



UC-PHONE-T & UC-PHONE-T-PLUS Crestron Flex VoIP Desk Phones for Microsoft Teams[®] Software

Supplemental Guide

Crestron Electronics, Inc.



Crestron product development software is licensed to Crestron dealers and Crestron Service Providers (CSPs) under a limited non-exclusive, non-transferable Software Development Tools License Agreement. Crestron product operating system software is licensed to Crestron dealers, CSPs, and end-users under a separate End-User License Agreement. Both of these Agreements can be found on the Crestron website at www.crestron.com/legal/software_license_agreement.

The product warranty can be found at www.crestron.com/legal/sales-terms-conditions-warranties.

The specific patents that cover Crestron products are listed at www.crestron.com/legal/patents.

Certain Crestron products contain open source software. For specific information, visit www.crestron.com/legal/open-source-software.

Crestron, the Crestron logo, and Crestron XiO Cloud are either trademarks or registered trademarks of Crestron Electronics, Inc. in the United States and/or other countries. Microsoft Teams is either a trademark or registered trademark of Microsoft Corporation in the United States and/or other countries. Other trademarks, registered trademarks, and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Crestron disclaims any proprietary interest in the marks and names of others. Crestron is not responsible for errors in typography or photography.

This document was written by the Technical Publications department at Crestron.
©2019 Crestron Electronics, Inc.

Contents

- Introduction** **1**

- Deployment** **1**

- Requirements** **2**
 - IT Administrator 2
 - End User 2

- Configuration** **2**
 - Phone Settings 2
 - Set Language 3
 - Time & Date 4
 - Display 5
 - Phone Lock 6
 - Bluetooth® 7
 - Debug 8
 - About 8
 - Network (Admin Only) 9
 - Debug (Admin Only) 13
 - Admin Password (Admin Only) 15
 - Web Configuration 17
 - Connect to the Device 17
 - Log Out from the Device 18
 - Status 19
 - Network 19
 - Features 24
 - Settings 27
 - Security 36

- Crestron XiO Cloud Service** **39**
 - Claim a Single Device 39
 - Claim Multiple Devices 40

- Startup & Sign In** **43**

- Phone Operation** **46**
 - Physical Description 46
 - Sign In 47
 - The Teams Phone Display 49
 - Calls Screen 50

Meetings Screen.....	53
Voicemail	55
Microsoft Teams Rollout	56

UC-PHONE-T & UC-PHONE-T-PLUS Crestron Flex VoIP Desk Phones for Microsoft Teams® Software

Introduction

The UC-PHONE-T & UC-PHONE-T-PLUS Crestron Flex VoIP Desk Phones for Microsoft Teams® software (respectively sold as UC-P100-T & UC-P110-T) are designed for use with the Microsoft Teams intelligent communications platform. These phones enable superior voice calling and full-duplex hands-free conferencing in a stylish desktop package. A consistent user experience at every desk, workstation, and meeting space is provided via the familiar and intuitive Microsoft Teams touch screen UI, affording simple operation with comprehensive call and contact management features, built-in calendaring, and one-touch meeting joins.

This supplemental guide discusses the requirements and configuration instructions for the UC-PHONE-T & UC-PHONE-T-PLUS phones. For information on installing these phones, refer to the UC-PHONE-S /UC-PHONE-T DO Guide (Doc 8358) and the UC-PHONE-S-PLUS/UC-PHONE-T-PLUS DO Guide (Doc 8359) at www.crestron.com/manuals.

Deployment

To make the most of Microsoft Teams, refer to <https://docs.microsoft.com/en-us/MicrosoftTeams/teams-overview> for recommendations on deploying Microsoft Teams throughout an organization.

Requirements

IT Administrator

The IT administrator should have the following knowledge and skills:

- General Skills
 - IP Networking
 - Basic phone terminology
- Crestron-specific skills
 - Crestron XiO Cloud™ service (Cloud Provisioning) helps an administrator quickly manage all devices within an environment. The platform allows an administrator to add devices to a system in order to manage device status, change settings, update firmware, set up new users, manage access levels and manage automated alerts. For training, visit <https://www.crestron.com/en-US/Support/Tools/Applications/Training-Online-Course?id=31>.

NOTE: You must be logged in to your Crestron.com account to access the training course.

End User

The end user should have the following:


- A Microsoft Teams account
- Knowledge of Microsoft Teams

Configuration

The phone is configured with the touch screen (phone settings) and a computer with web browser software (device settings). When using a computer, the phone and computer must be connected to a commonly accessible network.

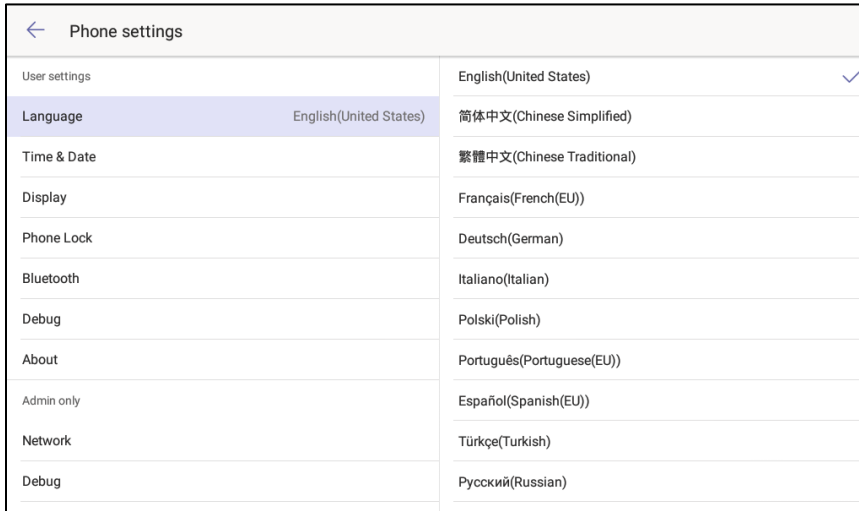
Phone Settings

The device's phone settings can be used to view information about the device, adjust the volume, set the language, view the privacy policy, and configure the device.

To access the partner settings, tap  on the Microsoft Teams start screen. The Phone settings menu is displayed.

NOTE: Partner settings can also be accessed from the main application. To access the partner settings, tap , **Settings**, and then **Device Settings**.

Phone Settings (Language screen shown)



To exit the Phone settings menu, tap ←.

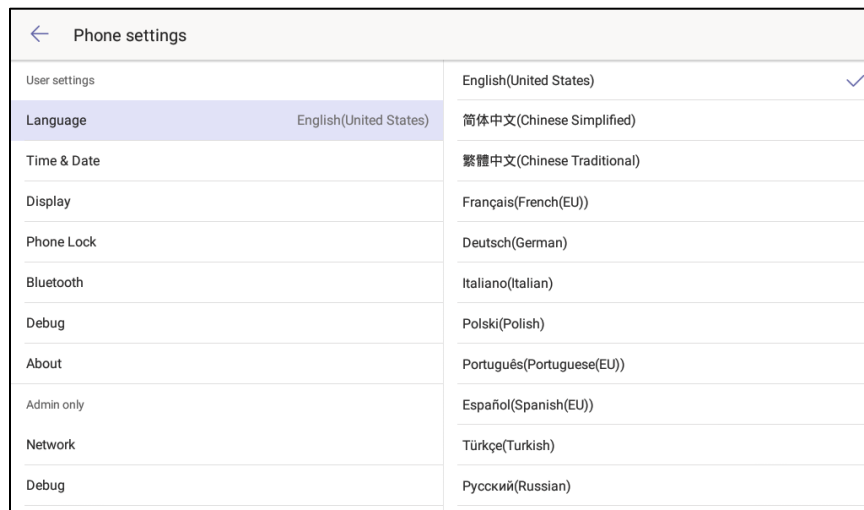
Set Language

The currently selected language is displayed in the language field.

To select a new language:

1. Tap **Language**. A list of languages will display on the right side of the screen.

Language

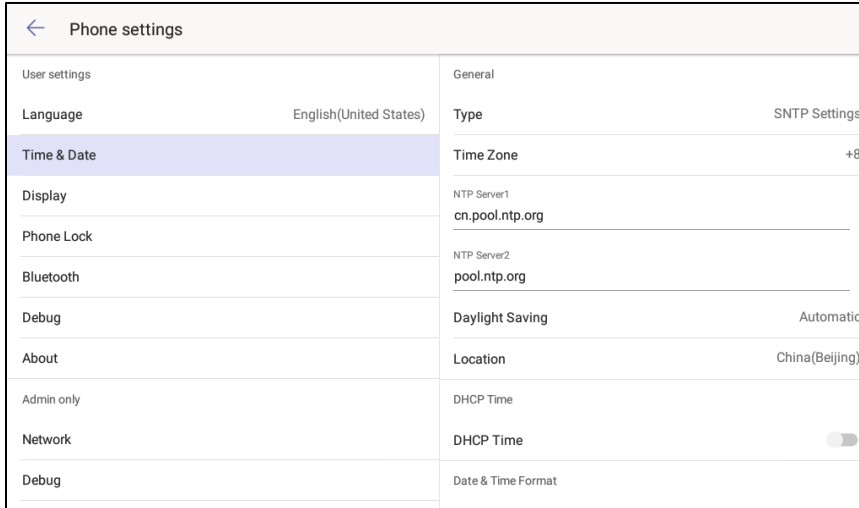


2. Tap a language to select it.
3. A message will display asking to confirm the change. Tap **OK** to change the language, or tap **CANCEL** to cancel.

Time & Date

Tap **Time & Date** to configure the settings the phone will use for determining the time and date. Settings are displayed on the right side of the screen.

Time & Date



Type

Tap **Type** and select whether manual settings or an SNTP (time) server will be used.

- **Manual Settings**

When choosing **Manual Settings**, tap on the following fields and set as needed.

- **Date:** Touch and drag up or down to scroll through settings for year, month, and date. Tap **OK** when done or tap **CANCEL** to cancel.
- **Time:** Touch and drag up or down to scroll through settings for hour, minutes, seconds, and AM or PM. Tap **OK** when done or tap **CANCEL** to cancel.
- **DHCP Time:** Select whether the phone updates time with the offset time offered by the DHCP server.
- **Date & Time Format:** Select the formats for the date (**WWW MMM DD**, **DD-MMM-YY**, **YYYY-MM-DD**, **DD/MM/YYYY**, **MM/DD/YY**, **DD MMM YYYY**, or **WWW DD MMM**) and time (**12 Hour** or **24 Hour**). Tap **OK** when done or tap **CANCEL** to cancel.

- **SNTP Settings**

When choosing **SNTP Settings**, tap on the following fields and set as needed.

- **Time Zone:** Touch and drag up or down to scroll through the amount of time difference from Greenwich Mean Time (GMT). Tap **OK** when done or tap **CANCEL** to cancel.

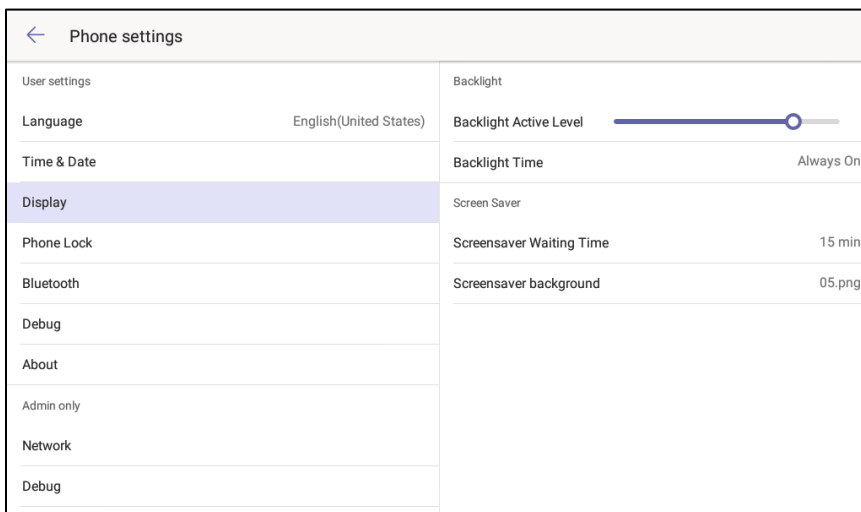
NOTE: Some settings will prompt for locale selection after selecting the time difference. Tap the desired locale and tap **OK**.

- **NTP Server 1:** Enter the URL of the primary time server and tap **Next**.
- **NTP Server 2:** Enter the URL of the secondary time server and tap **Next**.
- **Daylight Saving:** Tap **Disabled**, **Enabled**, or **Automatic**. Tap **OK** when done or tap **CANCEL** to cancel.
- **Location:** Select the location of the phone.
- **DHCP Time:** Select whether the phone updates time with the offset time offered by the DHCP server.
- **Date & Time Format:** Select the formats for the date (**WWW MMM DD**, **DD-MMM-YY**, **YYYY-MM-DD**, **DD/MM/YYYY**, **MM/DD/YY**, **DD MMM YYYY**, or **WWW DD MMM**) and time (**12 Hour** or **24 Hour**). Tap **OK** when done or tap **CANCEL** to cancel.

Display

Tap **Display** to configure the display's backlight and screen saver settings. Settings are displayed on the right side of the screen.

Display



- **Backlight Settings**

The backlight level and duration can be set from the **Backlight** section of the **Display** settings.

- **Backlight Active Level:** Touch and drag left or right to adjust the amount of backlighting.
- **Backlight Time:** Touch and drag up or down to scroll through the amount of time the backlight stays lit. Tap **OK** when done or tap **CANCEL** to cancel.

- **Screen Saver Settings**

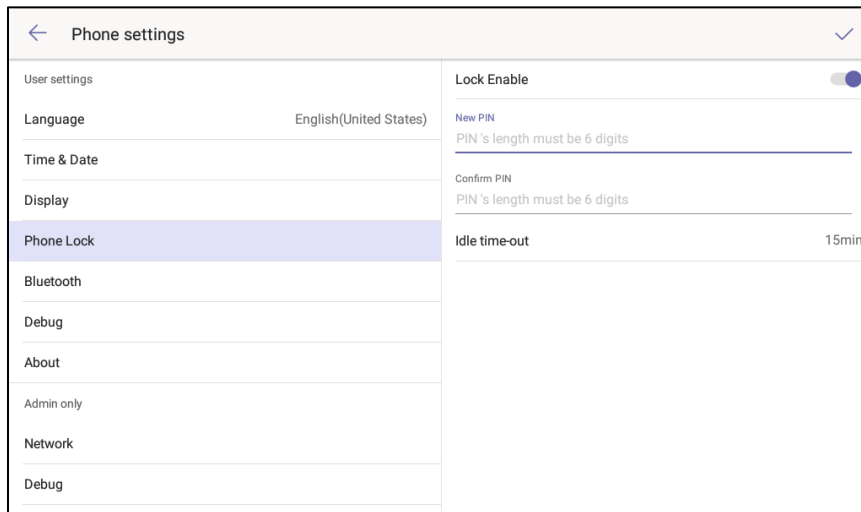
The screen saver wait time and background can be set from the **Screen Saver** section of the **Display** settings.

- **Screensaver Waiting Time:** Touch and drag up or down to specify the amount of time before the screen saver activates. Tap **OK** when done or tap **CANCEL** to cancel.
- **Screensaver Background:** Touch and drag up or down to select the screensaver to use. Tap **OK** when done or tap **CANCEL** to cancel.

Phone Lock

Tap **Phone Lock** to configure the phone's lock feature. Settings are displayed on the right side of the screen.

