Configuring Features, Templates, Services, and Users

After you install Cisco Cius devices in your network, configure their network settings, and add them to Cisco Unified Communications Manager, you must use Cisco Unified Communications Manager Administration to configure telephony features, optionally modify phone templates, set up services, and assign users.

This chapter provides an overview of these configuration and setup procedures. Cisco Unified Communications Manager Administration documentation provides detailed instructions for these procedures.

For suggestions about how to provide users with information about features and what information to provide, see Providing Information to Users Through a Website.

For information about setting up Cisco Cius devices in non-English environments, see Supporting International Users.

This chapter comprises the following topics:

Telephony Features Available for Cisco Cius

After you add a Cisco Cius to Cisco Unified Communications Manager, you can add functionality to the Cisco Cius. The following table includes a list of supported telephony features, many of which you can configure using Cisco Unified Communications Manager Administration. The Reference column lists Cisco Unified Communications Manager and other documentation that contains configuration procedures and related information.

For more information about using these features, see the *Cisco Cius User Guide*.

Note Cisco Unified Communications Manager Administration also provides several service parameters that you can use to configure various telephony functions. For more information about accessing and configuring service parameters, see the Cisco Unified Communications Manager Administration Guide. For more information about the functions of a service, click on the name of the parameter or the question mark help button in the **Service Parameter Configuration** window.

Table 1: Telephony Features for Cisco Cius

Feature	Description	Configuration reference
All Calls	Allows a user to view a list of active and held calls, sorted in chronological order (oldest first), and incoming and completed calls, sorted newest to oldest	• For more information, see the *Cisco Cius User Guide*. • Requires no configuration.
Auto Dial	Allows the Cisco Cius user to choose from matching numbers in the Recent Call History, which includes placed, received and missed calls. To place the call, the user can choose a number from any of these call lists or continue to enter digits manually.	Requires no configuration.
Barge	Allows a user to join a nonprivate call on a shared phone line. Barge features adds a user to a call and converts it into a conference, allowing the user and other parties to access conference features. **Note** Cisco Cius can still use barge after the Built In Bridge Enable service parameter is set to off. To prevent a user from using the Barge feature on Cisco Cius, you must disable Barge in Feature Control Policy for the Cisco Cius device.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, Cisco Unified IP Phone Configuration chapter. • *Cisco Unified Communications Manager System Guide*, Cisco Unified IP Phone chapter. • *Cisco Unified Communications Manager Features and Services Guide*, Barge and Privacy chapter. • *Cisco Unified Communications Manager Administration Guide*, Feature Control Policy Configuration chapter.
Busy Lamp Field (BLF)	Allows a user to monitor the call state of a directory number associated with a speed-dial button, call log, or directory listing on Cisco Cius.	For more information, go to the Presence chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Feature	Description	Configuration reference
Call Forward	Allows users to redirect incoming calls to another number. Call forward options include Call Forward All, Call Forward Busy, Call Forward No Answer, and Call Forward No Coverage. Additional options include allowing calls that are placed from target number to ring through rather than be forwarded and preventing a call-forward loop from exceeding the maximum number of links in a call-forwarding chain. Call forward options can be assigned on a per-line basis.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, Directory Number Configuration chapter. • *Cisco Unified Communications Manager System Guide*, Cisco Unified IP Phone chapter. • Managing the User Options Web Pages, on page 30
Calling Line Identification (CLID)	Allows a user to enable the full, external number to be used for calling line identification.	For more information, see the Cisco Unified IP Phonechapter in the *Cisco Unified Communications Manager System Guide*.
Calling Line Identification Presentation (CLIP/CLIR)	Allows a user to enable or restrict the originating caller number on a case-by-case basis.	For more information, see the Cisco Unified IP Phone chapter in the *Cisco Unified Communications Manager System Guide*.
Conference	• Allows a user to talk simultaneously with multiple parties by calling each participant individually. • Allows any participant in a standard (ad hoc) conference to add or remove participants. • Allows users to join two or more calls that are on one line to create a conference call and remain on the call.	The service parameter Advance Adhoc Conference (disabled by default in Cisco Unified Communications Manager Administration) allows you to enable these features. For information about conferences, go to the Conference Bridges chapter in the *Cisco Unified Communications Manager System Guide*. For more information, see the Cisco Unified IP Phone chapter in the *Cisco Unified Communications Manager System Guide*. **Note** Be sure to inform your users whether these features are activated.

