Main page: Cisco Unified Presence, Release 7.x

Contents

Previous Topic

- Configuring the Cisco Unified Personal Communicator Client

- TFTP Server Connection

- Deskphone Control and LDAP TelephoneNumber Field

- Configuring the Proxy Listener and TFTP Addresses (required)

- Configuring the Service Parameter for Cisco Unified Personal Communicator (required)

- Configuring a Secure Connection Between Cisco Unified Presence and Cisco Unified Personal Communicator

- How to Configure CTI Gateway Settings for Desk Phone Control (required)

TFTP Server Connection

Cisco Unified Personal Communicator connects to the primary Trivial File Transfer Protocol (TFTP) server (whose address is retrieved from Cisco Unified Presence) at startup, for suspend and resume operations, and for the re-establishment of dropped network connections. When the connection is established, Cisco Unified Personal Communicator downloads the UPC<*username*>.cnf.xml configuration file from Cisco Unified Communications Manager for each user.

The configuration file contains the list of Cisco Unified Communications Manager primary and failover server addresses and the transport protocol for Cisco Unified Personal Communicator to use in softphone mode to connect to Cisco Unified Communications Manager.

After Cisco Unified Personal Communicator downloads the file successfully, the configuration information is made available to other Cisco Unified Personal Communicator subsystems, and Cisco Unified Personal Communicator disconnects from the TFTP server.

Each time Cisco Unified Personal Communicator tries to download the configuration file, the application attempts to contact the primary TFTP server. If the primary TFTP server does not respond, Cisco Unified Personal Communicator fails over to the backup TFTP servers, if any exist. Cisco Unified Personal Communicator fails over to the backup TFTP servers in the order specified in Cisco Unified Presence Administration,.

If all TFTP server connections fail, Cisco Unified Personal Communicator tries to load the last valid downloaded configuration from the following locations:

- For Windows XP: *drive*:\Documents and Settings*username*\Application Data\Cisco\Unified Personal Communicator
- For Windows Vista: *drive*:\Users*username*\AppData\Local\Cisco\Unified Personal Communicator

If the loading of the local file is successful, Cisco Unified Personal Communicator updates the Server Health window with a warning notification (yellow indicator). If the file transfer fails and the file does not exist, Cisco Unified Personal Communicator updates the Server Health window with a failure notification and switches to *Disabled* mode.

The following Cisco Unified Communications Manager failover restrictions apply to Cisco Unified Personal Communicator:

- Auto-registration is not supported.

- Cisco Unified Personal Communicator fails over to a configured TFTP server when it tries to download the configuration file. The application also tries to download the file from the backup TFTP servers.
- AutoUpdate and upgrades through TFTP are not supported for Cisco Unified Personal Communicator software.

Related Topics

- Configuring the Proxy Listener and TFTP Addresses
- Getting More Information

Deskphone Control and LDAP TelephoneNumber Field

You may need to index the telephoneNumber field on the LDAP server for deskphone control to work. There are two possible scenarios that this applies to:

- Deskphone control is not working, and the server health on Cisco Unified Personal Communicator displays the status "Not Connected - Stopped".
- The contact search on Cisco Unified Personal Communicator does not return the full results.

These issues could occur when you have a large Cisco Unified Personal Communicator user base, and the LDAP server is slow to respondto queries from Cisco Unified Presence. To fix the issue, index the telephoneNumber field on the LDAP server. Alternatively, if you use Windows Active Directory, change the Global Catalog port to 3268 (instead of using the standard LDAP port 389).

Configuring the Proxy Listener and TFTP Addresses

Before You Begin

- Read the TFTP server connection topic.
- Obtain the hostnames or IP addresses of the TFTP servers.

Restriction

We recommend that Cisco Unified Personal Communicator use TCP to communicate with the proxy server. If you use UDP to communicate with the proxy server, availability information for contacts in the Cisco Unified Personal Communicator contact list might not be available for large contact lists.

Procedure

1. Select **Cisco Unified Presence Administration > Application > Cisco Unified Personal Communicator > Settings**.
2. Select the Proxy Listener **Default Cisco SIP Proxy TCP Listener**.
3. Assign the primary (required) and backup (optional) TFTP server addresses in the fields provided. You can enter an IP address or an FQDN (Fully Qualified Domain Name).
4. Select **Save**.

Troubleshooting Tip

You can see the TFTP server addresses in the Server Health window in Cisco Unified Personal Communicator (**Help > Show Server Health** on Windows operating system).

Related Topics

- TFTP Server Connection
- Getting More Information

What To Do Next

Configuring the Service Parameter for Cisco Unified Personal Communicator

Configuring the Service Parameter for Cisco Unified Personal Communicator

You need to configure all the availability-related messages sent between Cisco Unified Personal Communicator and Cisco Unified Presence use TCP.