Phone Lock



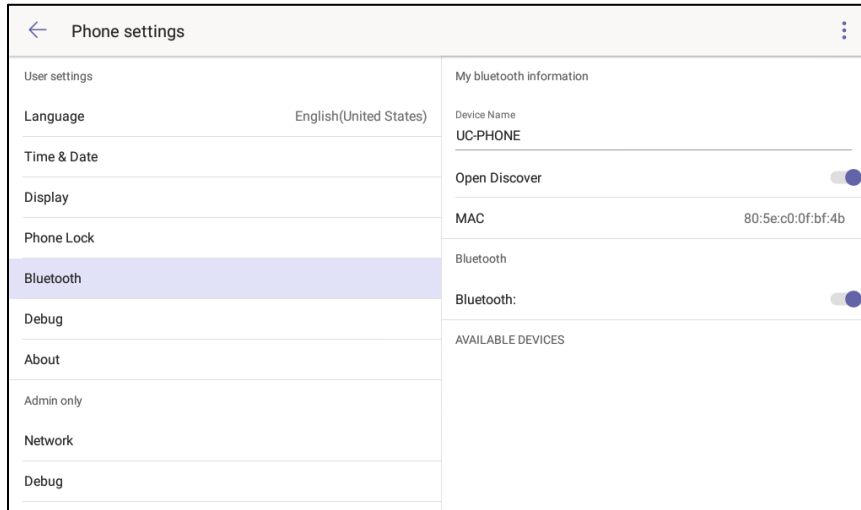
To enable and configure the phone lock feature, move the **Lock Enable** switch to the right and configure the lock. To disable the lock, move the **Lock Enable** switch to the left.

1. In the **New PIN** field, enter a six digit PIN.
2. In the **Confirm PIN** field, enter the six digit pin again.
3. Touch and drag up or down the **Idle time-out** field to select the time of inactivity before the phone locks.

Bluetooth®

The phone can connect with a compatible Bluetooth headset for wireless operation. Tap **Bluetooth** to configure the phone's Bluetooth feature. Settings are displayed on the right side of the screen.

Bluetooth



To enable and configure the Bluetooth feature, move the **Bluetooth** switch to the right. To disable the Bluetooth feature, move the **Bluetooth** switch to the left.

When enabled, a list of available Bluetooth devices that are in pairing mode are displayed under **AVAILABLE DEVICES**. Tap the device that is to be connected.

NOTE: To avoid conflicts, only one phone and one Bluetooth device should be in pairing mode at a time.

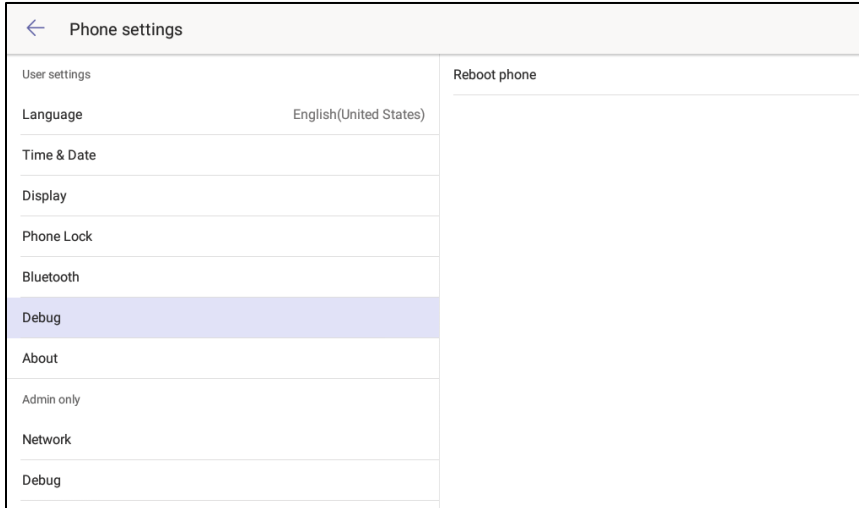
Once Bluetooth is enabled, the phone's device name can be set and the phone can be configured to be discoverable by other devices.

- **Device Name:** To change the device name, tap the device name and enter a new device name. Tap **Done** when finished.
- **Open Discover:** To allow the phone to be discovered by Bluetooth devices, move the **Open Discover** switch to the right.

Debug

Tap **Debug** to view controls for rebooting the phone. The reboot control appears on the right side of the screen.

Debug

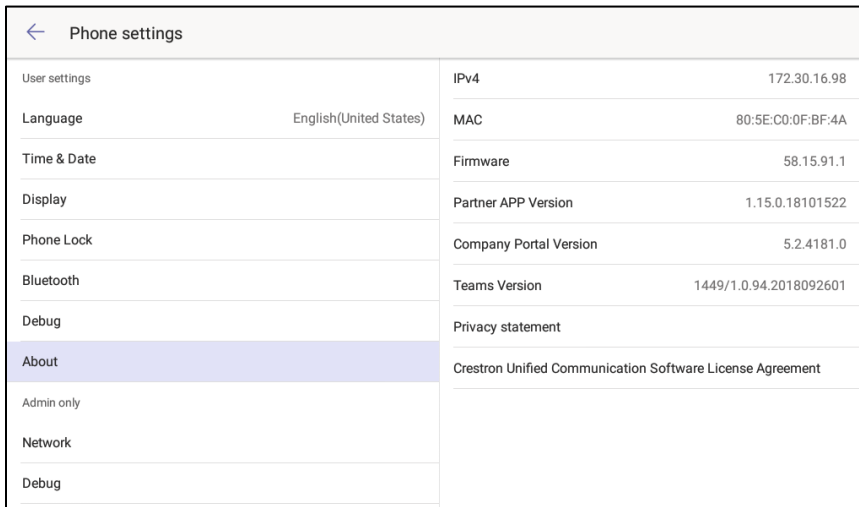


Tap **Reboot phone** to reboot the phone.

About

Tap **About** to view information about the phone's IP address, MAC address, firmware and software versions, the privacy statement, and the Crestron Unified Communication Software License Agreement.

About



The privacy statement and the Crestron® Unified Communications software license agreement are available for viewing.

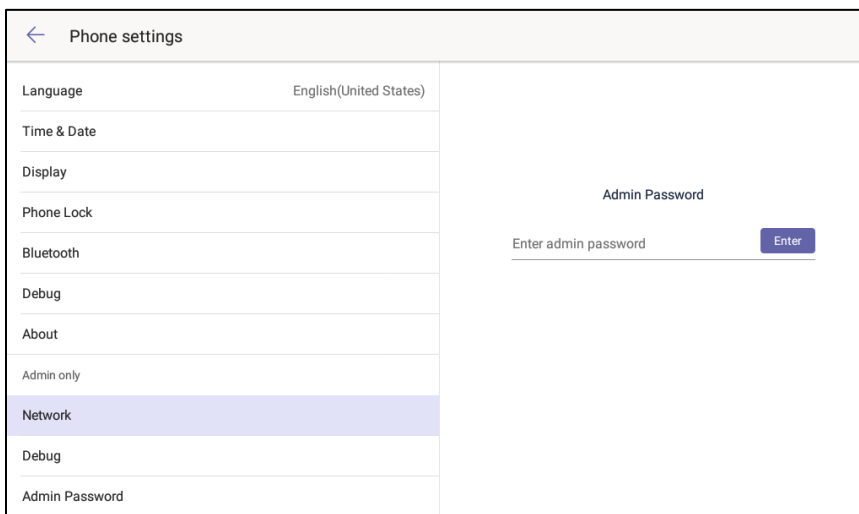
- Tap **Privacy statement** to view the privacy statement.
- Tap **Crestron Unified Communication Software License Agreement** to view the license agreement.

Network (Admin Only)

Tap **Network** to view and configure the phone's network settings.

Viewing and configuring the network settings requires the admin password. After tapping **Network**, the display prompts the user to enter the admin password.

Admin Password



Enter the admin password (default password = "admin") and tap **Enter**. The network settings are displayed on the right side of the screen.

NOTE: For information on changing the admin password, refer to "Admin Password (Admin Only)" on page 15.

Network

The screenshot shows the 'Phone settings' app with the 'Network' section selected. The settings are as follows:

Setting	Value
Language	English(United States)
Time & Date	
Display	
Phone Lock	
Bluetooth	
Debug	
About	
Admin only	
Network	
WAN Port	<input type="checkbox"/>
IP Mode	IPv4
IPv4 Type	DHCP
IPv4 Static DNS	<input type="checkbox"/>
IPv6 Type	DHCP
IPv6 Static DNS	<input type="checkbox"/>
VLAN	
WAN Port	<input type="checkbox"/>
VID	1
Priority	0
Debug	
Admin Password	

WAN Port

The **WAN Port** section determines the IP address format to use (IPv4, IPv6, or IPv4 and IPv6), the methods for obtaining an IP address (DHCP or Static), and the static IP address of the DNS servers.

- **IP Mode:** Touch and drag up or down to specify the IP addressing mode to use (IPv4, IPv6, or IPv4 and IPv6). Tap **OK** when done or tap **CANCEL** to cancel.
- **IPv4 Type:** Touch and tap the the method used for obtaining an IPv4 address (DHCP or **Static**). Tap **OK** when done or tap **CANCEL** to cancel.
- **IPv4 Static DNS:** Move the **IPv4 Static DNS** switch to the right to enter static IPv4 addresses for the primary and secondary DNS servers. When the switch is moved to the left, DHCP will be used to obtain addresses for the DSN servers.
- **IPv6 Type:** Touch and tap the the method used for obtaining an IPv6 address (DHCP or **Static**). Tap **OK** when done or tap **CANCEL** to cancel.
- **IPv6 Static DNS:** Move the **IPv6 Static DNS** switch to the right to enter static IPv6 addresses for the primary and secondary DNS servers. When the switch is moved to the left, DHCP will be used to obtain addresses for the DSN servers.

VLAN

The **VLAN** section configures the phone's Internet and PC ports as part of a VLAN.

- **WAN Port:** Move the **WAN Port** switch to the right to connect the Internet port and configure the port for operation. When the switch is moved to the left, the Internet port is no longer connected to the VLAN.

Once the Internet port is assigned to the VLAN, enter values for **VID** (1-4094) and **Priority** (1-7).

- **PC Port:** Move the **PC Port** switch to the right to connect the PC port and configure the port for operation. When the switch is moved to the left, the PC port is no longer connected to the VLAN.

Once the PC port is assigned to the VLAN, enter values for **VID** (1-4094) and **Priority** (0-7).

- **DHCP VLAN:** Move the **DHCP VLAN** switch to the right to enable and configure the DHCP VLAN discovery feature. When the switch is moved to the left, the DHCP VLAN discovery feature is disabled.

Once the PC port is assigned to the VLAN, enter values for **VID** (1-4094) and **Option** (1-255).

Web Server

The **Web Server** section enables and configures the web access types to be used (**HTTP** and **HTTPS**) by the phone.

- **HTTP Status:** Move the **HTTP Status** switch to the right to enable HTTP addressing. When the switch is moved to the left, HTTP addressing is no longer available.

Once the HTTP is enabled, enter the port number (1 through 65535) that should be used for HTTP communication in the **HTTP Port** field.

- **HTTPS Status:** Move the **HTTPS Status** switch to the right to enable HTTPS addressing. When the switch is moved to the left, HTTPS addressing is no longer available.

Once HTTPS is enabled, enter the port number (1 through 65535) that should be used for HTTPS communication in the **HTTPS Port** field.

802.1x Mode

The **802.1x** section enables and configures the phone to use 802.1x authentication.

Select an Authentication Method

To select a method of authentication:

- Tap the name of the authentication method to display a list of available authentication methods.
- Touch and drag up or down to scroll through the list of available methods. Refer to "Available Authentication Methods" below for details.
- Tap the method name to select, and then tap **OK**. The phone will prompt to reboot.
- Click **OK** to reboot the phone, or click **CANCEL** to continue configuration without rebooting.

Available Authentication Methods

- **EAP None:** When selected, authentication protocols are not used.
- **EAP-MD5:** When selected, MD5 authentication is used. MD5 is the base security requirement in the EAP standard and uses the username and password as the authentication credentials. Enter the identity and password in the Identity and MD5 Password fields.
- **EAP-TLS:** When selected, TLS authentication is used. Enter the identity and password in the Identity and MD5 Password fields. Other parameters are managed from the web interface. For details, refer to "802.1x" on page 23.
- **EAP-PEAP/MSCHAPv2:** When selected, PEAP/MSCHAPv2 authentication is used. Enter the identity and password in the Identity and MD5 Password fields. Other parameters are managed from the web interface. For details, refer to "802.1x" on page 23.
- **EAP-TTLS/EAP-MSCHAPv2:** When selected, TTLS/EAP-MSCHAPv2 authentication is used. Enter the identity and password in the Identity and MD5 Password fields. Other parameters are managed from the web interface. For details, refer to "802.1x" on page 23.
- **EAP-PEAP/GTC:** When selected, PEAP/GTC authentication is used. Enter the identity and password in the Identity and MD5 Password fields. Other parameters are managed from the web interface. For details, refer to "802.1x" on page 23.
- **EAP-TTLS/EAP-GTC:** When selected, TTLS/GTC authentication is used. Enter the identity and password in the Identity and MD5 Password fields. Other parameters are managed from the web interface. For details, refer to "802.1x" on page 23.
- **EAP-FAST:** When selected, FAST authentication is used. Enter the identity and password in the Identity and MD5 Password fields. Other parameters are managed from the web interface. For details, refer to "802.1x" on page 23.

LLDP

The **LLDP** section enables or disables the Link Layer Discovery Protocol (LLDP) feature on the phone and configures the interval (in seconds) for the Phone to send the LLDP request. To configure LLDP:

1. Move the **LLDP Status** switch to the right to enable LLDP. When the switch is moved to the left, LLDP is disabled.
2. Enter the interval (in seconds) for the phone to send the LLDP request in the **Packet Interval** field.

CDP

The **CDP** section enables or disables the Cisco Discovery Protocol (CDP) feature on the phone and configures the interval (in seconds) for the Phone to send the CDP request. To configure CDP:

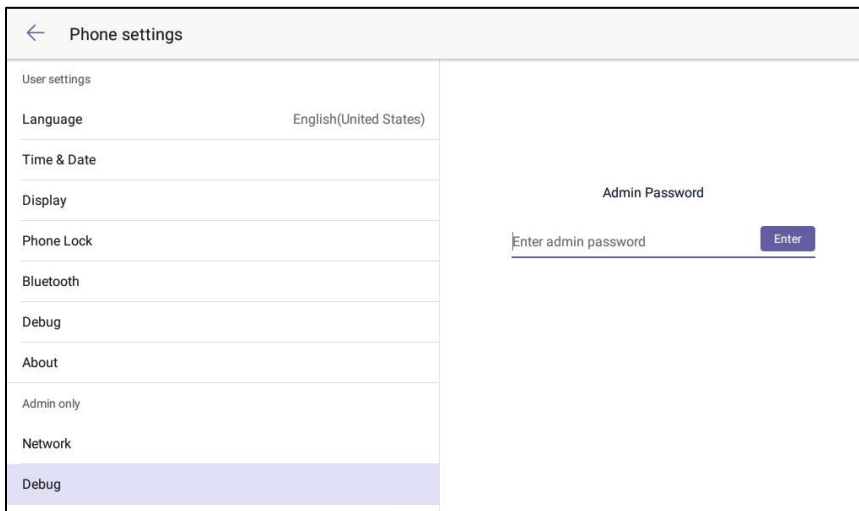
1. Move the **CDP Status** switch to the right to enable CDP. When the switch is moved to the left, CDP is disabled.
2. Enter the interval (in seconds) for the phone to send the CDP request in the **Packet Interval** field.

Debug (Admin Only)

Tap **Debug** to view and configure the phone's logging settings, reset the phone, and enable and/or disable screen captures.

Viewing and configuring the network settings requires the admin password. After tapping **Network**, the display prompts the user to enter the admin password.

