presence services from the central cluster.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Service Profile**.

Step 2 Do one of the following:

a) Click **Find** and select an existing service profile to edit.
b) Click **Add New** to create a new service profile.

Step 3 In the **IM and Presence Profile** section, configure IM and Presence services that you configured in the previous task:

a) From the **Primary** drop-down, select the database publisher node service.
b) From the **Secondary** drop-down, select the subscriber node service.

Step 4 Click **Save**.

What to do next

Disable Presence Users in Telephony Cluster, on page 12

Disable Presence Users in Telephony Cluster

If you've already completed an LDAP sync in your telephony deployment, use the Bulk Administration Tool to edit user settings in the Telephony cluster for IM and Presence users. This configuration will point Presence users to the Central Cluster for the IM and Presence Service.

Note This procedure assumes that you have already completed an LDAP sync in your telephony cluster. However, if you haven't yet completed the initial LDAP sync, you can add the Central Deployment settings for Presence users into your initial sync. In this case, do the following in your telephony cluster:

- Configure a Feature Group Template that includes the **Service Profile** that you just set up. Make sure that have the **Home Cluster** option selected and the **Enable User for Unified CM IM and Presence** option unselected.
- In **LDAP Directory Configuration**, add the **Feature Group Template** to your LDAP Directory sync.
- Complete the initial sync.

For additional details on configuring Feature Group Templates and LDAP Directory, see the "Configure End Users" part of the *System Configuration Guide for Cisco Unified Communications Manager*.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Query** > **Bulk Administration** > **Users** > **Update Users** > **Query**.

Step 2 From the Filter, select **Has Home Cluster Enabled** and click **Find**. The window displays all of the end users for whom this is their Home Cluster.

Step 3 Click **Next**.
In the **Update Users Configuration** window, the check boxes on the far left indicate whether you want to edit this setting with this query. If you don't check the left check box, the query will not update that field. The field on the right indicates the new setting for this field. If two check boxes appear, you must check the check box on the left to update the field, and in the right check box, enter the new setting.

Step 4 Under **Service Settings**, check the far left check box for each of the following fields to indicate that you want to update these fields, and then edit the adjacent setting as follows:

- **Home Cluster**—Check the right check box to enable the telephony cluster as the home cluster.
- **Enable User for Unified CM IM and Presence**—Leave the right check box unchecked. This setting disables the telephony cluster as the provider of IM and Presence.
- **UC Service Profile**—From the drop-down, select the service profile that you configured in the previous task. This setting points users to the IM and Presence central cluster, which will be the provider of the IM and Presence Service.

Note For Expressway Mobile and Remote Access configuration, see *Mobile and Remote Access via Cisco Expressway Deployment Guide* at https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html.

Step 5 Complete any remaining fields that you want. For help with the fields and their settings, see the online help.

Step 6 Under **Job Information**, select **Run Immediately**.

Step 7 Click **Submit**.

What to do next

Configure OAuth Refresh Logins , on page 14

Configure OAuth Refresh Logins

Enable OAuth Refresh Logins in the telephony cluster. This will enable the feature in the central clsuter as well.

Procedure

Step 1 Log in to Cisco Unified CM Administration on the telephony cluster.

Step 2 Choose **System** > **Enterprise Parameters**.

Step 3 Under **SSO And OAuth Configuration,** set the **OAuth with Refresh Login Flow** enterprise parameter to **Enabled**.

Step 4 If you edited the parameter setting, click **Save**.

Note When OAuth keys are regenerated, you must restart the Cisco XCP Authentication Service on all IM and Presence nodes for Jabber OAuth login to work.

Configure an ILS Network

For IM and Presence centralized clusters where there are more than one remote telephony clusters, you can use the Intercluster Lookup Service (ILS) to provision remote telephony clusters for the IM and Presence central cluster. ILS monitors the network and propagates network changes such as new clusters or address changes to the entire network.

Note This task flow focuses on ILS requirements around IM and Presence centralized cluster deployments. For additional ILS configuration around telephony, such as configuring Global Dial Plan Replication or URI Dialing, see the "Configure the Dial Plan" section of the *System Configuration Guide for Cisco Unified Communications Manager*.

Before you begin

If you are deploying ILS, make sure that you have done the following:

- Plan your ILS network topology. You must know which telephony clusters will be hubs and spokes.
- The telephony cluster to which the IM and Presence central cluster connects must be a hub cluster.
- You must configure a DNS SRV record that points to the publisher node of the hub cluster.

