Features and Services

Available Telephony Features

Cisco DX Series devices provide an integrated suite of collaborative applications, including Cisco WebEx, Cisco Unified Presence, instant messaging, email, visual voicemail, and Cisco Unified Communications Manager voice and video telephony features. These devices also support applications from Google Play.

After you install Cisco DX Series 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 and set up services.

Note Cisco Unified Communications Manager 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.

Agent Greeting

Allows an agent to create and update a prerecorded greeting that plays at the beginning of a customer call, before the agent begins the conversation with the caller. The agent can prerecord a single greeting or multiple ones as needed.

For more information, see:

- *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter
- *Features and Services Guide for Cisco Unified Communications Manager*, "Barge and Privacy" chapter

Enable Agent Greeting

Procedure

Step 1 Select **Device** > **Phone**.

Step 2 Locate the device that you want to configure.

Step 3 Scroll to the Device Information Layout pane and set **Built In Bridge** to On or Default.

Step 4 Choose **Save**.

Step 5 Check the setting of the bridge:

a) Choose **System** > **Service Parameters**.
b) Select the appropriate Server and Service.
c) Scroll to the Clusterwide Parameters (Device - Phone) pane and set **Builtin Bridge Enable** to On.
d) Choose **Save**.

All Calls

Allows a user to view a list of active and held calls; this list is sorted in chronological order (oldest first). The user can also view a list of incoming and completed calls; this list is sorted newest to oldest.

All Calls on Primary Line

Allows the primary line to assume the All Calls functionality. All incoming calls display in the primary line call list and can be answered on the primary line.

AutoAnswer

Connects incoming calls automatically after a ring or two. AutoAnswer works with either the speakerphone or the headset. If AutoAnswer for headset is enabled for a device, but no headset is connected to the device, the device will not automatically answer any calls.

For more information, see *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter.

Auto Dial

Allows the 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.

Barge

Allows a user to join a nonprivate call on a shared phone line. Barge adds a user to a call and converts the call into a conference. The user and other parties can then access conference features.

Note Users can still use Barge if the Built In Bridge Enable service parameter is set to Off. To prevent a user from using the Barge feature on a device, you must disable Barge in the Feature Control Policy for the device.

For more information, see:

- *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Setup" chapter
- *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter
- *Features and Services Guide for Cisco Unified Communications Manager*, "Barge and Privacy" chapter
- *Cisco Unified Communications Manager Administration Guide*, "Feature Control Policy Setup" chapter

Busy Lamp Field

Allows a user to monitor the call state of a directory number that is associated with a speed-dial button, call log, or directory listing on the device.

For more information, go to the "IM and Presence Service" chapter in the *Features and Services Guide for Cisco Unified Communications Manager*.

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:

- Allow calls that are placed from the target number to ring through rather than be forwarded.
- Prevent 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 Setup" chapter.
- *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter.

Calling Line Identification

Allows a user to enable the full, external number to be used for calling line identification.

For more information, see the "Cisco Unified IP Phones" chapter in the *Cisco Unified Communications Manager System Guide*.

Calling Line Identification Presentation

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 Phones" chapter in the *Cisco Unified Communications Manager System Guide*.

Cisco Extension Mobility

Allows users to temporarily access their device configuration, such as line appearances, services, and speed dials, from a shared device through login to the Cisco Extension Mobility service on that device.

Cisco Extension Mobility can be useful if users work from a variety of locations within your company or if they share a workspace with coworkers.

Note This feature is not supported for DX Series devices that are deployed with Mobile and Remote Access through Expressway.

To log in to a device, the user enters extension mobility credentials that the administrator supplies. These credentials differ from the user Screen Lock PIN.

For more information, see the "Extension Mobility" chapter in the *Features and Services Guide for Cisco Unified Communications Manager*.

Extension Mobility Multi-User

The extension mobility multi-user feature uses the extension mobility login/logout process. When the user logs in, the Cisco Unified Communications Manager server authenticates the user credentials; the server uses the same messaging scheme as the extension mobility feature.

When user A logs in to a device for the first time, the device goes through a reboot cycle and creates a user partition for user A on the device. The device presents user A with the Setup Wizard. User A gets dedicated space for personal apps and data, and the Call application works as it does on any Cisco DX Series device. After initial login, user A configures any app-related settings. When user A logs out from this device, the user settings are saved for the next time that user A logs in to the device.

When user A logs out from the device, user B can log in to the device with user B credentials. User B has the same experience upon obtaining the user B partition: for the first login, the Setup Wizard prompts user B to set up personal apps and data, and user B also has a Call application that works as usual on a Cisco DX Series device.

Partitions are completely separate, so that any user can never see the data of any other user.

