Cisco IP Conference Phone Features and Setup

Cisco IP Phone User Support

If you are a system administrator, you are likely the primary source of information for Cisco IP Phone users in your network or company. It is important to provide current and thorough information to end users.

To successfully use some of the features on the Cisco IP Phone (including Services and voice message system options), users must receive information from you or from your network team or must be able to contact you for assistance. Make sure to provide users with the names of people to contact for assistance and with instructions for contacting those people.

We recommend that you create a web page on your internal support site that provides end users with important information about their Cisco IP Phones.

Consider including the following types of information on this site:

- User guides for all Cisco IP Phone models that you support
- Information on how to access the Cisco Unified Communications Self Care Portal
- List of features supported
- User guide or quick reference for your voicemail system

Migration of your Phone to a Multiplatform Phone Directly

You can migrate your enterprise phone to a multiplatform phone easily in one step without using transition firmware load. All you need is to obtain and authorize the migration license from the server.

For more information, see https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/MPP/MPP-conversion/enterprise-to-mpp/cuip_b_conversion-guide-ipphone.html

Set Up a New Softkey Template

You need to add softkeys to a softkey template to give users access to some features. For example, if you want users to be able to use do not disturb, you need to enable the softkey. For more information, see the documentation for your particular Cisco Unified Communications Manager release.

You may want to create several templates. For example, you might want a template for the phone in a conference room, and another template for a phone in an executive's office.

This procedure takes you through the steps to create a new softkey template and assign it to a specific phone. Similar to other phone features, you can also use the template for all your conference phones or a group of phones.

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration as an administrator.

Step 2 Select **Device** > **Device Settings** > **Softkey Template**.

Step 3 Click **Find**.

Step 4 Select one of the following options:

- Cisco Unified Communications Manager 11.5 and previous releases—**Standard User**
- Cisco Unified Communications Manager 12.0 and later releases—**Personal Conference User** or **Public Conference User**.

Step 5 Click **Copy**.

Step 6 Change the name of the template.

For example, 8832 Conference Room Template.

Step 7 Click **Save**.

Step 8 Go to the **Configure Softkey Layout** page from the top right menu.

Step 9 For each call state, set the features to display.

Step 10 Click **Save**.

Step 11 Return to the **Find/List screen** from the top right menu.

You see your new template in the list of templates.

Step 12 Select **Device** > **Phone**.

Step 13 Find the phone to have the new template and select it.

Step 14 In the **Softkey Template** field, select the new softkey template.

Step 15 Click **Save** and **Apply Config**.

Related Topics

Cisco Unified Communications Manager Documentation

Configure Phone Services for Users

You can give users access to Cisco IP Phone Services on the IP phone. You can also assign a button to different phone services. The IP phone manages each service as a separate application.

Before a user can access any service:

- Use Cisco Unified Communications Manager Administration to configure services that are not present by default.
- The user must subscribe to services by using the Cisco Unified Communications Self Care Portal. This web-based application provides a graphical user interface (GUI) for limited, end-user configuration of IP phone applications. However, a user cannot subscribe to any service that you configure as an enterprise subscription.

For more information, see the documentation for your particular Cisco Unified Communications Manager release.

Before you set up services, gather the URLs for the sites that you want to set up and verify that users can access those sites from your corporate IP telephony network. This activity is not applicable for the default services that Cisco provides.

Procedure

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

Step 2 Verify that your users can access the Cisco Unified Communications Self Care Portal, from which they can select and subscribe to configured services.

See Self Care Portal Overview for a summary of the information that you must provide to end users.

Related Topics

Cisco Unified Communications Manager Documentation

Phone Feature Configuration

You can set up phones to have a variety of features, based on the needs of your users. You can apply features to all phones, a group of phones, or to individual phones.

When you set up features, the Cisco Unified Communications Manager Administration window displays information that is applicable to all phones and information that is applicable to the phone model. The information that is specific to the phone model is in the Product Specific Configuration Layout area of the window.

For information on the fields applicable to all phone models, see the Cisco Unified Communications Manager documentation.

When you set a field, the window that you set the field in is important because there is a precedence to the windows. The precedence order is:

1. Individual phones (highest precedence)
2. Group of phones
3. All phones (lowest precedence)

For example, if you don't want a specific set of users to access the phone Web pages, but the rest of your users can access the pages, you:

1. Enable access to the phone web pages for all users.
2. Disable access to the phone web pages for each individual user, or set up a user group and disable access to the phone web pages for the group of users.
3. If a specific user in the user group did need access to the phone web pages, you could enable it for that particular user.

Related Topics

Configure User Credentials Persistent for Expressway Sign-In, on page 27

Set Up Phone Features for All Phones

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration as an administrator.

Step 2 Select **System** > **Enterprise Phone Configuration**.

Step 3 Set the fields you want to change.

Step 4 Check the **Override Enterprise Settings** check box for any changed fields.

Step 5 Click **Save**.

Step 6 Click **Apply Config**.

Step 7 Restart the phones.

Note This will impact all phones in your organization.

Related Topics

Product Specific Configuration, on page 5

Set Up Phone Features for a Group of Phones

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration as an administrator.

