UC-P100-S & UC-P110-S-PLUS Crestron Flex VoIP Desk Phones for Skype® for Business

Supplemental Guide

Crestron Electronics, Inc.

Contents

UC-P100-S & UC-P110-S-PLUS Crestron Flex VoIP Desk Phones for Skype® for Business

Introduction

The UC-PHONE-S & UC-PHONE-S-PLUS Crestron Flex VoIP Desk Phones for Skype® for Business (respectively sold as UC-P100-S & UC-P110-S) are premium VoIP desk phones designed for use with the Skype for Business 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 Skype® for Business 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-S & UC-PHONE-S-PLUS phones. For information on installing these phones, refer to the UC-PHONE-S/UC-PHONE-T Quick Start Guide (Doc 8358) and the UC-PHONE-S-PLUS/UC-PHONE-T-PLUS Quick Start Guide (Doc 8359) at www.crestron.com/manuals.

This guide is intended for administrators who need to properly configure, customize, manage, and troubleshoot the Skype for Business phones. This guide will help with understanding the Voice over Internet Protocol (VoIP) network and provides descriptions of all available phone features. This guide describes three methods for configuring phones: central provisioning, web user interface and phone user interface. The document will provide information on the following:

- Configure a phone on a provisioning server
- Configure a phone's features and functions via web/phone user interface
- Troubleshoot some common phone issues

Many of the features described in this guide involve network settings, which could affect the phone's performance in the network. An understanding of IP networking and a prior knowledge of IP telephony concepts are necessary.

The information in this guide is for UC-PHONE-S and UC-PHONE-S-PLUS phones running firmware version 55.9.91.1 or later.

Reading the Configuration Parameter Tables

Most features described in this guide include two tables. One is a summary table of provisioning methods used to configure the features. The other contains configuration parameters used to make the features work.

This brief section describes the conventions used in the summary table and configuration parameter table. In order to read the tables and successfully perform configuration changes, an understanding of these conventions is necessary.

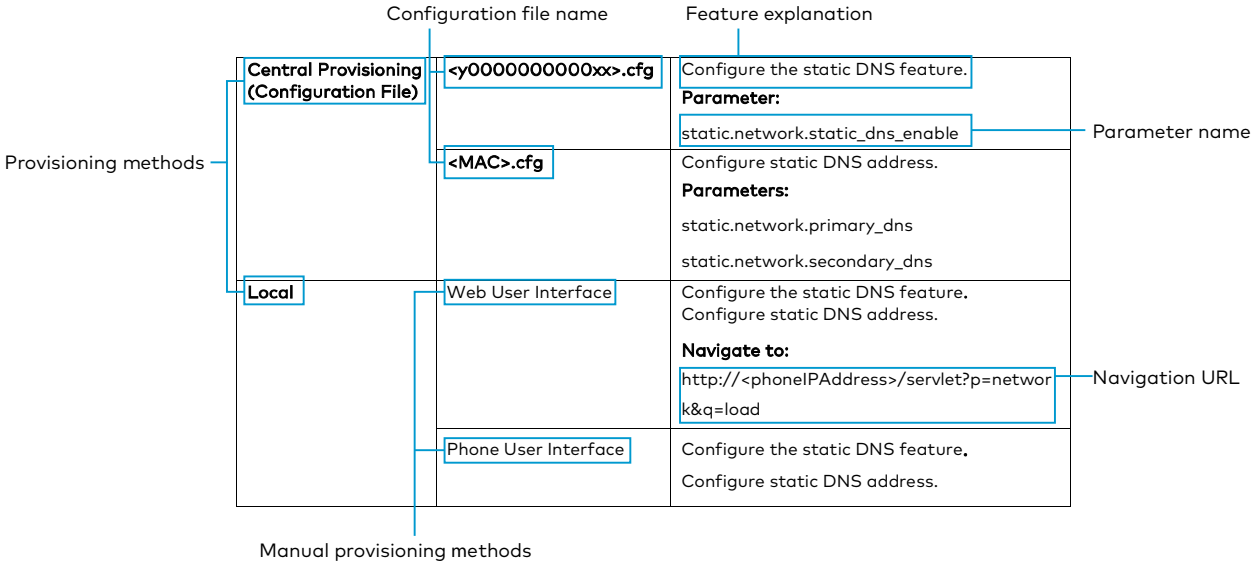
Summary Table Format

The following summary table indicates three methods; central provisioning, web user interface, and phone user interface, that can be used to configure a feature. Note that the types of methods used for each feature will vary.

The central provisioning method requires parameters to be configured in the CFG format. Configuration files provided by Crestron Files can be downloaded from the DOCUMENTATION section of each product page on the Crestron website. For more information on configuration files, refer to "Configuration Files" on page 85. As shown below, the table specifies the configuration file name and the corresponding parameters. That is, the <MAC>.cfg file contains the account.1.auto_answer parameter, and the <y0000000000xx>.cfg file contains the features.auto_answer_delay parameter.

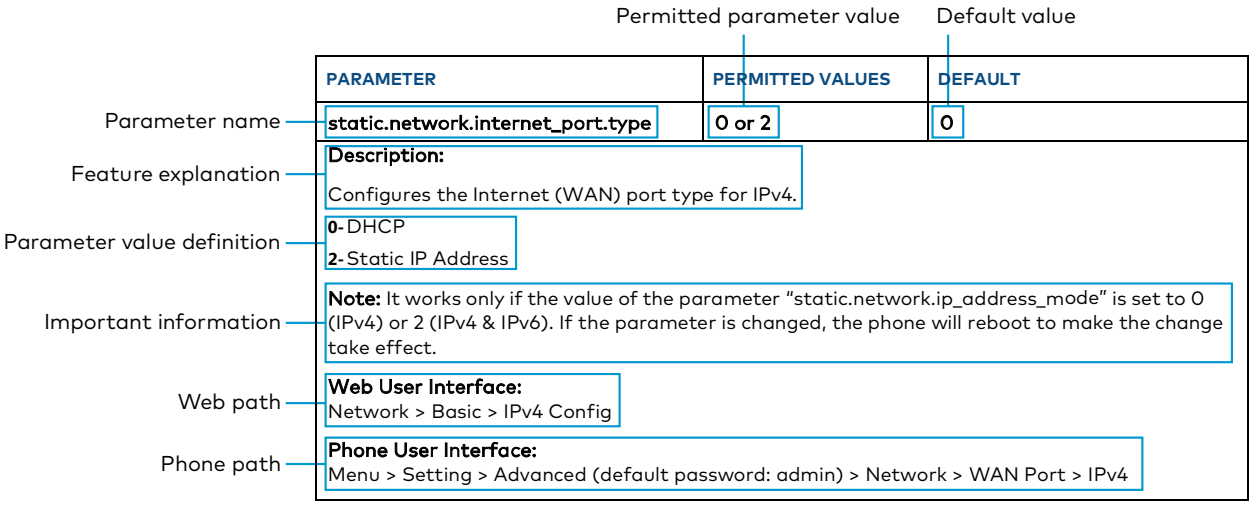
The web user interface method requires configuring features by navigating to the specified link. This navigation URL enables the user to quickly locate the webpage where the feature can be configured.

Summary Table Format



Configuration Parameter Table Format

The following configuration parameter table describes how to configure a parameter to make a feature (e.g., auto answer) work. The table also indicates three methods for configuring the feature (parameter name, web user interface, and phone user interface).



NOTE: The word "None" in the Web User Interface or Phone User Interface field means the feature cannot be configured via web/phone user interface.

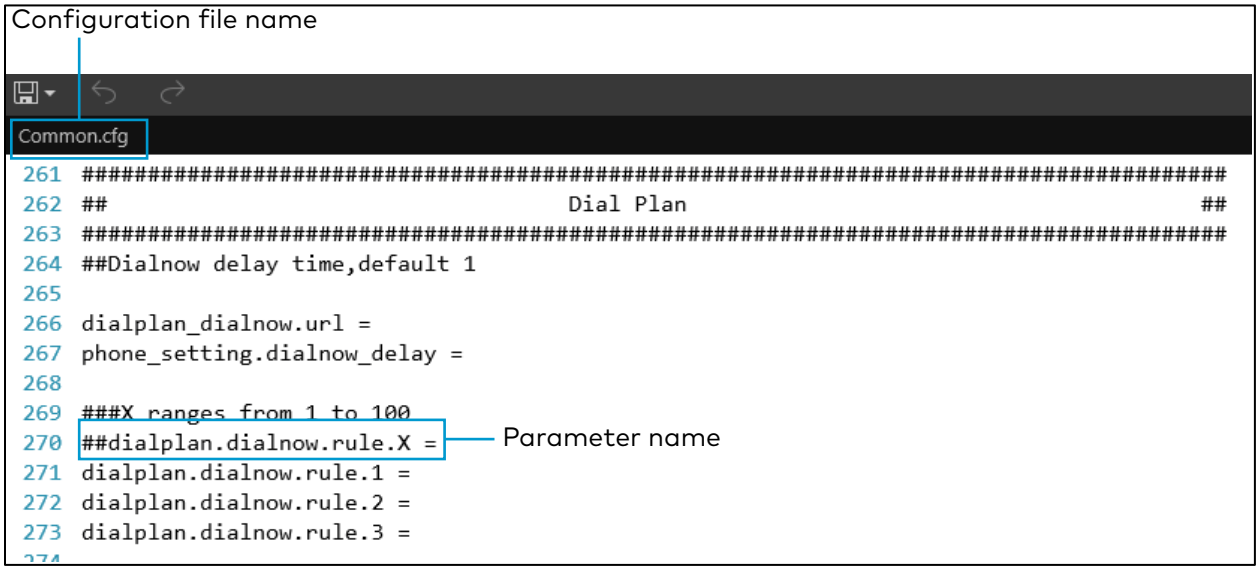
Method 1: Central Provisioning

This table specifies the details of account.1.auto_answer parameter, which enables or disables the auto answer feature. This parameter is disabled by default. To enable the auto answer feature, open the MAC.cfg file and locate the parameter name **account.1.auto_answer**. Set the parameter value to "1" to enable the auto answer feature or "0" to disable the auto answer feature.

Note that some parameters described in this guide contain one or more variables (e.g., X or Y), however, the variables in the parameters described in the CFG file are all replaced with a specific value in the scope of variable. A value may need to be assigned to the variable before searching and locating the specific parameter in the CFG file.

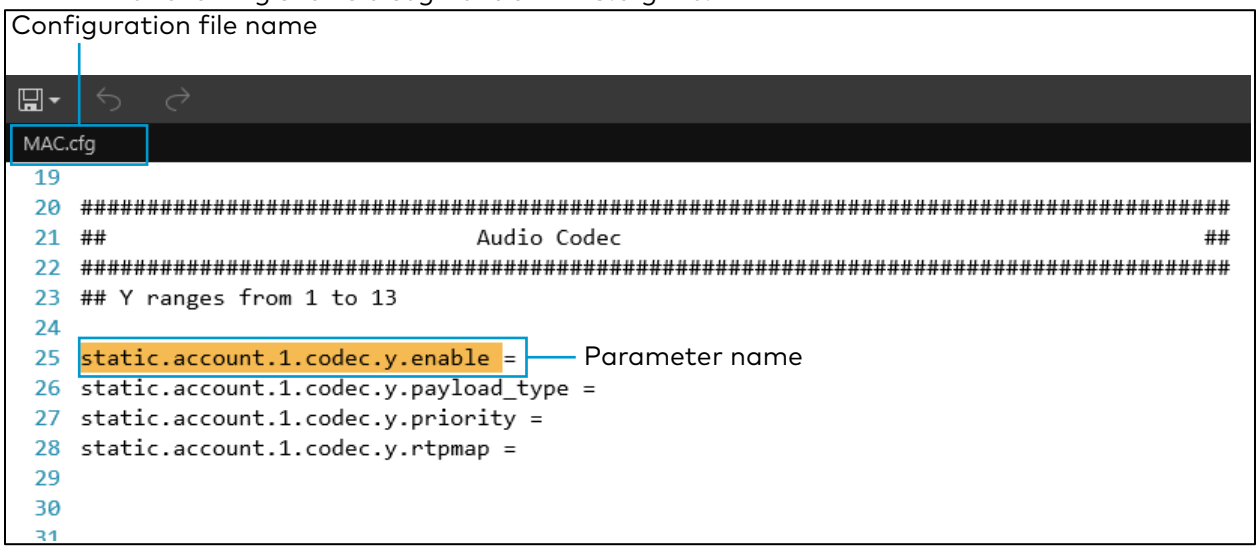
For example, to configure the dial-now rule, locate the parameter dialplan.dialnow.rule.X in the Common.cfg file and then configure as required (e.g., dialplan.dialnow.rule.1 = 123).

Common.cfg file



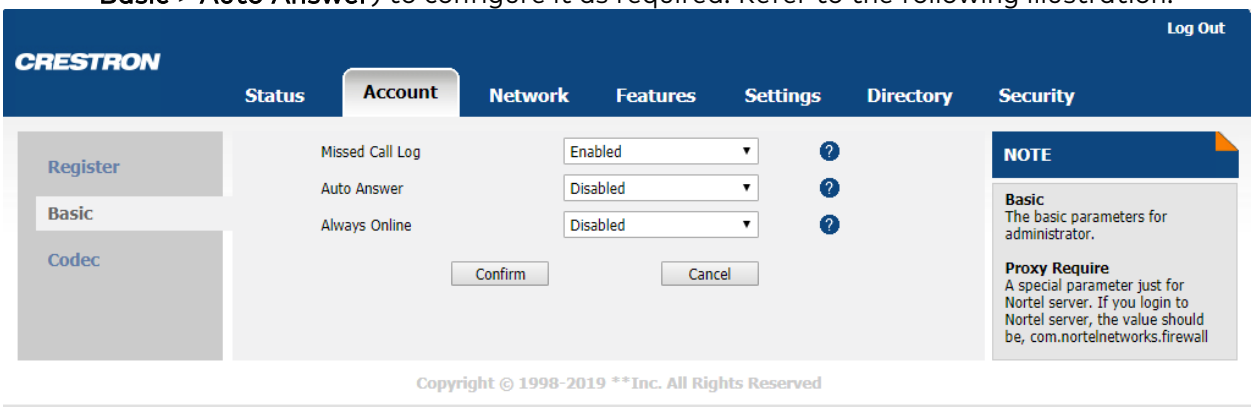
To enable the audio codec 1 for account 1, locate the static.account.1.codec.Y.enable in the MAC.cfg file and configure it as required (e.g., static.account.1.codec.1.enable = 1).

The following shows a segment of MAC.cfg file:



Method 2: Web User Interface

As described in "Summary Table Format" on page 2, a user can directly navigate to the specified webpage to configure the feature. The user can also log into the web user interface, and then locate the feature field according to the web path (e.g., **Account** > **Basic** > **Auto Answer**) to configure it as required. Refer to the following illustration.



To successfully log into the web user interface, the user name (default: admin) and password (default: admin) may need to be entered. For more information, refer to "The Web User Interface" on page 83.

Method 3: Phone User Interface

Certain features can also be configured through the phone user interface. Access the desired feature according to the phone path (e.g., **Menu** > **Setting** > **Features** > **Auto Answer**) and then configure as required.

Understanding VoIP Principle

VoIP (Voice over Internet Protocol) is a technology using the Internet Protocol instead of traditional Public Switch Telephone Network (PSTN) technology for voice communications.

It is a family of technologies, methodologies, communication protocols, and transmission techniques for the delivery of voice communications and multimedia sessions over IP networks. The Session Initiation Protocol (SIP) is a popular VoIP protocol that is found in widespread implementation.

Phone Features

The UC-PHONE-S and UC-PHONE-S-PLUS are designed to work with Skype for Business Server. These phones are characterized by a large number of functions, which simplify business communication with a high standard of security.

The UC-PHONE-S and UC-PHONE-S-PLUS phones provide a powerful and flexible IP communication solution for Ethernet TCP/IP networks, delivering excellent voice quality. When these phones register with Skype for Business accounts, a user can interact with their Skype for Business contacts on their phones through Microsoft's Active Directory® service.

Physical Features

This section lists the available physical features of Skype for Business phones.

- 7 in. 1024 x 600 pixel color touch screen with backlight (adjustable tilt on UC-PHONE-S-PLUS
- One Skype for Business account
- HD Voice: HD Codec, HD Handset, HD Speaker
- 20 dedicated hard keys
- One RJ-9 (4P4C) handset port
- One RJ-9 (4P4C) headset port
- Two RJ-45 10/100/1000Mbps Ethernet ports
- 4 LEDs: power, mute, headset, speakerphone
- Power over Ethernet (IEEE 802.3af)

Technical Features

Telephony Features

- Call Options: emergency call, call waiting, call hold, call mute, call forward, call transfer, group pickup and audio conference.
- Basic Features: live dialpad, dial plan, hotline, caller identity, auto answer.

Codecs and Voice Features

- Wideband codec: G.722, SILK_WB
- Narrowband codec: G.711, G.726, G.729, iLBC, G723, SILK_NB
- VAD, CNG, AEC, PLC, AJB, AGC
- Full-duplex speakerphone with AEC

Network Features

- NAT Traversal: STUN, TURN and ICE
- IP assignment: Static/DHCP
- VLAN assignment: LLDP/Static/DHCP/CDP
- Bridge mode for PC port
- HTTP/HTTPS server
- DNS client
- DHCP server
- IPv6 support

Management

- FTP/TFTP/HTTP/HTTPS auto-provision
- Configuration: browser/phone/auto-provision

Security

- HTTPS (server/client)
- Transport Layer Security (TLS)
- VLAN (802.1q), QoS
- Digest authentication using MD5/MD5-sess
- Secure configuration file via AES encryption
- Phone lock for personal privacy protection
- Admin/User configuration mode
- 802.1x authentication
- Incoming signaling validation

Getting Started

What IP Phones Need to Meet

In order to operate in a network successfully, Skype for Business phones require the following:

- A working IP network
- The latest firmware for Skype for Business phones
- An active and configured Skype for Business server

Initialization Process Overview

The initialization process of the phone is required for network connectivity and operation of the phone on a local network.

Once the phone is connected to the network via a power over Ethernet (PoE) connection, the phone begins its initialization process.

During the initialization process, the following events take place:

Load the ROM file

The ROM file resides in the flash memory of the phone and comes preloaded. During initialization, the phone runs a bootstrap loader that loads and executes the ROM file.

Configure the VLAN

If the phone is connected to a switch, the switch notifies the phone of the VLAN information defined on the switch (if using LLDP or CDP). The phone can then proceed with the DHCP request for its network settings (if using DHCP). For more information on VLAN, refer to “VLAN” on page 44.

Query the DHCP (Dynamic Host Configuration Protocol) Server

The Skype for Business phone is capable of querying a DHCP server. DHCP is enabled on the phone by default. The following network parameters can be obtained from the DHCP server during initialization:

- IP Address
- Subnet Mask
- Gateway
- Primary DNS (Domain Name Server)
- Secondary DNS

The phone’s network parameters must be configured manually if they are not supplied by the DHCP server. For more information on configuring network parameters manually, refer to “Configure Network Parameters Manually” on page 28.

Contact the Provisioning Server

If the phone is configured to obtain configurations from the provisioning server, it will connect to the provisioning server and download the configuration file(s) during startup. The phone will be able to resolve and update configurations written in the configuration file(s). If the phone does not obtain configurations from the provisioning server, the phone will use configurations stored in the flash memory. For more information, refer to "Set Up Phones with a Provisioning Server" on page 81.

Update Firmware

If the access URL of firmware is defined in the configuration file, the phone will download firmware from the provisioning server. If the MD5 value of the downloaded firmware file differs from that of the image stored in the flash memory, the phone will perform a firmware update.

Firmware can be manually upgraded if the phone does not download firmware from the provisioning server. For more information, refer to "Upgrade Firmware" on page 90.

Download the Resource Files

In addition to configuration file(s), the phone may require resource files before it can deliver service. These resource files are optional, but if some particular features are being deployed, these files are required. Language packs and ring tones are examples of resource files. For more information on resource files, refer to "Resource Files" on page 86.

Verify Startup

After connected to the power and network or a PoE connection, the phone begins the initializing process by cycling through the following steps:

1. The Power LED Indicator illuminates solid red.
2. The message "Welcome Initializing... please wait" appears on the LCD screen when the phone starts up. The phone enters the login screen.

Set Up a System

This section describes essential information on how to set up a phone network and phones with a provisioning server. It also provides instructions on how to set up a provisioning server, how to deploy phones from the provisioning server, how to upgrade firmware, and how to keep user personalized settings after auto provisioning.

This section provides the following information:

- Set Up a Phone Network
- Set Up Phones with a Provisioning Server

Set Up a Phone Network

These phones operate on an Ethernet local area network (LAN) which varies by organization and can be configured to accommodate a number of network designs.

In order to get your phones operating, basic network setup, such as IP address and subnet mask configuration must be performed. The IPv4 or IPv6 network parameters for the phone must be configured. The appropriate security (VLAN and/or 802.1x authentication) and Quality of Service (QoS) settings can also be configured for the phone.

This section describes how to configure all the network parameters for phones, and it provides information on the following topics:

- DHCP
- DHCP Option
- Configuring Network Parameters Manually
- Configuring Transmission Methods of the Internet Port and PC Port
- Configuring PC Port Mode
- Web Server Type
- VLAN
- IPv6 Support
- Quality of Service (QoS)
- 802.1x Authentication

DHCP

DHCP (Dynamic Host Configuration Protocol) is a network protocol used to dynamically allocate network parameters to network hosts. The automatic allocation of network parameters to hosts eases the administrative burden of maintaining an IP network. Skype for Business phones comply with the DHCP specifications documented in RFC 2131. If using DHCP, phones connected to the network become operational without having to be manually assigned IP addresses and additional network parameters.

DHCP can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	**<MAC>.cfg**	Configure DHCP on the phone. **Parameter:** static.network.internet_port.type
Local	Web User Interface	Configure DHCP on the phone. **Navigate to:** http://<phoneIPAddress>/servlet?p=network&q=load
	Phone User Interface	Configure DHCP on the phone.

Details of the Configuration Parameter

Parameter	Permitted Values	Default
static.network.internet_port.type	**0 or 2**	**0**

Description:

Configures the Internet (WAN) port type for IPv4.

0- DHCP

2- Static IP Address

Note: This feature works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6). If the parameter is changed, the phone will reboot to make the change take effect.

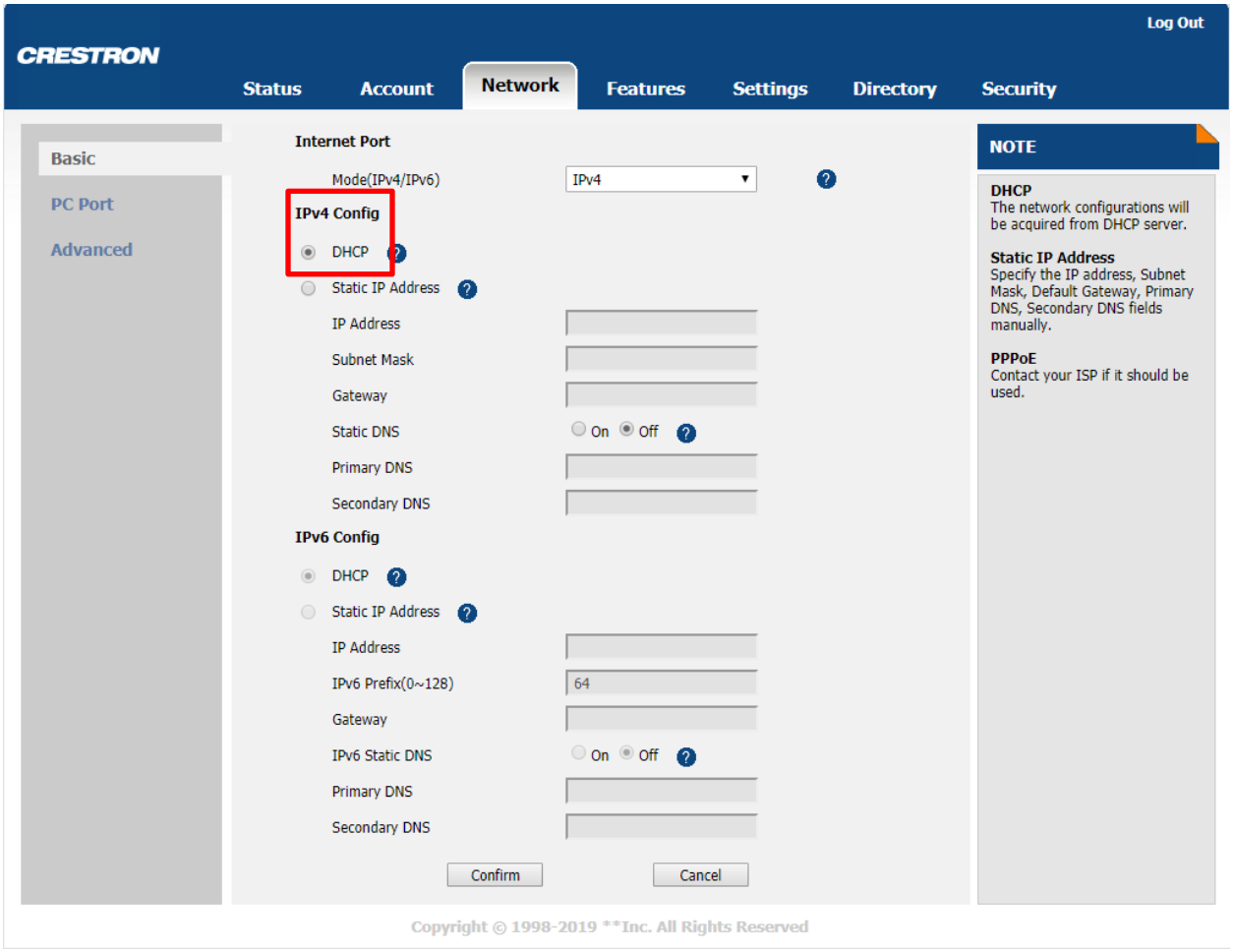
Web User Interface:
Network > Basic > IPv4 Config

Phone User Interface:
Menu > Setting > Advanced (default password: admin) > Network > WAN Port > IPv4

Configure via the Web User Interface

1. Click **Network** > **Basic**.

Network > Basic



2. In the **IPv4** section, select **DHCP.**
3. Click **Confirm** to accept the change. A dialog box pops up to prompt that settings will take effect after a reboot.
4. Click **OK** to reboot the phone.

Configure via the Phone User Interface

1. Tap **Setting** > **Advanced**.
2. Enter the Admin password (default password: admin), and then tap **OK**.
3. Tap **Network** on the left side of the display, and then tap **WAN Port**.
4. Tap **2. IPv4**.
5. Tap the value in the **1. Type** field, and then select **DHCP** from the drop-down list.

6. Tap **Save**.

Static DNS

Static DNS address(es) can be configured and used even though DHCP is enabled.

Static DNS can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the static DNS feature. **Parameter:** static.network.static_dns_enable
	<MAC>.cfg	Configure static DNS address. **Parameters:** static.network.primary_dns static.network.secondary_dns
Local	Web User Interface	Configure the static DNS feature. Configure static DNS address. **Navigate to:** http://<phoneIPAddress>/servlet?p=network&q=load
	Phone User Interface	Configure the static DNS feature. Configure static DNS address.

Details of the Configuration Parameters

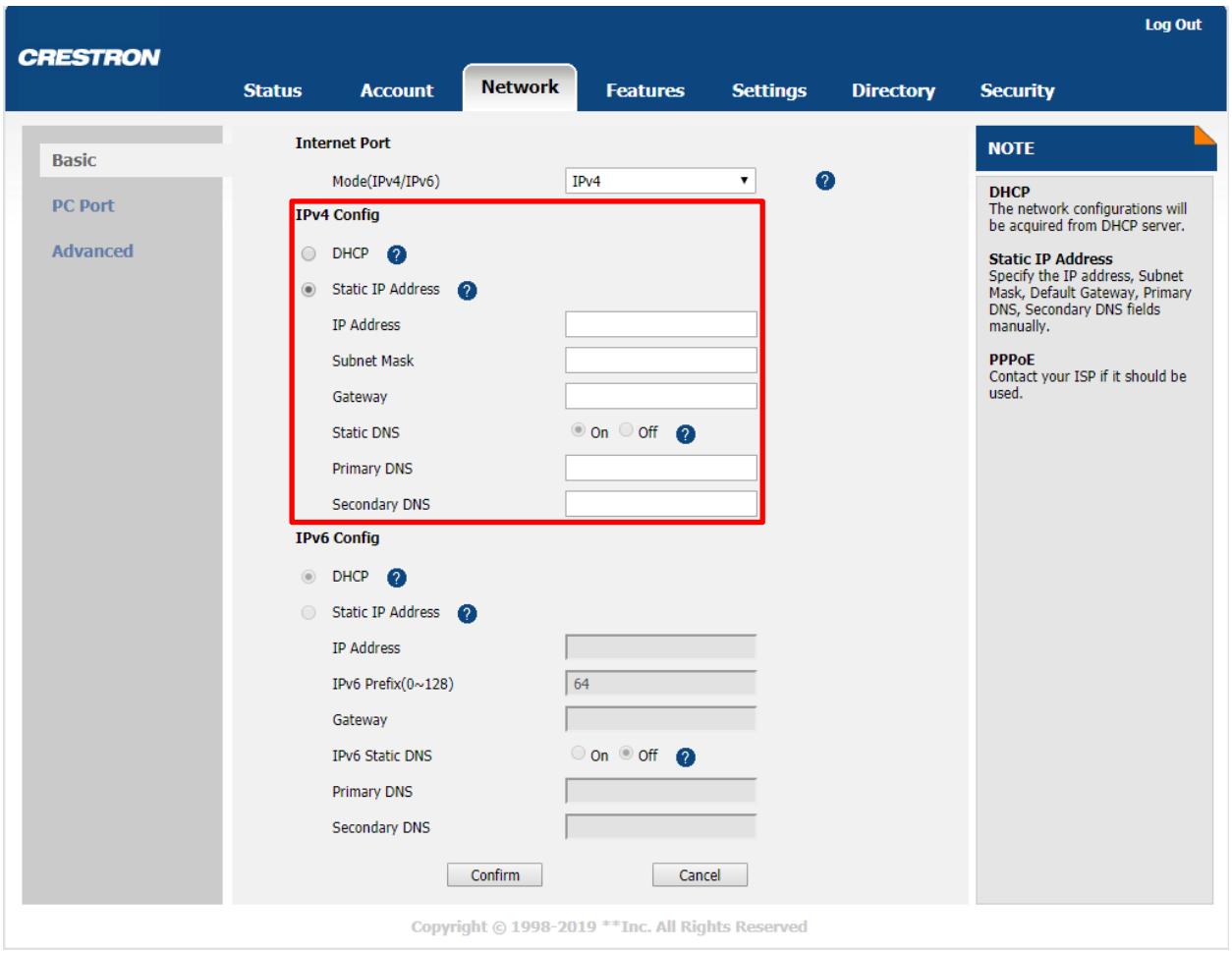
Parameter	Permitted Values	Default
static.network.static_dns_enable	**0 or1**	**0**
Description: Triggers the static DNS feature to on or off. **0**- Off, the phone will use the IPv4 DNS obtained from DHCP. **1**- On, the phone will use manually configured static IPv4 DNS. **Note:** This feature works only if the value of the parameter "static.network.internet_port.type" is set to 0 (DHCP). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Basic > IPv4 Config > Static DNS **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > WAN Port > IPv4 > Type (DHCP) > Static DNS		

Parameter	Permitted Values	Default
static.network.primary_dns	**IPv4 Address**	**Blank**
Description: Configures the primary IPv4 DNS server. **Example:** static.network.primary_dns = 202.101.103.55 **Note:** This feature works only if the value of the parameter "static.network.static_dns_enable" is set to 1 (On). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Basic > IPv4 Config > DHCP > Static DNS (On) > Primary DNS **Phone User Interface:** Menu > **Setting** > Advanced (default password: admin) > Network > WAN Port > IPv4 > Type (DHCP) > Static DNS (Enabled) > Primary DNS		
static.network.secondary_dns	**IPv4 Address**	**Blank**
Description: Configures the secondary IPv4 DNS server. **Example:** static.network.secondary_dns = 202.101.103.54 **Note:** This feature works only if the value of the parameter "static.network.static_dns_enable" is set to 1 (On). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Basic > IPv4 Config > DHCP > Static DNS (On) > Secondary DNS **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > WAN Port > IPv4 > Type (DHCP) > Static DNS (Enabled) > Secondary DNS		

Configure via the Web User Interface

1. Click **Network** > **Basic**.

Network > Basic



2. In the **IPv4 Config** section, select **DHCP.**
3. Set **Static DNS** to **On**.
4. Enter the DNS server addresses in the **Primary DNS** and **Secondary DNS** fields.
5. Click **Confirm** to accept the change. A dialog box pops up to prompt that settings will take effect after a reboot.
6. Click **OK** to reboot the phone.

Configure via the Phone User Interface

1. Tap **Setting** > **Advanced**
2. Enter the Admin password (default password: admin), and then tap **OK**.
3. Tap **Network** on the left side of the display, and then tap **WAN Port**.

4. Tap **2. IPv4**.
5. Tap the value in the **2. Static DNS** field, and then select **Enabled** from the drop-down list.
6. Enter the DNS server addresses in the **Pri. DNS** and **Sec. DNS** fields.
7. Tap **Save**.

DHCP Option

DHCP provides a framework for passing information to TCP/IP network devices. Network and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The data items themselves are also called options.

DHCP can be initiated by simply connecting the phone with the network. Skype for Business phones broadcast DISCOVER messages to request the network information carried in DHCP options, and the DHCP server responds with specific values in corresponding options.

The following table lists common DHCP options supported by phones.

Parameter	DHCP Option	Description
Subnet Mask	1	Specify the client's subnet mask.
Time Offset	2	Specify the offset of the client's subnet in seconds from Coordinated Universal Time (UTC).
Router	3	Specify a list of IP addresses for routers on the client's subnet.
Time Server	4	Specify a list of time servers available to the client.
Domain Name Server	6	Specify a list of domain name servers available to the client.
Log Server	7	Specify a list of MIT-LCS UDP servers available to the client.
Host Name	12	Specify the name of the client.
Domain Server	15	Specify the domain name that client should use when resolving hostnames via DNS.
Broadcast Address	28	Specify the broadcast address in use on the client's subnet.
Network Time Protocol Servers	42	Specify a list of NTP servers available to the client by IP address.
Vendor-Specific	43 (vendor class ID:CPE-OCPHONE)	Specify virtual local area network (VLAN) ID.
Information	43 (vendor class ID: MS-UC-Client)	Specify Skype for Business Server pool certificate provisioning service URL.

Parameter	DHCP Option	Description
Vendor Class Identifier	60	Identify the vendor type.
TFTP Server Name	66	Identify a TFTP server when the 'sname' field in the DHCP header has been used for DHCP options.
Boot file Name	67	Identify a boot file when the 'file' field in theDHCP header has been used for DHCP options.
Skype for Business Server	120	Specify a list of Skype for Business Servers available to the client.

For more information on DHCP options, refer to the Internet Engineering Task Force (IETF) specifications for RFC 2131 or RFC 2132 at ietf.org.

If DHCP options for automatically discovering the provisioning server address on the DHCP server cannot be configured, an alternate method is required. Connecting to the secondary DHCP server that responds to DHCP INFORM queries with a requested provisioning server address is one possibility. For more information, refer to the IETF specifications for RFC 3925. If a single alternate DHCP server responds, this is functionally equivalent to having the primary DHCP server respond with a valid provisioning server address. If no DHCP servers respond, the INFORM query process will retry and eventually time out.

DHCP Option 66 and Option 43

Skype for Business phones support obtaining the provisioning server address by detecting DHCP options during startup.

The phone will automatically detect option 66 for obtaining the provisioning server address. DHCP option 66 is used to identify the TFTP server. DHCP option 43 is a vendor-specific option, which is used to transfer the vendor-specific information.

The administrator can use vendor class identifier, specified by DHCP option 60, to send the phone a customized configuration in option 43. Depending on the vendor class ID it is configured for, the option 43 might have different values. Two vendor class identifiers are used when deploying with the Skype for Business Server: a VLAN ID request (vendor class ID: CPE- OCPHONE) and a certificate provisioning service URL request (vendor class ID: MS-UC-Client). For more information on DHCP option 60, refer to “DHCP Option 60” on page 21.

To use DHCP option 66 and option 43, make sure the **DHCP Active** feature is enabled.

DHCP Active can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure DHCP active. **Parameters:** static.auto_provision.dhcp_option.enable
Local	Web User Interface	Configure DHCP active. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-autop&q=load

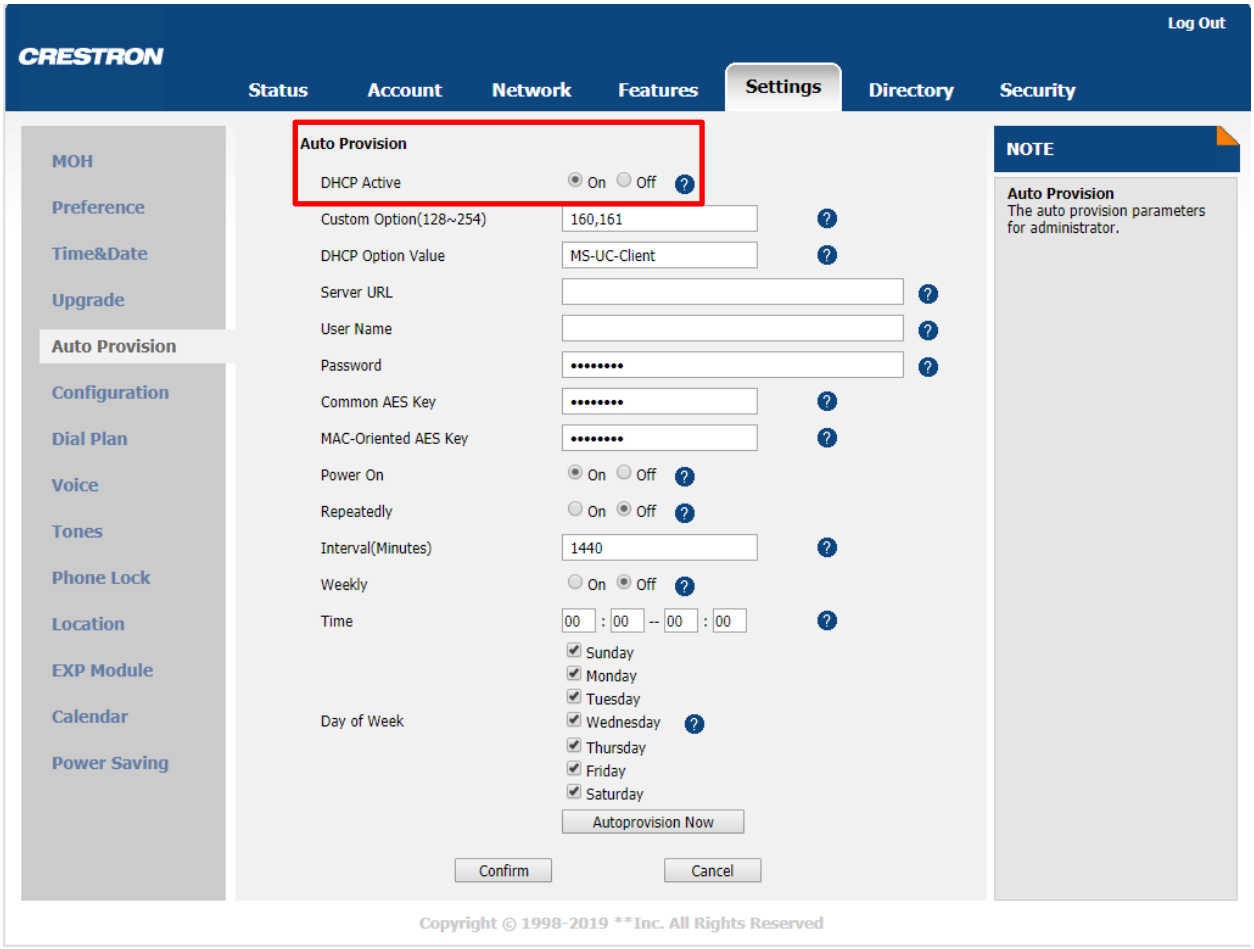
Details of the Configuration Parameter

Parameter	Permitted Values	Default
static.auto_provision.dhcp_option.enable	**0 or 1**	**1**
Description: Triggers the DHCP Active feature to on or off. **0**- Off **1**- On, the phone will obtain the provisioning server address by detecting DHCP options. **Web User Interface:** Settings > Auto Provision > DHCP Active **Phone User Interface:** None		

Configure via the Web User Interface

1. Click **Settings** > **Auto Provision**.

Settings > Auto Provision



2. In the **Auto Provision** section, set **DHCP Active** to **On**.
3. Click **Confirm** to accept the change.

DHCP Option 160 and Option 161

Skype for Business phones also support obtaining the provisioning server address by detecting a DHCP custom option during startup.

If DHCP Option 66 is not available, use a custom option (160 or 161) with the URL or IP address of the provisioning server. The phone will automatically detect option 160 or 161 for obtaining the provisioning server address.

To use DHCP option 160 or option 161, make sure the **DHCP Active** feature is enabled and custom option is configured.

DHCP Active can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure DHCP active. **Parameter:** static.auto_provision.dhcp_option.enable
		Configure the custom DHCP option for requesting provisioning server address. **Parameter:** static.auto_provision.dhcp_option.list_user_options
Local	Web User Interface	Configure the custom option. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-autop&q=load

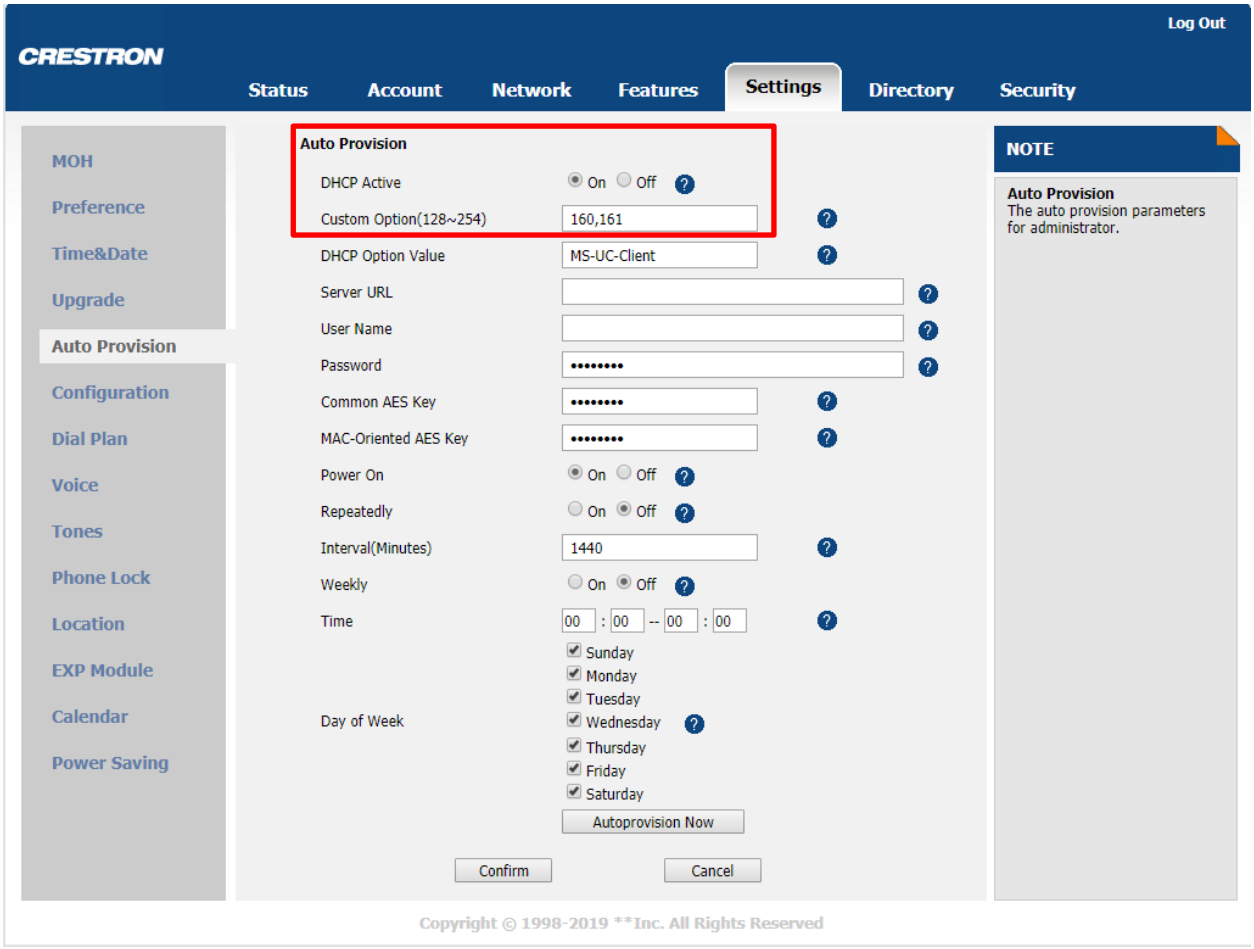
Details of the Configuration Parameters

Parameter	Permitted Values	Default
static.auto_provision.dhcp_option.enable	**0 or 1**	**1**
Description: Triggers the DHCP Option feature to on or off. **0**- Off **1**- On, the phone will obtain the provisioning server address by detecting DHCP options. **Web User Interface:** Settings > Auto Provision > DHCP Active **Phone User Interface:** None		
static.auto_provision.dhcp_option.list_user_options	**Integer from 128 to 254**	**160,161**
Description: Configures the custom DHCP option for requesting the provisioning server address. Multiple DHCP options are separated by commas. **Note**: This feature works only if the value of the parameter "static.auto_provision.dhcp_option.enable" is set to 1 (On). **Web User Interface:** Settings > Auto Provision > Custom Option(128~254) **Phone User Interface:** None		

Configure via the Web User Interface

1. Click **Settings** > **Auto Provision**.

Settings > Auto Provision



2. In the **Auto Provision** section, set **DHCP Active** to **On**.
3. Enter the custom option (**160** or **161**) in the **Custom Option(128~254)** field.
4. Click **Confirm** to accept the change.

NOTE: The phones also support obtaining the provisioning server address via Skype for Business Server (if configured) during the sign-in process. This method for obtaining provisioning server address has higher priority than the DHCP option.

DHCP Option 60

DHCP option 60 is used to identify the vendor class ID. By default, the vendor class ID is MS- UC-Client (case-sensitive).

DHCP option 60 can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure DHCP option 60. **Parameters:** static.auto_provision.dhcp_option.option60_value
Local	Web User Interface	Configure DHCP option 60. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-autop&q=load

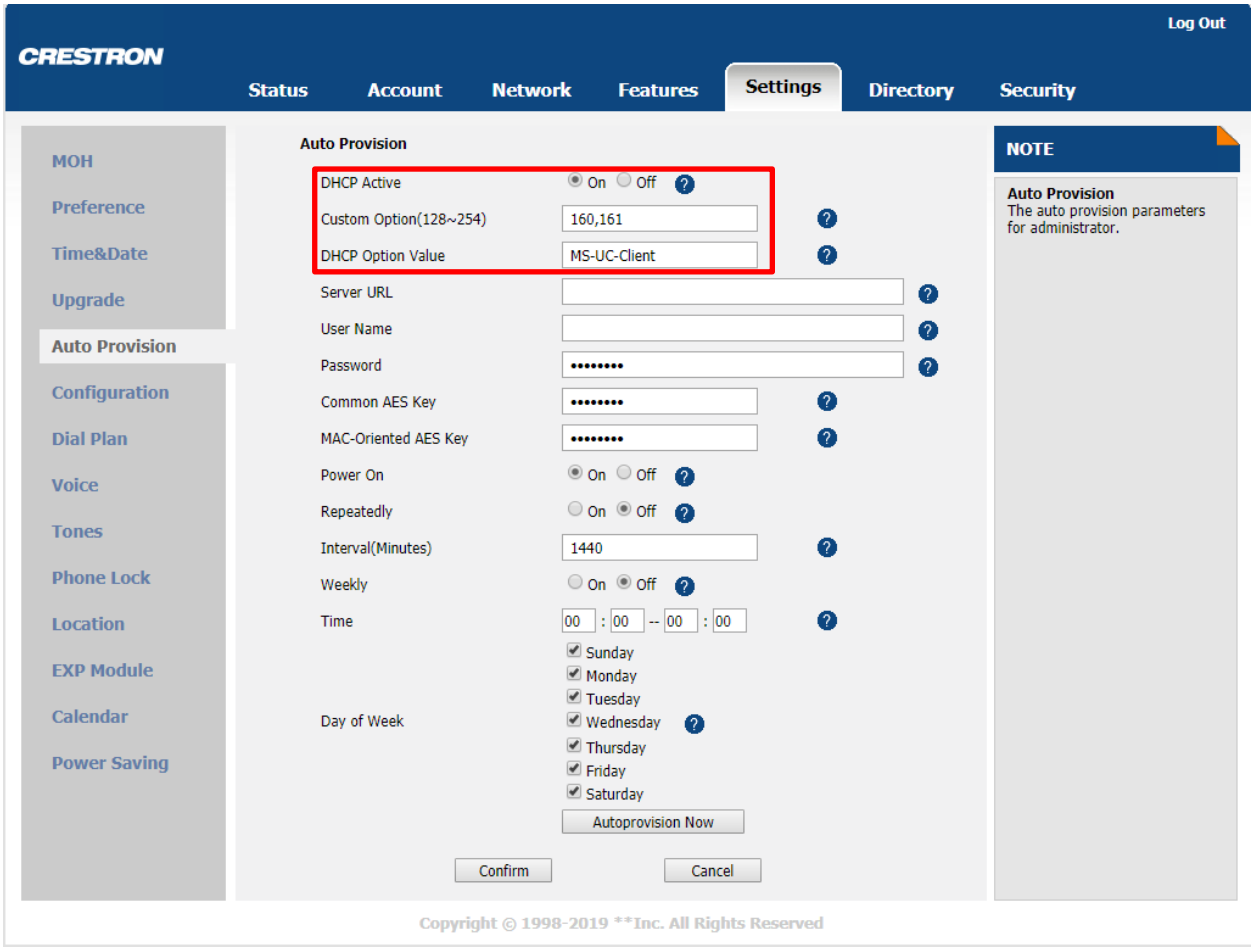
Details of the Configuration Parameter

Parameter	Permitted Values	Default
static.auto_provision.dhcp_option.option60_value	**String within 99 characters**	**MS-UC-Client**
Description: Configures the value (vendor class ID) of DHCP option 60. **Web User Interface:** Settings > Auto Provision > DHCP Option Value **Phone User Interface:** None		

Configure via the Web User Interface

1. Click **Settings** > **Auto Provision**.

Settings > Auto Provision



2. In the **Auto Provision** section, set **DHCP Active** to **On**.
3. Enter the host name in the **DHCP Option Value** field.
4. Click **Confirm** to accept the change.

DHCP Option 42 and Option 2

Skype for Business phones support using the NTP server address offered by DHCP. DHCP option 42 is used to specify a list of NTP servers available to the client by IP address. NTP servers should be listed in order of preference. DHCP option 2 is used to specify the offset of the client's subnet in seconds from Coordinated Universal Time (UTC).

To update time with the offset time offered by the DHCP server, make sure the **DHCP Time** feature is enabled at the path **Settings** > **Time & Date** > **DHCP Time**. For more information on how to configure the DHCP time feature, refer to "NTP Time Server" on page 136.

DHCP Option 12 Hostname

This option specifies the host name of the phone. The name may or may not be qualified with the local domain name (based on RFC 2132). See RFC 1035 for character restrictions.

DHCP option 12 hostname can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the DHCP option 12 hostname. **Parameter:** static.network.dhcp_host_name
Local	Web User Interface	Configure the DHCP option 12 hostname. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

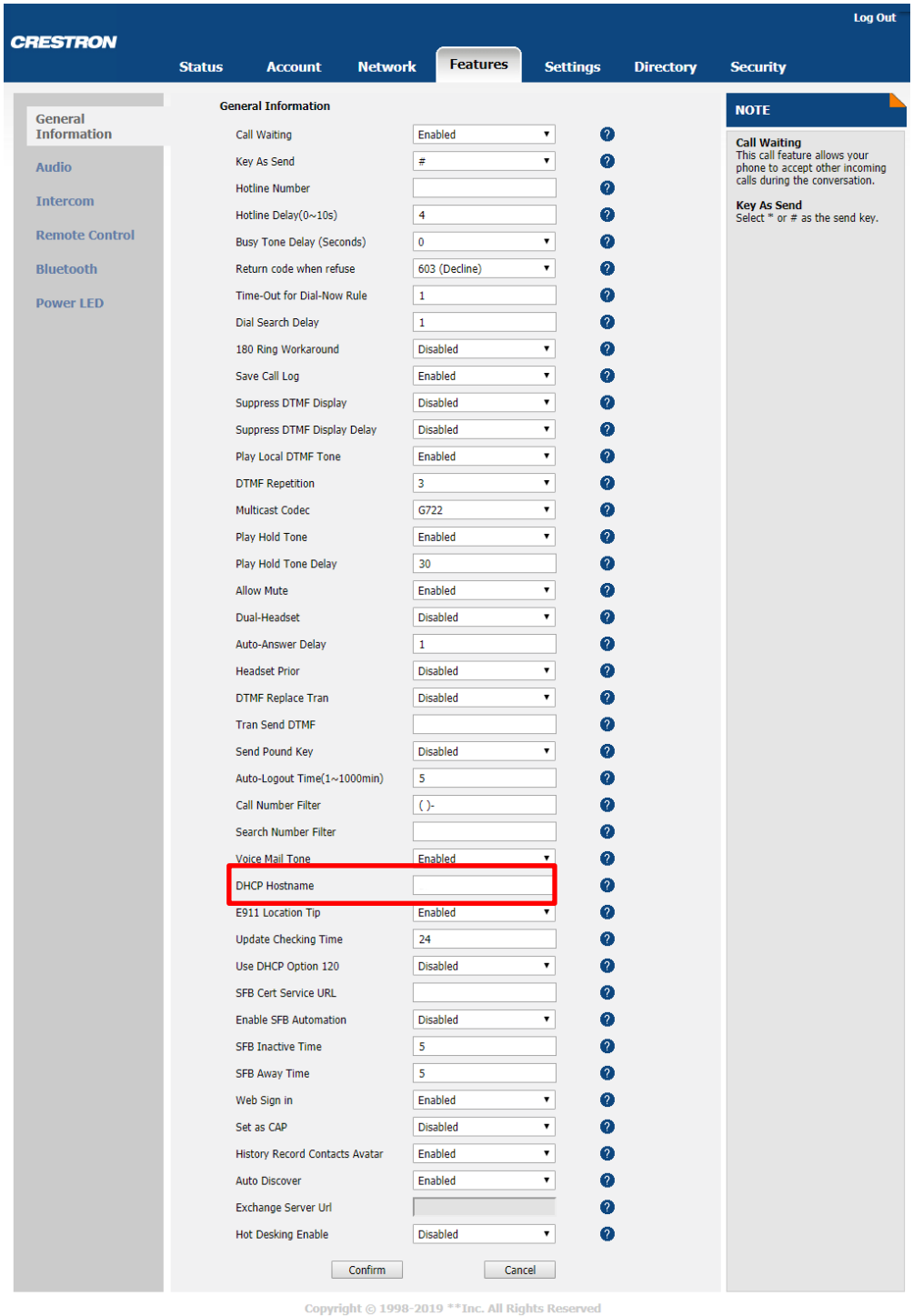
Details of the Configuration Parameter

PARAMETER	Permitted Values	Default
static.network.dhcp_host_name	**String within 99 characters**	**Refer to the following content**
Description: Configures the DHCP option 12 hostname on the phone. **Web User Interface:** Features > General Information > DHCP Hostname **Phone User Interface:** None		

Configure via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Enter the host name in the **DHCP Hostname** FIELD.

3. Click **Confirm** to accept the change. A dialog box pops up to prompt that settings will take effect after a reboot.
4. Click **OK** to reboot the phone.

DHCP Option 120

Skype for Business phones support obtaining Skype for Business Server address from DHCP. DHCP option 120 is used to specify a list of Skype for Business Servers available to the client.

DHCP option 120 can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure DHCP option 120. **Parameter:** sip.option120_get_lync_server.enable
Local	Web User Interface	Configure DHCP option 120. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

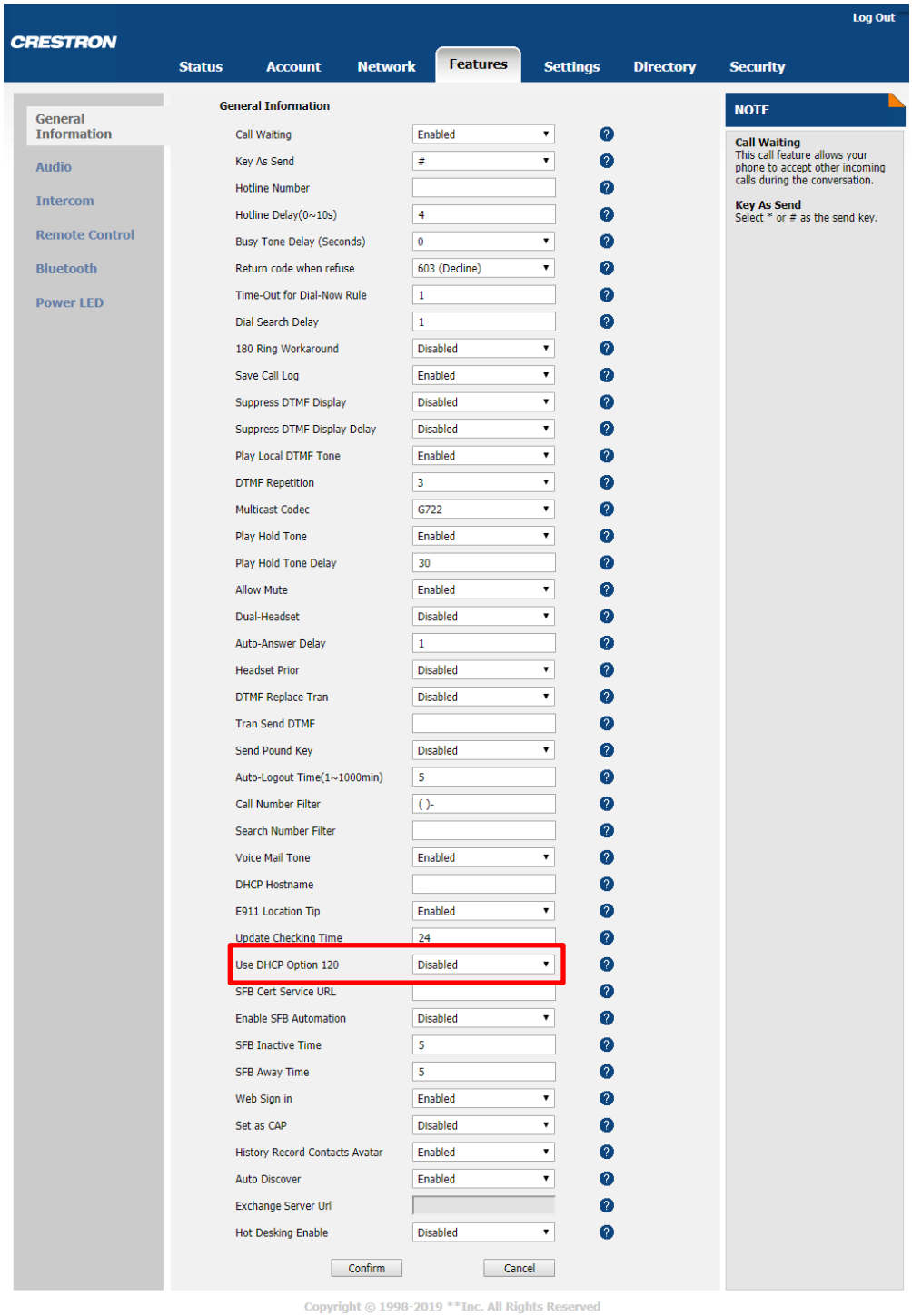
Details of the Configuration Parameter

Parameter	Permitted Values	Default
sip.option120_get_lync_server.enable	**0 or 1**	**0**
Description: Enables or disables phones to obtain the Skype for Business Server address from DHCP by detecting DHCP option 120. **0**- Disabled **1**- Enabled **Web User Interface:** Features > General Information > Use DHCP Option 120 **Phone User Interface:** None		

Configure via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Select **Enabled** or **Disabled** from the **Use DHCP Option 120** drop-down list.