Feature	Description	Configuration reference
Divert	After Enhanced Immediate Divert is enabled, it allows users to divert incoming calls directly to their voice messaging system.	For more information about diverting calls to voicemail, go to the Immediate Divert chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For more information about Enhanced Immediate Divert, see the Cisco Unified IP Phone chapter in the *Cisco Unified Communications Manager System Guide*.
Dock/Undock	Allows a user to continue a call that was initiated when the Cisco Cius device was docked when the user undocks the device.	*Cisco Cius User Guide*
Do Not Disturb (DND)	When DND is turned on, either no audible rings occur during the ringing-in state of a call, or no audible or visual notifications of any type occur. **Note** DND does not affect 911 calls. You can configure Cisco Cius to have a phone-button template with DND as one of the selected features. The following DND-related parameters are configurable in Cisco Unified Communications Manager Administration: • Do Not Disturb - This check box allows you to enable DND on a per-device basis. Choose **Cisco Unified Communications Manager Administration** > **Device** > **Phone** > **Phone Configuration**. • DND Incoming Call Alert - Choose the type of alert to play, if any, on a Cisco Cius for incoming calls when DND is active. This parameter is located on both the Common Phone Profile window and the Phone configuration window (Phone Configuration window value takes precedence). BLF Status Depicts DND - Enables DND status to override busy/idle state.	For more information, go to the Do Not Disturb chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Feature	Description	Configuration reference
Hold Status	Enables Cisco Cius devices with a shared line to distinguish between the local and remote lines that placed a call on hold.	No configuration is required.
Hold/Resume	Allows the user to move a connected call from an active state to a held state. To place a call on hold, tap the Hold button. To resume a call, choose the line with the held call and tap the Hold button.	Requires no configuration, unless you want to use music on hold. See Music-on-Hold in this table for information.
Ignore	Allows a user to ignore an incoming call from the notification window.	No configuration is required.
Message Waiting Indicator	A light on the media station handset that indicates that a user has one or more new voice messages.	For more information see: • *Cisco Unified Communications Manager Administration Guide*, Message Waiting Configuration chapter. • *Cisco Unified Communications Manager System Guide*, Voice Mail Connectivity to Cisco Unified Communications Manager chapter.
Music On Hold	Plays music while callers are on hold.	For more information see the Music On Hold chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Mute	Mutes the audio input for all input devices including, bluetooth and 3.5 mm handsets, media station and device speakers, and headset.	Requires no configuration.
Plus Dialing	Allows the user to dial E.164 numbers prefixed with a + sign. To dial the + sign, the user needs to press and hold the * key for at least 1 second. This applies to dialing the first digit for an on-hook or off-hook call only.	Requires no configuration.

Feature	Description	Configuration reference
Protected Calling	Provides a secure (encrypted) connection between two Cisco Cius devices or a Cisco Cius and IP phone. A security tone is played at the beginning of the call to indicate that both devices are protected. Some features, such as conference calling, shared lines, and Join Across Lines are not available when protected calling is configured. Protected calls are not authenticated.	For more information about security, see the Overview of Supported Security Features. For additional information, see the *Cisco Unified Communications Manager Security Guide*.
Ringtone Setting	Identifies ring type used for a line when Cisco Cius has another active call.	For more information, see the *Cisco Unified Communications Manager Administration Guide*, Directory Number Configuration chapter.
Ringtone	Users can customize how their Cisco Cius indicates an incoming call and a new voice message.	For more information, see the *Cisco Cius User Guide*.

Feature	Description	Configuration reference
Secure and Nonsecure Indication Tone		Requires no configuration.

Feature	Description	Configuration reference
	After a Cisco Cius is configured as secure (encrypted and trusted) in Cisco Unified Communications Manager, it can be given a protected status. After that, if desired, the protected device can be configured to play an indication tone at the beginning of a call: • Protected Device - To change the status of a secure Cisco Cius to protected, check the **Protected Device** check box in **Cisco Unified Communications Manager Administration** > **Device** > **Phone** > **Phone Configuration**. • Play Secure Indication Tone - To enable the protected Cisco Cius to play a secure or nonsecure indication tone, set the Play Secure Indication Tone to True. (The default is False.) You set this option in **Cisco Unified Communications Manager Administration** > **System** > **Service Parameters**. Select the server and then the Unified CM service. In the Service Parameter Configuration window, select the option in the Feature - Secure Tone area. (The default is False.) Only protected Cisco Cius devices hear these secure or nonsecure indication tones. (Nonprotected devices never hear tones.) If the overall call status changes during the call, the indication tone changes accordingly. At that time, the protected device plays the appropriate tone. A protected device plays or does not play a tone under these circumstances: • After the option to play the tone is enabled, Play Secure Indication Tone option is enabled (True): ◦ When end-to-end secure media is established and the call status is secure, Cisco Cius plays the secure indication tone (three long beeps with pauses). ◦ After end-to-end nonsecure media is established and the call status is nonsecure, Cisco Cius	

Feature	Description	Configuration reference
	plays the nonsecure indication tone (six short beeps with brief pauses). • If the Play Secure Indication Tone option is disabled, no tone is played.	
Secure Conference	• Allows secure Cisco Cius devices to place conference calls using a secure conference bridge. • As new participants are added, the secure call icon is displayed as long as all participants use secure devices. • The Conference List indicates the security level of each conference participant. Initiators can remove nonsecure participants from the Conference List. (Any participant can add or remove conference participants if the Advanced Adhoc Conference Enabled parameter is set.)	For more information about security, see the Overview of Supported Security Features. For additional information, see: • *Cisco Unified Communications Manager System Guide*, Conference Bridges chapter • *Cisco Unified Communications Manager Administration Guide*, Conference Bridge Configuration chapter • *Cisco Unified Communications Manager Security Guide*.
Shared Line	Allows a user to have multiple Cisco Cius devices that share the same phone number or allows a user to share a phone number with a coworker.	For more information, see the Understanding Directory Numbers chapter in the *Cisco Unified Communications Manager System Guide*.
Speed Dial	Allows a user to configure speed dial to a specific destination directory number.	-
Transfer	Allows users to redirect connected calls from their Cisco Cius device to another number. The user can connect two calls to each other. The user can remain on the line or transfer the call without staying on line.	Requires no configuration.
Unified Mobility	Allows users to extend call control capabilities of Cisco Unified Communications Manager from the primary workplace desk phone of a mobile worker to any location or device of their choosing.	For more information see the Cisco Unified Mobility chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Feature	Description	Configuration reference
Voice Messaging System	Enables callers to leave messages if calls are unanswered.	For more information see: • *Cisco Unified Communications Manager Administration Guide*, Cisco Voice-Mail Port Configuration chapter. • *Cisco Unified Communications Manager System Guide*, Voice Mail Connectivity to Cisco Unified Communications Manager chapter. • Configuring Visual Voicemail for Cius Devices, on page 22.