Step 2 Select **Device** > **Device Settings** > **Common Phone Profile**.

Step 3 Locate the profile.

Step 4 Navigate to the Product Specific Configuration Layout pane and set the fields.

Step 5 Check the **Override Enterprise Settings** check box for any changed fields.
Step 6 Click **Save**.
Step 7 Click **Apply Config**.
Step 8 Restart the phones.

Related Topics

Product Specific Configuration, on page 5

Set Up Phone Features for a Single Phone

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration as an administrator.
Step 2 Select **Device** > **Phone**
Step 3 Locate the phone associated with the user.
Step 4 Navigate to the Product Specific Configuration Layout pane and set the fields.
Step 5 Check the **Override Common Settings** check box for any changed fields.
Step 6 Click **Save**.
Step 7 Click **Apply Config**.
Step 8 Restart the phone.

Related Topics

Product Specific Configuration, on page 5

Product Specific Configuration

The following table describes the fields in the Product Specific Configuration Layout pane. Some fields in this table only display in the **Device** > **Phone** page.

Table 1: Product Specific Configuration Fields

Field Name	Field Type Or Choices	Default	Description
Settings Access	Disabled Enabled Restricted	Enabled	Enables, disables, or restricts access to local configuration settings in the Settings app. With restricted access, the Preferences and System Information menus can be accessed. Some settings in the Wi-Fi menu are also accessible. With disabled access, the Settings menu does not display any options.

Field Name	Field Type Or Choices	Default	Description
Gratuitous ARP	Disabled Enabled	Disabled	Enables or disables the ability for the phone to learn MAC addresses from Gratuitous ARP. This capability is required to monitor or record voice streams.
Web Access	Disabled Enabled	Disabled	Enables or disables access to the phone web pages through a web browser. **Caution** If you enable this field, you may expose sensitive information about the phone.
Disable TLS 1.0 and TLS 1.1 for WebAccess	Disabled Enabled	Enabled	Controls the use of TLS 1.2 for a web server connection. • Disabled—A phone configured for TLS1.0, TLS 1.1, or TLS1.2 can function as a HTTPs server. • Enabled—Only a phone configured for TLS1.2 can function as a HTTPs server.
Enbloc Dialing	Disabled Enabled	Disabled	Controls the dialing method. • Disabled—The Cisco Unified Communications Manager waits for the interdigit timer to expire when there is a dial plan or route pattern overlap. • Enabled—The entire dialed string is sent to Cisco Unified Communications Manager once the dialing is complete. To avoid the T.302 timer timeout, we recommend that you enable Enbloc dialing whenever there is a dialplan or route pattern overlap. Forced Authorization Codes (FAC) or Client Matter Codes (CMC) do not support the Enbloc Dialing. If you use FAC or CMC to manage call access and accounting, then you cannot use this feature.
Days Backlight Not Active	Days of the week		Defines the days that the backlight does not turn on automatically at the time specified in the Backlight On Time field. Choose the day or days from the drop-down list. To choose more than one day, **Ctrl+click** each day that you want. See Schedule Power Save for Cisco IP Phone, on page 17.

Field Name	Field Type Or Choices	Default	Description
Backlight On Time	hh:mm		Defines the time each day that the backlight turns on automatically (except on the days specified in the Backlight Display Not Active field). Enter the time in this field in 24 hour format, where 0:00 is midnight. For example, to automatically turn the backlight on at 07:00 a.m. (0700), enter 07:00. To turn the backlight on at 02:00 p.m. (1400), enter 14:00. If this field is blank, the backlight automatically turns on at 0:00. See Schedule Power Save for Cisco IP Phone, on page 17.
Backlight On Duration	hh:mm		Defines the length of time that the backlight remains on after turning on at the time specified in the Backlight On Time field. For example, to keep the backlight on for 4 hours and 30 minutes after it turns on automatically, enter 04:30. If this field is blank, the phone turns off at the end of the day (0:00). If Backlight On Time is 0:00 and the backlight on duration is blank (or 24:00), the backlight does not turn off. See Schedule Power Save for Cisco IP Phone, on page 17.
Backlight Idle Timeout	hh:mm		Defines the length of time that the phone is idle before the backlight turns off. Applies only when the backlight was off as scheduled and was turned on by a user (by pressing a button on the phone or lifting the handset). For example, to turn the backlight off when the phone is idle for 1 hour and 30 minutes after a user turns the backlight on, enter 01:30. See Schedule Power Save for Cisco IP Phone, on page 17.
Backlight On When Incoming Call	Disabled Enabled	Enabled	Turns the backlight on when there is an incoming call.

Field Name	Field Type Or Choices	Default	Description
Enable Power Save Plus	Days of the week		Defines the schedule of days for which the phone powers off. Choose the day or days from the drop-down list. To choose more than one day, **Ctrl+click** each day that you want. When Enable Power Save Plus is turned on, you receive a message that warns about emergency (e911) concerns. **Caution** While Power Save Plus Mode (the "Mode") is in effect, endpoints that are configured for the mode are disabled for emergency calling and from receiving inbound calls. By selecting this mode, you agree to the following: (i) You take full responsibility for providing alternate methods for emergency calling and receiving calls while the mode is in effect; (ii) Cisco has no liability in connection with your selection of the mode and all liability in connection with enabling the mode is your responsibility; and (iii) You fully inform users of the effects of the mode on calls, calling and otherwise. To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. If the Allow EnergyWise Overrides remains checked but no days are selected in the Enable Power Save Plus field, Power Save Plus is not disabled. See Schedule EnergyWise on Cisco IP Phone, on page 18.

