



# CHAPTER 4

## Configuring Cisco IP Communicator

---

This chapter describes the configuration tasks that you or the user might need to perform after installation and before first use so that Cisco IP Communicator can function properly or so that users can access some features.

Some tasks in this chapter required configuration in Cisco Unified Communications Manager, formerly known as Cisco Unified CallManager.

- [Overview of Configuration Tasks, page 4-1](#)
- [About Required Configuration Tasks, page 4-4](#)
- [About Recommended or Optional Configuration Tasks, page 4-10](#)
- [About Local Configuration, page 4-13](#)
- [About Disabling Local Settings Access, page 4-13](#)
- [Disabling the Internal Web Server, page 4-14](#)
- [About Helping Users with Configuration Tasks, page 4-14](#)

## Overview of Configuration Tasks

[Table 4-1](#) and [Table 4-2](#) provide an overview of the required and recommended (optional) configuration tasks that you or the user might need to perform. The necessity of these tasks depends upon variables such as settings on the client PC and software VPN solution used by the user, among other factors.



### Note

- If you expect users to perform configuration tasks, provide them with detailed instructions, including access to the *User Guide for Cisco IP Communicator*. For details, see the [“About Helping Users with Configuration Tasks”](#) section on page 4-14.
- Some settings (such as configuring a custom audio port range) can be configured both locally (on the client PC) and remotely (in Cisco Unified Communications Manager Administration). Be aware that if a value is modified locally, the modified value becomes the active value, overwriting or preempting a value that is specified remotely. Therefore, once a setting is modified on the client PC, the only way to change it is on the client PC. For details, see the [“About Local Configuration”](#) section on page 4-13.

Table 4-1 Required Configuration Tasks

Task	Required?	Configuration Notes	For details, see...
Select and tune audio devices when prompted at startup	Required at initial startup. Allows the application to recognize installed audio devices.	Use the Audio Tuning Wizard, which automatically launches at initial start up. To manually launch: <ul style="list-style-type: none"> <li>• Cisco IP Communicator right-click menu.</li> <li>• Choose the program group from the Windows Start menu.</li> </ul> For device selection in Cisco IP Communicator: <b>right-click &gt; Preferences &gt; Audio</b> tab.	<a href="#">About Selecting and Tuning Audio Devices, page 4-5</a>
Specify a TFTP server address immediately after initial startup	Required if you are not using DHCP with Option 150 enabled in your network or if you want to specify an alternate TFTP address (only if you have not already specified this variable through a command-line option during deployment).	Cisco IP Communicator <b>right-click &gt; Preferences &gt; Network</b> tab > <b>TFTP Servers</b> section. If users share a PC and do not have elevated privileges, you must perform this task by using an administrator account.	<a href="#">How to Deploy the Application, page 3-2</a> <a href="#">About Specifying a TFTP Server, page 4-6</a> <a href="#">How to Resolve Startup Problems, page 8-5</a>
Select a device name when prompted after initial startup	Required at first launch if the client PC has multiple network interfaces or if it is a laptop with a docking station (and if you have not already specified this variable through a command-line option during deployment).	Cisco IP Communicator <b>right-click &gt; Preferences &gt; Network</b> tab > <b>Device Name</b> section. If users share a PC and do not have elevated privileges, you must perform this task by using an administrator account.	<a href="#">How to Deploy the Application, page 3-2</a> <a href="#">About Selecting a Device Name, page 4-7</a> <a href="#">How to Resolve Startup Problems, page 8-5</a>

Table 4-1 Required Configuration Tasks (continued)