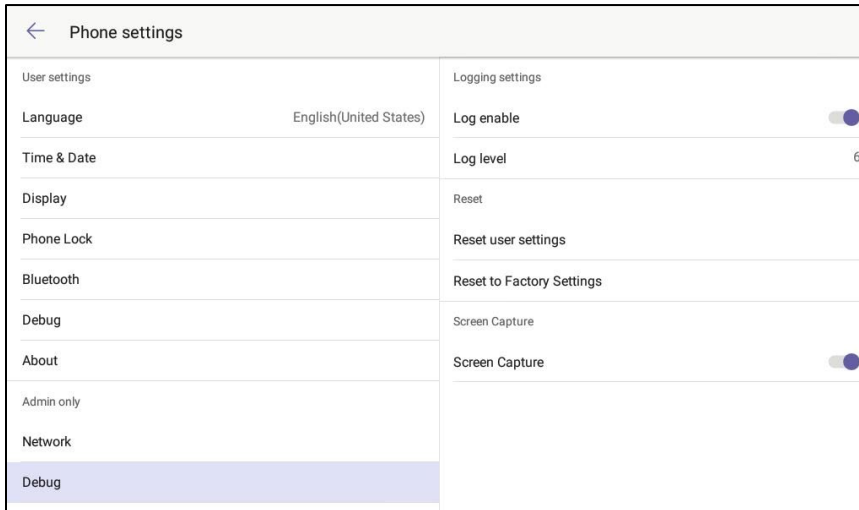
Admin Password



The screenshot shows the 'Phone settings' app interface. On the left is a navigation menu with categories: 'User settings' (Language: English(United States)), 'Time & Date', 'Display', 'Phone Lock', 'Bluetooth', 'Debug', 'About', 'Admin only', 'Network', and 'Debug' (highlighted). The main content area displays the 'Admin Password' prompt, which includes the text 'Enter admin password' and an 'Enter' button.

Enter the admin password (default password = "admin") and tap **Enter**. The debug settings are displayed on the right side of the screen.

Debug



Logging Settings

Logs are used for troubleshooting the phone. The **Logging settings** section enables and disables the logging function and configures the level of detail provided in logs created by the phone. To configure the phone's logging settings:

1. Move the **Log enable** switch to the right to enable logging. When the switch is moved to the left, logging is disabled.
2. Tap **Log level**, and then touch and drag up or down to scroll through the list of available methods.
3. Tap the log level to select it, and then tap **OK**. Otherwise, click **CANCEL** to cancel.

Reset

The **Reset** section allows you to reset phone settings to the factory default settings.

Reset User Settings

Use this function to reset user settings to the factory configuration.

1. Tap **Reset user settings**.
2. Tap **OK** to continue or **CANCEL** to cancel.

Reset to Factory Settings

Use this function to reset user and phone settings to the factory configuration.

1. Tap **Reset to Factory Settings**.

2. Tap **OK** to continue or **CANCEL** to cancel.

Screen Capture

The **Screen Capture** section allows you to use a web browser to view screen captures of the phone's display.

Move the **Screen Capture** switch to the right to enable the screen capture feature. When the switch is moved to the left, the screen capture feature is disabled.

Requirements

To take screen captures, the following is required:

- The IP address of the phone
- A PC with a web browser. The PC and phone should be on a commonly accessible network.
- The phone's administrative login credentials.

Procedure

Perform the following procedure to take screen captures.

1. Open the web browser and navigate to the **XXX.XXX.XXX.XXX/screencapture** where XXX.XXX.XXX.XXX is the IP address of the phone.
2. Enter the administrative login credentials. The browser will display a screen capture of whatever is on the phone's display.

Admin Password (Admin Only)

Tap **Admin Password** to change the admin password. Controls for changing the password are displayed on the right side of the screen.

Admin Password

Phone settings	
Language	English(United States)
Time & Date	
Display	
Phone Lock	
Bluetooth	
Debug	
About	
Admin only	
Network	
Debug	
Admin Password	

Old PWD

New PWD

Confirm PWD

1. Enter the old password in the **Old PWD** field.
2. Enter the new password in the **New PWD** field.
3. Confirm the new password in the **Confirm PWD** field and tap **DONE**.

Web Configuration

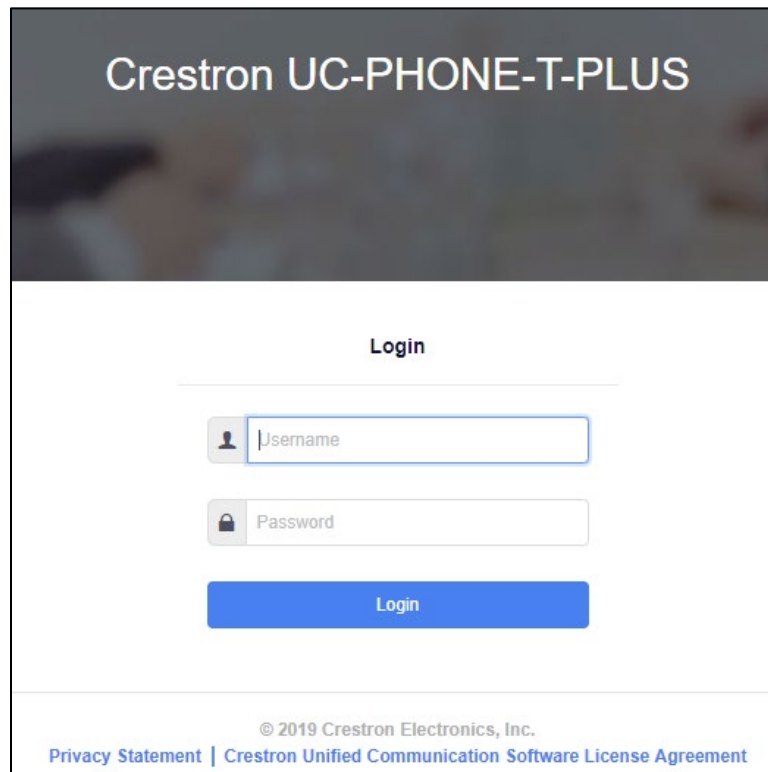
You can use web browser software on a computer to connect to the device and view web pages to configure the device.

Connect to the Device

To connect to the device, follow this procedure:

1. Obtain the device's IP address from the partner settings. For details, refer to "About" on page 8.
2. On the computer, open a web browser and navigate to the IP address of the device. The welcome screen is displayed.

Welcome Screen



Crestron UC-PHONE-T-PLUS

Login

Username

Password

Login

© 2019 Crestron Electronics, Inc.
[Privacy Statement](#) | [Crestron Unified Communication Software License Agreement](#)

3. Enter the default user name ("admin") and password ("admin").
4. Click **Sign In** to continue. The device's **Status** screen is displayed.

Status Screen

The screenshot shows the Crestron Status screen. On the left is a dark sidebar with a menu: Status (selected), Network, Features, Settings, and Security. The main content area is divided into sections: Version, Device Certificate, Network, IPv4, and Network Common. Each section has a title with a question mark icon and a table of details. A 'NOTE' box on the right explains the 'Version' and 'Network' sections.

Section	Parameter	Value
Version	Firmware Version	58.15.91.1
	Hardware Version	55.2.3.0.0.0.0
	Microsoft Teams Version	1449/1.0.94.2018092601
Device Certificate	Device Certificate	Factory Installed
Network	Internet Port	IPv4
IPv4	WAN Port Type	DHCP
	WAN IP Address	172.30.16.153
	Subnet Mask	255.255.255.0
	Gateway	172.30.16.1
	Primary DNS	192.168.200.133
	Secondary DNS	192.168.200.134
Network Common	MAC Address	80:5E:C0:0F:BF:4A
	Bluetooth MAC	80:5E:C0:0F:BF:4B
	WAN Port Status	100Mbps Full Duplex
	PC Port Status	Link Down
	Device Type	Bridge
	Uptime	0 days 00:43
	Current Time	26 Jan 2019 01:27:02 AM

NOTE
Version
It shows the firmware version, hardware version and Teams version.
Network
It shows the network settings of Internet (WAN) port.
[Click here to get more product documents.](#)

The **Status** screen displays information about the device and allows configuration of the device's operating parameters:

- Status contains general information about the device and network information. Click **Network** to view network information.
- Network configures the device for operation in a network environment.
- Features configures the phone lock, Bluetooth, and LEF operation.
- Settings configures the backlight and screensaver, the date and time, auto provisioning, diagnostic information, tones, and power saving features. The settings session is also used to upgrade firmware.
- Security configures the phone passwords (user and admin) as well as how certificates are used.

Tap ▼ to view submenus for each section. Tap ▲ to hide the submenus.

Log Out from the Device

To log out from the device and return to the welcome screen, click **Logout**.

Status

Click **Status** to view information about the device. The Status screen displays information about the operating software, security certificate, network operation, Ethernet information, and other network information.

Network

The **Network** menu contains sections for basic network configuration, configuring the device's PC port, and advanced network configuration. Click a section name to configure parameters.

Basic

Click **Basic** to configure the basic network parameters such as IP address, subnet mask, default gateway, and DNS servers.

Network - Basic

The screenshot shows the 'Network - Basic' configuration page. On the left is a navigation menu with 'Basic' selected. The main content area is divided into three sections: 'Internet Port', 'IPv4 Config', and 'IPv6 Config'. In the 'Internet Port' section, the 'Mode(IPv4/IPv6)' dropdown is set to 'IPv4'. The 'IPv4 Config' section has 'Configuration Type' set to 'DHCP'. The 'IPv6 Config' section has 'Configuration Type' set to 'DHCP'. A 'NOTE' box on the right explains DHCP and IPv6 support. At the bottom are 'Confirm' and 'Cancel' buttons.

Section	Parameter	Value
Internet Port	Mode(IPv4/IPv6)	IPv4
	Configuration Type	DHCP
IPv4 Config	Configuration Type	DHCP
	IP Address	
	Subnet Mask	
	Default Gateway	
	Static DNS	OFF
	Primary DNS	
	Secondary DNS	
IPv6 Config	Configuration Type	DHCP
	IP Address	
	IPv6 Prefix(0-128)	64
	Default Gateway	
	Static IPv6 DNS	OFF
	Primary DNS	
	Secondary DNS	

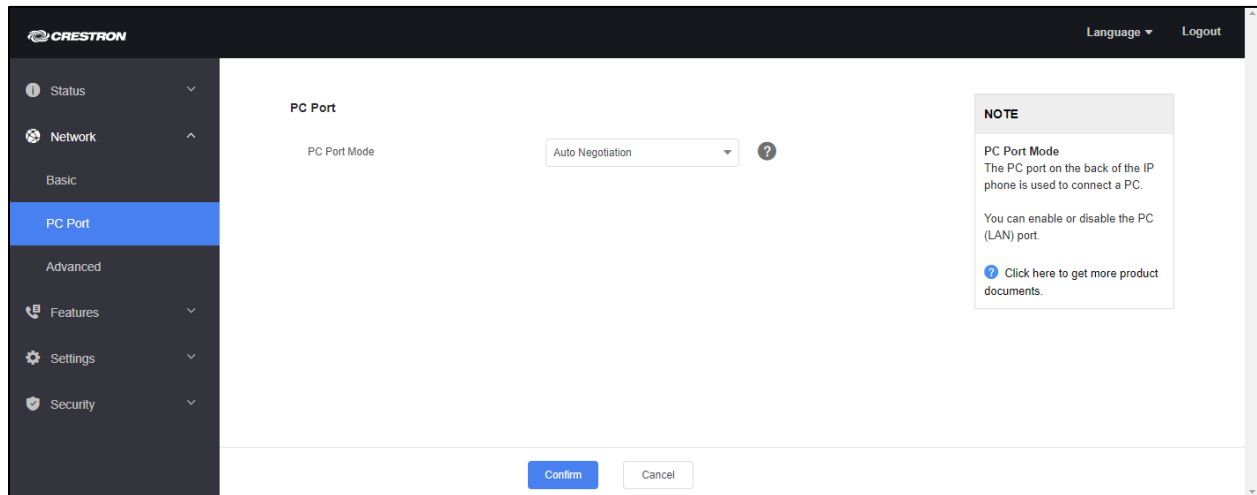
1. Select the mode of operation for the Internet port (IPv4, IPv6, or IPv4 & IPv6) from the **Mode (IPv4/IPv6)** drop-down list.

- Depending on the mode chosen, configure the IPv4, IPv6, or IPV4 and IPv6 parameters.
 - Configuration Type:** Select **DHCP** to obtain the IP address, subnet mask, default gateway, and DNS server from a DHCP server. Otherwise, select **Static IP** to manually enter values.
 - Static DNS:** Set to **ON** to specify static addresses for the primary and secondary DNS servers when DHCP is enabled. Otherwise, set to **OFF** to obtain DNS server addresses from the DHCP server.
- Click **Confirm** to save settings or **Cancel** to cancel.

PC Port

The PC port on the back of the Phone can be used to connect a PC for a connection to the LAN. You can enable or disable the port.

Network – PC Port



- Click **PC Port** to configure the PC port.
- Select the mode of operation from the **PC Port Mode** drop-down list.
 - Select **Auto Negotiation** from the drop-down list to provide a LAN connection to a PC connected to the PC port.
 - Select **Disabled** from the drop-down list to disable the PC port.
- Click **Confirm** to save settings or **Cancel** to cancel.

Advanced

The **Advanced** section configures the Link Layer Discovery Protocol (LLDP), the Cisco Discover Protocol (CDP), the VLAN, port transmission methods, web server functionality, 802.1x authentication, data packet spanning, and Stateless Address Autoconfiguration (SLAAC). Click **Advanced** to configure these parameters. The **Advanced** section is displayed.

When all settings are made, click **Confirm** to save settings or **Cancel** to cancel.

Network – Advanced

CRESTRON
Language ▾ Logout

- Status ▾
- Network ▾
- Basic
- PC Port
- Advanced
- Features ▾
- Settings ▾
- Security ▾

NOTE

Network advance

[Click here to get more product documents.](#)

LLDP ?

Active

Packet Interval (1-3600s)

CDP ?

Active

Packet Interval (1-3600s)

VLAN ?

WAN Port

Active

VID (1-4094)

Priority

PC Port

Active

VID (1-4094)

Priority

DHCP VLAN

Active

Option (1-255)

Port Link ?

WAN Port Link

PC Port Link

Web Server ?

HTTP

HTTP Port (1-65535)

HTTPS

HTTPS Port (1-65535)

802.1x ?

802.1x Mode

Provisioning Mode

Anonymous Identity

Identity

MD5 Password

CA Certificates

Device Certificates

Span To PC ?

Span To PC Port

ICMPv6 Status ?

Active

LLDP

The **LLDP** section enables or disables the Link Layer Discovery Protocol (LLDP) feature on the phone and configures the interval (in seconds) for the Phone to send the LLDP request. To configure LLDP:

1. Move the **Active** switch to **ON** enable LLDP. When the switch is moved to **OFF**, LLDP is disabled.
2. Enter the interval (in seconds) for the phone to send the LLDP request in the **Packet Interval** field.

CDP

The **CDP** section enables or disables the Cisco Discovery Protocol (CDP) feature on the phone and configures the interval (in seconds) for the Phone to send the CDP request. To configure CDP:

1. Move the **Active** switch to **ON** to enable CDP. When the switch is moved to Move the **Active** switch to **ON**, CDP is disabled.
2. Enter the interval (in seconds) for the phone to send the CDP request in the **Packet Interval** field.

VLAN

The **VLAN** section configures the phone's Internet and PC ports as part of a VLAN.

- **WAN Port:** Move the **Active** switch to **ON** to connect the Internet port and configure the port for operation. When the switch is set to **OFF**, the Internet port is no longer connected to the VLAN.

Once the Internet port is assigned to the VLAN, enter a value for **VID** (1-4094) and select a priority level (0-7) from the **Priority** drop-down list.

- **PC Port:** Move the **PC Port** switch to **ON** to connect the PC port and configure the port for operation. When the switch is set to **OFF**, the PC port is no longer connected to the VLAN.

Once the PC port is assigned to the VLAN, enter a value for **VID** (1-4094) and select a priority level (0-7) from the **Priority** drop-down list.

- **DHCP VLAN:** Move the **Active** switch to **ON** to enable and configure the DHCP VLAN discovery feature. When the switch is set to **OFF**, the DHCP VLAN discovery feature is disabled.

Once the PC port is assigned to the VLAN, enter values for **VID** (1-4094) and **Option** (1-255).

