C H A P T E R **4**

Configuring Settings on the Cisco Unified IP Phone

The Cisco Unified IP Phone includes many configurable network and device settings that you may need to modify before the phone is functional for your users. You can access these settings, and change many of them, through menus on the phone.

This chapter includes the following topics:

Configuration Menus on the Cisco Unified IP Phone 7970 Series

The Cisco Unified IP Phone includes the following configuration menus:

- Network Configuration menu—Provides options for viewing and making a variety of network settings. For more information, see the "Network Configuration Menu" section on page 4-7.

- Device Configuration menu—Provides access to sub-menus from which you can view a variety of non network-related settings. For more information, see the "Device Configuration Menu" section on page 4-15.

- Security Configuration menu—Provides options for displaying and modifying security settings. For more information, see the "Security Configuration Menu" section on page 4-31.

Before you can change option settings on the Network Configuration menu, you must unlock options for editing. See the "Unlocking and Locking Options" section on page 4-4 for instructions.

For information about the keys you can use to edit or change option settings, see the "Editing Values" section on page 4-5.

You can control whether a phone user has access to phone settings by using the Settings Access field in the Cisco Unified CallManager Administration Phone Configuration Settings page. See *Cisco Unified CallManager Administration Guide* for more information.

Related Topics

- Unlocking and Locking Options, page 4-4
- Editing Values, page 4-5
- Overview of Options Configurable from a Phone, page 4-6
- Network Configuration Menu, page 4-7
- Device Configuration Menu, page 4-15
- Security Configuration Menu, page 4-31

Displaying a Configuration Menu

To display a configuration menu, perform the following steps.

✎

Note   You can control whether a phone has access to the Settings menu or to options on this menu by using the Settings Access field in the Cisco Unified CallManager Administration Phone Configuration page. The Settings Access field accepts these values:

- **Enabled**—Allows access to the Settings menu.
- **Disabled**—Prevents access to the Settings menu.
- **Restricted**—Allows access to the User Preferences menu and allows volume changes to be saved. Prevents access to other options on the Settings menu.

If you cannot access an option on the Settings menu, check the Settings Access field. For more information, see *Cisco Unified CallManager Administration Guide*.

Procedure

Step 1   Press the **Settings** button to access the Settings menu.

Step 2   Perform one of these actions to display the Network Configuration menu or the Device Configuration menu:

- Use the **Navigation** button to select the desired menu and then press the **Select** softkey.
- Use the keypad on the phone to enter the number that corresponds to the menu.
- Press the menu name on the touchscreen.

Step 3   To display a sub-menu, repeat Step 2.

Step 4   To exit a menu, press the **Exit** softkey.

Related Topics

- Unlocking and Locking Options, page 4-4

- Editing Values, page 4-5
- Overview of Options Configurable from a Phone, page 4-6
- Network Configuration Menu, page 4-7
- Device Configuration Menu, page 4-15
- Security Configuration Menu, page 4-31

Unlocking and Locking Options

Configuration options that can be changed from a phone are locked by default to prevent users from making changes that could affect the operation of a phone. You must unlock these options before you can change them.

When options are inaccessible for modification, a *locked* padlock icon appears on the configuration menus. When options are unlocked and accessible for modification, an *unlocked* padlock icon appears on these menus.

To unlock or lock options, press ****#**. This action either locks or unlocks the options, depending on the previous state.

Make sure to lock options after you have made your changes.

⚠️ **Caution**   Do not press ****#** to unlock options and then immediately press ****#** again to lock options. The phone will interpret this sequence as ****#****, which will reset the phone. To lock options after unlocking them, wait at least 10 seconds before you press ****#** again.

Related Topics

- Displaying a Configuration Menu, page 4-3
- Editing Values, page 4-5
- Overview of Options Configurable from a Phone, page 4-6
- Network Configuration Menu, page 4-7
- Device Configuration Menu, page 4-15

Editing Values

When you edit the value of an option setting, follow these guidelines:

- Use the keys on the keypad to enter numbers and letters.

- To enter letters using the keypad, use a corresponding number key. Press the key one or more times to display a particular letter. For example, press the 2 key once for "a," twice quickly for "b," and three times quickly for "c." After you pause, the cursor automatically advances to allow you to enter the next letter.

- To enter a period (for example, in an IP address), press the **.** (period) softkey or press **＊** on the keypad.

- Press the **<<** softkey if you make a mistake. This softkey deletes the character to the left of the cursor.

- Press the **Cancel** softkey before pressing the **Save** softkey to discard any changes that you have made.

Note   The Cisco Unified IP Phone provides several methods you can use to reset or restore option settings, if necessary. For more information, see the "Resetting or Restoring the Cisco Unified IP Phone" section on page 9-18.