Extension mobility multi-user offers an enterprise multi-user approach: the system administrator decides which devices are configured for extension mobility multi-user, and provides credentials for those users that can log in to a particular device. With proper credentials, users can log in only to a particular device and configure their own accounts, which includes removal of their own accounts. Users cannot modify the accounts of other users on the same device.

An algorithm limits the number of users that can log in to a particular device. The maximum number of users on a device depends on the usage of each user. When the flash memory on the device drops below a certain quotient, the account of the least recently logged in user is deleted to create space for a new user to log in. Thus, a new user never fails to log in due to lack of space on the device.

Set Up Cisco Extension Mobility

Perform the procedures in the order shown in the following steps to configure Cisco Extension Mobility for DX Series devices.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Device Profile** and click **Add New**.

a) Enter the Device Type.
b) Enter the Device Profile Name, and click **Save**.
c) Enter the directory numbers and required information and click **Save**.

Step 2 Choose **User Management** > **End User** and select or create a user.

a) In Extension Mobility Available Profiles, choose the user device profile and click the down arrow; this places the service that you chose in the Controlled Profiles box.
b) Click **Save**.

Step 3 Choose **Device** > **Phone**.

a) Choose your device type.
b) Select a user ID.
c) In the Product Specific Configuration Layout area of the **Phone Configuration** window, in Extension Information, check **Enable Extension Mobility**.
d) In the Product Specific Configuration Layout area of the **Phone Configuration** window, choose the **Enabled** value for the Multi-User drop-down list box.

Cisco Mobility

Enables users to manage business calls by using a single phone number and pick up in-progress calls on the desktop phone and a remote device, such as on a mobile phone. Users can restrict the group of callers according to phone number and time of day.

Cisco Mobility for Cisco DX Series devices requires Cisco Unified Communications Manager Release 9.0(1) or later.

For more information, see the "Cisco Mobility" chapter in the *Features and Services Guide for Cisco Unified Communications Manager*

Conference

- Allows a user to talk simultaneously with multiple parties; to do so, the feature calls 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 Advanced Adhoc Conference (disabled by default in Cisco Unified Communications Manager) allows you to enable these features.

For information about conferences, go to the "Conference Bridges" chapter in the *Cisco Unified Communications Manager System Guide*.

Secure Conference

Secure Conference allows secure devices to place conference calls through use of a secure conference bridge. As new participants are added, the Secure Call icon is displayed as long as all participants use secure devices.

For additional information, see:

- *Cisco Unified Communications Manager System Guide*, "Conference Bridges" chapter
- *Cisco Unified Communications Manager Administration Guide*, "Conference Bridge Setup" chapter
- *Cisco Unified Communications Manager Security Guide*

Divert

After Enhanced Immediate Divert is enabled, the feature allows users to divert incoming calls directly to their voice messaging system.

For more information about diverting calls to voicemail, see the "Immediate Divert" chapter in the *Features and Services Guide for Cisco Unified Communications Manager*.

For more information about Enhanced Immediate Divert, see the "Cisco Unified IP Phones" chapter in the *Cisco Unified Communications Manager System Guide*.

Do Not Disturb

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.

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. In Cisco Unified Communications Manager Administration, choose **Device** > **Phone** > **Phone Configuration**.
- DND Incoming Call Alert - Choose the type of alert to play, if any, on a device for incoming calls when DND is active. This parameter is located in both the **Common Phone Profile** window and the **Phone Configuration** window. (The **Phone Configuration** window value takes precedence.)

For more information, see the "Do Not Disturb" chapter in the *Features and Services Guide for Cisco Unified Communications Manager*.

Gateway Recording

This feature directs the Media Gateway to send the call to the recording server and thus improve call monitoring.

For more information, see the "Monitoring and Recording" chapter in the *Features and Services Guide for Cisco Unified Communications Manager*.

Hold Status

Enables devices with a shared line to distinguish between the local and remote lines that placed a call on hold.

Hold and Resume

Allows the user to move a connected call from an active state to a held state.

Music on Hold

Plays music while callers are on hold.

For more information, see the "Music On Hold" chapter in the *Features and Services Guide for Cisco Unified Communications Manager*.

Ignore

Allows a user to ignore an incoming call from the notification window.

Message Waiting Indicator

A light on the handset indicates that a user has one or more new voice messages.

For more information, see:

- *Cisco Unified Communications Manager Administration Guide*, "Message Waiting Setup" chapter
- *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager" chapter

Mute

Mutes the audio input for all input devices, including device speakers, handset, and headsets.

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 only to dialing the first digit for an on-hook or off-hook call.

Protected Calling

Provides a secure (encrypted) connection between two devices. 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 additional information, see the *Cisco Unified Communications Manager Security Guide*.

Ringtone Setting

Identifies ring type used for a line when the device has another active call.

For more information, see the "Directory Number Setup" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Ringtone

Users can customize how their device indicates an incoming call and a new voice message.