Port Link

The **Port Link** section configures the transmission method of the Internet and PC ports.

- Select the transmission method of the Internet port from the WAN Port Link drop-down list.

- Select the transmission method of the PC port from the PC Port Link drop-down list.

Web Server

The **Web Server** section configures the phone's web server functions.

- **HTTP:** Set to **ON** to enable an http connection to the phone. Set to **OFF** to disable an http connection to the phone.
- **HTTP Port (1-65535):** Enter the port number the phone uses for http communications.
- **HTTPS:** Set to **ON** to enable an https connection to the phone. Set to **OFF** to disable an https connection to the phone.
- **HTTPS Port (1-65535):** Enter the port number the phone uses for https communications.

NOTE: If **HTTP** and **HTTPS** are set to **OFF**, the web configuration tool is disabled when the phone reboots. All configuration may be done through "Phone Settings" on page 2.

802.1x

The **802.1x** section enables and configures the phone to use 802.1x authentication. Select the authentication mode from the **802.1x Mode** drop-down list.

- **EAP None:** When selected, authentication protocols are not used.
- **EAP-MD5:** When selected, MD5 authentication is used. MD5 is the base security requirement in the EAP standard and uses username and password as the authentication credentials. Enter the identity and password in the **Identity** and **MD5 Password** fields.
- **EAP-TLS:** When selected, TLS authentication is used.
 - a. Enter the identity and password in the **Identity** and **MD5 Password** fields.
 - b. Upload a CA certificate and/or a device certificate. To upload a CA certificate, click inside the **CA Certificates** field, select a certificate file, and click **Upload**. To upload a device certificate, click inside the **Device Certificates** field, select a certificate file, and click **Upload**.
- **EAP-PEAP/MSCHAPv2:** When selected, PEAP/MSCHAPv2 authentication is used.
 - a. Enter the identity and password in the **Identity** and **MD5 Password** fields.
 - b. Upload a CA certificate. To upload a CA certificate, click inside the **CA Certificates** field, select a certificate file, and click **Upload**.
- **EAP-TTLS/EAP-MSCHAPv2:** When selected, PEAP/MSCHAPv2 authentication is used.
 - a. Enter the identity and password in the **Identity** and **MD5 Password** fields.

- b. Upload a CA certificate. To upload a CA certificate, click inside the **CA Certificates** field, select a certificate file, and click **Upload**.
- **EAP-PEAP/GTC:** When selected, PEAP/GTC authentication is used.
 - a. Enter the identity and password in the **Identity** and **MD5 Password** fields.
 - b. Upload a CA certificate. To upload a CA certificate, click inside the **CA Certificates** field, select a certificate file, and click **Upload**.
- **EAP-TTLS/EAP-GTC:** When selected, TTLS/GTC authentication is used.
 - a. Enter the identity and password in the **Identity** and **MD5 Password** fields.
 - b. Upload a CA certificate. To upload a CA certificate, click inside the **CA Certificates** field, select a certificate file, and click **Upload**.
- **EAP-FAST:** When selected, FAST authentication is used. Enter the identity and password in the **Identity** and **MD5 Password** fields.

Span to PC

The **Span to PC** sets the phone to span data packets received from the Internet port to the PC port.

To span data packets from the Internet port to the PC port, set **Span to PC Port** to **ON**. To turn off spanning, set **Span to PC Port** to **OFF**.

ICMPv6 Status

The phone can obtain IPv6 network settings using the Stateless Address Autoconfiguration (SLAAC) method.

To use SLAAC to obtain network settings, set **Active** to **ON**. Otherwise, set **Active** to **OFF**.

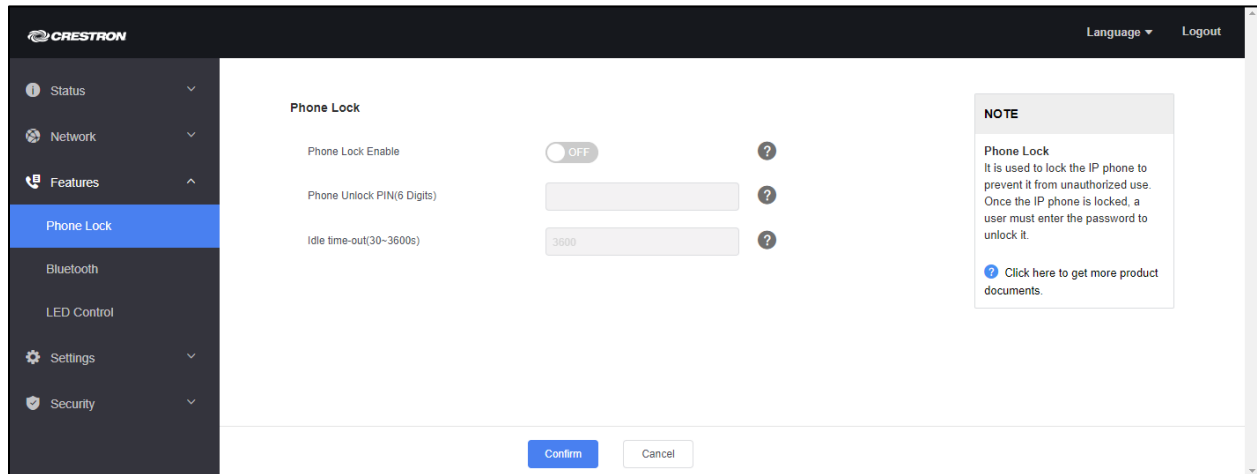
Features

The **Features** menu contains sections for configuring the lock, Bluetooth, and LED operation. Click a section name to configure parameters.

Phone Lock

The phone lock function locks the phone to prevent it from unauthorized use. When the phone is locked, a user must enter the password to unlock it. The **Phone Lock** section enables the lock, sets the unlock code, and sets the amount of idle time before locking the phone. Click **Phone Lock** to configure these parameters. The **Phone Lock** section is displayed.

Features – Phone Lock

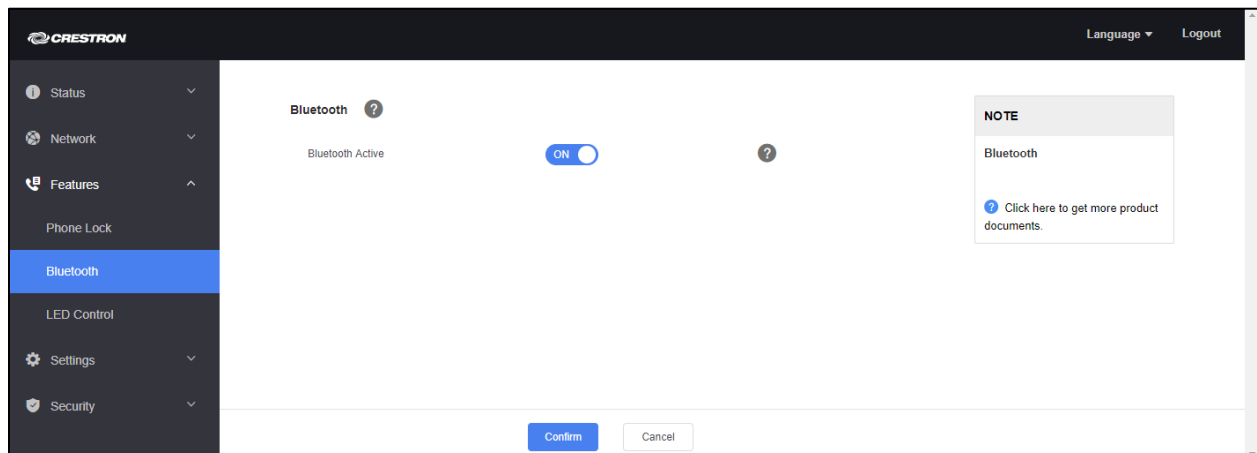


1. Set **Phone Lock Enable** to **ON** to use the phone lock feature. To turn off the phone lock feature, set **Phone Lock Enable** to **OFF**.
2. Enter a six digit lock code in the **Phone Unlock PIN (6 Digits)** field.
3. Enter the amount of idle time (in seconds) to elapse before the phone locks in the **Idle time-out (30-3600s)** field.
4. Click **Confirm** to save settings or **Cancel** to cancel.

Bluetooth

The phone can connect with a compatible Bluetooth headset for wireless operation. Click **Bluetooth** to view controls for enabling or disabling Bluetooth. The **Bluetooth** section is displayed.

Features – Bluetooth



1. Set **Bluetooth Active** to **ON** to enable Bluetooth communications between the phone and a paired device. To turn off Bluetooth communication, set **Bluetooth Active** to **OFF**.

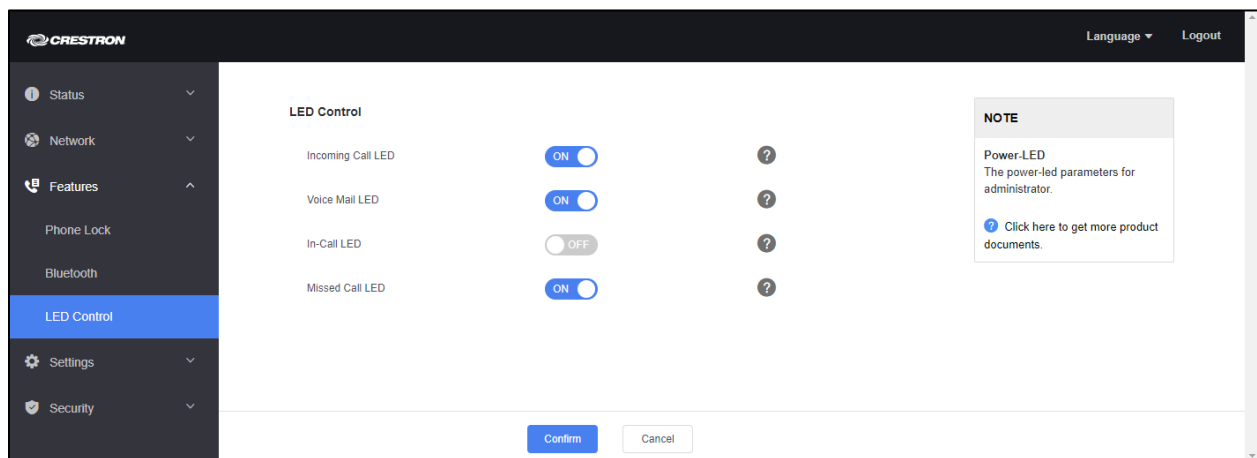
NOTE: To pair the phone with a Bluetooth device, refer to "Bluetooth®" on page 7.

2. Click **Confirm** to save settings or **Cancel** to cancel.

LED Control

The LED on the top right of the display can be configured to indicate certain conditions. Click **LED Control** to view controls for configuring LED behavior. The **LED Control** section is displayed.

Features – LED Control



- Set **Incoming Call LED** to **ON** to have the LED flash when the phone receives a call. To turn off LED notification for incoming calls, set **Incoming Call LED** to **OFF**.
- Set **Voice Mail LED** to **ON** to have the LED flash when the phone receives a voice mail message or text message. To turn off LED notification for incoming voice mail messages and text messages, set **Voice Mail LED** to **OFF**.
- Set **In-Call LED** to **ON** to have the LED light when the phone is in use. To turn off LED notification, set **In-Call LED** to **OFF**.
- Set **Missed Call LED** to **ON** to have the LED light when a call is missed. To turn off LED notification for missed calls, set **Missed Call LED** to **OFF**.

Click **Confirm** to save settings or **Cancel** to cancel.

Settings

The **Settings** menu contains sections for configuring the screen, setting the time and date, managing firmware, provisioning the phone, configuring data output, configuring the dial tone, and configuring power saving options. Click a section name to configure parameters.

Preference

The **Preference** section controls the display's backlight and the screensaver to show when the phone is idle. Click **Preference** to display the **Preference** section.

Settings – Preference

The screenshot shows the Crestron Settings application interface. On the left is a dark sidebar menu with the following items: Status, Network, Features, Settings (expanded), Preference (highlighted in blue), Time&Date, Upgrade, Auto Provision, Configuration, Tones, Power Saving, and Security. The main content area is titled 'Settings – Preference' and contains two sections: 'Backlight' and 'Screen saver'. The 'Backlight' section has two dropdown menus: 'Brightness' (set to 8) and 'Backlight Time(seconds)' (set to 'Always On'). The 'Screen saver' section has two dropdown menus: 'Screensaver Wait Time' (set to '30 s') and 'Screensaver Background' (set to '07.png'). Each dropdown menu has a question mark icon to its right. On the right side of the main area, there is a 'NOTE' box with the following text: 'NOTE', 'Backlight: Specify the brightness of the LCD screen.', 'Screen saver: Specify the screen saver of the LCD screen.', and a link: 'Click here to get more product documents.' At the bottom of the main area, there are two buttons: 'Confirm' (blue) and 'Cancel' (white).

Backlight

Configure the backlight for use.

1. Select a brightness level from the **Brightness** drop-down list.
2. Select a duration for the backlight from the **Backlight Time (seconds)** drop-down list.
3. Click **Confirm** to save settings or **Cancel** to cancel.

Screen saver

Configure the screensaver for use.

1. Select the wait time from the **Screensaver Wait Time** drop-down list.
2. Select a screensaver file from the **Screensaver Background** drop-down list.
3. Click **Confirm** to save settings or **Cancel** to cancel.

Time & Date

The **Time&Date** section controls the clock that is displayed on the phone's idle screen. Click **Time&Date** to display the **Time&Date** section.

Settings – Time & Date

The screenshot displays the 'Time&Date' settings page in the Crestron interface. The left sidebar shows navigation options: Status, Network, Features, Settings (expanded), Preference, Time&Date (selected), Upgrade, Auto Provision, Configuration, Tones, Power Saving, and Security. The main content area is titled 'Time&Date' and contains the following settings:

- DHCP Time:** ON (toggle)
- Manual Time:** OFF (toggle)
- NTP By DHCP Priority:** High (dropdown)
- Primary Server:** cn.pool.ntp.org (text input)
- Secondary Server:** pool.ntp.org (text input)
- Update Interval (15-86400s):** 1000 (text input)
- Time Zone:** -8 China, Singapore, Australia... (dropdown)
- Daylight Saving Time:** Disabled, Enabled, Automatic (radio buttons)
- Location:** None (dropdown)
- Fixed Type:** DST By Date, DST By Week (radio buttons)
- Start Date:** Month, Day, Hour (text inputs)
- End Date:** Month, Day, Hour (text inputs)
- Offset(minutes):** (text input)
- Time Format:** Hour 12 (dropdown)
- Date Format:** DD MMM YYYY (dropdown)

At the bottom of the settings area are 'Confirm' and 'Cancel' buttons. On the right side, there is a 'NOTE' section with the following text:

NOTE

Time and Date
It displays on the idle screen of IP phones.

Time Zone
A time zone is a region on Earth that has a uniform standard time. It is convenient for areas in close commercial or other communication to keep the same time.

NTP Server
The IP phones synchronize the time and date automatically from the NTP time server by default.

Daylight Saving Time
It is the practice of temporary advancing clocks during the summer time so that evenings have more daylight and mornings have less. Typically, clocks are adjusted forward one hour at the start of spring and backward in autumn.

[Click here to get more product documents.](#)

Adjust the following settings as necessary.

- **DHCP Time:** To have the phone update the time with the offset time offered by the DHCP server, set **DHCP Time** to **ON**. Otherwise, set to **OFF**.
- **Manual Time:** To manually set the date and time, set **Manual Time** to **ON** and enter the date, time, time format, and date format.
- **NTP By DHCP Priority:** To set the phone to use the DHCP setting over a manual setting, select **High** from the drop-down list. Otherwise, select **Low** from the drop-down list.
- **Primary Server** and **Secondary Server:** Enter the hostname or IP address of the primary and secondary time servers.
- **Update Interval (15-86400s):** Enter the interval (in seconds) to update the date and time from the NTP server.