Configuring Product-Specific Options

Cisco Unified Communications Manager Administration allows you to set some product-specific configuration parameters for Cisco Cius in any of the following windows:

- Enterprise Phone Configuration window (**System** > **Enterprise Phone Configuration**)
- Common Phone Profile window (**Device** > **Device Settings** > **Common Phone Profile**); Product Specific Configuration Layout portion of window
- Device Phone Configuration window (**Device** > **Phone** > **Add New** > **Cius**); Product Specific Configuration Layout portion of window

The following table shows the product-specific configuration options.

Table 2: Cisco Cius Product-Specific Configuration Options

Feature	Description	Default
Disable USB	Disables the USB ports on the device and media station.	False.
SDIO	Indicates whether the SDIO device on the device is enabled or disabled.	Disabled.
Bluetooth	Indicates whether the Bluetooth service on the Cisco Cius device can or cannot be enabled.	Enabled.

Feature	Description	Default
Days Display Not Active	Allows the user to specify the days that the backlight is to remain off by default.	Typically this would be Saturday and Sunday for U.S. corporate customers. **Note** The list contains all of the days of the week. To turn off backlight on Saturday and Sunday hold down Control and select Saturday and Sunday.
Display On Time	Indicates the time of day the display is to automatically turn itself on for days listed in the off schedule.	07:30. Maximum length: 5. **Note** Enter value in a 24-hour format, where 0:00 is the beginning of the day and 23:59 is the end of the day.
Display On Duration	Indicates the amount of time the display is to be active when it is turned on by the programmed schedule.	10:30. Maximum length: 5. **Note** Maximum value is 24 hours. This value is in hours and minutes format. “1:30” would activate the display for 1 hour and 30 minutes.
Display Idle Timeout	Indicates how long to wait before the display is turned off when it was turned on by user activity.	01:00 Maximum length: 5 **Note** Maximum value is 24 hours. This value is in hours and minutes format. “1:30” would turn off the display after 1 hour and 30 minutes of inactivity. For more information, see the Configuring Screen Lock and Display Idle Time Out, on page 24.
Display On When Incoming Call	When the device is in screen saver mode, this will turn the display on when a call is ringing.	Enabled.
RTCP	Maintains statistic for audio. Also used for lip sync in video calls.	Disabled.

Feature	Description	Default
Advertise G.722 and iSAC Codecs	Indicates whether the phone application will advertise the wideband codecs to the Cisco Unified Communications Manager. Codec negotiation involves two steps: 1 The phone application must advertise the supported codecs to the Cisco Unified Communications Manager. 2 When the Cisco Unified Communications Manager gets the list of supported codecs from all phones involved in the call attempt, it chooses a commonly supported codec based on various factors, including the region pair setting.	Use System Default Valid values: • System Default - Phone application will defer to the setting specified in the enterprise parameter, Advertise G.722 and iSAC Codecs. • Disabled - Phone application will not advertise the wideband codecs to the Cisco Unified Communications Manager. • Enabled - Phone application will advertise the wideband codecs to the Cisco Unified Communications Manager.
Video Calling	When enabled, indicates that the device will participate in video calls.	Enabled.

Feature	Description	Default
Wifi	Indicates whether the Wi-Fi on the device is enabled or disabled.	Enabled. **Note** For the Enterprise and Common settings, the Wifi parameter is set at the default value (enabled) and the **Override Common Settings** check box is checked. **Note** For the Device setting, the Wifi parameter is left at the default value (enabled) but without the **Override Common Settings** check box checked. **Tip** Cisco recommends that a new common phone profile be created for Cisco Cius devices with **Wifi** parameter set to enabled if the deployment environment default setting at the enterprise and common level is disabled, unless it is the company's policy to set the Wifi default to disabled for all devices.
PC Port	Indicates whether the PC port on the media station is enabled or disabled. **Note** The port labeled **COMPUTER** on the back of the media station connects a PC or workstation to the media station so they can share a single network connection.	Enabled.
Span to PC Port	Indicates whether the device will forward packets transmitted and received on the media station network port to the PC port. **Note** Select **Enabled** if an application is being run on the PC port that requires monitoring of the device traffic, such as monitoring and recording applications or network packet-capture tools used for diagnostic purposes. To use this feature PC Voice VLAN access must be enabled.	Disabled.

Feature	Description	Default
PC Voice VLAN Access	Indicates whether a device attached to the PC port on the media station is allowed access to the Voice VLAN. **Note** Disabling Voice VLAN Access prevents the attached PC from sending and receiving data on the Voice VLAN. It also prevents the PC from receiving data sent and received by the device.	Enabled.
PC Port Remote Configuration	Allows remote configuration of the PC port speed and duplex of the device when docked.	Disabled.
Switch Port Remote Configuration	Allows remote configuration of the switch port speed and duplex of the device when docked. This overrides any manual configuration on the device. **Caution** Be aware that configuring this port may cause the device to lose network connectivity when it is on the media station.	Disabled.
Gratuitous ARP	Indicates whether the device will learn MAC addresses from Gratuitous ARP responses. **Note** Disabling the device ability to accept Gratuitous ARP will prevent applications that use this mechanism for monitoring and recording of voice streams from working.	Disabled.
Cisco Discovery Protocol (CDP): Switch Port	Allows administrator to enable or disable CDP on the media station switch port. **Warning** Disable CDP on the Network port only if the media station is connected to a non-Cisco switch. For further details, consult the Cisco Unified Communications Manager Administration Guide.	Enabled.
Cisco Discovery Protocol (CDP): PC Port	Indicates whether CDP is supported on the PC port.	Enabled.
Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port	Allows administrator to enable or disable Link Layer Discovery Protocol (LLDP-MED) on the media station switch port.	Enabled.