Secure and Nonsecure Indication Tone

After a device 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 device to protected in Cisco Unified Communications Manager Administration, check **Protected Device** in **Device** > **Phone** > **Phone Configuration**.
- Play Secure Indication Tone - To enable the protected device 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 at **System** > **Service Parameters**. Choose the server and then the Cisco CallManager service. In the **Service Parameter Configuration** window, choose the option in the Feature - Secure Tone area. (The default is False.)

Only protected 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, the device plays the secure indication tone (three long beeps with pauses).
  - After end-to-end nonsecure media is established and the call status is nonsecure, the device plays the nonsecure indication tone (six short beeps with brief pauses).
- If the Play Secure Indication Tone option is disabled, no tone plays.

Serviceability

Allows administrators to gather debug information quickly and easily from devices.

This feature uses SSH to access each phone remotely. SSH must be enabled on each phone for this feature to function.

Shared Line

Allows a user to have multiple devices that share the same directory number or allows a user to share a directory number with a coworker.

For more information, see the “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 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.

Uniform Resource Identifier Dialing

The Uniform Resource Identifier (URI) Dialing feature allows the user to place calls by using an alphanumeric URI address as a directory number, for example, bob@cisco.com. The user must enter the URI address to select the contact.

The screen displays the call information for the URI call. The call logs record the URI call information in the Call History and the Details page.

For more information, see *Features and Services Guide for Cisco Unified Communications Manager*.

Video Toggle

Users can toggle video off or on during video calls.

Voice Messaging System

Enables callers to leave messages if calls are unanswered.

For more information, see:

- *Features and Services Guide for Cisco Unified Communications Manager*
- *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager" chapter

Set Up Visual Voicemail

Visual Voicemail is configured for all 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 devices.

Procedure

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

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

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

- If you are configuring for Cisco Unified IP Phone standalone configuration, enter the fully qualified domain name of the Cisco Unified IP Phone system.
- If you are configuring for Cisco Unified IP Phone failover configuration, enter the DNS alias of the Cisco Unified IP Phone system.

Step 4 Save changes and click **Apply Config**.
For more information about configuration and synchronization of Visual Voicemail, see the "Voice-Mail Profile Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide*.

Set Up Visual Voicemail for Specific User or 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 Choose the device that associates with 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 you are configuring for Cisco Unified IP Phone standalone configuration, enter the fully qualified domain name of the Cisco Unified IP Phone system.
- If you are configuring for Cisco Unified IP Phone failover configuration, enter the DNS alias of the Cisco Unified IP Phone system.

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

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

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

Step 7 To configure Cisco Unified Communications Manager so that directory photos are configured in Visual Voice Mail, choose **Device** > **Device Settings** > **Common Phone Profile**, choose a Common Phone Profile, and enter the URL for your organization's photo directory in the **Company Photo Directory** field.
For more information about configuration and synchronization of Visual Voicemail, see the "Voice-Mail Profile Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide*.

Feature Buttons

The following table provides information about features that are available on the call control bar, and features that you need to configure as programmable feature buttons. An "X" in the table indicates that the feature is

supported for the corresponding button type. Of the two button types, only programmable feature buttons require configuration in Cisco Unified Communications Manager administration.

Table 1: Features and Corresponding Buttons

Feature Name	Call Control Bar Button	Programmable Feature Button
Call Back		X
Call Forward	X	
Call Forward All		X
Call Park	X	
Call Pickup		X
Cisco Mobility		X
Conference (Add)	X	
Divert		X
Do Not Disturb		X
End Call	X	
Group Pickup		X
Hold	X	
Hunt Group		X
Intercom		X
Malicious Call Identification (MCID)		X
Meet Me		X
Privacy		X
Redial		X
Share (DX70 & DX80 only)	X	
Speed Dial		X
Stop Video		X
Transfer	X	

Set Up Feature Control Policies

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

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.

Step 4 Click **Save**.

Step 5 Apply the policy to Cisco DX Series devices by including it in the following settings:

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

Feature Control Policy Default Values

The following table shows the list of features that you can configure, and the default value.

Table 2: Feature Control Policy Default Values

Feature	Default value
Barge	Enabled
Call Back	Enabled
Call PickUp	Disabled
Conference List	Enabled

Feature	Default value
Divert (Alerting)	Disabled
Divert (Connected)	Disabled
Forward All	Enabled
Group Call PickUp	Disabled
Meet Me	Disabled
Mobility	Disabled
Other Call PickUp	Disabled
Park	Disabled
Redial	Enabled
Report Caller	Disabled
Report Quality	Disabled
Speed Dial	Enabled

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

Phone Button Templates

Phone button templates let you assign speed dials and call-handling features to programmable buttons.

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

Modify Phone Button Templates

For more information about Phone services, see "IP Phone Services Setup" chapter in the *Cisco Unified Communications Manager Administration Guide*. For more information about configuring line buttons, see "Cisco Unified IP Phone Setup" chapter and "Configuring Speed-Dial Buttons" section in the *Cisco Unified Communications Manager Administration Guide*.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Phone Button Template**.