Related Topics

Overview of Options Configurable from a Phone

The settings that you can change on a phone fall into several categories, as shown in Table 4-1. For a detailed explanation of each setting and instructions for changing them, see the "Network Configuration Menu" section on page 4-7.

✎ **Note**   There are several options on the Network Configuration menu and on the Device Configuration Menu that are for display only or that you can configure from Cisco Unified CallManager. These options are also described in the "Network Configuration Menu" section on page 4-7 and the or the "Device Configuration Menu" section on page 4-15.

Table 4-1   Settings Configurable from the Phone

Category	Description	Network Configuration Menu Option
DHCP settings	Dynamic Host Configuration Protocol (DHCP) automatically assigns IP address to devices when you connect them to the network. Cisco Unified IP Phones enable DHCP by default.	DHCP Enabled
		DHCP Address Released
IP settings	If you do not use DHCP in your network, you can make IP settings manually.	Domain Name
		IP Address
		Subnet Mask
		Default Router 1-5
		DNS Server 1-5
TFTP settings	If you do not use DHCP to direct the phone to a TFTP server, you must manually assign a TFTP server. You can also assign an alternative TFTP server to use instead of the one assigned by DHCP.	TFTP Server 1
		Alternate TFTP
		TFTP Server 2
VLAN settings	Admin. VLAN ID allows you to change the administrative VLAN used by the phone. PC VLAN allows the phone to interoperate with third-party switches that do not support a voice VLAN.	Admin. VLAN ID
		PC VLAN

Table 4-1   Settings Configurable from the Phone (continued)

Category	Description	Network Configuration Menu Option
Port settings	Allow you to set the speed and duplex of the network and access ports.	SW Port Configuration
		PC Port Configuration

Related Topics

- Displaying a Configuration Menu, page 4-3
- Unlocking and Locking Options, page 4-4
- Editing Values, page 4-5
- Network Configuration Menu, page 4-7
- Device Configuration Menu, page 4-15

Network Configuration Menu

The Network Configuration menu provides options for viewing and making a variety of network settings. Table 4-2 describes these options and, where applicable, explains how to change them.

For information about how to access the Network Configuration menu, see the "Displaying a Configuration Menu" section on page 4-3.

Before you can change an option on this menu, you must unlock options as described in the "Unlocking and Locking Options" section on page 4-4. The **Edit**, **Yes**, or **No** softkeys for changing network configuration options appear only if options are unlocked.

For information about the keys you can use to edit options, see the "Editing Values" section on page 4-5.

Table 4-2   Network Configuration Menu Options

Option	Description	To Change
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IP address.	Display only—Cannot configure.
BOOTP Server	Indicates whether the phone obtains its configuration from a Bootstrap Protocol (BootP) server instead of from a DHCP server.	Display only—Cannot configure.
MAC Address	Unique Media Access Control (MAC) address of the phone.	Display only—Cannot configure.
Host Name	Unique host name that the DHCP server assigned to the phone.	Display only—Cannot configure.
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.	1. Unlock network configuration options. 2. Set the DHCP Enabled option to No. 3. Scroll to the Domain Name option, press the **Edit** softkey, and then enter a new domain name. 4. Press the **Validate** softkey and then press the **Save** softkey.
IP Address	Internet Protocol (IP) address of the phone. If you assign an IP address with this option, you must also assign a subnet mask and default router. See the Subnet Mask and Default Router options in this table.	1. Unlock network configuration options. 2. Set the DHCP Enabled option to No. 3. Scroll to the IP Address option, press the **Edit** softkey, and then enter a new IP Address. 4. Press the **Validate** softkey and then press the **Save** softkey.

Table 4-2   Network Configuration Menu Options (continued)

Option	Description	To Change
Subnet Mask	Subnet mask used by the phone.	1. Unlock network configuration options. 2. Set the DHCP Enabled option to No. 3. Scroll to the Subnet Mask option, press the **Edit** softkey, and then enter a new subnet mask. 4. Press the **Validate** softkey and then press the **Save** softkey.
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the phone. If you are not using DHCP in your network and you want to change this server, you must use the TFTP Server 1 option. If you set the Alternate TFTP option to yes, you must enter a non-zero value for the TFTP Server 1 option. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL file on the phone, you must unlock the CTL file before you can save changes to the TFTP Server 1 option. In this case, the phone will delete the CTL file when you save changes to the TFTP Server 1 option. For information about the CTL file, refer to *Cisco Unified CallManager Security Guide*. For information about unlocking the CTL file, see the "Security Configuration Menu" section on page 4-31.	1. Unlock the CTL file, if necessary. 2. If DHCP is enabled, set the Alternate TFTP option to Yes. 3. Scroll to the TFTP Server 1 option, press the **Edit** softkey, and then enter a new TFTP server IP address. 4. Press the **Validate** softkey, and then press the **Save** softkey.