- **Time Zone:** Set the time zone (relative to GMT) of the phone's location from the drop-down list.
- **Daylight Savings Time:** Select a Daylight Savings Time operating mode.
 - **Disabled:** Daylight Savings Time is not used.
 - **Enabled:** Daylight Savings Time is used with manual entry of start and end dates. Specify the start and end dates (month and date), hours, and offset (minutes) in the Start Date Month, Day, Hour fields, End Date Month, Day, Hour fields, and Offset(minutes) field.
 - **Automatic:** Daylight Savings Time is used automatically based on location. The location is selected from the Location drop-down list.
- **Time Format:** Select the format to use for displaying time from the **Time Format** drop-down list.

Click **Confirm** to save settings or **Cancel** to cancel.

Upgrade

The **Upgrade** section provides information about the device's firmware and provides controls for resetting user settings, restoring factory default settings, rebooting the device, and upgrading the device's firmware. Click **Upgrade** to display the **Upgrade** section.

Settings – Upgrade

The screenshot displays the 'Upgrade' section of the Crestron settings interface. On the left, a navigation menu lists various settings categories, with 'Upgrade' highlighted. The main content area is titled 'Version' and lists the following information:

Item	Version
Firmware Version	58.15.91.6
Hardware Version	55.2.3.0.0.0.0
Company Portal Version	5.2.4185.0
Microsoft Teams Version	1449/1.0.94.2018121201

Below the version information, there are three sections with action buttons:

- Reset:** Includes 'Reset User Settings' and 'Restore Factory Defaults' buttons.
- Reboot:** Includes a 'Reboot' button.
- Upgrade:** Includes an 'Upgrade Firmware' section with a file selection area (currently showing 'No selected file(.rom)') and an 'Upload' button.

On the right side, a 'NOTE' box provides additional information:

- Reset to Factory Setting:** Resets the IP phone to factory configurations.
- Reboot:** Reboots the IP phone.
- Upgrading Firmware:** Upgrades firmware manually. A link is provided to 'Click here to get more product documents'.

Version

The **Version** section provides information about the device's firmware and other software.

Reset

The **Reset** section provides controls for resetting the user settings and restoring the factory default settings.

- Click **Reset User Settings** to reset all the user settings.
- Click **Restore** to restore the device to the factory default settings.

Reboot

The **Reboot** section provides a control for rebooting the device. Click **Reboot** to reboot the device.

Upgrade

The **Upgrade** section provides controls for updating the device firmware. To upload new firmware, click inside the empty field, select a firmware file, and click **Upload**.

Auto Provision

The **Auto Provision** section provides controls for configuring auto provision operations.

Settings – Auto Provision

The screenshot displays the 'Auto Provision' configuration page in the Crestron web interface. The left sidebar shows the navigation menu with 'Auto Provision' selected. The main content area is titled 'Auto Provision' and contains the following settings:

- DHCP Active: ON
- Custom Option:
- DHCP Option Value:
- Server URL:
- Username:
- Password:
- Attempt Expired Time(s):
- Common AES Key:
- MAC-Oriented AES Key:
- Power On: ON
- Repeatedly: OFF
- Interval(Minutes):
- Weekly: OFF
- Time: : :
- Day of Week: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
- Auto Provision Now:
- XIO Cloud Connection: ON

A 'NOTE' box on the right side of the page contains the following text:

NOTE
Auto Provision
Begin time should be earlier than end time!

When the IP phone is triggered to perform auto provisioning, it will request to download the configuration files from the provisioning server. During the auto provisioning, the IP phone will download and update configuration files to the phone flash.

[Click here to get more product documents.](#)

At the bottom of the page, there are 'Confirm' and 'Cancel' buttons.

Adjust the following settings as necessary.

- **DHCP Active:** To have the phone obtain the provisioning server address by detecting DHCP options, set **DHCP Active** to **ON**. Otherwise, set to **OFF**.
- **Custom Option:** Configures the custom DHCP option for requesting a provisioning server address. Values must be integers from 128 to 254. Multiple DHCP options are separated by commas.

NOTE: **DHCP Active** must be set to **ON**.

- **DHCP Option Value:** Configures the value (vendor name of the device) of DHCP option 60.
- **Server URL:** If static addressing is used, enter the access URL of the provisioning server.
- **Username:** Enter the user name for accessing the provisioning server. Maximum length is 32 characters.
- **Password:** Enter the password for accessing the provisioning server. Maximum length is 32 characters.
- **Attempt Expired Time(s):** Configures the time (in seconds) to wait after a file transfer fails before retrying the transfer via auto provisioning. Integer values from 1 to 300 are allowed.
- **Common AES Key:** Configures the plaintext AES key for decrypting the Common CFG file.
- **MAC-Oriented AES Key:** configures the plaintext AES key for decrypting the MAC-Oriented CFG file.
- **Power On:** Configures whether the phone should perform auto provisioning when powered on. If set to **ON**, auto provisioning will be performed when the phone turns on. If set **OFF**, auto provisioning will not be performed when the phone turns on.
- **Repeatedly:** Set to **ON** to turn on the repeat auto provisioning feature. Set to **OFF** to turn off the repeat auto provisioning feature.
- **Interval (Minutes):** Configures the interval (in minutes) for the phone to perform the auto provisioning repeatedly. Integer values from 1 to 43200 are allowed

NOTE: **Repeatedly** must be set to **ON**.

- **Weekly:** Set to **ON** to turn on the weekly auto provisioning feature on a weekly basis. Set to **OFF** to turn off the weekly auto provisioning feature.
- **Time:** Configures the begin time and end time (hour and minute) of the day when the phone should perform the weekly auto provisioning process

NOTE: **Weekly** must be set to **ON**.

- **Day of Week:** Select the day(s) of the week when the auto provisioning process will occur.

NOTE: Weekly must be set to ON.

- Click **Auto Provision Now** to manually start the auto provision process.
- **XiO Cloud Connection:** Set to **ON** to enable the phone to connect with Crestron XiO Cloud service. Set to **OFF** to disable the phone's connection to Crestron XiO Cloud service. For more information, refer to "Crestron XiO Cloud Service" on page 39.

Click **Confirm** to save settings or **Cancel** to cancel.

Configuration

The **Configuration** section is used to import and export configuration files (.bin and .cfg), capture packets for troubleshooting, and configure logging operations for troubleshooting.

Settings – Configuration

The screenshot shows the Crestron Configuration settings page. The left sidebar contains navigation options: Status, Network, Features, Settings (selected), Preference, Time&Date, Upgrade, Auto Provision, Configuration (selected), Tones, Power Saving, and Security. The main content area is titled 'Configuration' and includes the following sections:

- Configuration:** Import Configuration (No selected file(.bin) / Import), Export Configuration (Export).
- CFG Configuration:** Import CFG Configuration File (No selected file(.cfg) / Import), Export CFG Configuration File (All Settings / Export).
- Pcap:** Pcap Type (Enhanced), Pcap Feature (Start / Stop).
- Local Log:** Enable Local Log (ON), Local Log Level (2), Max Log File Size (2048-20480KB) (20480), Export Local Log (Export).
- Syslog:** Enable Syslog (OFF), Syslog Server (/ Port 514), Syslog Transport Type (UDP), Syslog Level (6), Syslog Facility (Kernel Messages), Syslog Prepend MAC (OFF).
- Export All Diagnostic Files:** Start / Stop / Export.

A **NOTE** box on the right states: "Configuration IP phones can provide feedback in a variety of forms such as log files, packets, status indicators and so on, which can help an administrator more easily find the system problem and fix it." It lists "- Log Files", "- Capturing Packets", and "- Configuration File (*.cfg*.bin)". It also notes: "The *.bin file you export may contain some your personal data, including contacts, history records, web-side login information, etc. If you do not want to export this information, please clear them first on the phone." and includes a link: "Click here to get more product documents."

At the bottom of the page, there are 'Confirm' and 'Cancel' buttons. A description box for the 'Export All Diagnostic Files' section reads: "Description: 1.Start the diagnosis problem. Stop the diagnosis problem. Export all diagnostic files."

Configuration

The configuration section can import and export .bin configuration files.

- To import a .bin configuration file, click inside the empty field, select a .bin file, and click **Import**.
- To export a .bin configuration file, click **Export**.

NOTE: .bin files may contain personal data, including contacts, history records, web-side login information, etc. If you do not want to export this information, clear them on the phone before exporting.

CFG Configuration

The CFG Configuration section can import and export .cfg configuration files.

- To import a .cfg configuration file, click inside the empty field, select a .cfg file, and click **Import**.
- To export a .cfg configuration file, select the settings to export from the drop-down list, and click **Export**.

Pcap

The phone can be set to capture packets for troubleshooting. To capture packets, select the type of packet to capture from the **Pcap Type** drop-down list.

- **Normal:** After clicking **Start**, the capture file is saved on the phone. Click **Stop** and export to export the capture file to the PC.
- **Enhanced** After clicking **Start**, the capture file is saved directly to the PC and the files is continuously saved while capturing packets.

Local Log

The **Local Log** section configures the phone to record log files locally.

- **Enable Local Log:** To enable local logging, set **Enable Local Log** to **ON**. To turn off local logging, set **Enable Local Log** to **OFF**.
- **Local Log Level:** Sets the detail level of local log information to be reported to the MAC-sys.log file. Select a detail level from the drop-down list.
 - **0:** system is unusable
 - **1:** action must be taken immediately
 - **2:** critical condition
 - **3:** error conditions
 - **4:** warning conditions
 - **5:** normal but significant condition

- **6:** informational
- **Max Log File Size (2048-20480KB):** Specify the maximum size (in KB) of the log files (MAC-boot.log and MAC-sys.log) to be stored on the phone.
- **Export Local Log:** Click Export to export the local log files sys.log or boot.log.

Syslog

The **Syslog** section configures the phone to upload log messages to the syslog server in real time.

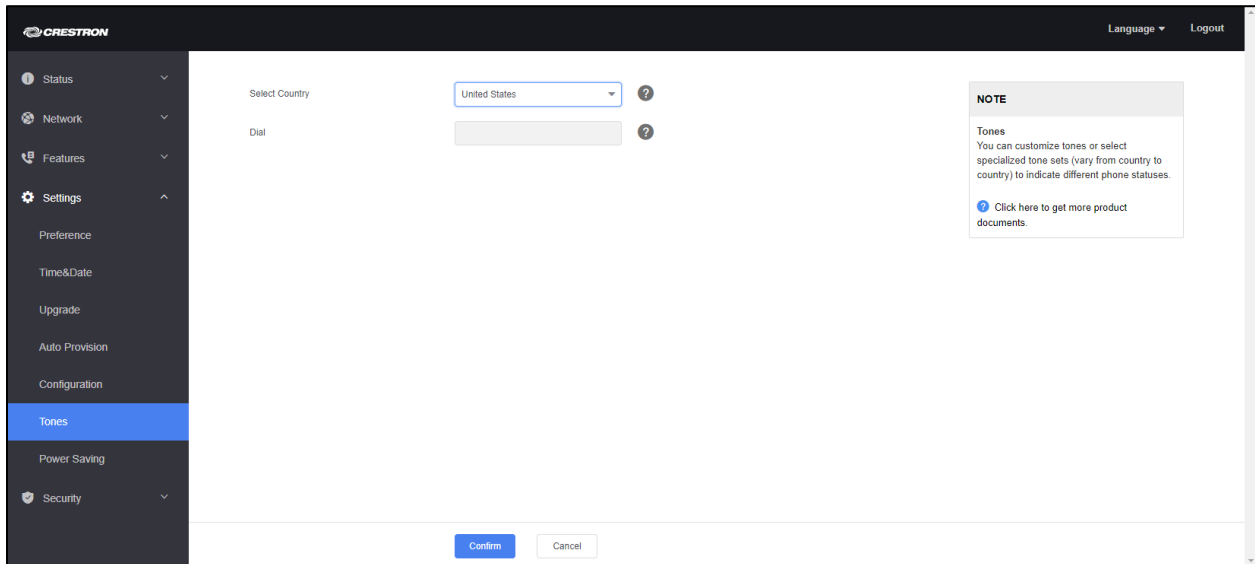
- **Enable Syslog:** To enable the uploading of log messages to the syslog server, set **Enable Syslog** to **ON**. To turn off logging, set **Enable Syslog** to **OFF**.
- **Syslog Server:** Enter the IP address of the syslog server and port number to use in the **Syslog Server** and **Port** fields.
- **Syslog Transport Type:** Select the transport protocol that the phone uses when exporting log messages to the syslog server from the drop-down list.
- **Syslog Level:** Sets the detail level of syslog information that displays in the syslog. Select a detail level from the drop-down list.
 - **0:** system is unusable
 - **1:** action must be taken immediately
 - **2:** critical condition
 - **3:** error conditions
 - **4:** warning conditions
 - **5:** normal but significant condition
 - **6:** informational
- **Syslog Facility:** Sets the facility that generates the log messages. Select a facility from the **Syslog Facility** drop-down list.
- **Syslog Prepend Mac:** Set to **ON** to prepend the phone's MAC address to log messages that are exported to the syslog server. Set to **OFF** to export log messages to the syslog server without the phone's MAC address.
- **Export All Diagnostic Files:** Use these controls to start and stop the diagnostics process and export the results.
 - Click **Start** to begin capturing signal traffic in the Pcap trace, boot.log, sys.log, and .bin configuration files. The system log level will be automatically set to 6. The file format of the exported diagnostic file is *.tar.
 - Click **Stop** to stop capturing signal traffic.
 - Click **Export** to open the file download window, and then save the diagnostic file to the local PC. A diagnostic file named allconfig.tgz will be exported to the local PC.

Click **Confirm** to save settings or **Cancel** to cancel.

Tones

The **Tones** section sets the tone set used by the phone to indicate different phone statuses. Tone sets vary from country to country and customized tone sets can be used as well.

Settings – Tones



The screenshot shows the Crestron Settings interface for the 'Tones' section. On the left is a navigation menu with options: Status, Network, Features, Settings (selected), Preference, Time&Date, Upgrade, Auto Provision, Configuration, Tones (highlighted), Power Saving, and Security. The main content area has a 'Select Country' dropdown menu currently set to 'United States' and a 'Dial' input field. A 'NOTE' box on the right states: 'Tones: You can customize tones or select specialized tone sets (vary from country to country) to indicate different phone statuses. Click here to get more product documents.' At the bottom of the page are 'Confirm' and 'Cancel' buttons.

- Select the tone set to use (based on country) from the **Select Country** drop-down list.
- If **Custom** is selected, a custom tone can be entered in the **Dial** field. Tones are specified as follows:

tone list = element[,element] [,element]...

Where:

element = [!]Freq1[+Freq2][+Freq3][+Freq4] /Duration

Freq: the frequency of the tone (ranges from 200 to 4000 Hz). If it is set to 0 Hz, it means the tone is not played.

A tone is comprised of at most four different frequencies.

Duration: the duration (in milliseconds) of the dial tone, ranges from 0 to 30000ms.

You can configure at most eight different tones for one condition, and separate them by commas. (for example, 250/200,0/1000,200+300/500,200+500+800+1500/1000).

To have the phone play tones once, add an exclamation mark "!" before tones (for example, !250/200,0/1000,200+300/500,200+500+800+1500/1000).

Click **Confirm** to save settings or **Cancel** to cancel.

Power Saving

The **Power Saving** section is used to control phone's power-saving mode. The power-saving mode turns off the phone's backlight and screen to conserve energy. The phone can be configured to enter the power-saving mode based on office schedules and usage.

Settings – Power Saving

Day	Start Time	End Time
Monday	7 AM	7 PM
Tuesday	7 AM	7 PM
Wednesday	7 AM	7 PM
Thursday	7 AM	7 PM
Friday	7 AM	7 PM
Saturday	7 AM	7 AM
Sunday	7 AM	7 AM

Setting	Value
Office Hour Idle TimeOut	120
Off Hour Idle TimeOut	10
User Input Extension Idle TimeOut	10

Office Hours

Set office hours for each day of the week to specify when the phone would typically be in use.