Step 2 Click **Find**.

Step 3 Choose the device model.

Step 4 Choose **Copy**, enter a name for the new template, and choose **Save**.

The **Phone Button Template Configuration** window opens.

Step 5 Identify the button that you would like to assign, and select **Service URL** from the Features drop-down list that associates with the line.

Step 6 Click **Save** to create a new phone button template that uses the service URL.

Step 7 Choose **Device** > **Phone** and open the **Phone Configuration** window for the device.

Step 8 Choose the new phone button template from the **Phone Button Template** drop-down list.

Step 9 Click **Save** to store the change and then click **Reset** to implement the change.
The user can now access the Self Care Portal and associate the service with a button on the device.

Configure Product-Specific Options

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

- **Enterprise Phone Configuration** window (**System** > **Enterprise Phone Configuration**)
- **Common Phone Profile window** (**Device** > **Device Settings** > **Common Phone Profile**), in the Product Specific Configuration Layout portion of window
- **Device Phone Configuration** window (**Device** > **Phone** > **Add New** > **Cisco DX650, Cisco DX70, or Cisco DX80**), in the Product Specific Configuration Layout area of window

The following table shows the product-specific configuration options.

Table 3: Cisco DX Series Product-Specific Configuration Options

Feature	Description
Disable Speakerphone	Disables only the speakerphone functionality. Disabling speakerphone functionality does not affect the headset. You can use lines and speed dials with headset/handset. Default: False
Disable Speakerphone and Headset	Disables all speakerphone functions and the headset microphone. Default: False
Disable USB	Disables the USB ports on the device. Default: False
SDIO	Indicates whether the SDIO device on the device is enabled or disabled. Default: Disabled
Bluetooth	Indicates whether the Bluetooth service on the device is enabled or disabled. Default: Enabled

Feature	Description
Allow Bluetooth Contacts Import	Allows the user to import and sync contacts and call history from their Bluetooth device. Default: Enabled
Allow Bluetooth Mobile Handsfree Mode	Allows the user to use their mobile phone line on the desk phone. Default: Enabled
Days Display Not Active	Allows the user to specify the days that the backlight is to remain off by default. Default: Typically 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 choose Saturday and Sunday.
Display On Time	Indicates the time of day the display is to automatically turn itself on for days that are listed in the off schedule. Default: 07:30 Maximum length: 5 **Note** Enter value in a 24-hour format, where 00:00 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. Default: 10:30 Maximum length: 5 **Note** Maximum value is 24 hours. This value is in hours and minutes format. For example, “01:30” activates the display for 1 hour and 30 minutes.
Display On When Incoming Call	When the device is in screen saver mode, this setting turns the display on when a call is ringing. Default: Enabled

Feature	Description
Enable Power Save Plus	To enable the Power Save Plus feature, select the day(s) that you want the device to power off on schedule. You can select multiple days by pressing and holding the Control key while clicking on the days that you want Power Save Plus to operate. In Power Save Plus mode, enough power is maintained to illuminate one key. All other functions of the device are turned off. Power Save Plus mode turns off the device for the time period specified in the Phone On Time and Phone Off Time fields. This time period is usually outside of your organization's regular operating hours. The illuminated key allows a user to press it to restore full power to the device. After pressing the illuminated key, the phone power-cycles and reregisters with Unified CM before it becomes fully operational. When you select day(s) in this field, the following notice displays to indicate e911 concerns. By enabling Power Save Plus, you are agreeing to the terms specified in this Notice. While Power Save Plus Mode is in effect, endpoints configured for the mode are disabled for emergency calling and from receiving inbound calls. By selecting this mode, you agree to the following: **1** You are taking full responsibility for providing alternate methods for emergency calling and receiving calls while the mode is in effect. **2** Cisco has no liability in connection with your selection of the mode and all liability in connection with enabling the mode is your responsibility. **3** You will fully inform users of the effects of the mode on calls, calling and otherwise. Default: No days selected
Phone On Time	This field determines the time that the device turns on automatically on the days that are selected in the Enable Power Save Plus list box. Enter the time in 24 hour format, where 00:00 represents midnight. For example, to automatically turn the phone on at 7:00 a.m., (0700), enter 07:00. To turn the phone on at 2:00 p.m. (1400), enter 14:00.If this field is blank, the device automatically turns on at 00:00. Default: 0:00 Maximum length: 5
Phone Off Time	This field determines the time of day that the device will turn itself off on the days that are selected in the Enable Power Save Plus list box. Enter the time in the following format hours:minutes. If this field is blank, the device automatically turns off at midnight (00:00). **Note** If Phone On Time is blank (or 00:00) and Phone Off Time is blank (or 24:00), the device will remain on continuously, effectively disabling the Power Save Plus feature unless you allow EnergyWise to send overrides. Default: 24:00 Maximum length: 5