Table 4-2   Network Configuration Menu Options (continued)

Option	Description	To Change
TFTP Server 2	Optional backup TFTP server that the phone uses if the primary TFTP server is unavailable. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL file on the phone, you must unlock the CTL file before you can save changes to the TFTP Server 2 option. In this case, the phone will delete the CTL file when you save changes to the TFTP Server 2 option. For information about the CTL file, refer to *Cisco Unified CallManager Security Guide*. For information about unlocking the CTL file, see to the "Security Configuration Menu" section on page 4-31.	1. Unlock the CTL file, if necessary. 2. Unlock network configuration options. 3. Enter an IP address for the TFTP Server 1 option. 4. Scroll to the TFTP Server 2 option, press the **Edit** softkey, and then enter a new backup TFTP server IP address. 5. Press the **Validate** softkey, and then press the **Save** softkey.
Default Router 1 Default Router 2 Default Router 3 Default Router 4 Default Router 5	Default router used by the phone (Default Router 1) and optional backup routers (Default Router 2–5).	1. Unlock network configuration options. 2. Set the DHCP Enabled option to No. 3. Scroll to the appropriate Default Router option, press the **Edit** softkey, and then enter a new router IP address. 4. Press the **Validate** softkey. 5. Repeat Steps 3 and 4 as needed to assign backup routers. 6. Press the **Save** softkey.

Table 4-2   Network Configuration Menu Options (continued)

Option	Description	To Change
DNS Server 1 DNS Server 2 DNS Server 3 DNS Server 4 DNS Server 5	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–5) used by the phone.	1. Unlock network configuration options. 2. Set the DHCP Enabled option to No. 3. Scroll to the appropriate DNS Server option, press the **Edit** softkey, and then enter a new DNS server IP address. 4. Press the **Validate** softkey. 5. Repeat Steps 3 and 4 as needed to assign backup DNS servers. 6. Press the **Save** softkey.
Operational VLAN ID	Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the phone is a member. If the phone has not received an auxiliary VLAN, this option indicates the Administrative VLAN. If neither the auxiliary VLAN nor the Administrative VLAN are configured, this option is blank.	The phone obtains its Operational VLAN ID via Cisco Discovery Protocol (CDP) from the switch to which the phone is attached. To assign a VLAN ID manually, use the Admin VLAN ID option.
Admin. VLAN ID	Auxiliary VLAN in which the phone is a member. Used only if the phone does not receive an auxiliary VLAN from the switch, ignored otherwise.	1. Unlock network configuration options. 2. Scroll to the Admin. VLAN ID option, press the **Edit** softkey, and then enter a new Admin VLAN setting. 3. Press the **Validate** softkey and then press the **Save** softkey.
DHCP Enabled	Indicates whether DHCP is being used by the phone.	1. Unlock network configuration options. 2. Scroll to the DHCP Enabled option and press the **No** softkey to disable DHCP, or press the **Yes** softkey to enable DHCP. 3. Press the **Save** softkey.

Table 4-2   Network Configuration Menu Options (continued)

Option	Description	To Change
DHCP Address Released	Releases the IP address assigned by DHCP.	1. Unlock network configuration options. 2. Scroll to the DHCP Address Released option and press the **Yes** softkey to release the IP address assigned by DHCP, or press the **No** softkey if you do not want to release this IP address. 3. Press the **Save** softkey.
Alternate TFTP	Indicates whether the phone is using an alternative TFTP server.	1. Unlock network configuration options. 2. Scroll to the Alternate TFTP option and press the **Yes** softkey if the phone should use an alternative TFTP server. Press the **No** softkey otherwise. 3. Press the **Save** softkey.

Table 4-2   Network Configuration Menu Options (continued)

Option	Description	To Change
SW Port Configuration	Speed and duplex of the network port (labeled 10/100 SW on the Cisco Unified IP Phone 7970, and 10/100/1000 SW on the Cisco Unified IP Phone 7971G-GE). Valid values: • Auto Negotiate • 10 Half—10-BaseT/half duplex • 10 Full—10-BaseT/full duplex • 100 Half—100-BaseT/half duplex • 100 Full—100-BaseT/full duplex • 1000 Full—1000-BaseT/full duplex If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to auto-negotiate. If you change the setting of this option, you must change the PC Port Configuration option to the same setting.	1. Unlock network configuration options. 2. Scroll to the SW Port Configuration option and then press the **Edit** softkey. 3. Scroll to the setting that you want and then press the **Select** softkey. 4. Press the **Save** softkey.