Procedure

1. Select **Cisco Unified Presence Administration > System > Service Parameters**.
2. Select a **Cisco Unified Presence** server from the Server menu.
3. Select **Cisco UP SIP Proxy** as the service on the Service Parameter Configuration window.
4. Set **Use Transport in Record-Route Header** to **On** in the SIP Parameters (Clusterwide) section.
   This forces the Proxy to use the transport parameter in the record-route header.
5. Select **Save**.

Related Topics

- Configuring the Proxy Listener and TFTP Addresses
- Getting More Information

What To Do Next

Configuring a Secure Connection Between Cisco Unified Presence and Cisco Unified Personal Communicator

Configuring a Secure Connection Between Cisco Unified Presence and Cisco Unified Personal Communicator

If you want to exchange a CA-signed certificate between Cisco Unified Presence and Cisco Unified Personal Communicator ,you must generate a Certificate Signing Request (CSR) and import a tomcat certificate for Cisco Unified Presence. Refer to the steps below for a high level overview of this process.

Cisco Unified Personal Communicator uses the certificate called **tomcat**. The trust chain for this certificate is called **tomcat-trust**. Note: There can only be one tomcat certificate, but there can be more than one tomcat-trust.

Procedure

1. Select **Cisco Unified OS Administration > Security > Certificate Management**.

2. Select **Find** to list all certificates.

3. Select the tomcat certificate.

4. Select **Generate CSR**.

5. Send the CSR to your certificate authority.

6. Upload the signing chain of the certificate one at a time as 'tomcat-trust' on Cisco Unified Presence. You will need to do this before you upload the signed certificate that your CA returns to you. If you receive a Geotrust (Equifax) or Verisign certificate, you just need to upload the appropriate root certificate.

7. When the CA returns your signed certificate, select **Cisco Unified OS Administration > Security > Certificate Management > Upload Certificate** to upload the signed certificate to Cisco Unified Presence.

8. Upload the resulting certificate as "tomcat." Make sure to save this certificate file. List the name of your signing certificate as the 'Root Certificate'.

9. Restart the Tomcat service from the CLI using this command:

```
utils service restart Cisco Tomcat
```

The new certificate is not valid until you restart the Tomcat service.

Troubleshooting Tips

- When you generate the CSR, we recommend that you backup your system using the Disaster Recovery System on Cisco Unified Presence. If you do not backup your system, and if you regenerate the tomcat certificate, you will invalidate your signing chain and you will no longer be able to use your signed certificate.
- If you have an internal CA, in a signing chain, there will be at least a trusted root certificate. The trusted root certificate may sign an intermediate certificate, or it may sign your certificate directly. If there is an intermediate certificate, then it will sign your certificate. The root and the intermediate certificate make up the "signing chain." You need to upload each of the certificates in the chain to Cisco Unified Presence. In each case, upload it as "tomcat-trust."
- Do not attempt to upload a PKCS#7 (concatenated certificate chain), sometimes called a 'p7b'.
- You should only upload public keys. Do not upload a PKCS#12.

What To Do Next

How to Configure CTI Gateway Settings for Desk Phone Control

How to Configure CTI Gateway Settings for Desk Phone Control

Note: The procedures in this topic are only applicable if you are configuring Cisco Unified Personal Communicator for desk phone control.

Desk Phone Control and the CTI Connection Failures

The CTI gateway provides desk phone control (phone-association mode) to Cisco Unified Personal Communicator users. You must specify CTI gateway server names, addresses, ports, and protocol types on Cisco Unified Presence so that the information required to reach the CTI gateway server can be downloaded when the user logs in to Cisco Unified Personal Communicator.

If the CTI connection to Cisco Unified Communications Manager is lost while Cisco Unified Personal Communicator is operating in desk phone mode, the application tries to reestablish the connection to the primary and then to the backup servers. Connection attempts continue on a round-robin basis, beginning again with the primary server. Successive attempts to reconnect to a server occur at intervals of 4, 8, 16, 32, and 60 seconds (maximum) until a connection is re-established.

Scenario	Expected Recovery Behavior
CTI connection fails and no calls are present	• Cisco Unified Personal Communicator attempts to reconnect to the next available CTI server.

