Configure Cisco Unified Communications Manager for IM and Presence Service

Integration Overview

This section details the tasks that you should have completed on Cisco Unified Communications Manager in order to complete configuration on IM and Presence Service.

Cisco Unified Communications Manager Integration Prerequisites

Before you configure the IM and Presence Service to integrate with Cisco Unified Communications Manager, make sure that you complete the following general configuration tasks on Cisco Unified Communications Manager. For details on how to configure Cisco Unified Communications Manager, refer to the *System Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

The table below lists essential configuration tasks for IM and Presence Service integration. Refer to the online help for descriptions of fields and their options.

Table 1: Required Configuration on Cisco Unified Communications Manager

Task	Description
Modify the User Credential Policy	We recommend that you set an expiration date on the credential policy for users. The only type of user that does not require a credential policy expiration date is an Application user. Cisco Unified Communications Manager does not use the credential policy if you are using an LDAP server to authenticate your users on Cisco Unified Communications Manager. **Cisco Unified CM Administration** > **User Management** > **User Settings** > **Credential Policy Default**
Configure the phone devices, and associate a Directory Number (DN) with each device	Enable **Allow Control of Device from CTI** to allow the phone to interoperate with the client. **Cisco Unified CM Administration** > **Device** > **Phone**
Configure the users, and associate a device with each user	Ensure that the user ID value is unique for each user. **Cisco Unified CM Administration** > **User Management** > **End User**
Associate a user with a line appearance	For details, see: **Cisco Unified CM Administration** > **Device** > **Phone**
Add users to CTI-enabled user group	To enable desk phone control, you must add the users to a CTI-enabled user group. **Cisco Unified CM Administration** > **User Management** > **User Group**
Certificate exchange	The certificate exchange between Cisco Unified Communications Manager and the IM and Presence Service is handled automatically during the installation process. However, if there is an issue and you need to complete the certificate exchange manually, refer to Certificate Exchange with Cisco Unified Communications Manager.

Note If Cisco Unified Communications Manager Tomcat certificates that you upload to the IM and Presence Service contain hostnames in the SAN field, all of them should be resolvable from the IM and Presence Service. The IM and Presence Service must be able to resolve the hostname via DNS or the Cisco Sync Agent service will not start. This is true regardless of whether you use a hostname, IP Address, or FQDN for the Node Name of the Cisco Unified Communications Manager server.

SIP Trunk Configuration on Cisco Unified Communications Manager

Complete these tasks to configure the SIP trunk connection to Cisco Unified Communications Manager.

Procedure

	Command or Action	Purpose
Step 1	Configure a SIP Trunk Security Profile, on page 3	Configure a SIP Trunk Security Profile for the trunk connection between Cisco Unified Communications Manager and the IM and Presence Service.
Step 2	Configure SIP Trunk for IM and Presence Service, on page 4	Assign the SIP Trunk Security Profile to a SIP trunk and configure the trunk connection between Cisco Unified Communications Manager and IM and Presence Service.
Step 3	Configure SRV Cluster Name, on page 5	Optional. Complete this procedure only if you are using DNS SRVs on the SIP trunk between Cisco Unified Communications Manager and the IM and Presence Service and you use an SRV address other than the IM and Presence default domain. In this case, configure the **SRV Cluster Name** service parameter. Otherwise, you can skip this task.
Step 4	Configure the Presence Gateway, on page 6	On the IM and Presence Service, assign Cisco Unified Communications Manager as a presence gateway, thereby allowing the systems to exchange Presence information.
Step 5	Configure a SIP PUBLISH Trunk, on page 6	Optional. Use this procedure to configure a SIP PUBLISH trunk for IM and Presence. When you turn on this setting, Cisco Unified Communications Manager publishes phone presence for all line appearances that are associated with users licensed on Cisco Unified Communications Manager for the IM and Presence Service.
Step 6	Verify Services on Cisco Unified Communications Manager, on page 7	Verify that required services are running on Cisco Unified Communications Manager.
Step 7	Configure Phone Presence from Off-Cluster Cisco Unified Communications Manager, on page 7	Configure Cisco Unified Communications Manager as a TLS Peer subject of the IM and Presence Service. TLS is required if you want to allow phone presence from a Cisco Unified Communications Manager that is outside of the IM and Presence Service cluster.

Configure a SIP Trunk Security Profile

On Cisco Unified Communications Manager, configure a SIP Trunk Security Profile for the trunk connection with the IM and Presence Service.

Procedure

Step 1 In **Cisco Unified CM Administration** > **System** > **Security** > **SIP Trunk Security Profile**, click **Find**.