Field Name	Field Type Or Choices	Default	Description
Phone On Time	hh:mm		Determines when the phone automatically turns on for the days that are in the Enable Power Save Plus field. Enter the time in this field in 24-hour format, where 00:00 is midnight. For example, to automatically power up the phone at 07:00 a.m. (0700), enter 07:00. To power up the phone at 02:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00. The Phone On Time must be at least 20 minutes later than the Phone Off Time. For example, if the Phone Off Time is 07:00, the Phone On Time must be no earlier than 07:20. See Schedule EnergyWise on Cisco IP Phone, on page 18.
Phone Off Time	hh:mm		Defines the time of day that the phone powers down for the days that are selected in the Enable Power Save Plus field. If the Phone On Time and the Phone Off Time fields contain the same value, the phone does not power down. Enter the time in this field in 24-hour format, where 00:00 is midnight. For example, to automatically power down the phone at 7:00 a.m. (0700), enter 7:00. To power down the phone at 2:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00. The Phone On Time must be at least 20 minutes later than the Phone Off Time. For example, if the Phone Off Time is 7:00, the Phone On Time must be no earlier than 7:20. See Schedule EnergyWise on Cisco IP Phone, on page 18.

Field Name	Field Type Or Choices	Default	Description
Phone Off Idle Timeout	hh:mm		Indicates the length of time that the phone must be idle before the phone powers down. The timeout occurs under the following conditions: • When the phone was in Power Save Plus mode, as scheduled, and was taken out of Power Save Plus mode because the phone user pressed the Select key. • When the phone is repowered by the attached switch. • When the Phone Off Time is reached but the phone is in use. See Schedule EnergyWise on Cisco IP Phone, on page 18.
Enable Audible Alert	Checkbox	Unchecked	When enabled, instructs the phone to play an audible alert starting 10 minutes before the time that the Phone Off Time field specifies. This check box applies only if the Enable Power Save Plus list box has one or more days selected. See Schedule EnergyWise on Cisco IP Phone, on page 18.
EnergyWise Domain	Up to 127 characters		Identifies the EnergyWise domain that the phone is in. See Schedule EnergyWise on Cisco IP Phone, on page 18.
EnergyWise Secret	Up to 127 characters		Identifies the security secret password that is used to communicate with the endpoints in the EnergyWise domain. See Schedule EnergyWise on Cisco IP Phone, on page 18.

Field Name	Field Type Or Choices	Default	Description
Allow EnergyWise Overrides	Check box	Unchecked	Determines whether you allow the EnergyWise domain controller policy to send power level updates to the phones. The following conditions apply: • One or more days must be selected in the Enable Power Save Plus field. • The settings in Cisco Unified Communications Manager Administration take effect on schedule even if EnergyWise sends an override. For example, assuming the Phone Off Time is set to 22:00 (10:00 p.m.), the value in the Phone On Time field is 06:00 (6:00 a.m.), and the Enable Power Save Plus has one or more days selected. • If EnergyWise directs the phone to turn off at 20:00 (8:00 p.m.), that directive remains in effect (assuming no phone user intervention occurs) until the configured Phone On Time at 6:00 a.m. • At 6:00 a.m., the phone turns on and resumes receiving the power level changes from the settings in Cisco Unified Communications Manager Administration. • To change the power level on the phone again, EnergyWise must reissue a new power level change command. To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. If the Allow EnergyWise Overrides remains checked but no days are selected in the Enable Power Save Plus field, Power Save Plus is not disabled. See Schedule EnergyWise on Cisco IP Phone, on page 18.
Join And Direct Transfer Policy	Same line enable Same line disable	Same line, across line enable	Controls the ability of a user to join and transfer calls. • Same line enable—Users can directly transfer or join a call on the current line to another call on the same line. • Same line disable— Users can't join or transfer calls on the same line. The join and transfer features are disabled and the user can't do the direct transfer or join function.

Field Name	Field Type Or Choices	Default	Description
Recording Tone	Disabled Enabled	Disabled	Controls the playing of the tone when a user is recording a call
Recording Tone Local Volume	Integer 0–100	100	Controls the volume of the recording tone to the local user.
Recording Tone Remote Volume	Integer 0–100	50	Controls the volume of the recording tone to the remote user.
Recording Tone Duration	Integer 1–3000 milliseconds		Controls the duration of the recording tone.
Log Server	String of up to 256 characters		Identifies the IPv4 syslog server for phone debug output. The format for the address is: **address:<port>@@base=<0-7>;pfs=<0-1>**
Remote Log	Disabled Enabled	Disabled	Controls the ability to send logs to the syslog server.
Log Profile	Default Preset Telephony SIP UI Network Media Upgrade Accessory Security Energywise MobileRemoteAccess	Preset	Specifies the predefined logging profile. • Default—Default debug logging level • Preset—Does not overwrite the phone local debug logging setting • Telephony—Logs information about Telephony or call features • SIP—Logs information about SIP signaling • UI—Logs information about the phone user interface • Network—Logs network information • Media—Logs media information • Upgrade—Logs upgrade information • Accessory—Logs accessory information • Security—Logs security information • Energywise—Logs energy-savings information • MobileRemoteAccess—Logs Mobile and Remote Access through Expressway information
IPv6 Log Server	String of up to 256 characters		Identifies the IPv6 syslog server for phone debug output.

