Unified PhoneProxy FAQ

Document ID: 72790

Contents

Introduction
Usage
Configuration
User Management
Security and Encryption
Updates, Backup, and Maintenance
CallManager Configuration
Related Information

Introduction

This document answers frequently asked questions about the Cisco Unified PhoneProxy.

Refer to Cisco Technical Tips Conventions for information on document conventions.

Usage

Q. Can you connect a PC to the back of an IP Phone that is activated and registered to Cisco Unified PhoneProxy and get corporate data?

A. No. Cisco Unified PhoneProxy facilitates a Signaling Connection Control Part (SCCP) connection (and related RTP, TFTP, and HTTP traffic) from a phone to a Cisco Unified CallManager through a firewall. It has no affect on data connections to the corporate network for uses other than IP Phones. The user connected to the back of a phone has access to the local LAN only. They must create a VPN connection in order to access corporate data.

Q. In the Voice and Data VLAN Bridge use case, does Cisco IP Communicator work on a mobile device, such as a PDA? Can it register to Cisco Unified PhoneProxy and make calls?

A. The Voice and Data VLAN Bridge use case maintains a separation between the voice VLAN and the data VLAN, but still supports IP Communicator deployments for mobile workers. Refer to the Cisco Unified PhoneProxy Administration Guide for more information on use cases.

In the Voice and Data VLAN Bridge use case the Cisco Unified PhoneProxy does not affect how well the Cisco IP Communicator works on a mobile device. It only proxies the SCCP connection (and related RTP, TFTP, and HTTP traffic).

Cisco Unified PhoneProxy does not impede or facilitate access to corporate networks, except as specifically allowed for the phone to function properly. If your corporate network requires it, you must use VPN before Cisco Unified PhoneProxy, but the VPN connection does not need to be turned on for the phone to function. However, IP Communicator is the exception.

The IP Communicator phone service can be disrupted when VPN is turned on and off.

In addition, you can experience moderate to severe audio quality problems when a phone is connected with VPN because VPN cannot implement specific quality of service levels required by the RTP stream. Refer to Cisco Unified PhoneProxy Administration Guide for more information on audio issues.

Q. Where do you SFTP update files to?

A. If you must manually place an update file on the Cisco Unified PhoneProxy, establish a secure FTP (SFTP) connection to the south IP address (or the management IP address if it is enabled), and then place the file in the incoming folder.

Note: You can retrieve updates from the Web with this command: **get update** <*url*>.

Q. Does RTP traffic travel directly from one remote IP phone to another remote IP phone?

A. No. RTP traffic is always routed through the Cisco Unified PhoneProxy. However, Cisco Unified PhoneProxy does not track state information about each phone. Therefore, it is not aware that the two calls from two different phones are in fact one call between two phones.

Q. What codecs are supported by remote phones that communicate with the Cisco Unified PhoneProxy?

A. Because Cisco Unified PhoneProxy does not support media transformations, any codec is supported. However, a problem arises with encrypted media when (RTP payload + RTP header) mod 64 does not equal 43, 44, 45, or 46. Therefore, 20 ms g.711 is acceptable; 30 ms g.711 is not acceptable.

In order to calculate this value, use the modulo (mod) operation. The mod operation returns the remainder when one number is divided by another. For example, 13 mod 5 returns 3.

For g.711 with an RTP payload of 160 and an RTP header of 12, use these calculations:

160+12=172

172 mod 64 = 44

44 is an acceptable value.

Note: Another way to interpret this operation is to find the number closest to 172 that is divisible by 64, which is 128. The remainder of 172 − 128 is 44. Therefore, 172 mod 64 = 44.

Note: You can also use Google Calculator in order to determine the results of a mod operation. Enter the mod operation in the search field at Google.com .

Configuration

Q. What do I need to program in a phone before I give it to the end user?

A. Besides an alternate TFTP server address that points to the proxy, you do not need to program any additional settings in the phone. However, the phone should be provisioned in Cisco Unified CallManager if automatic registration is disabled.

Note: You might need to configure the end−user cable or DSL router. If the router does not support stateful packet inspection, you might need to configure (User Datagram Protocol) UDP port forwarding or place the phone in the Demilitarized Zone (DMZ), especially for music on hold.