Task	Required?	Configuration Notes	For details, see...
If you have not done so already, run the Cisco IP Communicator Administration Tool, and enable HTTP access. Specify the URL in Cisco Unified Communications Manager Administration	Required to resolve audio IP address detection problems caused by unsupported VPN clients. Recommended to improve performance for remote users and to install the Directory Wizard.	Obtain the tool from the product software download web site: <a href="http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278468661">http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278468661</a> . It is located inside the zipped folder with your build. Enter the getIP.asp URL in Cisco Unified Communications Manager Administration ( <b>Device &gt; Phone</b> , Phone Configuration window, IP Address Autodetection URL field).	<a href="#">Resolving Audio IP Address Auto-Detection Problems</a> , page 4-10 <a href="#">How to Resolve Startup Problems</a> , page 8-5
Provide users with username and password	Required for these features: <ul style="list-style-type: none"> <li>Quick Search Directory</li> <li>User Options web pages</li> </ul>	In Cisco Unified Communications Manager Administration: Release 5.x and later: <b>User Management &gt; End User</b> Release 4.x: <b>User &gt; Add a New User</b>	<a href="#">Specifying User Authentication Information for Quick Search with Windows-Based Cisco Unified Communications Managers</a> , page 5-13 <a href="#">Appendix A, “Providing Information to Users About Cisco IP Communicator”</a>

**Note**

If multiple users share a PC, the device name and TFTP server settings remain with the PC; all other settings in this environment follow the user.

**Table 4-2 Recommended (Optional) Configuration Tasks**

Task	Required?	Who configures where?	For details, see...
Modify advanced audio properties	Optional. Recommended for advanced users to improve sound quality.	Cisco IP Communicator <b>right-click &gt; Preferences &gt; Audio</b> tab > <b>Advanced</b> button.	<a href="#">Modifications for Remote Use, page 4-12</a>
Specify low-bandwidth setting for remote use	Optional. Remote users with low-bandwidth connections might experience better audio quality by using a low-bandwidth codec.	Cisco IP Communicator <b>right-click &gt; Preferences &gt; Audio</b> tab.	<a href="#">Modifications for Remote Use, page 4-12</a>
Configure a custom audio port range	Optional. You might use this option if you want to open up a single port to pass audio through a firewall or want to apply a QoS <sup>1</sup> policy by using a restricted range of RTP <sup>2</sup> ports.	Cisco IP Communicator <b>right-click &gt; Preferences &gt; Audio</b> tab > <b>Network</b> button.  Or, from Cisco Unified Communications Manager Administration in the Phone Configuration window, Product Specific Configuration section.  Local configuration takes precedence over Cisco Unified Communications Manager configuration.	<a href="#">Selections for Audio Port Range, page 4-11</a>

1. QoS = quality of service
2. RTP = Real-Time Transport Protocol

**Related Topics**

- [About Required Configuration Tasks, page 4-4](#)
- [About Recommended or Optional Configuration Tasks, page 4-10](#)
- [About Helping Users with Configuration Tasks, page 4-14](#)
- [Customizing Cisco IP Communicator, page 6-1](#)
- [Troubleshooting Cisco IP Communicator, page 8-1](#)

## About Required Configuration Tasks

You might need to complete these tasks before Cisco IP Communicator can function properly or before a user can access important features. The necessity of these tasks depends upon variables such as settings on the client PC and the software VPN solution used by the user, among other factors.

Topics in this section include:

- [About Selecting and Tuning Audio Devices, page 4-5](#)
- [About Specifying a TFTP Server, page 4-6](#)
- [About Selecting a Device Name, page 4-7](#)
- [About Audio IP Address Auto-Detection Problems, page 4-9](#)

## About Selecting and Tuning Audio Devices

At first launch after installation, users must select and tune audio devices before using those devices with Cisco IP Communicator. At initial start up, the Audio Tuning Wizard automatically launches, and users must complete the wizard before Cisco IP Communicator launches.

Users are not prompted to use the Audio Tuning Wizard again unless the audio device that they try to select by other means cannot be found (because it has not yet been tuned), or in cases where users directly modify the volume on an audio device. Users can manually launch the Wizard from the Cisco IP Communicator right-click menu or from the Windows Start menu.