For information on designing an ILS network, see the *Cisco Collaboration System Solution Reference Network Design* at http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-implementation-design-guides-list.html.

Procedure

	Command or Action	Purpose
Step 1	Configure Cluster IDs for ILS, on page 15	Set unique Cluster IDs for each telephony cluster. ILS will not work while the Cluster ID is set to `StandAloneCluster` (the default setting).
Step 2	Enable ILS on Telephony Clusters, on page 15	Configure and activate ILS on the publisher node of each telephony cluster in the ILS network.
Step 3	Verify ILS Network is Running, on page 17	When ILS is working, you can see all of your remote clusters from the **ILS Configuration** window of your telephony clusters with an "Up to Date" synchronization status.

Configure Cluster IDs for ILS

Each cluster within the ILS network must have a unique Cluster ID. Use this procedure to give your telephony clusters unique cluster IDs.

Procedure

Step 1 Log in to Cisco Unified CM Administration on the publisher node.

Step 2 Choose **System** > **Enterprise Parameters**.

Step 3 Change the value of the **Cluster ID** parameter from `StandAloneCluster` to a unique value that you set. ILS will not work while the Cluster ID is `StandAloneCluster`.

Step 4 Click **Save**.

Step 5 Repeat this procedure on the publisher node of each telephony cluster that you want to join into the ILS network. Each cluster must have a unique ID.

What to do next

Enable ILS on Telephony Clusters, on page 15

Enable ILS on Telephony Clusters

Use this procedure to configure and activate ILS on your Cisco Unified Communications Manager telephony clusters.

Note

- Configure your hub clusters before configuring your spoke clusters.
- For help with the fields and their settings, refer to the online help.

Before you begin

Configure Cluster IDs for ILS, on page 15

Procedure

Step 1 Log into Cisco Unified CM Administration on the publisher node of your telephony cluster.

Step 2 Choose **Advanced Features** > **ILS Configuration**.

Step 3 From the **Role** drop-down list box, select **Hub Cluster** or **Spoke Cluster** depending on which type of cluster you are setting up.

Step 4 Check the **Exchange Global Dial Plan Replication Data with Remote Clusters** check box.

Step 5 Configure **ILS Authentication Details**.

a) If you want to use TLS authentication between the various clusters, check the **Use TLS Certificates** check box.

Note If you use TLS, you must exchange CA-signed certificates between the nodes in your cluster.

b) If you want to use password authentication (regardless of whether TLS is used), check the **Use Password** check box and enter the password details.

Step 6 Click **Save**.

Step 7 In the **ILS Cluster Registration** popup, configure your registration details:

- In the **Registration Server** text box, enter the publisher node IP address or FQDN for the hub cluster to which you want to connect this cluster. If this is the first hub cluster in your network, you can leave the field blank.
- Make sure that the **Activate the Intercluster Lookup Service on the publisher in this cluster** check box is checked.

Step 8 Click **OK**.

Step 9 Repeat this procedure on the publisher node of each telephony cluster that you want to add to the ILS network. Depending on the sync values that you configured, there may be a delay while the cluster information propagates throughout the network.

If you chose to use Transport Layer Security (TLS) authentication between clusters, you must exchange Tomcat certificates between the publisher node of each cluster in the ILS network. From Cisco Unified Operating System Administration, use the Bulk Certificate Management feature to:

- Export certificates from the publisher node of each cluster to a central location
- Consolidate exported certificates in the ILS network
- Import certificates onto the publisher node of each cluster in your network

For details, see the "Manage Certificates" chapter of the *Administration Guide for Cisco Unified Communications Manager*.

What to do next

After ILS is up and running, and you have exchanged certificates (if required), Verify ILS Network is Running, on page 17

Verify ILS Network is Running

Use this procedure to confirm that your ILS network is up and running.

Procedure

Step 1 Log in to the publisher node on any of your telephony clusters.

Step 2 From Cisco Unified CM Administration choose **Advanced Features** > **ILS Configuration**.

Step 3 Check the **ILS Clusters and Global Dial Plan Imported Catalogs** section. Your ILS network topology should appear.

Mobile and Remote Access Configuration

Cisco Unified Communications Mobile and Remote Access is a core part of the Cisco Collaboration Edge Architecture. It allows endpoints such as Cisco Jabber to have their registration, call control, provisioning, messaging and presence services provided by Cisco Unified Communications Manager when the endpoint is not within the enterprise network. The Expressway provides secure firewall traversal and line-side support for Unified CM registrations.