Feature	Description
Phone Off Idle Timeout	This field represents the number of minutes that the device must be idle before the device will request the power sourcing equipment (PSE) to power down the device. The value in this field takes effect: • When the device was in Power Save Plus mode as scheduled and was taken out of Power Save Plus mode because the user pressed a key • When the device is repowered by the attached switch • When the Phone Off Time is met but the device is in use. The unit is minutes. The default is 60. The range is 20 to 1440.
Enable Audible Alert	This checkbox, when enabled, instructs the device to play an audible alert ten minutes prior to the time specified in the field, Phone Off Time. The default is disabled. This checkbox only applies if the Enable Power Save Plus list box has one or more days selected.
EnergyWise Domain	This field defines the EnergyWise domain in which the phondevice is participating. An EnergyWise domain is required by the Power Save Plus feature. If you have chosen days in the Enable Power Save Plus list box, you must also provide an EnergyWise domain. The default is blank. Maximum length: 127
EnergyWise Endpoint Security Secret	This field defines the password (shared secret) used to communicate within the EnergyWise domain. An EnergyWise domain and secret is required by the Power Save Plus feature. If you have chosen days in the Enable Power Save Plus list box, you must also provide an EnergyWise domain and secret. The default is blank. Maximum length: 127
Allow EnergyWise Overrides	This checkbox determines whether you will allow the EnergyWise domain controller policy to send power level updates to the phones. A few conditions apply; first, one or more days must be selected in the Enable Power Save Plus field. If the Enable Power Save Plus list box does not have any days selected, the device will ignore the EnergyWise directive to turn off the device. Second, the settings in Unified CM Administration will take effect on schedule even if EnergyWise sends an override. For example, assume the Display Off Time is set to 22:00 (10 p.m.), the value in the Display On Time field is 06:00 (6 a.m.), and the Enable Power Save Plus has one or more days selected. If EnergyWise directs the device to turn off at 20:00 (8 p.m.), that directive will remain in effect (assuming no user intervention occurs) until the configured Phone On Time at 6 a.m. At 6 a.m., the device will turn on and resume receiving its power level changes from the settings in Unified CM Administration. To change the power level on the device again, EnergyWise must reissue a new power level change command. Also, any user interaction will take effect so if a user presses a key after EnergyWise has directed the device to power off, the device will power on as a result of the user action. The default is unchecked.

Feature	Description
Recording Tone	This can be used to configure whether the recording tone is enabled or disabled on the device. Default: Disabled
Recording Tone Local Volume	This can be used to configure the loudness setting of the recording tone that the local party hears. This loudness setting applies regardless of the actual device used for hearing (handset, speakerphone, headset). The loudness setting should be in the range of 0% to 100%, with 0% being no tone and 100% being at the same level as the current volume setting. The default value is 100%.
Recording Tone Remote Volume	This can be used to configure the loudness setting of the recording tone that the remote party hears. The loudness setting should be in the range of 0% to 100%, with 0% being less than -66dBM and 100% being -4dBM. The default value is -10dBM or 50%.
Recording Tone Duration	Indicates the length of time in milliseconds for which the recording tone is inserted in the audio stream. The default for this parameter is set to the value in the Network locale file for this field. The valid range for this parameter is a value between 1 and 3000 milliseconds.
Advertise G.722 and iSAC Codecs	Indicates whether the Call application advertises the wideband codecs to the Cisco Unified Communications Manager. Codec negotiation involves two steps: 1 The Call application must advertise the supported codecs to Cisco Unified Communications Manager. 2 When Cisco Unified Communications Manager gets the list of supported codecs from all devices that are 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 - Call application defers to the setting that is specified in the enterprise parameter, Advertise G.722 and iSAC Codecs. • Disabled - Call application does not advertise the wideband codecs to Cisco Unified Communications Manager. • Enabled - Call application advertises the wideband codecs to Cisco Unified Communications Manager.
Video Calling	When enabled, indicates that the device will participate in video calls. Default: Enabled