Idle TimeOut (minutes)

- **Office Hour Idle TimeOut:** Enter a time (in minutes) for the phone to wait in the idle state before entering power-saving mode during office hours.
- **Off Hour Idle TimeOut:** Enter a time (in minutes) for the phone to wait in the idle state before entering power-saving mode during off hours.
- **User Input Extension Idle TimeOut:** Enter a time (in minutes) for the phone to wait in the idle state after using the phone, before entering power-saving mode.

Click **Confirm** to save settings or **Cancel** to cancel.

Security

The **Security** section sets the phone's admin and user passwords and also manages trusted certificates and server certificates that are used by the phone for authentication.

Password

The **Password** section sets the admin and user passwords for using and configuring the phone.

Security – Password

The screenshot shows the Crestron web interface for the Password configuration page. The sidebar on the left contains the following items: Status, Network, Features, Settings, Security, Password (highlighted), Trusted Certificates, and Server Certificates. The main content area has the following fields: User Type (dropdown menu with 'admin' selected), Old Password (text input), New Password (text input), and Confirm Password (text input). Each field has a help icon (question mark). At the bottom of the main content area are 'Confirm' and 'Cancel' buttons. On the right side, there is a 'NOTE' box with the following text: 'User Password/ Administrator Password: When logging into the web user interface, you need to enter the user name and password. You can change the user/ administrator password for security. Click here to get more product documents.'

Perform the following procedure to set a password.

1. Select a user type (**admin** or **user**) from the **User Type** drop-down list.
2. Enter the old password in the **Old Password** field.
3. Enter the new password in the **New Password** field.
4. Confirm the new password in the **Confirm Password** field.
5. Click **Confirm** to save settings or **Cancel** to cancel.

Trusted Certificates

The **Trusted Certificates** section manages the list of Transport Layer Security (TLS) trusted certificates that the phone uses to verify certificates sent by the server.

Security – Trusted Certificates

The screenshot shows the Crestron web interface for the Trusted Certificates configuration page. The sidebar on the left contains the following items: Status, Network, Features, Settings, Security, Password, Trusted Certificates (highlighted), and Server Certificates. The main content area has the following elements: a table with columns '#', 'Issued To', 'Issued By', 'Expiration', and a checkbox column. The table currently contains 'No data'. Below the table is a 'Delete' button. There are two toggle switches: 'Only Accept Trusted Certificates' (set to ON) and 'Common Name Validation' (set to OFF). Below these is a dropdown menu for 'CA Certificates' set to 'All Certificates'. The 'Import Trusted Certificates' section includes an 'Upload Trusted Certificate File' field with a file selection button and an 'Upload' button. At the bottom of the main content area are 'Confirm' and 'Cancel' buttons. On the right side, there is a 'NOTE' box with the following text: 'Transport Layer Security (TLS) Trusted Certificate: When the IP phone requests a TLS connection with a server, the IP phone should verify the certificate sent by the server to decide whether it is trusted based on the trusted certificates list. The IP phone has 30 built-in trusted certificates. You can upload 10 custom certificates at most. The format of the trusted certificate files must be *.pem, *.cer, *.crt and *.der and the maximum file size is 5MB. Click here to get more product documents.'

The phone has 30 built-in trusted certificates. Ten more custom certificates can be uploaded to the phone. Trusted certificates must be *.pem, *.cer, *.crt and *.der file types.

The maximum file size is 5 MB.

- Set **Only Accept Trusted Certificates** to **ON** to have the phone only trust server certificates that are in the list of trusted certificates. To have the phone trust all certificates presented by the server, set **Only Accept Trusted Certificates** to **OFF**.
- Set **Common Name Validation** to **ON** to have the phone validate the **CommonName** or **SubjectAltName** of each certificate sent by the server. To skip validation of these values, set **Common Name Validation** to **OFF**.
- Select the type of certificates in the Trusted Certificates list the phone will use to authenticate for TLS connection from the **CA Certificates** drop-down line.
- To upload a trusted certificate, click inside the **Upload Trusted Certificate File** field, select a certificate file (*.pem, *.cer, *.crt and *.der file types), and click **Upload**.

Click **Confirm** to save settings or **Cancel** to cancel.

Server Certificates

The **Server Certificates** section manages the list of Transport Layer Security (TLS) server certificates that the phone sends to authenticate client connections.

Security – Server Certificates

The screenshot displays the 'Server Certificates' configuration screen in the Crestron mobile app. On the left is a navigation menu with options like Status, Network, Features, Settings, Security, Password, and Trusted Certificates. The main area contains a table with headers: #, Issued To, Issued By, Expiration, and a checkbox. The table is currently empty with 'No data' in the center and a 'Delete' button on the right. Below the table, there are two sections: 'Device Certificates' with a 'Default Certificates' dropdown menu, and 'Import Server Certificates' with an 'Upload Server Certificate File' field and an 'Upload' button. A 'NOTE' section on the right provides detailed information about Transport Layer Security (TLS) server certificates, including a definition of unique certificates (issued by the Yealink Certificate Authority) and generic certificates (issued by the Yealink Certificate Authority). At the bottom of the screen, there are 'Confirm' and 'Cancel' buttons.

The phone has two types of built-in server certificates: a unique server certificate and a generic server certificate. Only one additional server certificate can be uploaded to the phone. The existing server certificate will be overridden by the new one. Trusted certificates must be *.pem or *.cer file types. The maximum file size is 5 MB.

A unique server certificate is unique to a phone (based on the MAC address) and issued by the Certificate Authority (CA).

A generic server certificate is issued by the Yealink Certificate Authority (CA). The phone send a generic certificate for authentication only if a unique certificate does not exist.

- Select the type of certificate the phone will send for authentication from the **Device Certificates** drop-down list.
- To upload a server certificate, click inside the **Upload Server Certificate File** field, select a certificate file (*.pem or *.cer file types), and click **Upload**.

Crestron XiO Cloud Service

The Crestron XiO Cloud™ service can be used to deploy and manage multiple devices across an enterprise.

The Crestron XiO Cloud™ service requires devices to be claimed so they can be managed by the service. To claim a single device or multiple devices, perform one of the following procedures.

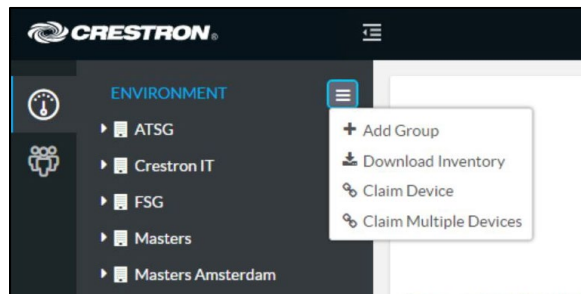
Claim a Single Device

1. Record the MAC address and serial number that are labeled on the shipping box or on a sticker attached to the device. The MAC address and serial number are required to add the device to the Crestron XiO Cloud environment.

NOTE: Use the MAC address labelled "MAC Address."

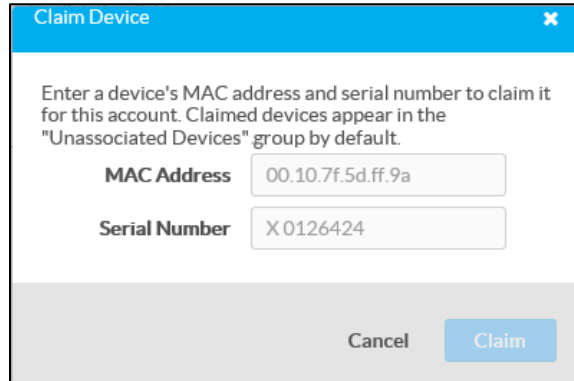
2. Open a web browser, and log in to the Crestron XiO Cloud service at <https://portal.crestron.io>.
3. Click the **ENVIRONMENT** menu button (☰) to display the Environment menu.

Environment Menu



4. Click **Claim Device**. The **Claim Device** dialog box is displayed.

Claim Device Dialog Box



Claim Device

Enter a device's MAC address and serial number to claim it for this account. Claimed devices appear in the "Unassociated Devices" group by default.

MAC Address 00.10.7f.5d.ff.9a

Serial Number X 0126424

Cancel Claim

5. Enter the MAC address and serial number recorded in step 1 in the **MAC Address** and **Serial Number** fields, respectively.
6. Click **Claim**. A message indicating a successful claiming displays.

NOTE: If an error message displays stating the device does not exist, connect the device to a network that has access to the Internet, wait 15 minutes, and then try again.

7. Click **X** to close the dialog box. The host name of the claimed device appears in the device tree under the group **Unassociated Devices**.

The device can now be managed or assigned to a group. For information on creating environments, managing devices, and managing users with the Crestron XiO Cloud service, refer to the Crestron XiO Cloud Service User Guide Guide (Doc. 8214) at www.crestron.com/manuals.

Claim Multiple Devices

1. Record all of the MAC addresses and respective serial numbers in a comma delimited, CSV file, and then save it to a location that is accessible to the computer used to access the Crestron XiO Cloud service. The CSV file should be formatted as shown below:

CSV File Format

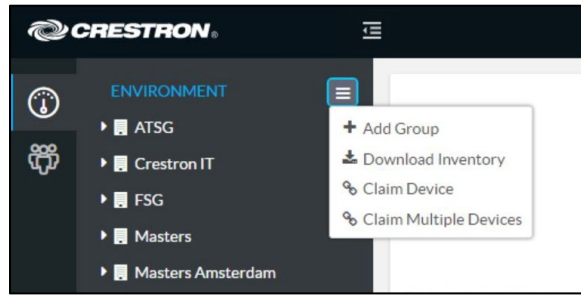
```
MAC Address,Serial Number
00.10.7e.8b.81.b6,17284712
00.10.7e.8b.8c.87,17284570
00.10.7e.96.83.93,1716JBG01207
00.10.7e.96.92.0a,1716JBG01550
00.10.7e.8b.87.c1,17284670
```

NOTES:

- MAC addresses and serial numbers are labeled on the shipping box or on a sticker attached to the device.
 - Use the MAC address labelled "MAC Address."
-

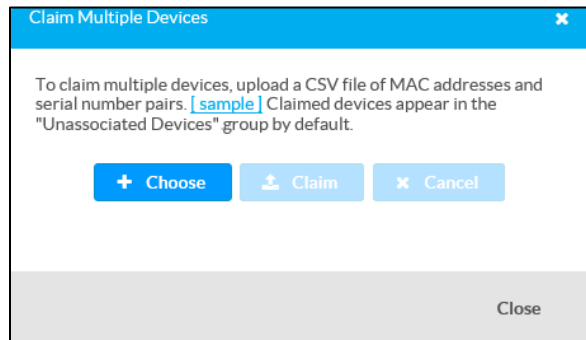
2. Open a web browser, and log in to the Crestron XiO Cloud service at <https://portal.crestron.io>.
3. Click the **ENVIRONMENT** menu icon (☰) to display the Environment menu.

Environment Menu



4. Click **Claim Multiple Devices** from the drop-down menu. The **Claim Multiple Devices** dialog box is displayed.

Claim Multiple Devices Dialog Box



5. Click + **Choose** and select the CSV file created in step 1.
6. Click **Claim** to claim all of the devices listed in the file. A message indicating the claim status of each device is displayed.

NOTE: If an error message displays stating the device does not exist, connect the device to a network that has access to the Internet, wait 15 minutes, and then try again.

7. Click X in the upper right corner to close the dialog box. The host names of the claimed devices appear in the device tree under the group **Unassociated Devices**.

The devices can now be managed or assigned to a group. For information on creating environments, managing devices, and managing users with the Crestron XiO Cloud service, refer to the Crestron XiO Cloud User Guide (Doc. 8214) at www.crestron.com/manuals.

Startup & Sign In

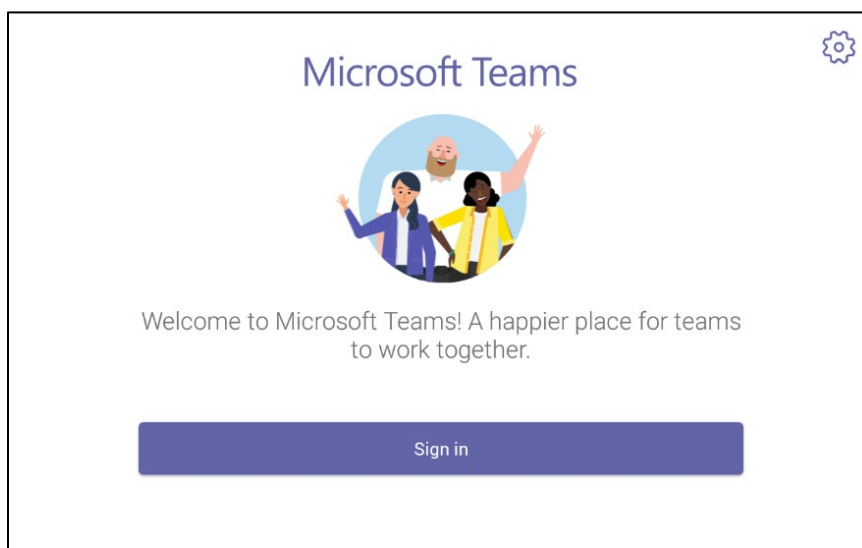
After connecting the phone to a Power over Ethernet connection, the phone will boot up and ask to select a language.

1. Tap the desired interface language and tap ✓. The Crestron privacy statement will display.

NOTE: The interface language can be changed if desired. Refer to "Set Language" on page 3 for details.

2. Tap **Agree** to continue. The Microsoft Teams start screen is displayed.

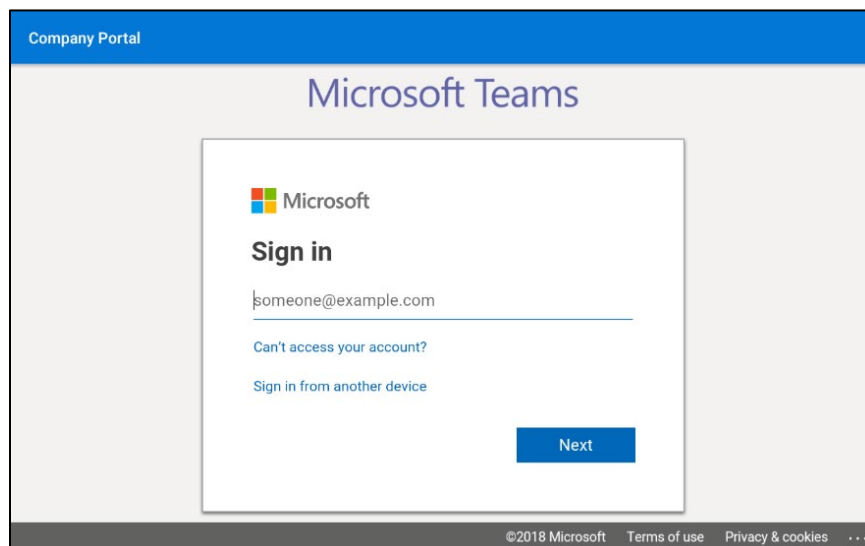
Microsoft Teams Start Screen



3. Tap **Sign in** to display the **Sign in** screen.

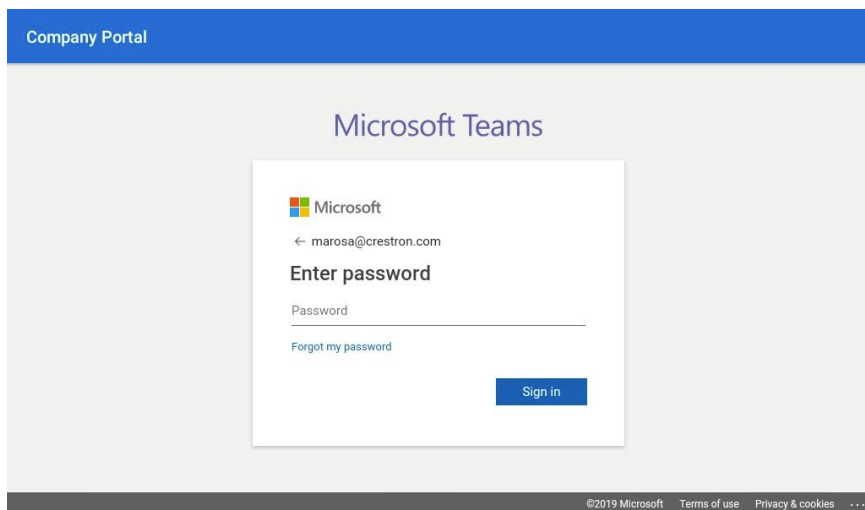
NOTE: You can also tap ⚙️ on the top right to set the partner settings. For details, refer to "Partner Settings" on page 2.