For details about installing devices while Cisco IP Communicator is running, see the information about removing and re-installing audio devices in the user guide at this URL:

[http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_user_guide_list.html)

### Related Topics

- [Device Selection for Use with Audio Modes and the Ringer, page 4-5](#)
- [Device Tuning, page 4-5](#)
- [Common Tuning Mistakes, page 4-6](#)

## Device Selection for Use with Audio Modes and the Ringer

Before users can use an audio device that requires a device driver, they must select at least one audio mode (headset, speakerphone, or handset) for the device. Users should also make sure that the device that they want to use to alert them to incoming calls is selected as the ringer. For details about audio mode selections, see the user guide at this URL:

[http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_user_guide_list.html)

### Related Topics

- [Device Tuning, page 4-5](#)
- [Common Tuning Mistakes, page 4-6](#)

## Device Tuning

After selecting a device for each audio mode and the ringer, users must tune the device before using it. Tuning a device means testing and, if necessary, adjusting the input/output levels of the device from the Audio Tuning Wizard.

The Audio Tuning Wizard runs at the first launch of Cisco IP Communicator after installation, pops up if the user tries to select an untuned device from the Preferences menu, and can be launched anytime from the Cisco IP Communicator right-click menu. If users have changed the volume levels for an audio device since last tuning it, Cisco IP Communicator prompts them to retune, revert to previous settings, or cancel.



### Note

Changing the volume level on a USB device directly (such as moving the volume slider on a USB headset) alters the volume level as perceived by the Audio Tuning Wizard. However, changing the volume level on the Cisco IP Communicator interface does not.

Ideally, users should use the Audio Tuning Wizard to establish acceptable volume levels for both listening and speaking for each audio device, and then rely on the volume controls on Cisco IP Communicator to adjust volume levels for listening on a per-call basis thereafter. This strategy allows users to maintain acceptable volume settings in the Audio Tuning Wizard without requiring constant adjustments. In this case, users can choose the revert option when prompted instead of relaunching the Audio Tuning Wizard.

**Related Topics**

- [Device Selection for Use with Audio Modes and the Ringer, page 4-5](#)
- [Common Tuning Mistakes, page 4-6](#)

## Common Tuning Mistakes

Users often initially set the volume levels high from the master or wave sliders in the Audio Tuning Wizard and later reduce the levels by using Microsoft Windows volume controls or laptop sound keys because other applications sound too loud. When users subsequently discover that Cisco IP Communicator sounds too soft, users set the volume button on the main Cisco IP Communicator interface to sharply increase the call volume.

**Note**

---

A high volume setting in the application can cause voices to sound distorted.

---

For details about adjusting the volume through the Audio Tuning Wizard, see the voice quality section in the troubleshooting chapter of the *User Guide for Cisco IP Communicator* at this URL:

[http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_user_guide_list.html)

**Related Topics**

- [Device Selection for Use with Audio Modes and the Ringer, page 4-5](#)
- [Device Tuning, page 4-5](#)

## About Specifying a TFTP Server

You must specify a TFTP server for each Cisco IP Communicator device if either of the these conditions apply:

- You are not using DHCP Option 150 in your network
- You want to specify an alternate TFTP server

**Note**

---

If you specify a device name by using the command line-option when you deploy the application, you do not need to specify the TFTP server address after installation.

---

Unless local access is disabled, users can also specify this setting in Cisco IP Communicator (**right-click** > **Preferences** > **Network** tab > **TFTP Servers** section), but you must tell them which TFTP server addresses to enter.

If your company uses Cisco IP Communicator in an environment where users do not have administrative privileges, and if multiple users share a PC, this task cannot be completed by the user. You must use an administrator account to run Cisco IP Communicator one time after installation on each machine and select the network interface (if this selection is required). This instruction also applies to selecting network interface (device name) in this circumstance.