Feature	Description
Device UI Profile	Changes the device user interface characteristics to optimize for specific user personas such as basic video callers (Simple mode) or general collaboration users (Enhanced). Default: Simple
Wifi	Indicates whether the Wi-Fi on the device is enabled or disabled. **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 you create a new common phone profile for devices with Wifi parameter set to Enabled if the deployment environment default setting at the enterprise and common level is Disabled, unless it is company policy to set the Wifi default to Disabled for all devices. Default: Enabled
PC Port	Indicates whether the PC port is enabled or disabled. Default: Enabled
Span to PC Port	Indicates whether the device will forward packets that are transmitted and received on the PC port. **Note** Choose **Enabled** if an application is running on the PC port that requires monitoring of the device traffic, such as monitoring and recording applications or network packet-capture tools that are used for diagnostic purposes. To use this feature, PC Voice VLAN access must be enabled. Default: Disabled
PC Voice VLAN Access	Indicates whether a device that is attached to the PC port is allowed access to the Voice VLAN. **Note** Disabling Voice VLAN Access prevents the attached PC from transmission and receipt of data on the Voice VLAN. It also prevents the PC from receiving data sent and received by the device. Default: Enabled
PC Port Remote Configuration	Allows remote configuration of the PC port speed and duplex of the device. Default: Disabled
Switch Port Remote Configuration	Allows remote configuration of the switch port speed and duplex of the device. This overrides any manual configuration on the device. Default: Disabled

Feature	Description
Detect Unified CM Connection Failure	This field determines the sensitivity that the phone has for detecting a connection failure to Cisco Unified Communications Manager (Unified CM), which is the first step before device failover to a backup Unified CM/SRST occurs. Valid values specify Normal (detection of a Unified CM connection failure occurs at the standard system rate) or Delayed (detection of a Unified CM connection failover occurs approximately four times slower than Normal). For faster recognition of a Unified CM connection failure, choose Normal. If you prefer failover to be delayed slightly to give the connection the opportunity to reestablish, choose Delayed. Note that the precise time difference between Normal and Delayed connection failure detection depends on many variables that are constantly changing. This only applies to the wired Ethernet connection. Default: Normal
Gratuitous ARP	Indicates whether the device will learn MAC addresses from Gratuitous ARP responses. **Note** Disabling the device ability to accept Gratuitous ARP prevents applications that use this mechanism for monitoring and recording of voice streams from working. Default: Disabled
Cisco Discovery Protocol (CDP): Switch Port	Allows administrator to enable or disable CDP on the switch port. **Warning** Disable CDP on the network port only if the device connects to a non-Cisco switch. For more details, see the *Cisco Unified Communications Manager Administration Guide*. Default: Enabled
Cisco Discovery Protocol (CDP): PC Port	Indicates whether CDP is supported on the PC port. Default: 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 switch port. Default: Enabled
Link Layer Discovery Protocol (LLDP): PC Port	Allows administrator to enable or disable Link Layer Discovery Protocol (LLDP) on the PC port. Default: 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. Default: Unknown

Feature	Description
Power Negotiation	Allows administrator to enable or disable Power Negotiation. **Note** Enable the Power Negotiation feature when the device 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+. Default: Enabled
Automatic Port Synchronization	Enables the phone to synchronize the PC and SW ports to the same speed and to duplex. Only ports configured for auto negotiate change speeds. Default: Disabled
802.1x Authentication	Specifies the 802.1x Authentication feature status. Options: • Enabled - The device uses 802.1X authentication to request network access. • Disabled - Default setting in which the device uses CDP to acquire VLAN and network access. Default: User controlled
Always On VPN	Indicates whether the device always starts the VPN AnyConnect client and establishes a connection with the configured VPN profile from Cisco Unified Communications Manager. Default: False
Store VPN Password on Device	This parameter controls whether VPN password can be stored on the device. Its value is used only when Password Persistence is set to true. If disabled, the user's VPN password is stored in memory and is automatically re-submitted upon subsequent connects. However, when the device reboots, the user will have to re-enter their VPN password again. If enabled, the user's VPN password is stored on the device and will persist across reboots. Default: False
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. Default: True
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, which consists of at least four alphanumeric characters, one of which must be a non-numeric character, and one must be a capital letter. Default: PIN

Feature	Description
Maximum 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
Enforce Screen Lock During Display-On Time	This parameter provides an unobtrusive lock policy that allows users to work freely with their device throughout the workday, without the device locking after the interval that is set in Cisco Unified Communications Manager. After work, the device locks as defined in the policy, to prevent unauthorized users from accessing it. The device always supports the user-controlled manual lock option (power button), for meetings or lunch breaks. The device remains locked until the user enters the PIN/password on next use. ON - Device locks during the workday or during display-on time (default setting). OFF - Device locks only during display-off time or after work hours, based on day/time settings listed above. Default: True **Note** Disabling this parameter overrides all third-party device administration policies that are installed on the device that relate to lock screen timeout.
Lock Device During Audio Call	When the device is in a charging state and an active voice call is in progress, an administrator can override the screen lock PIN enforcement timer to keep the screen active during an audio call. Screen lock timer takes effect after audio call is completed and timer is exceeded. Default: Disabled
Kerberos Server	Authentication server for web proxy Kerberos. Maximum length: 256
Kerberos Realm	Authentication realm for web proxy Kerberos. Maximum length: 256
Load Server	Indicates that the device will use an alternative server to obtain firmware loads and upgrades, rather than the defined TFTP server. Default: 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. Default: Enabled
Log Server	Specifies an IP address and port of a remote system to which log messages are sent. Default: IP address of remote system Maximum length: 32