Field Name	Field Type Or Choices	Default	Description
Cisco Discovery Protocol (CDP): Switch Port	Disabled Enabled	Enabled	Controls Cisco Discovery Protocol on the phone.
Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port	Disabled Enabled	Enabled	Enables LLDP-MED on the SW port.
LLDP Asset ID	String, up to 32 characters		Identifies the asset ID that is assigned to the phone for inventory management.
Energy Efficient Ethernet(EEE): Switch Port	Disabled Enabled	Disabled	Controls EEE on the switch port.
LLDP Power Priority	Unknown Low High Critical	Unknown	Assigns a phone power priority to the switch, thus enabling the switch to appropriately provide power to the phones.
802.1x Authentication	User Controlled Disabled Enabled	User Controlled	Specifies the 802.1x authentication feature status. • User Controlled—The user can configure the 802.1x on the phone. • Disabled—802.1x authentication is not used. • Enabled—802.1x authentication is used, and you configure the authentication for the phones.
Switch Port Remote Configuration	Disabled Auto Negotiate 10 Half 10 Full 100 Half 100 Full	Disabled	Allows you to configure the speed and duplex function of the phone SW port remotely. This enhances the performance for large deployments with specific port settings. If the SW ports are configured for Remote Port Configuration in Cisco Unified Communications Manager, the data cannot be changed on the phone.
SSH Access	Disabled Enabled	Disabled	Controls the access to the SSH daemon through port 22. Leaving port 22 open leaves the phone vulnerable to Denial of Service (DoS) attacks.
Ring Locale	Default Japan	Default	Controls the ringing pattern.

Field Name	Field Type Or Choices	Default	Description
TLS Resumption Timer	Integer 0–3600 seconds	3600	Controls the ability to resume a TLS session without repeating the entire TLS authentication process. If the field is set to 0, then the TLS session resumption is disabled.
FIPS Mode	Disabled Enabled	Disabled	Enables or disables the Federal Information Processing Standards (FIPS) mode on the phone.
Record Call Log from Shared Line	Disabled Enabled	Disabled	Specifies whether to record call log from a shared line.
Minimum Ring Volume	0 - Silent 1–15	0 - Silent	Controls the minimum ring volume for the phone.
Peer Firmware Sharing	Disabled Enabled	Enabled	Allows the phone to find other phones of the same model on the subnet and share updated firmware files. If the phone has a new firmware load, it can share that load with the other phones. If one of the other phones has a new firmware load, the phone can download the firmware from the other phone, instead of from the TFTP server. Peer firmware sharing: • Limits congestion on TFTP transfers to centralized remove TFTP servers. • Eliminates the need to manually control firmware upgrades. • Reduces phone downtime during upgrades when large numbers of phones are reset simultaneously. • Helps with firmware upgrades in branch or remote office deployment scenarios that run over bandwidth-limited WAN links.
Load Server	String of up to 256 characters		Identifies the alternate IPv4 server that the phone uses to obtain firmware loads and upgrades.
IPv6 Load Server	String of up to 256 characters		Identifies the alternate IPv6 server that the phone uses to obtain firmware loads and upgrades.

Field Name	Field Type Or Choices	Default	Description
Detect Unified CM Connection Failure	Normal Delayed	Normal	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. The precise time difference between Normal and Delayed connection failure detection depends on many variables that are constantly changing.
Special Requirement ID	String		Controls custom features from Engineering Special (ES) loads.
HTTPS Server	http and https Enabled https only	http and https Enabled	Controls the type of communication to the phone. If you select HTTPS only, the phone communication is more secure.
User Credentials Persistent for Expressway Sign in	Disabled Enabled	Disabled	Controls if the phone stores the users' sign-in credentials. When disabled, the user is always sees the prompt to sign into the Expressway server for Mobile and Remote Access (MRA). If you want to make it easier for users to log in, you enable this field so that the Expressway login credentials are persistent. The user then only has to enter their login credentials the first time. Any time after that (when the phone is powered on off-premises), the login information is prepopulated on the Sign-in screen. For more information, see the Configure User Credentials Persistent for Expressway Sign-In, on page 27.

Field Name	Field Type Or Choices	Default	Description
Customer support upload URL	String, up to 256 characters		Provides the URL for the Problem Report Tool (PRT). If you deploy devices with Mobile and Remote Access through Expressway, you must also add the PRT server address to the HTTP Server Allow list on the Expressway server. For more information, see the Configure User Credentials Persistent for Expressway Sign-In, on page 27.
Disable TLS Ciphers	See Disable Transport Layer Security Ciphers, on page 16.	None	Disables the selected TLS cipher. Disable more than one cipher suite by selecting and holding the **Ctrl** key on your computer keyboard.
Dedicate one line for Call Park	Disabled Enabled	Enabled	Controls whether a parked call occupies one line or not. For more information, see the Cisco Unified Communications Manager documentation.