Table 4-2   Network Configuration Menu Options (continued)

Option	Description	To Change
PC Port Configuration	Speed and duplex of the access port (labeled 10/100 PC on the Cisco Unified IP Phone 7970, and 10/100/1000 PC on the Cisco Unified IP Phone 7971G-GE). Valid values: • Auto Negotiate • 10 Half—10-BaseT/half duplex • 10 Full—10-BaseT/full duplex • 100 Half—100-BaseT/half duplex • 100 Full—100-BaseT/full duplex • 1000 Full—1000-BaseT/full duplex If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to auto-negotiate. If you change the setting of this option, you must change the SW Port Configuration option to the same setting.	1. Unlock network configuration options. 2. Scroll to the PC Port Configuration option and then press the **Edit** softkey. 3. Scroll to the setting that you want and then press the **Select** softkey. 4. Press the **Save** softkey.

Table 4-2   Network Configuration Menu Options (continued)

Option	Description	To Change
PC VLAN	Allows the phone to interoperate with 3rd party switches that do not support a voice VLAN. The Admin VLAN ID option must be set before you can change this option.	1. Unlock network configuration options. 2. Make sure the Admin VLAN ID option is set. 3. Scroll to the **PC VLAN** option, press the **Edit** softkey, and then enter a new PC VLAN setting. 4. Press the **Validate** softkey and then press the **Save** softkey.

Related Topics

Device Configuration Menu

The Device Configuration menu provides access to nine sub-menus from which you can view a variety of settings that are specified in the configuration file for a phone. (The phone downloads the configuration file from the TFTP server.) These sub-menus are:

- Security Configuration Menu, page 4-27
- QoS Configuration Menu, page 4-29
- Network Configuration, page 4-29

For instructions about how to access the Device Configuration menu and its sub-menus, see the "Displaying a Configuration Menu" section on page 4-3.

CallManager Configuration Menu

The CallManager Configuration menu contains the options CallManager 1, CallManager 2, CallManager 3, CallManager 4, and CallManager 5. These options show Cisco Unified CallManager servers that are available for processing calls from the phone, in prioritized order.

To change these options, use Cisco Unified CallManager Administration.

For an available Cisco Unified CallManager server, an option on the CallManager Configuration menu will show the Cisco Unified CallManager server IP address or name and one of the states shown in Table 4-3.

Table 4-3   Cisco Unified CallManager Server States

State	Description
Active	Cisco Unified CallManager server from which the phone is currently receiving call-processing services
Standby	Cisco Unified CallManager server to which the phone switches if the current server becomes unavailable
Blank	No current connection to this Cisco Unified CallManager server

An option may also display one of more of the designations or icons shown in Table 4-4:

Table 4-4   Cisco Unified CallManager Server Designations

Designation	Description
SRST	Indicates a Survivable Remote Site Telephony router capable of providing Cisco Unified CallManager functionality with a limited feature set. This router assumes control of call processing if all other Cisco Unified CallManager servers become unreachable. The SRST Cisco Unified CallManager always appears last in the list of servers, even if it is active.
	You configure an SRST router address in the Cisco Unified CallManager Administration SRST Reference Configuration page (choose **System > SRST**). You configure an SRST reference in the Device Pool Configuration page (choose **System > Device Pool**).
TFTP	Indicates that the phone was unable to register with a Cisco Unified CallManager listed in its configuration file and that it registered with the TFTP server instead.
(Authentication icon)	Indicates that the connection to the Cisco Unified CallManager is authenticated. For more information about authentication, refer to *Cisco Unified CallManager Security Guide*.
(Encryption icon)	Indicates that the connection to the Cisco Unified CallManager is authenticated and encrypted. For more information about authentication and encryption, refer to *Cisco Unified CallManager Security Guide*.

Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager 5.1 (SCCP), Cisco Unified IP Phones
OL-11523-01

4-17

HTTP Configuration Menu

The HTTP Configuration menu displays the URLs of servers from which the phone obtains a variety of information. This menu also displays information about the idle display on the phone.

Table 4-5 describes the options on the HTTP Configuration menu.

Table 4-5   HTTP Configuration Menu Options

Option	Description	To Change
Directories URL	URL of the server from which the phone obtains directory information.	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.
Services URL	URL of the server from which the phone obtains Cisco Unified IP Phone services.	Use Cisco Unified CallManager Administration to modify **> Device > Phone > Phone Configuration**.
Messages URL	URL of the server from which the phone obtains message services.	Use Cisco Unified CallManager Administration to modify **> Device > Phone > Phone Configuration**.
Information URL	URL of the help text that appears on the phone.	Use Cisco Unified CallManager Administration > **> Device > Phone > Phone Configuration**.
Authentication URL	URL that the phone uses to validate requests made to the phone web server.	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.
Proxy Server URL	URL of proxy server, which makes HTTP requests to non-local host addresses on behalf of the phone HTTP client and provides responses from the non-local host to the phone HTTP client.	Use Cisco Unified CallManager Administration to modify **> Device > Phone > Phone Configuration**.

