Cisco Unified Communications Manager configuration for integration with IM and Presence Service

User and Device Configuration on Cisco Unified Communications Manager before Integration Task List

Before you configure Cisco Unified Communications Manager for integration with the IM and Presence Service, make sure that the following user and device configuration is completed on Cisco Unified Communications Manager.

Table 1: Task List to Configure Users and Devices on Cisco Unified Communications Manager Before Integration with IM and Presence Service

Task	Description
Modify the User Credential Policy	This procedure is applicable only if you are integrating with Cisco Unified Communications Manager Release 6.0 or later. Cisco recommends 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** > **Credential Policy Default**
Configure the phone devices, and associate a Directory Number (DN) with each device	Check **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	This procedure is applicable only to Cisco Unified Communications Manager Release 6.0 or later. **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**
(Optional) Set directoryURI value for users	If the IM and Presence Service nodes are using the Directory URI IM address scheme, you must set the directoryURI value for the users. The user's Directory URI value can either be synchronized to the Cisco Unified Communications Manager LDAP Directory or manually updated. See the *Cisco Unified Communications Manager Administration Guide* for instructions to enable LDAP or to edit the Directory URI value manually for the user if LDAP is not enabled.

Note Because menu options and parameters may vary by Cisco Unified Communications Manager releases, see the Cisco Unified Communications Manager documentation that applies to your release.

Related Topics

LDAP Directory Integration

Configure Inter-Presence Group Subscription Parameter

You enable the Inter-Presence Group Subscription parameter to allow users in one Presence Group to subscribe to the availability information for users in a different presence group.

Restriction

You can only enable the Inter-Presence Group Subscription parameter when the subscription permission for the default Standard Presence Group, or any new Presence Groups, is set to **Use System Default**. To configure Presence Groups, choose **Cisco Unified CM Administration** > **System** > **Presence Groups**.

Procedure

Step 1 Choose **Cisco Unified CM Administration** > **System** > **Service Parameters**.

Step 2 Choose a Cisco Unified Communications Manager node from the Server menu.

Step 3 Choose **Cisco CallManager** from the Service menu.

Step 4 Choose **Allow Subscription** for Default Inter-Presence Group Subscription in the Clusterwide Parameters (System - Presence) section.

Step 5 Click **Save**.

Tip You no longer have to manually add the IM and Presence Service as an Application Server on Cisco Unified Communications Manager:

What to do next

Proceed to configure a SIP trunk on Cisco Unified Communications Manager.

SIP Trunk Configuration on Cisco Unified Communications Manager

The port number that you configure for the SIP Trunk differs depending on the version of the IM and Presence Service that you are deploying. For IM and Presence Service release 9.0(x) and later, configure the port number 5060 for the SIP Trunk.

Configure SIP Trunk Security Profile for IM and Presence Service

Procedure

Step 1 Choose **Cisco Unified CM Administration** > **System** > **Security** > **SIP Trunk Security Profile**.

Step 2 Click **Find.**

Step 3 Click **Non Secure SIP Trunk Profile**.

Step 4 Click **Copy** and enter CUP Trunk in the **Name** field.

Step 5 Verify that the setting for Device Security Mode is **Non Secure**.

Step 6 Verify that the setting for Incoming Transport Type is **TCP+UDP**.

Step 7 Verify that the setting for Outgoing Transport Type is **TCP**.

Step 8 Check to enable these items:

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

Step 9 Click **Save**.

What to do next

Proceed to configure the SIP trunk on Cisco Unified Communication Manager

Configure SIP Trunk for IM and Presence Service

You only configure one SIP trunk between a Cisco Unified Communications Manager cluster and an IM and Presence Service cluster. After you configure the SIP trunk, you must assign that SIP trunk as the IM and Presence PUBLISH Trunk on Cisco Unified Communications Manager by choosing **Cisco Unified CM Administration** > **System** > **Service Parameters**.