#### Related Topics

- [How to Deploy the Application, page 3-2](#)
- [About Selecting a Device Name, page 4-7](#)
- [About Local Configuration, page 4-13](#)

## About Selecting a Device Name

Cisco IP Communicator formulates its device name in these ways:

- By using the MAC address of the network interface that it associates with during the installation process. You can specify the network interface by using a command-line option while deploying the Cisco IP Communicator application (see the [“How to Deploy the Application” section on page 3-2](#)). In this case, users do not need to choose a network interface.
- By using a free-form device name. You can specify a free-form device name by using a command-line option while deploying the Cisco IP Communicator application but only if you are integrating with Cisco Unified Communications Manager Release 5.0(1) or later (see the [“How to Deploy the Application” section on page 3-2](#)). In this case, the user does not need to enter the free-form device name.

If you do not use a command-line option to specify a device name, Cisco IP Communicator makes the association automatically during the installation or prompts the user to make a selection:

- If there is only one enabled network interface available on the client PC, Cisco IP Communicator automatically associates with that interface.
- If multiple network interfaces are available, Cisco IP Communicator prompts the user to choose one (first launch only).
- Alternatively, if connecting to Cisco Unified Communications Manager Release 5.0(1) or later, the user can enter a free-form device name. The device name must be less than 15 characters, including alphanumeric characters, dot, dash, and underscores (but no spaces).

If you are using the network interface to create the device name, choosing the correct interface is critical because Cisco IP Communicator uses the MAC address of the associated network interface to identify its device name to Cisco Unified Communications Manager much like hardware-based Cisco Unified IP Phones. Therefore, every time Cisco IP Communicator starts, it verifies that the associated interface is still installed in the client PC. This prevents users from modifying the original device name for Cisco IP Communicator.

#### Related Topics

- [Device Name and Multiple Network Interfaces, page 4-8](#)
- [Device Name and Shared PCs, page 4-8](#)
- [Device Name After Disabling or Removing an Interface, page 4-8](#)

## Device Name and Multiple Network Interfaces

Tell users exactly which network interface to choose when multiple network interfaces exist (for example, a laptop that uses both a wireless (802.11) and wired (Ethernet) network interface, or a laptop with a docking station).

Choose the interface that is most likely to provide permanent connectivity or the one that is always enabled (even if it is inactive). In most cases, this means choosing an integrated Ethernet card over a wireless card, docking station, or PC card. Avoid choosing wireless cards because they can appear disabled if they are not associated with a base station.)

**Note**

At first launch, Cisco IP Communicator automatically chooses an Ethernet interface, if one is present. Because some laptop docking stations contain additional Ethernet interfaces, advise laptop users to undock before launching the application for the first time. Doing so helps Cisco IP Communicator choose the appropriate network.

**Related Topics**

- [Device Name and Shared PCs, page 4-8](#)
- [Device Name After Disabling or Removing an Interface, page 4-8](#)

## Device Name and Shared PCs

If your company uses Cisco IP Communicator in an environment where users do not have administrative privileges, and if multiple users share a PC, a user cannot select the device name. Instead, you must use an administrator account to run Cisco IP Communicator one time after installation on each client PC and select the device name (if this selection is required). This instruction also applies to specifying a TFTP server address in this circumstance, if one is required.

**Related Topics**

- [About Specifying a TFTP Server, page 4-6](#)
- [Device Name and Multiple Network Interfaces, page 4-8](#)
- [Device Name After Disabling or Removing an Interface, page 4-8](#)

## Device Name After Disabling or Removing an Interface

If you use a network interface to create the device name, and if the associated network interface is later disabled or removed, Cisco IP Communicator prompts the user to either re-install the interface or choose a new interface. If you or the user choose a new interface, you must create a new device record in Cisco Unified Communications Manager to preserve the original DN for the user, softkey template, settings, and so on. Delete the old device record.

Tell users to coordinate with you before choosing a new interface.

**Related Topics**

- [Device Name and Multiple Network Interfaces, page 4-8](#)
- [Device Name and Shared PCs, page 4-8](#)

## About Audio IP Address Auto-Detection Problems

If the PC on which Cisco IP Communicator is running uses an unsupported software VPN client, audio IP address auto-detection does not work. The resulting symptom is one-way audio.