Step 2 Click **Non Secure SIP Trunk Profile**.

Step 3 Click **Copy**.

Step 4 Enter a **Name** for the profile. For example, `IMP-SIP-Trunk-Profile`.

Step 5 Complete the following settings:

- The **Device Security Mode** is set to **Non Secure**.
- The**Incoming Transport Type** is set to **TCP+UDP**.
- The**Outgoing Transport Type** is set to **TCP**.

Step 6 Check the following check boxes:

- **Accept Presence Subscription**
- **Accept Out-of-Dialog REFER**
- **Accept Unsolicited Notification**
- **Accept Replaces Header**

Step 7 Click **Save**.

What to do next

Configure SIP Trunk for IM and Presence Service, on page 4

Configure SIP Trunk for IM and Presence Service

Set up the SIP trunk connection between Cisco Unified Communications Manager and the IM and Presence Service cluster.

Before you begin

Configure a SIP Trunk Security Profile, on page 3

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Trunk**

Step 2 Click **Add New**.

Step 3 From the **Trunk Type** drop-down list box, choose **SIP Trunk**.

Step 4 From the **Device Protocol** drop-down list box, choose **SIP**.

Step 5 From the **Trunk Service Type** drop-down list box, choose **None**.

Step 6 Click **Next**.

Step 7 In the **Device Name** field, enter a name for the trunk. For example, `IMP-SIP-Trunk`.

Step 8 Select a **Device Pool** from the drop-down list box.

Step 9 In the **SIP Information** section, assign the trunk to the IM and Presence Service by entering the address information for the IM and Presence cluster:

- If you are using a DNS SRV record for the IM and Presence Service, check the **Destination Address is an SRV** check box and enter the SRV in the **Destination Address** field.
- Otherwise, in the **Destination Address** field, enter the IP address or FQDN of the IM and Presence publisher node. Click the **(+)** button to add additional nodes. You can enter up to 16 nodes.

a) In the **Destination Address** field, enter the IP Address, FQDN, or DNS SRV of the IM and Presence node.

b) Check the **Destination Address is an SRV** if you are configuring a multinode deployment.

In this scenario, Cisco Unified Communications Manager performs a DNS SRV record query to resolve the name, for example `_sip._tcp.hostname.tld_sip._tcp.hostname.tld`. If you are configuring a single-node deployment, leave this checkbox unchecked and Cisco Unified Communications Manager will perform a DNS A record query to resolve the name, for example `hostname.tld`.

Cisco recommends that you use the IM and Presence Service default domain as the destination address of the DNS SRV record.

Note You can specify any domain value as the destination address of the DNS SRV record. No users need to be assigned to the domain that is specified. If the domain value that you enter differs from the IM and Presence Service default domain, you must ensure that the SIP Proxy Service Parameter called SRV Cluster Name on IM and Presence Service matches the domain value that you specify in the DNS SRV record. If you use the default domain, then no changes are required to the SRV Cluster Name parameter.

In both scenarios, the Cisco Unified Communications SIP trunk Destination Address must resolve by DNS and match the SRV Cluster Name configured on the IM and Presence node.

Step 10 For the **Destination Port**, enter `5060`

Step 11 From the **SIP Trunk Security Profile** drop-down list box, choose the SIP trunk security profile that you created in the previous task.

Step 12 From the **SIP Profile** drop-down list box, choose a profile. for example, the **Standard SIP Profile**

Step 13 Click **Save**.

What to do next

If you are using DNS SRVs on the SIP trunk between Cisco Unified Communications Manager and the IM and Presence Service and you use an address other than the IM and Presence default domain, Configure SRV Cluster Name, on page 5.

Otherwise, Configure a SIP PUBLISH Trunk, on page 6.

Configure SRV Cluster Name

If you are using DNS SRVs on the SIP trunk between Cisco Unified Communications Manager and the IM and Presence Service and you use an address other than the IM and Presence default domain, configure the **SRV Cluster Name** service parameter. Otherwise, you can skip this task.

Procedure

Step 1 From Cisco Unified CM IM and Presence Serviceability, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down menu, select the IM and Presence publisher node and click **Go**.

Step 3 From the **Service** drop-down, select the **Cisco SIP Proxy** service.

Step 4 In the **SRV Cluster Name** field, enter the SRV address.

Step 5 Click **Save**.

Configure a SIP PUBLISH Trunk

Use this optional procedure to configure a SIP PUBLISH trunk for IM and Presence. When you turn on this setting, Cisco Unified Communications Manager publishes phone presence for all line appearances that are associated with users licensed on Cisco Unified Communications Manager for the IM and Presence Service.