In the Destination Address field, enter a value using one of the following formats:

- Dotted IP Address
- Fully Qualified Domain Name (FQDN)
- DNS SRV

If high availability is configured for the IM and Presence cluster, multiple entries should be entered in the Dotted IP Address or FQDN to identify the various nodes in the cluster. DNS SRV cannot be used for an IM and Presence cluster if high availability is configured.

Before you begin

- Configure the SIP Trunk security profile on Cisco Unified Communications Manager.

- Read the Presence Gateway configuration options topic.

Procedure

Step 1 Choose **Cisco Unified CM Administration** > **Device** > **Trunk**.

Step 2 Click **Add New**.

Step 3 Choose **SIP Trunk** from the Trunk Type menu.

Step 4 Choose **SIP** from the Device Protocol menu.

Step 5 Choose **None** for the Trunk Service Type.

Step 6 Click **Next**.

Step 7 Enter **CUPS-SIP-Trunk** for the Device Name.

Step 8 Choose a device pool from the Device Pool menu.

Step 9 In the SIP Information section at the bottom of the window, configure the following values:

a) In the Destination Address field, enter the Dotted IP Address, or the FQDN, which can be resolved by DNS and must match the SRV Cluster Name configured on 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*. 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.

c) Enter `5060` for the Destination Port.

d) Choose **Non Secure SIP Trunk Profile** from the SIP Trunk Security Profile menu.

e) Choose **Standard SIP Profile** from the SIP Profile menu.

Step 10 Click **Save**.

Troubleshooting Tip

If you modify the DNS entry of the Publish SIP Trunk SRV record by changing the port number or IP address, you must restart all devices that previously published to that address and ensure each device points to the correct IM and Presence Service contact.

Related Topics

Configure Cluster-Wide DNS SRV Name for SIP Publish Trunk

Configure SIP Trunk Security Profile for IM and Presence Service, on page 4
Configure SIP Publish Trunk on IM and Presence Service
Presence Gateway Configuration Option

Configure Phone Presence for Unified Communications Manager Outside of Cluster

You can allow phone presence from a Cisco Unified Communications Manager that is outside of the IM and Presence Service cluster. Default requests from a Cisco Unified Communications Manager that is outside of the cluster will not be accepted by IM and Presence Service. You can also configure a SIP Trunk on Cisco Unified Communications Manager.

You must configure the TLS context before you configure the TLS peer subject.

Configure TLS Peer Subject

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 Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Security** > **TLS Peer Subjects**.

Step 2 Click **Add New**.

Step 3 Enter the IP Address of the external Cisco Unified Communications Manager in the **Peer Subject Name** field.

Step 4 Enter the name of the node in the **Description** field.

Step 5 Click **Save**.

What to do next

Configure the TLS context.

Configure TLS Context

Use the following procedure to configure TLS context.

Before you begin

Configure the TLS peer subject.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence AdministrationSystemSecurityTLS Context Configuration**.

Step 2 Click **Find**.

Step 3 Click **Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context**.

Step 4 From the list of available TLS peer subjects, choose the TLS peer subject that you configured.

Step 5 Move this TLS peer subject to Selected TLS Peer Subjects.

Step 6 Click **Save**.

Step 7 Restart the OAMAgent.

Step 8 Restart the Cisco Presence Engine.

Tip You must restart in this order for the changes to take effect.

Verify Required Services Are Running on Cisco Unified Communications Manager

You can view, start, and stop Cisco Unified Communications Manager services from a Cisco Unified Communications Manager node or an IM and Presence Service node. The following procedure provides steps to follow on a Cisco Unified Communications Manager node. To view Cisco Unified Communications Manager services from an IM and Presence Service node, choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Service Activation**.

Procedure

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

Step 2 Choose a Cisco Unified Communications Manager node from the Server menu.

Step 3 Make sure that the following services are running:

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

Tip To turn on a service on Cisco Unified Communications Manager, choose **Cisco Unified Serviceability** > **Tools** > **Service Activation.**