3. Click **Confirm** to accept the change.

Configure Network Parameters Manually

If DHCP is disabled or the phone cannot obtain network parameters from the DHCP server, the parameters must be configured manually. The following parameters should be configured for phones to establish network connectivity.

- IP Address
- Subnet Mask
- Default Gateway
- Primary DNS
- Secondary DNS

Network parameters can be configured manually using the configuration files or locally.

Central Provisioning (Configuration File)	**<MAC>.cfg**	Configure network parameters of the phone manually. **Parameters:** static.network.internet_port.type static.network.ip_address_mode static.network.internet_port.ip static.network.internet_port.mask static.network.internet_port.gateway static.network.primary_dns static.network.secondary_dns
Local	Web User Interface	Configure network parameters of the phone manually. **Navigate to**: http://<phoneIPAddress>/servlet?p=network&q=load
	Phone User Interface	Configure network parameters of the phone manually.

Details of the Configuration Parameters

Parameter	Permitted Values	Default
static.network.internet_port.type	**0 or 2**	**0**
Description: Configures the Internet (WAN) port type for IPv4. **0**- DHCP **2**- Static IP Address **Note:** This feature works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Basic > IPv4 Config **Phone User Interface:** Menu > Setting **>** Advanced (default password: admin) > Network > WAN Port > IPv4 > Type		
static.network.ip_address_mode	**0, 1 or 2**	**0**
Description: Configures the IP address mode. **0**- IPv4 **1**- IPv6 **2**- IPv4 & IPv6 **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Basic > Internet Port > Mode(IPv4/IPv6) **Phone User Interface:** Menu > Setting **>** Advanced (default password: admin) > Network > WAN Port > IP Mode		
static.network.internet_port.ip	**IPv4 Address**	**Blank**
Description: Configures the IPv4 address. **Example:** static.network.internet_port.ip = 192.168.1.20 **Note:** This feature works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.network.internet_port.type" is set to 2 (Static IP Address). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Basic > IPv4 Config > Static IP Address > IP Address **Phone User Interface:** Menu > Setting **>** Advanced (default password: admin) > Network > WAN Port > IPv4 > Type (Static IP) > IP Address		

Parameter	Permitted Values	Default
static.network.internet_port.mask	**Subnet Mask**	**Blank**
Description: Configures the IPv4 subnet mask. **Example:** static.network.internet_port.mask = 255.255.255.0 **Note:** This feature works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.network.internet_port.type" is set to 2 (Static IP Address). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Basic > IPv4 Config > Static IP Address > Subnet Mask **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > WAN Port > IPv4 > Type (Static IP) > Subnet Mask		
static.network.internet_port.gateway	**IPv4 Address**	**Blank**
Description: Configures the IPv4 default gateway. **Example:** static.network.internet_port.gateway = 192.168.1.254 **Note:** This feature works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.network.internet_port.type" is set to 2 (Static IP Address). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Basic > IPv4 Config > Static IP Address > Gateway **Phone User Interface:** Menu > Setting **>** Advanced (default password: admin) > Network > WAN Port > IPv4 > Type(Static IP) > Gateway		
static.network.primary_dns	**IPv4 Address**	**Blank**
Description: Configures the primary IPv4 DNS server. **Example:** static.network.primary_dns = 202.101.103.55 **Note:** This feature works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.network.internet_port.type" is set to 2 (Static IP Address). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Basic > IPv4 Config > Static IP Address > Static DNS (On) > Primary DNS **Phone User Interface:** Menu > Setting **>** Advanced (default password: admin) > Network > WAN Port > IPv4 > Type(Static IP) > Primary DNS		

Parameter	Permitted Values	Default
static.network.secondary_dns	IPv4 Address	Blank

Description:

Configures the secondary IPv4 DNS server.

Example:
static.network.secondary_dns = 202.101.103.54

Note: This feature works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.network.internet_port.type" is set to 2 (Static IP Address). If the parameter is changed, the phone will reboot to make the change take effect.

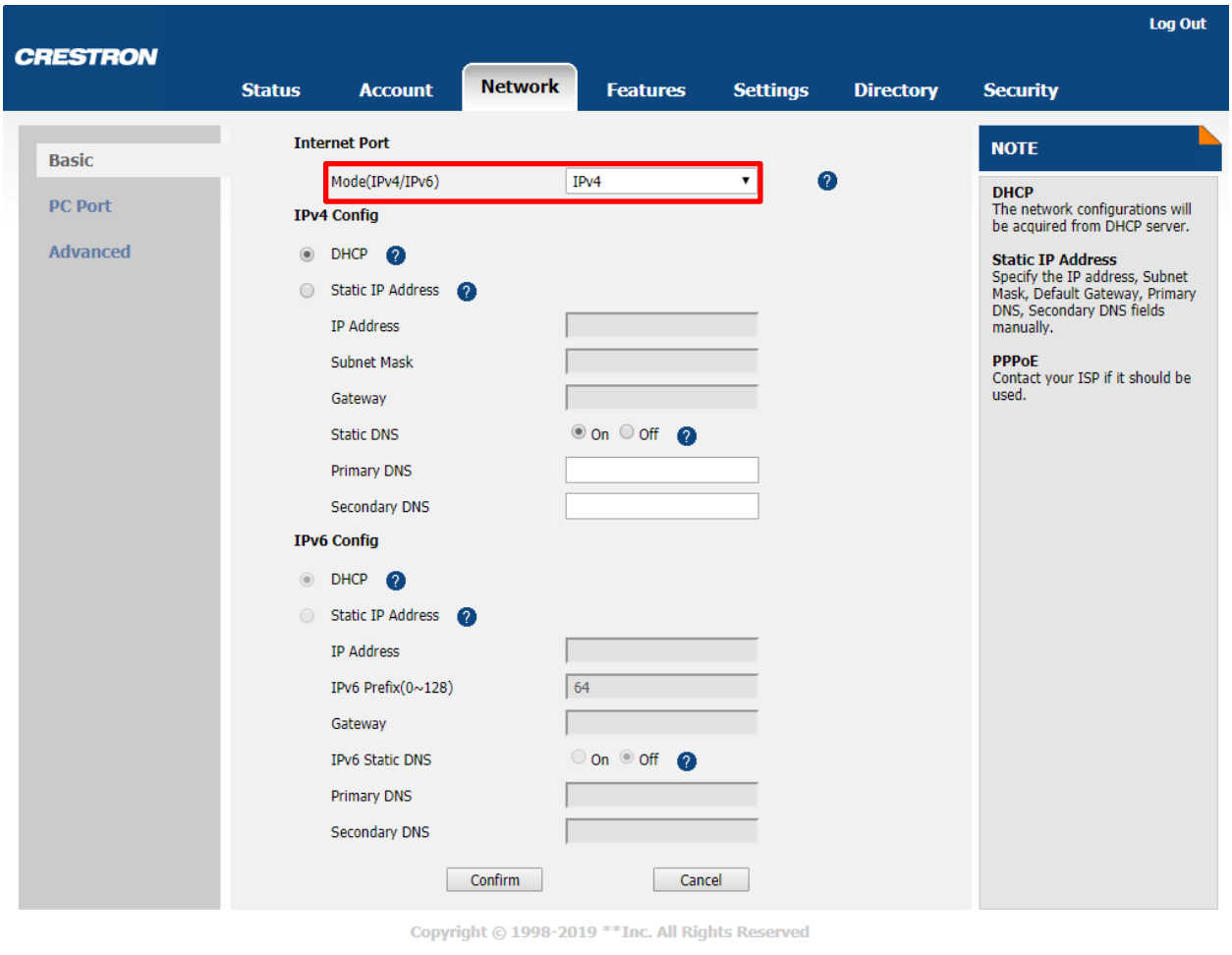
Web User Interface:
Network > Basic > IPv4 Config > Static IP Address > Static DNS (On) > Secondary DNS

Phone User Interface:
Menu > Setting > Advanced (default password: admin) > Network > WAN Port > IPv4 > Type(Static IP) > Secondary DNS

Configure the IP Address Mode via the Web User Interface

1. Click **Network** > **Basic**.

Network > Basic

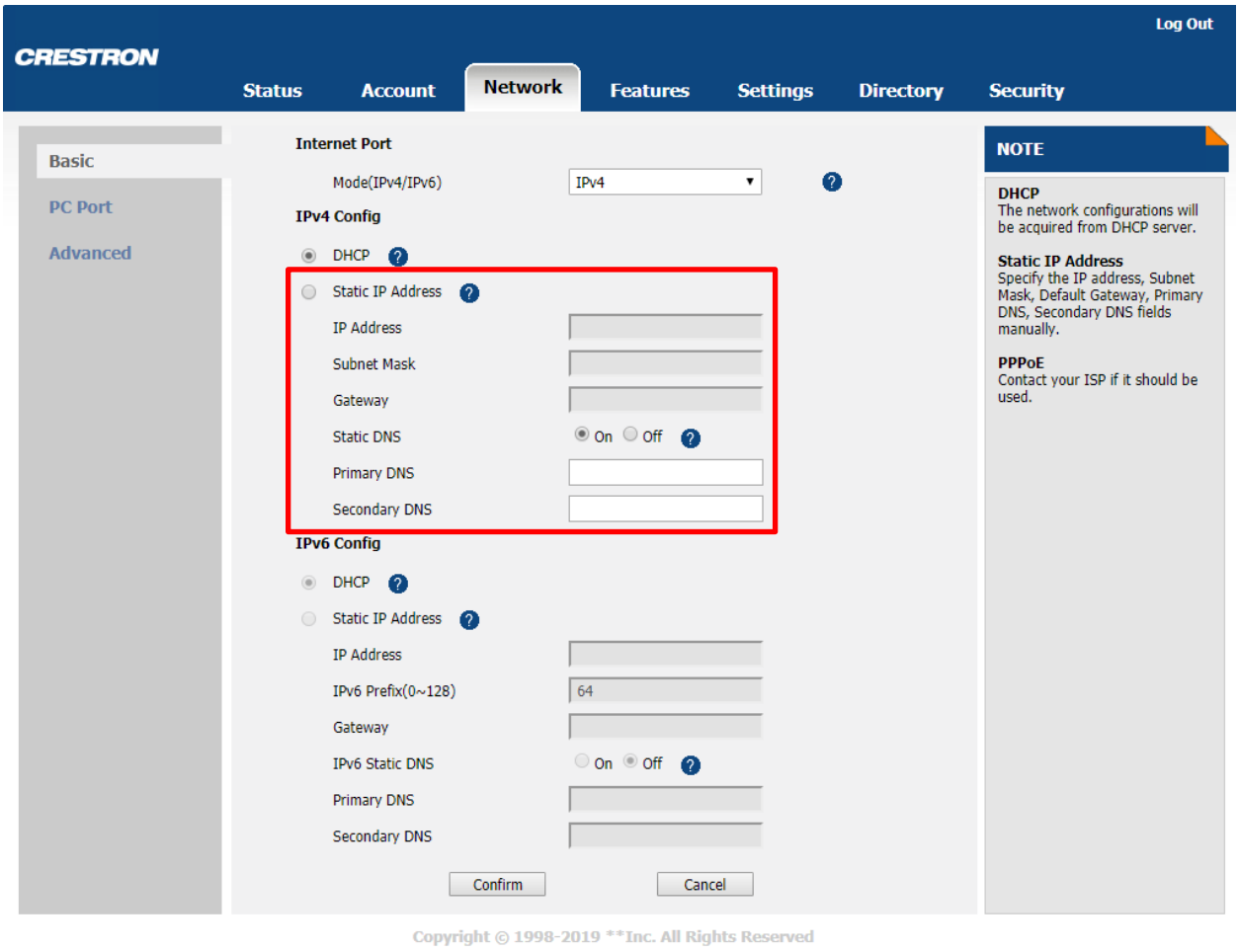


2. Select **IPv4** or **IPv6** from the **Mode(IPv4/IPv6)** drop-down list.
3. Click **Confirm** to accept the change. A dialog box pops up to prompt that settings will take effect after a reboot.
4. Click **OK** to reboot the phone.

Configure a Static IPv4 Address via the Web User Interface

1. Click **Network** > **Basic**.

Network > Basic



2. In the **IPv4 Config** section, select **Static IP Address**.
3. Enter the IP Address, Subnet Mask, Gateway, Primary DNS and Secondary DNS in the **IP Address**, **Subnet Mask**, **Gateway**, **Primary DNS** and **Secondary DNS** fields.
4. Click **Confirm** to accept the change. A dialog box pops up to prompt that settings will take effect after a reboot.
5. Click **OK** to reboot the phone.

Configure the IP Mode via the Phone User Interface

1. Tap **Setting** > **Advanced**
2. Enter the Admin password (default password: admin), and then tap **OK**.
3. Tap **Network** on the left side of the display, and then tap **WAN Port**.
4. Tap the value in the **1. Type** field, and then select **IPv4, IPv6**, or **IPv4 & IPv6** from the **1. IP Mode** drop-down list

Configure a Static IPv4 Address via the Phone User Interface

1. Tap **Setting** > **Advanced**
2. Enter the Admin password (default password: admin), and then tap **OK**.
3. Tap **Network** on the left side of the display, and then tap **WAN Port**.
4. Tap **2. IPv4**.
5. Tap the value in the **1. Type** field, and then select **Static IP**.
6. Enter the IP Address, Subnet Mask, Gateway, Primary DNS and Secondary DNS in the **IP Address**, **Subnet Mask**, **Gateway**, **Pri. DNS** and **Sec. DNS** fields.
7. Tap **Save**.

Configure Transmission Methods of the Internet Port and PC Port

Skype for Business phones support two Ethernet ports: **Internet** port and **PC** port. There are three optional methods of transmission configuration for phone Internet or PC Ethernet ports.

- Auto-negotiate
- Half-duplex
- Full-duplex

By default, the Internet and PC ports are set to **Auto-negotiate**.

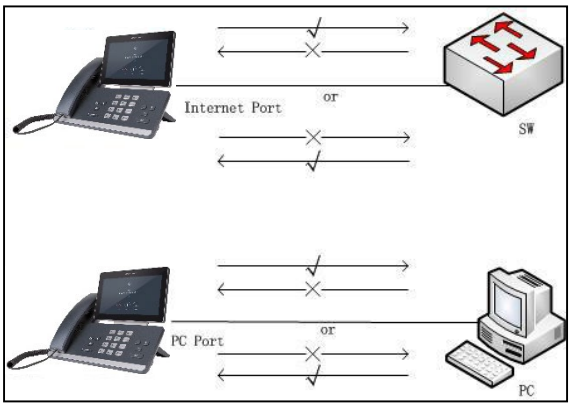
Autonegotiate

Autonegotiate means that two connected devices choose common transmission parameters (e.g., speed and duplex mode) to transmit voice or data over Ethernet. This process entails devices first sharing transmission capabilities and then selecting the highest performance transmission mode supported by both. The phone's Internet port and PC port can be configured to automatically negotiate during the transmission.

Half-duplex

Half-duplex transmission refers to transmitting voice or data in both directions, but in one direction at a time; this means one device can send data on the line, but not receive data simultaneously. Half-duplex transmission can be configured on the Internet port and PC port for the phone to transmit in 10Mbps or 100Mbps.

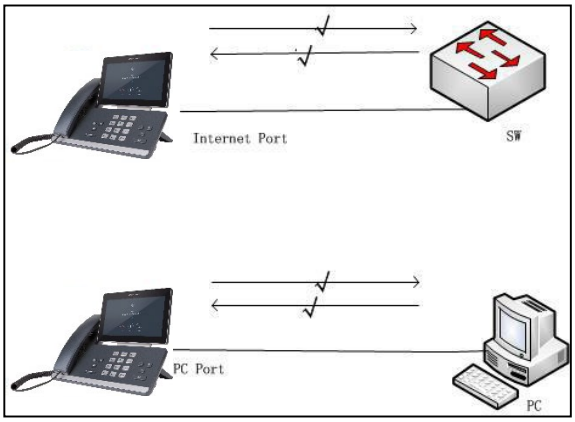
Half-duplex



Full-duplex

Full-duplex transmission refers to transmitting voice or data in both directions at the same time; this means one device can send data on the line while receiving data. Full-duplex transmission can be configured on the Internet port and PC port for the phone to transmit in 10Mbps, 100Mbps or 1000Mbps.

Full-duplex



The transmission methods of Ethernet ports can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the transmission methods of the Internet (WAN) port. **Parameters**: static.network.internet_port.speed_duplex static.network.pc_port.speed_duplex
Local	Web User Interface	Configure the transmission methods of the Internet (WAN) port. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load

Details of the Configuration Parameters

Parameter	Permitted Values	Default
static.network.internet_port.speed_duplex	**0, 1, 2, 3, 4 or 5**	**0**

Description:

Configures the transmission method of the Internet (WAN) port.

0- Auto Negotiate

1- Full Duplex 10Mbps

2- Full Duplex 100Mbps

3- Half Duplex 10Mbps

4- Half Duplex 100Mbps

5- Full Duplex 1000Mbps

Note: The transmission speed can be set to 1000Mbps/Auto Negotiation to transmit in 1000Mbps if the phone is connected to a switch that supports Gigabit Ethernet. This parameter should not be changed. If the parameter is changed, the phone will reboot to make the change take effect.

Web User Interface:
Network > Advanced > Port Link > WAN Port Link

Phone User Interface:
None

Parameter	Permitted Values	Default
static.network.pc_port.speed_duplex	0, 1, 2, 3 ,4 or 5	0

Description:

Configures the transmission method of the PC (LAN) port.

0- Auto Negotiate

1- Full Duplex 10Mbps

2- Full Duplex 100Mbps

3- Half Duplex 10Mbps

4- Half Duplex 100Mbps

5- Full Duplex 1000Mbps

Note: This setting works only if the value of the parameter "static.network.pc_port.enable" is set to 1 (Auto Negotiation). The transmission speed can be set to 1000Mbps/Auto Negotiation to transmit in 1000Mbps if the phone is connected to a switch that supports Gigabit Ethernet. This parameter should not be changed. If the parameter is changed, the phone will reboot to make the change take effect.

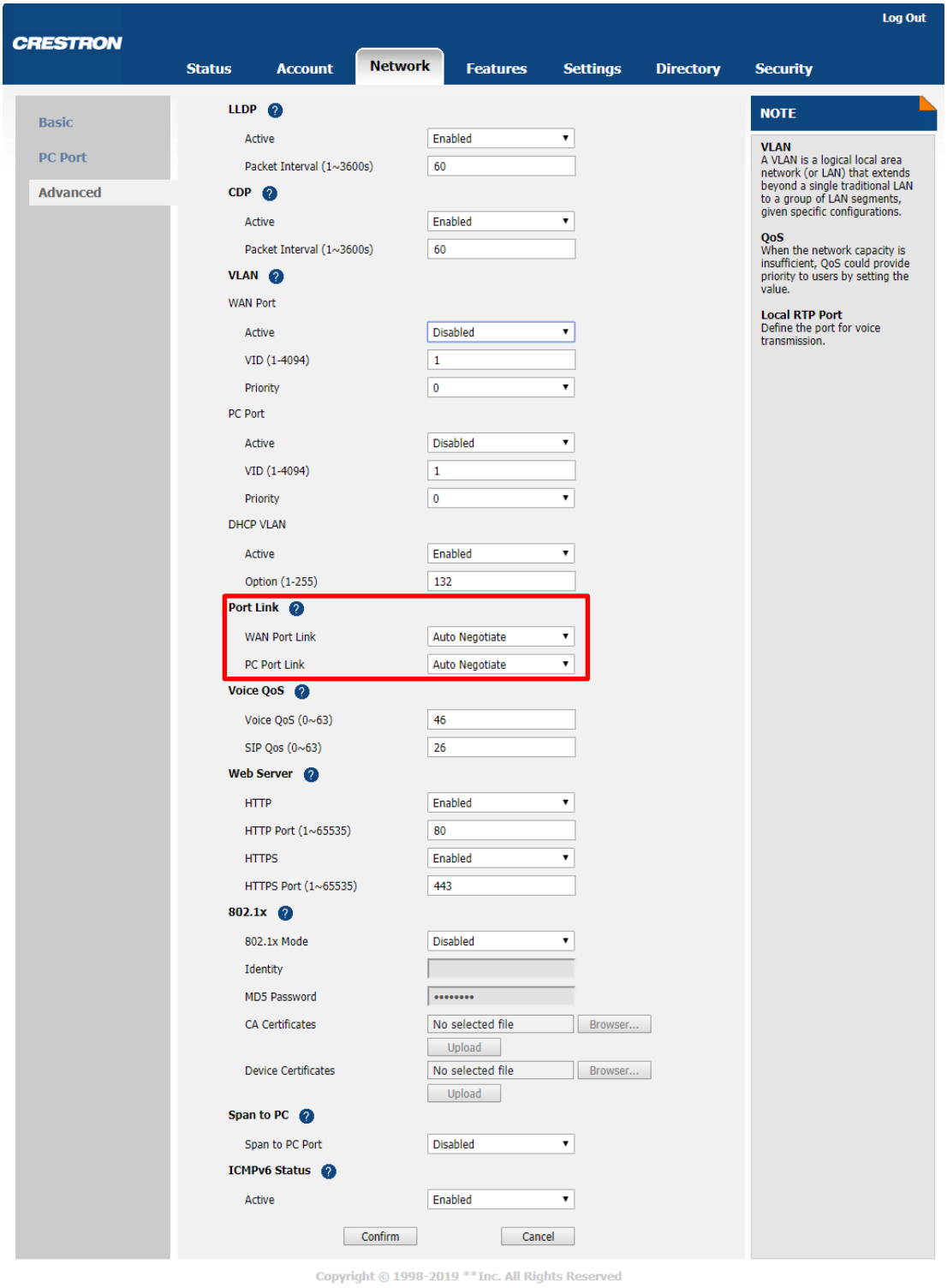
Web User Interface:
Network > Advanced > Port Link > PC Port Link

Phone User Interface:
None

Configure via the Web User Interface

1. Click **Network** > **Advanced**.

Network > Advanced



2. Select the desired setting from the **WAN Port Link** drop-down list.
3. Select the desired setting from the **PC Port Link** drop-down list.
4. Click **Confirm** to accept the change.

Configure PC Port Mode

The PC port on the back of the phone is used to connect a PC. The PC (LAN) port can be enabled or disabled via a web user interface or using configuration files.

PC port mode can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the PC (LAN) port. **Parameter:** static.network.pc_port.enable
Local	Web User Interface	Configure the PC (LAN) port. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-pcport&q=load

Details of the Configuration Parameter

Parameter	Permitted Values	Default
static.network.pc_port.enable	**0 or 1**	**1**
Description: Enables or disables the PC port. **0**- Disabled **1**- Auto Negotiation **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > PC Port > PC Port Active **Phone User Interface:** None		

Enable the PC Port via the Web User Interface

1. Click **Network** > **PC Port**.

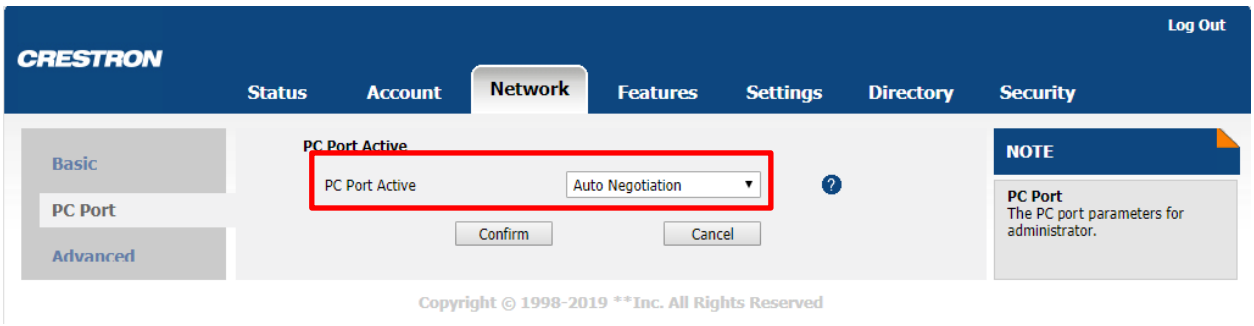
Network > PC Port

2. Select **Auto Negotiate** from the **PC Port Active** drop-down list.
3. Click **Confirm** to accept the change. A dialog box pops up to prompt that settings will take effect after a reboot.
4. Click **OK** to reboot the phone.

Disable the PC Port via the Web User Interface

1. Click **Network** > **PC Port**.

Network > PC Port



2. Select **Disabled** from the **PC Port Active** drop-down list.
3. Click **Confirm** to accept the change. A dialog box pops up to prompt that settings will take effect after a reboot.
4. Click **OK** to reboot the phone.

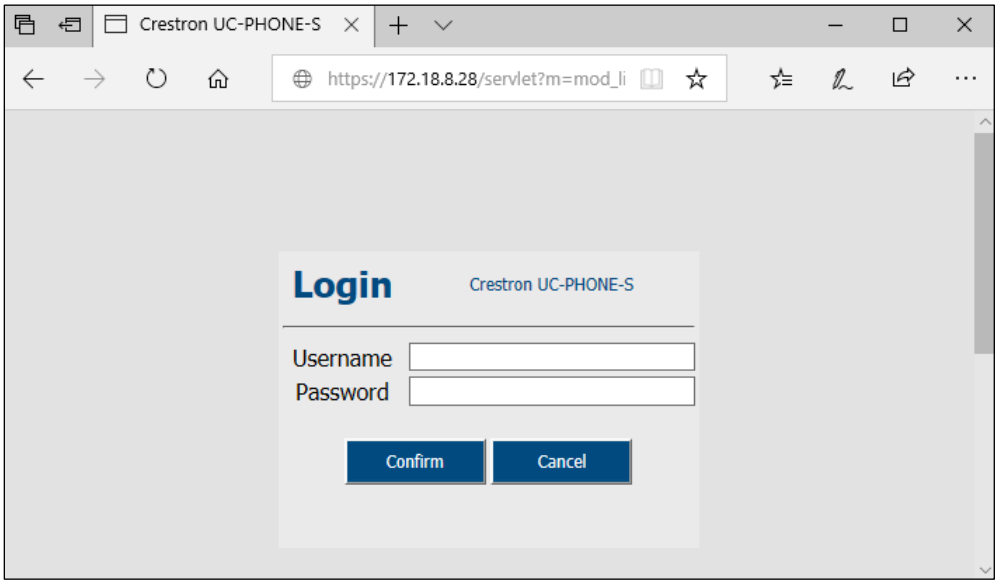
Web Server Types

The web server type determines the access protocol of the phone's web user interface. Skype for Business phones support both HTTP and HTTPS protocols for accessing the web user interface. This can be disabled when it is not needed or when it poses a security threat.

HTTP is an application protocol that runs on top of the TCP/IP suite of protocols. HTTPS is a web protocol that encrypts and decrypts user page requests as well as pages returned by the web server. Both HTTP and HTTPS port numbers are configurable.

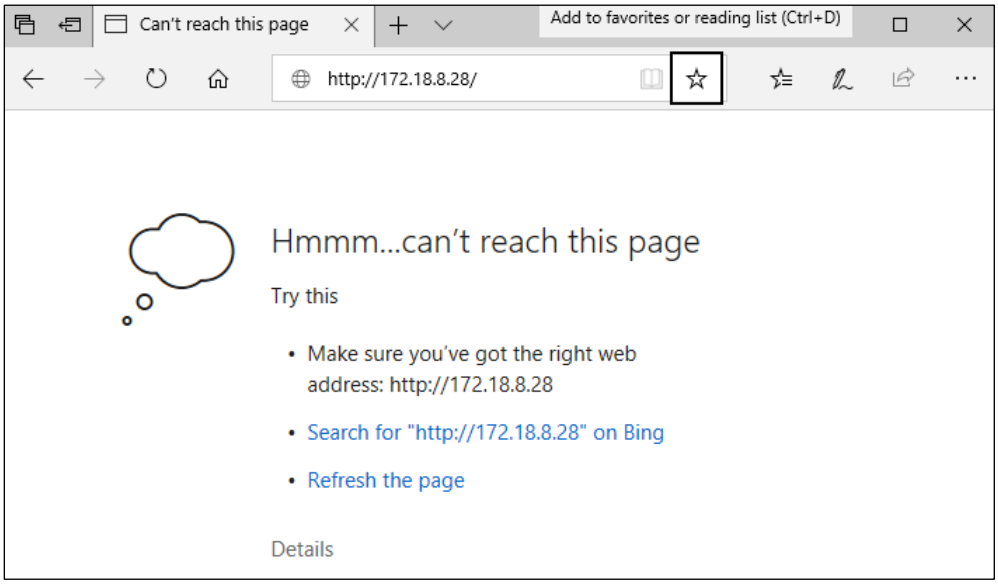
When access to the phone's web user interface using the HTTP/HTTPS protocol is enabled, the following screen is shown when accessing the web user interface.

Login page



When access to the phone's web user interface using the HTTP/HTTPS protocol is disabled, the following screen is shown when accessing the web user interface.

HTTP/HTTPS Protocol Disabled



Web server type can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the web access type, HTTP port and HTTPS port. **Parameters:** static.wui.http_enable static.network.port.http static.wui.https_enable static.network.port.https
Local	Web User Interface	Configure the web access type, HTTP port and HTTPS port. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load
	Phone User Interface	Configure the web access type, HTTP port and HTTPS port.

Details of the Configuration Parameters

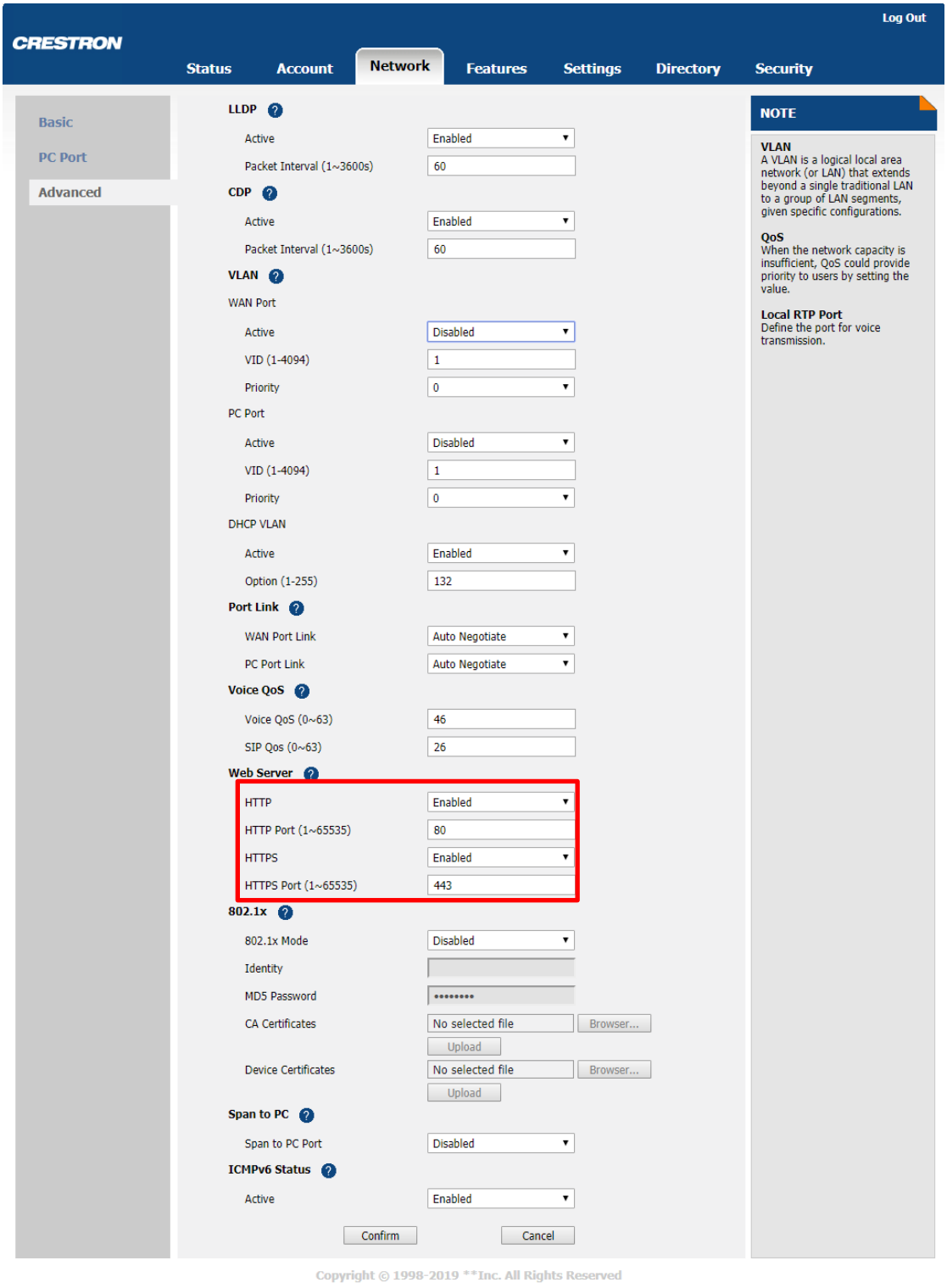
Parameter	Permitted Values	Default
static.wui.http_enable	**0 or 1**	**1**
Description: Enables or disables the user to access web user interface of the phone using the HTTP protocol. **0**- Disabled **1**- Enabled **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > Web Server > HTTP **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > Webserver Type > HTTP Status		
static.network.port.http	**Integer from 1 to 65535**	**80**
Description: Configures the HTTP port for the user to access web user interface of the phone using the HTTP protocol. **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > Web Server > HTTP Port(1~65535) **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > Webserver Type > HTTP Port		

Parameter	Permitted Values	Default
static.wui.https_enable	0 or 1	1
Description: Enables or disables the user to access web user interface of the phone using the HTTPS protocol. **0**- Disabled **1**- Enabled **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > Web Server > HTTPS **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > Webserver Type > HTTPS Status		
static.network.port.https	Integer from 1 to 65535	443
Description: Configures the HTTPS port for the user to access web user interface of the phone using the HTTPS protocol. **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > Web Server > HTTPS Port(1~65535) **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > Webserver Type > HTTPS Port		

Configure Web Server Type via the Web User Interface

1. Click **Network** > **Advanced**.

Network > Advanced



2. Select **Enabled** or **Disabled** from the **HTTP** drop-down list.
3. Enter the HTTP port number in the **HTTP Port(1~65535)** field. The default HTTP port number is 80.
4. Select **Enabled** or **Disabled** from the **HTTPS** drop-down list.
5. Enter the HTTPS port number in the **HTTPS Port(1~65535)** field. The default HTTPS port number is 443.
6. Click **Confirm** to accept the change. A dialog box pops up to prompt that settings will take effect after a reboot.
7. Click **OK** to reboot the phone.

Configure Web Server Type via the Phone User Interface

1. Tap **Setting** > **Advanced**
2. Enter the Admin password (default password: admin), and then tap **OK**.
3. Tap **Network** on the left side of the display, and then tap **3. Webserver Type**.
4. Select **Enabled** or **Disabled** from the **Http Status** drop-down list.
5. Enter the HTTP port number in the **Http Port(1~65535)** field. The default HTTP port number is 80.
6. Select **Enabled** or **Disabled** from the **Https Status** drop-down list.
7. Enter the HTTPS port number in the **Https Port(1~65535)** field. The default HTTPS port number is 443.
8. Tap **Save**.

VLAN

VLAN (Virtual Local Area Network) is used to logically divide a physical network into several broadcast domains. VLAN membership can be configured through software instead of physically relocating devices or connections. Grouping devices with a common set of requirements regardless of their physical location can greatly simplify network design. VLANs can address issues such as scalability, security and network management.

The purpose of VLAN configurations on the phone is to insert tags with VLAN information in the packets generated by the phone. When VLAN is properly configured for the ports (Internet port and PC port) on the phone, the phone will tag all packets from these ports with the VLAN ID. The switch receives and forwards the tagged packets to the corresponding VLAN according to the VLAN ID in the tag as described in IEEE Std 802.3.

VLAN on phones allows simultaneous access for a regular PC. This feature allows a PC to be daisy chained to a phone and the connection for both PC and phone to be trunked through the same physical Ethernet cable.

In addition to manual configuration, the phone also supports automatic discovery of VLAN via LLDP, CDP or DHCP. The assignment takes effect in this order: assignment via LLDP/CDP, manual configuration, then assignment via DHCP.

LLDP

LLDP (Linker Layer Discovery Protocol) is a vendor-neutral Link Layer protocol, which allows the phone to receive and/or transmit device-related information from/to directly connected devices on the network that are also using the protocol, and store the information about other devices. LLDP transmits information as packets called LLDP Data Units (LLDPDUs). An LLDPDU consists of a set of Type-Length-Value (TLV) elements, each of which contains a particular type of information about the device or port transmitting it.

LLDP-MED (Media Endpoint Discovery)

LLDP-MED is published by the Telecommunications Industry Association (TIA). It is an extension to LLDP that operates between endpoint devices and network connectivity devices. LLDP-MED provides the following capabilities for the endpoint:

- Capabilities Discovery: allows LLDP-MED endpoint to determine the capabilities that the connected switch supports and has enabled.
- Network Policy: provides voice VLAN configuration to notify the phone which VLAN to use and QoS-related configuration for voice data. It provides a "plug and play" network environment.
- Power Management: provides information related to how the phone is powered, power priority, and how much power the endpoint needs.
- Inventory Management: provides a means to effectively manage the phone and its attributes, such as model number, serial number and software revision.

TLVs supported by the phone are summarized in the following table:

TLV Type	tlv name	description
Mandatory **TLVs**	Chassis ID	The network address of the phone.
	Port ID	The MAC address of the phone.
	Time To Live	Seconds until data unit expires. The default value is 180s.
	End of LLDPDU	Marks end of LLDPDU.

TLV Type	tlv name	description
Optional **TLVs**	System Name	Name assigned to the phone.
	System Description	Description of the phone. Description includes firmware version of the phone.
	Capabilities	The supported and enabled phone capabilities. The Telephone capability is supported and enabled by default.
	Port Description	Description of port that sends data unit. The default value is “WAN PORT”.
IEEE Std 802.3 Organizationally Specific TLV	MAC/PHY Configuration/Status	Duplex mode and network speed settings of the phone. The Auto Negotiation is supported and enabled by default. The advertised capabilities of PMD. Auto-Negotiation is: 100BASE-TX (full duplex mode) 100BASE-TX (half duplex mode) 10BASE-T (full duplex mode) 10BASE-T (half duplex mode)

TLV Type	tlv name	description
TIA Organizationally Specific TLVs	Media Capabilities	The MED device type of the phone and the supported LLDP-MED TLV type can be encapsulated in LLDPDU. The supported LLDP-MED TLV types are: LLDP-MED Capabilities, Network Policy, Extended Power via MDI-PD, Inventory.
	Network Policy	Port VLAN ID, application type, L2 priority and DSCP value.
	Extended Power-via- MDI	Power type, source, priority and value.
	Inventory – Hardware Revision	Hardware revision of the phone.
	Inventory – Firmware Revision	Firmware revision of the phone.
	Inventory – Software Revision	Software revision of the phone.
	Inventory – Serial Number	Serial number of the phone.
	Inventory – Manufacturer Name	Manufacturer name of the phone.
	Inventory – Model Name	Model name of the phone.
	Asset ID	Assertion identifier of the phone.

LLDP can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure LLDP feature. **Parameters:** static.network.lldp.enable static.network.lldp.packet_interval
Local	Web User Interface	Configure LLDP feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load
	Phone User Interface	Configure LLDP feature.

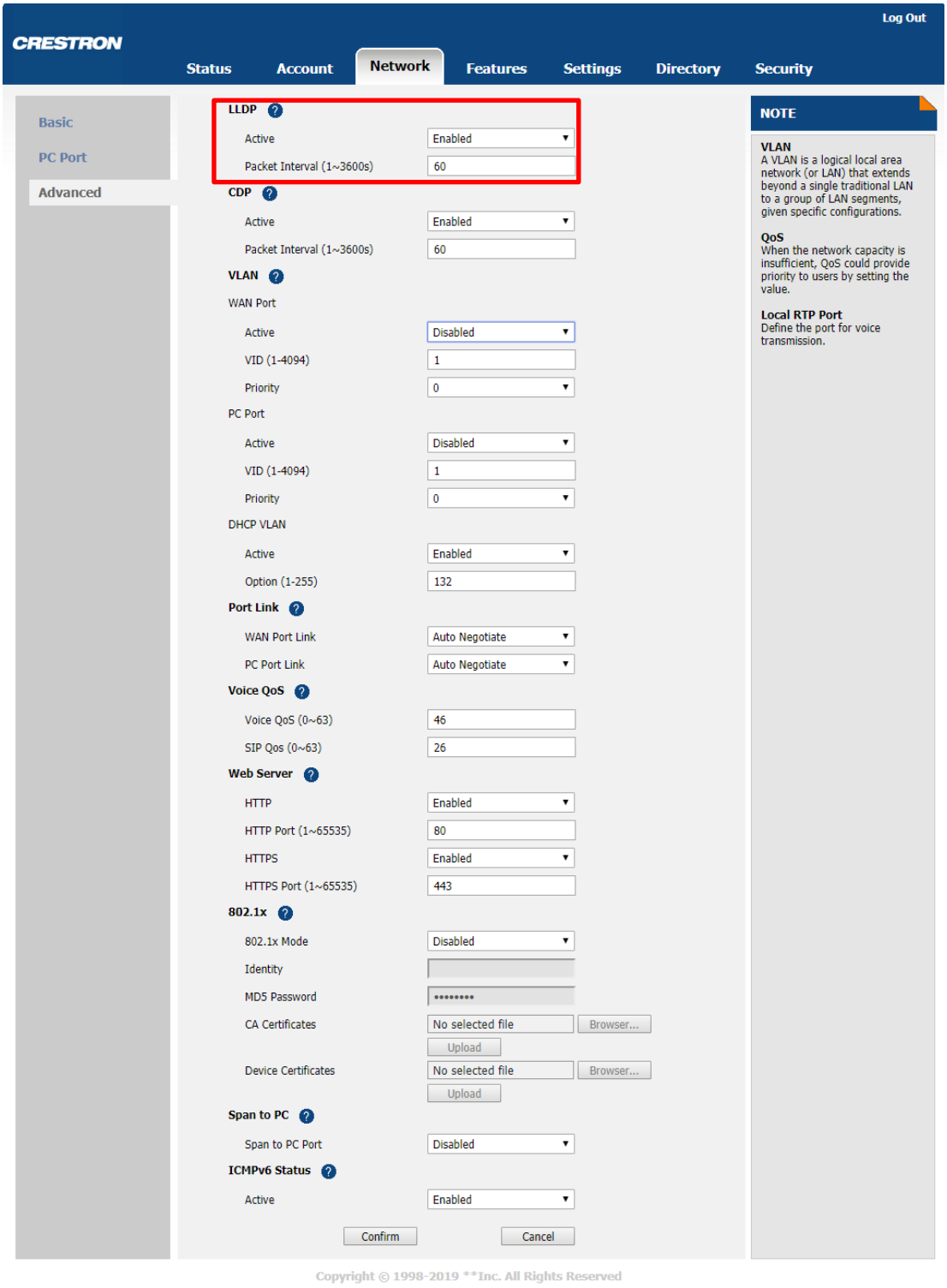
Details of the Configuration Parameters

Parameter	Permitted Values	Default
static.network.lldp.enable	0 or 1	1
Description: Enables or disables the LLDP (Linker Layer Discovery Protocol) feature on the phone. **0**- Disabled **1**- Enabled, the phone will attempt to determine its VLAN ID through LLDP. **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > LLDP > Active **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > LLDP > LLDP Status		
static.network.lldp.packet_interval	Integer from 1 to 3600	60
Description: Configures the interval (in seconds) for the phone to send the LLDP (Linker Layer Discovery Protocol) request. **Note:** This feature works only if the value of the parameter "static.network.lldp.enable" is set to 1 (Enabled). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > LLDP > Packet Interval (1~3600s) **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > LLDP > Packet Interval		

Configure LLDP via the Web User Interface

1. Click **Network** > **Advanced**.

Network > Advanced



2. In the **LLDP** section, select **Enabled** or **Disabled** from the **Active** drop-down list.
3. Enter the time interval in the **Packet Interval (1~3600s)** field.
4. Click **Confirm** to accept the change. A dialog box pops up to prompt that settings will take effect after a reboot.
5. Click **OK** to reboot the phone.

Configure LLDP Feature via the Phone User Interface

1. Tap **Setting** > **Advanced**
2. Enter the Admin password (default password: admin), and then tap **OK**.
3. Tap **Network** on the left side of the display, and then tap **5. LLDP**.
4. Set the **LLDP Status** to **On** or **Off** by tapping the desired setting
5. Enter the priority value (1-3600s) in the **Packet Interval** field.
6. Tap **Save**. The phone will prompt for a reboot.
7. Tap **OK** to reboot the phone.

CDP

CDP (Cisco® Discovery Protocol) allows phones to receive and/or transmit device-related information from/to directly connected devices on the network that are also using the protocol, and store the information about other devices.

If the CDP feature is enabled on phones, the phones will periodically advertise their own information to the directly connected CDP-enabled switch. The phones can also receive CDP packets from the connected switch. If the VLAN configurations on the phones are different from the ones sent by the switch, the phones will perform an update and reboot. This allows the phones to be plugged into any switch, obtain their VLAN IDs, and then start communications with the call control.

CDP can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure CDP feature. **Parameters:** static.network.cdp.enable static.network.cdp.packet_interval
Local	Web User Interface	Configure CDP. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load
	Phone User Interface	Configure CDP feature.

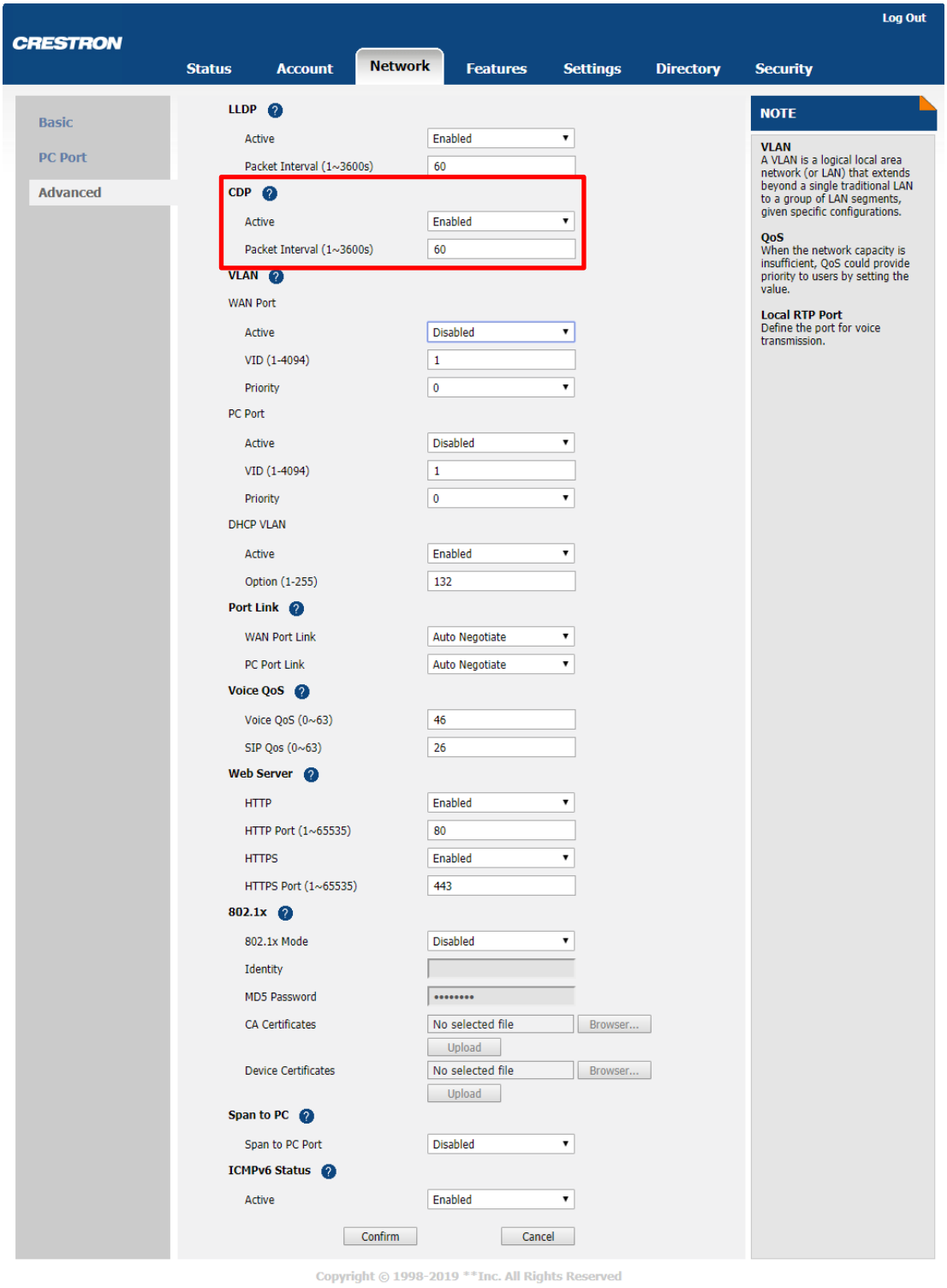
Details of the Configuration Parameters

Parameter	Permitted Values	Default
network.cdp.enable	0 or 1	1
Description: Enables or disables the CDP (Cisco Discovery Protocol) feature on the phone. **0**- Disabled **1**- Enabled, the phone will attempt to determine its VLAN ID through CDP. **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > CDP > Active **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > CDP > CDP Status		
static.network.cdp.packet_interval	Integer from 1 to 3600	60
Description: Configures the interval (in seconds) for the phone to send the CDP (Cisco Discovery Protocol) request. **Note:** This feature works only if the value of the parameter "network.cdp.enable" is set to 1 (Enabled). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > CDP > Packet Interval (1~3600s) **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > CDP > Packet Interval		

Configure CDP Feature via the Web User Interface

1. Click **Network** > **Advanced**.

Network > Advanced



2. In the CDP section, select **Enabled** or **Disabled** from the **Active** drop-down list.
3. Enter the time interval in the **Packet Interval (1~3600s)** field.
4. Click **Confirm** to accept the change. A dialog box pops up to prompt that settings will take effect after a reboot.
5. Click **OK** to reboot the phone

Configure CDP Feature via the Phone User Interface

1. Tap **Setting** > **Advanced**
2. Enter the Admin password (default password: admin), and then tap **OK**.
3. Tap **Network** on the left side of the display, and then tap **6. CDP**.
4. Set **CDP Status** to **On** or **Off** by tapping the desired setting
5. Enter the priority value (1-3600s) in the **CDP Interval** field.
6. Tap **Save**. The phone will prompt for a reboot.
7. Tap **OK** to reboot the phone.

Manual Configuration for VLAN in the Wired Network

VLAN is disabled on phones by default. VLAN can be configured for the Internet port and PC port manually. Before configuring VLAN on the phone, the VLAN ID must be obtained from the network administrator.

VLAN can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure VLAN for the Internet port and PC port manually. **Parameters:** static.network.vlan.internet_port_enable static.network.vlan.internet_port_vid static.network.vlan.internet_port_priority static.network.vlan.pc_port_enable static.network.vlan.pc_port_vid static.network.vlan.pc_port_priority
Local	Web User Interface	Configure VLAN for the Internet port and PC port manually. **Navigate to:** http://<phoneIPAddress>/servlet?p=network-adv&q=load
	Phone User Interface	Configure VLAN for the Internet port and PC port manually.

Details of the Configuration Parameters

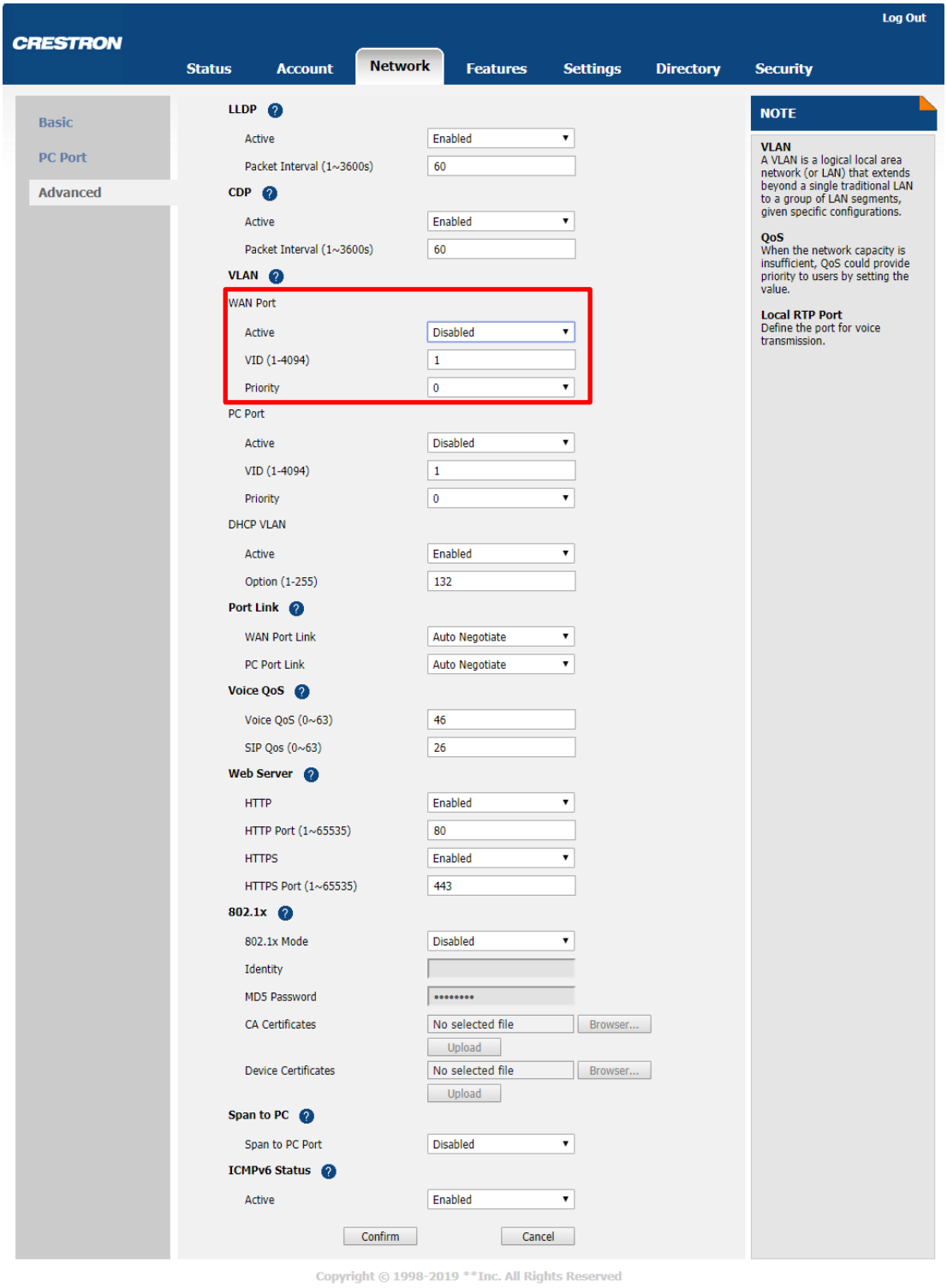
Parameter	Permitted Values	Default
static.network.vlan.internet_port_enable	0 or 1	0
Description: Enables or disables VLAN for the Internet (WAN) port. **0**- Disabled **1**- Enabled **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > VLAN > WAN Port > Active **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > VLAN > WAN Port > VLAN Status		
static.network.vlan.internet_port_vid	Integer from 1 to 4094	1
Description: Configures VLAN ID for the Internet (WAN) port. **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > VLAN > WAN Port > VID (1-4094) **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > VLAN > WAN Port > VID Number		
static.network.vlan.internet_port_priority	Integer from 0 to 7	0
Description: Configures VLAN priority for the Internet (WAN) port. 7 is the highest priority, 0 is the lowest priority. **Note:** This feature works only if the value of the parameter "static.network.vlan.internet_port_enable" is set to 1 (Enabled). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > VLAN > WAN Port > Priority **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > VLAN > WAN Port > Priority		

Parameter	Permitted Values	Default
static.network.vlan.pc_port_enable	0 or 1	0
Description: Enables or disables VLAN for the PC (LAN) port. **0**- Disabled **1**- Enabled **Note:** This feature works only if the value of the parameter "static.network.pc_port.enable" is set to 1 (Auto Negotiation). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > VLAN > PC Port > Active **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > VLAN > PC Port > VLAN Status		
static.network.vlan.pc_port_vid	Integer from 1 to 4094	1
Description: Configures VLAN ID for the PC (LAN) port. **Note:** This feature works only if the value of the parameter "static.network.pc_port.enable" is set to 1 (Auto Negotiation) and the value of the parameter "static.network.vlan.pc_port_enable" is set to 1 (Enabled). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > VLAN > PC Port > VID (1-4094) **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > VLAN > PC Port > VID Number		
static.network.vlan.pc_port_priority	Integer from 0 to 7	0
Description: Configures VLAN priority for the PC (LAN) port. 7 is the highest priority, 0 is the lowest priority. **Note:** This feature works only if the value of the parameter "static.network.pc_port.enable" is set to 1 (Auto Negotiation) and the value of the parameter "static.network.vlan.pc_port_enable" is set to 1 (Enabled). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > VLAN > PC Port > Priority **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > VLAN > PC Port > Priority		

Configure VLAN for Internet (WAN) Port via the Web User Interface

1. Click **Network** > **Advanced**.

Network > Advanced

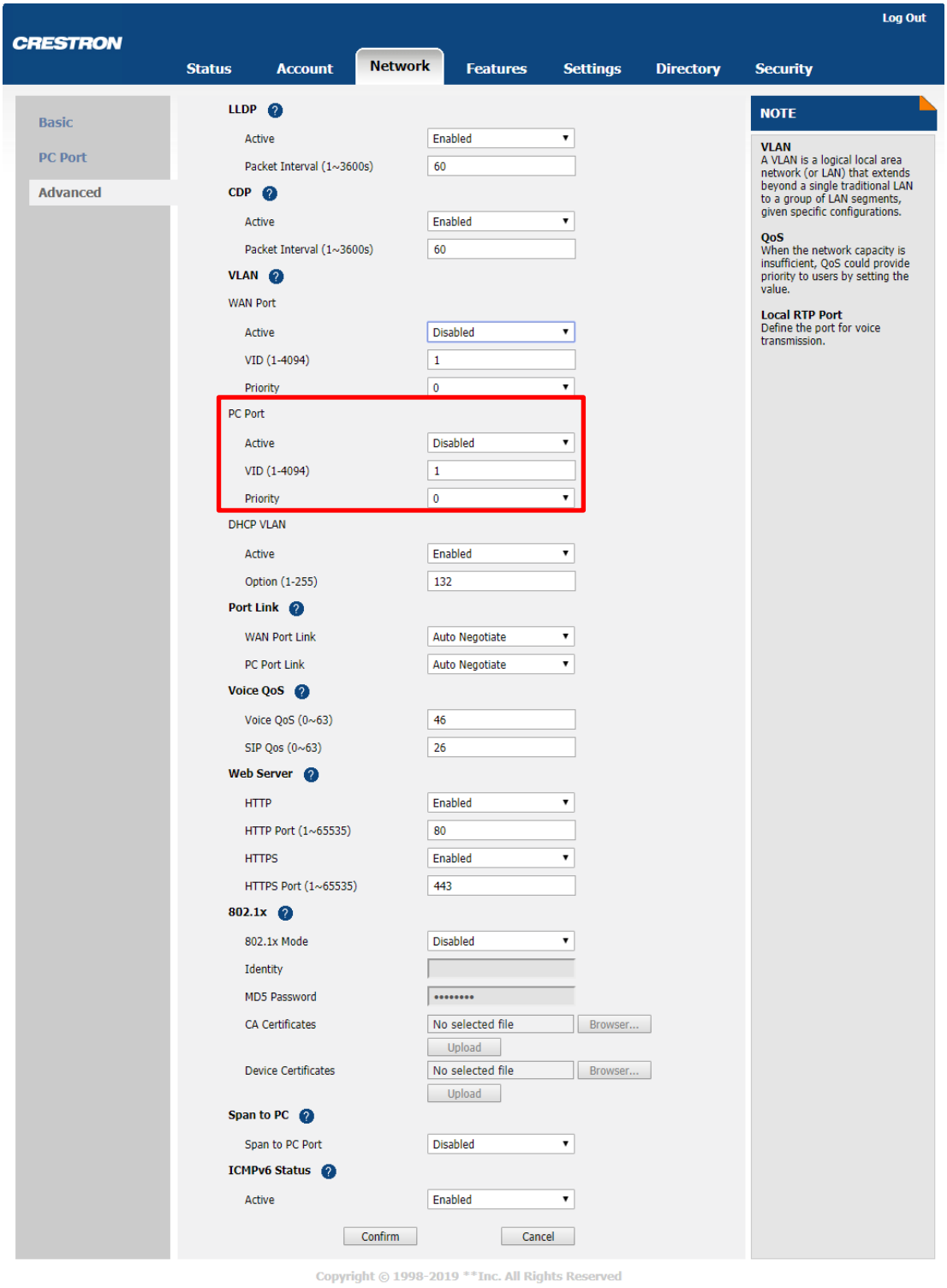


2. In the **WAN Port** section, select **Enabled** or **Disabled** from the **Active** drop-down list.
3. Enter the **VLAN ID** in the **VID (1-4094)** field.
4. Select the desired value (**0**-**7**) from the **Priority** drop-down list.
5. Click **Confirm** to accept the change. A dialog box pops up to prompt that the settings will take effect after a reboot.
6. Click **OK** to reboot the phone.