Feature	Description	Default
Link Layer Discovery Protocol (LLDP): PC Port	Allows administrator to enable or disable Link Layer Discovery Protocol (LLDP) on the media station PC port.	Enabled.
LLDP Asset ID	Allows administrator to set Asset ID for Link Layer Discovery Protocol.	Maximum length: 32.
LLDP Power Priority	Allows administrator to set Power Priority for Link Layer Discovery Protocol.	Unknown.
Power Negotiation	Allows administrator to enable or disable Power Negotiation. **Note** Enable the Power Negotiation feature when the media station is connected to a switch that supports power negotiation. However, if a switch does not support power negotiation, disable the Power Negotiation feature before you power up accessories over PoE+.	Enabled.
802.1x Authentication	Specifies the 802.1x authentication feature status. Options: • Enabled - Cisco Cius uses 802.1X authentication to request network access. • Disabled - Default setting in which the Cisco Cius uses CDP to acquire VLAN and network access.	User Controlled.
Always On VPN	Indicates whether the device will always start the VPN AnyConnect client and establish a connection with the configured VPN profile from Cisco Unified Communications Manager.	False. For more information about configuring VPN from Cisco Unified Communications Manager, see the VPN Configuration from Cisco Unified Communications Operating System Administration Guide, on page 18.
Allow User-Defined VPN Profiles	Controls whether the user can use the AnyConnect VPN client to create VPN profiles. If disabled, the user cannot create VPN profiles.	True. For more information about configuring VPNs on Cisco Cius, see the VPN Settings Menu Options.

Feature	Description	Default
Require Screen Lock	Indicates whether screen lock is required on the device. Options: • User controlled. • PIN - A numeric password that is at least four digits long. • Password - An alphanumeric password, consisting of at least four alphanumeric characters, one of which must be a non-numeric character, and one must be a capital letter.	PIN. For more information, see the Configuring Screen Lock and Display Idle Time Out, on page 24.
Screen Lock Timeout	Indicates maximum idle time in seconds before the device automatically locks the screen. After the screen is locked, the user password is required to unlock it	Default: 600. Minimum: 15. Maximum: 1800. For more information, see the Configuring Screen Lock and Display Idle Time Out, on page 24.
Lock Device	Allows the administrator to lock the device to prevent unauthorized user access.	Disabled.
Wipe Device	Allows the administrator to erase the user data and configuration on the device.	Disabled.
Secure Shell (SSH) Access	Determines whether the device will accept SSH connections. Disabling the SSH server functionality of the device will block access to the device. • Enabled. • Disabled.	Disabled.
Load Server	Indicates that the device will use an alternative server to obtain firmware loads and upgrades, rather than the defined TFTP server.	Hostname or the IP address of local server. Maximum length: 256.
Peer Firmware Sharing	Enables or disables Peer to Peer image distribution in order to allow a single device in a subnet to retrieve an image firmware file and then distribute it to its peers.	Enabled.
Log Server	Specifies an IP address and port of a remote system to which log messages are sent.	IP address of remote system. Maximum length: 32.

Feature	Description	Default
Web Access	Indicates whether the device will accept connections from a web browser or other HTTP client.	Disabled.
Android Debug Bridge (ADB)	Enables or disables the ADB on the device. Can be set to Enabled, Disabled, or User Controlled.	Disabled.
Allow Applications from Unknown Sources	Controls whether the user can install Android applications on the device from a URL or from Android packages (APK) that are received through email, through instant message (IM), or from a Secure Digital (SD) card. Can be set to Enabled, Disabled, or User Controlled.	Disabled.
Allow Applications from Android Market	Controls whether the user can install Android applications from the Android Marketplace.	False.
Allow Applications from Cisco AppHQ	Controls whether the user can install Android applications from Cisco AppHQ.	False.
AppHQ Domain	The fully-qualified domain name to use when users log into AppHQ. If empty, the user will specify their own domain name along with their username. The AppHQ domain is used to associate the user to a given Custom AppHQ store, if it exists. Example: cisco.com.	Empty field. Maximum length: 256.
Enable Cisco UCM App Client	Controls whether the Application Client runs on the device. When the Application Client is enabled, users can select the applications they want to install from the Cisco Unified Communications Manager.	False.
Company Photo Directory	Specifies the URL that the device can query for a user and get the image associated with that user. Example: http://www.cisco.com/dir/photo/zoom/%%uid%%, where uid is employee user ID.	Photo directory URL. Maximum length: 256.
Voicemail Server (Primary)	Hostname or IP address of the primary visual voicemail server.	IP address of primary visual voicemail server. Maximum length: 256.

Feature	Description	Default
Voicemail Server (Backup)	Hostname or IP address of the backup visual voicemail server.	IP address of backup visual voicemail server. Maximum length: 256.
Presence and Chat Server (Primary)	Hostname or IP address of the primary presence server.	IP address of primary presence server. Maximum length: 256.
Presence and Chat Server Type	Specifies the type of secondary presence and IM server for the device to use. Can be set to Cisco Unified Presence or Cisco WebEx Connect.	Cisco WebEx Connect.
Presence and Chat Single Sign-On (SSO) Domain	The enterprise domain used by Cisco WebEx Connect Cloud to perform Single-Sign-On (SSO) authentication against an enterprise.	Empty field. Maximum length: 256.

Note For additional configuration information, see the Cisco Cius Wireless LAN Deployment Guide.