Q. Does the Cisco Unified PhoneProxy save geographic preferences?

A. No. The Cisco Unified PhoneProxy does not save geographic preferences. When a user connects to a Cisco Unified PhoneProxy cluster, they are connected based on the number of users. For example, if you configure a cluster with nodes on the East Coast and West Coast, users are spread out evenly among the nodes. If you have 1500 users, 750 users are connected to each node. Some users on the West Coast might be assigned to the East Coast node, and some users on the East Coast might be assigned to the West Coast node.

Q. Does "No license enforcement" mean that in the Cisco Unified CallManager (where counts are tracked) all phones that come through a proxy appear as 1?

A. No. Each phone must be provisioned in the Cisco Unified CallManager and consumes the same number of license units it would without the Cisco Unified PhoneProxy. Refer to Cisco Unified PhoneProxy Administration Guide for more information.

User Management

Q. Can you import a user list from Cisco Unified CallManager or some other LDAP source?

A. At this time, Cisco Unified PhoneProxy does not integrate directly with these sources. However, you can import into the Management Console a comma−separated value (CSV) file in order to add multiple users.

Q. What does it mean to *activate* a call from a user perspective?

A. You can use these methods in order to activate a call:

- The end user activates the call through a web page. The user must supply a user name, password, and WAN IP address. (The WAN IP address is not the internal 192.168.x.x that the router gives.)

  Note: The web page detects the external IP address and fills in the correct address. However, based on the network, you might need to change that IP address.
- The administrator activates the call through the command−line interface. The administrator must supply a user name and IP address.
- The application activates the account and provides the user name, password, and IP address. You must enable the activation web service in order to use this method.

Q. Do I need to activate before each call, every day, or only once?

A. Activation remains activate as long as there is an SCCP connection between the IP phone and the Cisco Unified PhoneProxy. Since there is a good deal of keep−alive traffic with an SCCP connection, the activation should not time out.

The default activation idle timeout is 300 second (5 minutes). This idle time occurs only if the IP phone never actually registers after the account is activated. For example, the account is activated, but the phone is not plugged in to the network within 5 minutes, or the phone loses network connectivity (because of an Internet or power outage that lasts longer than 5 minutes), or the IP address changes (because the IP lease expires or because DHCP assigns a different address).

The Cisco Unified PhoneProxy expects to maintain a connection to that account and IP address. If that connection is interrupted for more than the configured amount of idle time, the account becomes inactive.

Note: Administrators can configure an authorization timeout that is separate from the idle timeout. The authorization timeout causes an active account to become inactive after a specified number of seconds, which requires users to authenticate again once the timeout value expires. This value is 0 seconds by default, which means the account does not automatically become inactive.

Security and Encryption

Q. Does security and encryption work with Cisco Unified CallManager 5.0?

A. Yes. Security and encryption has been tested and works with Cisco Unified CallManager 5.0.4 and 5.1.

Note: Cisco Unified CallManager 5.0 handles certificates differently than versions 4.x.

Q. Can the Cisco Unified PhoneProxy communicate securely with phones on the untrusted Internet while it remains unencrypted on the trusted internal network? Can the Cisco Unified PhoneProxy communicate securely with two phones on the untrusted Internet?

A. When security is turned on, all phones on the untrusted Internet must communicate securely with the Cisco Unified PhoneProxy, or they are not allowed to communicate. The call segment between the Cisco Unified PhoneProxy and a remote IP phone is encrypted. The call segment between two remote IP phones is encrypted, but the call segment between the Cisco Unified PhoneProxy or the internal Cisco Unified CallManager and IP phones remains unencrypted.

These images illustrate call segment encryption.

- For a remote Internet phone to internal corporate phone:
- For a remote Internet phone to another remote Internet phone:

Q. How do I configure the Adaptive Security Appliance (ASA) for Cisco Phone Proxy feature?

A. In order to configure the ASA for Cisco Phone Proxy feature, refer to Configuring the Cisco Phone Proxy Feature.

Q. What are the features supported by ASA Phone Proxy?

A. ASA phone proxy supports these features:

- Music on Hold (MoH)
- XML services

Q. Is it possible to add an HTTP proxy and use it with Phone Proxy?

A. A reverse HTTP proxy to Cisco Unified Communications Manager can be used to point the IP phones to pinhole in ASA. This solution is more secure than opening a Cisco Unified Communications Manager HTTP server and requires an HTTP reverse proxy server.

Q. Which version of PhoneProxy supports which SCCP version?

A. ASA version 8.0(4) includes Unified Communications features, such as *Phone Proxy* and *Mobile Proxy*, that supports SCCPv17 .