Configure VLAN for PC Port via the Web User Interface

1. Click **Network** > **Advanced**.

Network > Advanced



2. In the **PC Port** section, select **Enabled** or **Disabled** from the **Active** drop-down list.
3. Enter the **VLAN ID** in the **VID (1-4094)** field.
4. Select the desired value (**0**-**7**) from the **Priority** drop-down list.
5. Click **Confirm** to accept the change. A dialog box pops up to prompt that the settings will take effect after a reboot.
6. Click **OK** to reboot the phone.

Configure VLAN for Internet Port (or PC Port) via the Phone User Interface

1. Tap **Setting** > **Advanced**
2. Enter the Admin password (default password: admin), and then tap **OK**.
3. Tap **Network** on the left side of the display, tap **2. VLAN**, and then tap **1. WAN Port**.
4. Set **VLAN Status** to **On** or **Off** by tapping the desired setting
5. Enter the VLAN ID (1-4094) in the **VID Number** field.
6. Enter the priority value (0-7) in the **Priority** field.
7. Tap **Save**. The phone will prompt for a reboot.
8. Tap **OK** to reboot the phone.

DHCP VLAN

Skype for Business phones support VLAN discovery via DHCP. When the VLAN Discovery method is set to DHCP, the phone will examine DHCP option for a valid VLAN ID. The predefined option 132 is used to supply the VLAN ID by default. The DHCP option used to request the VLAN ID can be customized.

DHCP VLAN can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure DHCP VLAN discovery feature. **Parameters:** static.network.vlan.dhcp_enable static.network.vlan.dhcp_option
Local	Web User Interface	Configure DHCP VLAN discovery feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load
	Phone User Interface	Configure DHCP VLAN discovery feature.

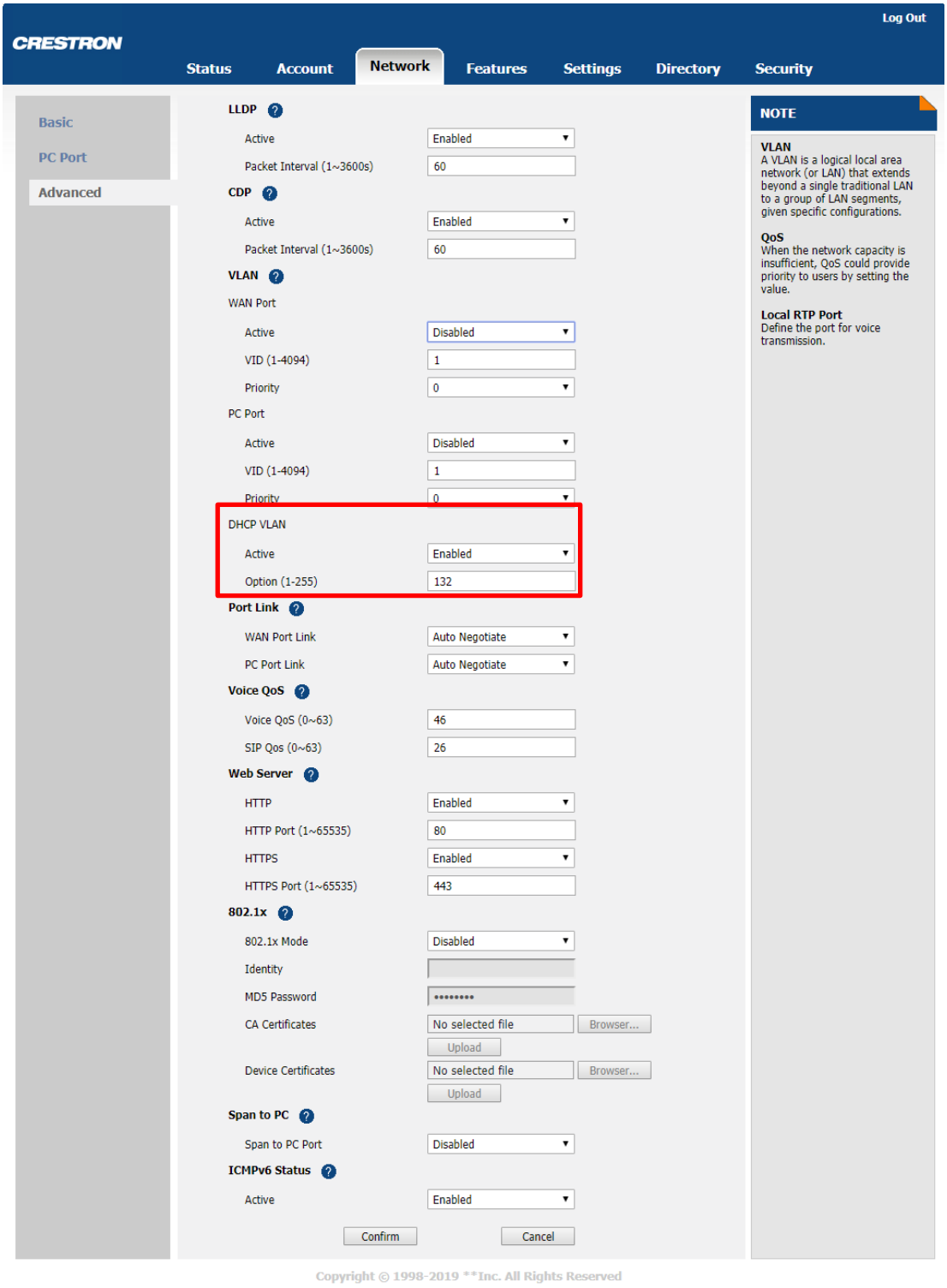
Details of the Configuration Parameters

Parameter	Permitted Values	Default
static.network.vlan.dhcp_enable	0 or 1	1
Description: Enables or disables DHCP VLAN discovery feature on the phone. **0**- Disabled **1**- Enabled **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > VLAN > DHCP VLAN > Active **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > VLAN > DHCP VLAN > DHCP VLAN		
static.network.vlan.dhcp_option	Integer from 1 to 255	132
Description: Configures the DHCP option from which the phone will obtain the VLAN settings. A maximum of five DHCP options can be configured. They must be separated by commas. **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > VLAN > DHCP VLAN > Option (1-255) **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > VLAN > DHCP VLAN > Option		

Configure DHCP VLAN Discovery via the Web User Interface

1. Click **Network** > **Advanced**.

Network > Advanced



2. In the **DHCP VLAN** section, select **Enabled** or **Disabled** from the **Active** drop-down list.
3. Enter the desired option in the **Option (1-255)** field. The default option is **132**.
4. Click **Confirm** to accept the change. A dialog box pops up to prompt that settings will take effect after a reboot.
5. Click **OK** to reboot the phone.

Configure DHCP VLAN Discovery via the Phone User Interface

1. Tap **Setting** > **Advanced**
2. Enter the Admin password (default password: admin), and then tap **OK**.
3. Tap **Network** on the left side of the display, and then tap **2. VLAN**.
4. Tap **3. DHCP VLAN**.
5. Set **DHCP VLAN** to **On** or **Off** by tapping the desired setting.
6. Tap the option number to enter an option in the **Option** field.
7. Tap **Save**. The phone will prompt for a reboot.
8. Tap **OK** to reboot the phone.

IPv6 Support

Because Internet Protocol version 4 (IPv4) uses a 32-bit address, it cannot meet the increased demands for unique IP addresses for all devices that connect to the Internet. Therefore, Internet Protocol version 6 (IPv6) is the next generation network layer protocol, which has been designed as a replacement for the current IPv4 protocol.

IPv6 is developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. The Skype for Business phone supports IPv4 addressing mode, IPv6 addressing mode, as well as an IPv4&IPv6 dual stack addressing mode. IPv4 uses a 32-bit address, consisting of four groups of three decimal digits separated by dots; for example, 192.168.1.100. IPv6 uses a 128-bit address, consisting of eight groups of four hexadecimal digits separated by colons; for example, 2026:1234:1:1:215:65ff:fe1f:caa.

VoIP network based on IPv6 can provide end-to-end security capabilities, enhanced Quality of Service (QoS), and a set of service requirements to guarantee performance while transporting traffic over the network.

If the network settings on the phone are configured for an IPv6 network, the IP address for the phone can be set by using SLAAC (ICMPv6), DHCPv6 or by manually entering an IP address. Ensure that the network environment supports IPv6. Contact the ISP for more information.

IPv6 Address Assignment Method

Supported IPv6 address assignment methods:

- **Manual Assignment:** An IPv6 address and other configuration parameters (e.g., DNS server) for the phone can be statically configured by an administrator.
- **Stateless Address Autoconfiguration (SLAAC)/ICMPv6:** SLAAC is one of the most convenient methods to assign IP addresses to IPv6 nodes. SLAAC requires no manual configuration of the phone, minimal (if any) configuration of routers, and no additional servers. To use IPv6 SLAAC, the phone must be connected to a network with at least one IPv6 router connected. This router is configured by the network administrator and sends out Router Advertisement announcements onto the link. These announcements can allow the on-link connected phone to configure itself with IPv6 address, as specified in RFC 4862.
- **Stateful DHCPv6:** The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) has been standardized by the IETF through RFC 3315. DHCPv6 enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes. It offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility. This protocol is a stateful counterpart to "IPv6 Stateless Address Autoconfiguration" (RFC 2462), and can be used separately or concurrently with the latter to obtain configuration parameters.

IPv6 Address and Network Setting Resources

The following table lists where the phone obtains the IPv6 address and other network settings:

DHCPv6	SLAAC (ICMPv6)	How the phone obtains the IPv6 address and network settings?
Disabled	Disabled	The static IPv6 address and other network settings must be manually configured.
Enabled	Disabled	The phone can obtain the IPv6 address and other network settings via DHCPv6.
Enabled	Enabled	If the SLAAC server is working, the server can specify the phone to obtain the IPv6 address and other network settings either from DHCPv6 or SLAAC. If the SLAAC server is not working, the phone will try to obtain the IPv6 address and other network settings via DHCPv6.

IPv6 can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	**<MAC>.cfg**	Configure the IPv6 address assignment method. **Parameters**: static.network.ip_address_mode static.network.ipv6_internet_port.type static.network.ipv6_internet_port.ip static.network.ipv6_prefix static.network.ipv6_internet_port.gateway static.network.ipv6_icmp_v6.enable
		Configure the IPv6 static DNS address. **Parameters**: static.network.ipv6_primary_dns static.network.ipv6_secondary_dns
	<y0000000000xx>.cfg	Configure the IPv6 static DNS. **Parameter:** static.network.ipv6_static_dns_enable
Local	Web User Interface	Configure the IPv6 address assignment method. Configure the IPv6 static DNS. Configure the IPv6 static DNS address. **Navigate to:** http://<phoneIPAddress>/servlet?p=network&q=load
	Phone User Interface	Configure the IPv6 address assignment method. Configure the IPv6 static DNS. Configure the IPv6 static DNS address.

Details of the Configuration Parameters

Parameter	Permitted Values	Default
static.network.ip_address_mode	**0, 1 or 2**	**0**
Description: Configures the IP address mode. **0**- IPv4 **1**- IPv6 **2**- IPv4 & IPv6 **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Basic > Internet Port > Mode (IPv4/IPv6) **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > WAN Port > IP Mode		

Parameter	Permitted Values	Default
static.network.ipv6_internet_port.type	**0 or 1**	**0**
Description: Configures the Internet (WAN) port type for IPv6. **0**- DHCP **1**- Static IP Address **Note:** This feature works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Basic > IPv6 Config **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > WAN Port > IPv6		
static.network.ipv6_static_dns_enable	**0 or 1**	**0**
Description: Triggers the static IPv6 DNS feature to on or off. **0**- Off, the phone will use the IPv6 DNS obtained from DHCP. **1**- On, the phone will use manually configured static IPv6 DNS. **Note:** This feature works only if the value of the parameter "static.network.ipv6_internet_port.type" is set to 0 (DHCP). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Basic > IPv6 Config > IPv6 Static DNS **Phone User Interface:** Menu > Setting > Advanced (default: admin) > Network > WAN Port > IPv6 > Type(DHCP) > Static DNS		
static.network.ipv6_internet_port.ip	**IPv6 address**	**Blank**
Description: Configures the IPv6 address. **Example:** static.network.ipv6_internet_port.ip = 2026:1234:1:1:215:65ff:fe1f:caa **Note:** This feature works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.network.ipv6_internet_port.type" is set to 1 (Static IP Address). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Basic > IPv6 Config > Static IP Address > IP Address **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > WAN Port > IPv6 > Type(Static IP) > IP Address		

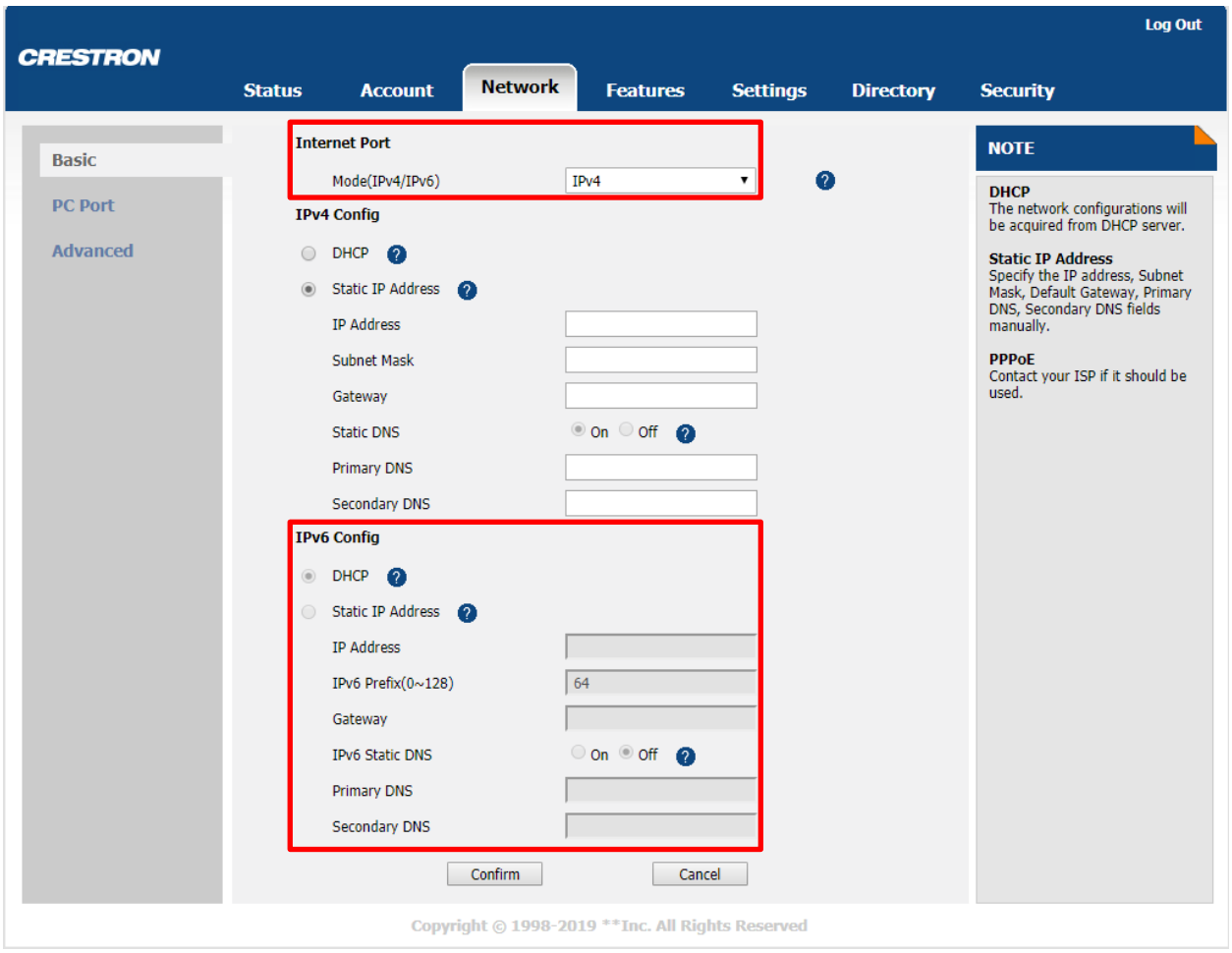
Parameter	Permitted Values	Default
static.network.ipv6_prefix	**Integer from 0 to 128**	**64**
Description: Configures the IPv6 prefix. **Note:** This feature works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.network.ipv6_internet_port.type" is set to 1 (Static IP Address). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Basic > IPv6 Config > Static IP Address > IPv6 Prefix(0~128) **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > WAN Port > IPv6 > Type(Static IP) > IPv6 IP Prefix		
static.network.ipv6_internet_port.gat eway	**IPv6 address**	**Blank**
Description: Configures the IPv6 default gateway. **Example:** static.network.ipv6_internet_port.gateway = 3036:1:1:c3c7:c11c:5447:23a6:255 **Note:** This feature works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.network.ipv6_internet_port.type" is set to 1 (Static IP Address). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Basic > IPv6 Config > Static IP Address > Gateway **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > WAN Port > IPv6 > Type(Static IP) > Gateway		
static.network.ipv6_primary_dns	**IPv6 address**	**Blank**
Description: Configures the primary IPv6 DNS server. **Example:** static.network.ipv6_primary_dns = 3036:1:1:c3c7: c11c:5447:23a6:256 **Note:** This feature works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). In a DHCP environment, the value of the parameter "static.network.ipv6_static_dns_enable" must be set to 1 (On). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Basic > IPv6 Config > Static IP Address > Primary DNS **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > WAN Port > IPv6 > Type(Static IP) > Primary DNS **Or** Menu > Setting > Advanced (default password: admin) > Network > WAN Port > IPv6 > Type(DHCP) > Static DNS(Enabled) > Primary DNS		

Parameter	Permitted Values	Default
static.network.ipv6_secondary_dns	**IPv6 address**	**Blank**
Description: Configures the secondary IPv6 DNS server. **Example:** static.network.ipv6_secondary_dns = 2026:1234:1:1:c3c7:c11c:5447:23a6 **Note:** This feature works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). In a DHCP environment, the value of the parameter "static.network.ipv6_static_dns_enable" must be set to 1 (On). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Basic > IPv6 Config > Static IP Address > Secondary DNS **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > WAN Port > IPv6 > Type(Static IP) > Secondary DNS **Or** Menu > Setting > Advanced (default password: admin) > Network > WAN Port > IPv6 > Type(DHCP) > Static DNS(Enabled) > Secondary DNS		
static.network.ipv6_icmp_v6.enable	**0 or 1**	**1**
Description: Enables or disables the phone to obtain IPv6 network settings via SLAAC (Stateless Address Autoconfiguration) method. **0**- Disabled **1**- Enabled **Note**: This feature works only if the value of the parameter "static.network.ipv6_internet_port.type" is set to 0 (DHCP). If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > ICMPv6 Status > Active **Phone User Interface:** None		

Configure IPv6 Address Assignment Method via the Web User Interface

1. Click **Network** > **Basic**.

Network > Basic



2. Select the **IPv6** or **IPv4 & IPv6** address mode from the **Mode(IPv4/IPv6)** drop-down list
3. In the **IPv6 Config** section, select **DHCP** or **Static IP Address**. If **Static IP Address** is selected, configure the IPv6 address and other configuration parameters in the corresponding fields.

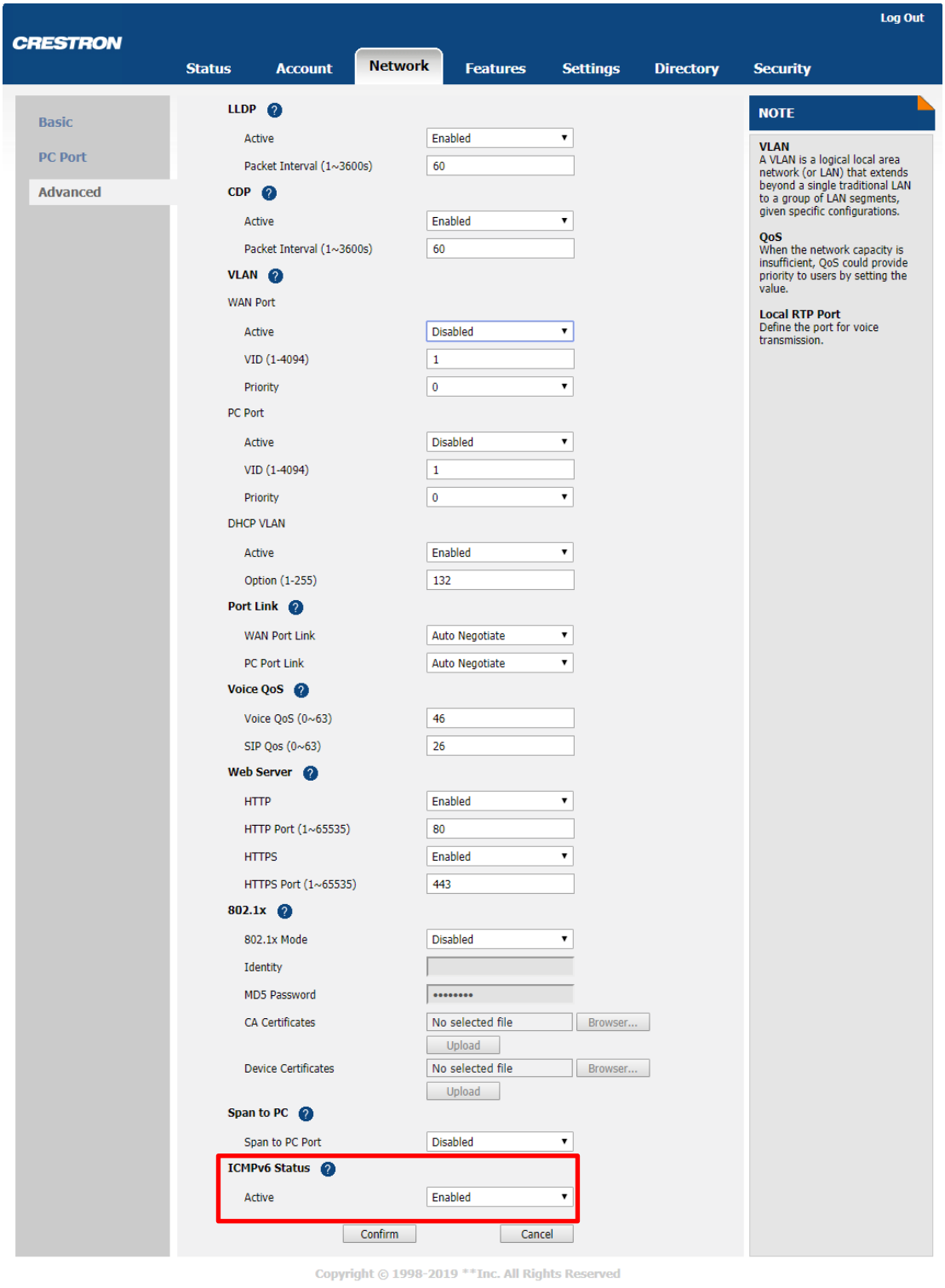
   NOTE: If DHCP is selected, the static DNS address can be configured in the corresponding fields.

4. Click **Confirm** to accept the change. A dialog box pops up to prompt that settings will take effect after a reboot.
5. Click **OK** to reboot the phone.

Configure SLAAC Feature via the Web User Interface

1. Click **Network** > **Advanced**.

Network > Advanced



2. In the **ICMPv6 Status** section, select **Enabled** or **Disabled** from the **Active** drop-down list.
3. Click **Confirm** to accept the change. A dialog box pops up to prompt that settings will take effect after a reboot.
4. Click **OK** to reboot the phone.

Configure IPv6 Address Assignment Method via the Phone User Interface

1. Tap **Setting** > **Advanced**.
2. Enter the Admin password (default password: admin), and then tap **OK**.
3. Tap Network on the left side of the display, and then tap **1. WAN Port**.
4. Tap then entry in the IP Mode field, and then tap **IPv4 & IPv6** or **IPv6**.
5. Tap **Save**. The phone will prompt for a reboot.
6. Tap **OK** to reboot the phone.

Configure IPv6 Static DNS When DHCP is Used via the Phone User Interface

1. Tap **Setting** > **Advanced**.
2. Enter the Admin password (default password: admin), and then tap **OK**.
3. Tap Network on the left side of the display, and then tap **3. IPv6**.
4. Select **DHCP** from the **1. Type** field drop-down list.
5. Select Enabled from the **2. Static DNS** field drop-down list.
6. Enter the addresses of the primary and secondary DNS servers in the **3. Pri.DNS** and **Sec.DNS** fields.
7. Tap **Save**. The phone will prompt for a reboot.
8. Tap **OK** to reboot the phone.

Quality of Service

Quality of Service (QoS) is the ability to provide different priorities for different packets in the network, allowing the transport of traffic with special requirements. QoS guarantees are important for applications that require fixed bit rate and are delay sensitive when the network capacity is insufficient. There are four major QoS factors to be considered when configuring a modern QoS implementation: bandwidth, delay, jitter and loss.

QoS provides better network service through the following features:

- Supporting dedicated bandwidth
- Improving loss characteristics
- Avoiding and managing network congestion

- Shaping network traffic
- Setting traffic priorities across the network

The Best-Effort service is the default QoS model in IP networks. It provides no guarantees for data delivering, which means delay, jitter, packet loss and bandwidth allocation are unpredictable. Differentiated Services (DiffServ or DS) is the most widely used QoS model. It provides a simple and scalable mechanism for classifying and managing network traffic and providing QoS on modern IP networks. Differentiated Services Code Point (DSCP) is used to define DiffServ classes and stored in the first six bits of the ToS (Type of Service) field. Each router on the network can provide QoS simply based on the DiffServ class. The DSCP value ranges from 0 to 63 with each DSCP specifying a particular per-hop behavior (PHB) applicable to a packet. A PHB refers to the packet scheduling, queuing, policing, or shaping behavior of a node on any given packet.

Four standard PHBs available to construct a DiffServ-enabled network and achieve QoS:

- **Class Selector PHB:** backwards compatible with IP precedence. Class Selector code points are of the form "xxx000". The first three bits are the IP precedence bits. These class selector PHBs retain almost the same forwarding behavior as nodes that implement IP precedence-based classification and forwarding.
- **Expedited Forwarding PHB:** the key ingredient in DiffServ model for providing a low-loss, low-latency, low-jitter and assured bandwidth service.
- **Assured Forwarding PHB:** defines a method by which BAs (Bandwidth Allocations) can be given different forwarding assurances.
- **Default PHB:** specifies that a packet marked with a DSCP value of "000000" gets the traditional best effort service from a DS-compliant node.

VoIP is extremely bandwidth and delay-sensitive. QoS is a major issue in VoIP implementations, regarding how to guarantee that packet traffic not be delayed or dropped due to interference from other lower priority traffic. VoIP can guarantee high-quality QoS only if the voice and the SIP packets are given priority over other kinds of network traffic. Skype for Business phones support the DiffServ model of QoS.

Voice QoS

In order to make VoIP transmissions intelligible to receivers, voice packets should not be dropped, excessively delayed, or made to suffer varying delay. DiffServ model guarantees high-quality voice transmission when the voice packets are configured to a higher DSCP value.

SIP QoS

SIP protocol is used for creating, modifying and terminating two-party or multi-party sessions. To ensure good voice quality, SIP packets emanated from phones should be configured with a high transmission priority.

DSCPs for voice and SIP packets can be specified respectively.

NOTE: For voice and SIP packets, the Skype for Business phone obtains DSCP info from the network policy if LLDP feature is enabled, which takes precedence over manual settings. For more information on LLDP, refer to LLDP on page 50.

QoS can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the DSCPs for voice packets and SIP packets. **Parameters:** static.network.qos.audiotos static.network.qos.signaltos
Local	Web User Interface	Configure the DSCPs for voice packets and SIP packets. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load

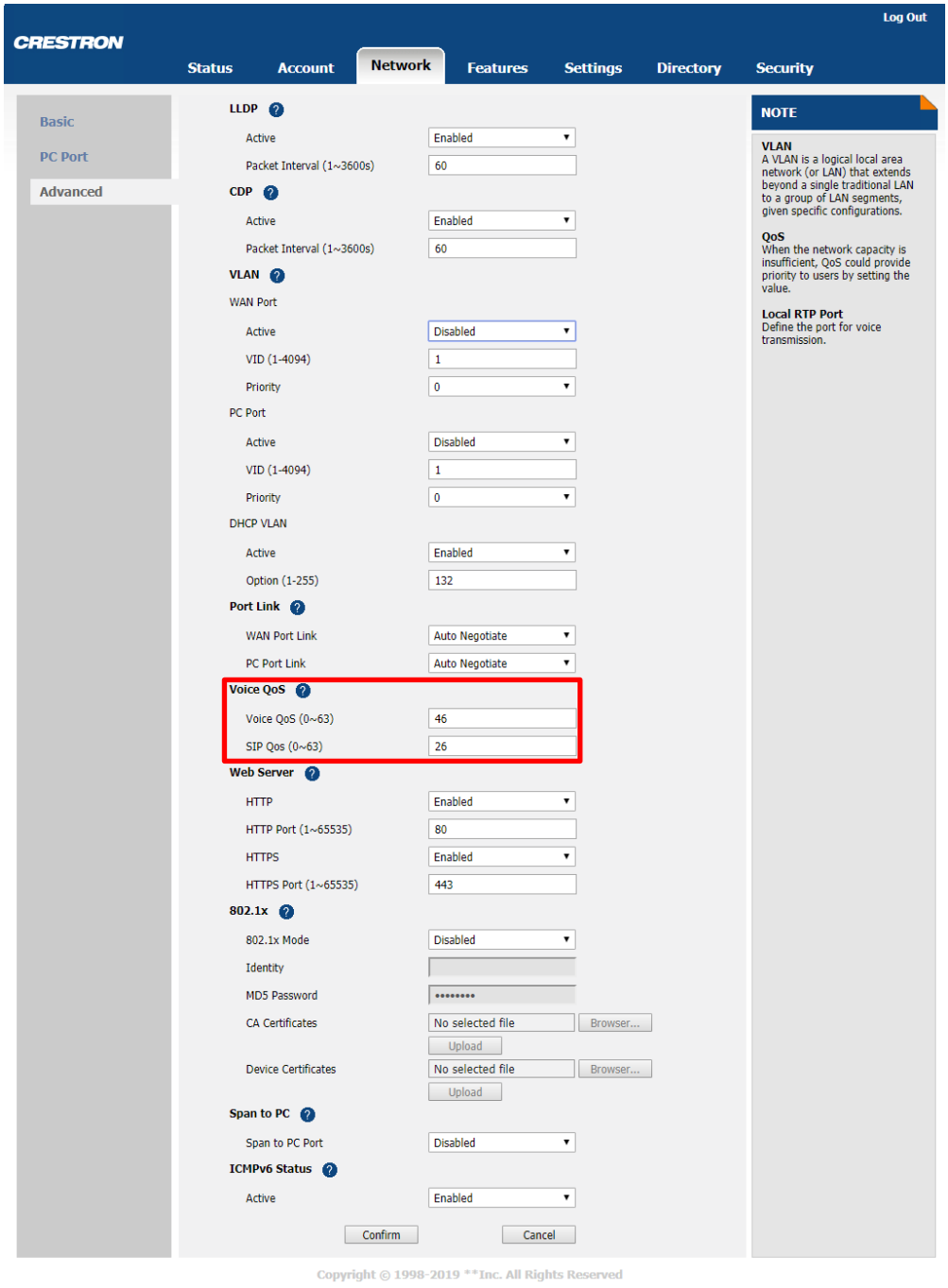
Details of the Configuration Parameters

Parameter	Permitted Values	Default
static.network.qos.audiotos	**Integer from 0 to 63**	**46**
Description: Configures the DSCP (Differentiated Services Code Point) for voice packets. The default DSCP value for RTP packets is 46 (Expedited Forwarding). **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > Voice QoS (0~63) **Phone User Interface:** None		
static.network.qos.signaltos	**Integer from 0 to 63**	**26**
Description: Configures the DSCP (Differentiated Services Code Point) for SIP packets. The default DSCP value for SIP packets is 26 (Assured Forwarding). **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > SIP QoS (0~63) **Phone User Interface:** None		

Configure DSCPs for Voice Packets and SIP Packets via the Web User Interface

1. Click **Network** > **Advanced**.

Network > Advanced



2. Enter the desired value in the **Voice QoS (0~63)** field.
3. Click **Confirm** to accept the change. A dialog box pops up to prompt that settings will take effect after a reboot.

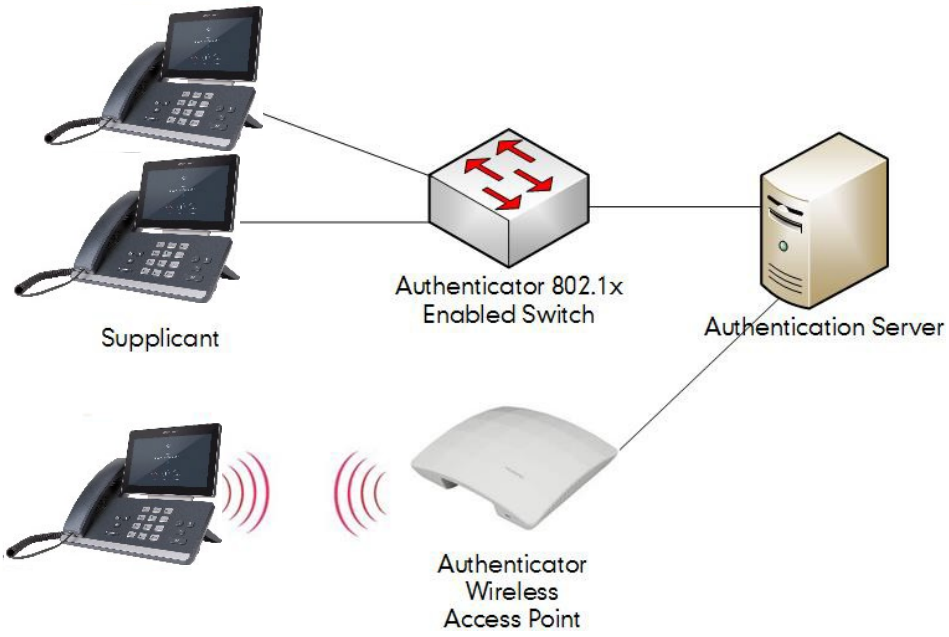
4. Click **OK** to reboot the phone.

802.1x Authentication

IEEE 802.1x authentication is an IEEE standard for Port-based Network Access Control (PNAC), part of the IEEE 802.1 group of networking protocols. It offers an authentication mechanism for devices to connect/link to a LAN or WLAN.

The 802.1x authentication involves three parties: a supplicant, an authenticator and an authentication server. The supplicant is the phone that wishes to attach to the LAN or WLAN. With 802.1x port-based authentication, the phone provides credentials, such as user name and password, for the authenticator, and then the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the phone is allowed to access resources located on the protected side of the network.

802.1x Authentication



Skype for Business phones support the following protocols for 802.1x authentication:

- EAP-MD5
- EAP-TLS (requires Device and CA certificates, requires no password)
- EAP-PEAP/MSCHAPv2 (requires CA certificates)
- EAP-TTLS/EAP-MSCHAPv2 (requires CA certificates)
- EAP-PEAP/GTC (requires CA certificates)
- EAP-TTLS/EAP-GTC (requires CA certificates)
- EAP-FAST (supports EAP In-Band provisioning, requires CA certificates if the provisioning mode is Authenticated Provisioning)

802.1x authentication can be configured using the configuration files or locally.

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the 802.1x authentication. **Parameters:** static.network.802_1x.mode static.network.802_1x.identity static.network.802_1x.md5_password static.network.802_1x.root_cert_url static.network.802_1x.client_cert_url
Local	Web User Interface	Configure the 802.1x authentication. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load
	Phone User Interface	Configure the 802.1x authentication.

Details of the Configuration Parameters

Parameter	Permitted Values	Default
static.network.802_1x.mode	**0, 1, 2, 3, 4, 5, 6 or 7**	**0**

Description:

Configures the 802.1x authentication method.

0- Disabled

1- EAP-MD5

2- EAP-TLS

3- EAP-PEAP/MSCHAPv2

4- EAP-TTLS/EAP-MSCHAPv2

5- EAP-PEAP/GTC

6- EAP-TTLS/EAP-GTC

7- EAP-FAST

Note: If the parameter is changed, the phone will reboot to make the change take effect.

Web User Interface:
Network > Advanced > 802.1x > 802.1x Mode

Phone User Interface:
Menu > Setting > Advanced (default password: admin) > Network > 802.1x > 802.1x Mode

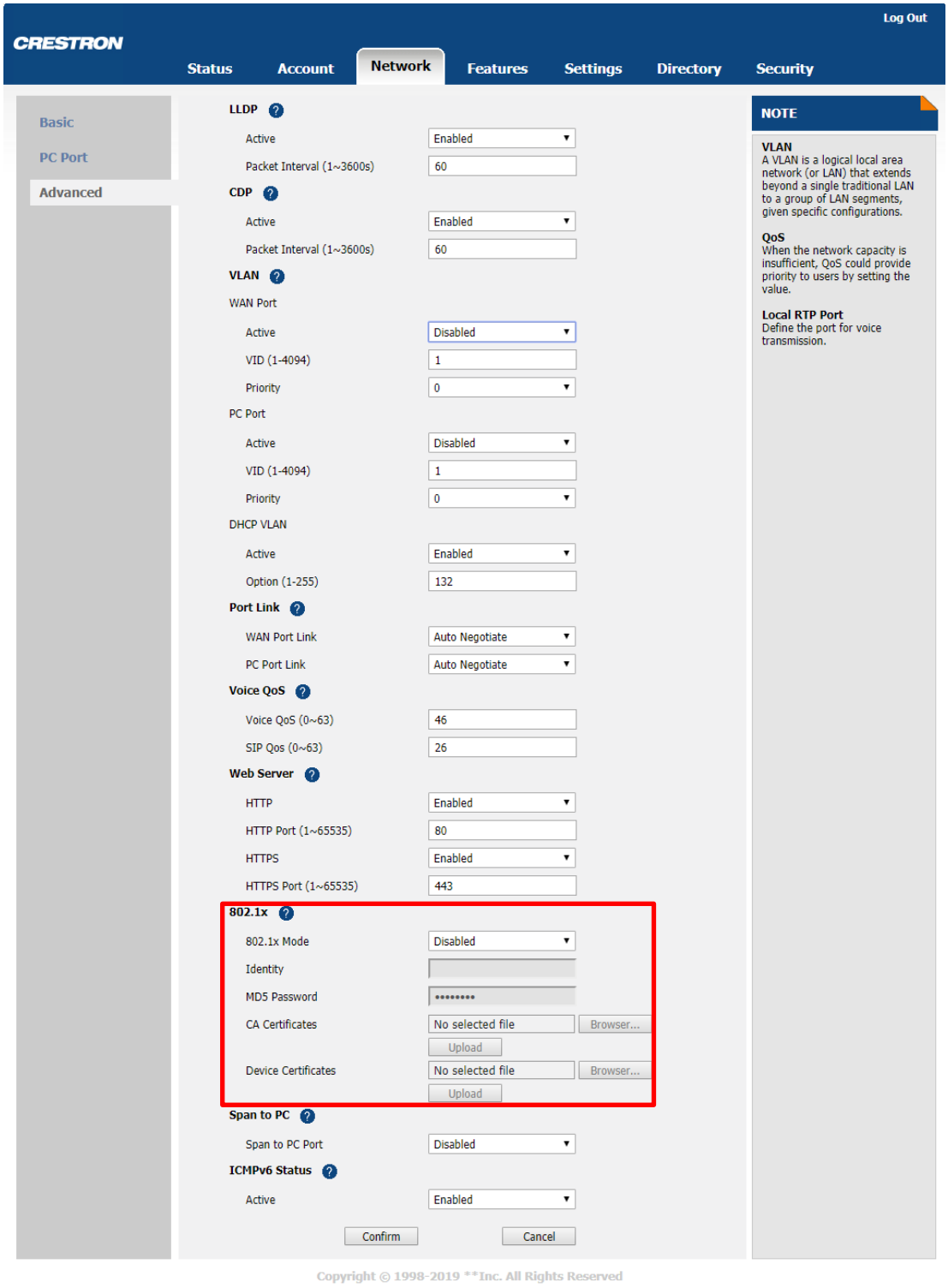
Parameter	Permitted Values	Default
static.network.802_1x.identity	**String within 32 characters**	**Blank**
Description: Configures the identity (or user name) for 802.1x authentication. **Example:** static.network.802_1x.identity = admin **Note:** This feature works only if the value of the parameter "static.network.802_1x.mode" is set to 1, 2, 3, 4, 5, 6 or 7. If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > 802.1x > Identity **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > 802.1x > Identity		
static.network.802_1x.md5_password	**String within 32 characters**	**Blank**
Description: Configures the password for 802.1x authentication. **Example:** static.network.802_1x.md5_password = admin123 **Note:** This feature works only if the value of the parameter "static.network.802_1x.mode" is set to 1, 3, 4, 5, 6 or 7. If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Network > Advanced > 802.1x > MD5 Password **Phone User Interface:** Menu > Setting > Advanced (default password: admin) > Network > 802.1x > MD5 Password		
static.network.802_1x.root_cert_url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the CA certificate. **Example:** static.network.802_1x.root_cert_url = http://192.168.1.10/ca.pem **Note:** This feature works only if the value of the parameter "static.network.802_1x.mode" is set to 2, 3, 4, 5, 6 or 7. The format of the certificate must be *.pem, *.crt, *.cer or *.der. **Web User Interface:** Network > Advanced > 802.1x > CA Certificates **Phone User Interface:** None		

Parameter	Permitted Values	Default
static.network.802_1x.client_cert_url	URL within 511 characters	Blank
Description: Configures the access URL of the device certificate. **Example:** static.network.802_1x.client_cert_url = http://192.168.1.10/client.pem **Note:** This feature works only if the value of the parameter "static.network.802_1x.mode" is set to 2 (EAP-TLS). The format of the certificate must be *.pem. **Web User Interface:** Network > Advanced > 802.1x > Device Certificates **Phone User Interface:** None		

Configure 802.1x Authentication via the Web User Interface

1. Click **Network** > **Advanced**.

Network > Advanced



2. In the **802.1x** block, select the protocol from the **802.1x Mode** drop-down list.
   - EAP-MD5
     i. Enter the user name for authentication in the **Identity** field.
     ii. Enter the password for authentication in the **MD5 Password** field.
   - EAP-TLS
     i. Enter the user name for authentication in the **Identity** field.
     ii. Leave the **MD5 Password** field blank.
     iii. In the **CA Certificates** field, click **Browser** to select the CA certificate (*.pem, *.crt, *.cer or *.der) from the local system.
     iv. In the **Device Certificates** field, click **Browser** to select the client (*.pem or *.cer) certificate from the local system.
     v. Click **Upload** to upload the certificates.
   - EAP-PEAP/MSCHAPv2
     i. Enter the user name for authentication in the **Identity** field.
     ii. Enter the password for authentication in the **MD5 Password** field.
     iii. In the **CA Certificates** field, click **Browser** to select the CA certificate (*.pem, *.crt, *.cer or *.der) from the local system.
     iv. Click **Upload** to upload the certificates.
   - EAP-TTLS/EAP-MSCHAPv2
     i. Enter the user name for authentication in the **Identity** field.
     ii. Enter the password for authentication in the **MD5 Password** field.
     iii. In the **CA Certificates** field, click **Browser** to select the CA certificate (*.pem, *.crt, *.cer or *.der) from the local system.
     iv. Click **Upload** to upload the certificates.
   - EAP-PEAP/GTC
     i. Enter the user name for authentication in the **Identity** field.
     ii. Enter the password for authentication in the **MD5 Password** field.
     iii. In the **CA Certificates** field, click **Browser** to select the CA certificate (*.pem, *.crt, *.cer or *.der) from the local system.
     iv. Click **Upload** to upload the certificates.
   - EAP-TTLS/EAP-GTC
     i. Enter the user name for authentication in the **Identity** field.
     ii. Enter the password for authentication in the **MD5 Password** field.

iii. In the **CA Certificates** field, click **Browser** to select the CA certificate (*.pem, *.crt, *.cer or *.der) from the local system.

iv. Click **Upload** to upload the certificates.

– EAP-FAST

i. Enter the user name for authentication in the **Identity** field.

ii. Enter the password for authentication in the **MD5 Password** field.

iii. In the **CA Certificates** field, click **Browser** to select the CA certificate (*.pem, *.crt, *.cer or *.der) from the local system.

iv. Click **Upload** to upload the certificates.

3. Click **Confirm** to accept the change. A dialog box pops up to prompt that settings will take effect after a reboot.
4. Click **OK** to reboot the phone.

Configure 802.1x Authentication via the Phone User Interface

1. Tap **Setting** > Advanced
2. Enter the Admin password (default password: admin), and then tap **OK**.
3. Tap **Network** on the left side of the display, and then tap **4. 802.1x**.
4. Select the 801.1x mode from the **802.1x Mode** field.
   – EAP-MD5

   i. Enter the user name for authentication in the **Identity** field.

   ii. Enter the password for authentication in the **MD5 Password** field.

   – EAP-TLS

   i. Enter the user name for authentication in the **Identity** field.

   ii. Leave the **MD5 Password** field blank.

   – EAP-PEAP/MSCHAPv2

   i. Enter the user name for authentication in the **Identity** field.

   ii. Enter the password for authentication in the **MD5 Password** field.

   – EAP-TTLS/EAP-MSCHAPv2

   i. Enter the user name for authentication in the **Identity** field.

   ii. Enter the password for authentication in the **MD5 Password** field.

   – EAP-PEAP/GTC

   i. Enter the user name for authentication in the **Identity** field.

   ii. Enter the password for authentication in the **MD5 Password** field.

- EAP-TTLS/EAP-GTC
  i. Enter the user name for authentication in the **Identity** field.
  ii. Enter the password for authentication in the **MD5 Password** field.
- EAP-FAST
  i. Enter the user name for authentication in the **Identity** field.
  ii. Enter the password for authentication in the **MD5 Password** field.

5. Tap **Save**. The phone reboots automatically to make the settings effective.

Set Up Phones with a Provisioning Server

This section provides basic instructions for setting up phones with a provisioning server.

Provisioning Points to Consider

- When provisioning a block of phones, we recommend using central provisioning as the primary configuration method. For more information on central provisioning, refer to "Central Provisioning" on page 82.
- A provisioning server maximizes flexibility when installing, configuring, upgrading, and managing the phones, and enables an adminstrator to store configuration on the server. A provisioning server can be set up on the local area network (LAN) or anywhere on the Internet. For more information, refer to "Set up a Provisioning Server" on page 88.
- If the phone is unable to obtain the address of a provisioning server during startup, and has not been configured with settings from any other source, the phone will use configurations stored in the flash memory. If the phone is unable to obtain the address of a provisioning server, and has previously been configured with settings, it will use those previous settings.

Provisioning Methods

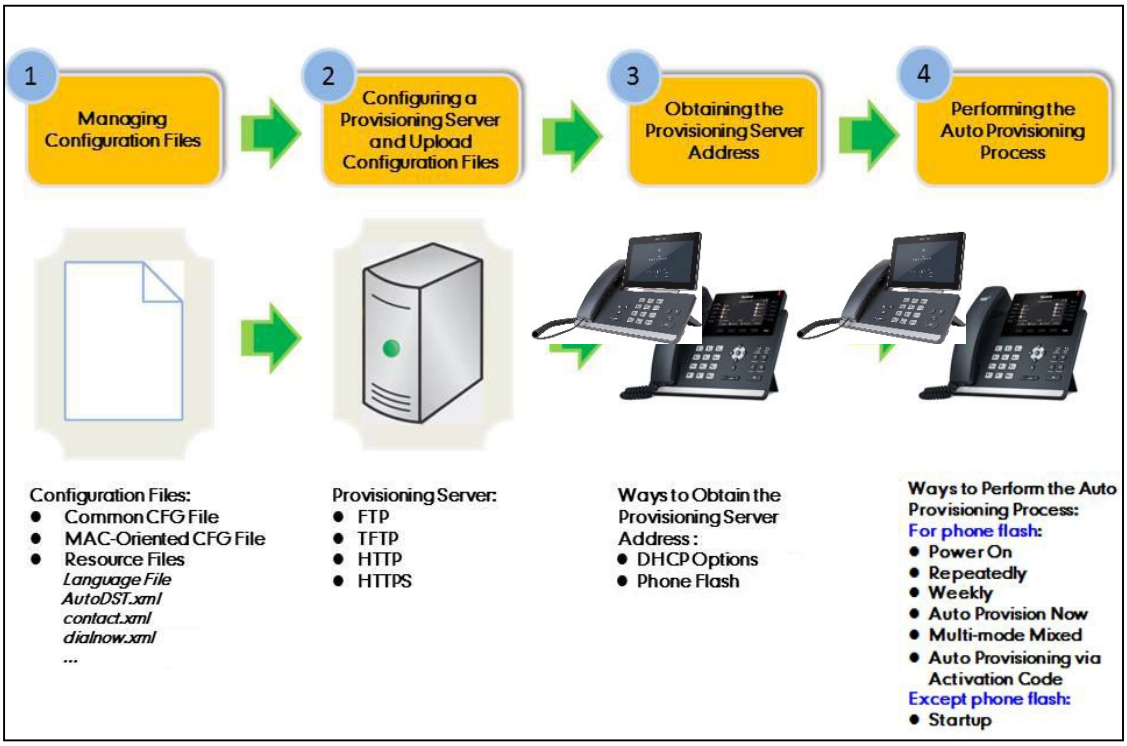
Skype for Business phones can be configured using the following methods:

- **Central Provisioning**: configuration files stored on a central provisioning server.
- **In-band Provisioning:** settings from the Skype for Business server pool.
- **Manual Provisioning:** operations on the web user interface or phone user interface.
- Combination of the above methods.

Central Provisioning

The following figure shows how the phone operates with the provisioning server when using the central provisioning method:

Central Provisioning



Using configuration files to provision phones and to modify features and configurations is called the central provisioning method. A text-based editing application can be used to edit configuration files, and then store configuration files to a provisioning server. Skype for Business phones can be centrally provisioned from a provisioning server. For more information on the provisioning server, refer to "Set up a Provisioning Server" on page 88. For more information on configuration files, refer to "Configuration Files" on page 85.

Skype for Business phones can obtain the provisioning server address during startup. Phones then download configuration files from the provisioning server, then resolve and update the configurations written in configuration files. This entire process is called auto provisioning. For more information on auto provisioning, refer the UC-PHONE Auto Provisioning Guide (Doc. 8368) from www.crestron.com/manuals.

In addition to the configuration files, the phones also download resource files during auto provisioning. For more information on resource files, refer to "Resource Files" on page 86.

In-Band Provisioning Settings

After the phone is signed in, the phone receives settings from the Skype for Business server pool through in-band provisioning.

Skype for Business in-band provisioning device settings take precedence over the same settings configured via central provisioning. To avoid configuration conflicts, ensure that the settings applied to phones are from one source or the other. If provisioning in-band, remove the parameters from the configuration files before using the central provisioning method. If using central provisioning, it is best practice to disable in-band provisioning device settings.

In-band provisioning device settings can be configured using the configuration files only.

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configures in-band provisioning device settings sent from Skype for Business server. **Parameter:** static.phone_setting.receive_inband.enable

Details of the Configuration Parameter

Parameter	Permitted Values	Default
static.phone_setting.receive_inband.enable	**0 or 1**	**1**
Description: Enables or disables in-band provisioning device settings sent from Skype for Business server. **0**- Disabled, the phone blocks in-band provisioning device settings sent from Skype for Business server. **1**- Enabled, the phone accepts in-band provisioning device settings sent from Skype for Business server. **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** None		

Manual Provisioning

Phones can be manually provisioned from the web user interface or the phone user interface.

The Web User Interface

Phones can be configured via the web user interface that is especially useful for remote configuration. As features and configurations vary by phone model and firmware version, options available on each page of the web user interface vary.

An administrator or user can configure phones via the web user interface; but accessing the web user interface requires a password. The default user name and password for the administrator are both "admin" (case-sensitive). The default user name and password for the user are both "user" (case-sensitive). For more information on configuring passwords, refer to "User and Administrator Passwords" on page 322.

This method enables configuration changes on a per-phone basis. Note that features that can be configured via the Web User Interface are limited. The web user interface method can be used as the sole configuration method or in conjunction with other provisioning methods.

Phones support both HTTP and HTTPS protocols for accessing the web user interface. For more information, refer to "Web Server Types" on page 39.

The Phone User Interface

Phones can be configured via the phone user interface on a per-phone basis. As with the web user interface, the phone user interface makes configurations available to users and administrators; but the **Advanced/Advanced Settings** option is only available to administrators and requires an administrator password (default: admin). For more information on configuring a password, refer to "User and Administrator Passwords" on page 322.

Provisioning Methods Priority

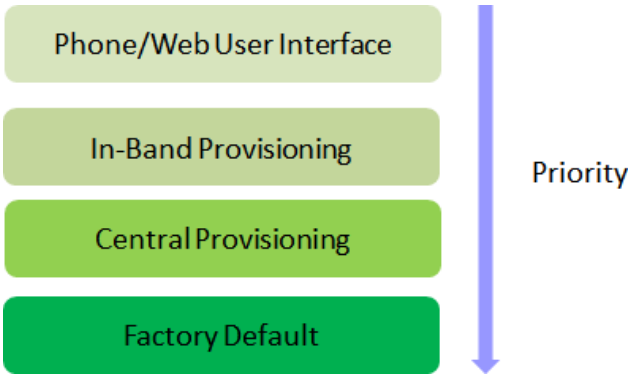
By default, different provisioning methods (central provisioning, in-band Provisioning and manual Provisioning) have no priority. Subsequent operations always override previous operations regardless of the provisioning method used.

For example, a user disables the phone lock feature via phone/web user interface manually, but the phone automatically receives in-band provisioning when the auto update timer expires, so that the phone lock feature is enabled automatically.

If users want to keep the personalized settings, the system administrator can enable the provisioning methods priority to ensure the provision with high priority will not be overwritten by the provision with low priority.

The provisioning methods priority is as follows (highest to lowest):

Provisioning Method Priority



NOTE: Static settings are related to network and central provisioning and have no priority. No matter which provisioning method is used to provision the phone, static settings always take effect. For more information on static settings, refer to "Appendix D: Static Settings" on page 387.

Provisioning methods priority can be configured using the configuration files only.

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configures the provisioning methods priority. **Parameter:** static.auto_provision.custom.protect

Details of the Configuration Parameter

Parameter	Permitted Values	Default
static.auto_provision.custom.protect	**0 or 1**	**0**

Description:

Enables or disables the provisioning methods priority.

0- Disabled, different provisioning methods (central provisioning, in-band provisioning and manual provisioning) have no priority. The subsequent operations always override previous operations regardless of the provisioning method being used.

1- Enabled, different provisioning methods have priority (phone/web user interface>in-band provisioning>central provisioning>factory defaults). The provision with high priority will not be overwritten by the provision with low priority.

Web User Interface:
None

Phone User Interface:
None

Configuration Files and Resource Files

When phones are configured with the central provisioning method, they will request to download the configuration files and resource files from the provisioning server.

The following sections describe the details of the configuration files and resource files:

- Configuration Files
- Resource Files
- Obtaining Configuration Files/Resource Files

Configuration Files

The configuration files are valid CFG files that can be created or edited using a text editor such as UltraEdit. An administrator can deploy and maintain a block of phones automatically through configuration files stored on a provisioning server.

Configuration files consist of:

- Common CFG File

  Common CFG file, named <y0000000000xx>.cfg, contains parameters that affect the basic operation of the phone, such as language and volume. It will be effective for all phones of the same model. The common CFG file has a fixed name.

  The following table lists the name of the common CFG file for each phone model:

Phone Model	Common CFG file
UC-PHONE-S-PLUS	y000000000058.cfg
UC-PHONE-S	y000000000056.cfg

  NOTE: The above file names must be used when using auto-provisioning. If manually updating the phone's firmware, any name can be used for the CFG file.

- MAC-Oriented CFG File

  MAC-Oriented CFG file, named <MAC>.cfg, contains parameters unique to a particular phone, such as account registration. It will only be effective with a specific phone.

  The MAC-Oriented CFG file is named after the MAC address of the phone. The MAC address, a unique 12-digit serial number assigned to each phone, can be obtained from the bar code on the back of the phone. For example, if the MAC address of a phone is 00156574B150, the name of the MAC-Oriented CFG file must be 00156574b150.cfg (case-sensitive).

Resource Files

When configuring certain features, resource files may need to be uploaded to the phones. Resource files are optional, but if the particular feature is being employed, these files are required.

When using the resource file for all phones of the same model, the access URL of resource file should be specified in the common CFG file. However, to specify the desired phone to use the resource file, the access URL of resource file should be specified in the MAC-Oriented CFG file. During provisioning, the phones will request the resource files in addition to the configuration files. For more information on the access URL of resource file, refer to description of the static.firmware.url parameter on page 94.

Language packs, ring tones, and local contact file are examples of resource files.

For more information on resource files, refer to "Obtain Configuration Files/Resource Files" below.

To delete resource files from a phone at a later date - for example, if the phone is being given to a new user –reset the phone to factory configuration settings. For more information, refer to "Resetting Issues" on page 372.

Obtain Configuration Files/Resource Files

Crestron supplied template configuration and resource files can be directly edited and customized as required. Files can be downloaded from the DOCUMENTATION section of each product page on the Crestron website.

Website Details

Phone Model	website
UC-PHONE-S-PLUS	www.crestron.com/direct/uc-p110-s
UC-PHONE-S	www.crestron.com/direct/uc-p100-s

The names of the Crestron-supplied template files are:

Template File Details

Template File		File Name	Description
Configuration Files	Common CFG File	Common.cfg	To deploy and maintain a block of Crestron phones. For more information, refer to "Common CFG File on page 86 and "MAC-Oriented CFG File" on page 86.
	MAC-Oriented CFG File	MAC.cfg	
Resource Files	AutoDST Template	AutoDST.xml	Modify time zone and DST settings for an area. For more information, refer to "Customize an AutoDST Template File" on page 150.
	Dial Now Template	dialnow.xml	Customize multiple dial now rules for phone. For more information, refer to "Customize a Dial-Now Template File" on page 166.
	Local Contact File	contact.xml	Add or modify multiple local contacts at a time for a phone. For more information, refer to "Customize a Local Contact File" on page 171.