Related Topics

Configure User Credentials Persistent for Expressway Sign-In, on page 27

Disable Transport Layer Security Ciphers

You can disable Transport Layer Security (TLS) ciphers with the **Disable TLS Ciphers** parameter. This allows you to tailor your security for known vulnerabilities, and to align your network with your company's policies for ciphers.

None is the default setting.

Disable more than one cipher suite by selecting and holding the **Ctrl** key on your computer keyboard. If you select all of the phone ciphers, then phone TLS service is impacted. Your choices are:

- None
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

For more information about phone security, see *Cisco IP Phone 7800 and 8800 Series Security Overview White Paper* (https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html).

Schedule Power Save for Cisco IP Phone

To conserve power and ensure the longevity of the phone screen display, you can set the display to turn off when it is not needed.

You can configure settings in Cisco Unified Communications Manager Administration to turn off the display at a designated time on some days and all day on other days. For example, you may choose to turn off the display after business hours on weekdays and all day on Saturdays and Sundays.

You can take any of these actions to turn on the display any time it is off:

- Press any button on the phone.

  The phone takes the action designated by that button in addition to turning on the display.
- Lift the handset.

When you turn the display on, it remains on until the phone has remained idle for a designated length of time, then it turns off automatically.

Procedure

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

Step 2 Locate the phone that you need to set up.

Step 3 Navigate to the Product Specific Configuration area and set the following fields:

- Days Display Not Active
- Display On Time
- Display On Duration
- Display Idle Timeout

Table 2: PowerSave Configuration Fields

Field	Description
Days Display Not Active	Days that the display does not turn on automatically at the time specified in the Display On Time field. Choose the day or days from the drop-down list. To choose more than one day, Ctrl-click each day that you want.

Field	Description
Display On Time	Time each day that the display turns on automatically (except on the days specified in the Days Display Not Active field). Enter the time in this field in 24-hour format, where 0:00 is midnight. For example, to automatically turn the display on at 07:00a.m., (0700), enter **07:00**. To turn the display on at 02:00p.m. (1400), enter **14:00**. If this field is blank, the display will automatically turn on at 0:00.
Display On Duration	Length of time that the display remains on after turning on at the time specified in the Display On Time field. Enter the value in this field in the format *hours:minutes*. For example, to keep the display on for 4 hours and 30 minutes after it turns on automatically, enter **04:30**. If this field is blank, the phone will turn off at the end of the day (0:00). **Note** If Display On Time is 0:00 and the display on duration is blank (or 24:00), the display will remain on continuously.
Display Idle Timeout	Length of time that the phone is idle before the display turns off. Applies only when the display was off as scheduled and was turned on by a user (by pressing a button on the phone or lifting the handset). Enter the value in this field in the format *hours:minutes*. For example, to turn the display off when the phone is idle for 1 hour and 30 minutes after a user turns the display on, enter **01:30**. The default value is 01:00.

Step 4 Select **Save**.

Step 5 Select **Apply Config**.

Step 6 Restart the phone.

Schedule EnergyWise on Cisco IP Phone

To reduce power consumption, configure the phone to sleep (power down) and wake (power up) if your system includes an EnergyWise controller.

You configure settings in Cisco Unified Communications Manager Administration to enable EnergyWise and configure sleep and wake times. These parameters are closely tied to the phone display configuration parameters.

When EnergyWise is enabled and a sleep time is set, the phone sends a request to the switch to wake it up at the configured time. The switch returns either an acceptance or a rejection of the request. If the switch rejects the request or if the switch does not reply, the phone does not power down. If the switch accepts the request, the idle phone goes to sleep, thus reducing the power consumption to a predetermined level. A phone that is not idle sets an idle timer and goes to sleep after the idle timer expires.

To wake up the phone, press Select. At the scheduled wake time, the system restores power to the phone, waking it up.

Procedure

Step 1 From the Cisco Unified Communications Manager Administration, select **Device** > **Phone**.

Step 2 Locate the phone that you need to set up.

Step 3 Navigate to the Product Specific Configuration area and set the following fields.

- Enable Power Save Plus
- Phone On Time
- Phone Off Time
- Phone Off Idle Timeout
- Enable Audible Alert
- EnergyWise Domain
- EnergyWise Secret
- Allow EnergyWise Overrides

Table 3: EnergyWise Configuration Fields

Field	Description
Enable Power Save Plus	Selects the schedule of days for which the phone powers off. Select multiple days by pressing and holding the Control key while clicking on the days for the schedule. By default, no days are selected. When Enable Power Save Plus is checked, you receive a message that warns about emergency (e911) concerns. **Caution** While Power Save Plus Mode (the "Mode") is in effect, endpoints that are configured for the mode are disabled for emergency calling and from receiving inbound calls. By selecting this mode, you agree to the following: (i) You take full responsibility for providing alternate methods for emergency calling and receiving calls while the mode is in effect; (ii) Cisco has no liability in connection with your selection of the mode and all liability in connection with enabling the mode is your responsibility; and (iii) You fully inform users of the effects of the mode on calls, calling and otherwise. **Note** To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. If the Allow EnergyWise Overrides remains checked but no days are selected in the Enable Power Save Plus field, Power Save Plus is not disabled.