Table 4-5   HTTP Configuration Menu Options (continued)

Option	Description	To Change
Idle URL	URL of an XML service that the phone displays when the phone has not been used for the time specified in the Idle URL Time option and no menu is open. For example, you could use the Idle URL option and the Idle URL Timer option to display a stock quote or a calendar on the LCD screen when the phone has not been used for 5 minutes.	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.
Idle URL Time	Number of seconds that the phone has not been used and no menu is open before the XML service specified in the Idle URL option is activated.	Use Cisco Unified CallManager Administration to modify **> Device > Phone > Phone Configuration**.

Locale Configuration Menu

The Locale Configuration menu displays information about the user locale and the network locale used by the phone. Table 4-6 describes the options on this menu.

Table 4-6   Locale Configuration Menu Options

Option	Description	To Change
User Locale	User locale associated with the phone user. The user locale identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.
User Locale Version	Version of the user locale loaded on the phone.	Display only—Cannot configure.
User Locale Char Set	Character set that the phone uses for the user locale.	Display only—Cannot configure.

Table 4-6   Locale Configuration Menu Options (continued)

Option	Description	To Change
Network Locale	Network locale associated with the phone user. The network locale identifies a set of detailed information that supports the phone in a specific location, including definitions of the tones and cadences used by the phone.	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.
Network Locale Version	Version of the network locale loaded on the phone.	Display only—Cannot configure.

UI Configuration Menu

The UI Configuration menu displays the status of various user interface features on the phone. Table 4-7 describes the options on this menu.

Table 4-7   UI Configuration Menu Options

Option	Description	To Change
Auto Call Select	Indicates whether the phone automatically shifts the call focus to an incoming call on the same line when the user is already on a call. When this option is enabled, the phone shifts the call focus to the most recent incoming call. When this option is disabled, all automatic focus changes, including Auto Line Select, are disabled regardless of their setting. Default: Enabled	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.
Auto Line Select	Indicates whether the phone shifts the call focus to incoming calls on all lines. When this option is disabled, the phone only shifts the call focus to incoming calls on the line that is in use. When this option is enabled, the phone shifts the call focus to the line with the most recent incoming call. Default: Disabled	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.

Table 4-7   UI Configuration Menu Options (continued)

Option	Description	To Change
BLF for Call Lists	Indicates whether the Busy Lamp Field (BLF) is enabled for call lists.	Use Cisco Unified CallManager Administration **> System > Enterprise Parameters**.
"more" Softkey Timer	Indicates the number of seconds that additional softkeys are displayed after the user presses **more**. If this timer expires before the user presses another softkey, the display reverts to the initial softkeys. Range: 5 to 30; 0 represents an infinite timer. Default: 5	Access the Phone Configuration page in Cisco Unified CallManager Administration.

Media Configuration Menu

The Media Configuration menu displays whether the headset, speakerphone, and video capability are enabled on the phone. This menu also displays options for recording tones that the phone may play to indicate that a call may be recorded. Table 4-8 describes the options on this menu.

Table 4-8   Media Configuration Menu Options

Option	Description	To Change
Headset Enabled	Indicates whether the **Headset** button is enabled on the phone.	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.
Speaker Enabled	Indicates whether the speakerphone is enabled on the phone.	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.
Video Capability Enabled	Indicates whether the phone can participate in video calls when connected to an appropriately equipped computer.	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.

Table 4-8   Media Configuration Menu Options (continued)

Option	Description	To Change
Recording Tone	Indicates whether a recording tone (often referred to as a *beep tone*) is enabled or disabled for the phone. If the recording tone option is enabled, the phone plays the beep tone in both directions of every call, regardless of whether the call actually gets recorded. The beep tone first sounds when a call is answered. You may want to notify your users if you enable this option. Default: Disabled Related Parameters: • Recording Tone Local Volume • Recording Tone Remote Volume • Recording Tone Duration Other related parameters—Beep tone frequency in hz, the length of the beep tone (called *duration*), and how often the beep tone plays (called *interval*)—are defined on a per-Network Locale basis in the xml file that defines tones. This xml file is usually named tones.xml or g3-tones.xml.	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.

Table 4-8   Media Configuration Menu Options (continued)

Option	Description	To Change
Recording Tone Local Volume	Indicates the loudness setting for the beep tone that is received by the party whose phone has the Recording Tone option enabled. This setting applies for each listening device (handset, speakerphone, headset). Range: 0 percent (no tone) to 100 percent (same level as current volume setting on the phone). Default: 100 See also: Recording Tone	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.