Override Common Settings check box

After you set the parameters, check the Override Common Settings check box for each setting you wish to update. If you do not check this check box, the corresponding parameter setting does not take effect. If you set the parameters at the three configuration windows, the setting takes precedence in the following order:

- **Phone Configuration** window
- **Common Phone Profile** window
- **Enterprise Phone Configuration** window

VPN Configuration from Cisco Unified Communications Operating System Administration Guide

The VPN Settings menu allows you to enable the VPN Client connection using the Secure Sockets Layer (SSL). Use the VPN connection when Cisco Cius is located outside a trusted network or when network traffic between Cisco Cius and Cisco Unified Communications Manager must cross untrusted networks.

Follow these steps from to configure VPN profiles. For more information, see the Cisco Unified Communications Manager Security Guide and the Cisco Unified Communications Operating System Administration Guide.

Procedure

Step 1 Set up VPN Concentrators for each VPN Gateway.

Step 2 Upload VPN certificates to a new Phone-VPN-Trust.

Step 3 Configure VPN Gateways. Choose **Advanced Features** > **VPN** > **VPN Gateway**.

Step 4 Enter Gateway Name, Description, and URL.

Note Up to 10 certificates can be assigned to a VPN Gateway. Assign at least one certificate to each gateway. Only certificates associated with the VPN role display in the available VPN certificates list.

The VPN Gateway URL is for the main concentrator in the gateway.

Step 5 Configure VPN Group. Choose **Advanced Features** > **VPN** > **VPN Group**.

Note Up to three VPN Gateways can be added to a VPN Group. The total number of certificates in the VPN Group cannot exceed 10.

Step 6 Configure VPN Profile. Choose **Advanced Features** > **VPN** > **VPN Profile**.

Note If **Enable Auto-Detect Network Connection** is enabled, the VPN client runs only if it detects that it is out of the corporate network.

If **Host ID Check** is enabled, the VPN Gateway certificate Common Name must match the URL to which the VPN client is connected.

If **Enable Password Persistence** is enabled, user password will be saved in Cisco Cius until a sign-in failure occurs.

Step 7 Configure VPN Feature. Choose **Advanced Features** > **VPN** > **VPN Feature Configuration**.

Step 8 Assign a Common Phone Profile. Choose **Device** > **Device Settings** > **Common Phone Profile**.

VPN Configuration Settings

The following table describes the VPN configuration options for Cisco Cius on Cisco Unified Communications Manager.

Table 3: VPN Configuration Options for Cisco Cius

Option	Description	To change
Administrator Provisioned VPN Gateway	VPN enabled with VPN Group Configuration.	Display Only - Cannot change.

Option	Description	To change
User Defined VPN Profiles	Shows if option is enabled or disabled.	Choose **Device** > **Device Settings** > **Product Specific Configuration**. Set Allow User Defined Profiles to On or Off. **Note** Available for multilevel configurations. Administrator may change at device, common, or enterprise levels. If the feature is disabled on the Cisco Unified Communications Manager, user-defined VPN profiles are removed from the list on Cisco Cius and **Add New VPN Connection** is disabled.
Always Require VPN	Shows if option is enabled or disabled.	Choose **Device** > **Device Settings** > **Product Specific Configuration**. Set Always Require VPN to On or Off. **Note** Always Require VPN setting overwrites enable and autoNetworkDetect values to True.

Note Network configuration changes can potentially affect an active VPN connection.

If VPN is enabled, no proxy will be configured or used for VPN.

VPN Authentication

Cisco Cius supports the following VPN authentication methods:

- Username and password
- Certificate only
- Password only

Note For Password Only authentication, the deviceID is prefilled as the username; Adaptive Security Appliance (ASA) configures the username.

The authentication specified on Cisco Unified Communications Manager must match authentication set on the ASA. If the authentication specified on Cisco Unified Communications Manager does not match that on the ASA, the user VPN is still allowed, but password persistence and autoConnect features are not applicable.

For more information on configuring VPNs on Cisco Cius, see the VPN Settings Menu Options.

AnyConnect VPN

AnyConnect is a VPN client that provides remote users with secure VPN connections to the Cisco 5500 Series ASA running ASA Version 8.0, and later (with AnyConnect Mobile License) or Adaptive Security Device Manager (ASDM) 6.0 and later.

For more information on ASA, see http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html.

Configuring Video Transmit Resolutions

Cisco Cius supports video calling via a 7-inch (177.8 mm), high-resolution multitouch color LCD and integrated camera. For Cisco Cius to send and receive video, that capability must be enabled in Cisco Unified Communications Manager. For more information, see the Configuring Product-Specific Options, on page 10.

To enable Cisco Cius to start streaming video immediately at the beginning of the call, enable **Video Calls** on the **Call Settings** menu (**Settings** > **Call settings**). The following table describes the optional values for the parameter.

Table 4: Video Call Settings

Option	Description
Off	Off
On - Good	On and set to experience a good video quality (CIF)
On - Better (Recommended)	On and set to experience a better video quality(w360p)
On - Best	On and set to experience the best video quality (720p)

Note When the Video Calls option is set to Off, the Auto Transmit Video setting will be grayed out. All video settings under the Call settings menu will be grayed out if Video Calling is disabled in the **Product Specific Configuration Layout** Window.

The following table summarizes the video resolutions and capabilities that Cisco Cius supports.