Field	Description
Phone On Time	Determines when the phone automatically turns on for the days that are in the Enable Power Save Plus field. Enter the time in this field in 24-hour format, where 00:00 is midnight. For example, to automatically power up the phone at 07:00 a.m. (0700), enter 07:00. To power up the phone at 02:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00. **Note** The Phone On Time must be at least 20 minutes later than the Phone Off Time. For example, if the Phone Off Time is 07:00, the Phone On Time must be no earlier than 07:20.
Phone Off Time	The time of day that the phone powers down for the days that are selected in the Enable Power Save Plus field. If the Phone On Time and the Phone Off Time fields contain the same value, the phone does not power down. Enter the time in this field in 24-hour format, where 00:00 is midnight. For example, to automatically power down the phone at 7:00 a.m. (0700), enter 7:00. To power down the phone at 2:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00. **Note** The Phone On Time must be at least 20 minutes later than the Phone Off Time. For example, if the Phone Off Time is 7:00, the Phone On Time must be no earlier than 7:20.
Phone Off Idle Timeout	The length of time that the phone must be idle before the phone powers down. The timeout occurs under the following conditions: • When the phone was in Power Save Plus mode, as scheduled, and was taken out of Power Save Plus mode because the phone user pressed the **Select** key. • When the phone is repowered by the attached switch. • When the Phone Off Time is reached but the phone is in use. The range of the field is 20 to 1440 minutes. The default value is 60 minutes.

Field	Description
Enable Audible Alert	When enabled, instructs the phone to play an audible alert starting 10 minutes before the time that the Phone Off Time field specifies. The audible alert uses the phone ringtone, which briefly plays at specific times during the 10-minute alerting period. The alerting ringtone plays at the user-designated volume level. The audible alert schedule is: • At 10 minutes before power down, play the ringtone four times. • At 7 minutes before power down, play the ringtone four times. • At 4 minutes before power down, play the ringtone four times. • At 30 seconds before power down, play the ringtone 15 times or until the phone powers off. This check box applies only if the Enable Power Save Plus list box has one or more days selected.
EnergyWise Domain	The EnergyWise domain that the phone is in. The maximum length of this field is 127 characters.
EnergyWise Secret	The security secret password that is used to communicate with the endpoints in the EnergyWise domain. The maximum length of this field is 127 characters.
Allow EnergyWise Overrides	This check box determines whether you allow the EnergyWise domain controller policy to send power level updates to the phones. The following conditions apply: • One or more days must be selected in the Enable Power Save Plus field. • The settings in Cisco Unified Communications Manager Administration take effect on schedule even if EnergyWise sends an override. For example, assuming the Phone Off Time is set to 22:00 (10:00 p.m.), the value in the Phone On Time field is 06:00 (6:00 a.m.), and the Enable Power Save Plus has one or more days selected. • If EnergyWise directs the phone to turn off at 20:00 (8:00 p.m.), that directive remains in effect (assuming no phone user intervention occurs) until the configured Phone On Time at 6:00 a.m. • At 6:00 a.m., the phone turns on and resumes receiving the power level changes from the settings in Unified Communications Manager Administration. • To change the power level on the phone again, EnergyWise must reissue a new power level change command. **Note** To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. If the Allow EnergyWise Overrides remains checked but no days are selected in the Enable Power Save Plus field, Power Save Plus is not disabled.

Step 4 Select **Save**.

Step 5 Select **Apply Config**.

Step 6 Restart the phone.

Set Up Do Not Disturb

When Do Not Disturb (DND) is turned on, the header on the conference phone screen is red.

For more information, see the Do Not Disturb information in the documentation for your particular Cisco Unified Communications Manager release.

Procedure

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

Step 2 Locate the phone to be configured.

Step 3 Set the following parameters.

- Do Not Disturb: This check box allows you to enable DND on the phone.
- DND Option: Ring Off, Call Reject, or Use Common Phone Profile Setting.
- DND Incoming Call Alert: Choose the type of alert, if any, to play on a phone for incoming calls when DND is active.

Note This parameter is located on in the Common Phone Profile window and the Phone Configuration window. The Phone Configuration window value takes precedence.

Step 4 Select **Save**.

Related Topics

Cisco Unified Communications Manager Documentation

Set Up Call Forward Notification

You can control the call forward settings.

Procedure

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

Step 2 Locate the phone to be set up.

Step 3 Configure the Call Forward Notification fields.

Field	Description
Caller Name	When this check box is checked, the caller name displays in the notification window. By default, this check box is checked.

Field	Description
Caller Number	When this check box is checked, the caller number displays in the notification window. By default, this check box is not checked.
Redirected Number	When this check box is checked, the information about the caller who last forwarded the call displays in the notification window. Example: If Caller A calls B, but B has forwarded all calls to C and C has forwarded all calls to D, the notification box that D sees contains the phone information for caller C. By default, this check box is not checked.
Dialed Number	When this check box is checked, the information about the original recipient of the call displays in the notification window. Example: If Caller A calls B, but B has forwarded all calls to C and C has forwarded all calls to D, then the notification box that D sees contains the phone information for caller B. By default, this check box is checked.