- [Supported Software VPN Clients, page 4-9](#)
- [How Cisco IP Communicator Obtains an Audio IP Address with a VPN, page 4-9](#)
- [Resolving Audio IP Address Auto-Detection Problems, page 4-10](#)

### Supported Software VPN Clients

Supported software VPN clients include Cisco Systems VPN Client 3.x or 4.x, and the Microsoft PPTP client. Other third-party VPN clients might be unsupported. A VPN solution is typically unsupported if it is not a Cisco product and does not function like a network interface card.

#### Related Topics

- [How Cisco IP Communicator Obtains an Audio IP Address with a VPN, page 4-9](#)
- [Resolving Audio IP Address Auto-Detection Problems, page 4-10](#)

### How Cisco IP Communicator Obtains an Audio IP Address with a VPN

Software VPN clients are overlaid on top of an existing IP network, meaning that there are essentially two IP addresses on the computer when a VPN is in use:

- The IP address from the underlying network
- The IP address provided by the VPN client that is used by parties on the remote side of the connection to communicate with applications on the computer

Some VPN clients, such as Cisco Systems VPN Client 3.x, assign the VPN IP address at a very low level, which makes it difficult for Cisco IP Communicator to specify the correct address. To eliminate this problem, Cisco IP Communicator queries the Cisco VPN client directly.

Other VPN Clients, such as the Microsoft PPTP client and Cisco VPN Client 4.x appear as alternative network interfaces. In these cases, the IP address can be selected with the same auto-detection process that is used to resolve selection when there are multiple interfaces.

Other third-party VPN clients might be unsupported and result in one-way audio. You can resolve this problem by running the Cisco IP Communicator Administration Tool to create a `getIP.asp` audio IP address reflector web page as described in the [“Resolving Audio IP Address Auto-Detection Problems” section on page 4-10](#). Cisco IP Communicator attempts to fetch this reflector page rather than using other methods of auto-detection. The reflector page returns the IP address from which it sees the request originate, which is a relatively reliable way to identify VPN IP address of Cisco IP Communicator.

#### Related Topics

- [Supported Software VPN Clients, page 4-9](#)
- [Modifications for Remote Use, page 4-12](#)

## Resolving Audio IP Address Auto-Detection Problems

### Before You Begin

Obtain the Administration Tool from the same software download web site as Cisco IP Communicator:

<http://www.cisco.com/cgi-bin/tablebuild.pl/ip-comm>

The tool is located inside the zipped build folder.

### Restriction

This procedure applies to Windows-based Cisco Unified Communications Managers only.

### Procedure

**Step 1** Run the Cisco IP Communicator Administration Tool, and select **Enable HTTP Access**. This creates a getIP.asp reflector web page.

**Step 2** In Cisco Unified Communications Manager Administration, specify the location of the getIP.asp web page on the Phone Configuration window (Product Specific Configuration section, IP Address Autodetection URL field).

By default, getIP.asp is stored at this URL:

<http://<server>/communicatorloads/communicator/getIP.asp>

To change the location of the getIP.asp reflector web page, copy the getIP.asp from the default location, place it in a new location, and enter the new URL in the Cisco Unified Communications Manager Administration (see Step 2). Make sure you place getIP.asp on a Microsoft IIS Web server so that auto-detection works properly.



### Tip

You can access the audio IP address settings from Cisco IP Communicator (**right-click** > **Preferences** > **Audio** tab > **Network** button > **Audio IP Address** section).

### Related Topics

- [Supported Software VPN Clients, page 4-9](#)
- [How Cisco IP Communicator Obtains an Audio IP Address with a VPN, page 4-9](#)
- [Modifications for Remote Use, page 4-12](#)

## About Recommended or Optional Configuration Tasks

You might need to complete these recommended configuration tasks because of certain network conditions (to improve audio quality, specify custom port range for RTP audio, or to modify settings for remote users on VPNs).