Table 4-8   Media Configuration Menu Options (continued)

Option	Description	To Change
Recording Tone Remote Volume	Indicates the loudness setting for the beep tone that the *remote party* receives. The *remote party* is the party who is on a call with the party whose phone has the Recording Tone option enabled. Range: 0 percent to 100 percent. (0 percent is -66 dBM and 100 percent is -3 dBM.) Default: 84 percent (-10dBM) See also: Recording Tone	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.
Recording Tone Duration	Indicates the length of time in milliseconds for which the beep tone plays. If the value you configure here is less than one third the interval, then this value overrides the default provided by the Network Locale. Range: 0 to 3000 **Note** For some Network Locales that use a complex cadence, this setting applies only to the first beep tone. See also: Recording Tone	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.

Power Save Configuration Menu

The Power Save Configuration menu displays the settings that control when the LCD screen on a phone turns off to conserve power. Table 4-9 describes the options on this menu.

For detailed information about configuring these settings, see the "Automatically Disabling the Cisco Unified IP Phone Touchscreen" section on page 6-11.

Table 4-9   Power Save Configuration Menu Options

Option	Description	To Change
Display On Time	Time each day that the LCD screen turns on automatically (except on the days specified in the Days Display Not Active field).	Use Cisco Unified CallManager Administration > **Device** > **Phone** > **Phone Configuration**.
Display On Duration	Length of time that the LCD screen remains on after turning on at the time shown in the Display On Time option.	Use Cisco Unified CallManager Administration > **Device** > **Phone** > **Phone Configuration**.
Display Idle Timeout	Length of time that the phone is idle before the display turns off. Applies only when the display was off as scheduled and was turned on by an end-user (by pressing a button on the phone, touching the touchscreen, or lifting the handset).	Use Cisco Unified CallManager Administration > **Device** > **Phone** > **Phone Configuration**.
Days Display Not Active	Days that the display does not turn on automatically at the time specified in the Display On Time option.	Use Cisco Unified CallManager Administration > **Device** > **Phone** > **Phone Configuration**.
Display On When Incoming Call	Indicates whether the LCD screen automatically illuminates when a call is received.	Use Cisco Unified CallManager Administration > **Device** > **Phone** > **Phone Configuration**.

Ethernet Configuration Menu

The Ethernet Configuration menu includes the options described in Table 4-10

Table 4-10   Ethernet Configuration Menu Options

Option	Description	To Change
Span to PC Port	Indicates whether the phone will forward packets transmitted and received on the network port to the access port. Enable this option if an application that requires monitoring of the phone's traffic is being run on the access port. These applications include monitoring and recording applications (common in call center environments) and network packet capture tools that are used for diagnostic purposes.	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.

Security Configuration Menu

The Security Configuration menu that you access from the Device Configuration menu displays settings that relate to security for phone.

Table 4-11 describes the options on the Security Configuration menu.

Note   The phone also has a Security Configuration menu that you access directly from the Settings menu. For information about the security options on that menu, see the see the "Security Configuration Menu" section on page 4-31.

Table 4-11   Security Configuration Menu Options

Option	Description	To Change
PC Port Disabled	Indicates whether the access port on the phone is enabled or disabled. **Note** If disabled, video will not work on this phone, even if video is enabled.	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous Address Resolution Protocol (ARP) responses. Disabling the phone's ability to accept Gratuitous ARP will prevent applications that use this mechanism to monitor and record voice streams from working. If voice monitoring is not desired, set this option to No (disabled).	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.
Voice VLAN Enabled	Indicates whether the phone allows a device attached to the access port to access the Voice VLAN. Setting this option to No (disabled) prevents the attached PC from sending and receiving data on the Voice VLAN. This setting also prevents the PC from receiving data sent and received by the phone. Set this setting to Yes (enabled) if an application that requires monitoring of the phone's traffic is running on the PC. These applications include monitoring and recording applications and network monitoring software.	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.
Web Access Enabled	Indicates whether web access is enabled (Yes) or disabled (No) for the phone.	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.

Table 4-11   Security Configuration Menu Options (continued)

Option	Description	To Change
Security Mode	Displays the security mode that is set for the phone.	Use Cisco Unified CallManager Administration to modify.
Logging Display	For use by the Cisco Technical Assistance Center (TAC), if necessary.	

QoS Configuration Menu

The QoS Configuration menu displays information that relates to quality of service (QoS) for the phone. Table 4-12 describes the options on this menu.

Table 4-12   QoS Configuration Menu Options

Option	Description	To Change
DSCP For Call Control	Differentiated Services Code Point (DSCP) IP classification for call control signaling.	Use Cisco Unified CallManager Administration **> System > Enterprise Parameters**.
DSCP For Configuration	DSCP IP classification for any phone configuration transfer.	Use Cisco Unified CallManager Administration **> System > Enterprise Parameters**.
DSCP For Services	DSCP IP classification for phone-based services.	Use Cisco Unified CallManager Administration **> System > Enterprise Parameters**.