Step 4 Select **Save**.

UCR 2008 Setup

The parameters that support UCR 2008 reside in Cisco Unified Communications Manager Administration. The following table describes the parameters and indicates the path to change the setting.

Table 4: UCR 2008 Parameter Location

Parameter	Administration Path
FIPS Mode	**Device** > **Device Settings** > **Common Phone Profile**
	System > **Enterprise Phone Configuration**
	Device > **Phones**
SSH Access	**Device** > **Phone**
	Device > **Device Settings** > **Common Phone Profile**
Web Access	**Device** > **Phone**
	System > **Enterprise Phone Configuration**
	Device > **Device Settings** > **Common Phone Profile**
System > **Enterprise Phone Configuration**	

Parameter	Administration Path
IP Addressing Mode	**Device** > **Device Settings** > **Common Device Configuration**
IP Addressing Mode Preference for Signaling	**Device** > **Device Settings** > **Common Device Configuration**

Set Up UCR 2008 in Common Device Configuration

Use this procedure to set the following UCR 2008 parameters:

- IP Addressing Mode
- IP Addressing Mode Preference for Signaling

Procedure

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

Step 2 Set the IP Addressing Mode parameter.

Step 3 Set the IP Addressing Mode Preference for Signaling parameter.

Step 4 Select **Save**.

Set Up UCR 2008 in Common Phone Profile

Use this procedure to set the following UCR 2008 parameters:

- FIPS Mode
- SSH Access
- Web Access

Procedure

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

Step 2 Set the FIPS Mode parameter to **Enabled**.

Step 3 Set the SSH Access parameter to **Disabled**.

Step 4 Set the Web Access parameter to **Disabled**.

Step 5 Set the 80-bit SRTCP parameter to **Enabled**.

Step 6 Select **Save**.

Set Up UCR 2008 in Enterprise Phone Configuration

Use this procedure to set the following UCR 2008 parameters:

- FIPS Mode
- Web Access

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **System** > **Enterprise Phone Configuration**.

Step 2 Set the FIPS Mode parameter to **Enabled**.

Step 3 Set the Web Access parameter to **Disabled**.

Step 4 Select **Save**.

Set Up UCR 2008 in Phone

Use this procedure to set the following UCR 2008 parameters:

- FIPS Mode
- SSH Access
- Web Access

Procedure

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

Step 2 Set the SSH Access parameter to **Disabled**.

Step 3 Set the FIPS Mode parameter to **Enabled**.

Step 4 Set the Web Access parameter to **Disabled**.

Step 5 Select **Save**.

Mobile and Remote Access Through Expressway

Mobile and Remote Access Through Expressway(MRA) lets remote workers easily and securely connect into the corporate network without using a virtual private network (VPN) client tunnel. Expressway uses Transport Layer Security (TLS) to secure network traffic. For a phone to authenticate an Expressway certificate and establish a TLS session, a public Certificate Authority that the phone firmware trusts must sign the Expressway certificate. It is not possible to install or trust other CA certificates on phones for authenticating an Expressway certificate.

The list of CA certificates embedded in the phone firmware is available at http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-technical-reference-list.html.

Mobile and Remote Access Through Expressway (MRA)works with Cisco Expressway. You must be familiar with the Cisco Expressway documentation, including the *Cisco Expressway Administrator Guide* and the *Cisco Expressway Basic Configuration Deployment Guide*. Cisco Expressway documentation is available at http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html.

Only the IPv4 protocol is supported for Mobile and Remote Access Through Expressway users.

For additional information about working with Mobile and Remote Access Through Expressway, see:

- *Cisco Preferred Architecture for Enterprise Collaboration, Design Overview*
- *Cisco Preferred Architecture for Enterprise Collaboration, CVD*
- *Unified Communications Mobile and Remote Access via Cisco VCS Deployment Guide*
- *Cisco TelePresence Video Communication Server (VCS), Configuration Guides*
- *Mobile and Remote Access Through Cisco Expressway Deployment Guide*

During the phone registration process, the phone synchronizes the displayed date and time with the Network Time Protocol (NTP) server. With MRA, the DHCP option 42 tag is used to locate the IP addresses of the NTP servers designated for time and date synchronization. If the DHCP option 42 tag is not found in the configuration information, the phone looks for the 0.tandberg.pool.ntp.org tag to identify the NTP servers.

After registration, the phone uses information from the SIP message to synchronize the displayed date and time unless an NTP server is configured in the Cisco Unified Communications Manager phone configuration.

Note If the phone security profile for any of your phones has TFTP Encrypted Config checked, you cannot use the phone with Mobile and Remote Access. The MRA solution does not support device interaction with Certificate Authority Proxy Function (CAPF).

SIP OAuth mode is supported for MRA. This mode allows you to use OAuth access tokens for authentication in secure environments.

Note For SIP OAuth in Mobile and Remote Access (MRA) mode, use only Activation Code Onboarding with Mobile and Remote Access when you deploy the phone. Activation with a username and password is not supported.