The overall solution provides :

1. **Off-premises access** : A consistent experience outside the network for Jabber and EX/MX/SX series clients.
2. **Security** : Secure business-to-business communications.
3. **Cloud services** : Enterprise grade flexibility and scalable solutions providing rich WebEx integration and Service Provider offerings.
4. **Gateway and interoperability services** : Media and signalling normalization, and support for non-standard endpoints.

Configuration

To configure Mobile and Remote Access on all telephony leaf clusters in Expressway-C. Choose **Configuration → Unified Communications → Unified CM Servers**.

To configure Mobile and Remote Access on centralized IM&P nodes cluster in Expressway-C. Choose **Configuration→ Unified Communications → IM and Presence Service nodes**.

To Enable the **"Mobile and Remote Access"**in Expressway-C. Choose **Configuration → Enable "Mobile and Remote Access"** and select the control options as per the table below.

Table 2: OAuth Enable Configuration

Authentication path	UCM / LADP basic authentication
Authorize by OAuth token with refresh	ON
Authorize by OAuth token	ON
Authorize by user credentia	No

Allow Jabber iOS clients to use embedded Safari browser	No
Check for internal authentication availability	Yes

Table 3: OAuth Disable Configuration

Authentication path	UCM / LADP basic authentication
Authorize by OAuth token with refresh	Off
Authorize by user credentia	On
Allow Jabber iOS clients to use embedded Safari browser	Off
Check for internal authentication availability	Yes

Note **For Information on Basic Mobile and Remote Access Configuration , Please refer :** https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

Upgrades with IM and Presence Central Deployments Require a Resync

If you have an IM and Presence Centralized Deployment and you upgrade the IM and Presence central cluster, or any remote telephony peer clusters, you must resynchronize your clusters after the upgrade is completed. You can resync your clusters from the **Centralized Deployment** window of Cisco Unified CM IM and Presence Administration by selecting your cluster peers and clicking the **Save and Synchronize** button.

IM and Presence Centralized Cluster Setup with SSO Enabled Remote Telephony Clusters for Subdomains

In the IM and Presence centralized deployment, if your remote telephony clusters are having multiple sub-domains, you can enable SOAP login to the remote access client (for example, Jabber) with SSO enabled.

This section covers the steps to configure a subdomain user login to Jabber in the SSO enabled remote telephony clusters. Consider a centralized deployment scenario, which consists of a centralized cluster and an SSO enabled remote telephony cluster associated with that centralized cluster.

To set up SSO enabled login for subdomains, complete the following steps:

Procedure

Step 1 Log in to the Cisco Unified CM Administration and do the following:

a) Synchronize users from LDAP to the leaf nodes and set the **Directory URI** field to **Mail ID** and SSO enabled. To know how to synchronize LDAP users, see LDAP Synchronization .
b) Synchronize the same users to the remote telephony node and set the **Directory URI** field to **Mail ID**.
c) In the **End User Configuration** page (**End Users** > **End User Management**), check the **Enable Users for Cisco Unified IM and Presence Service (Configure IM and Presence in the associated UC Service Profile)** option under **Service Settings** for the IM and Presence nodes to have the same users as in the centralized cluster.
d) In the **End User Configuration** page (**End Users** > **End User Management**), add users to the Cisco Call Manager (CCM) End Users Group using the **Permission Information** section.
e) Disable users for IM and Presence on the remote telephony cluster. To do this, uncheck the **Enable Users for Cisco Unified IM and Presence Service (Configure IM and Presence in the associated UC Service Profile)** option under **ServiceSettings**
f) Create the UC Service on the central cluster for the remote telephony cluster (**User Management** > **User Settings** > **UC Service Configuration**).
g) Create the service profile on central cluster and set this as the default service profile for the system and add the IM and Presence nodes to the IM and Presence Profile (**User Management** > **User Settings** > **Service Profile**).
h) Enable **OAuth with Refresh Login Flow** on the central cluster. In the **Enterprise Parameter Configuration** page, set the **OAuth with Refresh Login Flow** parameter to **Enabled**.

Step 2 Log in to the Cisco Unified IM and Presence Administration console and add the leaf node to the IM and Presence Service node (**System** > **Centralized Deployment**).

Integrate Phone Presence in Centralized Deployment

In the centralized deployment, you can get the phone presence information from a remote Unified CM cluster by configuring multiple SIP Trunks in the centralized IM and Presence node.