Table 5: Cisco Cius Video Transmit Resolutions and Capabilities

Resolution	Display parameters	Frame rate	Minimum bandwidth
QCIF	176 x 144	15 fps	16 kbps
QCIF	176 x 144	30 fps	64 kbps
CIF	352 x 288	15 fps	250 kbps
CIF	352 x 288	30 fps	250 kbps
w360p	640 x 360	15 fps	400 kbps
w360p	640 x 360	30 fps	400 kbps
VGA	640 x 480	15 fps	500 kbps
VGA	640 x 480	30 fps	500 kbps
720p	1280 x 720	30 fps	1000 kbps

Note Cisco Cius prefers w360p resolution over VGA; for bandwidths ranging from 400 kbps to 999 kbps, Cisco Cius will send w360p.

Configuring Instant Messaging and Presence

Instant Messaging and Presence (IM&P) allows users to communicate any time, any place, and with any device. Cisco Cius supports Jabber IM with either CUP or WebEx backend server. For security reasons, all cloud-based IM&P traffic is routed via proxy. See the Configuring Web Proxy, on page 24 for more information on configuring proxy.

Instant Messaging and Presence is configured at the device, group, or enterprise levels in the Product Specific Configuration window of Cisco Cius. See the Configuring Product-Specific Options, on page 10 for appropriate navigation in Cisco Unified Communications Manager Administration. Enter the Host name or IP address for the Presence and IM Server (Primary) and Presence and IM Server (Backup), and indicate the Presence and IM Server type. See Configuring Product-Specific Options, on page 10 for more information.

Configuring Visual Voicemail for Cius Devices

Visual Voicemail is configured for all Cius devices or to an individual user or group of users from Cisco Unified Communications Manager Administration. Use the following procedure to configure Visual Voicemail for all Cius devices:

Procedure

Step 1 In Cisco Unified Communications Manager Administration choose **Device** > **Device Settings** > **Common Phone Profile**.

Step 2 Select **Find** and choose **Standard Common Phone Profile**.

Step 3 In the **Product Specific Configuration Layou**t window, enter the following information in the **Voicemail Server (Primary)** field:

- If configuring for Cisco Unity Connection standalone configuration, enter the fully qualified domain name of the Cisco Unity Connection system.
- If configuring for Cisco Unity Connection failover configuration, enter the DNS alias of the Cisco Unity Connection system.

  Note Only Cisco Unity Connection is supported. Cisco Cius Visual Voicemail is not supported with Cisco Unity.

Step 4 Save changes and click **Apply Config**.
For more information on configuring and synchronizing Visual Voicemail, see the Voice-Mail Profile Configuration chapter of the *Cisco Unified Communications Manager Administration Guide*. For information on setting up a voicemail account, see the *Cisco Cius User Guide*.

Configuring Visual Voicemail for a Specific User or User Group

Use the following procedure to configure Visual Voicemail for a specific user or group of users:

Procedure

Step 1 In Cisco Unified Communications Manager Administration choose **Device** > **Device Phone**.

Step 2 Select the device associated to the user you are searching for.

Step 3 In the **Product Specific Configuration Layout** window, enter the following information in the **Voicemail Server (Primary)** field:

- If configuring for Cisco Unity Connection standalone configuration, enter the fully qualified domain name of the Cisco Unity Connection system.
- If configuring for Cisco Unity Connection failover configuration, enter the DNS alias of the Cisco Unity Connection system.

  Note Only Cisco Unity Connection is supported. Cisco Cius Visual Voicemail is not supported with Cisco Unity.

Step 4 Save changes and click **Apply Config**.

Step 5 Select **Reset** and **Restart** to deliver the new settings to the device.

Step 6 To allow secure messages on Cisco Cius, from Cisco Unity Connection Administration, choose **System Settings** > **Advanced API Configuration** and enable both **Allow Access to Secure Message Recordings through CUMI** and **Allow Message Attachments through CUMI**.

Note To configure Cisco Unified Communications Manager so that directory photos are configured in Cisco Cius Visual Voice Mail, choose **Device** > **Device Settings** > **Common Phone Profile**, select a Common Phone Profile, and enter the url for your organization's photo directory in the **Company Photo Directory Field**.

For more information on configuring and synchronizing Visual Voicemail, see the Voice-Mail Profile Configuration chapter of the *Cisco Unified Communications Manager Administration Guide*. For information on setting up a voicemail account, see the *Cisco Cius User Guide*.

Configuring Web Proxy

This feature allows the user to enable and configure Web Proxy. Web Proxy can be enabled or disabled on Cisco Cius and configured either manually or by specifying proxy auto-configuration (PAC) files. Using existing wired (Ethernet) and wireless (Wi-Fi) interfaces, you can add new proxy configuration and view, modify, or delete existing proxy configurations.

Use this procedure to add Web Proxy on Cisco Cius.

Procedure

Step 1 From the home screen choose **Settings** > **Wireless & network settings** > **Proxy settings**.

Step 2 Tap **Add Proxy**.

Step 3 Enter Type of proxy from drop-down menu - Direct, Manual, or Auto.

- For Direct proxy, choose **Wireless** from Network type and tap **Save**.
- For Manual proxy without authentication, choose Manual from Network type and enter Host name and Port. (Do not tap **Authentication**.) Tap **Save**.
- For Manual proxy with authentication, choose Manual from Network type and enter Host name and Port. Tap **Authentication** and then enter **User name and Password**. Tap **Save**.

  Note For details on supported authentication methods, see Authentication Methods

  To enable an existing proxy, choose **Settings** > **Wireless & network settings** > **Proxy settings** and tap **Proxy**.

  Note If VPN is enabled, no proxy will be configured or used for VPN.

Configuring Screen Lock and Display Idle Time Out

The Screen Lock Timeout value controls the normal Android idle timeout when the screen turns off and the screen lock is activated. The variable is configurable within a range of 1 to 60 minutes.