For some features, the filename can be customized customize as required. The following table lists the special characters supported by these phones.

Supported Special Characters

Platform	Server	
	HTTP/HTTPS	TFTP/FTP
Windows	**Supported:** ~ ` ! @ $ ^ ( ) _ - , . ' ; [ ] { } (including space)	**Supported:** ~ ` ! @ $ ^ ( ) _ - , . ' ; [ ] { } % & = + (including space)
	Not Supported: | < > : " / \ * ? # % & = +	**Not Supported:** | < > : " / \ * ? #

Platform	Server	
	HTTP/HTTPS	TFTP/FTP
Linux	**Supported:** ~ ` ! @ $ ^ ( ) _ - , . ' ; [ ] { } | < > : " (including space)	**Supported:** ~ ` ! @ $ ^ ( ) _ - , . ' ; [ ] { } | < > : " % & = + (including space)
	Not Supported: / \ * ? # % & = +	**Not Supported:** / \ * ? #

Set up a Provisioning Server

This section provides basic instructions for setting up a provisioning server and deploying phones from the provisioning server.

Why Use a Provisioning Server?

A provisioning server can be used to configure the phones, and allows for flexibility in upgrading, maintaining and configuration. Configuration files and resource files are normally located on this server.

When phones are triggered to perform auto provisioning, the phone will request to download the configuration files from the provisioning server. During the auto provisioning process, the phone will download and update configuration files to the phone's flash memory. For more information on auto provisioning, refer to the UC-PHONE Auto Provisioning Desk Phones for Microsoft® Teams® and Skype® for Business Supplemental Guide (Doc. 8368) at www.crestron.com/manuals.

Supported Provisioning Protocols

Skype for Business phones perform the auto provisioning function of downloading configuration files, downloading resource files and upgrading firmware. The transfer protocol is used to download files from the provisioning server. Skype for Business phones support several transport protocols for provisioning, including FTP, TFTP, HTTP, and HTTPS protocols. The transport protocol can be specified in the provisioning server address, for example, http://xxxxxxx. If not specified, the TFTP protocol is used. The provisioning server address can be an IP address, domain name or URL. If a user name and password are specified as part of the provisioning server address, for example, http://user:pwd@server/dir, they will be used only if the server supports them.

NOTES:

- A URL should contain forward slashes only and should not contain spaces. Escape characters are not supported.
- If a user name and password are not specified as part of the provisioning server address, the user name and password of the provisioning server configured on the phone will be used.
- There are two types of FTP methods—active and passive. The phones are not compatible with active FTP.

Configure a Provisioning Server

The provisioning server can be set up on the local LAN or anywhere on the Internet. We recommend using the following procedure if this is the first time setting up a provisioning server. For more information on how to set up a provisioning server, refer to UC-PHONE Auto Provisioning Desk Phones for Microsoft® Teams and Skype® for Business Supplemental Guide (Doc. 8368).

To set up the provisioning server:

1. Install a provisioning server application or locate a suitable existing server.
2. Create an account and home directory.
3. Set security permissions for the account.
4. Create configuration files and edit them as needed.
5. Copy the configuration files and resource files to the provisioning server.

For more information on how to deploy phones using configuration files, refer to "Deploy Phones from the Provisioning Server" below.

NOTE: Typically all phones are configured with the same server account, but the server account provides a means of conveniently partitioning the configuration. Give each account a unique home directory on the server and change the configuration on a per-line basis.

Deploy Phones from the Provisioning Server

During auto provisioning, the phones download the common configuration file first, and then the MAC-Oriented file. Therefore any parameter in the MAC-Oriented configuration file will override the same one in the common configuration file.

Crestron supplies configuration files for each phone model, which are delivered with the phone's firmware. The configuration files, supplied with each firmware release, must be used with that release. Otherwise, configurations may not take effect, and the phone will behave according to default settings. Before configuring parameters in the configuration files, Crestron recommends creating new configuration files containing only those parameters that require changes.

To deploy Skype for Business phones from the provisioning server:

1. Create per-phone configuration files by performing the following steps:
   a. Obtain a list of phone MAC addresses (the bar code label on the back of the phone or on the outside of the box).
   b. Create per-phone <MAC>.cfg files by using the MAC-Oriented CFG file from the distribution as templates.
   c. Edit the parameters in the file as needed.

2. Create new common configuration files by performing the following steps:
    a. Create <y0000000000xx>.cfg files by using the Common CFG file from the distribution as templates.
    b. Edit the parameters in the file as needed.
3. Copy configuration files to the home directory of the provisioning server.
4. Reboot phones to trigger the auto provisioning process.

Skype for Business phones discover the provisioning server address, and then download the configuration files from the provisioning server.

For more information on configuration files, refer to "Configuration Files" on page 85.

During the auto provisioning process, the phone supports the following methods to discover the provisioning server address:

- **DHCP**: DHCP option can be used to provide the address or URL of the provisioning server to phones. When the phone requests an IP address using the DHCP protocol, the resulting response may contain option 66 or the custom option (if configured) that contains the provisioning server address.
- **Static**: The server address can be manually configured via phone user interface or web user interface.

For more information, refer to the UC-PHONE Auto Provisioning Desk Phones for Microsoft® Teams and Skype® for Business Supplemental Guide (Doc. 8368).

Upgrade Firmware

The phone supports three methods to upgrade phone firmware:

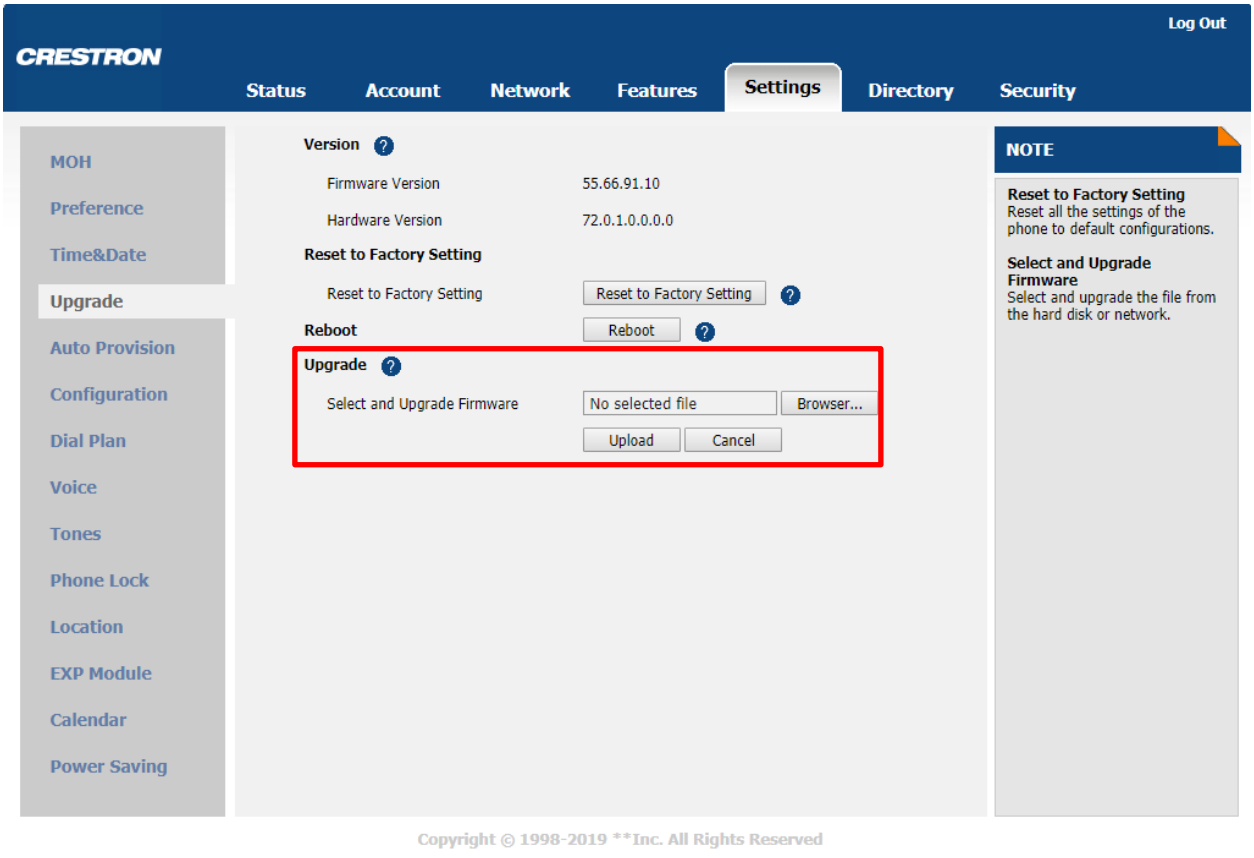
- **Upgrade firmware via the web user interface**: Download firmware in ROM format, and upload it to the phone via web user interface. This method can deploy a single phone.
- **Upgrade firmware from the provisioning server**: Download firmware in ROM format, and use the centralized provisioning method to upgrade the firmware. This method requires setting up a provisioning server, and uses configuration files to provision the phone.
- **Upgrade firmware from the Skype for Business Server**: Download firmware in CAB file format, and place the firmware on Skype for Business Server to provision the phone.

Upgrade Firmware via the Web User Interface

To manually upgrade firmware via the web user interface, store the firmware on a local PC in advance. To upgrade firmware via the web user interface:

1. Click **Settings** > **Upgrade**.

Settings > Upgrade



2. Click **Browser...** to locate the required firmware from the local PC.
3. Click **Upload**.
4. Click **OK** to confirm the upgrade.

NOTE: Do not close and refresh the browser when the Skype for Business phone is upgrading firmware via web user interface.

Upgrade Firmware From the Provisioning Server

Phones support using FTP, TFTP, HTTP and HTTPS protocols to download configuration files and firmware from the provisioning server, and then upgrade firmware automatically.

Phones can download firmware stored on the provisioning server in one of two ways:

- Check for configuration files and then download firmware during startup.

- Automatically check for configuration files and then download firmware at a fixed interval or specific time.

The method of checking for configuration files is configurable.

Configuration changes can be performed using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	<**y0000000000xx**>.cfg	Configure the way for the phone to check for configuration files. **Parameters:** static.auto_provision.power_on static.auto_provision.repeat.enable static.auto_provision.repeat.minutes static.auto_provision.weekly.enable static.auto_provision.weekly.begin_time static.auto_provision.weekly.end_time static.auto_provision.weekly.dayofweek
		Specify the access URL of firmware. **Parameter:** static.firmware.url
		Configure the phone to be reset to factory after an upgrade. **Parameter:** static.auto_provision.reset_factory.enable
Local	Web User Interface	Configure the way for the phone to check for configuration files. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-autop&q=load

Details of the Configuration Parameters

Parameter	Permitted Values	Default
static.auto_provision.power_on	**0 or 1**	**1**
Description: Triggers the power on feature to on or off. **Off**, the phone will not perform an auto provisioning process when powered on. **On**, the phone will perform an auto provisioning process when powered on. **Web User Interface:** Settings > Auto Provision > Power On **Phone User Interface:** None		

Parameter	Permitted Values	Default
static.auto_provision.repeat.enable	0 or 1	0
Description: Triggers the auto provision repeatedly feature to on or off. **Off**, the phone will not perform an auto provisioning process repeatedly. **On**, the phone will perform an auto provisioning process repeatedly. **Web User Interface:** Settings > Auto Provision > Repeatedly **Phone User Interface:** None		
static.auto_provision.repeat.minutes	Integer from 1 to 43200	1440
Description: Configures the interval (in minutes) for the phone to perform an auto provisioning process repeatedly. **Note:** This feature works only if the value of the parameter "static.auto_provision.repeat.enable" is set to 1 (On). **Web User Interface:** Settings > Auto Provision > Interval(Minutes) **Phone User Interface:** None		
static.auto_provision.weekly.enable	0 or 1	0
Description: Triggers the weekly feature to on or off. **Off** **On**, the phone will perform an auto provisioning process weekly. **Web User Interface:** Settings > Auto Provision > Weekly **Phone User Interface:** None		
static.auto_provision.weekly.begin_time	Time from 00:00 to 23:59	00:00
Description: Configures the begin time of the day for the phone to perform an auto provisioning process weekly. **Note:** This feature works only if the value of the parameter "static.auto_provision.weekly.enable" is set to 1 (On). **Web User Interface:** Settings > Auto Provision > Time **Phone User Interface:** None		

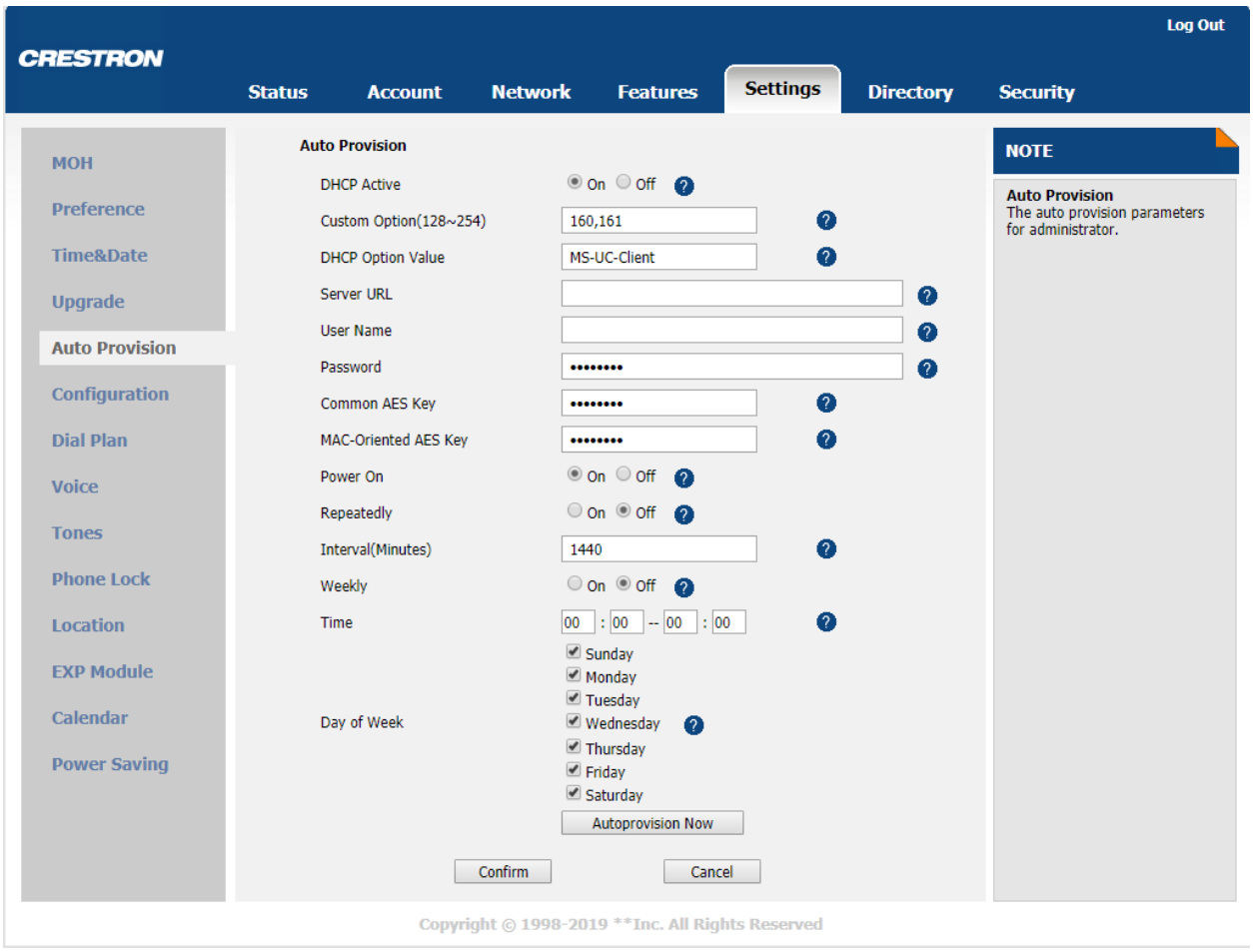
Parameter	Permitted Values	Default
static.auto_provision.weekly.end_time	Time from 00:00 to 23:59	00:00
Description: Configures the end time of the day for the phone to perform an auto provisioning process weekly. Auto provisioning will not be performed after the end time. **Note:** This feature works only if the value of the parameter "static.auto_provision.weekly.enable" is set to 1 (On). **Web User Interface:** Settings > Auto Provision > Time **Phone User Interface:** None		
static.auto_provision.weekly.dayofweek	0, 1, 2, 3, 4, 5, 6 or a combination of these digits	0123456
Description: Configures the days of the week for the phone to perform an auto provisioning process weekly. **0**- Sunday **1**- Monday **2**- Tuesday **3**- Wednesday **4**- Thursday **5**- Friday **6**- Saturday **Example:** static.auto_provision.weekly.dayofweek = 01 The phone will perform an auto provisioning process every Sunday and Monday. **Note:** This feature works only if the value of the parameter "static.auto_provision.weekly.enable" is set to 1 (On). **Web User Interface:** Settings > Auto Provision > Day of Week **Phone User Interface:** None		
static.firmware.url	URL within 511 characters	Blank
Description: Configures the access URL of the firmware file. **Example:** static.firmware.url = http://192.168.1.20/66.9.0.30.rom **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Settings > Upgrade > Select and Upgrade Firmware **Phone User Interface:** None		

Parameter	Permitted Values	Default
static.auto_provision.reset_factory.enable	0 or 1	0
Description: Enables or disables the phone to be reset to the factory default settings. **0**- Disabled **1**- Enabled **Note**: The phone can be reset to the factory default settings using this parameter once only.		

Configure the Way the Phone Checks for Configuration Files via the Web User Interface

1. Click **Settings** > **Auto Provision.**

Settings > Auto Provision



2. Make the necessary change.
3. Click **Confirm** to accept the change.

When the **Power On** setting is set to **On**, the phone will check configuration files stored on the provisioning server during startup and then download firmware from the server.

Upgrade Firmware from the Skype for Business Server

Firmware can be updated from the Skype for Business Server. Before updating the firmware, the update package (*.CAB) must be uploaded to the Skype for Business Update Server.

Automatic Updates

Update checking time defines a period of time for the phone to automatically check a firmware update on the Skype for Business Server. Update checking time can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure update checking time. **Parameter:** sfb.update_time
Local	Web User Interface	Configure update checking time. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

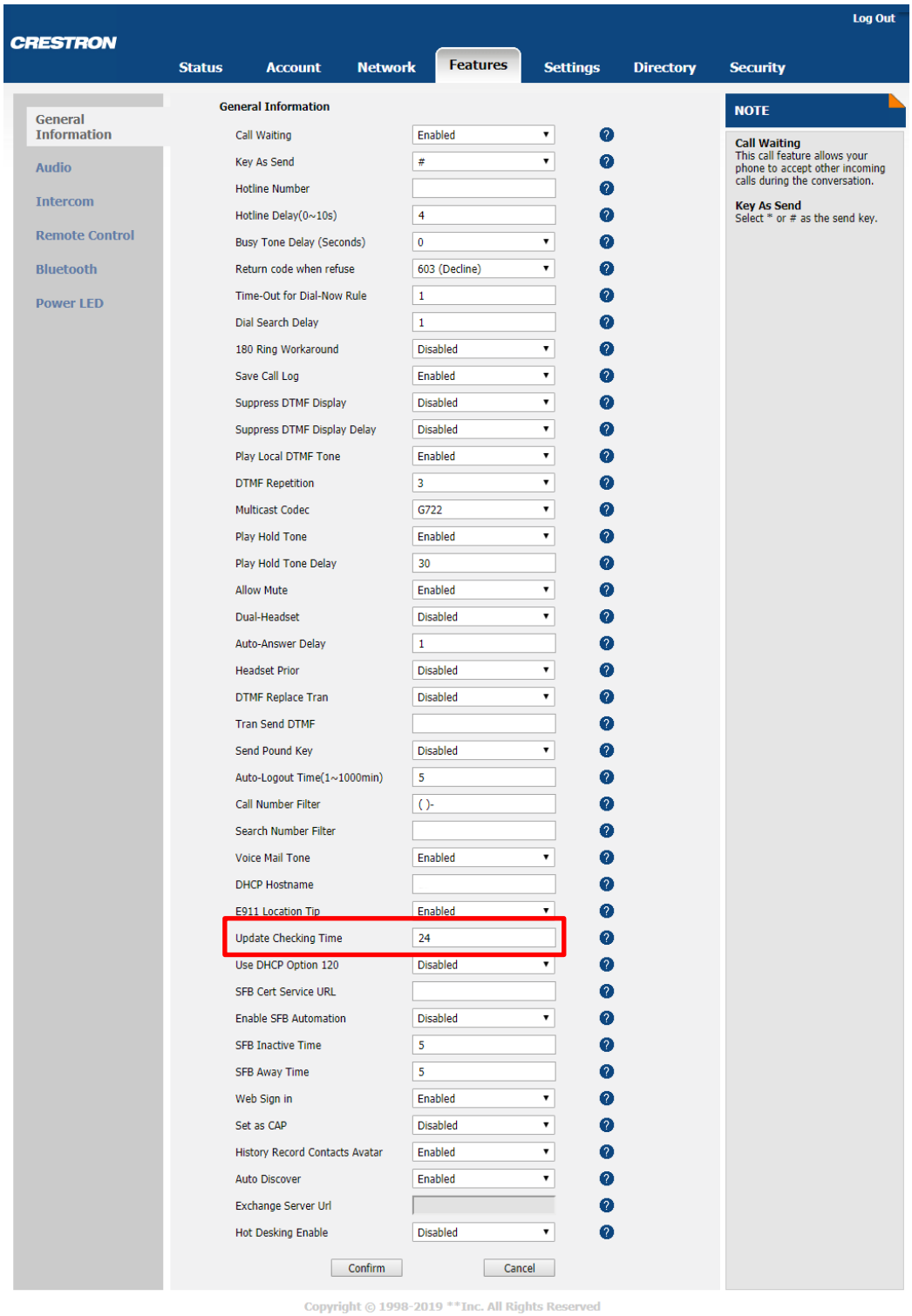
Details of the Configuration Parameter

Parameter	Permitted Values	Default
sfb.update_time	**Integer from 1 to 48**	**24**
Description: Configures the auto timer (in hours) for the phone to automatically check if there is a firmware update available on Skype for Business Server. If it is set to 24, the phone will check if a firmware update is available on the Skype for Business Server every 24 hours. **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Features > General Information > Update Checking Time **Phone User Interface:** None		

To configure the update checking time via the web user interface:

1. Click **Features** > **General Information**.

Features > General Information



2. Enter the Update Checking Time in the **Update Checking Time** field. A dialog box pops up to prompt that settings will take effect after a reboot.
3. Click **Confirm** to accept the change.

Update Firmware Manually

An update can be initiated immediately, just power off the phone and apply power again. The phone will boot up, check for updates and apply the updates. An update can also be triggered manually via the phone user interface.

To trigger an update manually via phone user interface:

1. Tap **Setting** > **Advanced**.
2. Enter the Admin password (default password: admin), and then tap **OK**.
3. Tap **Firmware Update** on the left side of the display.
4. Tap **Firmware Update** on the right side of the display.

Configure Basic Features

Sign Into Skype for Business

Skype for Business users are authenticated against the Microsoft Active Directory Domain Service. The following sign-in methods are available.

- **User Sign-in**: This method uses the user's credentials (sign-in address, user name, and password) to sign into the Skype for Business server. This sign-in method is applicable to On-Premises and Online accounts.
- **Web Sign-in:** This method uses the unique website shown on the phone to sign in. This sign-in method is only applicable to an Online account.

NOTE: If the phone reboots after successful login, the login credentials from the previous Sign-In will be cached. The user can sign in successfully without reentering their credentials.

If Active Directory Federation Services (ADFS) or Single Sign-On (SSO) authentication method is used, the user sign-in or web sign-in method can still be used to sign into Skype for Business successfully.

User Sign-In

Microsoft Skype for Business can be signed into on a phone with the user's login credentials, which includes the user's address, username, and password.

The user sign-in method can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure user sign-in method. **Parameter:** features.user_sign_in.enable
	<MAC>.cfg	Configure user sign-in information. **Parameters:** static.account.sfb.1.server static.account.sfb.1.user_name static.account.sfb.1.password
Local	Web User Interface	Configure user sign-in method. **Navigate to:** http://<phoneIPAddress>/servlet?p=account-register-lync&q=load&acc=0
	Phone User Interface	Configure user sign-in information.

Details of the Configuration Parameters

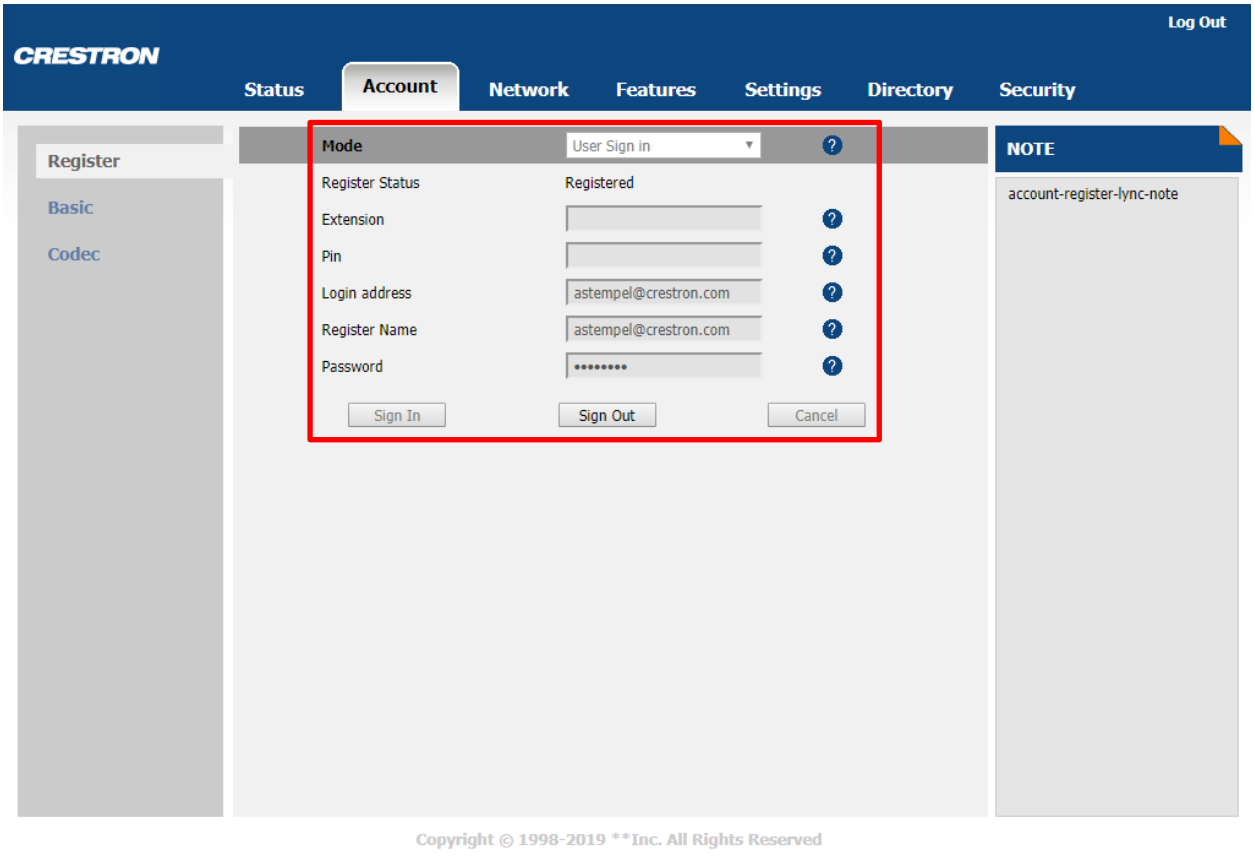
Parameter	Permitted Values	Default
features.user_sign_in.enable	**0 or 1**	**1**
Description: Enables or disables the User Sign-in method. **0**- Disabled **1**- Enabled **Web User Interface:** None **Phone User Interface:** None		
static.account.sfb.1.server	**SIP URI**	**Blank**
Description: Configures the sign-in address for the user sign-in method. The value format is username@domain.com. **Example:** static.account.sfb.1.server = 4040@crestronsfb.com **Web User Interface:** Account > Register > Login address **Phone User Interface:** Sign in > User Sign-in > Address		

Parameter	Permitted Values	Default
static.account.sfb.1.user_name	**String within 128 characters**	**Blank**
Description: Configures the user name for the user sign-in method. The value format is username@domain.com or username@domain, domain.com\username or domain\username. **Example:** static.account.sfb.1.user_name= 4040@crestronsfb.com **Web User Interface:** Account > Register > Register Name **Phone User Interface:** Sign in > User Sign-in > UserName		
static.account.sfb.1.password	**String within 99 characters**	**Blank**
Description: Configures the password for the user sign-in method. **Web User Interface:** Account > Register > Password **Phone User Interface:** Sign in > User Sign-in > Password		

Sign into the Skype for Business Server with User Sign-In via the Web User Interface

1. Click **Account** > **Register**.

Account > Register



2. Select **User Sign in** from the **Mode** drop-down list.
3. Enter the Skype for Business user's sign-in address (e.g., 4040@crestronsfb.com) in the **Login address** field.
4. Enter the Skype for Business user name (e.g., 4040@crestronsfb.com) in the **Register Name** field.
5. Enter the sign-in password in the **Password** field.
6. Click **Sign In** to accept the change.

Sign into the Skype for Business Server with User Sign-In via the Phone User Interface

1. Tap **User Sign-In**.
2. Enter the Skype for Business user's sign-in address (e.g., 4040@crestronsfb.com) in the **Sign-in Address** field.

3. Enter the Skype for Business user name (e.g., 4040@crestronsfb.com) in the **UserName** field.
4. Enter the sign-in password in the **Password** field.
5. Tap **Sign in**.

Web Sign-in

The Web Sign-In method can be used to sign into a Skype for Business Online account using a web browser.

Web sign-in can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the web sign-in method. **Parameter:** features.web_sign_in.enable
		Configure the Server URL for device pairing. **Parameter:** features.device_pairing.url
Local	Web User Interface	Configure web sign-in method. **Navigate to:** http://<phoneIPAddress>/servlet?p=account-register-lync&q=load&acc=0
	Phone User Interface	Configure web sign-in method.

Details of the Configuration Parameters

Parameter	Permitted Values	Default
features.web_sign_in.enable	**0 or 1**	**1**
Description: Enables or disables the user to sign into the phone using web sign-in method. **0**- Disabled **1**- Enabled **Web User Interface:** Features > General Information > Web Sign in **Phone User Interface:** None		

Parameter	Permitted Values	Default
features.device_pairing.url	URL within 512characters	https://bootstrap.pinauth.services.skypeforbusiness.com/

Description:

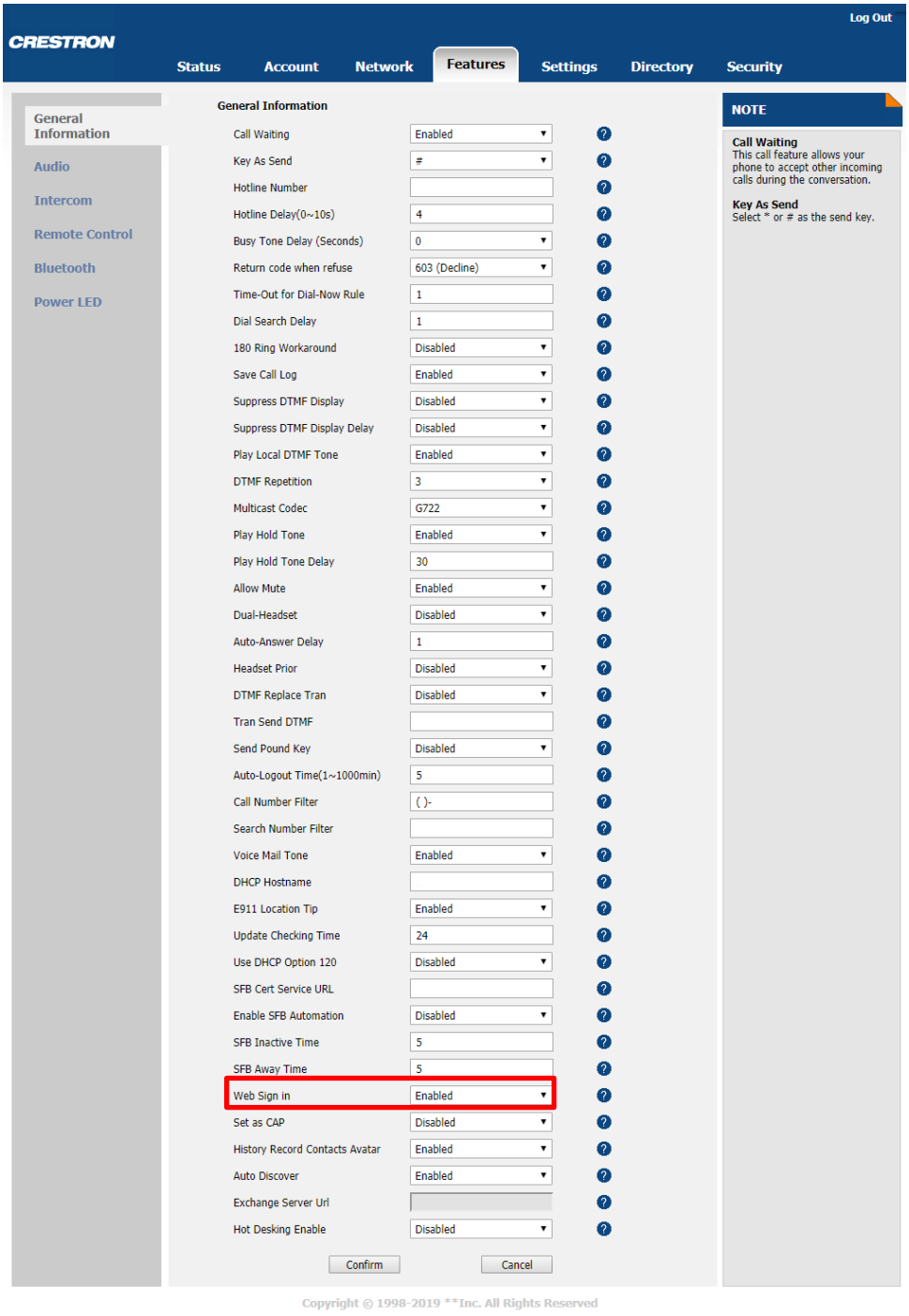
Configures the Server URL for device pairing, so that the phone can be signed into using the web sign-in method.

Example:
features.device_pairing.url= https://bootstrap.pinauth.services.skypeforbusiness.com/

Enable Web Sign-In via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Select **Enabled** or **Disabled** from the **Web Sign in** drop-down list.
   - If it is enabled, a user can sign into the Skype for Business Server using the web sign-in method.

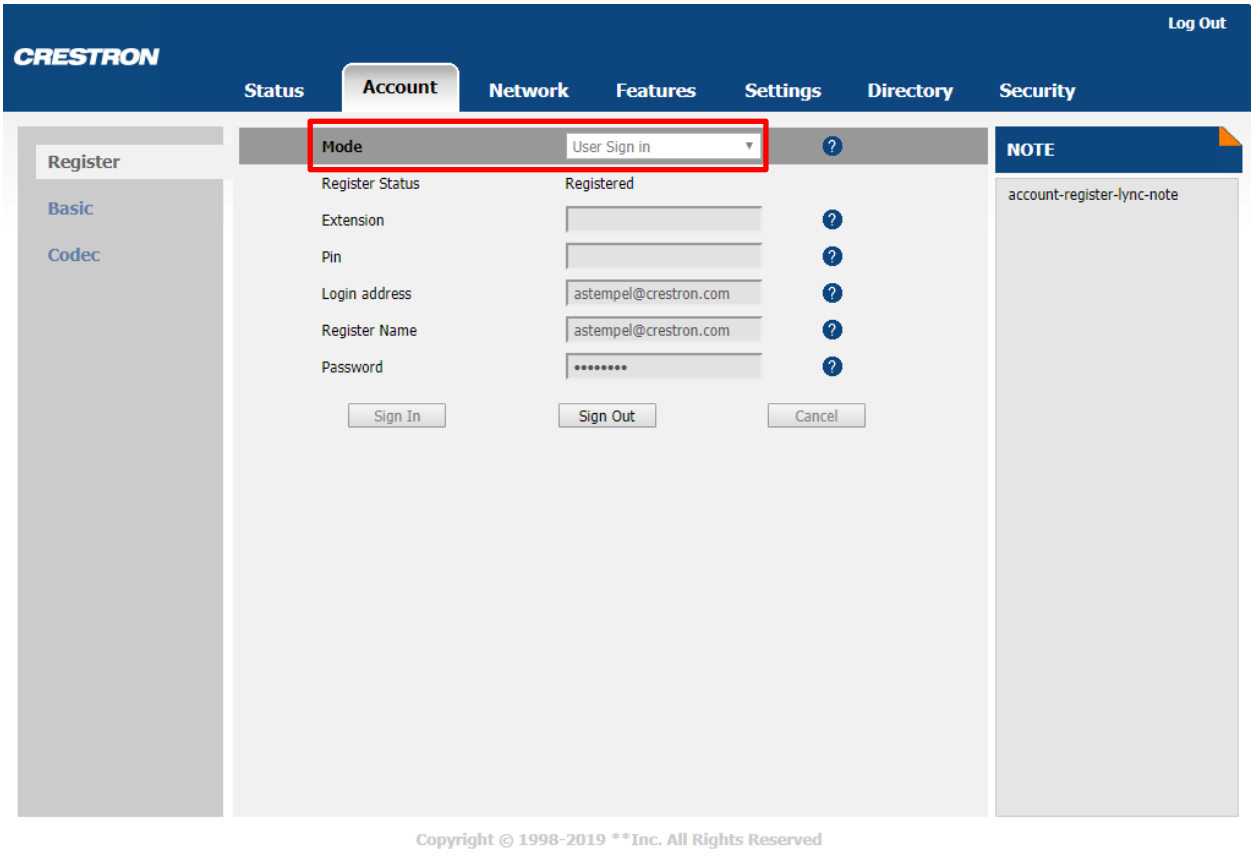
– If it is disabled, a user cannot sign into the Skype for Business Server using the web sign-in method.

3. Click **Confirm** to accept the change.

Sign Into the Skype for Business Server with the Web Sign-In method via the Web User Interface

1. Click **Account** > **Register**.

Account > Register



2. Select **Web Sign in** from the **Mode** drop-down list.

Account > Register, Web Sign in

3. Click **Sign in**. The phone will display a URL and a pairing code.
4. Open a web browser to the URL displayed in the previous step and use the displayed pairing code to complete the sign in process.

Sign Into the Skype for Business Server with the Web Sign-In method via the Phone User Interface

1. Tap **Web Sign-in**. The phone will display a URL and a pairing code.
2. Open a web browser to the URL displayed in the previous step and use the displayed pairing code to complete the sign in process.

Sign Out of Skype for Business

The Skype for Business Server can be signed out of via web or phone user interface directly.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the sign out feature. **Parameter:** phone_setting.idle_sign_out. enable
Local	Web User Interface	Sign out of Skype for Business Server. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-register-lync&q=load&acc=0
	Phone User Interface	Sign out of Skype for Business Server.

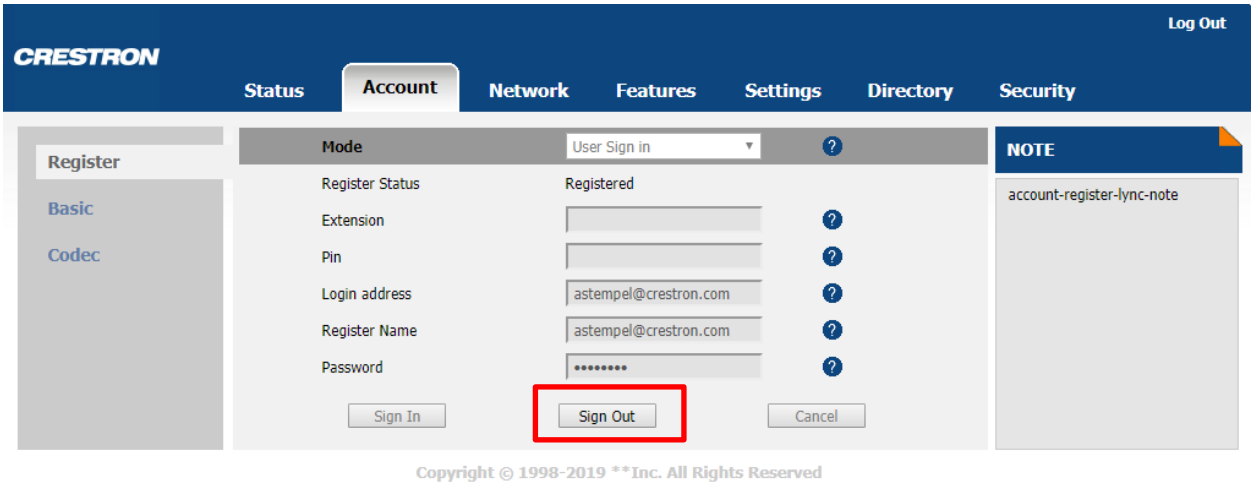
Details of the Configuration Parameter

Parameter	Permitted Values	Default
phone_setting.idle_sign_out.enable	**0 or 1**	**1**
Description: Enables or disables the phone to sign out of Skype for Business Server from the idle screen. **0**- Disabled, the Skype for Business Server can be signed out of on the phone by navigating to **Menu** > **Setting** > **Advanced** > **Sign Out**. **1**- Enabled, the Skype for Business Server can be signed out of by tapping on the avatar, and then selecting **Sign Out**.		

Sign Out of the Skype for Business Server via the Web User Interface

1. Click **Account** > **Register**.

Account > Register



2. Click **Sign Out** to accept the change.

Sign Out of the Skype for Business Server via the Phone User Interface

1. Tap the user icon on the top right of the display.
2. Tap **Sign Out**.
3. Tap **OK** to confirm or **Cancel** to cancel. The phone signs out of the Skype for Business Server.

After signing out of Skype for Business, the account-related features (call or view Skype for Business contacts, etc.) are not available. However, other available features can still be used.

Microsoft Exchange Integration

The Skype for Business phone can obtain the Microsoft Exchange Server address automatically via Auto discover request. This feature enables visual voicemail setup, call log synchronization, Outlook® contact search, and calendar retrieval.

If a phone fails to obtain the Microsoft Exchange Server address automatically, the address can be manually configured.

Microsoft Exchange Server can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configures the way to obtain the Microsoft Exchange Server address. **Parameter:** phone_setting.ews_autodiscover.enable
		Specify the Microsoft Exchange Server address manually. **Parameter:** phone_setting.ews_url
Local	Web User Interface	Configures the way to obtain the Microsoft Exchange Server address. Specify the Microsoft Exchange Server address. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

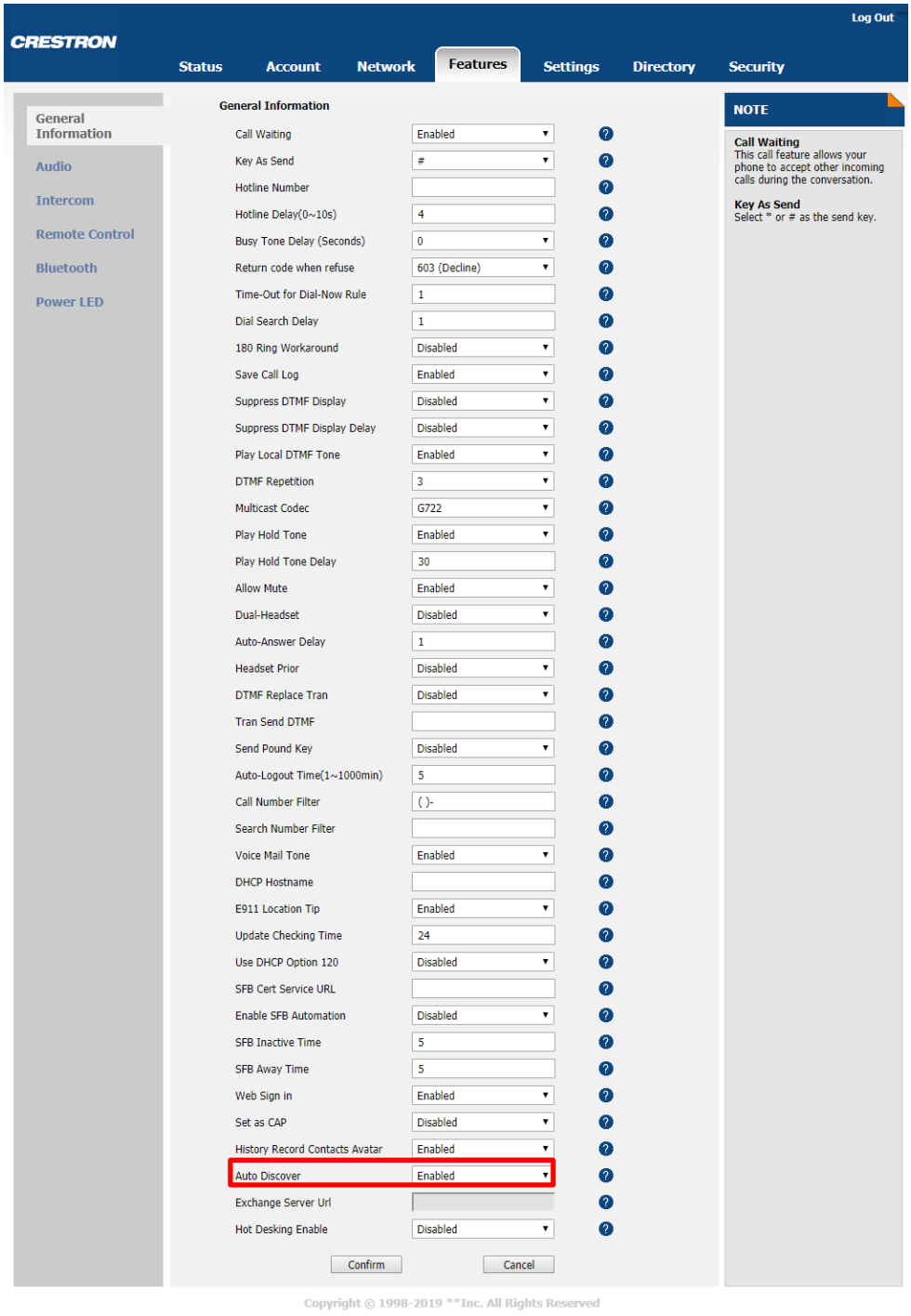
Details of the Configuration Parameters

Parameter	Permitted Values	Default
phone_setting.ews_autodiscover.enable	**0 or 1**	**1**
Description: Enables or disables the phone to obtain the Microsoft Exchange Server address automatically via Auto discover request. **0**- Disabled, the phone does not obtain the Microsoft Exchange Server address automatically via Auto discover request. The Microsoft Exchange Server address must be configured manually. **1**- Enabled, the phone will obtain the Microsoft Exchange Server address automatically via Auto discover request. **Web User Interface:** Features > General Information > Auto Discover **Phone User Interface:** None		
phone_setting.ews_url	**String**	**Blank**
Description: Specify the Microsoft Exchange Server address manually. **Note:** This feature works only if the value of the parameter "phone_setting.ews_autodiscover.enable" is set to **0** (Disabled). **Web User Interface:** Features > General Information > Exchange Server Url **Phone User Interface:** None		

Configure the Microsoft Exchange Server via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Do one of the following:
   - Select **Enabled** from the **Auto Discover** drop-down list to have the phone obtain the Microsoft Exchange Server address automatically.
   - Select **Disabled** from the **Auto Discover** drop-down list to enter the Microsoft Exchange Server address in the Exchange Server Url field.
3. Click **Confirm** to accept the change.

Exchange Authentication

Exchange authentication must be passed to access features associated with the Microsoft Exchange Server (history records, voice mail, Outlook contacts and calendars). By default, a phone will pass Exchange authentication automatically when accessing these features. Exchange authentication information may need to be entered manually when login password expires, or is changed by the system administrator.

Exchange authentication can be configured using the configuration files only.

Configuration Methods

Central Provisioning (Configuration File)	**<MAC>.cfg**	Configures the Exchange address for accessing the Microsoft Exchange Server. **Parameter:** static.account.sfb.1.ews.auth_address
		Configures the user name for accessing the Microsoft Exchange Server. **Parameter:** static.account.sfb.1.ews.auth_user
		Configures the password for accessing the Microsoft Exchange Server. **Parameter:** static.account.sfb.1.ews.auth_pwd
	<y0000000000xx>.cfg	Configures the phone to pop up a reminder about Exchange authentication failure. **Parameter:** phone_setting.ews_auth_popup.enable
Local	Phone User Interface	Configure the Exchange authentication information.

Details of the Configuration Parameters

Parameter	Permitted Values	Default
static.account.sfb.1.ews.auth_address	String within 128 characters	Blank
Description: Configures the Exchange address for accessing the Microsoft Exchange Server. **Example:** static.account.sfb.1.ews.auth_address = yl39@redmond.crestronsfb.com **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** On the authentication dialog box > Sign in address		
static.account.sfb.1.ews.auth_user	String within 129 characters	Blank
Description: Configures the user name for accessing the Microsoft Exchange Server. **Note**: If the parameter is changed, the phone will reboot to make the change take effect. **Example:** static.account.sfb.1.ews.auth_user = yl39@crestronsfb.com **Web User Interface:** None **Phone User Interface:** On the authentication dialog box > User name		
static.account.sfb.1.password	String within 130 characters	Blank
Description: Configures the password for accessing the Microsoft Exchange Server. **Note**: If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** On the authentication dialog box > Password		
phone_setting.ews_auth_popup.enable	0 or 1	1
Description: It enables or disables the phone to pop up a reminder about if the Exchange authentication failed. **0**- Disabled **1**- Enabled **Web User Interface:** None **Phone User Interface:** None		

Update Status Automatically

The Skype for Business Server helps keep a user's presence information up-to-date by monitoring idle time of their phone. Phone status turns to Inactive when a phone has been idle for the designated time. Phone status will change from Inactive to Away after another designated time.

Updating status automatically can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configures the inactive time (in minutes) of the phone. **Parameters:** sfb.presence.inactive_time sfb.presence.away_time
Local	Web User Interface	Configures the inactive time (in minutes) of the phone. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of the Configuration Parameters

Parameter	Permitted Values	Default
sfb.presence.inactive_time	**Integer from 5 to 360**	**5**

Description:

Configures the inactive time (in minutes) of the phone, after which the phone will change its status to Inactive automatically.

Example:
If it is set to 5, the phone will change its status to Inactive automatically after the phone has been inactive for 5 minutes.

Note: If the parameter is changed, the phone will reboot to make the change take effect.

Web User Interface:
Features > General Information > SFB Inactive Time

Phone User Interface:
None

Parameter	Permitted Values	Default
sfb.presence.away_time	Integer from 5 to 360	5

Description:

Configures the inactive time (in minutes) of the phone, after which the phone will change its status from Inactive to Away automatically.

Example:
If it is set to 5, the phone whose status is Inactive will change to Away automatically after 5 minutes.

Note: If the parameter is changed, the phone will reboot to make the change take effect.

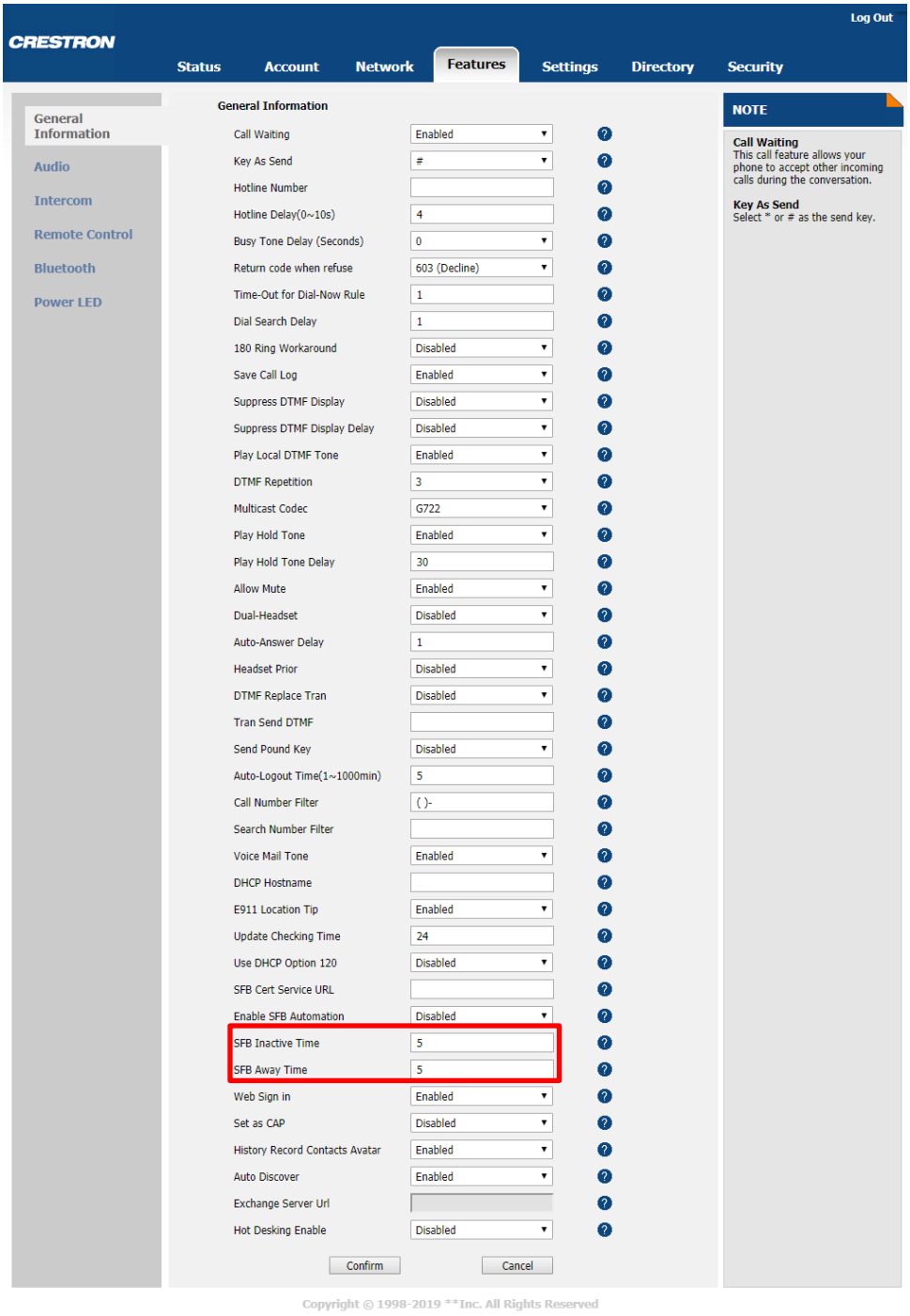
Web User Interface:
Features > General Information > SFB Away Time

Phone User Interface:
None

Configure the Automatic Status Updating Time via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Enter the inactive time in the **SFB Inactive Time** field.
3. Enter the away time in the **SFB Away Time** field.

4. Click **Confirm** to accept the change.

Always Online

The Always Online feature allows the phone to maintain the current status until it is manually changed. For example, the current status of the phone is **Available**, if the always online feature is enabled, then the phone status will stay **Available** until it is manually changed.

Always Online can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure always on line. **Parameter:** sfb.always_online.enable
Local	Web User Interface	Configure always on line. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0

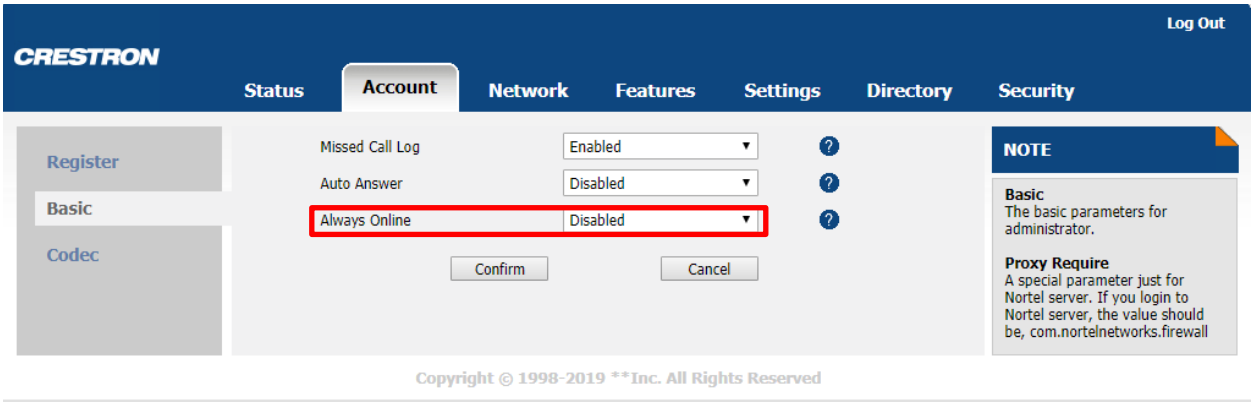
Details of the Configuration Parameter

Parameter	Permitted Values	Default
sfb.always_online.enable	**0 or 1**	**0**
Description: Enables or disables the phone to maintain current status until it is manually changed. **0**- Disabled **1**- Enabled **Note:** If the phone status is set to Do Not Disturb (DND) before dialing an emergency number, then the phone status will be changed to available after the emergency call even if the value of this parameter is set to 1 (Enabled). **Web User Interface:** Account > Basic > Always Online **Phone User Interface:** Menu > Setting > Basic > Always Online		

Configure Always Online via the Web User Interface

1. Click **Account** > **Basic**

Account > Basic



2. Select **Enabled** or **Disabled** from the **Always Online** drop-down list.
3. Click **Confirm** to accept the change.

Power LED Indicator

Power LED Indicator indicates power status and phone status. There are seven configuration options for the Power LED Indicator:

- **Common Power Light On:** Common Power Light On allows the Power LED Indicator to be turned on.
- **Ring Power Light Flash:** Ring Power Light Flash allows the Power LED Indicator to flash when the phone receives an incoming call.
- **Voice Mail Power Light Flash:** Voice Mail Power Light Flash allows the Power LED Indicator to flash when the phone receives a voice mail.
- **Mute Power Light On:** Mute Power Light On allows the Power LED Indicator to flash when a call is muted.
- **Hold/Held Power Light On:** Hold/Held Power Light On allows the Power LED Indicator to flash when a call is placed on hold or is held.
- **Talk/Dial Power Light On:** Talk/Dial Power Light On allows the Power LED Indicator to be turned on when the phone is busy.
- **Boss/Admin Power Light On:** Boss/Admin Power Light On allows the Power LED Indicator to be turned on when using the Boss-Admin Feature.