Unlike in the standard deployment where you can configure only one Unified CM cluster as the presence gateway, the system derestricts this limitation in the centralized deployment. It allows the administrators to add multiple CUCM clusters as presence gateways in the IM and Presence node. This helps get the phone presence information from the remote Unified CM clusters.

The following procedure provides steps to configure SIP trunks and other additional settings in the remote Cisco Unified CM clusters and the corresponding IM and Presence node.

Procedure

Step 1 From the **Cisco Unified CM Administration** user interface, do the following:

a) Choose **Device** > **Trunk**. Add a new SIP Trunk and point it to the IM and Presence publisher node as a leaf cluster.
b) Choose **System** > **Service Parameter Configuration**, choose **Call Manager**. In the **IM and Presence Publish Trunk** field, enter the IP address of the leaf cluster trunk that you added in the previous step.
c) Enable presence for all users available in the cluster. You can set the **Enable user for Unified CM IM and Presence (Configure IM and Presence in the associated UC service profile)** checkbox for all users in the **End User Configuration** page in one attempt using a BAT file in the backend.

Step 2 From **Cisco Unified CM IM and Presence Administration**, do the following:

a) In the **Cisco Unified CM IM and Presence Administration** user interface, choose **Presence** > **Presence Gateway** and select the IP address of the remote CUCM cluster from the drop-down list.

Note Ensure that you delete the remote Unified CM cluster from the **Presence Gateway Configuration** window, before deleting it form the **Centralized Deployment Page**.

To update the Remote CUCM cluster address in the **Centralized Deployment Page**, you need to:

- Delete the remote Unified CM cluster from the **Presence Gateway Configuration** window.
- Edit the CUCM address on the **Centralized Deployment Page.**

  .
- Re-add the Unified CM cluster in the **Presence Gateway Configuration** window.

b) Choose **System** > **Security** > **Incoming ACL** and create a new ACL by adding the IP address of the remote Cisco Unified CM.

Important This note is applicable for release 14SU1 onwards.

Note Create a new Incoming ACL by adding the IP address of all the remote Cisco Unified CM publisher and subscriber nodes from where IM and Presence is expecting publish SIP messages.

c) Choose **System** > **Security** > **TLS Peer Subject** and add the IP address of the remote Cisco Unified CM.

Important This note is applicable for release 14SU1 onwards.

Note Create a TLS Peer Subject and add the IP address of all the remote Cisco Unified CM publisher and subscriber nodes from where IM and Presence is expecting publish SIP messages.

d) Choose **System** > **Security** > **TLS Context Configuration**. In the **TLS Peer Subject Mapping** section, select the TLS Peer Subject created for the remote Cisco Unified CM in the previous step from the **Available TLS Peer Subject** box and move it to the **Selected TLS Peer Subject** box.

Step 3 Restart the **Cisco OAMAgent** on all cluster nodes.

Step 4 Restart the **Cisco Presence Engine**.

Note In the IM and Presence Service centralized deployment, you can change the Cisco Jabber status to **Do Not Disturb (DND)**. The same status is reflected on the controlled Cisco IP Phone and Jabber device. However, the DND status change doesn't reflect in case of shared line, where more than one device is configured with the same directory number (DN) in a centralized deployment.

Centralized Deployment Interactions and Restrictions

Feature	Interaction
ILS Hub Cluster	If the ILS hub cluster is down, and more than one telephony cluster exists, the Central Cluster feature does not work.

Feature	Interaction
ILS Deployments	If you are deplying an IM and Presence central cluster and you are also deploying ILS, you can deploy ILS in the telephony clusters only. You cannot deploy ILS on the Cisco Unified Communications Manager instance for the IM and Presence central cluster. This instance is for provisioning only and does not handle telephony.
Rich Presence	In a Centralized deployment, users' rich presence is computed by Cisco Jabber. Users' telephony presence is displayed only when if the user is logged in to Jabber.
Unified Communications Manager Cluster Status	In a centralized deployment, the Unified Communications Manager cluster status appears as**Synchronized for OAuth Refresh Logins**. This feature is available from 11.5(1)SU3 onwards. When you add a Unified Communications Manager cluster to 11.5(1)SU3 or earlier release, the cluster status appears as Unsynchronized under Cisco Unified CM IM and Presence Administration, **System** > **Centralized Deployment** as it does not support OAuth Refresh Logins. Whereas these clusters are compatible for centralized IM and Presence Service deployment using SSO or LDAP directory credentials. **Note** There is no functional impact on Cisco Jabber user login.