Q. Which voice features (for example, MOH, Call transfer, Conference) are supported on Phone Proxy?

A. Music on Hold (MoH) is supported by ASA Phone Proxy, but some phones connected through a Cisco ASA Phone Proxy (codebase 8.2(1)) cannot hear the local MOH audio sources from CUCM. This issue is documented by the Cisco bug ID CSCso81816 (registered customers only) . Calls could be placed on Hold or Transfered with the help of ASA Phone Proxy. Enterprise features like conference calls are also supported on remote phones connected through an ASA phone proxy.

Updates, Backup, and Maintenance

Q. Can I recover the administrator password for the Cisco Unified PhoneProxy?

A. The administration settings within the Management Console are password protected. This password cannot be recovered. You must create a new configuration and password.

You can also protect with a password these areas of the Cisco Unified PhoneProxy CLI:

- *maint* partition You can password protect the maintenance partition. However, it is not password protected by default. In order to create a *maint* password, you must be in the maintenance partition. If the maintenance password is lost, you cannot recover it.
- *image0* and *image1* partitions The *image0* and *image1* partitions are protected by a password that is separate from the *maint* partition password. You can set the image partition password from within the image partition or from within the maintenance

partition.

Q. Is there a way to update the *maint* bootimage?

A. No. The *maint* bootimage cannot be updated. There should be no reason to update this bootimage.

Q. When the node of a Cisco Unified PhoneProxy cluster fails, does the next Unified PhoneProxy send phone registrations to the Cisco Unified CallManager? Does this situation cause performance issues?

A. The Cisco Unified PhoneProxy only transfers data that the phones send. For example, in a Cisco Unified CallManager cluster, if one of the members of that cluster goes down, all the phones failover to the another CallManager and register. The phones have an open connection to the standby Unified CallManager, so they send a registration request. A few more messages are sent between the phone and Unified CallManager. However, the phone does not realize the primary CallManager is down until they miss a heartbeat. Since the heartbeat function for the phones are not synchronized, the registration attempts are distributed across a 30 second interval, and performance is not affected.

Q. How does a phone know to register with the Cisco Unified PhoneProxy secondary node if the primary node is down?

A. The heartbeat function for each phone is called every 30 seconds. When they miss a beat, the phone registers with the secondary node and then attempts to register again with the primary node.

CallManager Configuration

Q. Does the Cisco Unified PhoneProxy appear in Cisco Unified CallManager?

A. No. The phones that are proxied appear in Cisco Unified CallManager, but the Cisco Unified PhoneProxy does not appear.

Note: Within the Cisco Unified CallManager, all phones that are registered and proxied display the same IP address. This IP address is the south interface IP address of the Cisco Unified PhoneProxy, which is on the same subnet as the voice VLAN for CallManager.

Q. Do I need to configure each phone in the proxy and in the Cisco Unified CallManager?

A. Yes. The phone should be provisioned in Cisco Unified CallManager ahead of time if automatic registration has been disabled. Also, an account for the phone should be created and published to the Cisco Unified PhoneProxy through the Management Console. In order to create the account, you must specify a user name, password, station ID of the phone (for example, SEP112233445566), and the CallManager to proxy the registration to. When the user activates the account, they must provide the user name, password, and IP address.

Note: Within the Cisco Unified CallManager, all phones that are registered and proxied display the same IP address. This IP address is the south interface IP address of the Cisco

Unified PhoneProxy, which is on the same subnet as the voice VLAN for CallManager.

Q. Are partitions, calling search spaces, and dialed numbers controlled by Cisco Unified CallManager?

A. Yes. The phone, dialed number, calling search spaces, and partitions should be provisioned in Cisco Unified CallManager. Cisco Unified CallManager retains all control over dial plans.

The Cisco Unified PhoneProxy is not aware of line numbers, route patterns, calling search spaces, or partitions. The Cisco Unified PhoneProxy only proxies the phone registration (and RTP).

Related Information

- **Cisco Unified PhoneProxy Documentation**
- **Cisco Unified PhoneProxy Administration Guide**
- **Voice Technology Support**
- **Voice and Unified Communications Product Support**
- **Recommended Reading: Troubleshooting Cisco IP Telephony**
- **Technical Support & Documentation − Cisco Systems**

Updated: Dec 06, 2006 Document ID: 72790