The Power LED Indicator can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the Power LED Indicator. **Parameters:** phone_setting.common_power_led_enable phone_setting.ring_power_led_flash_enable phone_setting.mail_power_led_flash_enable phone_setting.mute_power_led_flash_enable phone_setting.hold_and_held_power_led_flash_enable phone_setting.talk_and_dial_power_led_enable phone_setting.boss_admin.talk_power_light.enable
Local	Web User Interface	Configure the Power LED Indicator. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-powerled&q=load

Details of the Configuration Parameters

Parameter	Permitted Values	Default
phone_setting.common_power_led_enable	**0 or 1**	**0**
Description: Enables or disables the Power LED Indicator to be turned on. **0**- Disabled (Power LED Indicator is off) **1**- Enabled (Power LED Indicator glows red) **Web User Interface:** Features > LED > Common Power Light On **Phone User Interface:** None		
phone_setting.ring_power_led_flash_enable	**0 or 1**	**1**
Description: Enables or disables the Power LED Indicator to flash when the phone receives an incoming call. **0**- Disabled (Power LED Indicator does not flash) **1**- Enabled (Power LED Indicator fast flashes (300ms) red) **Web User Interface:** Features > LED > Ring Power Light Flash **Phone User Interface:** None		

Parameter	Permitted Values	Default
phone_setting.mail_power_led_flash_enable	0 or 1	0
Description: Enables or disables the Power LED Indicator to flash when the phone receives a voice mail. **0**- Disabled (Power LED Indicator does not flash) **1**- Enabled (Power LED Indicator slow flashes (1000ms) red) **Web User Interface:** Features > LED > Voice Mail Power Light Flash **Phone User Interface:** None		
phone_setting.mute_power_led_flash_enable	0 or 1	0
Description: Enables or disables the Power LED Indicator to flash when a call is muted. **0**- Disabled (Power LED Indicator does not flash) **1**- Enabled (Power LED Indicator fast flashes (300ms) red) **Web User Interface:** Features > LED > Mute Power Light On **Phone User Interface:** None		
phone_setting.hold_and_held_power_led_flash_enable	0 or 1	0
Description: Enables or disables the Power LED Indicator to flash when a call is placed on hold or is held. **0**- Disabled (Power LED Indicator does not flash) **1**- Enabled (Power LED Indicator fast flashes (500ms) red) **Web User Interface:** Features > LED > Hold/Held Power Light On **Phone User Interface:** None		
phone_setting.talk_and_dial_power_led_enable	0 or 1	0
Description: Enables or disables the Power LED Indicator to be turned on when the phone is busy. **0**- Disabled (Power LED Indicator is off) **1**- Enabled (Power LED Indicator glows red) **Web User Interface:** Features > **LED** > Talk/Dial Power Light On **Phone User Interface:** None		

Parameter	Permitted Values	Default
phone_setting.boss_admin.talk_power_light.enable	0 or 1	0

Description:

Enables or disables the Power LED Indicator to be turned on when using the Boss-Admin feature.

0- Disabled (Power LED Indicator is off)

1- Enabled (Power LED Indicator is solid red)

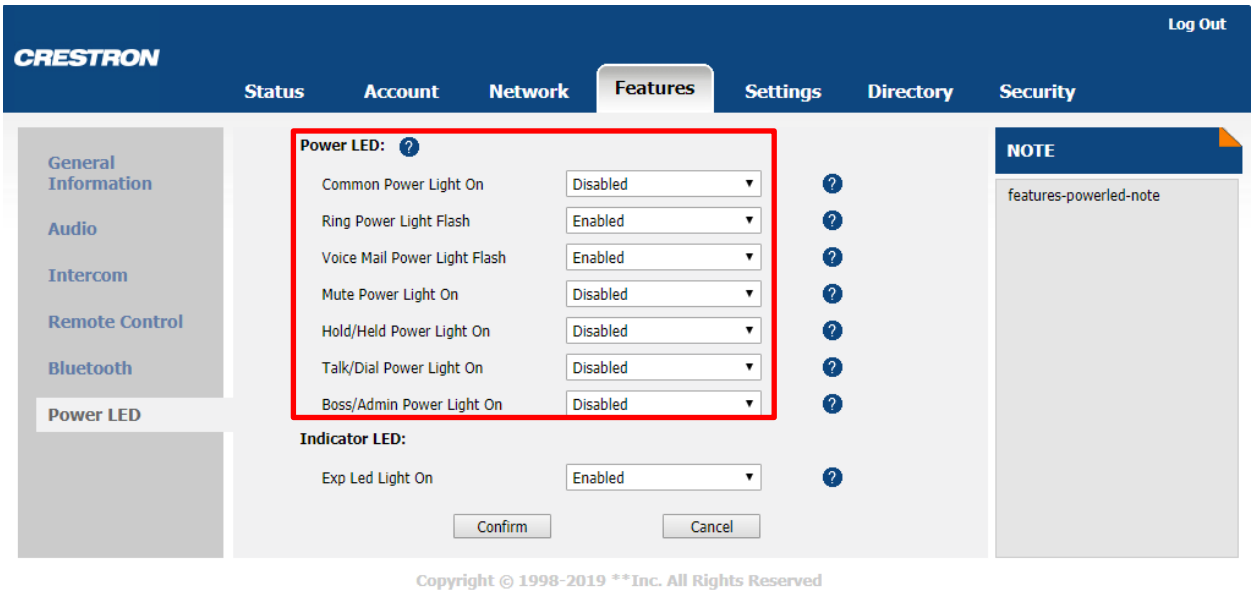
Web User Interface:
Features > LED > Boss/Admin Power Light On

Phone User Interface:
None

Configure the Power LED Indicator via the Web User Interface

1. Click **Features** > **Power LED**.

Features > Power LED



2. Select **Enabled** or **Disabled** from the **Common Power Light On** drop-down list.
3. Select **Enabled** or **Disabled** from the **Ring Power Light Flash** drop-down list.
4. Select **Enabled** or **Disabled** from the **Voice Mail Power Light Flash** drop-down list.
5. Select **Enabled** or **Disabled** from the **Mute Power Light On** drop-down list.
6. Select **Enabled** or **Disabled** from the **Hold/Held Power Light On** drop-down list.
7. Select **Enabled** or **Disabled** from the **Talk/Dial Power Light On** drop-down list.
8. Select **Enabled** or **Disabled** from the **Boss/Admin Power Light On** drop-down list.

9. Click **Confirm** to accept the change.

Screen Saver

The screen saver will automatically start when the phone is idle for the preset waiting time. To stop the screen saver and return to the idle screen at any time, press a key on the phone or tap the touch screen.

Users can select to display the built-in screen saver or a custom screen saver. To set the custom screen saver for the phone, the custom screen saver must be uploaded in advance. If multiple pictures are uploaded, all pictures are displayed in slide-show style when screen saver starts.

The screen saver image format must meet the following:

Screen Saver Image Format

Format	Resolution	Single File Size	Note
*.jpg, *.png, *.bmp, or *.jpeg	<=2.0 megapixels	<=5MB	2MB of space should be reserved for the phone

Screen saver can be configured using the following methods.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the time to wait in the idle state before the screen saver starts. **Parameter:** screensaver.wait_time
		Configure the type of screen saver to display. **Parameter:** screensaver.type
		Specify the access URL of the custom screen saver image. **Parameter:** screensaver.upload_url
		Delete custom screen saver image. **Parameter:** screensaver.delete
		Configure the phone to display the clock and icons when the screen saver starts. **Parameter:** screensaver.display_clock.**enable**
		Configure the interval for the phone to change the picture when the screen saver starts. **Parameter:** screensaver.picture_change_interval

		Configure the interval for the phone to move the clock and icons when the screen saver starts. **Parameter:** screensaver.clock_move_interval
Local	**Web User Interface**	Configure the idle time before the screen saver starts. Configure the type of screen saver to be displayed. Upload the custom screen saver image. Delete custom screen saver images. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-preference&q=load
	Phone User Interface	Configure the screen saver.

Details of the Configuration Parameters

Parameter	Permitted Values	Default
screensaver.wait_time	**15, 30, 60, 120, 300, 600, 1800, 3600, 7200, 10800, 21600**	**21600**

Description:

Configures the time (in seconds) to wait in the idle state before the screen saver starts.

15-15s

30-30s

60-1min

120-2min

300-5min

600-10min

1800-30min

3600-1h

7200-2h

10800-3h

21600-6h

Web User Interface:
Settings > Preference > Screensaver Wait Time

Phone User Interface:
Menu > Setting > Basic > Display > Screensaver > Wait Time

Parameter	Permitted Values	Default
screensaver.type	0 or 1	0

Description:

Configures the type of screen saver to display.

0- System, the LCD screen will display the built-in picture.

1- Custom, the LCD screen will display the custom screen saver images (configured by the parameter "screensaver.upload_url"). If multiple images are uploaded, the phone will display all images alternately. The time interval is configured by the parameter "screensaver.picture_change_interval".

Web User Interface:
Settings > Preference > Screensaver Type

Phone User Interface:
Menu > Setting > Basic > Display > Screensaver > Screensaver Type

Note: This feature is configurable only if custom image file(s) have been uploaded to the phone.

screensaver.upload_url	URL within 511 characters	Blank

Description:

Configures the access URL of the custom screen saver image.

Example:
screensaver.upload_url = http://192.168.10.25/Screencapture.jpg

During the auto provisioning process, the phone connects to the HTTP provisioning server "192.168.10.25", and downloads the screen saver image "Screencapture.jpg".

To download multiple screen saver images to the phone simultaneously, configure as follows:

screensaver.upload_url = http://192.168.10.25/Screencapture.jpg

screensaver.upload_url = http://192.168.10.25/Screensaver.jpg

Note: This feature works only if the value of the parameter "screensaver.type" is set to 1 (Custom).

Web User Interface:
Settings > Preference > Upload Screensaver

Phone User Interface:
None

Parameter	Permitted Values	Default
screensaver.delete	http://localhost/all or http://localhost/name.(jpg/png/bmp)	Blank

Description:

Deletes the specified or all custom screen saver images.

Example:
Delete all custom screen saver images: screensaver.delete = http://localhost/all
Delete a custom screen saver image (e.g., Screencapture.jpg): screensaver.delete = http://localhost/Screencapture.jpg

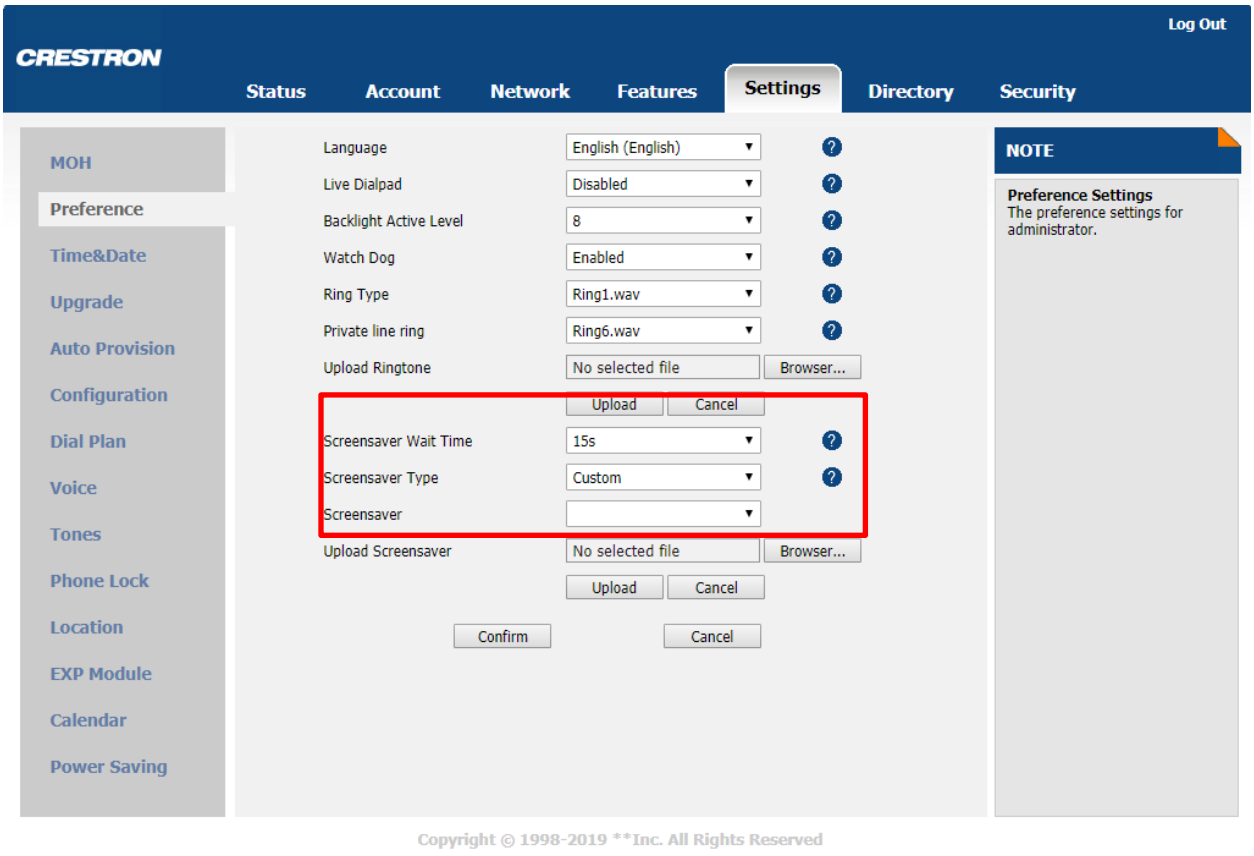
Web User Interface:
Settings > Preference > Del

Phone User Interface:
None

Upload a Custom Screen Saver via the Web User Interface

1. Click **Settings** > **Preference**.

Settings > Preference



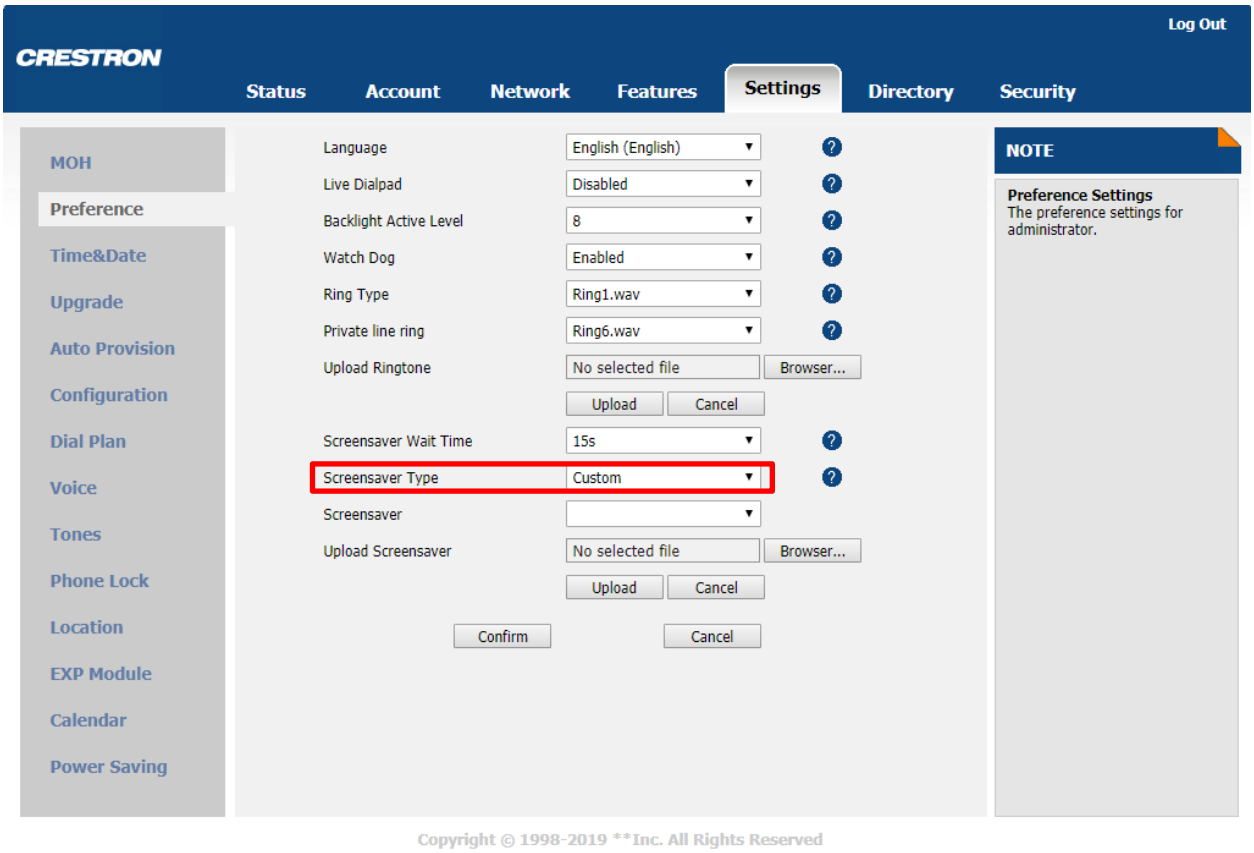
2. Select **Custom** from the **Screensaver Type** drop-down list.

3. In the **Upload Screensaver** field, click **Browser** to locate the custom picture from the local system. The **Upload Screensaver** field appears only if Screensaver Type is set to **Custom**.
4. Click **Upload** to upload the file. The custom screen saver appears in the **Screensaver** drop-down list. The **Screensaver** field appears only if **Screensaver Type** is set to **Custom**.
5. Click **Confirm** to accept the change.

Set the System Screen Saver via the Web User Interface

1. Click **Settings** > **Preference**.

Settings > Preference

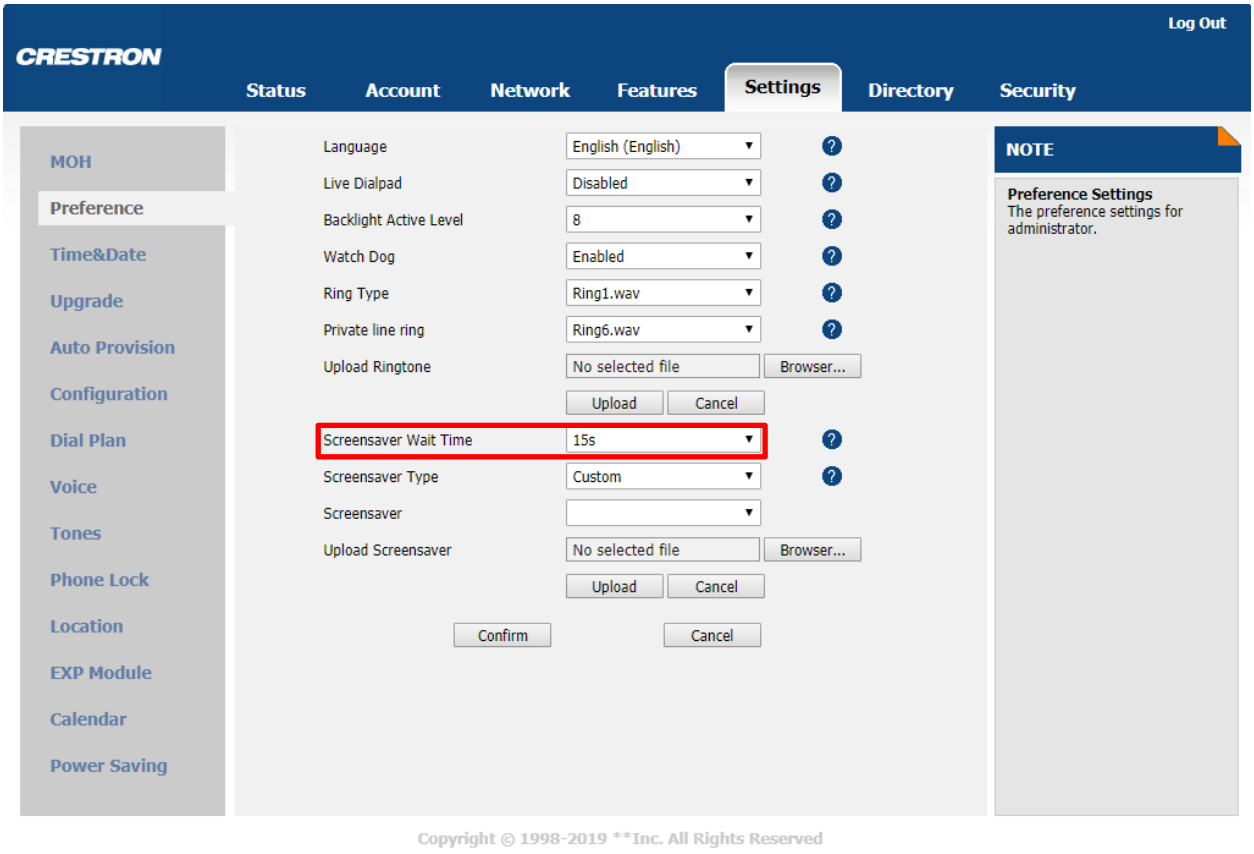


2. Select **System** from the **Screensaver Type** drop-down list.
3. Click **Confirm** to accept the change.

Configure the System Screen Saver Wait Time via the Web User Interface

1. Click **Settings** > **Preference**.

Settings > Preference



2. Select the wait time from the **Screensaver Wait Time** drop-down list.
3. Click **Confirm** to accept the change.

Configure the System Screen Saver via the Web User Interface

1. Tap **Setting** > **Basic** > **Display** > **2. Screen Saver**.
2. Select the wait time from the **Screen Saver Wait Time** drop-down list.
3. Tap the screen saver to use.

Power Saving

The power-saving feature turns off the backlight and screen to conserve energy. The phone enters power-saving mode after it has been idle for a certain period of time. The phone will exit power-saving mode if a phone event occurs (i.e., the phone receives an incoming call, or a key on the phone is pressed).

If the screen saver is enabled on a phone, the power-saving mode will still occur. For example, if a screen saver is configured to display after the phone has been idle for 5 minutes, and power-saving mode is configured to turn off the backlight and screen after the phone has been idle for 15 minutes, the backlight and screen will be turned off 10 minutes after the screen saver displays.

The following power-saving settings can be configured:

- **Office Hour:** When the work day starts and the length of each day.
- **Idle TimeOut (minutes):** The period of time the phone should be idle before the screen turns off.

  Different timeouts can be specified for office hours (Office Hour Idle Timeout) and non- office hours (Off Hour Idle Timeout). By default, the Office Hours Idle Timeout is much longer than the Off Hours Idle Timeout.

  A separate timeout period that applies after a key is pressed or the screen is tapped can be specified as well. This is called the User Input Extension Idle TimeOut. A User Input Extension Idle TimeOut that is higher than the Office Hours and Off Hours Idle Timeouts can be set so that when the phone is actively used, the phone, power-saving mode won't initiate as often.

NOTE: To determine which idle timeout applies: When a key is pressed or the screen is tapped, the idle timeout period that applies (User Input Extension Idle TimeOut or Office Hours/Off Hours Idle Timeout) will be the timeout with the highest value.

Power saving can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the power-saving feature. **Parameter:** features.power_saving.enable
		Configure the office hour. **Parameters:** features.power_saving.office_hour.monday features.power_saving.office_hour.tuesday features.power_saving.office_hour.wednesday features.power_saving.office_hour.thursday features.power_saving.office_hour.friday features.power_saving.office_hour.saturday features.power_saving.office_hour.sunday
		Configures idle time before the phone enters power-saving mode. **Parameters:** features.power_saving.office_hour.idle_timeout features.power_saving.off_hour.idle_timeout features.power_saving.user_input_ext.idle_timeout
Local	Web User Interface	Configure the power-saving feature. Configure the office hour. Configures idle time before the phone enters power-saving mode. **Navigate to:** http://<phoneIPAddress/servlet?p=settings-powersaving&q=load

Details of the Configuration Parameters

Parameter	Permitted Values	Default
features.power_saving.enable	0 or 1	1
Description: Enables or disables the power-saving feature. **0**- Disabled **1**- Enabled **Web User Interface:** Settings > Power Saving > Power Saving **Phone User Interface:** None		

Parameter	Permitted Values	Default
features.power_saving.office_hour.idle_timeout	Integer from 1 to 960	960
Description: Configures the time (in minutes) to wait in the idle state before the phone enters power-saving mode during the office hours. **Example**: features.power_saving.office_hour.idle_timeout = 600 The phone will enter power-saving mode when it has been inactive for 600 minutes (10 hours) during the office hours. **Web User Interface:** Settings > Power Saving > Office Hour Idle TimeOut **Phone User Interface:** None		
features.power_saving.off_hour.idle_timeout	Integer from 1 to 10	10
Description: Configures the time (in minutes) to wait in the idle state before the phone enters power- saving mode during the non-office hours. **Example**: features.power_saving.off_hour.idle_timeout = 10 The phone will enter power-saving mode when it has been inactivated for 10 minutes during the non-working hours. **Web User Interface:** Settings > Power Saving > Off Hour Idle TimeOut **Phone User Interface:** None		
features.power_saving.user_input_ext.idle_timeout	Integer from 1 to 30	10
Description: Configures the minimum time (in minutes) to wait in the idle state - after using the phone - before the phone enters power-saving mode. **Example**: features.power_saving.user_input_ext.idle_timeout = 10 **Web User Interface:** Settings > Power Saving > User input extension Idle TimeOut **Phone User Interface:** None		

Parameter	Permitted Values	Default
features.power_saving.office_hour.Monday	Integer from 0 to 23, Integer from 0 to 23	7,19
features.power_saving.office_hour.Tuesday		7,19
features.power_saving.office_hour.Wednesday		7,19
features.power_saving.office_hour.Thursday		7,19
features.power_saving.office_hour.Friday		7,19
features.power_saving.office_hour.Saturday		7,7
features.power_saving.office_hour.Sunday		7,7

Description:

Configures the starting time and ending time of the day's office hour. Starting time and ending time are separated by a comma.

Example:
features.power_saving.office_hour.monday = 7,19

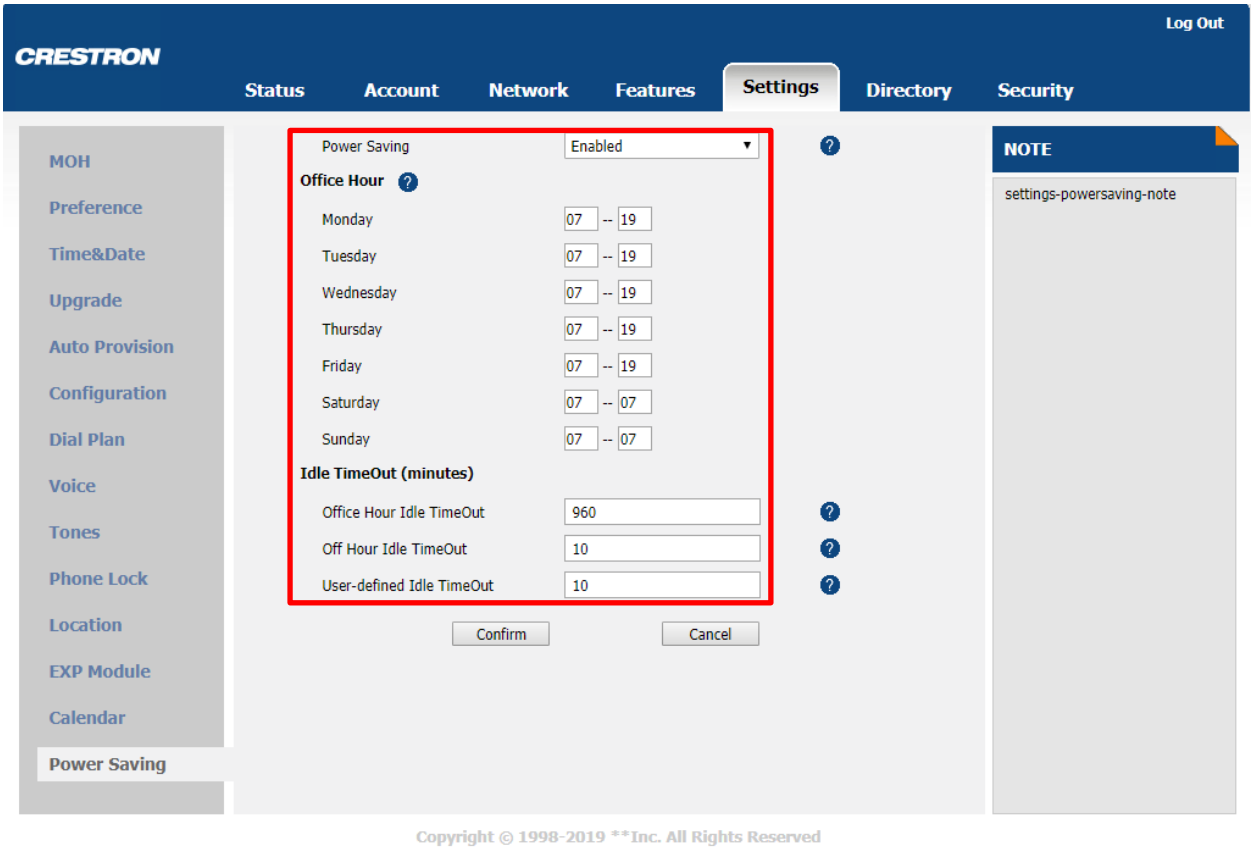
Web User Interface:
Settings > Power Saving > Monday/Tuesday/Wednesday/Thursday/Friday/Saturday/Sunday

Phone User Interface:
None

Configure the Power-Saving Feature via the Web User Interface

1. Click **Settings** > **Power Saving**.

Settings > Power Saving



2. Enter the start time and end time respectively for each day of the week in the **Office Hour** fields.
3. Enter the Office Hours Idle TimeOut value (1-960) in the **Office Hour Idle TimeOut** field.
4. Enter the Off Hours Idle TimeOut value (1-10) in the **Off Hour Idle TimeOut** field.
5. Enter the User-defined Idle TimeOut value (1-30) in the **User-defined Idle TimeOut** field.
6. Click **Confirm** to accept the change.

Backlight

The backlight brightness of the LCD screen during phone activity and inactivity can be changed. The backlight brightness automatically changes when the phone is idle for a specified time.

Backlight Active Level is used to adjust the backlight intensity of the LCD screen when the phone is active.

Backlight can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the backlight of the LCD screen. **Parameters:** phone_setting.active_backlight_level phone_setting.inactive_backlight_level
Local	Web User Interface	Configure the backlight of the LCD screen. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-preference&q=load
	Phone User Interface	Configure the backlight of the LCD screen.

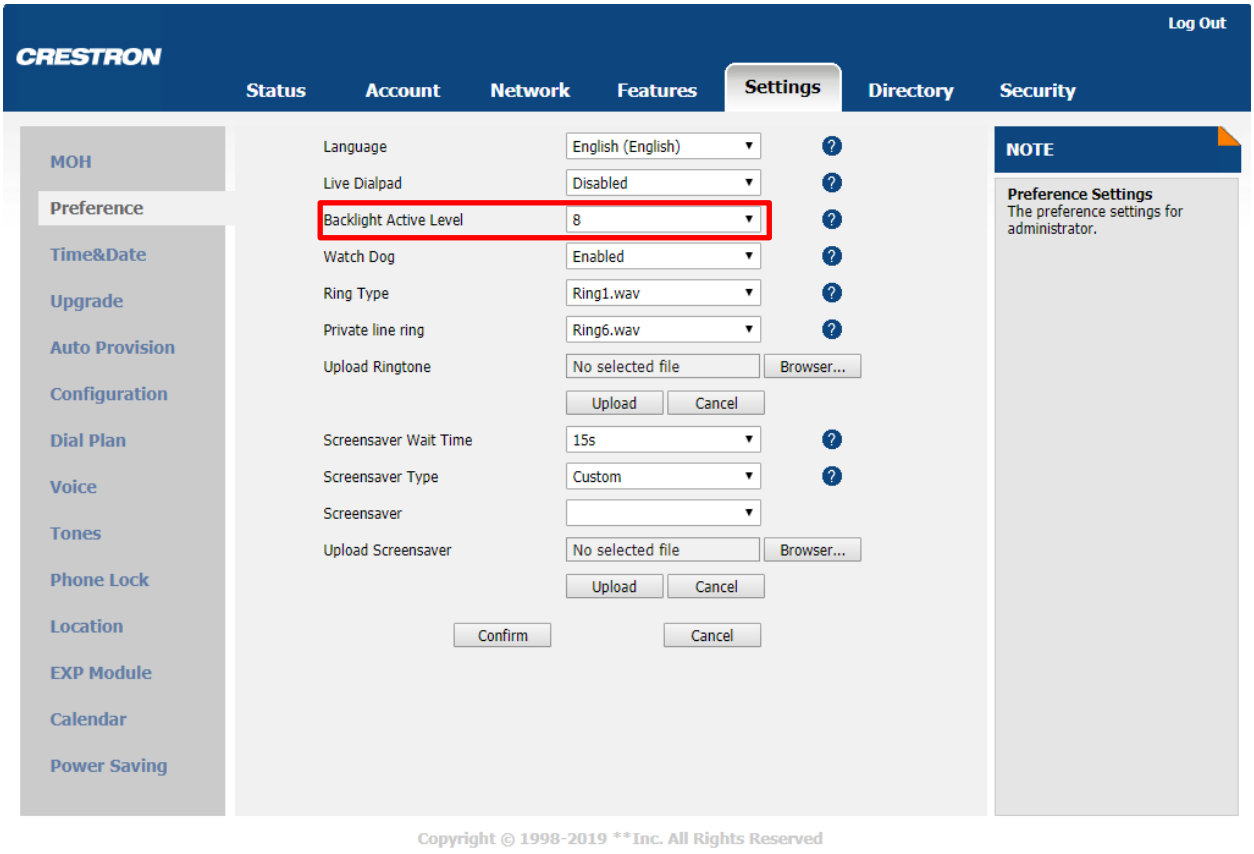
Details of the Configuration Parameter

Parameter	Permitted Values	Default
phone_setting.active_backlight_level	**Integer from 1 to 10**	**10**
Description: Configures the intensity of the LCD screen when the phone isactive. 10 is the highest intensity. **Web User Interface:** Settings > Preference > Backlight Active Level **Phone User Interface:** Menu > Setting > Basic > Display > Backlight > Backlight Active Level		

Configure the Backlight via the Web User Interface:

1. Click **Settings > Preference**.

Settings > Preference



2. Select the Backlight Active Level value from **Backlight Active Level** the drop-down list
3. Click **Confirm** to accept the change.

Configure the Backlight via the Phone User Interface:

1. Tap **Setting** > **Basic** > **Display** > **1. Backlight**.
2. Touch and drag the **1. Backlight Active Level** slider control to adjust the backlight level.
3. Select the amount of time the backlight will stay on from the **2. Backlight Time** drop-down list.

Bluetooth

Bluetooth enables low-bandwidth wireless connections within a range of 32 feet (10 meters). The best performance is in the 3 to 6 feet (1 to 2 meters) range. A user can activate/deactivate the Bluetooth mode and then pair and connect the Bluetooth headset with a phone.

The Bluetooth device name can be personalized. The pre-configured Bluetooth device name will display in the scanning list of other devices. It is helpful for the other Bluetooth devices to identify and pair with a phone.

Bluetooth mode can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure Bluetooth mode. **Parameter:** features.bluetooth_enable
		Configure the Bluetooth device name. **Parameter:** features.bluetooth_adapter_name
Local	Web User Interface	Configure Bluetooth mode. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-bluetooth&q=load
	Phone User Interface	Configure Bluetooth mode. Configure the Bluetooth device name.

Details of the Configuration Parameters

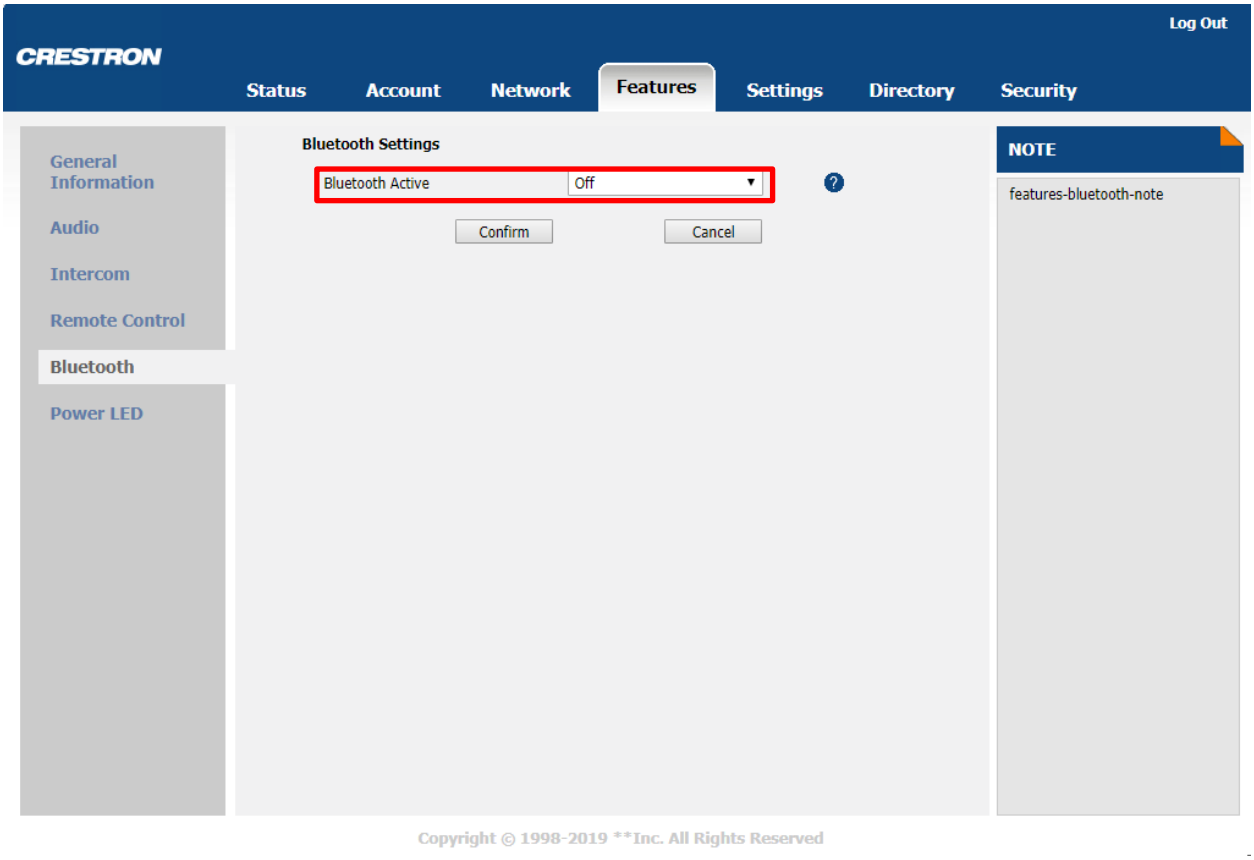
Parameter	Permitted Values	Default
features.bluetooth_enable	0 or 1	0
Description: Triggers Bluetooh mode to on or off. **0**- Off **1**- On **Web User Interface:** Features > Bluetooth > Bluetooth Active **Phone User Interface:** Menu > Setting > Basic > Bluetooth > Bluetooth		

Parameter	Permitted Values	Default
features.bluetooth_adapter_name	String within 64 characters	Refer to the following content
Description: Configures the Bluetooth device name. **Note**: This feature works only if the value of the parameter "features.bluetooth_enable" is set to 1 (On). **Web User Interface:** None **Phone User Interface:** Menu > Setting > Basic > Bluetooth > Bluetooth (On) > Edit My Device Information > Device Name		

Activate the Bluetooth Mode via the Web User Interface:

1. Click **Features** > **Bluetooth**.

Features > Bluetooth



2. Select **On** or **Off** from the **Bluetooth Active** drop-down list.
3. Click **Confirm** to accept the change.

Activate the Bluetooth Mode via the Phone User Interface

1. Tap **Setting** > **Basic** > **Bluetooth**.
2. Tap **On** in the **Bluetooth** field to turn on Bluetooth.

Edit the Device Information via the Phone User Interface

1. Tap **Setting** > **Basic** > **Bluetooth**.
2. Tap **Edit My Device Information**.
3. Tap inside the **Device Name** field to edit the name.
4. Select whether the **Open Discover** feature is **On** or **Off**.
5. Tap **Save**.

Time and Date

Phones maintain a local clock and calendar. Time and date are displayed on the idle screen of phones.

The following table lists available configuration methods for time and date.

Time and Date Configuration Methods

Option	Configuration Methods
NTP time server	Configuration Files Web User Interface Phone User Interface
Time Zone	Configuration Files Web User Interface Phone User Interface
Time	Web User Interface Phone User Interface
Time Format	Configuration Files Web User Interface Phone User Interface
Date	Web User Interface Phone User Interface

Option	Configuration Methods
Date Format	Configuration Files Web User Interface Phone User Interface
Daylight Saving Time	Configuration Files Web User Interface

NTP Time Server

A time server is a computer server that reads the actual time from a reference clock and distributes this information to clients in a network. The Network Time Protocol (NTP) is the most widely used protocol that distributes and synchronizes time in the network.

The phones synchronize the time and date automatically from the NTP time server by default. The NTP time server address can be provided by the DHCP server or it can be configured manually. The NTP by DHCP Priority feature configures the priority for the phone to use the NTP time server address provided by the DHCP server or an address that is configured manually.

Time Zone

A time zone is a region that has a uniform standard time. When configuring the phone to obtain the time and date from the NTP time server, the time zone must be set.

NTP time server and time zone can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the NTP server. **Parameter:** phone_setting.hide_ntp_server.enable
	<MAC>.cfg	Configure NTP by DHCP priority feature and DHCP time feature. **Parameters:** local_time.manual_ntp_srv_prior local_time.dhcp_time
		Configure the NTP server, time zone. **Parameters:** local_time.ntp_server1 local_time.ntp_server2 local_time.interval local_time.time_zone local_time.time_zone_name
Local	Web User Interface	Configure NTP by DHCP priority feature and DHCP time feature. Configure the NTP server, time zone. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-datetime&q=load
	Phone User Interface	Configure DHCP time feature. Configure the NTP server and time zone.

Details of the Configuration Parameters

Parameter	Permitted Values	Default
local_time.manual_ntp_srv_prior	0 or 1	0
Description: Configures the priority for the phone to use the NTP server address offered by the DHCP server. **0**- High, use the NTP server address offered by the DHCP server **1**- Low, use the NTP server address configured manually **Web User Interface:** Settings > Time & Date > NTP by DHCP Priority **Phone User Interface:** None		
local_time.dhcp_time	0 or 1	0
Description: Enables or disables the phone to update time with the offset time offered by the DHCP server. **0**- Disabled **1**- Enabled **Note:** This feature is only available to offset from GMT 0. **Web User Interface:** Settings > Time & Date > DHCP Time **Phone User Interface:** Menu > Setting > Basic > Date & Time > DHCP Time		
phone_setting.hide_ntp_server.enable	0 or 1	0
Description: It enables or disables the phone to hide NTP Server configurations on the LCD screen. **0**- Disabled **1**- Enabled, the NTP Server configurations on the LCD screen will be hidden, so that the NTP Server address cannot be configured manually. **Web User Interface:** None **Phone User Interface:** None		
local_time.ntp_server1	IP Address or Domain Name	cn.pool.ntp.org
Description: Configures the IP address or the domain name of the NTP server 1. **Example:** local_time.ntp_server1 = 192.168.0.5 **Web User Interface:** Settings > Time & Date > Primary Server **Phone User Interface:** Menu > Setting > Basic > Date & Time > General > SNTP Settings > NTP Server1		

Parameter	Permitted Values	Default
local_time.ntp_server2	IP Address or Domain Name	cn.pool.ntp.org
Description: Configures the IP address or the domain name of the NTP server 2. If the NTP server 1 is not configured or cannot be accessed, the phone will request the time and date from the NTP server 2. **Example:** local_time.ntp_server2 = 192.168.0.6 **Web User Interface:** Settings > Time & Date > Secondary Server **Phone User Interface:** Menu > Setting > Basic > Date & Time > General > SNTP Settings > NTP Server2		
local_time.interval	Integer from 15 to 86400	1000
Description: Configures the interval (in seconds) to update time and date from the NTP server. **Example:** local_time.interval = 1000 **Web User Interface:** Settings > Time & Date > Synchronism (15~86400s) **Phone User Interface:** None		
local_time.time_zone	-11 to +14	+8
Description: Configures the time zone. **Example:** local_time.time_zone = +8 For more available time zones, refer to “Appendix B: Time Zones” on page 383. **Web User Interface:** Settings > Time & Date > Time Zone **Phone User Interface:** Menu > Setting > Basic > Date & Time > General > SNTP Settings > Time Zone		

Parameter	Permitted Values	Default
local_time.time_zone_name	String within 32 characters	China (Beijing)

Description:

Configures the time zone name.

The available time zone names depend on the time zone configured by the parameter "local_time.time_zone". For more information on the available time zone names for each time zone, refer to "Appendix B: Time Zones" on page 383.

Example:
local_time.time_zone_name = United States-Eastern Time

Note: This feature works only if the value of the parameter "local_time.summer_time" is set to 2 (Automatic) and the parameter "local_time.time_zone" is configured in advance.

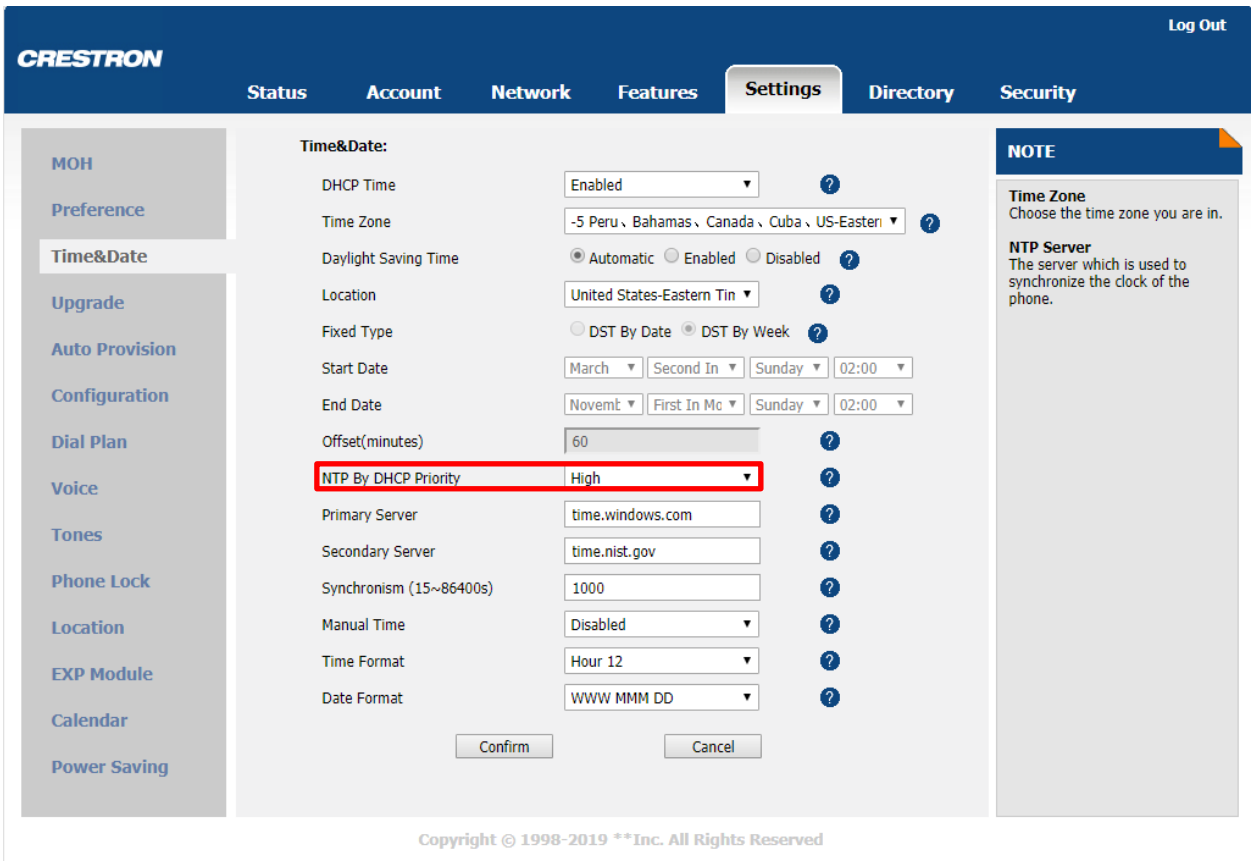
Web User Interface:
Settings > Time & Date > Location

Phone User Interface:
Menu > Setting > Basic > Date & Time > General > SNTP Settings > Location

Configure NTP by DHCP Priority Feature via the Web User Interface

1. Click **Settings** > **Time&Date**.

Settings > Time&Date

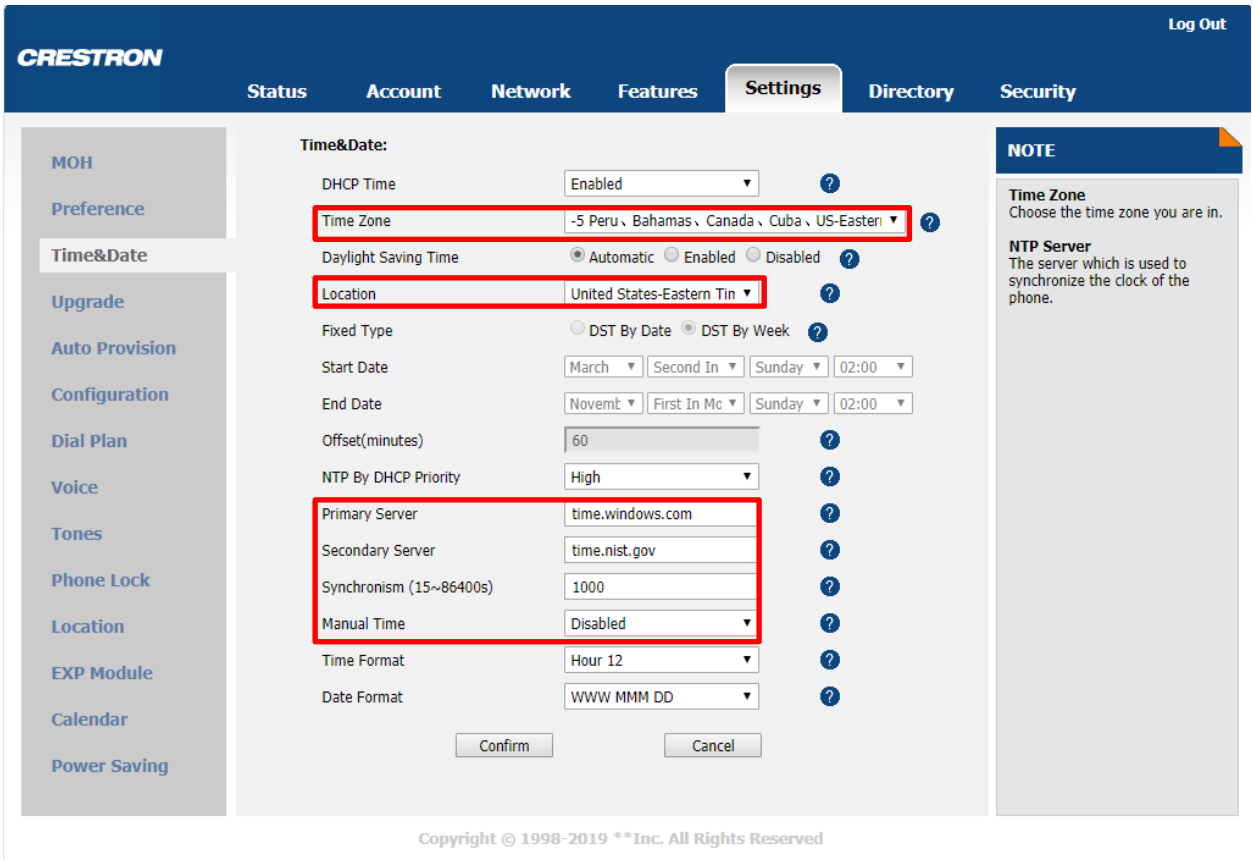


2. Select the desired value from the **NTP by DHCP Priority** drop-down list.
3. Click **Confirm** to accept the change.

Configure the NTP Server and Time Zone via the Web User Interface

1. Click **Settings** > **Time & Date**.

Settings > Time&Date



2. Select **Disabled** from the **Manual Time** drop-down list.
3. Select the time zone from the **Time Zone** drop-down list.
4. Select the location from the **Location** drop-down list.
5. Enter the domain name or IP address in the **Primary Server** and **Secondary Server** field respectively.
6. Enter the time interval in the **Synchronism (15~86400s)** field.
7. Click **Confirm** to accept the change.

Configure SNTP Settings via the Phone User Interface

1. Tap **Setting** > **Basic** > **Time & Date** > **General**.
2. Select **SNTP** from the **Type** drop-down list.

3. Select the time zone setting from the **Time Zone** drop-down list.
4. Enter the domain name or IP address of SNTP server in the **NTP Server1** and NTP **Server2** fields respectively.
5. Select the daylight savings time mode from **Daylight Saving Time** options.
6. Select a location from the **Location** drop down list.
7. Tap **Save**.

Time and Date Settings

The time and date can be set manually when phones cannot obtain the time and date from the NTP time server. The time and date display can use one of several different formats.

Time and date can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<MAC>.cfg**	Configure the time and date manually. **Parameter:** local_**time**.manual_time_enable Configure the time and date formats. **Parameters:** **local_time.time_format** **local**_time.date_format
Local	Web User Interface	Configure the time and date manually. Configure the time and date formats. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-datetime&q=load
	Phone User Interface	Configure the time and date manually. Configure the time and date formats.

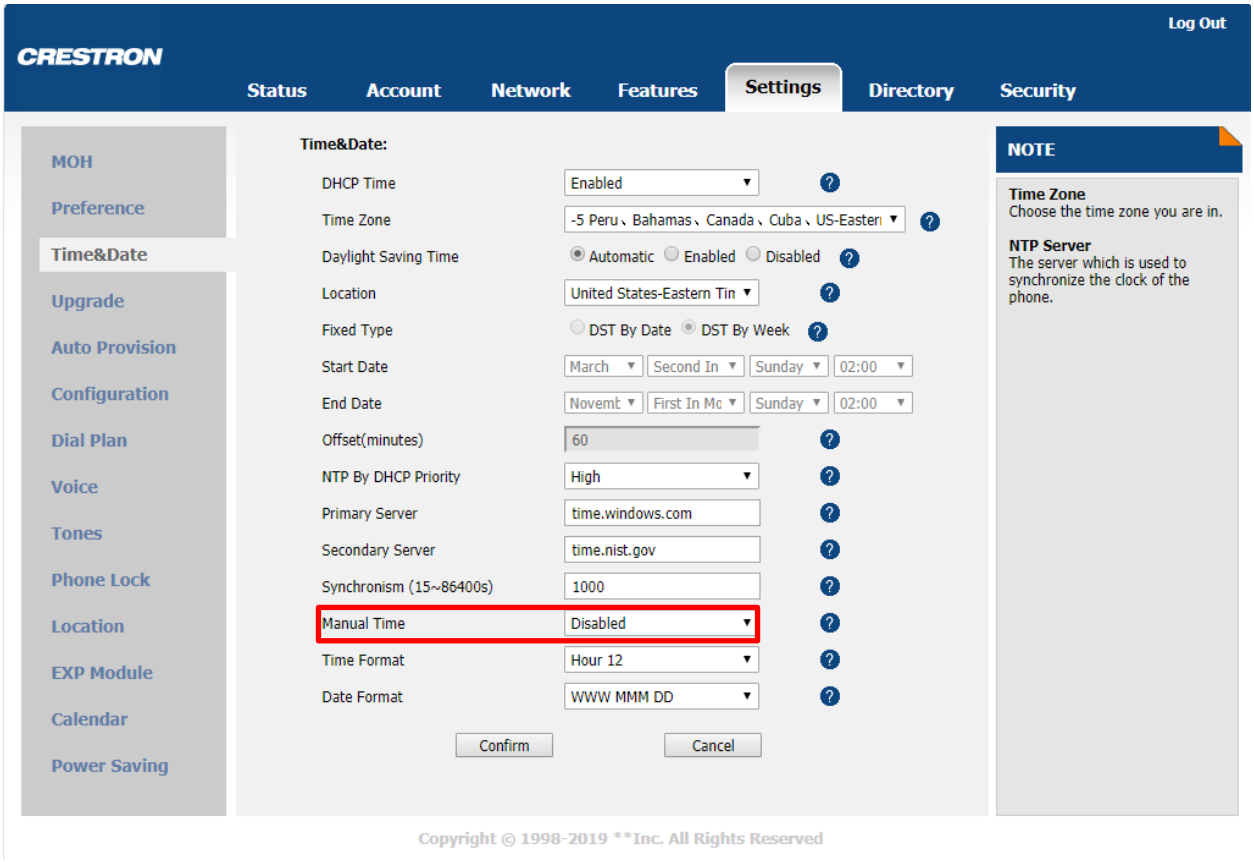
Details of the Configuration Parameters

Parameter	Permitted Values	Default
local_time.manual_time_enable	0 or 1	0
Description: Enables or disables the phone to obtain the time and date from manual settings. **0**- Diabled, obtain the time and date from NTP server **1**- Enabled, obtain the time and date from manual settings **Web User Interface:** Settings > Time & Date > Manual Time **Phone User Interface:** None		
local_time.time_format	0 or 1	1
Description: Configures the time format. **0**- Hour 12, the time will be displayed in 12-hour format with AM or PM specified. **1**- Hour 24, the time will be displayed in 24-hour format (for example, 2:00 PM displays as 14:00). **Web User Interface:** Settings > Time & Date > Time Format **Phone User Interface:** Menu > Setting > Basic > Date & Time > Time & Date Format > Time Format		
local_time.date_format	0, 1, 2, 3, 4, 5 or 6	0
Description: Configures the date format. Valid **values are:** **0**- WWW MMM DD **1**- DD-MMM-YY **2**- YYYY-MM-DD **3**- DD/MM/YYYY **4**- MM/DD/YY **5**- DD MMM YYYY **6**- WWW DD MMM **Note:** "WWW" represents the abbreviation of the week, "DD" represents a two-digit day, "MMM" represents the first three letters of the month, "YYYY" represents a four-digit year, and "YY" represents a two-digit year. **Web User Interface:** Settings > Time & Date > Date Format **Phone User Interface:** Menu > Setting > Basic > Date & Time > Time & Date Format > Date Format		

Configure the Time and Date Manually via the Web User Interface

1. Click **Settings** > **Time & Date**.

Settings > Time&Date

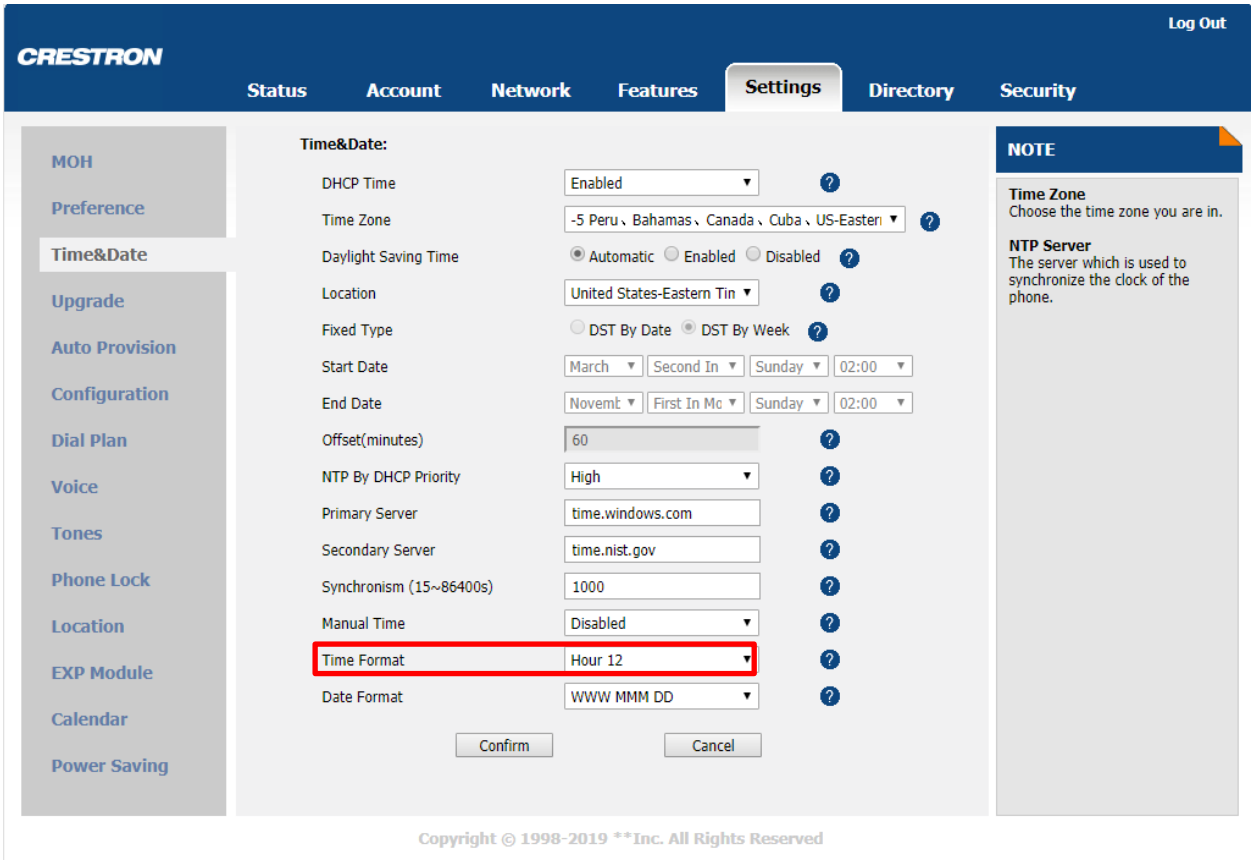


2. Select **Enabled** from the **Manual Time** drop-down list.
3. Enter the time and date in the corresponding fields.
4. Click **Confirm** to accept the change.