	• Until a connection is established, the Cisco Unified Personal Communicator user cannot initiate any new calls through the application. No new incoming call notifications are provided through the application.* The user has manual control of the desk phone for making and receiving calls. • When Cisco Unified Personal Communicator reconnects to one of the CTI servers, Cisco Unified Personal Communicator users again have the ability to control and monitor new calls through the application.
CTI connection fails with one or more calls present	• Cisco Unified Personal Communicator attempts to reconnect to the next available CTI server. • Existing calls are unaffected, but the user no longer has control through Cisco Unified Personal Communicator and does not receive any updates or changes in the call state. Any existing Cisco Unified Personal Communicator session window closes.* The user has manual control of the physical phone for making and receiving calls. • When Cisco Unified Personal Communicator reconnects to one of the CTI servers, it opens a new session window for each call and shows the current state. • Cisco Unified Personal Communicator remains connected to the current server (whether primary or backup) until the user relaunches Cisco Unified Personal Communicator or when a connection failure causes it to reconnect.

Related Topics

- Configuring CTI Gateway Server Names and Addresses
- Getting More Information

Configuring CTI Gateway Server Names and Addresses

You do not need to perform this procedure if you previously configured Cisco Unified Communications Manager with an IP address through the **Cisco Unified Communications Manager Administration > System > Server** menu. Cisco Unified Presence dynamically creates a TCP-based CTI gateway host profile for that address, and automatically populates the CTI gateway fields on Cisco Unified Presence.

Before You Begin

- Make sure that you have completed this configuration on Cisco Unified Communications Manager:
  - ♦ Configured the phone devices for CTI device control.
  - ♦ Added the Cisco Unified Personal Communicator users to a CTI-enabled user group.
- Obtained the hostnames or IP addresses of the CTI gateway.

Procedure

1. Select **Cisco Unified Presence Administration > Application > Cisco Unified Personal Communicator > CTI Gateway Server**.
2. Select **Add New**.
3. Enter information into the fields.

Field	Setting
Name	Enter the server name.
Description	(Optional) Enter a server description.
Hostname/IP Address	Enter an IP address or the FQDN (Fully Qualified Domain Name) of Cisco Unified Communications Manager that is running the CTI service.
Port	Enter **2748**.
Protocol Type	Select **TCP**.

4. Select **Save**.

Troubleshooting Tip

You can see the CTI gateway information in the Server Health window in Cisco Unified Personal Communicator (**Help > Show Server Health** on Windows operating system).

Related Topics

- User and Device Configuration on Cisco Unified Communications Manager
- Desk Phone Control and the CTI Connection Failures
- Getting More Information

What To Do Next

Creating CTI Gateway Profiles

Creating CTI Gateway Profiles

You must create CTI gateway profiles in Cisco Unified Presence Administration and assign primary and backup servers for redundancy.

Before You Begin

- You must create the CTI gateway profile before you can add Cisco Unified Personal Communicator licensed users to the application profile.
- You must first specify CTI gateway server names and addresses in **Application > Cisco Unified Personal Communicator > CTI Gateway Server** before you can select the servers as primary or backup servers in this procedure.
- Cisco Unified Presence dynamically creates a TCP-based CTI gateway profile based on the *hostname* of Cisco Unified Communications Manager. Before using this profile, verify that Cisco Unified Presence and Cisco Unified Personal Communicator clients can ping Cisco Unified Communications Manager by the DNS name. If they cannot contact the server, you need to add the *IP address* of Cisco Unified Communications Manager in Cisco Unified Presence Administration (**Application > Cisco Unified Personal Communicator > CTI Gateway Server**). You do not need to delete the host profiles that are created automatically.
- If you previously configured Cisco Unified Communications Manager with an IP address through the **Cisco Unified Communications Manager Administration > System > Server** menu, Cisco Unified Presence dynamically creates a TCP-based CTI gateway profile based on that address. The fields in Cisco Unified Presence Administration (**Application > Cisco Unified Personal Communicator > CTI Gateway Profile**) are automatically populated, and you need only add users to the default CTI TCP profile that is created (see Step 3).

Procedure

1. Select **Application > Cisco Unified Personal Communicator > CTI Gateway Profile**.
2. Select **Add New**.
3. Enter information into the fields.

Field	Setting
Name	Enter the profile name.
Description	(Optional) Enter a profile description.
Primary CTI Gateway Server and Backup CTI Gateway Server	Select a primary server and backup servers.
Make this the Default CTI Gateway Profile for the System	Check so that any new users that are added to the system are automatically placed into this default profile. Users who are already synchronized to Cisco Unified Presence from Cisco Unified Communications Manager are not added to the default profile. However, once the default profile is created, any users synchronized after that are added to the default profile.

4. Select **Add Users to Profile**.

5. Use the Find and List Users window to find and select users.

6. Select **Add Selected** to add users to the profile

7. Select **Save** in the main CTI Gateway Profile window.

Related Topics

- Configuring CTI Gateway Server Names and Addresses
- Getting More Information

What To Do Next

Configuring Firewalls to Pass Cisco Unified Personal Communicator Traffic