- [Modification of Advanced Audio Settings, page 4-11](#)
- [Selections for Audio Port Range, page 4-11](#)
- [Modifications for Remote Use, page 4-12](#)

## Modification of Advanced Audio Settings

Modifying advanced audio properties are optional. Users might want to increase noise suppression levels to reduce or eliminate background noise. You access the advanced audio settings from Cisco IP Communicator (**right-click** > **Preferences** > **Audio** tab > **Advanced** button).

For details about the fields in this window and for troubleshooting voice quality issues, see the user guide at this URL:

[http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps5475/products_user_guide_list.html)

### Related Topics

- [Selections for Audio Port Range, page 4-11](#)
- [Modifications for Remote Use, page 4-12](#)

## Selections for Audio Port Range

You might need to select an audio port range for Cisco IP Communicator to use if the network uses a custom port range for RTP audio. For example, if a single port is opened to allow audio to pass through a firewall or if a policy has been applied to only those routers and switches with a restricted range of RTP ports.

You can do this from the Phone Configuration window (Product Specific Configuration section) in Cisco Unified Communications Manager Administration. Alternately, users can do this from Cisco IP Communicator (**right-click** > **Preferences** > **Audio** tab > **Network** button > **Audio Port Range** section).



### Note

---

The Audio Port Range controls in Cisco IP Communicator are not functional when the device is configured as SIP in Cisco Unified Communications Manager. Instead, the port setting is in the SIP device profile.

---



### Note

---

Unless local settings access is disabled, you can configure the audio port range locally (on the client PC) and remotely (in Cisco Unified Communications Manager Administration). Be aware that if the value is modified locally, the modified value becomes the active value, overwriting or preempting a value that is specified remotely. Therefore, once a setting is modified on the client PC, the only way to change it is on the client PC.

---

### Related Topics

- [QoS Modifications to Prioritize Voice Traffic, page 1-9](#)
- [Modifications for Remote Use, page 4-12](#)
- [About Local Configuration, page 4-13](#)

## Modifications for Remote Use

Depending on the VPN client that is used to connect to the network, users who run Cisco IP Communicator remotely, or outside of the LAN, might need to modify certain settings in Cisco IP Communicator. [Table 4-3](#) describes these settings.

**Table 4-3** *Modifications for Remote Use*

Configuration Task	Purpose	Where to Do It
Optimize for low bandwidth.	<p>Remote users with low-bandwidth connections might experience better audio quality by using a low-bandwidth codec.</p> <p>For details about supported audio formats, see the release notes at this URL:  <a href="http://www.cisco.com/en/US/products/sw/voice/sw/ps5475/prod_release_notes_list.html">http://www.cisco.com/en/US/products/sw/voice/sw/ps5475/prod_release_notes_list.html</a></p>	Cisco IP Communicator <b>right-click &gt; Preferences &gt; Audio tab &gt; Optimize for Low Bandwidth.</b>
Specify the TFTP address at first startup.	<p>Remote users are probably not going to receive their TFTP address from DHCP. However, Cisco IP Communicator caches the last TFTP address that it received and tries to use it the next time it starts up.</p> <p>First-time remote users with a freshly installed application cannot use Cisco IP Communicator until they have specified a TFTP address.</p>	<p>Cisco IP Communicator <b>right-click &gt; Preferences &gt; Network tab &gt; Use these TFTP Servers.</b></p> <p>See the “<a href="#">About Specifying a TFTP Server</a>” section on page 4-6.</p>
Run the Cisco IP Communicator Administration Tool.	<p>Obtain the tool from the product software download web site:  <a href="http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278468661">http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278468661</a>.</p> <p>It is located inside the zipped folder with your build.</p> <p>Enabling HTTP access improves the performance for remote users.</p> <p>It resolves audio IP address auto-detection problems caused by unsupported software VPN clients. You must enter the URL for getIP.asp (an IP address reflector page) in Cisco Unified Communications Manager Administration.</p>	<p>Cisco IP Communicator <b>right-click &gt; Preferences &gt; Audio tab &gt; Network &gt; Audio IP Address</b> section.</p> <p>See the “<a href="#">Resolving Audio IP Address Auto-Detection Problems</a>” section on page 4-10.</p>

### Related Topics

- [About Helping Users with Configuration Tasks](#), page 4-14
- [Troubleshooting Cisco IP Communicator](#), page 8-1

## About Local Configuration

Many required and recommended configuration tasks can be performed locally on the client PC by you or the user. However, the tasks that require access to Cisco Unified Communications Manager Administration must be performed by you.