Configure the Time and Date Format via the Web User Interface

1. Click **Settings** > **Time & Date**.

Settings > Time&Date



2. Select the time format from the **Time Format** drop-down list.
3. Select the date format from the **Date Format** drop-down list.
4. Click **Confirm** to accept the change.

Configure the Date and Time Manually via the Phone User Interface

1. Tap **Setting** > **Basic** > **Time & Date** > **General**.
2. Select **Manual Setting** from the **Type** drop-down list.
3. Enter the date and time in the respective fields.
4. Tap **Save**.

Configure the Date and Time Format via the Phone User Interface

1. Tap **Setting** > **Basic** > **Time & Date** > **Format**.
2. Select the date format from the **Date Format** drop-down list.
3. Select the time format from the **Time Format** drop-down list.

4. Tap **Save**.

Daylight Saving Time

The default setting for DST is Automatic, so it can be set automatically from the current time zone configuration. DST for the desired area can be configured as required.

Daylight saving time can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<MAC>.cfg**	Configure DST. **Parameters:** local_time.summer_time local_time.dst_time_type local_time.start_time local_time.end_time local_time.offset_time
Local	Web User Interface	Configure DST. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-datetime&q=load

Details of the Configuration Parameters

Parameter	Permitted Values	Default
local_time.summer_time	**0, 1 or 2**	**2**
Description: Configures Daylight Saving Time (DST) feature. **0**- Disabled **1**- Enabled **2**- Automatic **Web User Interface:** Settings > Time & Date > Daylight Saving Time **Phone User Interface:** Menu > Setting > Basic > Date & Time > General > SNTP Settings > Daylight Saving		

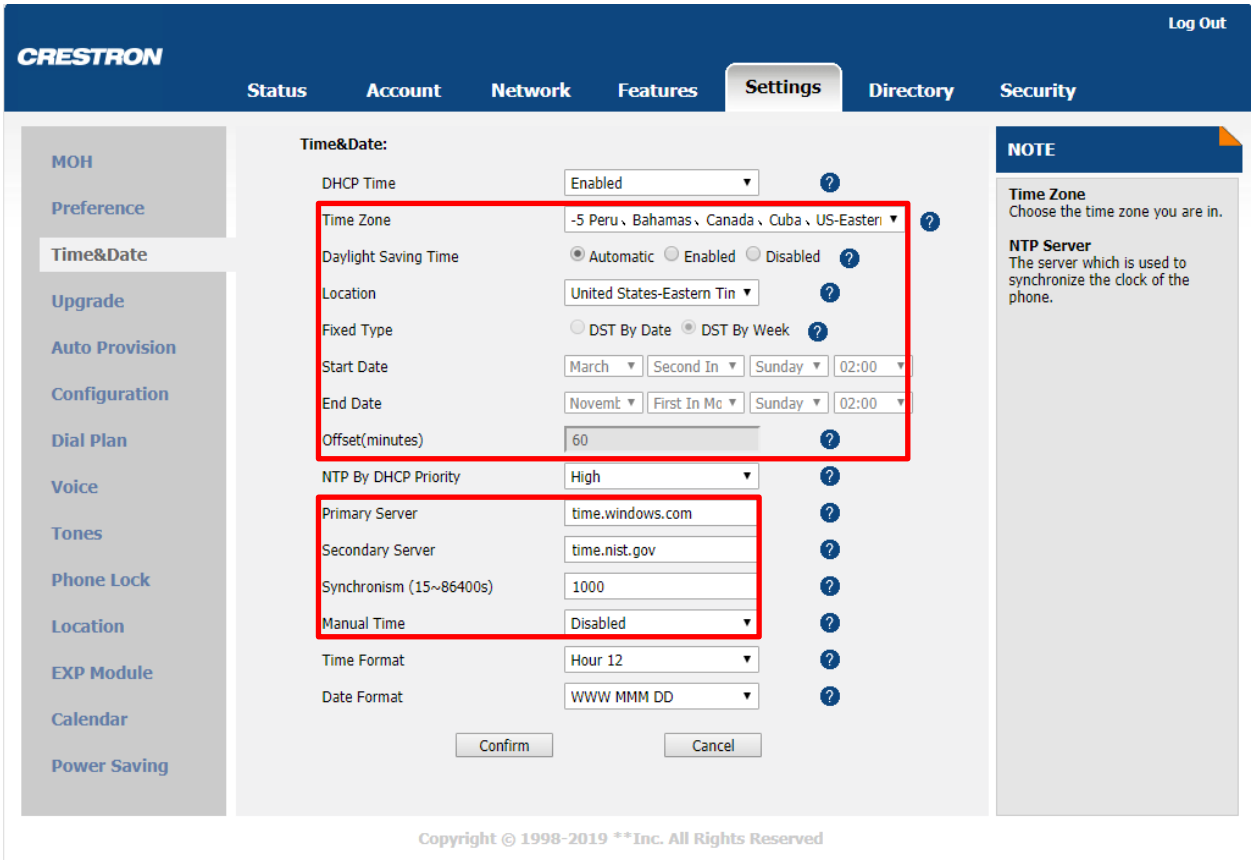
Parameter	Permitted Values	Default
local_time.dst_time_type	**0 or 1**	**0**
Description: Configures the DST time type. **0**- DST By Date **1**- DST By Week **Note:** This feature works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled). **Web User Interface:** Settings > Time & Date > Fixed Type **Phone User Interface:** None		
local_time.start_time	**Time**	**1/1/0**
Description: Configures the start time of the DST. **Value formats are:** • Month/Day/Hour (for DST By Date) • Month/Day of Week's Occurrence Within the Month/Day of Week/Hour of Day (for DST By Week) If "local_time.dst_time_type" is set to 0 (DST By Date), use the mapping: **Month:** 1=January, 2=February,..., 12=December **Day:** 1=the first day in a month,..., 31= the last day in a month **Hour:** 0=0am, 1=1am,..., 23=11pm If "local_time.dst_time_type" is set to 1 (DST By Week), use the mapping: **Month:** 1=January, 2=February,..., 12=December **Day of Week Last in Month:** 1=the first week in a month,..., 5=the last week in a month **Day of Week:** 1=Monday, 2=Tuesday,..., 7=Sunday **Hour of Day:** 0=0am, 1=1am,..., 23=11pm **Note:** This feature works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled). **Web User Interface:** Settings > Time & Date > Start Date **Phone User Interface:** None		

Parameter	Permitted Values	Default
local_time.end_time	Time	12/31/23
Description: Configures the end time of the DST. **Value formats are:** • Month/Day/Hour (for DST By Date) • Month/Day of Week's Occurrence Within the Month/Day of Week/Hour of Day (for DST By Week) If "local_time.dst_time_type" is set to 0 (DST By Date), use the mapping: **Month:** 1=January, 2=February,..., 12=December **Day:** 1=the first day in a month,..., 31= the last day in a month **Hour:** 0=0am, 1=1am,..., 23=11pm If "local_time.dst_time_type" is set to 1 (DST By Week), use the mapping: **Month:** 1=January, 2=February,..., 12=December **Day of Week Last in Month:** 1=the first week in a month,..., 5=the last week in a month **Day of Week:** 1=Monday, 2=Tuesday,..., 7=Sunday **Hour of Day:** 0=0am, 1=1am,..., 23=11pm **Note:** This feature works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled). **Web User Interface:** Settings > Time & Date > End Date **Phone User Interface:** None		
local_time.offset_time	Integer from -300 to 300	Blank
Description: Configures the offset time (in minutes) of DST. **Note:** This feature works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled). **Web User Interface:** Settings > Time & Date > Offset(minutes) **Phone User Interface:** None		

Configure the DST via the Web User Interface

1. Click **Settings** > **Time & Date**.

Settings > Time&Date



2. Select **Disabled** from the **Manual Time** drop-down list.
3. Select the time zone from the **Time Zone** drop-down list.
4. Enter the domain name or IP address in the **Primary Server** and **Secondary Server** field respectively.
5. Enter the time interval (in seconds) in the **Synchronism (15~86400s)** field.
6. Select **Enabled** in the **Daylight Saving Time** field.
   - Select DST by Date
     i. Select **DST by Date** in the **Fixed Type** field.
     ii. Enter the start date in the **Start Date** field.
     iii. Enter the end date in the **End Date** field.
   - Select DST by Week
     i. Select **DST by Week** in the **Fixed Type** field.
     ii. Enter the start week in the **Start Week** field.

iii. Enter the end week in the **End Week** field.

7. Enter the offset time in the **Offset(minutes)** field.
8. Click **Confirm** to accept the change.

Customize an AutoDST Template File

The time zone and corresponding DST pre-configurations exist in the AutoDST file. If the DST is set to Automatic, the phone obtains the DST configuration from the AutoDST file. The AutoDST file can be customized if required. The AutoDST file allows the addition or modification of time zone and DST settings for an area each year.

Before customizing, the AutoDST file is required. The DST template can be downloaded from the documentation section of the UC-PHONE-S and UC-PHONE-S-PLUS web pages at www.crestron.com.

For more information on obtaining the template file, refer to "Obtain Configuration Files/Resource Files" on page 87.

The following table lists description of each element in the template file:

Template File Elements

Element	Type	Values	Description
DSTData	required	no	File root element
DST	required	no	Time Zone item's root element
szTime	required	[+/-][X]:[Y], X=0~14, Y=0~59	Time Zone
szZone	required	String (if the content is more than one city, it is the best to keep the daylight saving time the same)	Time Zone name
iType	optional	0/1 **0**: DST By Date **1**: DST By Week	DST time type (This item is needed to configure DST.)
szStart	optional	**Month/Day/Hour** (for **iType=0**) Month: 1~12 Day: 1~31 Hour: 0 (midnight)~23 **Month/Week of Month/Day of Week/Hour of Day** (for **iType=1**) Month: 1~12 Week of Month: 1~5 Day of Week: 1~7 Hour of Day: 0 (midnight)~23	Start time of the DST
szEnd	optional	Same as szStart	End time of the DST
szOffset	optional	Integer from -300 to 300	The offset time (in minutes) of DST

When customizing an AutoDST file, keep the following in mind:

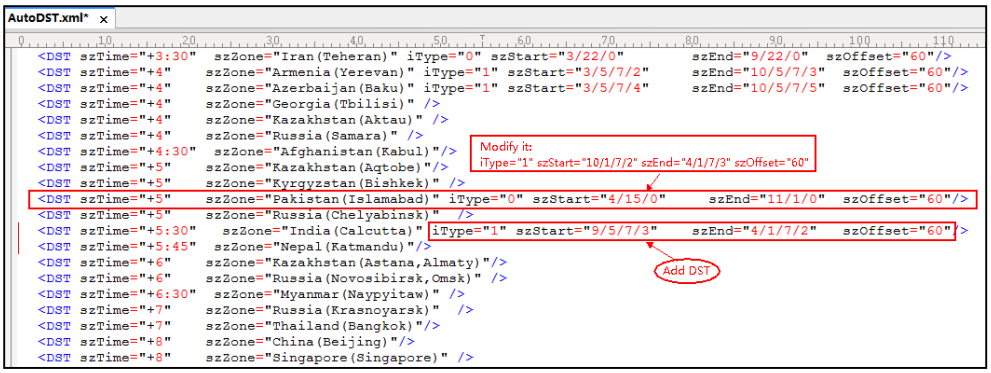
- <DSTData> indicates the start of a template and </DSTData> indicates the end of a template.
- Add or modify time zone and DST settings between <DSTData> and </DSTData>.
- The display order of time zone is corresponding to the szTime order specified in the AutoDST.xml file.
- If the start time of DST is greater than the end time, the valid time of DST is from the start time of this year to the end time of the next year.

NOTE: The typical DST definition is from March until November of the same year. However, some countries have DST from November until April of the following year. In this case, the numeric value of November (month 11) is greater than April (month 4), so the DST is calculated as November of the current year until April of the following year.

Customize an AutoDST File

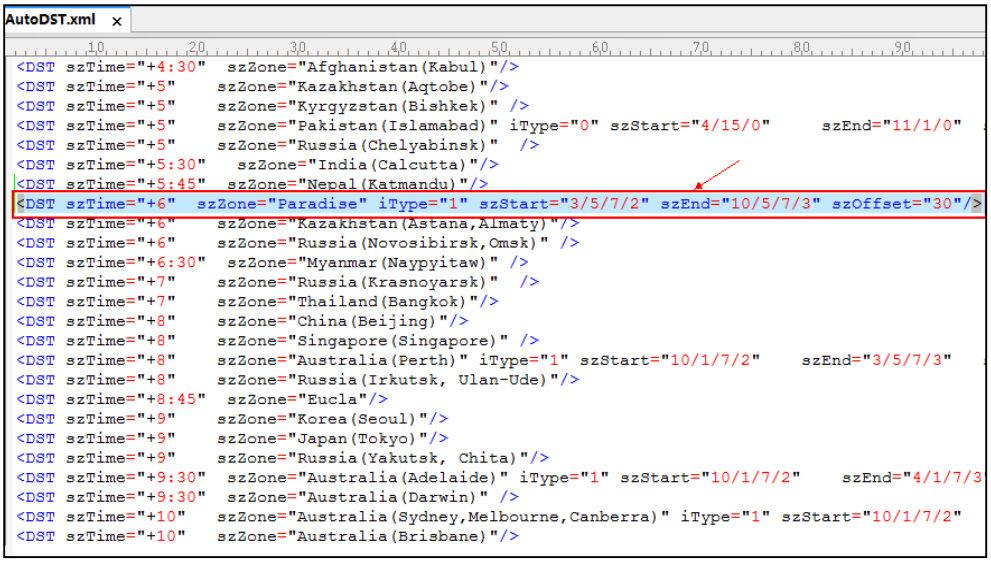
1. Open the AutoDST file using an ASCII editor.
2. Add or modify time zone and DST settings as needed in the AutoDST file.
   - **Example 1**
     To modify the DST settings for the existing time zone "+5 Pakistan(Islamabad)" and add DST settings for the existing time zone "+5:30 India(Calcutta)".

     AutoDst.xml File



– **Example 2**
Add a new time zone (+6 Paradise) with daylight saving time offset of 30 minutes.

AutoDST.xml File



3. Save this file and place it to the provisioning server (e.g., 192.168.1.100).
4. Specify the access URL of the AutoDST file in the configuration files.

The access URL of the AutoDST file can be specified using the configuration files.

Configuration Methods

Central Provisioning (Configuration File)	**<MAC>.cfg**	Specify the access URL of the AutoDST file. **Parameter:** auto_dst.url

Details of the Configuration Parameter

Parameter	Permitted Values	Default
auto_dst.url	URL within 511 characters	Blank

Description:

Configures the access URL of the AutoDST file (AutoDST.xml).

Example:
auto_dst.url = tftp://192.168.1.100/AutoDST.xml

During the auto provisioning process, the phone connects to the provisioning server "192.168.1.100", and downloads the AutoDST file "AutoDST.xml". After update, a new time zone "Paradise" and updated DST of "Pakistan (Islamabad)" and "India (Calcutta)" will be present via web user interface: Settings > Time & Date > Time Zone.

Note: This feature works only if the value of the parameter "local_time.summer_time" is set to 2 (Automatic).

Web User Interface:
None

Phone User Interface:
None

Language

Skype for Business phones support multiple languages. Languages used on the phone user interface and web user interface can be specified respectively as required.

The following languages are supported by the phone user interface and the web user interface:

- English
- Chinese Simplified
- Chinese Traditional
- French
- German
- Italian
- Polish
- Portuguese
- Spanish
- Turkish

Specify the Language to Use

The default language used on the phone user interface is English. If the language of a web browser is not supported by the phone, the web user interface will use English by default. Languages for the phone user interface and web user interface can be specified.

Specify the language for the phone user interface or the web user interface using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Specify the languages for the phone user interface and the web user interface. **Parameters:** static.lang.gui static.lang.wui
Local	Web User Interface	Specify the language for the web user interface. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-preference&q=load
	Phone User Interface	Specify the language for the phone user interface.

Details of the Configuration Parameters

Parameter	Permitted Values	Default
static.lang.gui	**Refer to the following content**	**English**

Description:

Configures the language used on the phone user interface.

Permitted Values:
English, Chinese Simplified, Chinese Traditional, French, German, Italian, Polish, Portuguese, Spanish, Turkish, or the custom language name.

Example:
static.lang.gui = English
To use the custom language (e.g., Guilan) for the phone, configure the parameter "static.lang.gui = Guilan".

Web User Interface:
None

Phone User Interface:
Menu > Setting > Basic > Language

Parameter	Permitted Values	Default
static.lang.wui	Refer to the following content	English

Description:

Configures the language used on the web user interface.

Permitted Values:
English, Chinese Simplified, Chinese Traditional, French, German, Italian, Polish, Portuguese, Spanish, Turkish, or the custom language name.

Example:
static.lang.wui = English
If the language of the browser is not supported by the phone, the web user interface will use English by default.

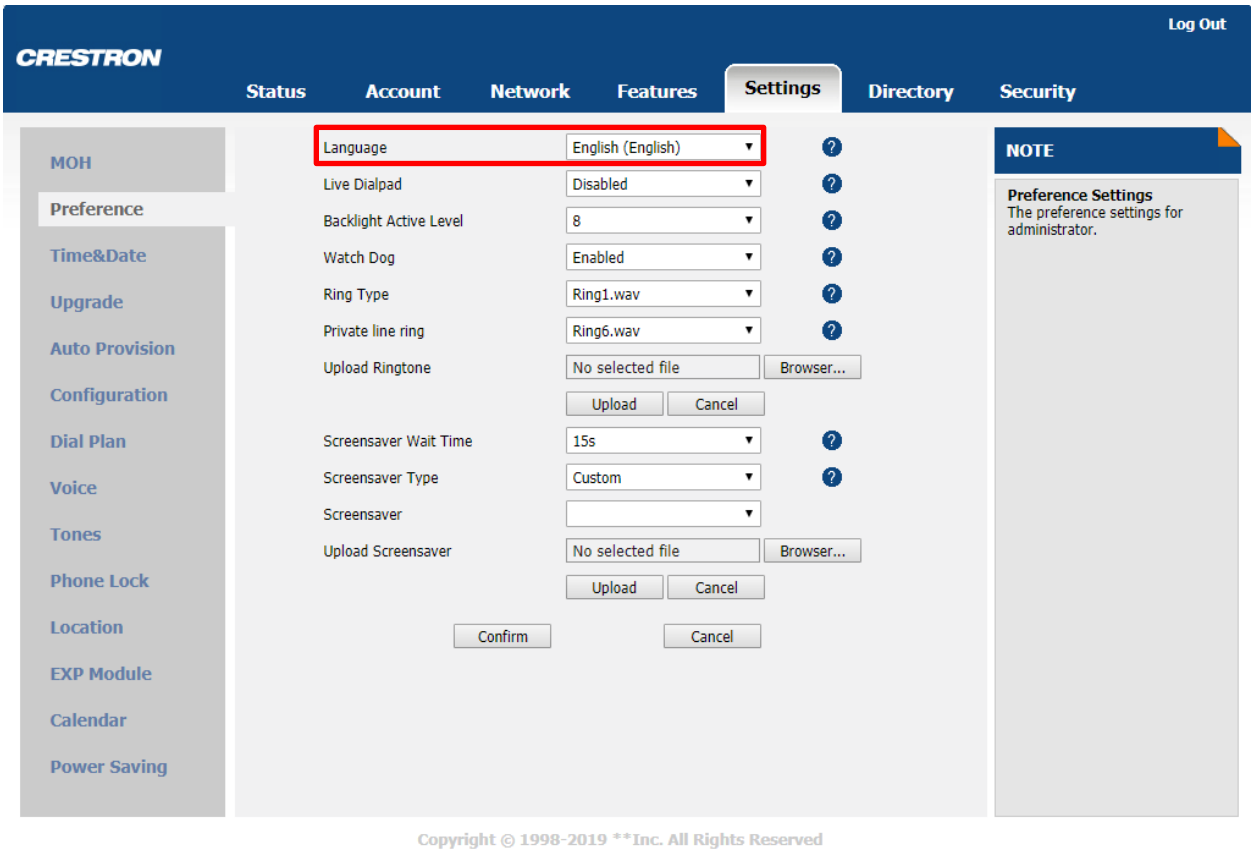
Web User Interface:
Settings > Preference > Language

Phone User Interface:
None

Specify the Language for the Web User Interface via the Web User Interface

1. Click **Settings** > **Preference**.

Settings > Preference



2. Select the language from the **Language** drop-down list.

3. Click **Confirm** to accept the change.

Specify the Language for the Phone User Interface via the Phone User Interface

1. Tap **Setting** > **Basic** > **Language**.
2. Tap the desired language on the right side of the screen.
3. Tap **Save**.

Key as Send

Key as send allows assigning the pound key ("#") or asterisk key ("*") as the send key. Send tone allows the phone to play a key tone when a user presses the send key. Key tone allows the phone to play a key tone when a user presses any key. Send tone works only if key tone is enabled.

Key as send can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure a send key. **Parameter:** features.key_as_send
		Configure send pound key. **Parameter:** features.send_pound_key
Local	Web User Interface	Configure a send key. Configure send pound key. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure a send key.

Details of the Configuration Parameters

Parameter	Permitted Values	Default
features.key_as_send	**0, 1 or 2**	**1**
Description: Configures the "#" or "*" key as the send key. **0-** Disabled, neither "#" nor "*" can be used as the send key. **1-** # key, the pound key is used as the send key. **2-** * key, the asterisk key is used as the send key. **Web User Interface:** Features > General Information > Key As Send **Phone User Interface:** Menu > Setting > Features > Key as send		

Parameter	Permitted Values	Default
features.send_pound_key	0 or 1	0

Description:

Enables or disables the phone not to send any pound key when pressing double #.

0- Disabled, the phone will dial out "#" when the user presses the # key for the second time.

1- Enabled, the phone will dial out "##" when the user presses the # key for the third time.

Note: This feature works only if the value of the parameter "features.key_as_send" is set to 1 (Enabled).

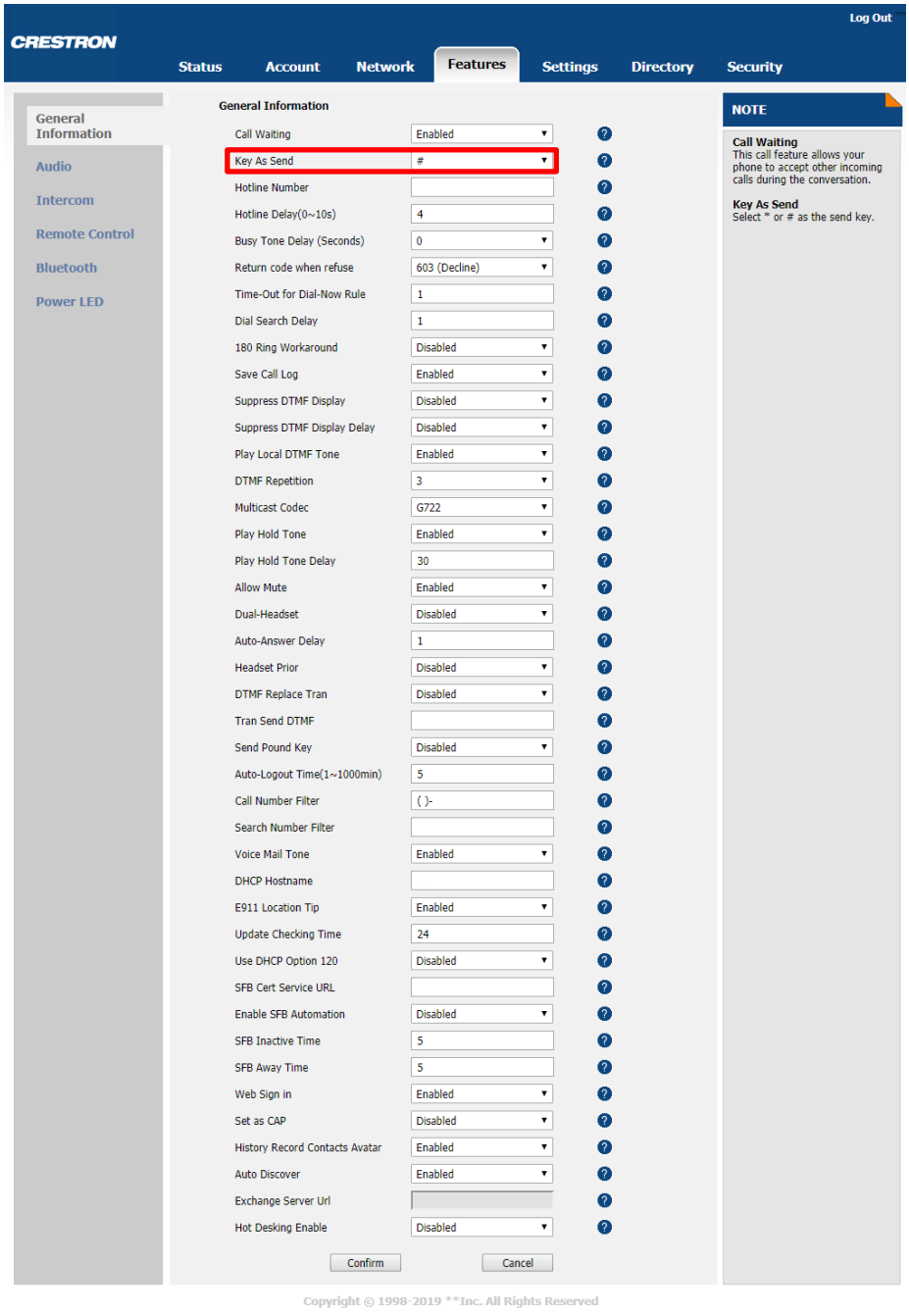
Web User Interface:
Features > General Information > Send Pound Key

Phone User Interface:
None

Configure a Send Key via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Select the key to use from the **Key As Send** drop-down list.
3. Click **Confirm** to accept the change.

Configure a Send Key via the Phone User Interface

1. Tap **Setting** > **Features** > **Key as Send**.
2. Tap inside the **Key as Send** field to select a key or to disable the feature.
3. Tap **Save**.

Send Tone

Send tone allows the phone to play a key tone when a user presses the send key. This feature works only if key tone is enabled. For more information on key tone, refer to "Key Tone" on page 160.

Send tone can be configured using the following methods.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure a send tone. **Parameter:** features.send_key_tone
Local	Web User Interface	Configure a send tone. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-audio&q=load

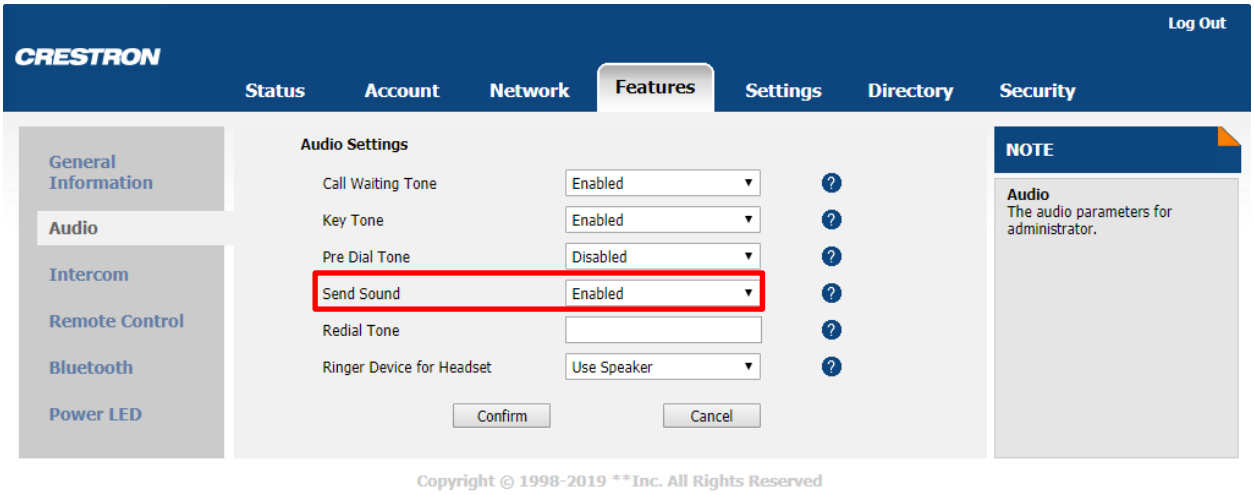
Details of the Configuration Parameter

Parameter	Permitted Values	Default
features.send_key_tone	**0 or 1**	**1**
Description: Enables or disables the phone to play a key tone when a user presses a send key. **0**- Disabled **1**- Enabled **Note**: This feature works only if the value of the parameter "features.key_tone" is set to 1 (Enabled). **Web User Interface:** Features > Audio > Send Sound **Phone User Interface:** None		

Configure a Send Tone via the Web User Interface

1. Click **Features** > **Audio**.

Features > Audio



2. Select **Enabled** or **Disabled** from the **Send Sound** drop-down list.
3. Click **Confirm** to accept the change.

Key Tone

Key tone allows the phone to play a key tone when a user presses any key from the numeric keypad.

Key tone can be configured using the following methods.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure a key tone. **Parameter:** features.key_tone
Local	Web User Interface	Configure a key tone. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-audio&q=load
	Phone User Interface	Configure a key tone.

Details of the Configuration Parameter

Parameter	Permitted Values	Default
features.key_tone	0 or 1	1

Description:

Enables or disables the phone to play a key tone when a user presses any key on the phone keypad.

0- Disabled

1- Enabled

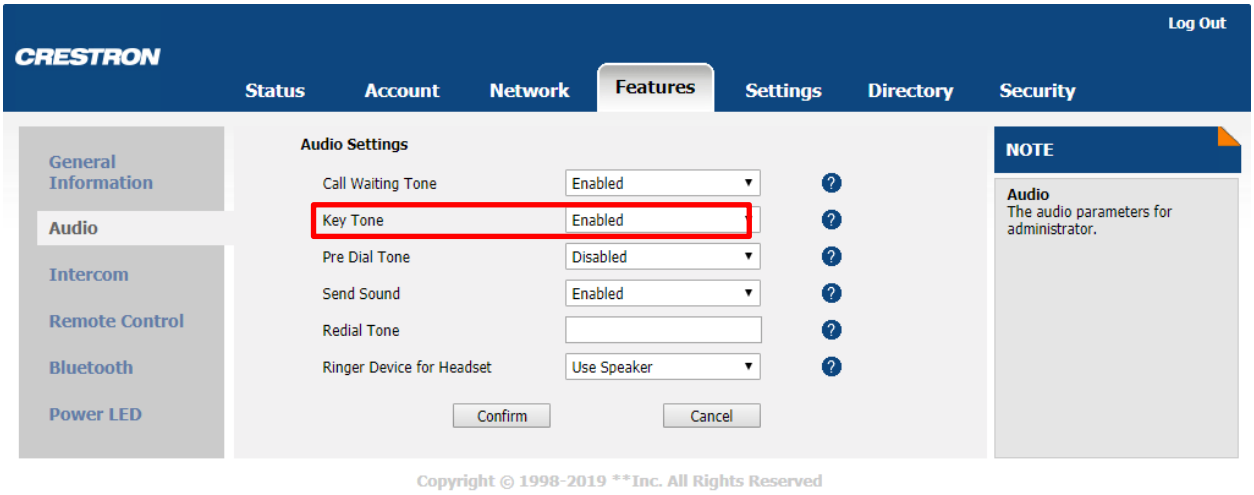
Web User Interface:
Features > Audio > Key Tone

Phone User Interface:
Menu > Setting > Basic > Sounds > Key Tone

Configure a Key Tone via the Web User Interface:

1. Click **Features** > **Audio**.

Features > Audio



2. Select **Enabled** or **Disabled** from the **Key Tone** drop-down list.
3. Click **Confirm** to accept the change.

Configure a Key Tone via the Phone User Interface:

1. Tap **Setting** > **Basic** > **Sounds** > **Key Tone**.
2. Tap **On** or **Off** to turn the feature on or off.
3. Tap **Save**.

Dial Plan

Dial plan is a string of characters that governs the way the phone processes the inputs received from the phone's keypads. The system administrator can use regular expression to define dial plan.

The dial plan is configured on the Skype for Business server by the system administrator, the phone can use the dial plan received from the Skype for Business server with the method of In- band provisioning. When the user enters digits on the dialing screen, the phone will match the digits to a dial plan.

Dial Now

Dial-now is a string used to match numbers entered by the user. When entered numbers match the predefined dial-now rule, the phone will automatically dial out the numbers without pressing the send key. Skype for Business phones support up to 100 dial-now rules, which can be created either one by one or in batch using a dial-now rule template. For more information on how to customize a dial-now template, refer to "Customize a Dial-Now Template File" on page 166.

Time Out for Dial Now Rule

The phone will automatically dial out the entered number, which matches the dial now rule, after a specified period of time.

Dial-now rule can be created using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Create the dial-now rule for the phone. **Parameter:** dialplan.dialnow.rule.X
		Configure the delay time for the dial-now rule. **Parameter:** phone_setting.dialnow_delay
Local	Web User Interface	Create the dial-now rule for the phone. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-dialnow&q=load
		Configure the delay time for the dial-now rule. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

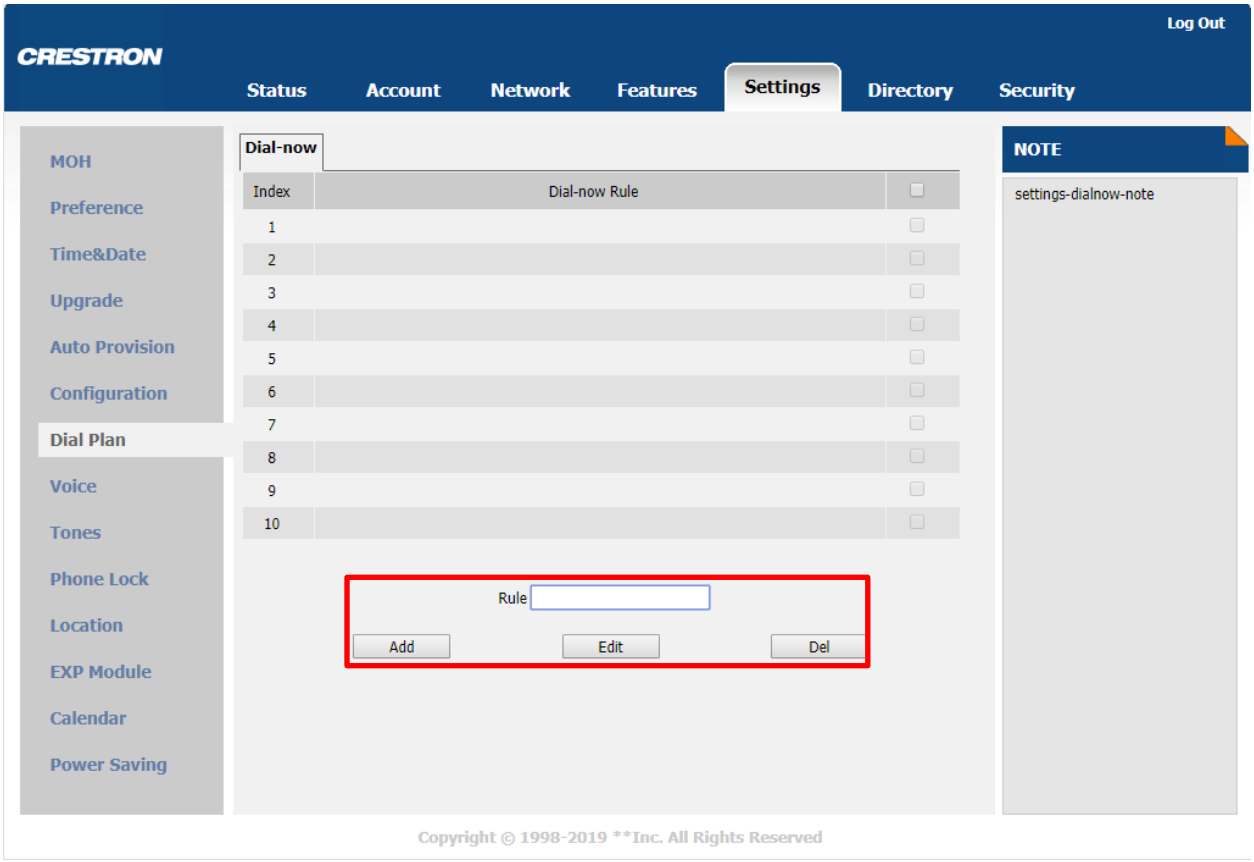
Details of the Configuration Parameters

Parameter	Permitted Values	Default
dialplan.dialnow.rule.X **(X ranges from 1 to 100)**	**String within 511 characters**	**Blank**
Description: Configures the dial-now rule (the string used to match the numbers entered by the user). When entered numbers match the predefined dial-now rule, the phone will automatically dial out the numbers without pressing the send key. **Example:** dialplan.dialnow.rule.1 = 123 **Web User Interface:** Settings > Dial Plan > Dial-now > Rule **Phone User Interface:** None		
phone_setting.dialnow_delay	**Integer from 0 to 14**	**1**
Description: Configures the delay time (in seconds) for the dial-now rule. When entered numbers match the predefined dial-now rule, the phone will automatically dial out the entered number after the designated delay time. **Web User Interface:** Features > General Information > Time-Out for Dial-Now Rule **Phone User Interface:** None		

Create a Dial-Now Rule via the Web User Interface

1. Click **Settings** > **Dial Plan**.

Settings > Dial Plan

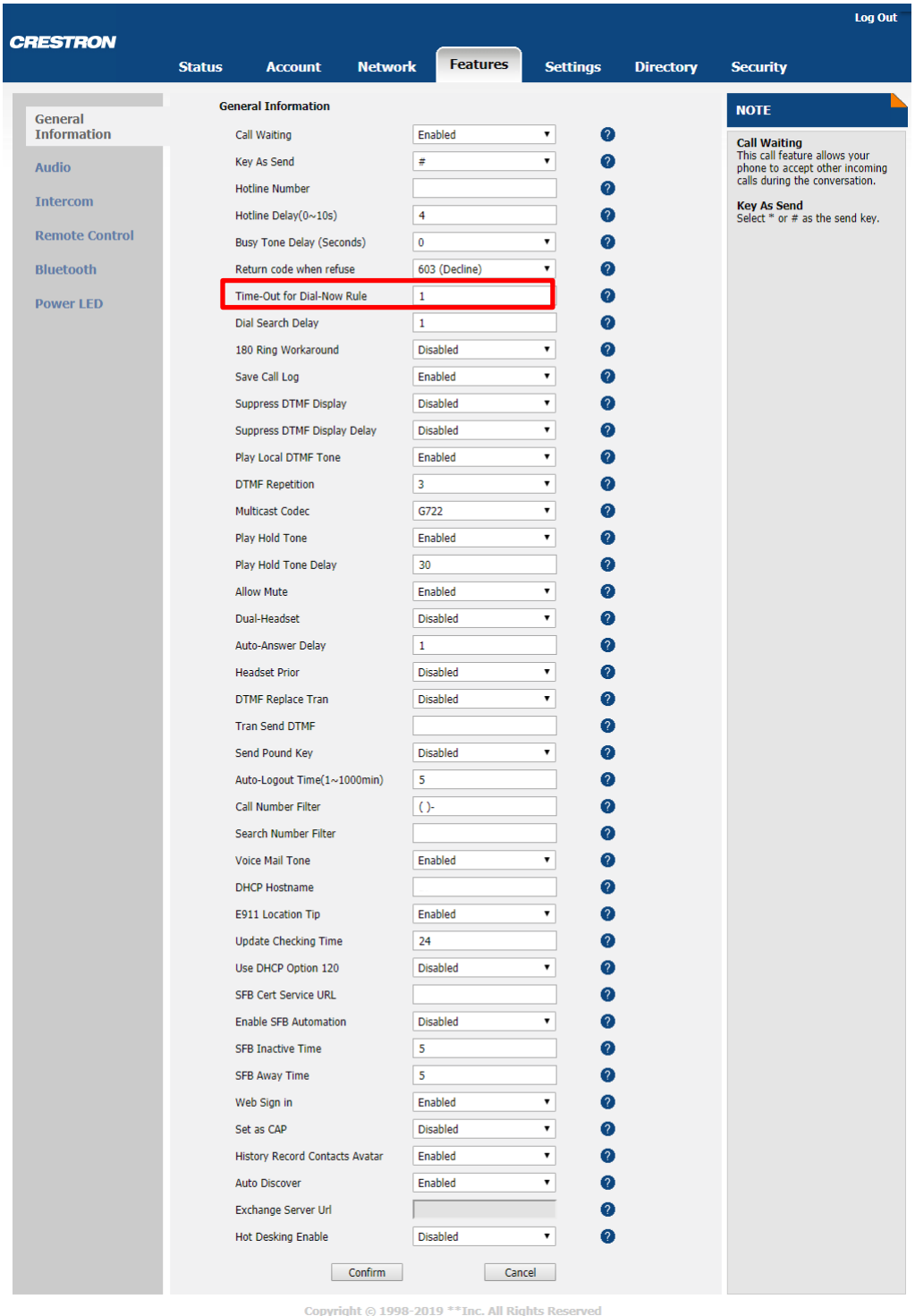


2. Enter the dial value in the **Rule** field.
3. Click **Add** to add the dial-now rule.

Configure the Delay Time for the Dial-Now Rule via the Web User Interface

1. Click **Features** > General Information.

Features > General Information



2. Enter the time-out time within 0-14 (in seconds) in the **Time-Out for Dial-Now Rule** field.
3. Click **Confirm** to accept the change.

Customize a Dial-Now Template File

The dial-now template helps with the creation of multiple dial-now rules. After setup, place the dial-now template to the provisioning server and specify the access URL in the configuration files.

Contact Crestron for a dial-now template. For more information on obtaining the dial-now template, refer to "Obtain Configuration Files/Resource Files" on page 87.

When editing a dial-now template, observe the following:

- <DialNow> indicates the start of a template and </DialNow> indicates the end of a template.
- When specifying the line for the dial-now rule, the valid value is 0 or 1. Whether the value is blank or set to 0 or 1, the dial-now rule will be applied to account 1.
- At most 100 rules can be added to the phone.

The expression syntax in the dial-now rule template is the same as that introduced in "Dial Plan" on page 162.

To customize a Dial-Now template:

1. Open the template file using an ASCII editor.
2. Create dial-now rules between <DialNow> and </DialNow>.

   For example:

   <data DialNowRule="99" LineID="1" /> Where:

   DialNowRule="" specifies the dial-now rule.

   LineID="" specifies the desired line for this rule. Whether the value is blank or set to 0 or 1, the dial-now rule will be applied to account 1.

Dial-Now Template

```
<?xml version="1.0" encoding="UTF-8"?>
<DialNow>
  <data DialNowRule="11" LineID="1" />
  <Data DialNowRule="22" LineID="" />
<data DialNowRule="*xx" LineID="1" />
<data DialNowRule="#xx" LineID="1" />
<data DialNowRule="000" LineID="1" />
<data DialNowRule="106" LineID="1" />
<data DialNowRule="101" LineID="1" />
<data DialNowRule="11xx" LineID="1" />
<data DialNowRule="12[23]x" LineID="1" />
<data DialNowRule="124xx" LineID="1" />
<data DialNowRule="1251xx" LineID="1" />
<data DialNowRule="1[38]xxxxxxxx" LineID="1" />
<data DialNowRule="13[1-9]xxx" LineID="1" />
<data DialNowRule="1345xxxx" LineID="1" />
<data DialNowRule="0[2-9]xxxxxxxx" LineID="1" />
<data DialNowRule="2xxx" LineID="1" />
<data DialNowRule="[3-9]xxxxxxx" LineID="1" />
<data DialNowRule="99" LineID="1" />
</DialNow>
```

Add a new dial-now rule

To change the dial-now rule, specify the values within double quotes.

3. Save the change and place this file to the provisioning server.
4. Specify the access URL of the dial-now template.

Specify the access URL of the dial-now template using configuration files.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the access URL of the dial-now template. **Parameter:** dialplan_dialnow.url

Details of the Configuration Parameter

Parameter	Permitted Values	Default
dialplan_dialnow.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the dial-now rule template file. **Example:** dialplan_dialnow.url = http://192.168.10.25/dialnow.xml During the auto provisioning process, the phone connects to the provisioning server "192.168.10.25", and downloads the dial-now rule file "dialnow.xml". **Web User Interface:** None **Phone User Interface:** None		

Hotline

Hotline, sometimes referred to as hot dialing, is a point-to-point communication link in which a call is automatically directed to a preset hotline number. If the handset is lifted, the Speakerphone key or line key is pressed, and nothing is done for a specified time interval, the phone will automatically dial the hotline number. Skype for Business phones only support one hotline number.

Hotline can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the hotline number. **Parameter:** features.hotline_number
		Specify the time (in seconds) the phone waits before automatically dialing out the hotline number. **Parameter:** features.hotline_delay
Local	Web User Interface	Configure the hotline number. Specify the time (in seconds) the phone waits before automatically dialing the hotline number. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure the hotline number. Specify the time (in seconds) the phone waits before automatically dialing out the hotline number.

Details of the Configuration Parameters

Parameter	Permitted Values	Default
features.hotline_number	**String within 32 characters**	**Blank**
Description: Configures the hotline number that the phone automatically dials out when the handset is lifted, or the Speakerphone/off-hook key or line key is pressed. Leaving it blank disables hotline feature. **Example:** features.hotline_number = 1234 **Web User Interface:** Features > General Information > Hotline Number **Phone User Interface:** Menu > Setting > Features > Hotline > Hot Number		

Parameter	Permitted Values	Default
features.hotline_delay	Integer from 0 to 10	4

Description:

Configures the waiting time (in seconds) for the phone to automatically dial out the hotline number.

If it is set to 0 (0s), the phone will immediately dial out the preconfigured hotline number when the handset is lifted or the Speakerphone/off-hook key are pressed.

If it is set to a value greater than 0, the phone will wait the designated seconds before dialing out the predefined hotline number when the handset is lifted or if the Speakerphone/off-hook key is pressed.

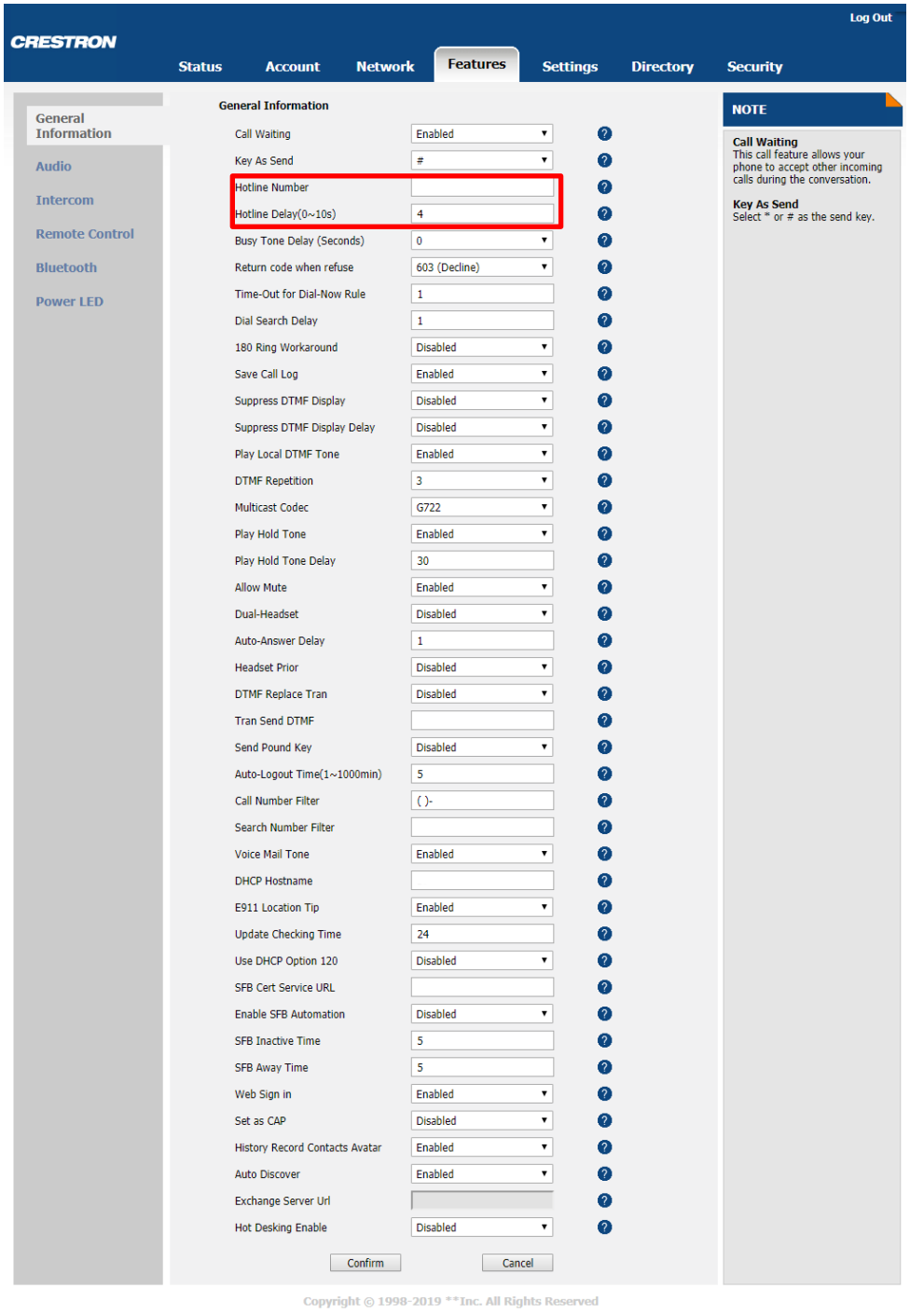
Web User Interface:
Features > General Information > Hotline Delay(0~10s)

Phone User Interface:
Menu > Setting > Features > Hotline > HotLine Delay

Configure Hotline via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Enter the hotline number in the **Hotline Number** field.
3. Enter the delay time (in seconds) in the **Hotline Delay(0~10s)** field.

4. Click **Confirm** to accept the change

Configure Hotline via the Phone User Interface

1. Tap **Setting** > **Features** > **Hotline**.
2. Enter the hotline number in the **Hot Number** field.
3. Enter the waiting time (in seconds) in the **Hotline Delay(s)** field.
4. Tap **Save** to accept the change.

Contact Management

A phone can store local contacts, Skype for Business contacts and Outlook contacts.

Skype for Business Directory

The Skype for Business directory on a phone stores all Skype for Business contacts (up to 1000 contacts). A user can search, add, view or delete Skype for Business contacts either by the phone or by the Skype for Business client.

Local Directory

Skype for Business phones also maintain a local directory. When adding a contact to the local directory, in addition to name and phone numbers, the user can also specify the ring tone and group for the local contact. Contacts can be added either one by one or in batch using a local contact file. The file format must be *.xml or *.csv.

Customize a Local Contact File

Contacts can be added one by one on the phone directly. Multiple contacts can be added at one time and/or contacts can be shared between phones using the local contact template file. After setup, place the template file to the provisioning server and specify the access URL of the template file in the configuration files. The existing local contacts on the phones will be overridden by the downloaded local contacts.

Contact Crestron for a local contact template.

For more information on obtaining the template file, refer to "Obtain Configuration Files/Resource Files" on page 87.

The following table lists meaning of each variable in the local contact template file:

Contact Template File Elements

Element	Values	Description
root_group	no	Group list's root element.
group	no	Group's root element.
display_name	All Contacts Favoritelist	An element of group. Group name.

Element	Values	Description
root_contact	no	Contact list's root element.
contact	no	Contact's root element.
display_name	String	An element of contact. Contact name. **Note:** This value cannot be blank or duplicated.
office_number	String	Office number of the contact.
mobile_number	String	Mobile number of the contact.
other_number	String	Other number of the contact.
address	String	Contact's address.
line	Valid Value: -1 or 0 - -1 stands for Auto (the first registered line) - 0 stands for line1	Since the Skype for Business phones only support account 1, no matter which account is selected (0 or 1), the contacts will all be added to account 1.
ring	Format of the value:	An element of contact.
	System ring tone: - **Auto** - **Resource:Silent.wav** - **Resource:Splash.wav** - **Resource:RingN.wav** (integer N ranges from 1 to 8) Custom ring tone: **Custom:Name.wav**	Contact ring tone.
email	String	Contact's email address.
title	String	Contact's title.
priority	0~32.	It is only applicable to local favorites. Favorites display consecutively, according to their priority. The favorite with the lowest number displays first.
group_id_name	Valid Value: All Contacts, Favoritelist	Group name of a contact.

The following shows the procedure for customizing a local contact file for Skype for Business phones:

To customize a Local Contact file

1. Open the template file using an ASCII editor.
2. For each contact to be added, add the following string to the file. Each starts on a separate line:

   <contact display_name="" office_number=" mobile_number="" other_number="" address=" " line="" ring="" email="" title="" priority="" group_id_name="" />

3. Specify the values within double quotes. For example:

   <contact display_name="Yealink" office_number="123" mobile_number="234" other_number="345" address="china" line="-1" ring="Auto" email="456@crestronuc.com" title="manager" priority="0" group_id_name="All Contacts" />

   Local Contact File

```
<root_group>
  <group display_name="All Contact" />
  <group display_name="Favoritelist" />
  <group />
</root_group>
<root_contact>
  <contact display_name="Crestron" office_number="123"
mobile_number="234" other_numer="345" address="USA" line="-1"
ring="Auto" email=456@crestronuc.com title= "manager" priority="0"
group_id_name="All Contacts" />
</root_contact>
```

4. Save the change and place this file to the provisioning server.
5. Specify the access URL of the custom local contact template in the configuration files. For example:

   local_contact.data.url = tftp://192.168.10.25/contact.xml

   During the auto provisioning process, the phone connects to the provisioning server "192.168.10.25", and downloads the contact file "contact.xml".

Local directory can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Specify the access URL of the local contact file (*.xml). **Parameter:** local_contact.data.url
Local	Web User Interface	Add a new contact to the local directory. To import or export the local contact file. **Navigate to**: http://<phoneIPAddress>/servlet?p=contactsbasic&q=load&num=1&g roup=
	Phone User Interface	Add a new contact to the local directory.

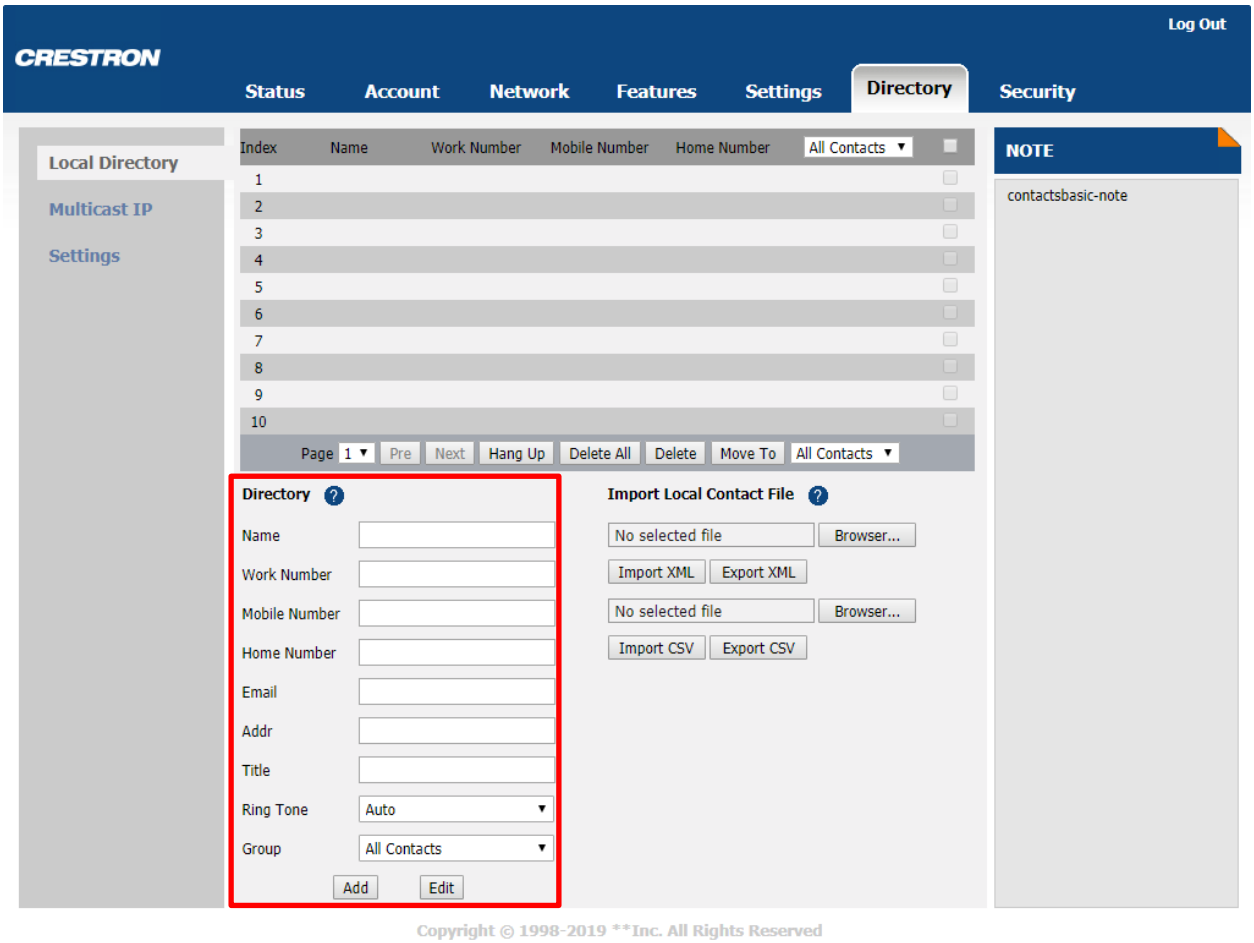
Details of the Configuration Parameter

Parameter	Permitted Values	Default
local_contact.data.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the local contact file (*.xml). **Example:** local_contact.data.url = http://192.168.10.25/contact.xml **Web User Interface:** Directory > Local Directory > Import Local Contact File **Phone User Interface:** None		

Add a Contact to the Local Directory via the Web User Interface

1. Click **Directory** > **Local Directory**.

Directory > Local Directory

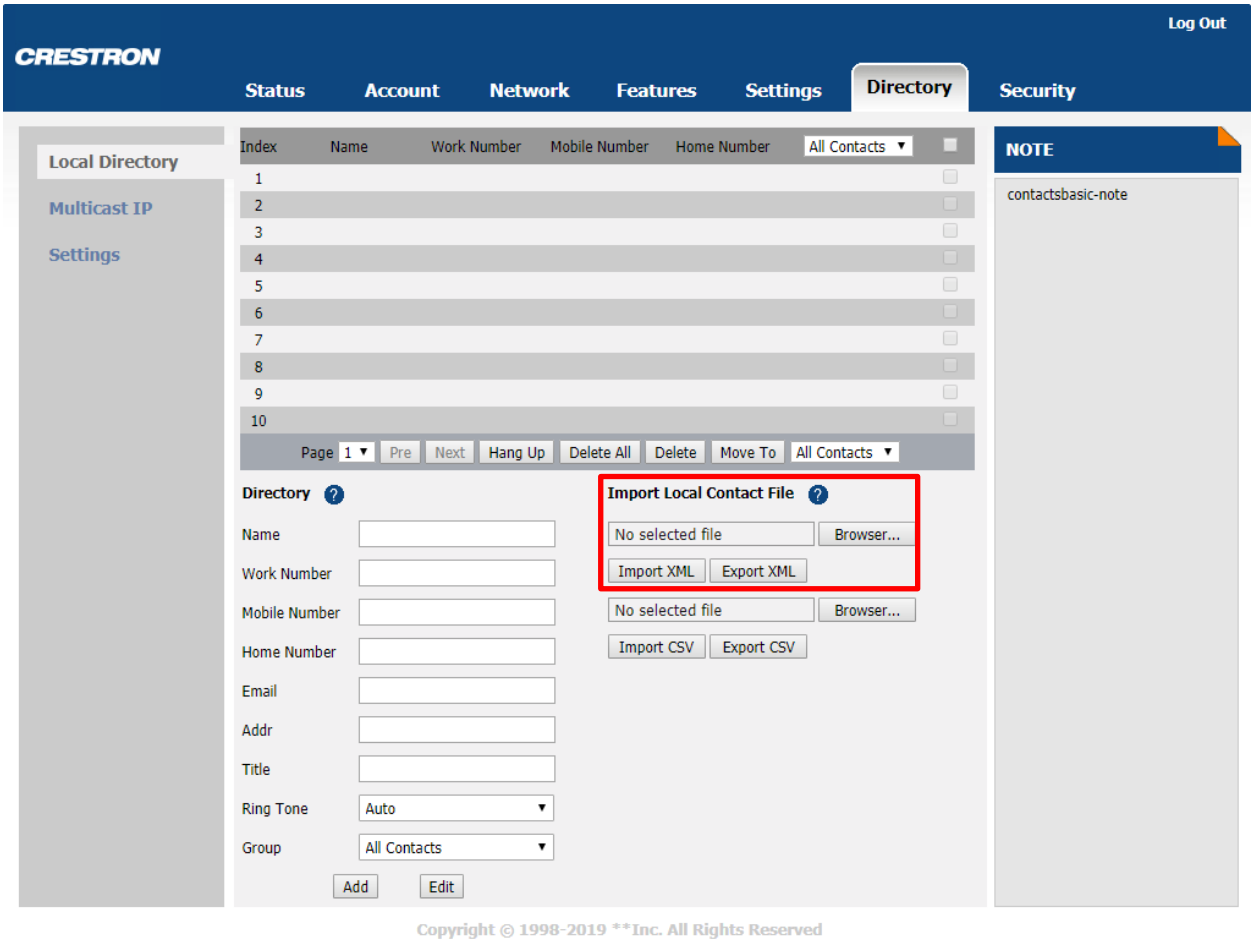


2. In the **Directory** section, enter name, work number, mobile number, home numbers, email, address and title in the corresponding fields.
3. Select the ring tone from the **Ring Tone** drop-down list.
4. Select **All Contacts** from the Ring Tone drop-down list.
5. Click **Add** to add the contact.