Microsoft Teams Sign In Screen



4. Tap the **email address** field and use the on-screen keyboard to enter the email address of the Microsoft Teams account. Tap **Go** when finished. The Enter Password screen is displayed.

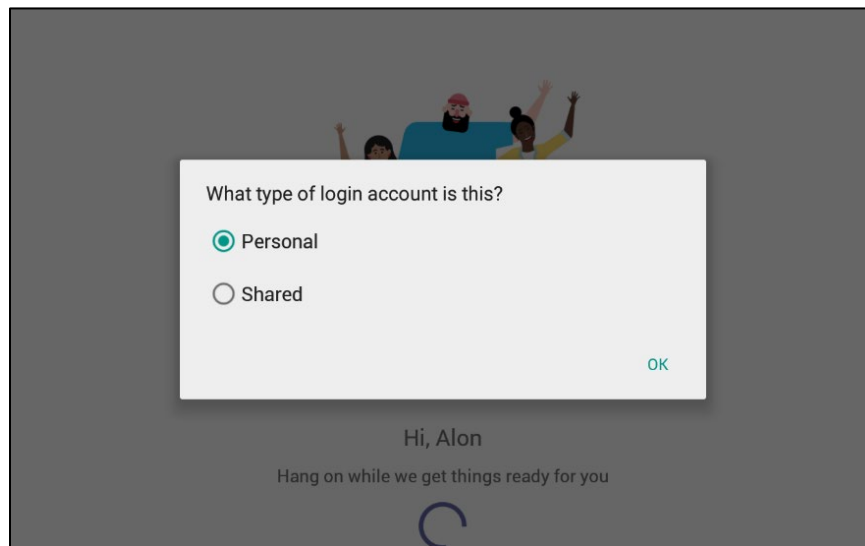
Enter Password Screen



5. Tap the **Password** field and use the on-screen keyboard to enter the password of the Microsoft Teams account. Tap **Go** when finished.

If configured, the phone will perform two-step verification. Otherwise, the phone will ask you to select the type of login account.

Select Account Type



The device can be set up with a personal account or a shared account.

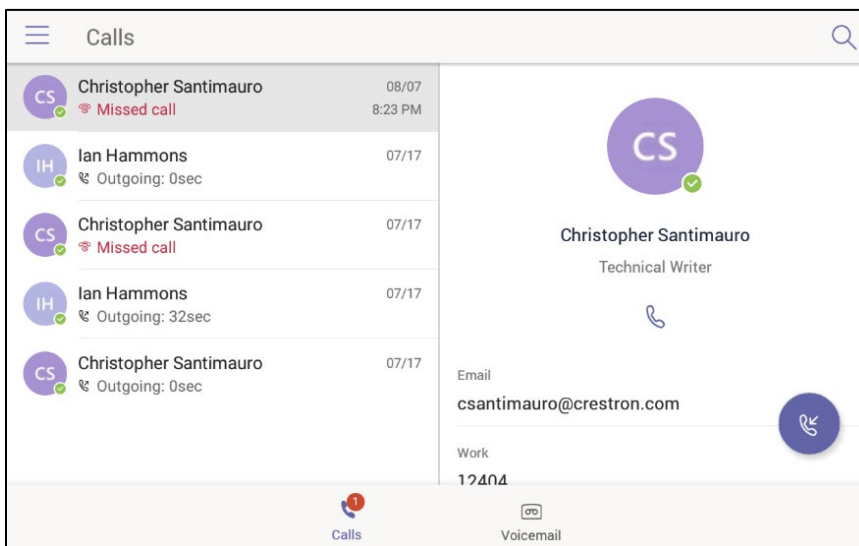
Use the **Personal** setting if the device is to be placed on a user's desk. Devices with a personal account will show call history and have access to voice mail.

Use the **Shared** setting if the device will be placed in a conference room. Call history information and voice mail features are not available.

Select an account type and tap **OK**.

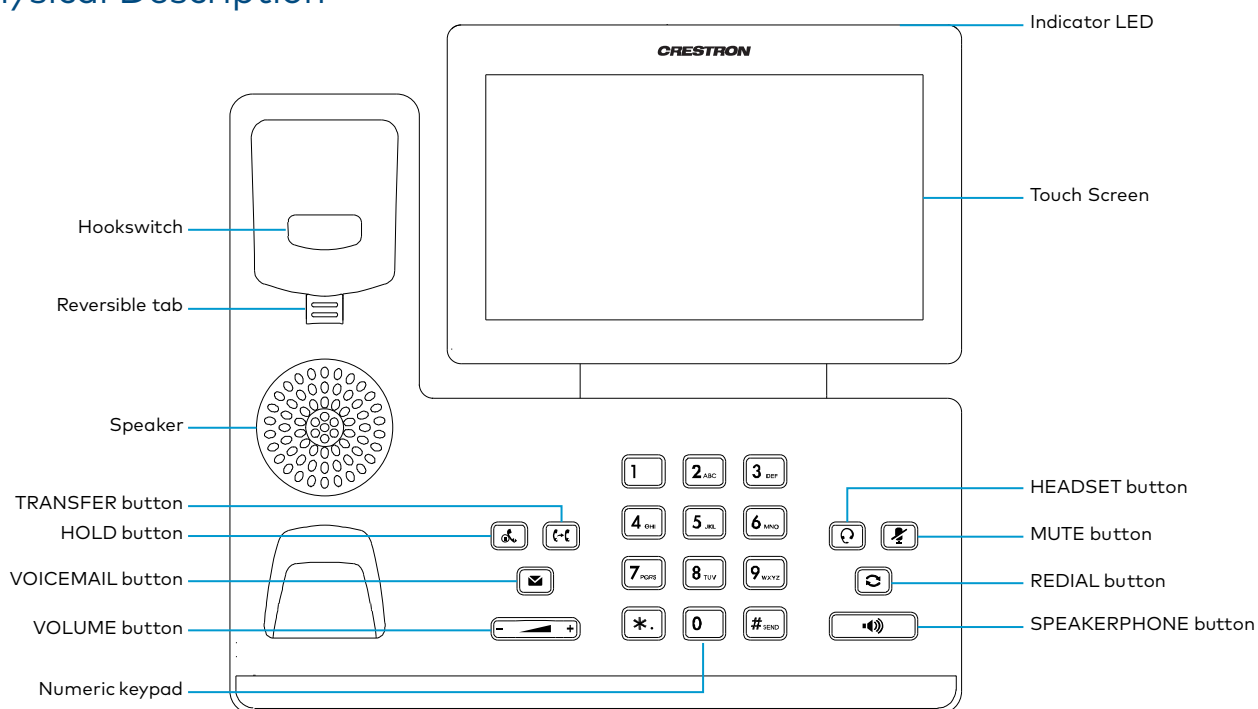
The device will log into the Microsoft Teams service and display the home screen.

Home Screen



Phone Operation

Physical Description

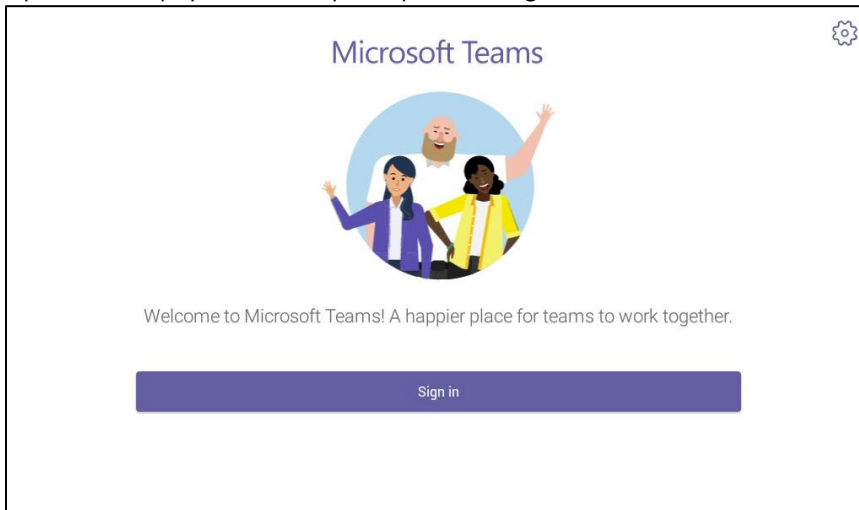


- **Hookswitch:** The hookswitch connects or disconnects the phone from the phone line. The hookswitch is automatically activated when the handset is lifted from the phone.
- **Reversible Tab:** Secures the handset in the handset cradle when the phone is mounted vertically.
- **Speaker:** Used for speakerphone functions.
- **TRANSFER:** Transfers a call.
- **HOLD:** Press to place a call on hold. Press again to resume the call.
- **VOICEMAIL:** Press to access voicemail.
- **VOLUME:** Press **-** to lower the volume. Press **+** to raise the volume.
- **Numeric Keypad:** Use to dial numbers or enter information.
- **Indicator LED:** Indicates call status, message status and phone's system status.
 - Red: The phone is initializing.
 - Fast-flashing red: The phone is ringing.
 - Slow-flashing red: The phone receives a voicemail or misses a call.
- **Touch Screen:** Tap to select and highlight screen items.

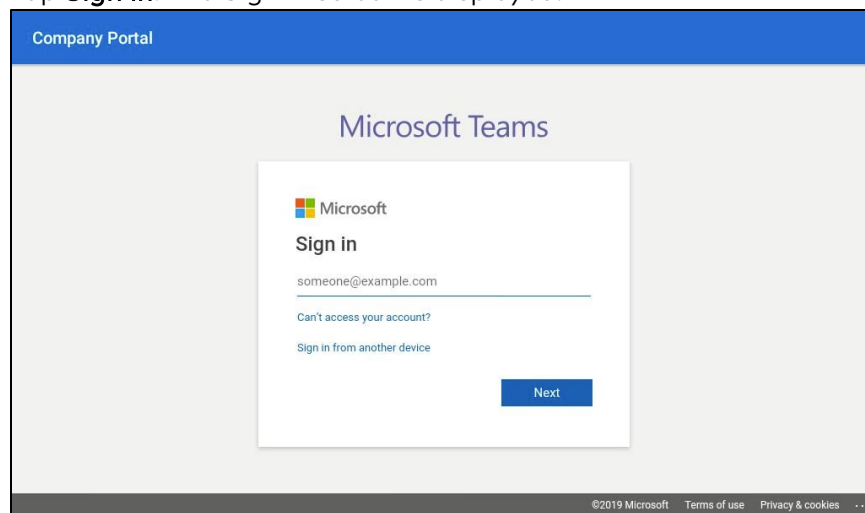
- **HEADSET:** Press to toggle the headset on or off. The button glows green when the headset is in use.
- **MUTE:** Press to toggle the microphone on or off. The button glows red when the mute feature is activated.
- **REDIAL:** Press to redial the last-dialed number.
- **SPEAKERPHONE:** Press to toggle the speakerphone for hands free operation. The button glows green when the speakerphone is activated.

Sign In

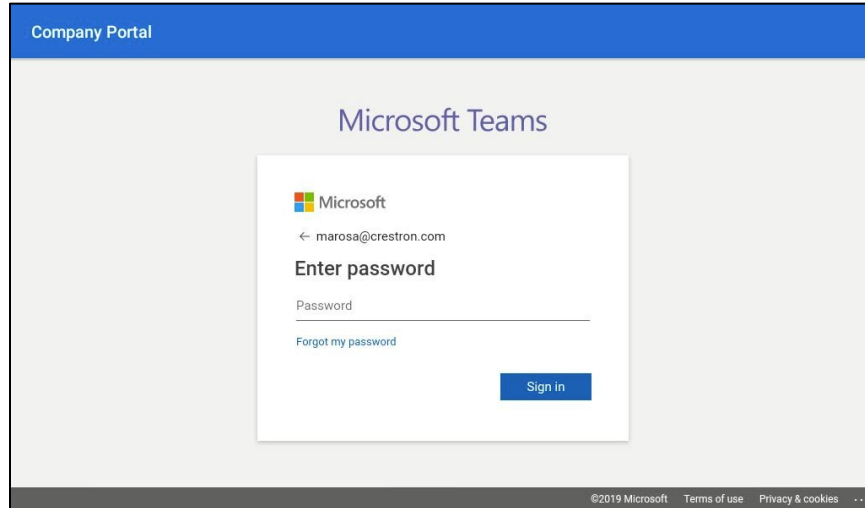
Upon startup, you will be prompted to sign in to the Microsoft Teams application.



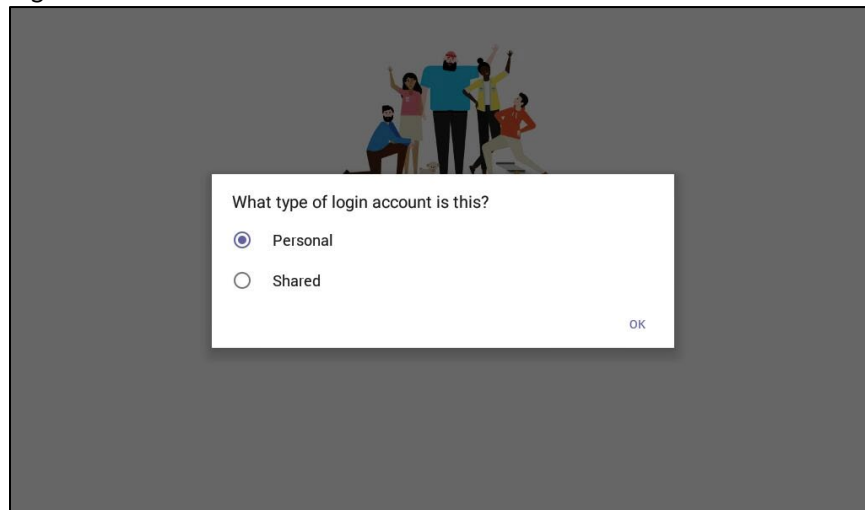
1. Tap **Sign in**. The Sign in screen is displayed.



2. Tap the email address field to display the on-screen keyboard and enter the sign-in address. Tap **Next** when done.



3. Tap the password field to display the on-screen keyboard and enter the password. Tap **Sign in** when done. The device will ask you to select the type of login account.



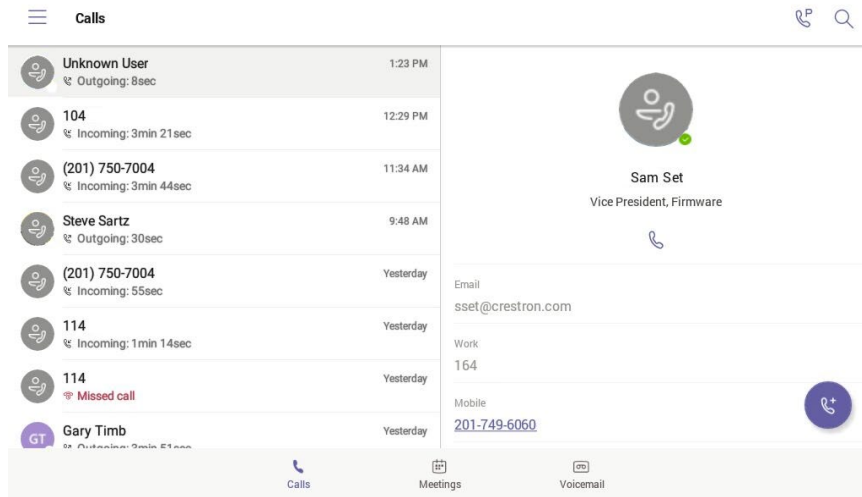
The device can be set up with a personal account or a shared account.