SIP OAuth mode requires Expressway x14.0(1) and later, or Cisco Unified Communications Manager 14.0(1) and later.

For additional information on SIP OAuth mode see *Feature Configuration Guide for Cisco Unified Communications Manager*, Release 14.0(1) or later.

Deployment Scenarios

The following table shows various deployment scenarios for Mobile and Remote Access Through Expressway.

Scenario	Actions
On-premises user logs in to the enterprise network, after deploying Mobile and Remote Access Through Expressway.	The enterprise network is detected, and the phone registers with Cisco Unified Communications Manager as it would normally.

Scenario	Actions
Off-premises user logs in to the enterprise network with Mobile and Remote Access Through Expressway.	The phone detects that it is in off-premises mode, the Mobile and Remote Access Through Expressway Sign-In window appears, and the user connects to the corporate network. Users must have a valid service name, username, and password to connect to the network. Users must also reset the service mode to clear the Alternate TFTP setting before they can access the company network. This clears the Alternate TFTP Server setting so the phone detects the off-premises network. If a phone is being deployed out of the box, users may skip the reset Network Settings requirement. If users have DHCP option 150 or option 66 enabled on their network router, they may not be able to sign in to the corporate network. Users should disable these DHCP settings or configure their static IP address directly.

Configure User Credentials Persistent for Expressway Sign-In

When a user signs in to the network with Mobile and Remote Access Through Expressway, the user is prompted for a service domain, username, and password. If you enable the User Credentials Persistent for Expressway Sign-In parameter, user login credentials are stored so that they do not need to reenter this information. This parameter is disabled by default.

You can set up credentials to persist for a single phone, a group of phones, or all phones.

Related Topics

Phone Feature Configuration, on page 3
Product Specific Configuration, on page 5

Problem Report Tool

Users submit problem reports to you with the Problem Report Tool.

Note The Problem Report Tool logs are required by Cisco TAC when troubleshooting problems. The logs are cleared if you restart the phone. Collect the logs before you restart the phones.

To issue a problem report, users access the Problem Report Tool and provide the date and time that the problem occurred, and a description of the problem.

If the PRT upload fails, you can access the PRT file for the phone from the URL **`http://<phone-ip-address>/FS/<prt-file-name>`**. This URL is displayed on the phone in the following cases:

- If the phone is in the factory default state. The URL is active for 1 hour. After 1 hour, the user should try to submit the phone logs again.
- If the phone has downloaded a configuration file and the call control system allows web access to the phone.

You must add a server address to the **Customer Support Upload URL** field on Cisco Unified Communications Manager.

If you are deploying devices with Mobile and Remote Access through Expressway, you must also add the PRT server address to the HTTP Server Allow list on the Expressway server.

Configure a Customer Support Upload URL

You must use a server with an upload script to receive PRT files. The PRT uses an HTTP POST mechanism, with the following parameters included in the upload (utilizing multipart MIME encoding):

- devicename (example: “SEP001122334455”)
- serialno (example: “FCH12345ABC”)
- username (the username configured in Cisco Unified Communications Manager, the device owner)
- prt_file (example: “probrep-20141021-162840.tar.gz”)

A sample script is shown below. This script is provided for reference only. Cisco does not provide support for the upload script installed on a customer's server.

```
<?php

// NOTE: you may need to edit your php.ini file to allow larger
// size file uploads to work.
// Modify the setting for upload_max_filesize
// I used:  upload_max_filesize = 20M

// Retrieve the name of the uploaded file
$filename = basename($_FILES['prt_file']['name']);

// Get rid of quotes around the device name, serial number and username if they exist
$devicename = $_POST['devicename'];
$devicename = trim($devicename, "'\"");

$serialno = $_POST['serialno'];
$serialno = trim($serialno, "'\"");

$username = $_POST['username'];
$username = trim($username, "'\"");

// where to put the file
$fullfilename = "/var/prtuploads/".$filename;

// If the file upload is unsuccessful, return a 500 error and
// inform the user to try again

if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
        header("HTTP/1.0 500 Internal Server Error");
        die("Error: You must select a file to upload.");
}

?>
```

Note The phones only support HTTP URLs.

Procedure

Step 1 Set up a server that can run your PRT upload script.

Step 2 Write a script that can handle the parameters listed above, or edit the provided sample script to suit your needs.

Step 3 Upload your script to your server.

Step 4 In Cisco Unified Communications Manager, go to the Product Specific Configuration Layout area of the individual device configuration window, Common Phone Profile window, or Enterprise Phone Configuration window.

Step 5 Check **Customer support upload URL** and enter your upload server URL.

Example:

http://example.com/prtscript.php

Step 6 Save your changes.

Set the Label for a Line

You can set up a phone to display a text label instead of the directory number. Use this label to identify the line by name or function. For example, if your user shares lines on the phone, you could identify the line with the name of the person that shares the line.

When adding a label to a key expansion module, only the first 25 characters are displayed on a line.

Procedure

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

Step 2 Locate the phone to be configured.

Step 3 Locate the line instance and set the Line Text Label field.

Step 4 (Optional) If the label needs to be applied to other devices that share the line, check the Update Shared Device Settings check box and click **Propagate Selected**.

Step 5 Select **Save**.