Import an XML Contact List File via the Web User Interface

1. Click **Directory** > **Local Directory**.

Directory > Local Directory

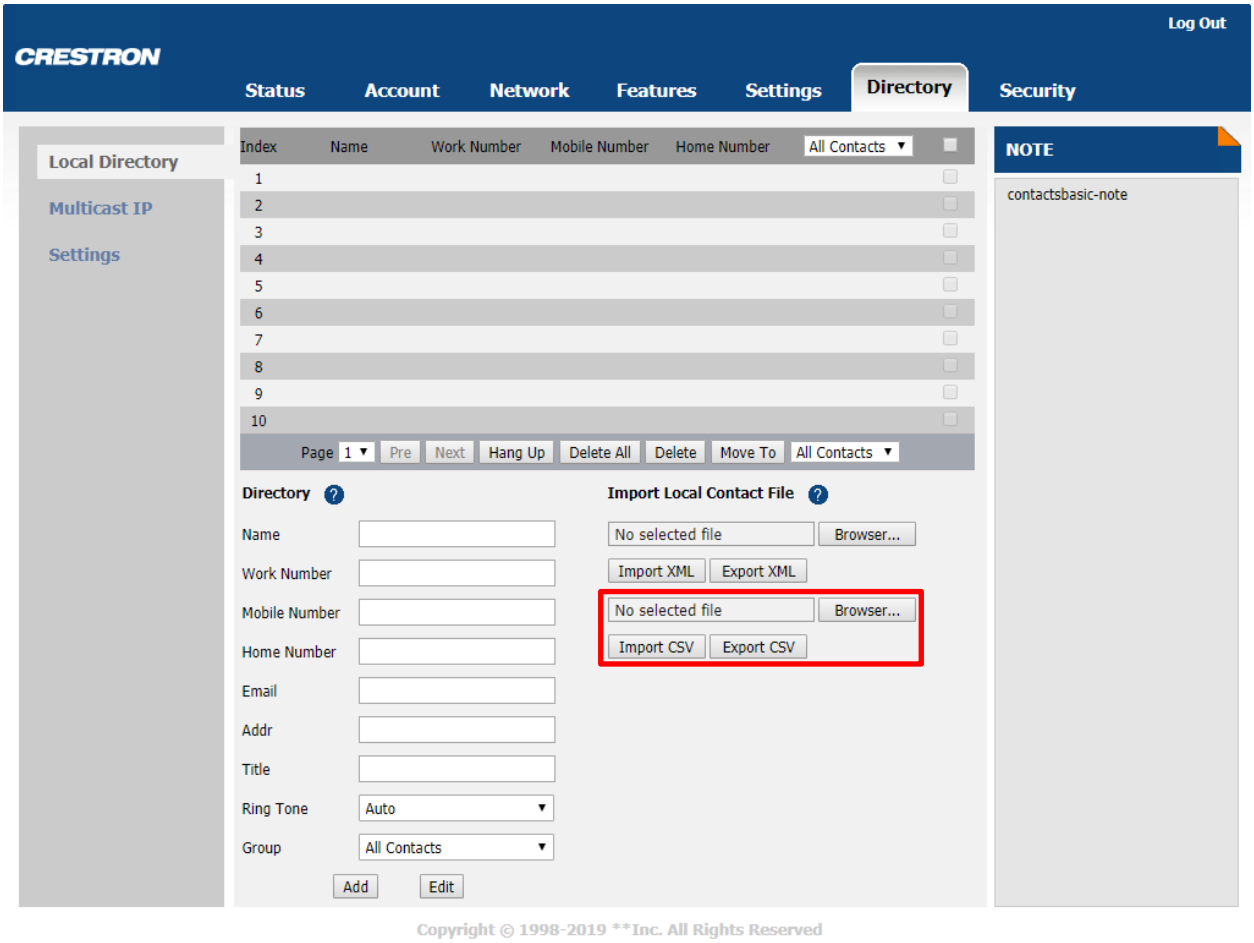


2. Click **Browser** to locate a contact list file (the file format must be *.xml) from the local system.
3. Click **Import XML** to import the contact list. The web user interface prompts "The original contact will be covered, Continue?".
4. Click **OK** to complete importing the contact list.

Import a CSV Contact List File via the Web User Interface

1. Click **Directory** > **Local Directory**.

Directory > Local Directory



2. Click **Browser** to locate a contact list file (the file format must be *.csv) from the local system.
3. (Optional.) Check the **Show Title** checkbox. It will prevent importing the title of the contact information which is located in the first line of the CSV file.
4. Click **Import CSV** to import the contact list.
5. (Optional.) Select **On** in the **Delete Old Contacts** field to delete all existing contacts while importing the contact list.
6. Select the contact information to import into the local directory from the **Index** drop-down list. At least one item should be selected to be imported into the local directory.
7. Click **Import** to complete importing the contact list.

Export a Contact List via the Web User Interface

1. Click **Directory** > **Local Directory**.
2. Click **Export XML** (or **Export CSV**).
3. Click **Save** to save the contact list to the local system.

Add a Local Favorite via the Phone User Interface

1. Enter a name in the search bar (tap **Search**) or view the call logs (tap **History**).
2. Tap the contact to be added.
3. Tap **Add to Local**. The contact is added to the **Local Directory** contact group.

NOTE: The contact with the lowest priority number displays first.

Manage Local Favorites

Local favorites and Skype for Business favorites of the phone are displayed on the idle screen. By default, local favorites are displayed before the Skype for Business favorites.

The phone can be configured to display local favorites on the idle screen and the display order of the local favorites can also be configured.

Local favorite contacts are indicated by a  icon. Skype for Business favorite contacts are indicated by the presence status icon.

NOTE: Only Skype for Business favorites display presence status.

Local favorites can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure whether to display local favorites on the idle screen. **Parameter:** sfb.local_favorite.enable
		Configure the display order of the local favorites on the idle screen. **Parameter:** sfb.local_favorite.sort
Local	Web User Interface	Configure whether to display local favorites on the idle screen. Configure the display order of the local favorites on the idle screen. **Navigate to**: http://<phoneIPAddress>/servlet?p=contacts-settings&q=load

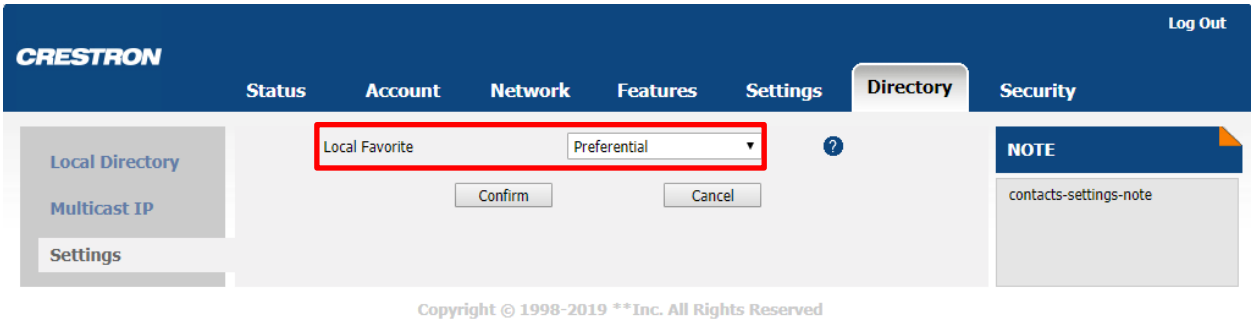
Details of the Configuration Parameters

Parameter	Permitted Values	Default
sfb.local_favorite.enable	0 or 1	1
Description: Enables or disables the phone to display local favorites on the idle screen. **0**- Disabled, local favorites are not displayed on the idle screen, only Skype for Business favorites are displayed on the idle screen. **1**- Enabled, local favorites and Skype for Business favorites are displayed on the idle screen. Web **User Interface:** Directory > Settings > Local Favorite **Phone User Interface:** None		
sfb.local_favorite.sort	1 or 2	1
Description: Configures the order of the local favorites on the idle screen. **0**- Preferential, the local favorites will be displayed before the Skype for Business favorites on the idle screen. **1**- General, the local favorites will be displayed after the Skype for Business favorites on the idle screen. **Note:** This feature works only if the value of the parameter "sfb.local_favorite.enable" is set to 1 (Enabled). Web **User Interface:** Directory > Settings > Local Favorite **Phone User Interface:** None		

Configure the Display Order of Local Favorites via the Web User Interface

1. Click **Directory** > **Settings**.

Directory > Settings



2. Select **Disabled**, **Preferential**, or **General** from the **Local Favorite** drop-down list.
   - **Disabled:** Only Skype for Business favorites are displayed on the idle screen.
   - **Preferential:** Local favorites will be displayed before the Skype for Business favorites on the idle screen.

– **General:** Local favorites will be displayed after the Skype for Business favorites on the idle screen.

3. Click **Confirm** to accept the change.

Outlook Contacts

Skype for Business Server and Exchange Server are integrated. Outlook contacts can only be added through Microsoft Outlook. Once contacts are in Outlook, a user can view and search Outlook contacts on their phone.

Outlook contacts can be configured using the configuration files only.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configures the phone to display a directory called Outlook Contacts. **Parameter:** exchange.outlook_contact.enable
		Configures how many Outlook contacts can be displayed when a user performs a search. **Parameter:** phone_setting.search_outlook_contacts.return_number
		Configures the phone to synchronize Outlook contacts from the Microsoft Exchange Server. **Parameter:** exchange.outlook_contact_sync.enable
		Configures the interval (in minutes) that the phone automatically checks if an Outlook contacts update is available on the Microsoft Exchange Server. **Parameter:** phone_setting.outlook_contacts.update_time
		Configures the maximum Outlook contacts that can be downloaded from the Microsoft Exchange Server. **Parameter:** exchange.outlook_contact.request_number

Details of the Configuration Parameters

Parameter	Permitted Values	Default
exchange.outlook_contact.enable	0 or 1	0
Description: Enables or disables the phone to display a directory called Outlook Contacts. This directory will include the user's Outlook contacts. **0**- Disabled **1**- Enabled **Web User Interface:** None **Phone User Interface:** None		
phone_setting.search_outlook_contacts.return_number	20	Refer to the following content
Description: Configures the number of results that are displayed when performing a search from the Outlook Directory. **Web User Interface:** None **Phone User Interface:** None		
exchange.outlook_contact_sync.enable	0 or 1	1
Description: Enables or disables the phone to synchronize Outlook contacts from the Exchange Server. **0**- Disabled **1**- Enabled **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** None		

Parameter	Permitted Values	Default
phone_setting.outlook_contacts.update_time	Integer from 0 to 100	10
Description: Configures the interval (in minutes) for the phone to automatically check if any Outlook contact updates are available on the Microsoft Exchange Server. If it is set to 10 (in minutes), the phone will check if any Outlook contact updates are available on the Microsoft Exchange Server every 10 minutes. If an update is available, the phone will download the Outlook contacts. **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** None		
exchange.outlook_contact.request_number	Integer from 1 to 5000	Refer to the following content
Description: Configures the maximum number of Outlook contacts that can be downloaded from the Exchange Server. The default value is 500. **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** None		

Search for Outlook Contacts

Outlook contacts can be searched from the predialing screen only. To search for a contact, tap **Search**, and then start typing the name of the contact with the numeric keypad or use the on-screen keyboard to enter a name. The phone performs an Intelligent search (i.e., press the **2** key to search the letters "2, a, b and c").

Entries whose name or phone number matches the characters entered will appear on the display. The search results include Skype for Business contacts, local contacts and Microsoft Outlook contacts.

View Outlook Contacts

If the phone has been configured to display a directory named Outlook Contacts using the parameter "exchange.outlook_contact.enable", the Outlook Contacts directory will be displayed.

Call Log

Save Call Log

The call log contains call information such as remote party identification, time and date, and call duration. It can be used to redial previous outgoing calls, return incoming calls, and save contact information from call log lists to the contact directory.

Skype for Business phones maintain a local call log. The call log consists of four lists: All Calls, Missed Calls, Placed Calls, and Received Calls. Each call log list supports up to 100 entries. To store call information, the save call log feature must be enabled in advance. The call history information can be accessed via the phone user interface only.

Call log can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure call log feature. **Parameter:** features.save_call_history
Local	Web User Interface	Configure call log feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure call log feature.

Details of the Configuration Parameter

Parameter	Permitted Values	Default
features.save_call_history	**0 or 1**	**1**

Description:

Enables or disables the phone to save the local call log.

0- Disabled, the phone cannot save the missed calls, placed calls, received calls and the forwarded calls in the call log lists.

1- Enabled

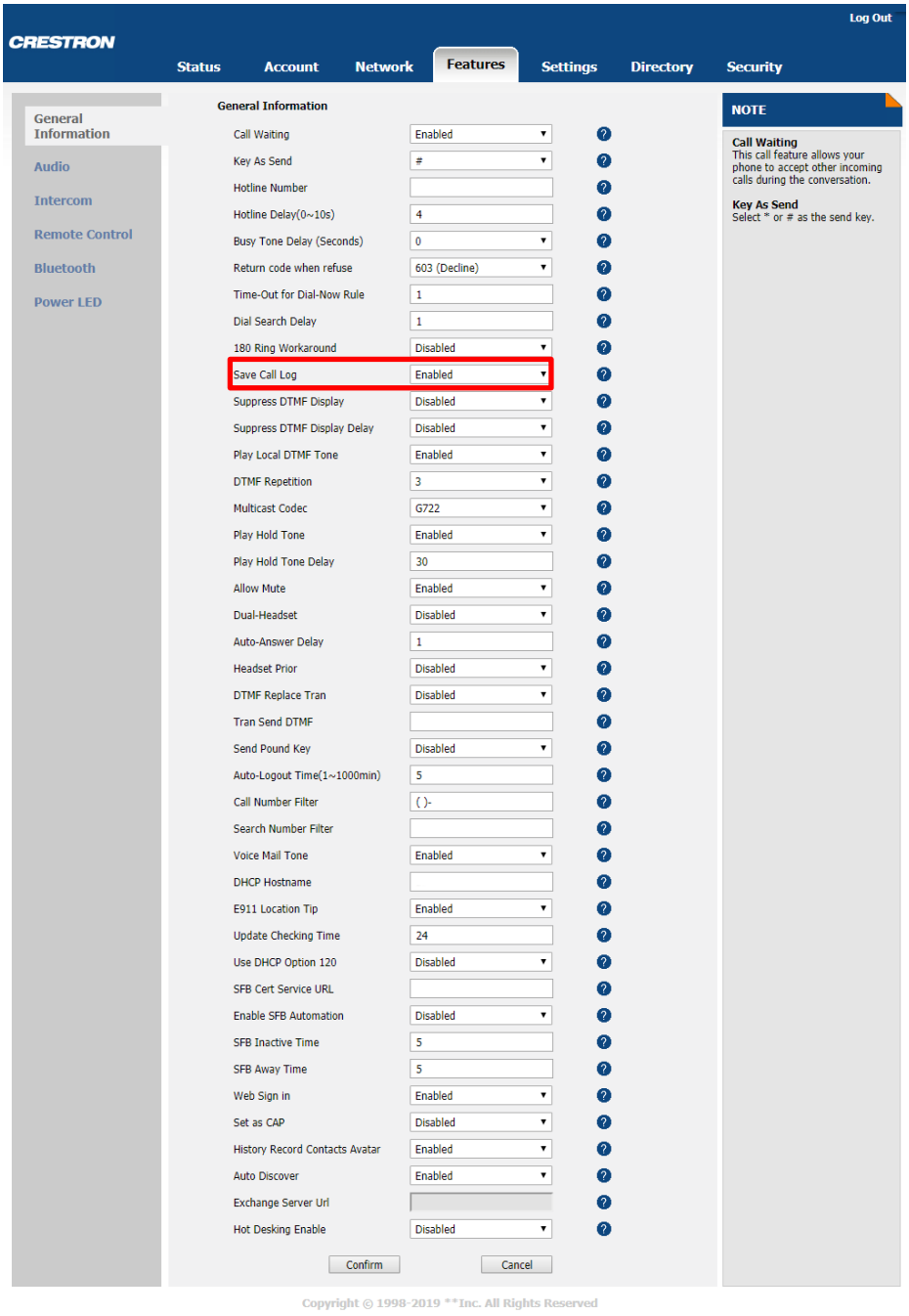
Web User Interface:
Features > General Information > Save Call Log

Phone User Interface:
Menu > Setting > Features > History Setting > History Record

Save Call Log Feature via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Select **Enabled** or **Disabled** from the **Save Call Log** drop-down list.
3. Click **Confirm** to accept the change.

Configure Call Log Feature via the Phone User Interface

1. Tap **Setting** > **Features** > **History Setting**.
2. In the **History Record** setting, tap **On** to turn on the call log. Tap **Off** to turn off the call log.
3. Tap **Save**.

Export Call Log

The user or administrator can download the call logs to the local system to check the phone events.

Exporting call log can be configured via web user interface.

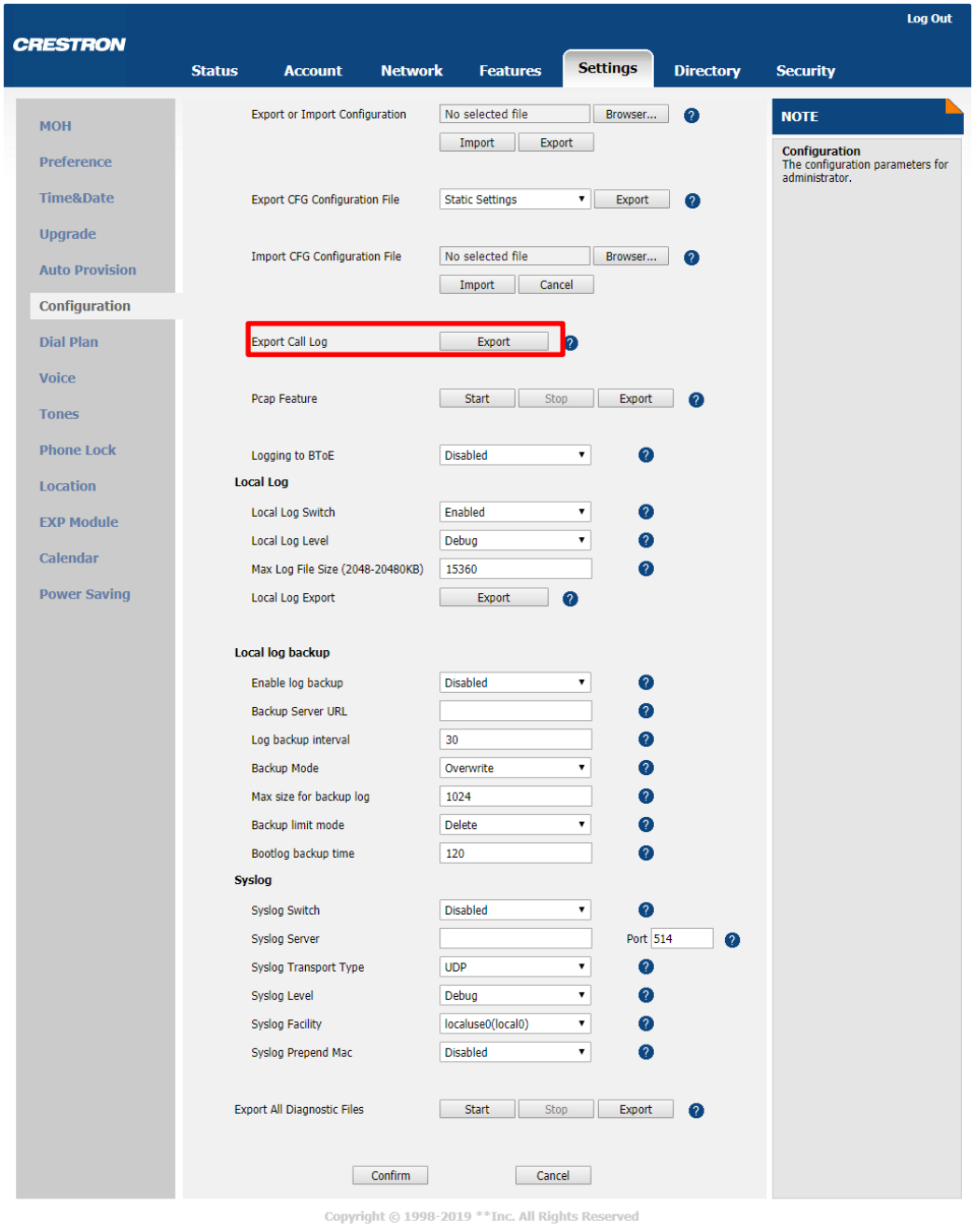
Configuration Methods

Local	Web User Interface	Export the call log. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-config&q=load

Export the Call Log via the Web User Interface

1. Click **Settings** > **Configuration**.

Settings > Configuration



2. Click **Export** to open file download window, and then save the file to the local PC.

Missed Call Log

Missed call log allows the phone to display the number of missed calls with an indicator icon on the idle screen, and to log missed calls in the Missed Calls list. Once the user accesses the Missed Calls list, the indicator icon on the idle screen disappears.

The missed call log can be configured using the following methods.

Configuration Methods

Central Provisioning (Configuration File)	**<MAC>.cfg**	Configure missed call log feature. **Parameter:** account.1.missed_calllog
Local	Web User Interface	Configure missed call log feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0

Details of the Configuration Parameter

Parameter	Permitted Values	Default
account.1.missed_calllog	**0 or 1**	**1**

Description:

Enables or disables the phone to indicate and record missed calls for the account.

0- Disabled, the phone does not display the indicator on the idle screen and does not log the missed call in the Missed Calls list.

1- Enabled, the phone displays an indicator icon on the idle screen and logs the missed call in the Missed Calls list.

Note: This feature works only if the value of the parameter "features.save_call_history" is set to 1 (Enabled).

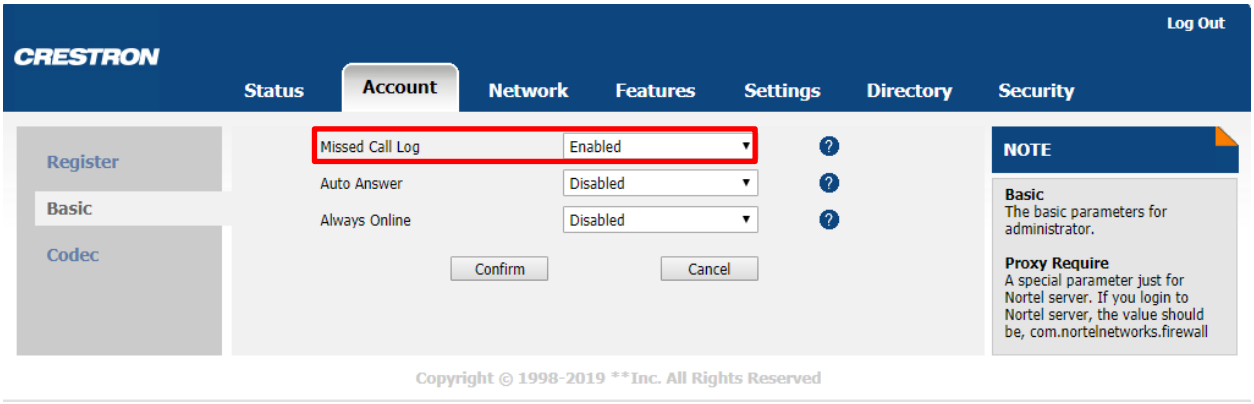
Web User Interface:
Account > Basic > Missed Call Log

Phone User Interface:
None

Configure the Missed Call Log via the Web User Interface

1. Click **Account** > **Basic**.

Account > Basic



2. Select **Enabled** or **Disabled** from the **Missed Call Log** drop-down list.
3. Click **Confirm** to accept the change.

History Record Contacts Avatar

The History record contacts avatar allows the phone to display the contact avatar for every history record.

The History record contacts avatar can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<MAC>.cfg**	Configure the contacts avatar for history record. **Parameter:** features.call_history_contacts_avator.enable
Local	Web User Interface	Configure the contacts avatar for history record. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of the Configuration Parameter

Parameters	Permitted Values	Default
features.call_history_contacts_avator.enable	0 or 1	1

Description:

Enables or disables the phone to display the contact avatars for every history record.

0- Disabled, the phone does not display contact avatars.

1- Enabled, the phone displays contact avatars.

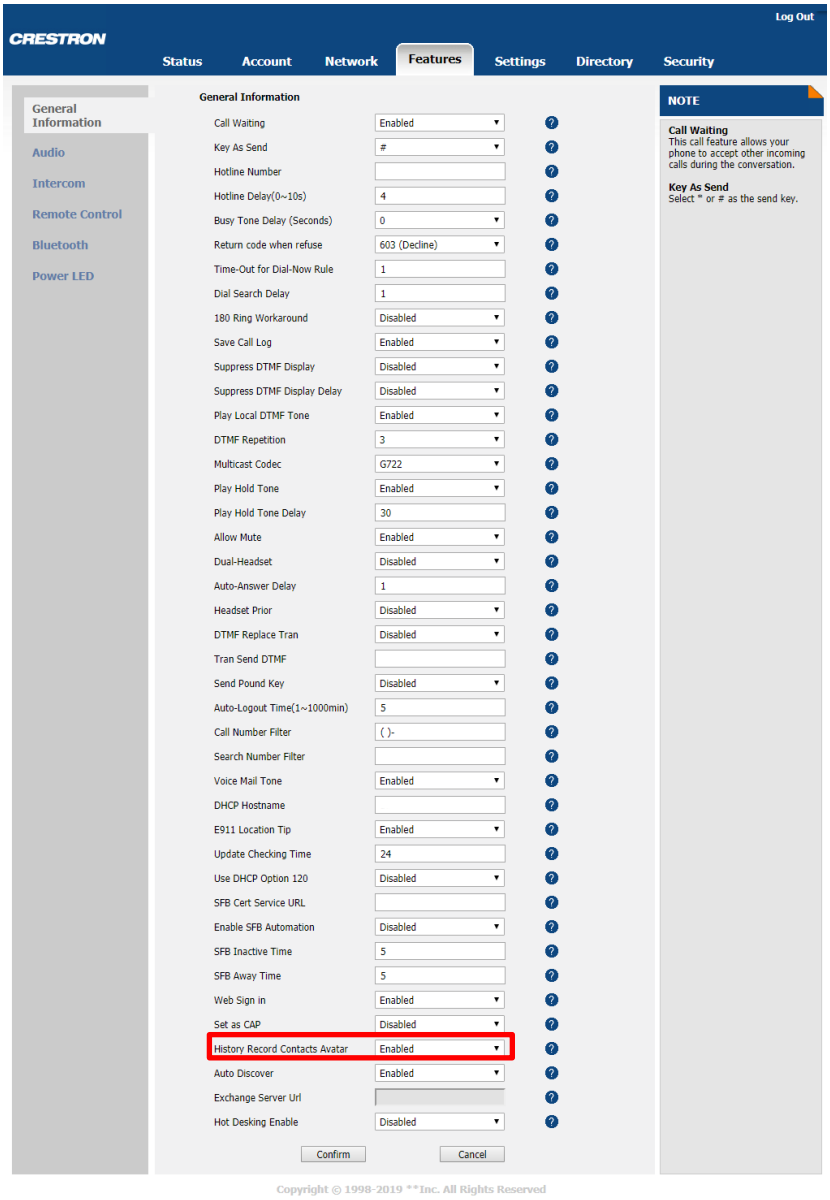
Web User Interface:
Features > General Information > History Record Contacts Avatar

Phone User Interface:
Menu > Setting > Features > History Setting > Contacts Avatar

Configure Contacts Avatar Feature via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Select **Enabled** or **Disabled** from the **History Record Contacts Avatar** drop-down list.
3. Click **Confirm** to accept the change.

Configure Contacts Avatar Feature via the Phone User Interface

1. Tap **Setting** > **Advanced** > **Features** > **History Setting**.
2. In the **Contacts Avatar** setting, tap **On** to turn on the feature. Tap **Off** to turn off the feature.

3. Tap **Save**.

Dial Search Delay

Dial search delay defines a period of delay time before the phone automatically displays the search results. It is applicable only when searching for contacts on the dialing screen.

Dial search delay can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure dial search delay feature. **Parameter**: sfb.search_delay_time
Local	Web User Interface	Configure dial search delay feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

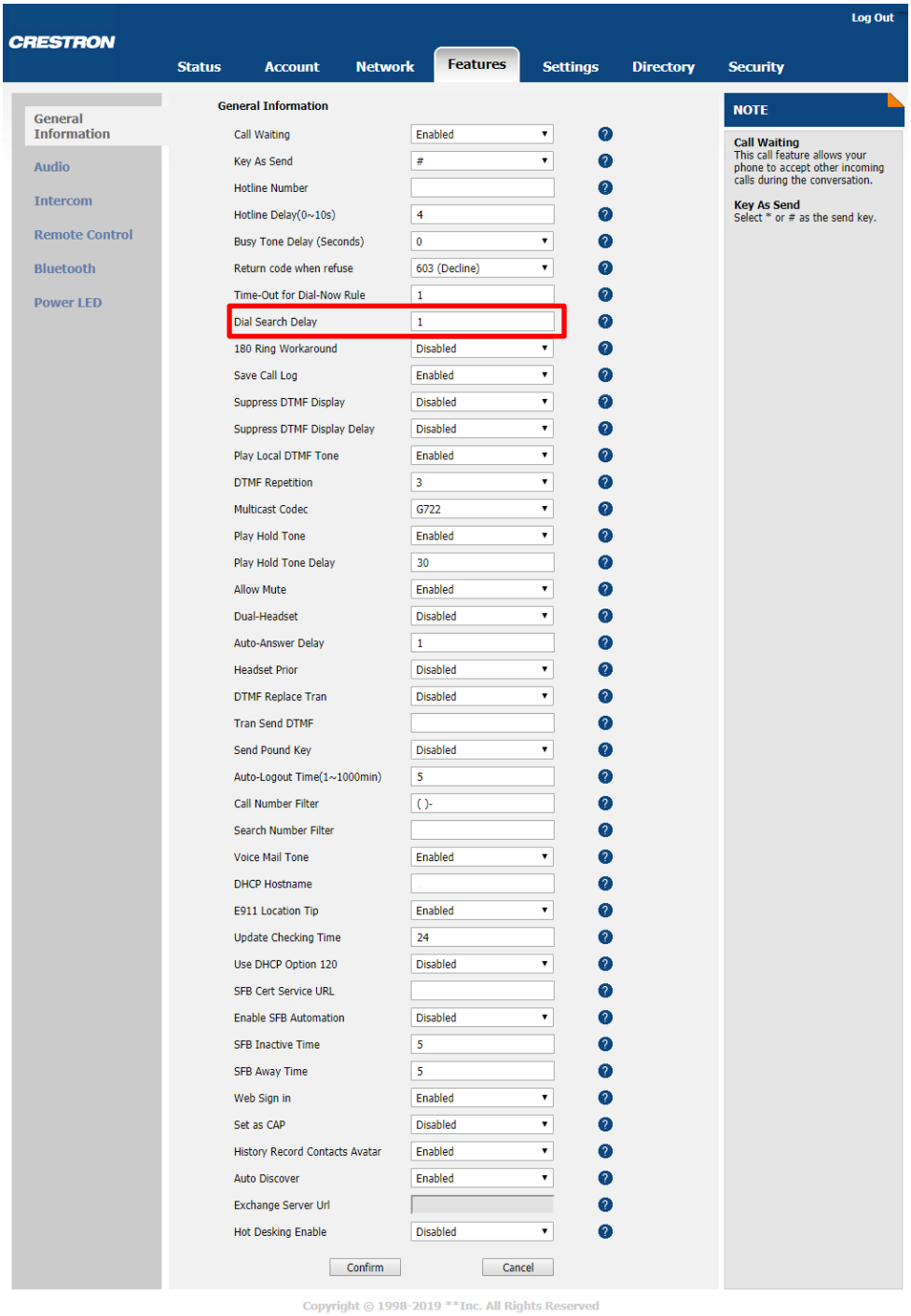
Details of the Configuration Parameter

Parameter	Permitted Values	Default
sfb.search_delay_time	**Integer from 1 to 10**	**1**
Description: Configures the delay time (in seconds) for the phone to automatically display the search results on the dialing screen. **Example:** sfb.search_delay_time = 1 **Web User Interface:** Features > General Information > Dial Search Delay **Phone User Interface:** None		

Configure Dial Search Delay via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Select the dial search delay time (in seconds) from the **Dial Search Delay** drop-down list.

3. Click **Confirm** to accept the change.

Live Dialpad

Live Dialpad allows the phone to automatically dial out the entered phone number after a specified period of time.

Live Dialpad can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure live dialpad. **Parameters:** phone_setting.predial_autodial phone_setting.inter_digit_time
Local	Web User Interface	Configure live dialpad. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-preference&q=load

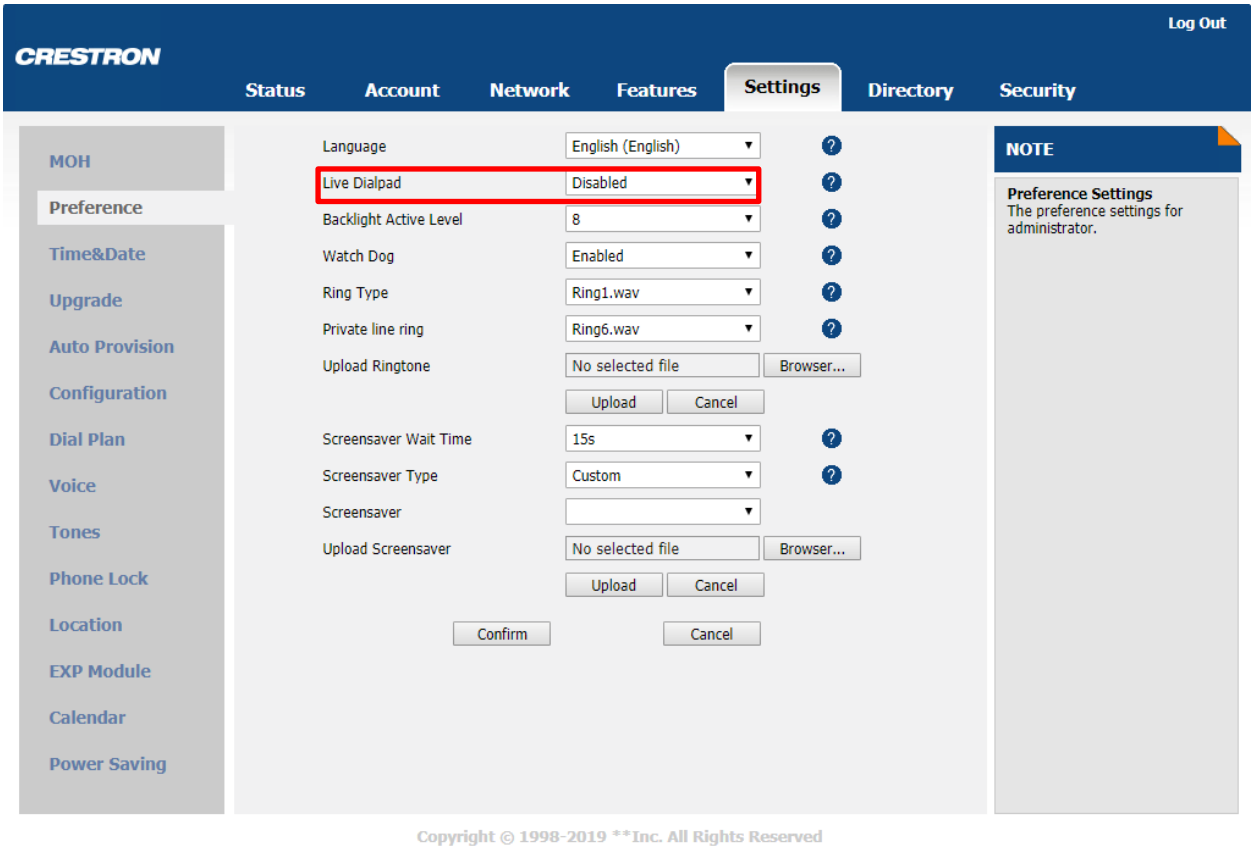
Details of the Configuration Parameters

Parameter	Permitted Values	Default
phone_setting.predial_autodial	**0 or 1**	**0**
Description: Enables or disables the Live Dialpad feature. **0**- Disabled **1**- Enabled, the phone will automatically dial out the entered phone number on the dialing screen without pressing a send key. **Web User Interface:** Settings > Preference > Live Dialpad **Phone User Interface:** None		
phone_setting.inter_digit_time	**Integer from 1 to 14**	**8**
Description: Configures the delay time (in seconds) for the phone to automatically dial out the entered digits without pressing a send key. **Note:** This feature works only if the value of the parameter "phone_setting.predial_autodial" is set to 1 (Enabled). **Web User Interface:** None **Phone User Interface:** None		

Configure Live Dialpad via the Web User Interface

1. Click **Settings** > **Preference**.

Settings > Preference



2. Select **Enabled** or **Disabled** from the **Live Dialpad** drop-down list.
3. Click **Confirm** to accept the change.

Call Waiting

Call waiting enables a user to receive another call when there is already an active call. If it is disabled, the new incoming call will be rejected automatically.

The Call Waiting feature can be enabled and set to have the phone play a warning tone to avoid missing important calls during a call. The Call Waiting tone works only if Call Waiting is enabled. The Call Waiting tone can be customized or specialized tone sets can be selected (vary from country to country) for the phone. For more information, refer to "Tones" on page 277.

Call waiting and call waiting tone can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure call waiting and call waiting tone. **Parameter:** call_waiting.enable call_waiting.tone
Local	Web User Interface	Configure call waiting. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
		Configure call waiting tone. **Navigate** to: http://<phoneIPAddress>/servlet?p=features-audio&q=load
	Phone User Interface	Configure call waiting and call waiting tone.

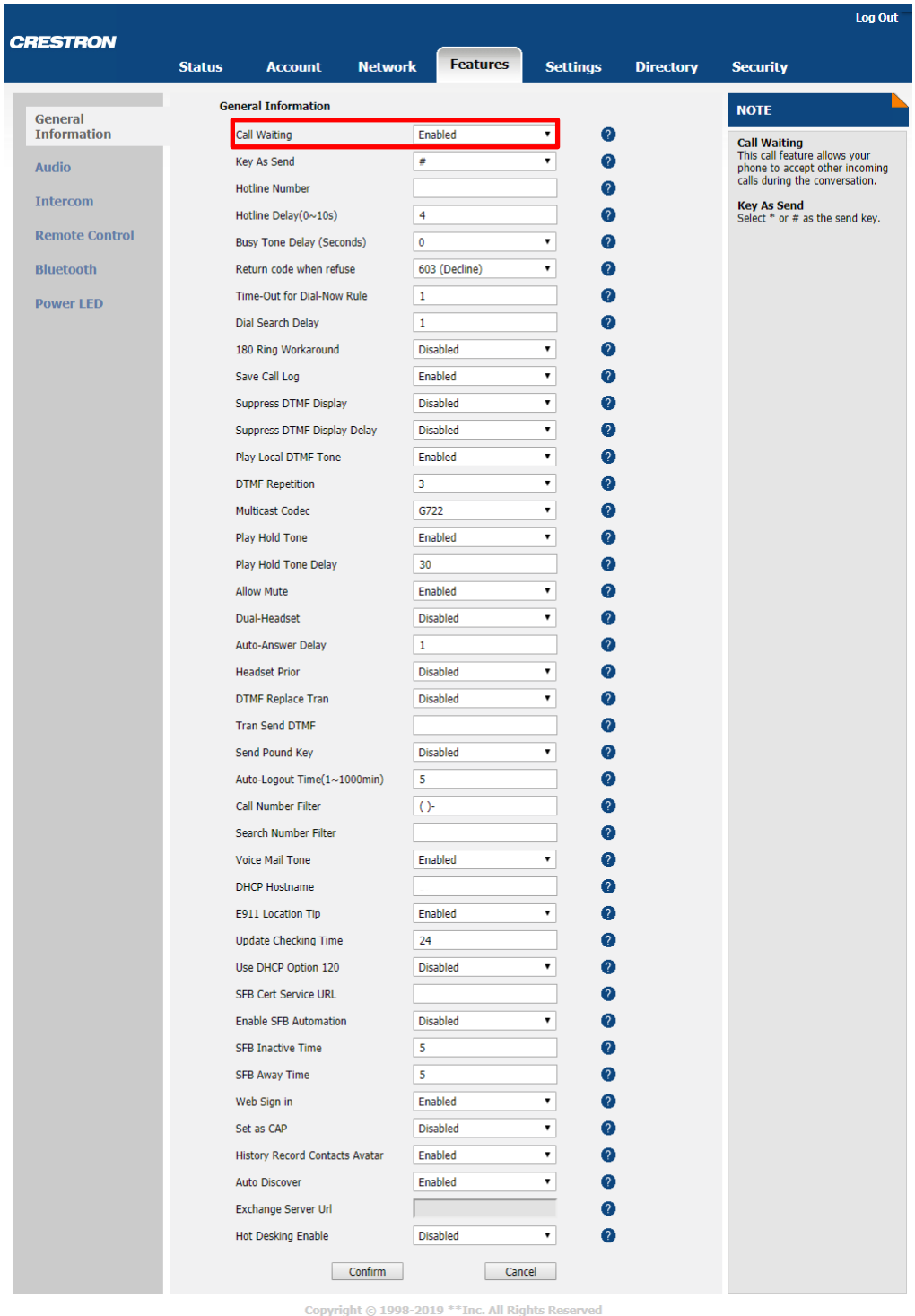
Details of the Configuration Parameter

Parameter	Permitted Values	Default
call_waiting.enable	**0 or 1**	**1**
Description: Enables or disables the Call Waiting feature. **0**- Disabled, a new incoming call is automatically rejected by the phone with a busy message while during a call. **1**- Enabled, the LCD screen will display a new incoming call while on a call. **Web User Interface:** Features > General Information > Call Waiting **Phone User Interface:** Menu > Setting > Features > Call Waiting > Call Waiting		
call_waiting.tone	**0 or 1**	**1**
Description: Enables or disables the phone to play the call waiting tone when the phone receives an incoming call during a call. **0**- Disabled **1**- Enabled **Note:** This feature works only if the value of the parameter "call_waiting.enable" is set to 1 (Enabled). **Web User Interface:** Features > Audio > Call Waiting Tone **Phone User Interface:** Menu > Setting > Features > Call Waiting > Play Tone		

Configure Call Waiting via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Select **Enabled** or **Disabled** from the **Call Waiting** drop-down list.

3. Click **Confirm** to accept the change.

Configure Call Waiting via the Phone User Interface

1. Tap **Setting** > **Features** > **Call Waiting**.
2. In the **Call Waiting** setting, tap **On** to turn on the feature. Tap **Off** to turn off the feature.
3. In the **Play Tone** setting, tap **On** to turn on the feature. Tap **Off** to turn off the feature.
4. Tap **Save**.

Auto Answer

Auto answer allows the phone to automatically answer an incoming call. Skype for Business phones will not automatically answer the incoming call during a call even if auto answer is enabled. Auto-Answer delay defines a period of delay time before the phone automatically answers incoming calls.

An auto answer tone allows the phones to play a tone when an incoming call is automatically answered. The auto answer tone can be customized or specialized tone sets can be selected (vary from country to country) for the phone. For more information, refer to "Tones" on page 277.

Auto answer can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<MAC>.cfg**	Configure auto answer. **Parameter:** account.1.auto_answer
	<y0000000000xx>.cfg	Specify a period of delay time for auto answer. **Parameter:** features.auto_answer_delay
Local	Web User Interface	Configure auto answer. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-basic&q=load&acc=0 Specify a period of delay time for auto answer. **Navigate to**:http://<phoneIPAddress>servlet?p=features-general&q=load

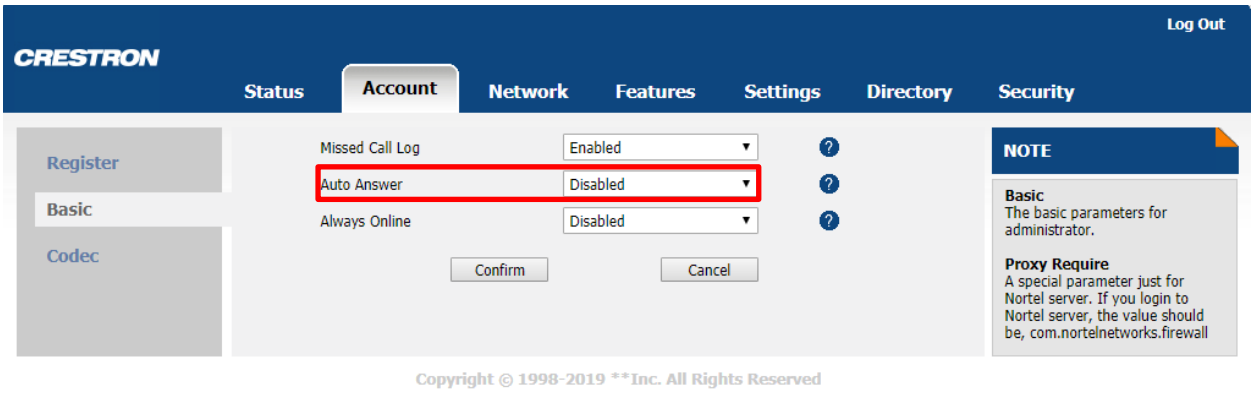
Details of the Configuration Parameters

Parameter	Permitted Values	Default
account.1.auto_answer	0 or 1	0
Description: Enables or disables the Auto Answer feature for the account. **0**- Disabled **1**- Enabled, the phone can automatically answer an incoming call. **Note:** The phone cannot automatically answer the incoming call during a call even if auto answer is enabled. **Web User Interface:** Account > Basic > Auto Answer **Phone User Interface:** Menu > Setting > Features > Auto Answer > Line 1 > Auto Answer		
features.auto_answer_delay	Integer from 1 to 4	1
Description: Configures the delay time (in seconds) before the phone automatically answers an incoming call. **Web User Interface:** Features > General Information > Auto-Answer Delay(1~4s) **Phone User Interface:** None		

Configure Auto Answer via the Web User Interface

1. Click **Account** > **Basic**.

Account > Basic

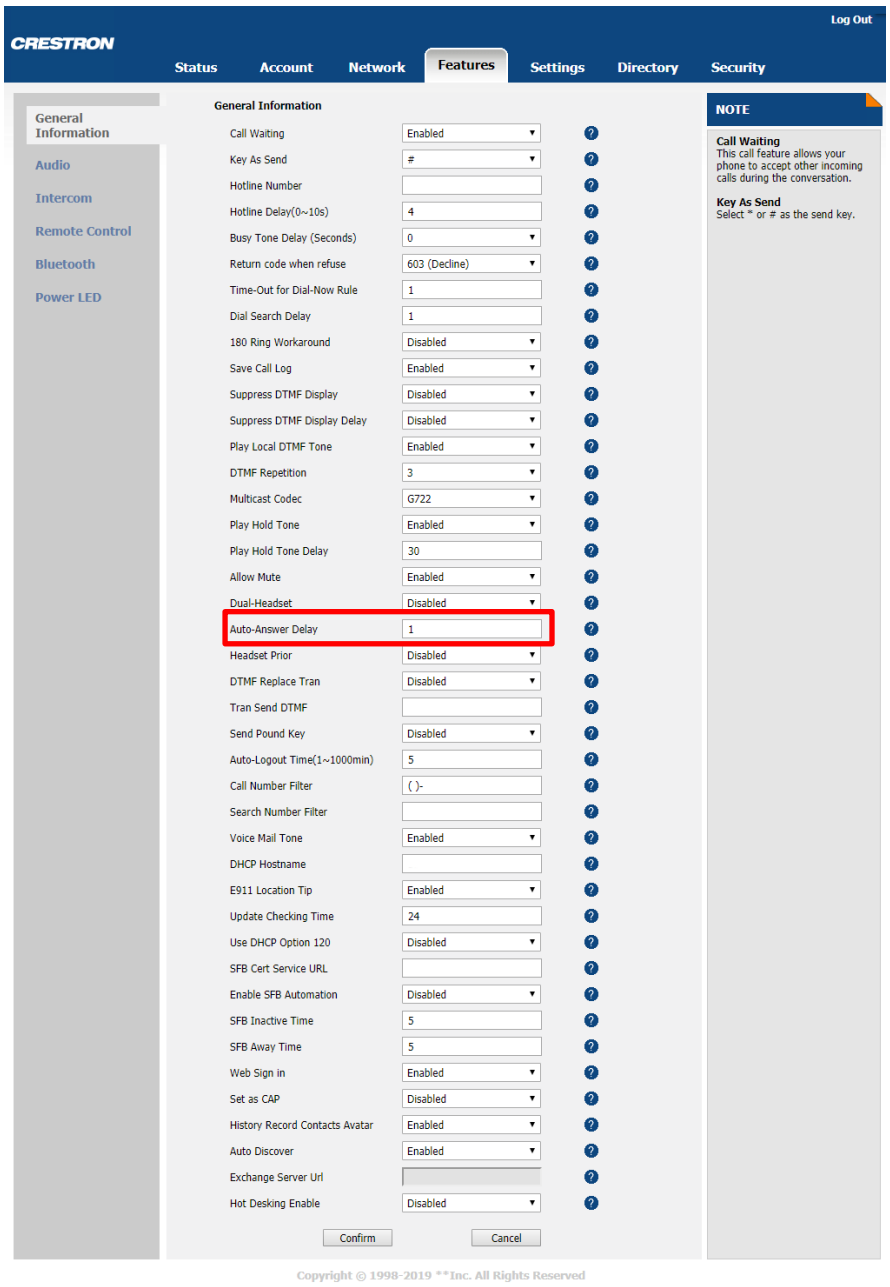


2. Select **Enabled** or **Disabled** from the **Auto Answer** drop-down list.
3. Click **Confirm** to accept the change.

Configure a Period of Delay Time for Auto Answer via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Enter the delay time (in seconds) in the **Auto-Answer Delay** field.
3. Click **Confirm** to accept the change.

Configure Auto Answer via the Phone User Interface

1. Tap > **Setting** > **Features** > **Auto Answer**.
2. In the **Account 1** setting, tap **On** to turn on the feature. Tap **Off** to turn off the feature.
3. Tap **Save**.

Busy Tone Delay

The Busy tone delay can be set for a period of time during which the busy tone is audible.

The Busy tone delay can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure busy tone delay. **Parameter:** features.busy_tone_delay
Local	Web User Interface	Configure busy tone delay. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

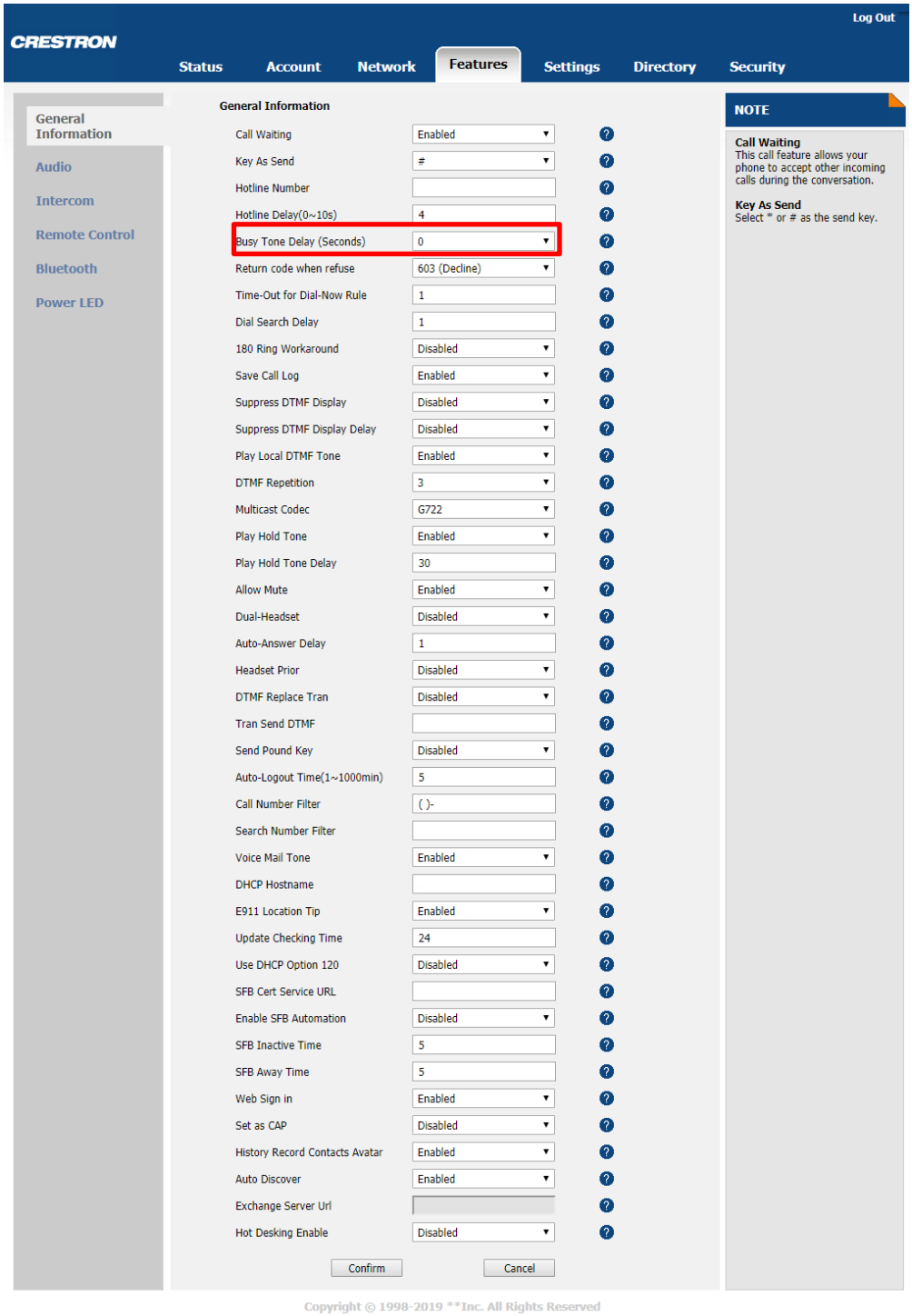
Details of the Configuration Parameter

Parameter	Permitted Values	Default
features.busy_tone_delay	**0, 3 or 5**	**0**
Description: Configures the duration (in seconds) for the busy tone. **0**- 0s, the phone will not play a busy tone. **3**- 3s, a busy tone plays for 3 seconds on the phone. **5**- 5s **Web User Interface:** Features > General Information > Busy Tone Delay (Seconds) **Phone User Interface:** None		

Configure Busy Tone Delay via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Select the delay time (in seconds) from the **Busy Tone Delay (Seconds)** drop-down list.