Feature	Description
Log Profile	Run the pre-defined debug command remotely. Default: Preset
Web Access	Indicates whether the device accepts connections from a web browser or other HTTP client. Default: Disabled
SSH Access	This parameter indicates whether the device accepts SSH connections. Disabling the SSH server functionality of the device will block access to the device. Default: Disabled
Android Debug Bridge (ADB)	Enables or disables the ADB on the device. Can be set to Enabled, Disabled, or User Controlled. Default: Disabled
Multi-User	Indicates whether multi-user is enabled or disabled on the device. Default: Disabled
Allow Applications from Unknown Sources	Controls whether the user can install Android applications on the device from a URL or from Android application package files (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. Default: Disabled
Allow Applications from Google Play	Controls whether the user can install Android applications from Google Play. **Note** Some applications that are found in Google Play may have hardware requirements that are not available on Cisco DX Series devices, such as GPS or a rear-facing camera. Cisco cannot guarantee that an application that is downloaded from a third-party site will work. Default: False
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 Cisco Unified Communications Manager. Default: False
Background Image	This parameter specifies the default wallpaper file. Only the administrator disables end user access to phone wallpaper list, could this parameter take effect. Maximum length: 64

Feature	Description
Company Photo Directory	Specifies the URL that the device can query for a user and get the image that is associated with that user. Example: http://www.cisco.com/dir/photo/zoom/%%uid%%, where uid is employee user ID. Default: Photo directory URL Maximum length: 256
Voicemail Server (Primary)	Hostname or IP address of the primary visual voicemail server. Default: IP address of primary visual voicemail server Maximum length: 256
Voicemail Server (Backup)	Hostname or IP address of the backup visual voicemail server. Default: IP address of backup visual voicemail server Maximum length: 256
Presence and Chat Server (Primary)	Hostname or IP address of the primary presence server. Default: 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. Default: Cisco WebEx Connect
Presence and Chat Single Sign-On (SSO) Domain	The enterprise domain that Cisco WebEx Connect Cloud uses to perform Single Sign-On (SSO) authentication against an enterprise. Default: Empty field Maximum length: 256
Multi-User URL	This parameter specifies the URL of the extension mobility server. Maximum length: 256
User Credentials Persistent for Expressway Sign In	This parameter controls whether Expressway credentials can be stored on the device. Default: Disabled
Customer support upload URL	This sets a server address to which the user can send problem report files from the 'Problem Reporting Tool' on the endpoint. Maximum length: 256

Note For additional configuration information, see the *Cisco DX Series 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:

1 **Phone Configuration** window

2 **Common Phone Profile** window

3 **Enterprise Phone Configuration** window

Video Transmit Resolution Setup

Cisco DX Series devices support video calling through a high-resolution multitouch color LCD and integrated camera. For the device to send and receive video, the video capability must be enabled in Cisco Unified Communications Manager.

Note When the Video Calls option is set to Off, the Auto Transmit Video setting is dimmed. All video settings under the Call settings menu are dimmed if Video Calling is disabled in the **Product Specific Configuration Layout** window.

Table 4: Video Transmit Resolutions and Capabilities

Video Type	Video Resolution	FPS	Video Bit Range Rate (bandwidth)	DX650 External Camera Support
240p	432 x 240	15	64-149 kbps	Yes, but the Logitech C930e uses a video resolution of 424 x 240.
240p	432 x 240	30	150-299 kbps	Yes, but the Logitech C930e uses a video resolution of 424 x 240.
360p	640 x 360	30	300-599 kbps	Yes

Video Type	Video Resolution	FPS	Video Bit Range Rate (bandwidth)	DX650 External Camera Support
480p	848 x 480	30	600-799 kbps	Yes, but the Logitech C920-C uses a video resolution of 864 x 480.
576p	1024 x 576	30	800-1299 kbps	Yes
600p	1024 x 600	30	800-3000 kbps	No
720p	1280 x 720	30	900-1999 kbps	Yes
1080p	1920 x 1080	30	2000-4000 kbps	Yes
CIF	352 x 288 (4:3)	30	64-299 kbps	Yes
VGA	640 x 480 (4:3)	30	400-1500 kbps	Yes

Note The external camera does not support some of these resolutions, such as 600p, and the minimum bit rate at which the external camera can operate is 64 kbps.

Note When a Cisco DX650 is in a call that is using the Logitech C920-C Webcam, and the remote device only supports Packetization mode 0, the maximum transmit resolution is 640x360. When Packetization mode 1 is used, the maximum transmit resolution is 1920x1080.

Note The optimal resolution over VGA for a Cisco DX Series device is w360p; for bandwidths ranging from 400 kbps to 999 kbps, the device will send w360p.