Procedure

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Presence** > **Settings** > **Standard Configuration**.

Step 2 From the **CUCM IM and Presence Publish Trunk** drop-down, select the SIP trunk that you configured on Cisco Unified Communications Manager for the IM and Presence Service.

Step 3 Click **Save**.

Note When you save this new setting, the **IM and Presence Publish Trunk** service parameter in Cisco Unified Communications Manager also updates with this new setting.

What to do next

Verify Services on Cisco Unified Communications Manager, on page 7

Configure the Presence Gateway

Use this procedure on the IM and Presence Service to assign Cisco Unified Communications Manager as a presence gateway. This configuration enables the presence information exchange between Cisco Unified Communications Manager and the IM and Presence Service.

Procedure

Step 1 From **Cisco Unified CM IM and Presence Administration** > **Presence** > **Gateways**.

Step 2 Click **Add New**.

Step 3 From the **Presence Gateway** drop-down list box, choose **CUCM**.

Step 4 Enter a **Description**.

Step 5 In the **Presence Gateway** field, enter one of the following options:

- IP address or FQDN of the Cisco Unified Communications Manager publisher node
- DNS SRV that resolves to the Cisco Unified Communications Manager subscriber nodes

Step 6 Click **Save**.

What to do next

Configure a SIP PUBLISH Trunk, on page 6

Verify Services on Cisco Unified Communications Manager

Use this procedure to verify that required services are running on Cisco Unified Communications Manager nodes.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Control Center - Feature Services**.

Step 2 From the **Server** menu, choose Cisco Unified Communications Manager cluster node and click **Go**.

Step 3 Make sure that the following services are running. If they are not running, start them.

- Cisco CallManager
- Cisco TFTP
- Cisco CTIManager
- Cisco AXL Web Service (for data synchronization between IM and Presence and Cisco Unified Communications Manager)

Step 4 If any of the above services are not running, select the service and click **Start**.

Configure Phone Presence from Off-Cluster Cisco Unified Communications Manager

You can allow phone presence from a Cisco Unified Communications Manager that is outside of the IM and Presence Service cluster. However, in order for the IM and Presence Service to accept a SIP PUBLISH from a Cisco Unified Communications Manager outside of its cluster, the Cisco Unified Communications Manager needs to be listed as a TLS Trusted Peer of the IM and Presence

Procedure

	Command or Action	Purpose
Step 1	Add Cisco Unified Communications Manager as TLS Peer, on page 8	Add Cisco Unified Communications Manager as a TLS peer of the IM and Presence Service.

	Command or Action	Purpose
Step 2	Configure a TLS Context for Unified Communications Manager, on page 8	Add the Cisco Unified Communications Manager TLS poeer

Add Cisco Unified Communications Manager as TLS Peer

In order for the IM and Presence Service to accept a SIP PUBLISH from a Cisco Unified Communications Manager outside of its cluster, the Cisco Unified Communications Manager needs to be listed as a TLS Trusted Peer of the IM and Presence Service.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration** > **System** > **Security** > **TLS Peer Subjects**, click **Add New**.

Step 2 Enter the IP Address of the external Cisco Unified Communications Manager in the **Peer Subject Name** field.

Step 3 Enter the name of the node in the **Description** field.

Step 4 Click **Save**.

What to do next

Configure TLS Context

Configure a TLS Context for Unified Communications Manager

Use the following procedure to add the Cisco Unified Communications Manager TLS peer that you configured in the previous task to a selected TLS peer.

Before you begin

Add Cisco Unified Communications Manager as TLS Peer, on page 8

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration** > **System** > **Security** > **TLS Context Configuration**, click **Find**.

Step 2 Click **Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context**.

Step 3 From the list of available TLS peer subjects, choose the TLS peer subject that you configured for Cisco Unified Communications Manager.

Step 4 Move this TLS peer subject to Selected TLS Peer Subjects.

Step 5 Click **Save**.

Step 6 Restart the Cisco OAMAgent on all cluster nodes:

a) From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**.

b) From the **Server** drop-down list box, choose the IM and Presence server and click **Go**

c) Under **IM and Presence Services**, select **Cisco OAMAgent** and click **Restart**.
d) Restart the service on all cluster nodes.

Step 7 After the OAM Agent restarts, restart the Cisco Presence Engine.

a) Choose **Tools** > **Control Center - Feature Services**.
b) From the **Server** drop-down list box, choose the IM and Presence node and click **Go**.
c) Under **IM and Presence Services**, select **Cisco Presence Engine** and click **Restart**.
d) Restart the service on all cluster nodes.

What to do next

Verify Services on Cisco Unified Communications Manager, on page 7