The Display Idle Time Out value controls how long the display will stay on before dimming or going off while the device is docked. If Cisco Cius is in the Always On Mode, the device will dim. If Cisco Cius is in

the Nightlight Mode, it will turn off completely. The Display Idle Time Out value is configurable up to a maximum value of 24 hours.

When Cisco Cius is docked, the Screen Lock Timeout and Display Idle Time Out timers operate in parallel. Cisco Cius will not dim or turn off until the Display Idle Time Out value is reached. The following table shows the relationship of the Screen Lock Timeout value and Display Idle Time Out value.

Table 6: Screen Lock and Display Idle Time Out Value Relationship

Condition	Outcome
Screen Lock Timeout value less than Display Idle Time Out value	When the Screen Lock Timeout value is reached, screen stays at full brightness; locked screen displays.
Display Idle Time Out value less than Screen Lock Timeout value	When the Display Idle Time Out value is reached, two outcomes are possible: • If Cisco Cius is in Always On mode, the device will dim when the Display Idle Time Out value is reached. When the Screen Lock Timeout value is reached, the device will lock and remain dimmed. • If Cisco Cius is in Nightlight mode, the device will lock and turn off when the Display Idle Time Out value is reached. When the Screen Lock Timeout value is reached, no additional changes occur.
Screen Lock Timeout value the same as the Display Idle Time Out value	When the value is reached, screen stays at full brightness; locked screen displays.

Configuring Screen Unlock/Password Reset

This feature allows the user to reset the PIN/password that is used for unlocking the screen. The user can reset the PIN/password by using Cisco Unified Communications Manager, Cisco AppHQ, or configured Google Account credentials. Use the following procedure to reset the PIN/password using Cisco Unified Communications Manager.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **User Management** > **End User**.

Step 2 Click **Add New**.

Step 3 Enter required User Information.

Step 4 In the **Device Information** window, select the device that you want to associate the user with.

Step 5 Click **Save**.

Step 6 In the **Permissions Information** window, assign the user Cisco Unified Communications Manager Administration permissions.

Step 7 In the **Permissions Information** window, select **Standard CCM End Users**.

Step 8 Click **Save** and **Apply Config**. After the device re-registers, the user is configured to the device. For information on resetting the PIN/password on Cisco Cius, see the following:

- Screen Lock and Unlock PIN and Password Reset
- *Cisco Cius User Guide*

Virtual Desktop Infrastructure

Virtual Desktop Infrastructure (VDI) allows users to access applications/software in hosted virtual desktop. Cisco Cius supports third-party virtual desktop clients from leading third party vendors - Citrix Receiver, Wyse PocketCloud Pro, and Vmware View Client.

Citrix Receiver uses XenServer with Independent Computing Architecture (ICA) protocol. The following table indicates the ports used by the application.

Table 7: Ports Used by Citrix Receiver

Condition	Port used
Basic ICA connection	1494
Session reliability	2598
SSL	443

Wyse PocketCloud uses VMWare View desktop virtualization and management with Remote Desktop Protocol (RDP). The following table indicates the ports used by the application.

Table 8: Ports Used by Wyse PocketCloud

Condition	Port used
RDP	3389

Condition	Port used
VNC	5900

Note For additional information on Citrix Receiver, Wyse PocketCloud Pro, and VMware View Client, see the product description for each application in AppHQ.

For additional information on ports used by Cisco Cius, see the Ports Used By Cisco Cius.

Provisioning Applications

Cisco Cius users can download applications to customize and extend the capabilities of the device. Applications are available from the Cisco AppHQ and the Android marketplace. Cisco Unified Communications Manager Administration provides access to applications through configuration of the following parameters (in the Product Specific Configuration window):

- Allow Applications from Unknown Sources - Controls the ability of user to install applications from sources other than AppHQ or Android marketplace.
- Allow Applications from Android Market - Controls the ability of user to install applications from Android marketplace.
- Allow Applications from Cisco AppHQ - Controls the ability of Admin to push applications from AppHQ.
- Enable Cisco Unified CM Application Client - Controls the ability of Admin to push applications from Cisco Unified Communications Manager.

For best performance and deployment of applications provisioned through Cisco Unified Communications Manager, Cisco recommends specifying the versionCode when creating service. If versionCode is not specified, the device will search for an updated Android Package (APK) file on site each time. Blank versionCode is useful during development of application. The versionCode is an integer and is different than the versionName that users can view from the Settings application. If users are obtaining applications through AppHQ, no versionCode information is required to be set by administrators.

Note For upgrading system applications, including those bundled with the firmware, the versionCode of the Cisco Unified Communications Manager Administration-provisioned application must be greater than the versionCode of the system application.

Note The desktop virtualization applications in AppHQ have been optimized to run on Cisco Cius. Do not download generic versions from other application repositories.

Modifying Phone Button Templates

Phone button templates let you assign speed-dial and call-handling features to programmable buttons. Call-handling features that can be assigned to buttons include **All Calls**, **Do Not Disturb**, **Privacy**, **Speed Dial**, and **Mobility**.

Ideally, you modify templates before registering Cisco Cius devices on the network. In this way, you can access customized phone button template options from Cisco Unified Communications Manager during registration.

To modify a phone button template, choose **Device** > **Device Settings** > **Phone Button Template** in Cisco Unified Communications Manager Administration. To assign a phone button template to a Cisco Cius, use the **Phone Button Template** field in the **Cisco Unified Communications Manager Administration Phone Configuration** window. See the *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide* for more information.

Configuring Feature Control Policies

You can limit the appearance of some telephony features on Cisco Cius by enabling or disabling these features in the feature control policy configuration. If you disable a feature in the feature control policy configuration for Cisco Cius, you restrict user access to the feature.