Use the **Personal** setting if the device is to be placed on a user's desk. Devices with a personal account will show call history and have access to voice mail.

Use the **Shared** setting if the device will be placed in a conference room. Call history information and voice mail features are not available.

Select an account type and tap **OK**.

The device will log into the Microsoft Teams service and display the Calls screen.



The Teams Phone Display

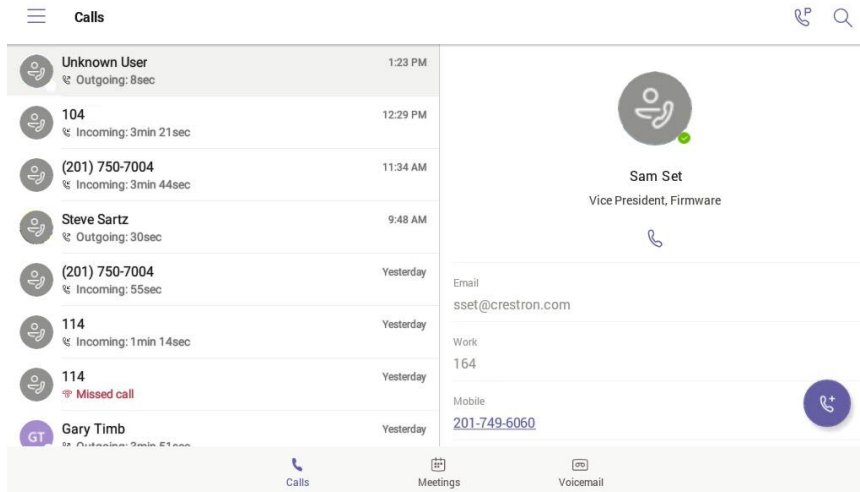
The Teams phone display consists of three separate screens.

- **Calls:** Displays the call log (Personal use only), searches for contacts, and makes phone calls.
- **Meetings:** Lists all scheduled meetings and creates new meetings.
- **Voicemail** (Personal use only): Lists all voicemail messages.

NOTE: At any time, you can make a call by picking up the handset, pressing the headset button, or pressing the speakerphone button and dialing the number on the numeric keypad.

Calls Screen

Tap **Calls** to show the Calls screen. The Calls screen displays the call log on the left side of the screen and the contact information from the selected call log entry on the right side of the screen.



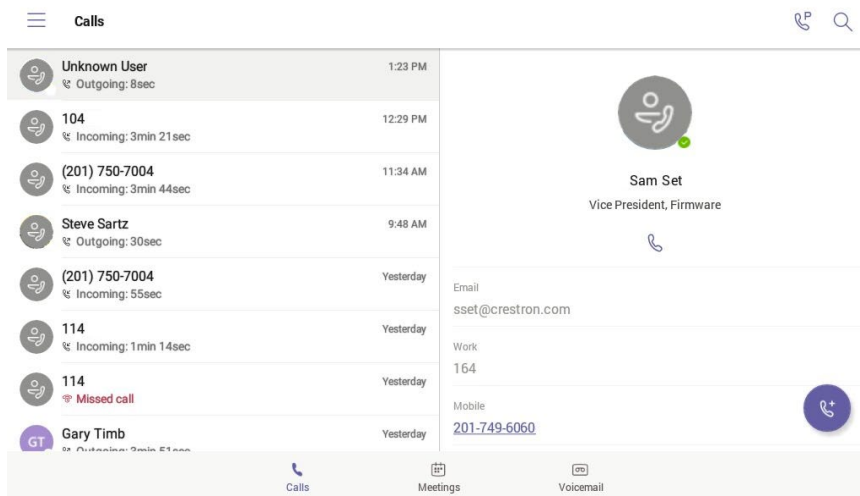
To navigate the call log, drag up or down to scroll through the call log.

From the Keypad

To make a call, pick up the handset, press the headset button, or press the speakerphone button and dial the number.

From the Call Log

Tap a call log entry. The call details are shown on the right side of the screen.



Tap any of the contact options shown for the contact to call

Search for a Contact


When searching for a contact, you can call an individual contact or search for multiple contacts and create a group call.

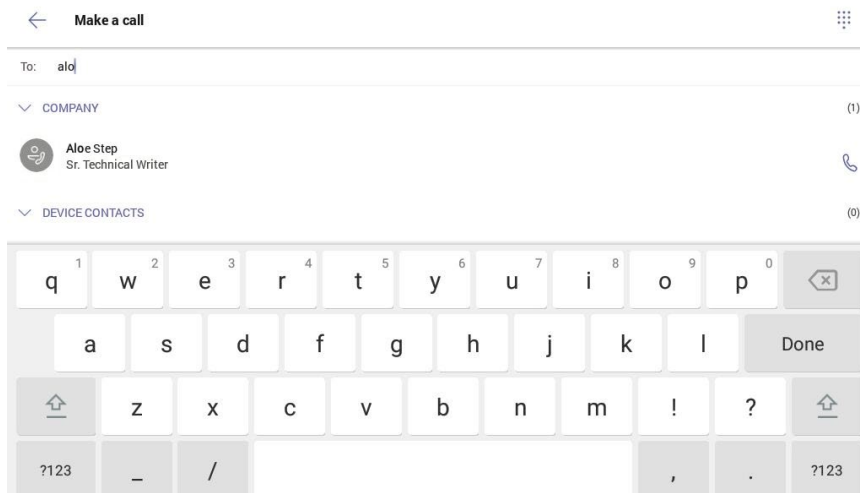
1. Tap  to display the search screen.



Direct Call

You can directly call a contact by either dialing their phone number or searching for a contact.

- Directly call a contact.
Dial the desired phone number and tap  next to the number to place the call.
- Search for a contact.
 - a. Tap inside the **To** field to display the on-screen keyboard to search by name.
 - b. Type the name of the desired contact. Search results are shown below the **To** field.



- c. Tap  next to a contact to place the call.

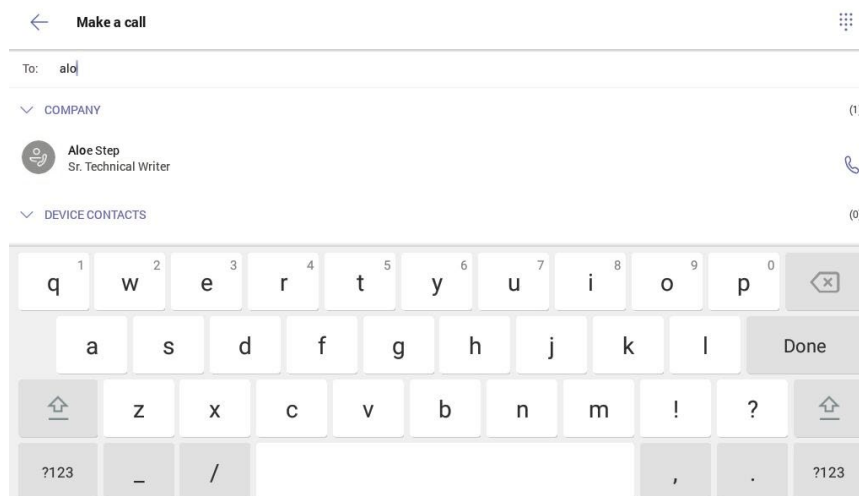
Create a Group Call

You can create a group call with the numeric keypad and on-screen keypad.

1. Add a number or contact to the group call.
 - Add a phone number
 - i. Dial the desired phone number and tap the number to add it to the group call. The number appears in the **To** field.



- ii. Repeat for each phone number to add to the group call.
- Add a contact
 - i. Tap inside the **To** field to display the on-screen keyboard to search by name.
 - ii. Type the name of the desired contact. Search results are shown below the **To** field.



- iii. Tap the contact name to add it to the group call. The contact appears in the **To** field.

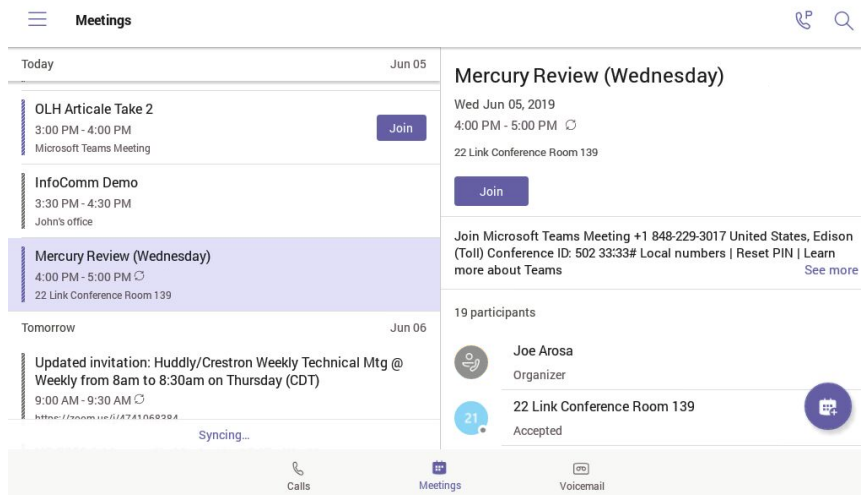


- iv. Repeat steps i through iii for each contact to add to the group call.

2. Tap  to start the group call.

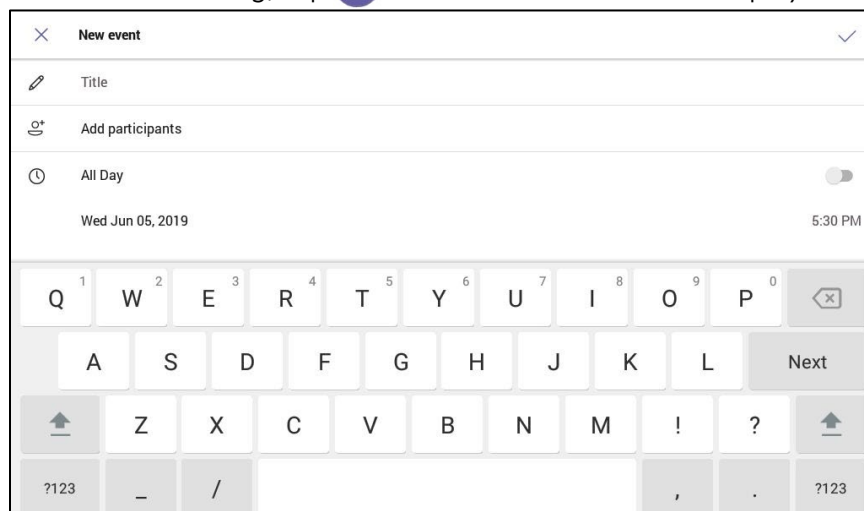
Meetings Screen

Tap **Meetings** to show the Meetings screen. The Meetings screen displays the schedule of meetings on the left side of the screen and the meeting details for the selected meeting on the right side of the screen.

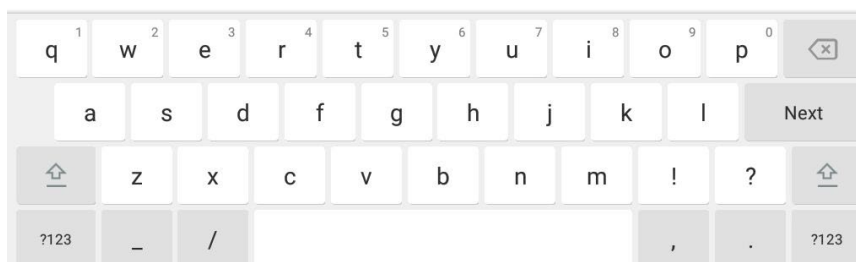




- To navigate the list of meetings, drag up or down to scroll through the list of meetings.
- To join a meeting, tap **Join** in the meeting list or in the meeting details. The phone will connect to the meeting.

- To create a meeting, tap . The New event screen is displayed.



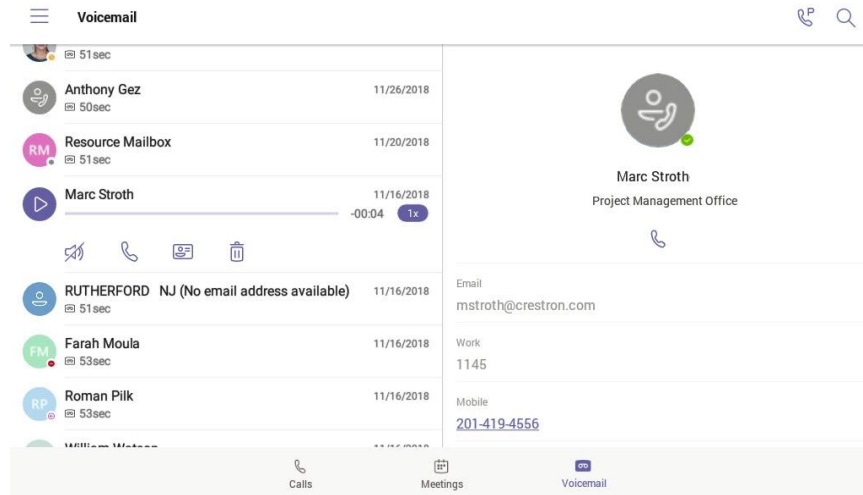
- Tap inside the **Title** field and use the on-screen keyboard to name the event.
- Tap inside the **Add participants** field and enter the name or email address for each participant.

- Tap  when all the participants have been entered.
- Tap the date to select a date, and then tap the time to select a time. If the meeting is going to be an all day event, select **All Day**.
- If the meeting will be held in a physical location in addition to a Microsoft Teams meeting, Enter the location in the **Location** field.
- Select the frequency of the meeting in the **Repeat** field.
- Select how a participant's schedule should be marked during the meeting in the **Show as** field.
- Enter a description of the meeting in the **Description** field.
- Tap  to save the meeting and invite the participants.

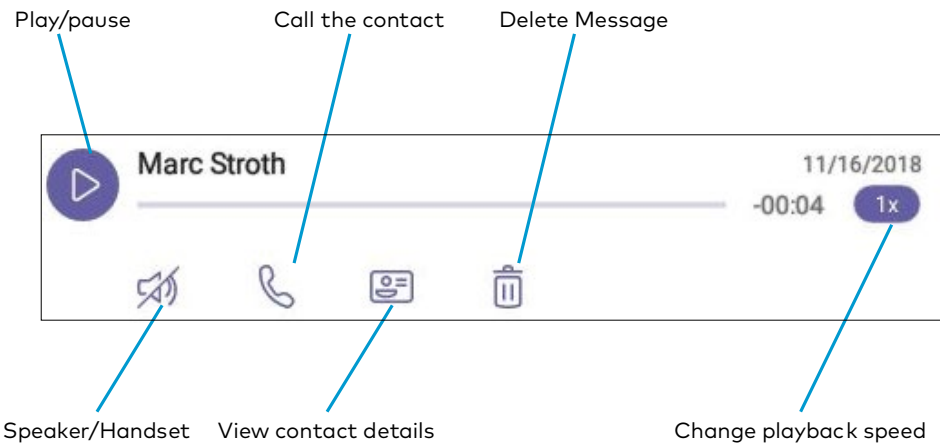
Voicemail

Tap **Voicemail** to show the Voicemail screen. The Voicemail screen displays the recorded voicemail messages and playback controls on the left side of the screen and the contact details for the selected voicemail message on the right side of the screen.



- To navigate the list of voicemail messages, drag up or down on the left side of the screen to scroll through the list of messages.
- Tap a message to display playback controls and message transcription (if available). The caller's contact information is displayed on the right side of the screen.

Voicemail controls



Microsoft Teams Rollout

For information on Microsoft Teams software, visit <https://docs.microsoft.com/en-us/MicrosoftTeams/teams-overview>

This page is intentionally left blank.