Instant Messaging and Presence Setup

Instant Messaging and Presence allows users to communicate at any time, any place, and with any device. Cisco DX Series devices support Jabber IM with either Cisco Unified Presence or WebEx back end server. For security reasons, all cloud-based IM and Presence traffic is routed through a proxy.

Instant Messaging and Presence is configured at the device, group, or enterprise levels in the **Product Specific Configuration** window for the device. Enter the hostname or IP address for the Presence and IM Server (Primary) and Presence and IM Server type.

Application Setup

Users can download applications to customize and extend the capabilities of the device. Applications are available from Google Play. Cisco Unified Communications Manager Administration provides access to applications through configuration of the following parameters (in the Product Specific Configuration Layout area of the individual device configuration window or **Common Phone Profile** window):

- Allow Applications from Unknown Sources: Controls the ability of user to install applications from sources other than Google Play.
- Allow Applications from Google Play: Controls the ability of user to install applications from Google Play.
- Enable Cisco UCM App Client: Controls the ability of administrator to push applications from Cisco Unified Communications Manager.

  UCM App is the client on the device that can be used to subscribe or unsubscribe Android applications that are created on Cisco Unified Communications Manager. This client provides the same functionality as subscribing or unsubscribing Android applications from Cisco Unified Communications Manager, but adds the convenience of doing so from the device.

Enable Cisco UCM App Client

Procedure

Step 1 In the Product Specific Configuration Layout portion of the **Device Configuration** window of a device, check the **Enable Cisco UCM App Client** check box.

Step 2 Click **Save.**

Step 3 Click **Apply Config**.
This action installs the UCM App client on the device.

After the UCM App client is installed on the device, the device user can subscribe or unsubscribe to applications that are created in Cisco Unified Communications Manager by logging in to the UCM App client.

Create End User to Log In to UCM App

The administrator must create an end user, associate the end user with the device, and assign the end user as device owner before the end user can log in to the UCM App.

Procedure

Step 1 Create an end user. (In Cisco Unified Communications Manager Administration, choose **User Management** > **End User** to create a new end user.)

Step 2 Associate the device with the end user, so that the device is displayed under Controlled Devices for the end user.

Step 3 Assign the Standard CCM End User permissions to the end user.

Step 4 In the **Device Configuration** window for the device, assign this end user in the **Owner User ID** field.

Subscribe User with UCM App

A device user uses the UCM app on the device to subscribe or unsubscribe applications that were created on Cisco Unified Communications Manager.

Procedure

Step 1 Use the end user credentials to log in to UCM App on the device.
Upon successful login, the UCM App displays all Android applications that have been created in Cisco Unified Communications Manager.

Step 2 To subscribe to an application, check the check box next to the application name.
This action triggers the download and installation of the application on the device.

Note Some applications present detailed information to the user. Upon checking the box or choosing the application, the user sees a second screen. To subscribe to these applications, check the box on the second screen and tap **Back**. This action triggers the installation.

Step 3 To unsubscribe from an application, uncheck the check box next to the application name.

Push Android APK Files Through Cisco Unified Communications Manager

To push Android APK files from Cisco Unified Communications Manager, first configure the application as a phone service and then subscribe a device to the service.

Procedure

Step 1 Extract the AndroidManifest file from the APK by using the following apktool:

http://code.google.com/p/android-apktool/

Step 2 Add the Android Service in Cisco Unified Communications Manager Administration.

Step 3 Subscribe the device to the Android Service.

Add Android Service in Cisco Unified Communications Manager Administration

Follow these steps to add an Android service in Cisco Unified Communications Manager Administration.

Before You Begin

Use this procedure after you extract an AndroidManifest file from an APK.

Procedure

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

Step 2 Click **Add New**.

Step 3 In the **Service Name** field, enter a name that matches the package name from the AndroidManifest file that you extracted from the APK.

Step 4 In the **Service Category** drop-down list box, choose **Android APK**.

Step 5 Other fields in this window are optional: you may enter information that you see in the AndroidManifest file.

Step 6 Check the **Enable** check box.

Step 7 Click **Save**.

Subscribe Device to Android Phone Service

Before You Begin

You must add an Android phone service in Cisco Unified Communications Manager Administration before you can subscribe a device to that phone service.

Procedure

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

Step 2 In the **Find and List Phone** window that is displayed, find the device to subscribe to the Android phone service.

Step 3 Click the Device Name entry for the device that you choose.

Step 4 In the **Phone Configuration** window for the device, choose **Subscribe/Unsubscribe Services** from the **Related Links** drop-down list box.

The Subscribed Cisco IP Phone Services for <device name> window opens.

Step 5 In the Subscribed Cisco IP Phone Services window for the device, use the **Select a service** drop-down list box to choose the service that you created.
This action triggers subscription of the device to the service that you specify.

Step 6 Click **Next**.

Step 7 Click **Subscribe**.