Use the following steps to create a Feature Control Policy.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Feature Control Policy**.
The **Find and List Feature Control Policy** window appears.

Step 2 Click **Add New** to define a set of policies.

Step 3 Enter the following settings:

- Name - Enter a name for a new Feature Control Policy.
- Description - Enter a description.
- Feature Control Section - Check the check box for the features for which you want to change the default setting. The table in Feature Control Policy Default Values, on page 29 shows the list of features that can be configured and the default value.

Step 4 Click **Save**.

Step 5 Apply the policy to Cisco Cius by including it in the following settings:

- Enterprise Parameters Configuration - Applies to all Cisco Cius devices in the system
- Common Phone Profile Configuration - Applies to all Cisco Cius devices in a group
- Phone Configuration - Applies to an individual Cisco Cius device

Feature Control Policy Default Values

The following table shows the list of features that can be configured and the default value.

Table 9: Feature Control Policy Default Values

Feature	Default values
Barge	Enabled
Call Back	Enabled
Conference List	Enabled
Divert (Alerting)	Disabled
Divert (Connected)	Disabled
Forward All	Enabled
Mobility	Disabled
Park	Disabled
Redial	Enabled
Report Caller	Disabled
Report Quality	Disabled
Speed Dial	Enabled

For more information, see the Feature Control Policy Configuration chapter in the *Cisco Unified Communications Manager Administration Guide*.

Configuring Reset Options/Load Upgrades

Cisco Cius receives configuration changes and load upgrades from Cisco Unified Communications Manager. Cisco Cius handles request changes by the following:

- Reset will wait for active call to end.
- If the device screen is on, user receives a popup dialog notifying the user about the changes and the need for restart. The dialog provides the following options:
  - Restart - Dismisses the popup and restarts the device (default action).
  - Snooze - Dismisses the popup for an hour. User can snooze for a maximum of 24 hours, after which is the device will restart.

Note The popup has a countdown timer of 60 seconds. The default action will begin if the user does not act.

Once snoozed, the user has the option to manually reset the device at any time from the notifications list.

◦ If the device screen is off, active audio or music keeps the request waiting.

Adding Users to Cisco Unified Communications Manager

Adding users to Cisco Unified Communications Manager allows you to display and maintain information about users and allows each user to perform these tasks:

- Set up speed-dial and call-forwarding numbers
- Subscribe to services that are accessible from Cisco Cius

You can add users to Cisco Unified Communications Manager individually or in batches. To add users individually, follow these steps:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **User Management** > **End User**.

Step 2 Click **Add New**.

Step 3 In the **User Information** window, enter required information.

Step 4 In the **Device Information** window, select the device that you want to associate the user with.

Step 5 Assign the user Cisco Unified Communications Manager Administration End User Permissions.

Step 6 Click Save and **Apply Config**.
For more information, go to the End User Configuration chapter in the *Cisco Unified Communications Manager Administration Guide*.

To add users in batches, use the Bulk Administration Tool. This method also allows you to set an identical default password for all users.

For more information, go to the Bulk Administration chapter in the*Cisco Unified Communications Manager Administration Guide*.

Managing the User Options Web Pages

From the **User Options** web page, users can customize and control several Cisco Cius features and settings. For detailed information about the **User Options** web pages, see the User Group Configuration chapter of the *Cisco Unified Communications Manager Administration Guide.*

Add User to Cisco Unified Communications Manager user group

Before a user can access the **User Options** web pages, you must add the user to the standard Cisco Unified Communications Manager end user group and associate the appropriate Cisco Cius with the user.

To add the user to the standard Cisco Unified Communications Manager user group, follow these steps:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **User Management** > **User Group**.
The **Find and List Users** window appears.

Step 2 Enter the appropriate search criteria and click **Find**.

Step 3 Click on the **Standard CCM End Users** link.
The **User Group Configuration** window for the Standard CCM End Users appears.

Step 4 Click **Add End Users to Group**.
The **Find and List Users** window appears.

Step 5 Use the **Find User** drop-down list boxes to find the users that you want to add, and click **Find**.

Step 6 A list of users that match your search criteria appears.

Step 7 In the list of records that is displayed, click the check box next to the users that you want to add to this user group. If the list comprises multiple pages, use the links at the bottom to see more results.
Note The list of search results does not display users that already belong to the user group.

Step 8 Click **Add Selected**.

Associate Cisco Cius with user

To associate Cisco Cius with a user, follow these steps:

Procedure

Step 1 **End User** From Cisco Unified Communications Manager Administration, choose **User Management** > **End User**.
The **Find and List Users** window appears.

Step 2 Enter the appropriate search criteria and click **Find**.

Step 3 In the list of records that is displayed, click the link for the user.

Step 4 Click **Device Association**.
The **User Device Association** window appears.

Step 5 Enter the appropriate search criteria and click **Find**.

Step 6 Choose the device that you want to associate with the user by checking the check box to the left of the device.

Step 7 Click **Save Selected/Changes** to associate the device with the user.
Make sure to provide users with the following information about the **User Options** web pages:

- The URL required to access the application. This URL is: `http://<server_name:portnumber>/ccmuser/`, where `server_name` is the host on which the web server is installed.
- A user ID and default password are needed to access the application.
  These settings correspond to the values you entered after you added the user to Cisco Unified Communications Manager (see the Configuring Reset Options/Load Upgrades, on page 29).

For additional information, see:

- User Group Configuration, *Cisco Unified Communications Manager Administration Guide*
- End User Configuration, *Cisco Unified Communications Manager Administration Guide*
- Role Configuration, *Cisco Unified Communications Manager Administration Guide*