Related Topics

Network Configuration

The Network Configuration menu displays device-specific network configuration settings on the phone. Table 4-13 describes the options in this menu.

Table 4-13   Network Configuration Menu Options

Option	Description	To Change
Load Server	Used to optimize installation time for phone firmware upgrades and offload the WAN by storing images locally, negating the need to traverse the WAN link for each phone's upgrade. You can set the Load Server to another TFTP server IP address or name (other than the TFTP Server 1 or TFTP Server 2) from which the phone firmware can be retrieved for phone upgrades. When the Load Server option is set, the phone contacts the designated server for the firmware upgrade. **Note** The Load Server option allows you to specify an alternate TFTP server for phone upgrades only. The phone continues to use TFTP Server 1 or TFTP Server 2 to obtain configuration files. The Load Server option does not provide management of the process and of the files, such as file transfer, compression, deletion, and so on.	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.

Table 4-13   Network Configuration Menu Options (continued)

Option	Description	To Change
RTP Control Protocol	Indicates whether the phone supports the Real-Time Control Protocol (RTCP). Settings include: • Enabled • Disabled—default If this feature is disabled, several call statistic values display as 0. For additional information, see the following sections: • Call Statistics Screen, page 7-17 • Streaming Statistics, page 8-15	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.

Related Topics

Security Configuration Menu

The Security Configuration menu that you access directly from the Settings menu provides information about various security settings. It also provides access to the CTL File screen and the Trust List menu, if a CTL file is installed on the phone.

Table 4-14 describes the options on the Security Configuration menu.

Note   The phone also has a Security Configuration menu that you access from the Device menu. For information about the security options on that menu, see the "Security Configuration Menu" section on page 4-27.

Table 4-14   *Security Menu Settings*

Option	Description	To Change
Web Access Enabled	Indicates whether web access is enabled (Yes) or disabled (No) for the phone.	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.
Security Mode	Displays the security mode that is set for the phone.	Use Cisco Unified CallManager Administration **> Device > Phone > Phone Configuration**.
MIC	Indicates whether a manufacturing installed certificate (used for the security features) is installed on the phone (Yes) or is not installed on the phone (No).	For information about how to manage the MIC for your phone, refer to the "Using the Certificate Authority Proxy Function" chapter in *Cisco Unified CallManager Security Guide*.
LSC	Indicates whether a locally significant certificate (used for the security features) is installed on the phone (Yes) or is not installed on the phone (No).	For information about how to manage the LSC for your phone, refer to the "Using the Certificate Authority Proxy Function" chapter in *Cisco Unified CallManager Security Guide*.
CTL File	Displays the MD5 hash of the certificate trust list (CTL) file that is installed in the phone. If no CTL file is installed on the phone, this field displays No. (If security is configured for the phone, the CTL file installs automatically when the phone reboots or resets.	For more information about this file, refer to the "Configuring the Cisco CTL Client" section in *Cisco Unified CallManager Security Guide*. If a CTL file is installed on the phone, also provides access to the CTL File screen. For more information, see the "CTL File Screen" section on page 4-33.
Trust List	If a CTL file is installed on the phone, provides access to the Trust List menu.	For more information, see the "Trust List Menu" section on page 4-35.
CAPF Server	Displays the IP address and the port of the CAPF that the phone uses.	For more information about this server, refer to the "Using the Certificate Authority Proxy Function" section in *Cisco Unified CallManager Security Guide*.

Table 4-14   Security Menu Settings (continued)

Option	Description	To Change
802.1X Authentication	Allows you to enable 802.1X authentication for this phone.	See the "802.1X Authentication and Status" section on page 4-36.
802.1X Authentication Status	Displays real-time status progress of the 802.1X authentication transaction.	Display only—Cannot configure.

CTL File Screen

The CTL File screen includes the options described in Table 4-15.

Table 4-15   CTL File Settings

Option	Description	To Change
CTL File	Displays the MD5 hash of the CTL file that is installed in the phone. If security is configured for the phone, the CTL file installs automatically when the phone reboots or resets. • A locked padlock icon in this option indicates that the CTL file is locked. • An unlocked padlock icon indicates that the CTL file is unlocked.	For more information about this file, refer to the "Configuring the Cisco CTL Client" section in *Cisco Unified CallManager Security Guide*.