Some settings (such as configuring a custom audio port range) can be configured both locally (on the client PC) and remotely (in Cisco Unified Communications Manager Administration). Be aware that if a value is modified locally, the modified value becomes the active value, overwriting or preempting a value that is specified remotely. Therefore, once a setting is modified on the client PC, the only way to change it is on the client PC.

To prevent this scenario, you can disable access to some network settings so that they appear grayed-out on the client PC.

### Related Topics

- [About Disabling Local Settings Access, page 4-13](#)

## About Disabling Local Settings Access

To prevent users from modifying settings that you have already specified and which are normally accessible from the client PC (such as the Alternate TFTP Server setting), you must disable settings access when you provision the Cisco IP Communicator device record prior to deployment. Otherwise, if a user modifies these settings, you are locked out of performing any changes remotely and must override local settings from the client desktop.



### Note

---

Keep in mind that local configuration (on the client PC) always takes precedence over remote configuration (from Cisco Unified Communications Manager Administration) for those settings that are accessible from both locations.

---

You disable settings access on the Phone Configuration window (Product Specific Configuration section, Settings Access field) in Cisco Unified Communications Manager Administration.

The affected settings appear grayed-out in Cisco IP Communicator:

- All settings accessed from the Settings button
- Settings in Cisco IP Communicator:
  - **right-click > Preferences > Network** tab: all settings in the TFTP Servers section and the Use This Device Name field
  - **right-click > Preferences > Audio** tab > **Network** button: all settings in the Audio Port Range section

### Related Topics

- [About Specifying a TFTP Server, page 4-6](#)
- [Selections for Audio Port Range, page 4-11](#)
- [Disabling the Internal Web Server, page 4-14](#)
- [About Helping Users with Configuration Tasks, page 4-14](#)

# Disabling the Internal Web Server

If necessary, you can disable the internal web server for Cisco IP Communicator. You might do this for these reasons:

- Security
- The internal web server interferes with another web server running on the PC.

To disable the server, create a Windows registry value using the regedit utility.

## Restrictions

Disabling the internal web server prevents remote access to operational information.

## Procedure

- 
- Step 1** Open Windows regedit from the command line or from **Start > Run**.
- Step 2** In regedit, choose **HKEY\_LOCAL\_MACHINE\SOFTWARE\Cisco Systems, Inc.\Communicator**.
- Step 3** From the Edit menu, choose **New > DWORD value**.
- Step 4** Rename the value WebServerDisabled (this value does not appear by default), and set it to any non-zero value.
- 



### Tip

To enable the web server again, delete this key or set it to zero.

---

## Related Topics

- [About Operational Information Displayed Remotely from a Web Page, page 7-14](#)

# About Helping Users with Configuration Tasks

With a few exceptions, most of the configuration tasks that are recommended or required for Cisco IP Communicator to function properly must be performed on the client PC and are likely to be performed by users.

As the administrator, you should be prepared to perform configuration tasks at the client PC on behalf of users, or you should provide users with the specific information necessary to complete these tasks. The *User Guide for Cisco IP Communicator* provides general information to help users perform the configuration, but users are likely to need more specific direction from you—most tasks are recommended on the basis of certain technical conditions that users might not know how to recognize or interpret.

## Related Topics

- [Overview of Configuration Tasks, page 4-1](#)
- [Providing Information to Users About Cisco IP Communicator, page A-1](#)