Table 4-15   CTL File Settings (continued)

Option	Description	To Change
CAPF Server	IP address of the CAPF server used by the phone. Also displays a certificate icon if a certificate is installed for this server.	For more information about this server, refer to the "Using the Certificate Authority Proxy Function" section in *Cisco Unified CallManager Security Guide*.
CallManager / TFPT Server	IP address of a Cisco Unified CallManager and TFTP server used by the phone. Also displays a certificate icon if a certificate is installed for this server. If neither the primary TFTP (TFTP Server 1) server nor the backup TFTP server (TFTP Server 2) is listed in the CTL file, you must unlock the CTL file before you can save changes that you make to the TFTP Server 1 option or to the TFTP Server 2 option on the Network Configuration menu.	For information about changing these options, see the "Network Configuration Menu" section on page 4-7.

Unlocking the CTL File

To unlock the CTL file from the Security Configuration menu, follow these steps:

Procedure

Step 1   Press ****#** to unlock options on the CTL File menu.

If you decide not to continue, press ****#** again to lock options on this menu.

Step 2   Highlight the CTL option.

Step 3   Press the **Unlock** softkey to unlock the CTL file.

After you change and save the TFTP Server 1 or the TFTP Server 2 option, the CTL file will be locked automatically.

> ✎
>
> **Note**   When you press the **Unlock** softkey, it changes to **Lock**. If you decide not
> to change the TFTP Server 1 or TFTP Server 2 option, press the **Lock**
> softkey to lock the CTL file.

Trust List Menu

The Trust List menu displays information about all of the servers that the phone
trusts and includes the options described in Table 4-16.

Table 4-16   *Trust List Menu Settings*

Option	Description	To Change
CAPF Server	IP address of the CAPF used by the phone. Also displays a certificate ⊞ icon if a certificate is installed for this server.	For more information about these settings, refer to the "Configuring the Cisco CTL Client" section in *Cisco Unified CallManager Security Guide*.
CallManager / TFPT Server	IP address of a Cisco Unified CallManager and TFTP server used by the phone. Also displays a certificate ⊞ icon if a certificate is installed for this server.	For more information about these settings, refer to the "Configuring the Cisco CTL Client" section in *Cisco Unified CallManager Security Guide*.
SRST Router	IP address of the trusted SRST router that is available to the phone, if such a device has been configured in Cisco Unified CallManager Administration. Also displays a certificate ⊞ icon if a certificate is installed for this server.	For more information about these settings, refer to the "Configuring the Cisco CTL Client" section in *Cisco Unified CallManager Security Guide*.

802.1X Authentication and Status

The 802.1X Authentication and 802.1X Authentication Status menus allow you to enable 802.1X authentication and monitor its progress. These options are described in Table 4-17 and Table 4-18.

You can access these menus by pressing the **Settings** button and choosing **Security Configuration > 802.1X Authentication** and **Security Configuration > 802.1X Authentication Status**.

Table 4-17   *802.1X Authentication Settings*

Option	Description	To Change
Device Authentication	Determines whether 802.1X authentication is enabled: • **Enabled**—Phone uses 802.1X authentication to request network access. • **Disabled**—Default setting in which the phone uses CDP to acquire VLAN and network access.	1. Choose **Settings > Security Configuration > 802.1X Authentication > Device Authentication**. 2. Set the Device Authentication option to Enabled or Disabled. 3. Press the **Save** softkey.
EAP-MD5	Specifies a password for use with 802.1X authentication using the following menu options (described in the following rows): • Device ID • Shared Secret • Realm	Choose **Settings > Security Configuration > 802.1X Authentication > EAP-MD5**.
	Device ID—Derivative of the phone's model number and unique MAC address displayed in this format: CP-<model>-SEP-<MAC>	Display only—Cannot configure.
	Shared Secret—Choose a password to use on the phone and on the authentication server. The password must be between 6 and 32 characters, consisting of any combination of numbers or letters. **Note** If you disable 802.1X authentication or perform a factory reset of the phone, the shared secret is deleted.	1. Choose **EAP-MD5 > Shared Secret**. 2. Enter the shared secret. 3. Press **Save**. See the "Troubleshooting Cisco Unified IP Phone Security" section on page 9-12 for assistance in recovering from a deleted shared secret.
	Realm—Indicates the user network domain, always set as *Network*	Display only—Cannot configure.

Table 4-18   802.1X Authentication Real-Time Status

Option	Description	To Change
802.1X Authentication Status	Real-time progress of the 802.1X authentication status, displaying one of the following states: • Disabled—802.1X is disabled and transaction was not attempted • Disconnected—Physical link is down or disconnected • Connecting—Trying to discover or acquire the authenticator • Acquired—Authenticator acquired, awaiting authentication to begin • Authenticating—Authentication in progress • Authenticated—Authentication successful or implicit authentication due to timeouts • Held—Authentication failed, waiting before next attempt (approximately 60 seconds)	Display only—Cannot configure.