3. Click **Confirm** to accept the change.

Return Code When Refuse

Return code when refuse defines the return code and reason of the SIP response message for the refused call. The caller's phone LCD screen displays the reason according to the received return code. Available return codes and reasons are:

- 404 (Not Found)
- 480 (Temporarily Not Available)
- 486 (Busy Here)
- 603 (Decline)

Return code for refused call can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Specify the return code and the reason of the SIP response message when refusing a call. **Parameter:** features.normal_refuse_code
Local	Web User Interface	Specify the return code and the reason of the SIP response message when refusing a call. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

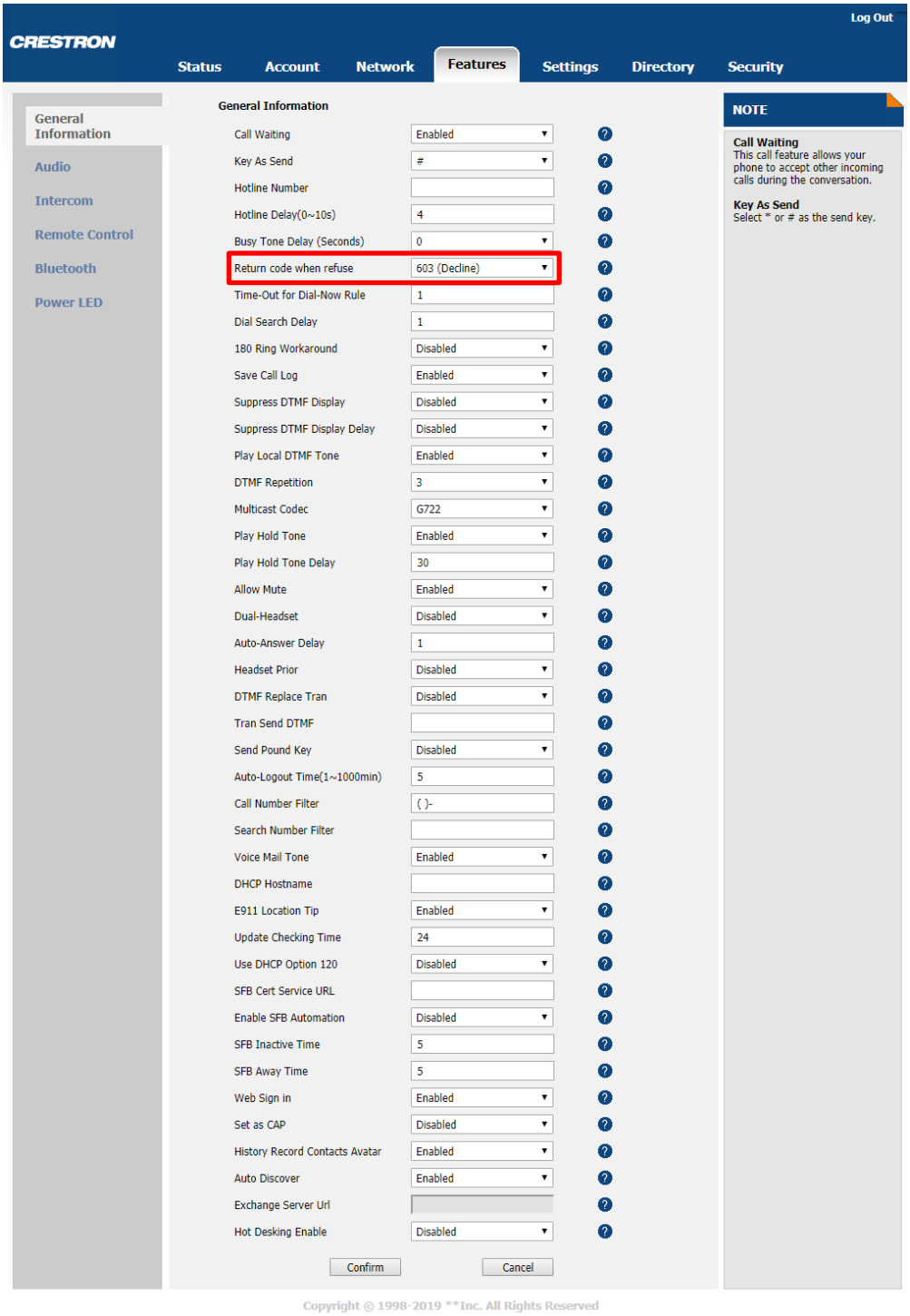
Details of the Configuration Parameter

Parameter	Permitted Values	Default
features.normal_refuse_code	**404, 480, 486 or 603**	**603**
Description: Configures a return code and reason of SIP response messages when the phone rejects an incoming call. A specific reason is displayed on the caller's phone LCD screen. **404-** Not Found **408-** Temporarily Not Available **486-** Busy Here, the caller's phone LCD screen will display the message "Busy Here" when the callee rejects the incoming call. **603-** Decline **Web User Interface:** Features > General Information > Return Code When Refuse **Phone User Interface:** None		

Specify the Return Code and the Reason When Refusing a Call via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Select the return code from the **Return Code When Refuse** drop-down list.

3. Click **Confirm** to accept the change.

Early Media

Early media refers to media (e.g., audio and video) played to the caller before a SIP call is actually established.

Current implementation supports early media through the 183 message. When the caller receives a 183 message with SDP before the call is established, a media channel is established. This channel is used to provide the early media stream for the caller.

180 Ring Workaround

180 ring workaround defines whether to deal with the 180 message received after the 183 message. When the caller receives a 183 message, it suppresses any local ringback tone and begins to play the media received. 180 ring workaround allows the phone to resume and play the local ringback tone upon a subsequent 180 message received.

180 ring workaround can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure 180 ring workaround. **Parameter:** phone_setting.is_deal180
Local	Web User Interface	Configure 180 ring workaround. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

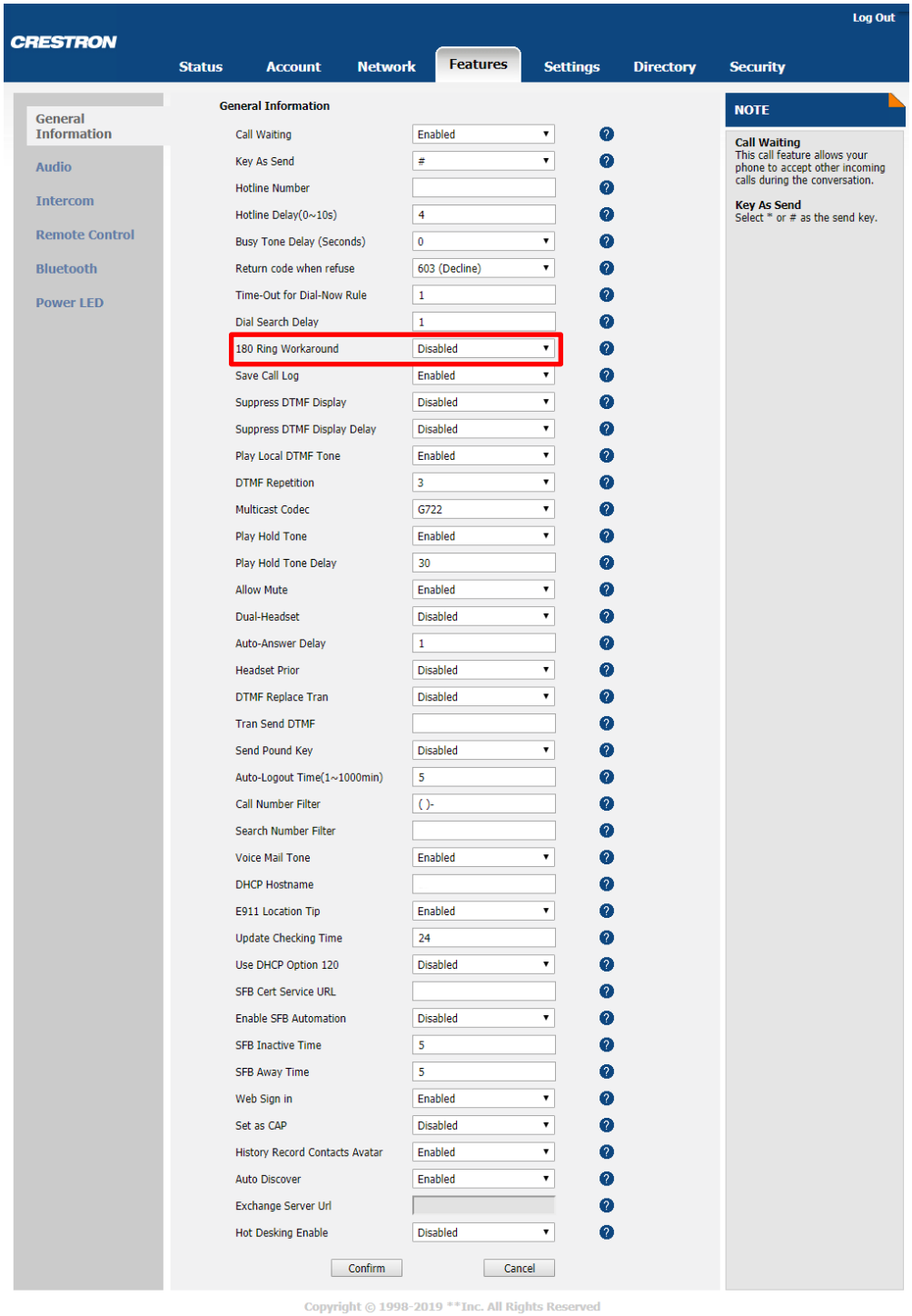
Details of the Configuration Parameter

Parameter	Permitted Values	Default
phone_setting.is_deal180	**0 or 1**	**0**
Description: Enables or disables the phone to deal with the 180 SIP message received after the 183 SIP message. **0**- Disabled **1**- Enabled, the phone will resume and play the local ringback tone upon a subsequent 180 message received. **Web User Interface:** Features > General Information > 180 Ring Workaround **Phone User Interface:** None		

Configure 180 Ring Workaround via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Select **Enabled** or **Disabled** from the **180 Ring Workaround** drop-down list.

3. Click **Confirm** to accept the change.

Incoming Call Display

Configure whether the phone preferentially shows the incoming call even when the phone is in use.

Incoming call focus can be configured using the configuration files only.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the Incoming call display. **Parameters:** phone_setting.incoming_call.priority phone_setting.incoming_call_when_dialing.priority

Details of the Configuration Parameters

Parameter	Permitted Values	Default
phone_setting.incoming_call.priority	**0 or 1**	**1**
Description: Enables or disables the phone to preferentially show incoming calls in any condition. **0**- Disabled, the phone shows the incoming call only after the phone returns to idle. **1**- Enabled **Web User Interface:** None **Phone User Interface:** None		
phone_setting.incoming_call_when_dialing.priority	**0 or 1**	**1**
Description: Enables or disables the phone to preferentially show incoming calls when the user is dialing a call. **0**- Disabled, the phone shows the incoming call after dialing a call. **1**- Enabled, the phone shows the incoming call even though the user is dialing a call. **Note:** This feature works only if the value of the parameter "phone_setting.incoming_call.priority" is set to 1 (Enabled). **Web User Interface:** None **Phone User Interface:** None		

Call Hold

Call hold is used to place an active call on hold. It enables a user to pause activity on an active call so that they can use the phone for another task (e.g., to place or receive another call).

When a call is placed on hold, the phones send an INVITE request with HOLD SDP to request remote parties to stop sending media and to inform them that they are being held. Skype for Business phones support two call hold methods, one is RFC 3264, which sets the "a" (media attribute) in the SDP to sendonly, recvonly or inactive (e.g., a=sendonly). The other is RFC 2543, which sets the "c" (connection addresses for the media streams) in the SDP to zero (e.g., c=0.0.0.0).

Call hold tone allows phones to play a warning tone at regular intervals when there is a call on hold. The warning tone is played through the speakerphone.

Call hold can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the call hold tone and call hold tone delay. **Parameters:** features.play_hold_tone.enable features.play_hold_tone.delay
Local	Web User Interface	Configure the call hold tone and call hold tone delay. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of the Configuration Parameters

Parameter	Permitted Values	Default
features.play_hold_tone.enable	**0 or 1**	**1**
Description: Enables or disables the phone to play a warning tone when there is a call on hold. **0**- Disabled **1**- Enabled **Web User Interface:** Features > General Information > Play Hold Tone **Phone User Interface:** None		

Parameter	Permitted Values	Default
features.play_hold_tone.delay	Integer from 3 to 3600	30

Description:

Configures the interval (in seconds) at which the phone plays a warning tone when there is a call on hold.

If it is set to 30 (30s), the phone will play a warning tone every 30 seconds when there is a call on hold.

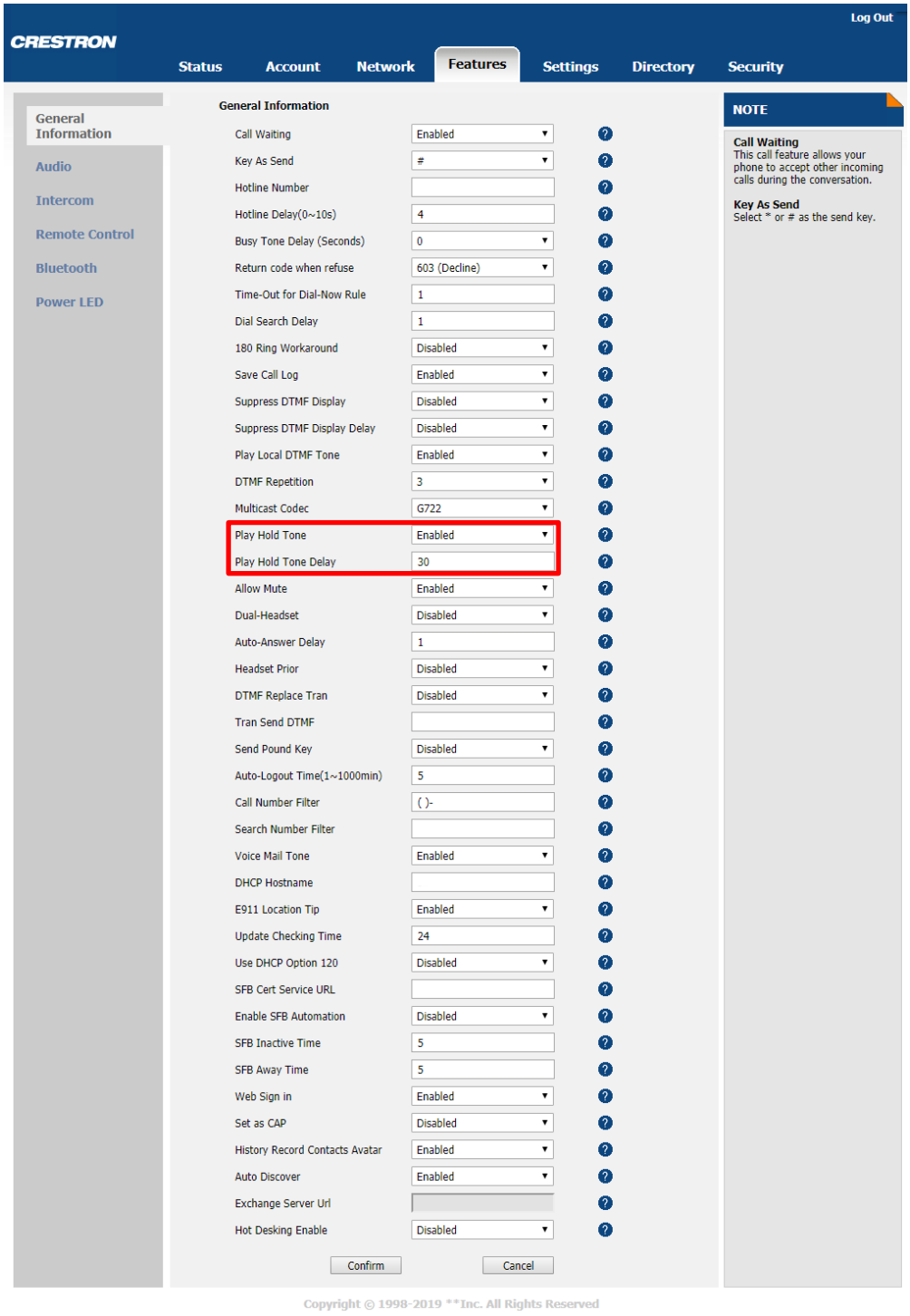
Note: This feature works only if the value of the parameter "features.play_hold_tone.enable" is set to 1 (Enabled).

Web User Interface:
Features > General Information > Play Hold Tone Delay

Phone User Interface:
None

Configure Call Hold Tone and Call Hold Tone Delay via the Web User Interface

1. Click **Features** > **General Information**.



2. Select **Enabled** or **Disabled** from the **Play Hold Tone** drop-down list.
3. Enter the delay time in the **Play Hold Tone Delay** field.

4. Click **Confirm** to accept the changes.

Music on Hold

Music on Hold (MoH) is the business practice of playing recorded music to fill the silence experienced by the party who has been placed on hold. When a call is placed on hold, the phone will play a ring tone to the held party.

Users can upload a custom music to the phone or use the music sent from the Skype for Business via In-band provisioning method.

The uploaded music format must meet the following:

Music File Format

Format	Single File Size	Duration
.wav	1~500K	1~30s

NOTE: The music file must be in PCMU/PCMA audio format, mono channel, 8K sample rate and 16 bit resolution.

Music on hold can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the music on hold feature. **Parameter:** sfb.music_on_hold.enable
		Configure the music on hold mode. **Parameter:** sfb.music_on_hold.mode
		Specify the access URL of the custom ring tone. **Parameter:** sfb.music_on_hold.url
		Delete the custom music files. **Parameter:** sfb.music_on_hold.delete
Local	Web User Interface	Configure the music on hold feature. Configure the music on hold mode. Specify the access URL of the custom ring tone. Delete the custom music files. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-moh&q=load

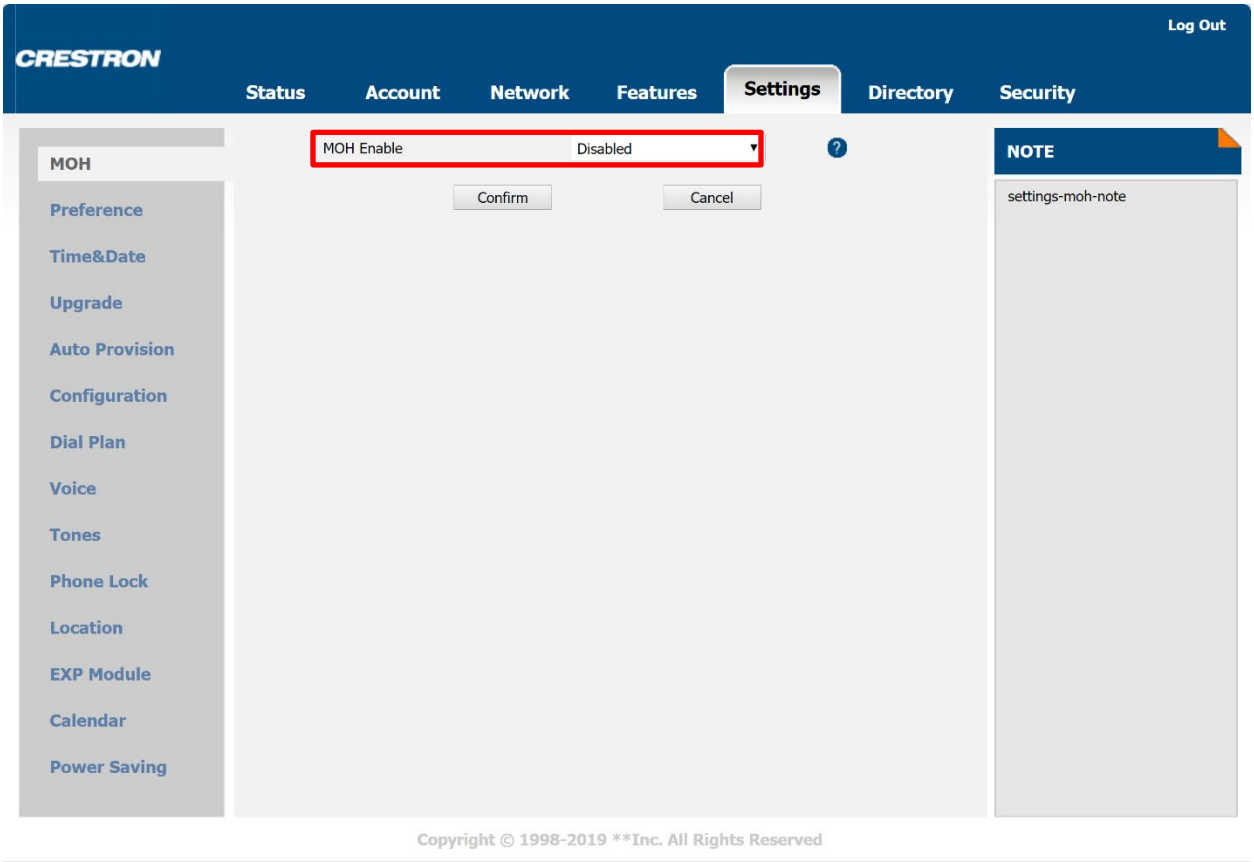
Details of the Configuration Parameters

Parameter	Permitted Values	Default
sfb.music_on_hold.enable	**0 or 1**	**0**
Description: Enables or disables the phone to play a music for the held party. **0**- Disabled **1**- Enabled **Web User Interface:** Settings > MOH > MOH Enable **Phone User Interface:** None		
sfb.music_on_hold.mode	**0 or 1**	**1**
Description: Configures the source of the music played for the held party. **0**- Inband Provision **1**- Local Custom **Web User Interface:** Settings > MOH > MOH Mode **Phone User Interface:** None		
sfb.music_on_hold.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom music file. **Example:** sfb.music_on_hold.url = tftp://192.168.1.100/Customring.wav **Web User Interface:** Settings > MOH > MOH File **Phone User Interface:** None		
sfb.music_on_hold.delete	**http://localhost/all**	**Blank**
Description: Delete all custom music files. **Example:** sfb.music_on_hold.delete = http://localhost/all **Web User Interface:** Settings > MOH > Delete **Phone User Interface:** None		

Configure Music on Hold via the Web User Interface

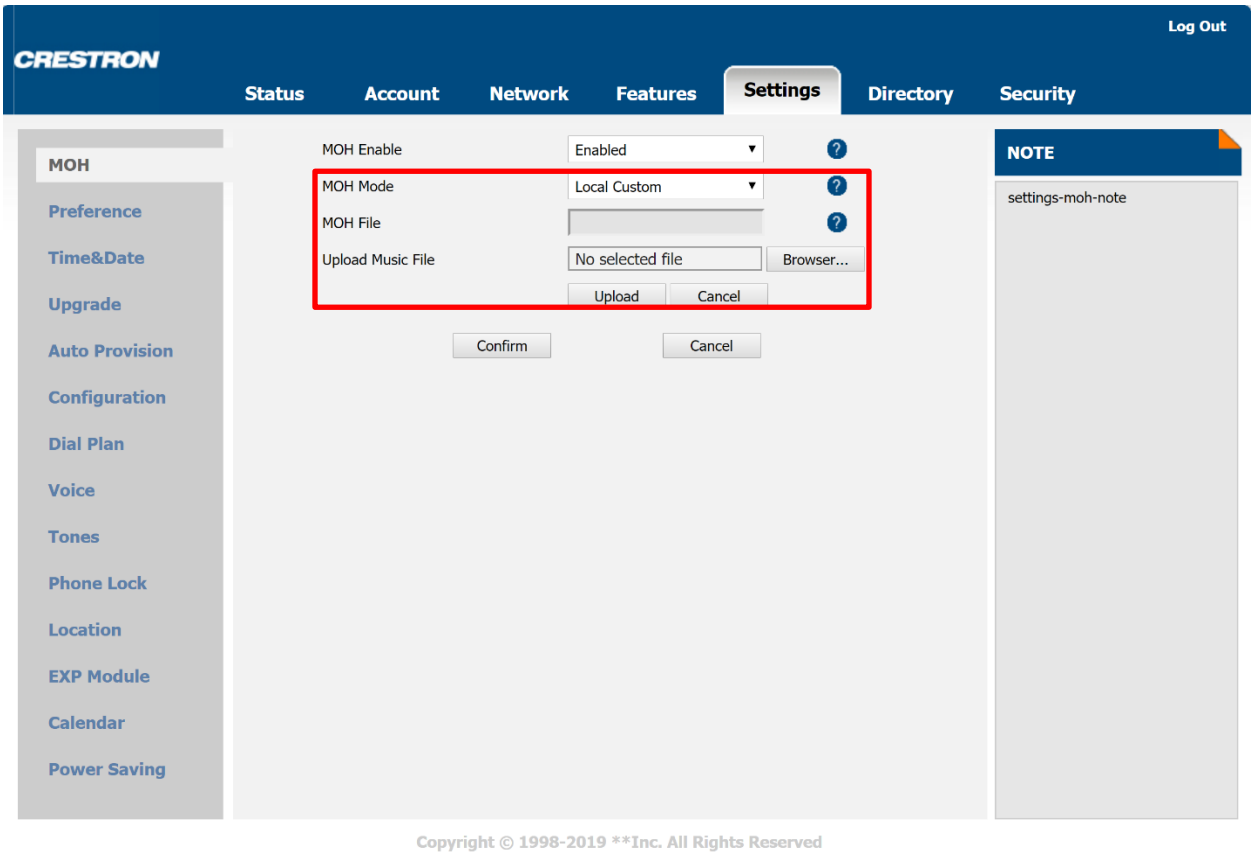
1. Click **Settings** > **MOH**.

Settings > MOH



2. Select **Enabled** from the **MOH Enable** drop-down list.

Settings > MOH



3. Select **Inband Provision** or **Local Custom** from the **MOH Mode** dropl-down list.
   - If **Inband Provision** is selected, the phone will play the music sent from the Skype for Business Server to the held party.
   - If **Local Custom** is selected, click **Browser** in the **Upload Music File** field to select a music file saved in the local computer, and then click **Upload** to upload the custom music. The held party will hear the custom music.
4. Click **Confirm** to accept the changes.

Call Forward

The phone provides a flexible call forwarding feature that enables a user to forward incoming calls to another destination. Skype for Business phones redirect an incoming INVITE message by responding with a 303 Moved See Other message, which contains a Contact header with a new URI.

Call forwarding has following types:

- **Forward Calls to a Contact:** Incoming calls are forwarded to a preset number or contact.

- **Simultaneously Ring to a Contact:** The preset number will ring simultaneously when a phone receives an incoming call.
- **Forward to Voice Mail:** Incoming calls are forwarded to voicemail.
- **Forward to Delegates:** If delegates are assigned to a line, all incoming calls can be forwarded directly to the delegates.
- **Simultaneously Ring to Delegates:** If delegates are assigned to a line, delegates' phones can be enabled to simultaneously ring when the user receive incoming calls.
- **Simultaneously Ring to Team Call:** If team-call group assigned to a user's line, team-call members' phones can be enabled to simultaneously ring when the user receives incoming calls. For more information on how to configure a team-call group, refer to "Set Up a Team-Call Group" on page 215.

Skype for Business phones support the redirected call information sent by the SIP server with Diversion header, per draft-levy-sip-diversion-08, or History-info header, per RFC 4244. The Diversion/History-info header is used to inform the phone of a call's history. For example, when a phone has been set to enable call forward, the Diversion/History-info header allows the receiving phone to indicate where the call was from, and from which phone number it was forwarded.

Call forward can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure diversion/history-info feature. **Parameter:** features.fwd_diversion_enable
Local	Phone User Interface	Configure call forward.

Details of the Configuration Parameter

Parameter	Permitted Values	Default
features.fwd_diversion_enable	**0 or 1**	**1**
Description: Enables or disables the phone to present the diversion information when an incoming call is forwarded to a phone. **0**- Disabled **1**- Enabled **Web User Interface:** Features->General Information->Diversion/History-Info **Phone User Interface:** None		

Enable Call Forward via the Phone User Interface

1. Tap **Setting** > **Features** > **Call Forward**.

2. Tap **On** to turn the feature on.
3. Tap the method for handling an incoming call.
   - **Forward Calls to a Contact:** Select the contact that will receive a forwarded call.
   - **Simultaneously Ring to a Contact:** Select the contact that will simultaneously receive the incoming call.
   - **Forward to Voicemail:** Direct incoming calls to voicemail.
4. Select the amount of time (in seconds) before a call is forwarded from the **Reject call delay(s)** drop-down list.

Team-Call Group

A team-call group is a team of people who can answer work calls. Members can be added or removed, and can can also be configured to determine when they can answer calls for a team member. Team-call group can be configured via Skype for Business client only.

As an example, there is a team of people working on the same project or tasks. If a user is away from their desk and their phone rings, anyone in the team-call group can answer the call for the absent member. As soon as any team member picks up the phone, the other phones stop ringing.

Set Up a Team-Call Group

Team-Call groups are set up with the Skype for Business client software.

Team-Call Ringtone

The team-call ring tone feature allows the phone to play a distinct ringtone when receiving a team-call.

Team-call ring tone can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure a ring tone for the team-call. **Parameter:** phone_setting.team_call_ring.enable phone_setting.team_call_ring_type
Local	Phone User Interface	Configure a ring tone for the team-call.

Details of the Configuration Parameters

Parameter	Permitted Values	Default
phone_setting.team_call_ring.enable	0 or 1	1
Description: Enables or disables the phone to play a distinct ringtone for team-call. **0**- Disabled, incoming calls to team-call group will use the phone's ring tone. The phone's ring tone is configured by the parameter "phone_setting.ring_type". **1**- Enabled, a distinct ringtone can be set for the team-call. **Web User Interface:** None **Phone User Interface:** None		
phone_setting.team_call_ring_type	Refer to the following content	Ring1.wav
Description: Configures a ring tone for the team-call. **Permitted Values:** Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav, Splash.wav or custom ring tone name (e.g., Customring.wav). **Example:** • **To configure a phone built-in ring tone (e.g., Ring1.wav):** phone_setting.team_call_ring_type = Ring1.wav • **To configure a custom ring tone (e.g., Customring.wav):** phone_setting.team_call_ring_type = Customring.wav **Web User Interface:** None **Phone User Interface:** Menu > Setting > Basic > Sounds > Ring Tones > Team Call		

Set a Ringtone for the Team-call via the Phone User Interface

1. Tap **Setting** > **Basic** > **Sounds** > **Ring Tones** > **Team Call**.
2. Tap a ring tone.
3. Tap **Save**.

Response Group

If a user signs into the phone using an On-Premises account, the Response Group feature can be used. However, the current Online environment does not support this feature.

A response group is a feature that routes and queues incoming calls to group numbers, called agents, such as to a help desk or a customer service desk.

When someone calls a response group, the call is routed to an agent based on a hunt group or the caller's answers to interactive voice response (IVR) questions. The Response Group application uses standard response group routing methods to route the call to the

next available agent. After a call agent accepts the call, other agents' phones stop ringing.

The routing methods for Response Group are as follows:

- LongestIdle – Calls are routed to the agent who has been idle (that is, not involved in a Skype for Business activity) for the longest period of time.
- RoundRobin – Calls are routed to the next available agent on the list.
- Serial – Calls are always routed to the first agent on the list, and are only routed to other agents if this person is not available or does not answer within the allotted time.
- Parallel – Calls are routed to all agents at the same time, except for agents whose presence status indicates that they are in a call or otherwise unavailable.
- Attendant – Calls are routed to all agents at the same time, even if the agent's presence status indicates that he or she is in a call or otherwise unavailable. The only exception occurs when an agent has set his or her presence to Do Not Disturb.

The default routing method is Parallel.

For information on creating a response group, refer to "Deployment process for Response Group in Skype for Business 2015" on Microsoft TechNet.

Response Group Ringtone

The Response Group Ringtone feature allows the phone to play a distinct ringtone when receiving a response group call.

Response Group Ringtone can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure a ringtone for the Response Group calls. **Parameters:** phone_setting.rsg_call_ring.enable phone_setting.rsg_call_ring_type
Local	**Phone User Interface**	Configure a ringtone for the Response Group calls.

Details of the Configuration Parameters

Parameter	Permitted Values	Default
phone_setting.rsg_call_ring.enable	0 or 1	1
Description: Enables or disables a distinct ringtone for Response Group calls. **0**- Disabled, incoming calls to Response Group will use the phone's ringtone. The phone's ringtone is configured by the parameter "phone_setting.ring_type". **1**- Enabled, a distinct ringtone can be set for Response Group calls. **Web User Interface:** None **Phone User Interface:** None		
phone_setting.rsg_call_ring_type	Refer to the following content	Ring1.wav
Description: Configures a ringtone for Response Group calls. **Permitted Values:** Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav, Splash.wav or custom ringtone name (e.g., Customring.wav). **Example:** • **To configure a phone built-in ringtone (e.g., Ring6.wav):** phone_setting.rsg_call_ring_type = Ring6.wav • **To configure a custom ringtone (e.g., Customring.wav):** phone_setting.rsg_call_ring_type = Customring.wav **Web User Interface:** None **Phone User Interface:** Menu > Setting > Basic > Sounds > Ring Tones > Response Group		

Set a Ringtone for the Response Group via the Phone User Interface

1. Tap **Setting** > **Basic** > **Sounds** > **Ring Tones** > **Response Group**.
2. Tap a ringtone.
3. Tap **Save**.

Call Queue

If a user signs into the phone using an Online account, the Call Queue feature can be used. The On-Premises environment does not support this feature.

A Call Queue is a feature that routes and queues incoming calls to group numbers, called agents, such as for a help desk or a customer service desk.

When someone calls a phone number that is set up with a Call Queue, they hear a greeting first (if any is set up), and then they will be put in the queue and wait for the available call agent. The person calling hears music while they are on hold, and the call in the queue will ring all call agents at the same time. After a call agent accepts the call, other agents' phones stop ringing.

For information on creating a Call Queue, refer to "Create an Office 365 Phone System Call Queue" on Microsoft TechNet.

Call Number Filter

The Call Number Filter feature allows the phone to automatically filter out particular characters when dialing a number.

The Call Number Filter can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the characters the phone filters out when dialing a number. **Parameters:** features.call_num_filter
Local	**Web User Interface**	Configure the characters the phone filters out when dialing a number. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of the Configuration Parameter

Parameter	Permitted Values	Default
features.call_num_filter	**String within 99 characters**	**()-**

Description:

Configures the characters the phone filters out when dialing a number.

If the dialed number contains the configured characters, the phone will automatically filter out those characters when dialing. But if the dialed SIP address contains the configured characters, the phone will not filter out those characters when dialing.

Example:
features.call_num_filter = .

If the user dials 3.61, the phone will filter out the character "."first, and then dial out 361.

If the user dials ralf.siebken@crestronsfb.com, the phone will not filter out the character "." in the SIP address.

Note: If it is left blank, the phone will not automatically filter out any characters when dialing a number. To filter just a space, set the value to " ," (a space followed by a comma).

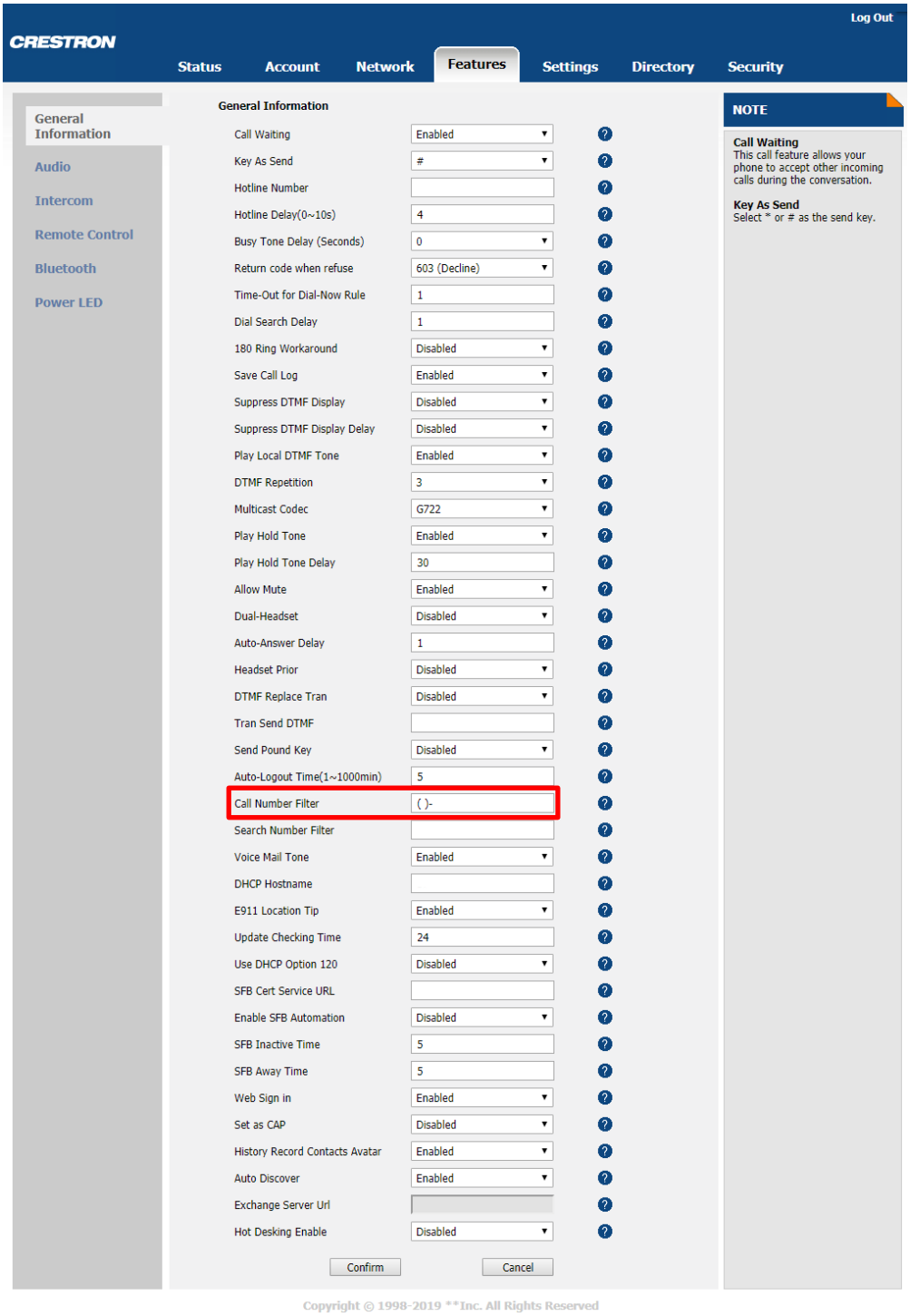
Web User Interface:
Features > General Information > Call Number Filter

Phone User Interface:
None

Configure the Characters Filtered by the Phone When Dialing via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Enter the filter character(s) in the **Call Number Filter** field.

3. Click **Confirm** to accept the change.

Search Number Filter

The Search Number Filter feature allows the phone to automatically filter out the particular characters when searching for contacts.

The Search Number filter can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the characters the phone filters out when searching for contacts. **Parameter:** features.search_num_filter
Local	Web User Interface	Configure the characters the phone filters out when searching for contacts. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

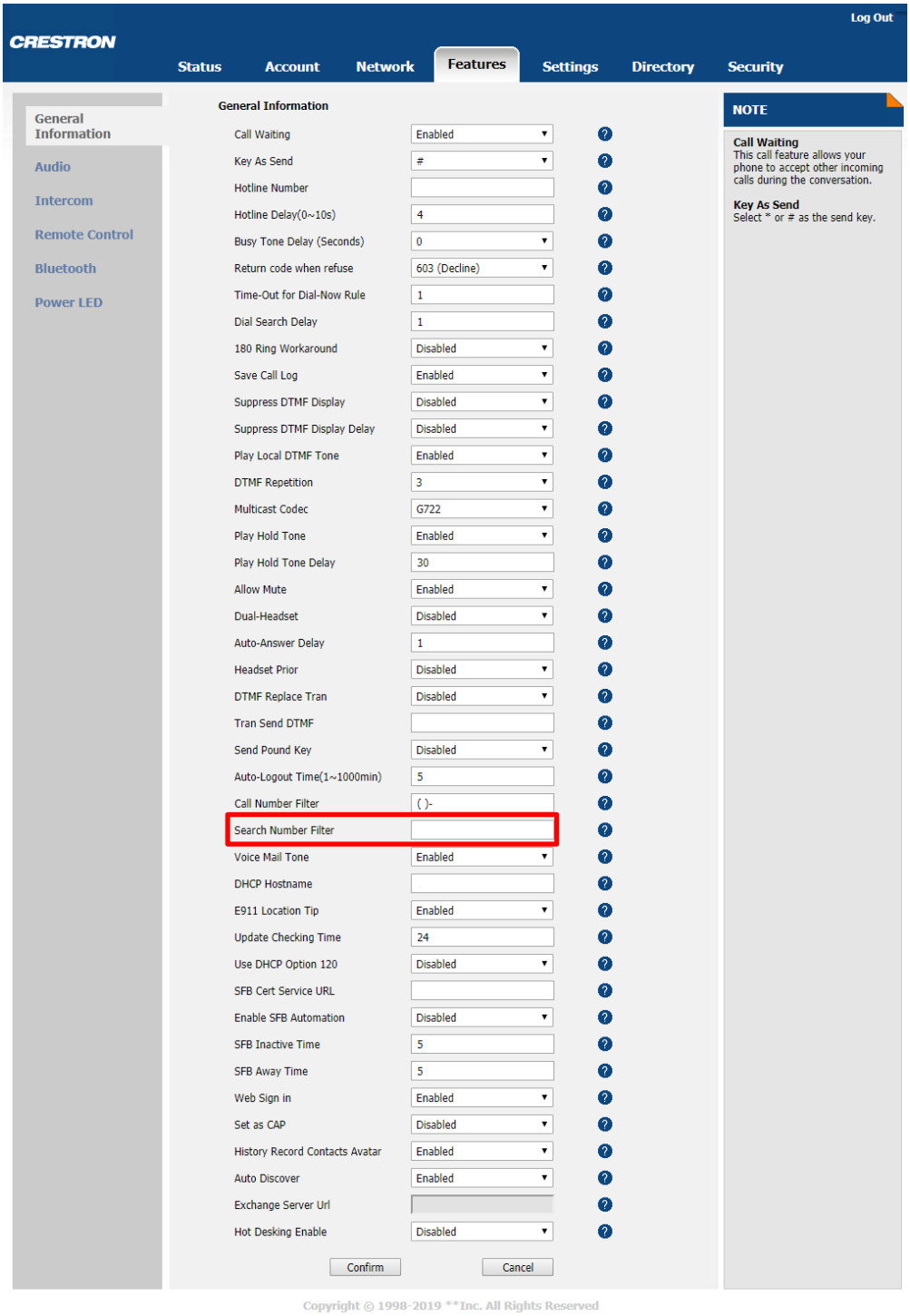
Details of the Configuration Parameter

Parameter	Permitted Values	Default
features.search_num_filter	**String within 255 characters**	**Blank**
Description: Configures the characters the phone filters out when searching for contacts. If the entered number contains configured characters, the phone will automatically filter out these characters when searching for contacts. **Example:** features.search_num_filter = - If a user enters 40-38, the phone will filter out the character -, and then search 4038. **Note**: If it is left blank, the phone will not automatically filter out any characters when searching for contacts. To filter out just a space, set the value to " ," (a space followed by a comma). **Web User Interface:** Features > General Information > Search Number Filter **Phone User Interface:** None		

Configure the Characters Filtered by the Phone When Searching for Contacts via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Enter the filter character(s) in the **Search Number Filter** field.

3. Click **Confirm** to accept the change.

Allow Mute

A user can mute the microphone of the active audio device during an active call, so that the other party cannot hear them. If the Allow Mute feature is disabled, an active call cannot be muted.

Allow Mute can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the Allow Mute feature. **Parameter:** features.allow_mute
Local	Web User Interface	Configure the Allow Mute feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

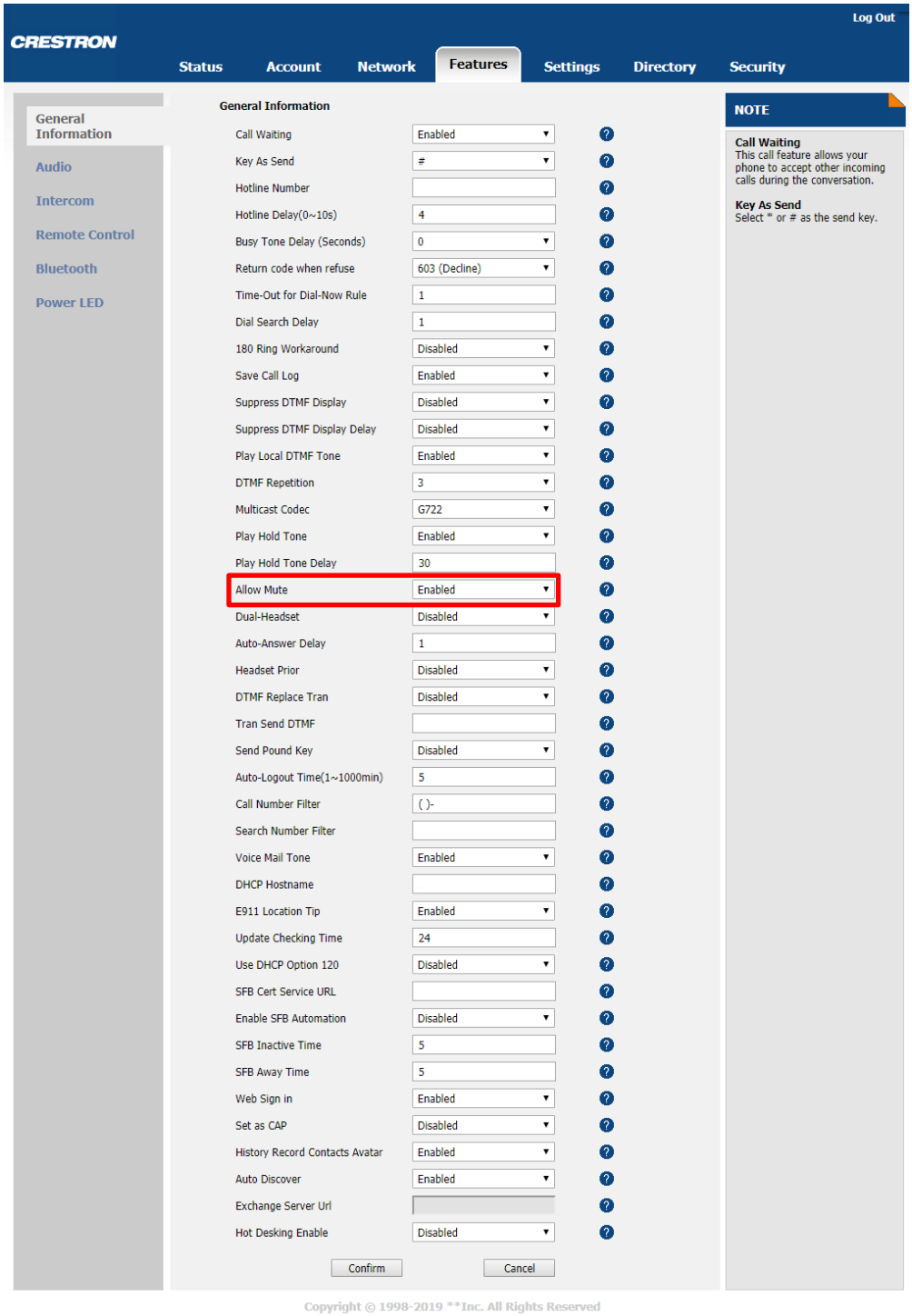
Details of the Configuration Parameter

Parameter	Permitted Values	Default
features.allow_mute	**0 or 1**	**1**
Description: Enables or disables muting on an active call. **0**- Disabled **1**- Enabled **Web User Interface:** Features > General Information > Allow Mute **Phone User Interface:** None		

Configure Allow Mute via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Select **Enabled** or **Disabled** from the **Allow Mute** drop-down list.

3. Click **Confirm** to accept the change.

Intercom

The Intercom feature allows establishing an audio conversation directly. The phone can answer intercom calls automatically.

Outgoing Intercom Calls

Intercom is a useful feature in office environments to quickly connect with an operator or secretary. Users can press an intercom key to view the intercom list, and then place an outgoing intercom call from the intercom list.

Outgoing intercom calls can be configured using the following methods.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the outgoing intercom calls feature. **Parameters:** features.intercom.enable features.intercom.outgoing intercom.x.label intercom.x.value
Local	Web User Interface	Configure the outgoing intercom calls feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-intercom&q=load
	Phone User Interface	Configure the outgoing intercom calls feature.

Details of the Configuration Parameters

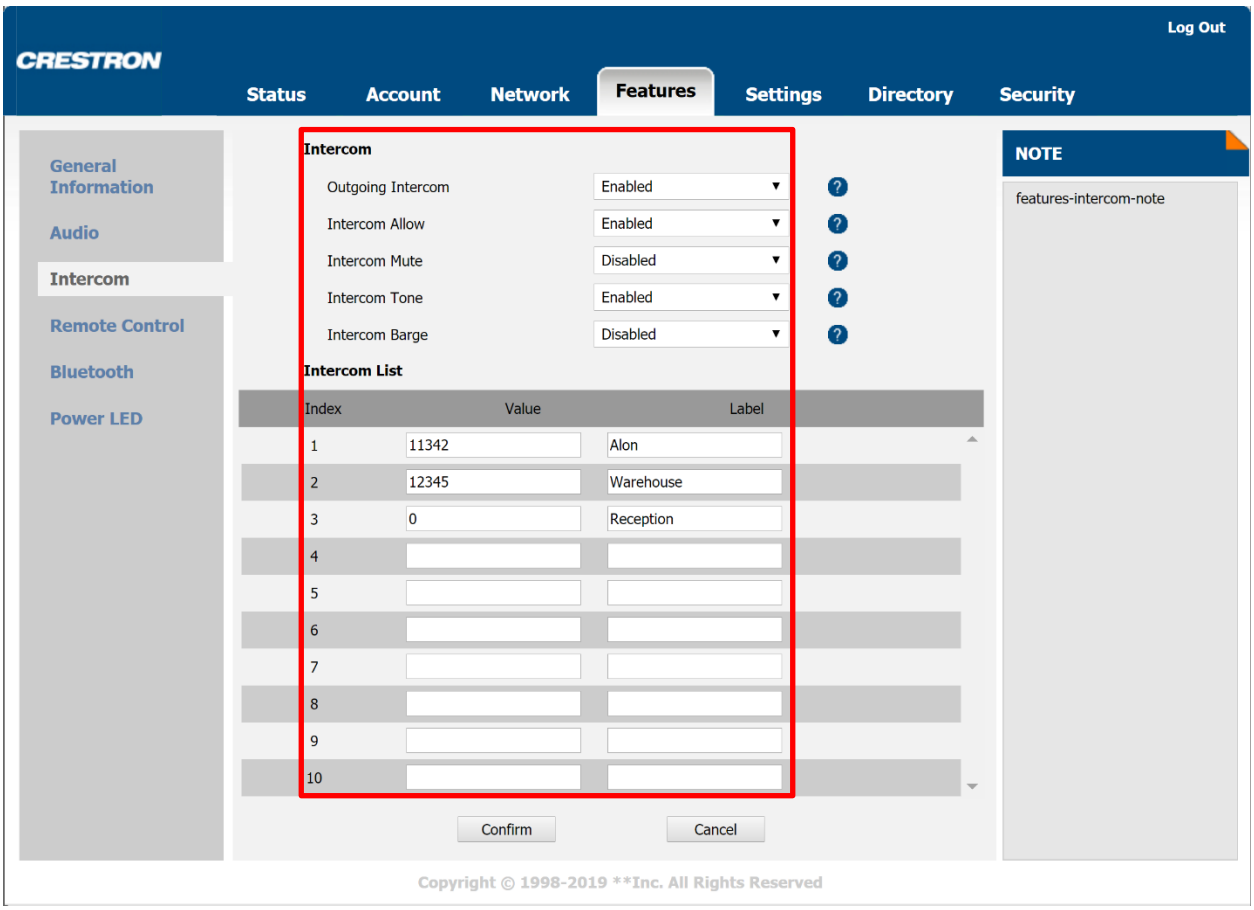
Parameter	Permitted Values	Default
features.intercom.enable	**0 or 1**	**1**
Description: Enables or disables the display of intercom configurations. **0**- Disabled **1**- Enabled. **Web User Interface:** None **Phone User Interface:** None		

Parameter	Permitted Values	Default
features.intercom.outgoing	0 or 1	0
Description: Enables or disables placement of an outgoing intercom call from the intercom list. **0**- Disabled **1**- Enabled **Web User Interface:** Features > Intercom > Outgoing Intercom **Phone User Interface:** Menu > Setting > Features > Intercom > Outgoing Intercom		
intercom.x.label (x ranges from 1 to 10)	String	Blank
Description: (Optional.) Configures the label displayed on the intercom list. **Note:** This feature works only if the values of parameters "features.intercom.enable" and "features.intercom.outgoing" are set to 1 (Enabled). **Example:** intercom.1.label = Test **Web User Interface:** Features > Intercom > Label **Phone User Interface:** Menu > Setting > Features > Intercom List > Option > Edit > Label		
intercom.x.value (x ranges from 1 to 10)	String	Blank
Description: Configures the intercom number displayed on the intercom list. **Note:** This feature works only if the values of parameters "features.intercom.enable" and "features.intercom.outgoing" are set to 1 (Enabled). **Example:** intercom.1.value = 4038 **Web User Interface:** Features > Intercom > Value **Phone User Interface:** Menu > Setting > Features > Intercom List > Option > Edit > Value		

Configure Outgoing Intercom Calls via the Web User Interface

1. Click **Features** > **Intercom**.

Features > Intercom



2. Select **Enabled** from the **Outgoing Intercom** drop-down list.
3. (Optional.) Enter the string that will appear on the intercom list in the **Label** field.
4. Enter the target extension number in the **Value** field.
5. Repeat steps 3 and 4 to add more target extension numbers.
6. Click **Confirm** to accept the changes.

Configure Outgoing Intercom Calls via the Phone User Interface

1. Tap **Setting** > **Features** > **Intercom**.
2. In the **Outgoing Intercom** setting, tap **On** to turn on the feature. Tap **Off** to turn off the feature.
3. Tap **Save**.

Configure Target Extension Number via the Phone User Interface

1. Do one of the following to enter the intercom list:
   - Tap **Intercom**.
   - Tap **Setting** > **Features** > **Intercom List**.
2. Tap the right side of an intercom entry, and then tap **Edit**.
3. Enter a label and value in the **Label** and **Value** fields.
4. Tap **Save**.
5. Repeat steps 2 to 5 to add more target extension numbers.

Incoming Intercom Calls

The phone can process incoming calls differently depending on settings. There are four configuration options for incoming intercom calls:

- **Intercom Allow:** Intercom Allow allows the phone to answer an incoming intercom call. If this feature is disabled, the phone will handle an incoming intercom call like a normal incoming call.
- **Intercom Mute:** Intercom Mute allows the phone to mute the microphone for incoming intercom calls.
- **Intercom Tone:** Intercom Tone allows the phone to play a warning tone before answering an intercom call.
- **Intercom Barge:** Intercom Barge allows the phone to automatically answer an incoming intercom call even when an active call is in progress. The active call will be placed on hold. If this feature is disabled, the phone will handle an incoming intercom call like a normal incoming call while there is already an active call on the phone.

Incoming intercom calls can be configured using the following methods.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the incoming intercom call feature. **Parameters:** features.intercom.allow features.intercom.mute features.intercom.tone features.intercom.barge
Local	Web User Interface	Configure the incoming intercom call feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-intercom&q=load
	Phone User Interface	Configure the incoming intercom call feature.

Details of the Configuration Parameters

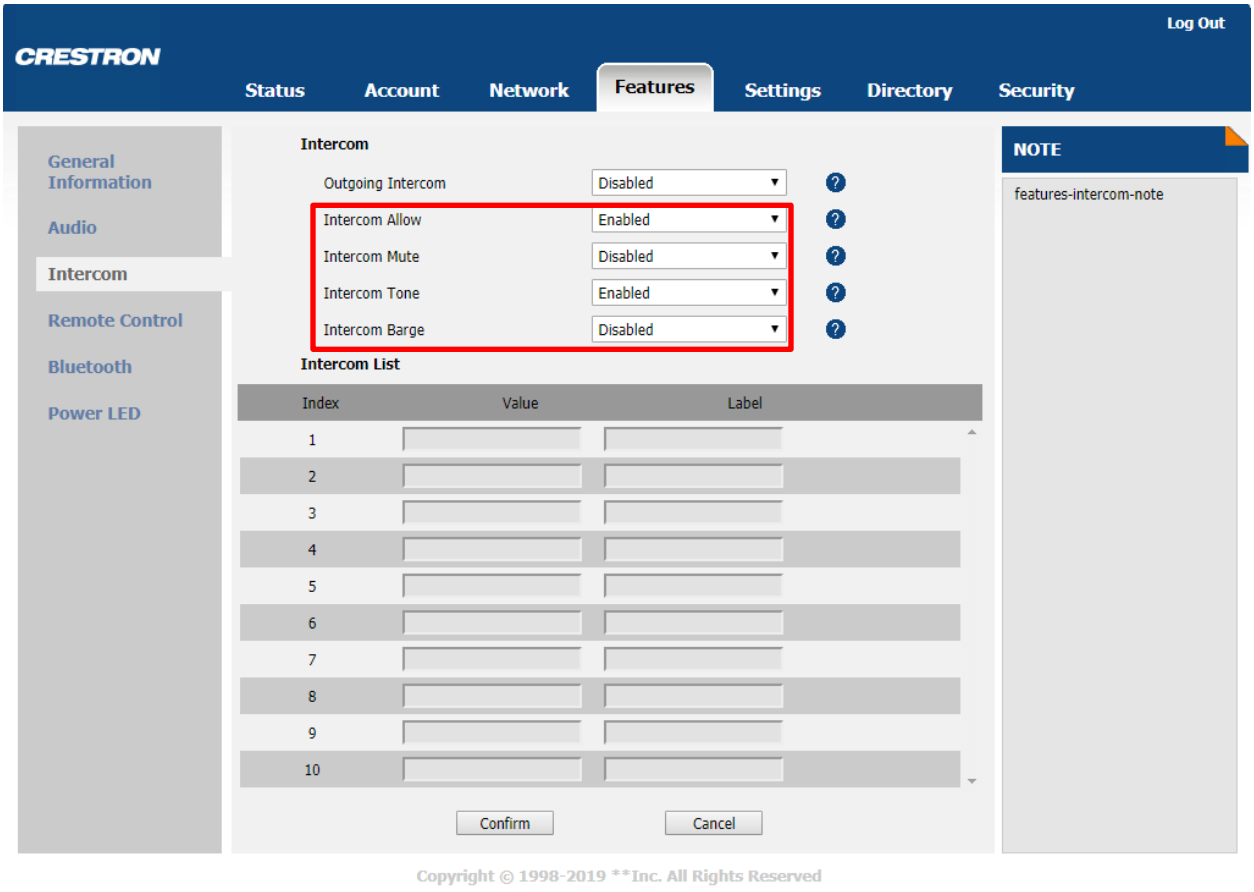
Parameter	Permitted Values	Default
features.intercom.allow	**0 or 1**	**1**
Description: Enables or disables answering an incoming intercom call. **0**- Disabled, the phone will handle an incoming intercom call like a normal incoming call. **1**- Enabled, the phone will automatically answer an incoming intercom call. **Web User Interface:** Features > Intercom > Intercom Allow **Phone User Interface:** Menu > Setting > Features > Intercom > Intercom Allow		
features.intercom.mute	**0 or 1**	**0**
Description: Enables or disables muting the microphone when answering an intercom call. **0**- Disabled **1**- Enabled, the microphone is muted for intercom calls, and then the other party cannot hear the user. **Note:** This feature works only if the value of the parameter "features.intercom.allow" is set to 1 (Enabled). **Web User Interface:** Features > Intercom > Intercom Mute **Phone User Interface:** Menu > Setting > Features > Intercom > Intercom Mute		

Parameter	Permitted Values	Default
features.intercom.tone	0 or 1	1
Description: Enables or disables playing a warning tone when answering an intercom call. **0**- Disabled **1**- Enabled **Note:** This feature works only if the value of the parameter "features.intercom.allow" is set to 1 (Enabled). **Web User Interface:** Features > Intercom > Intercom Tone **Phone User Interface:** Menu > Setting > Features > Intercom > Intercom Tone		
features.intercom.barge	0 or 1	0
Description: Enables or disables answering an incoming intercom call while there is already an active call on the phone. **0**- Disabled, the phone will handle an incoming intercom call like a normal incoming call while there is already an active call on the phone. **1**- Enabled, the phone will automatically answer the intercom call while there is already an active call on the phone and place the active call on hold. **Note:** This feature works only if the values of parameters "features.intercom.allow" and "call_waiting.enable" are set to 1 (Enabled). **Web User Interface:** Features > Intercom > Intercom Barge **Phone User Interface:** Menu > Setting > Features > Intercom > Intercom Barge		

Configure Incoming Intercom via the Web User Interface

1. Click **Features** > **Intercom**.

Features > Intercom



2. Select **Enabled** or **Disabled** from the **Intercom Allow**, **Intercom Mute**, **Intercom Tone** and **Intercom Barge** drop-down lists.
3. Click **Confirm** to accept the changes.

Configure Incoming Intercom via the Phone User Interface

1. Tap **Setting** > **Features** > **Intercom**.
2. Tap **On** or **Off** from the **Intercom Allow**, **Intercom Mute**, **Intercom Tone**, and **Intercom Barge** fields
3. Tap **Save**.

Calendar

Skype for Business phones integrate with the Microsoft Exchange calendar feature. If a phone is configured to connect to the Microsoft Exchange Server, and Microsoft® Outlook® is installed on site, a user can view Skype conferences, appointments, meetings and events, or join the Skype conference from their phone.

To use the calendar feature on a phone, the user must sign into the phone using User Sign-In or Web Sign-in method so the phone can display the Microsoft Exchange calendar.

Calendar can be configured using the configuration files only.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the calendar feature. **Parameter:** sfb.calendar.enable
		Configure the meeting reminder. **Parameter:** phone_setting.calendar_reminder
		Configure the interval of meeting reminder. **Parameter:** phone_setting.calendar_reminder.interval
		Configures the interval (in seconds) for the phone to automatically check if any calendars update available on Microsoft Exchange Server. **Parameter:** phone_setting.calendar.update_time

Details of the Configuration Parameters

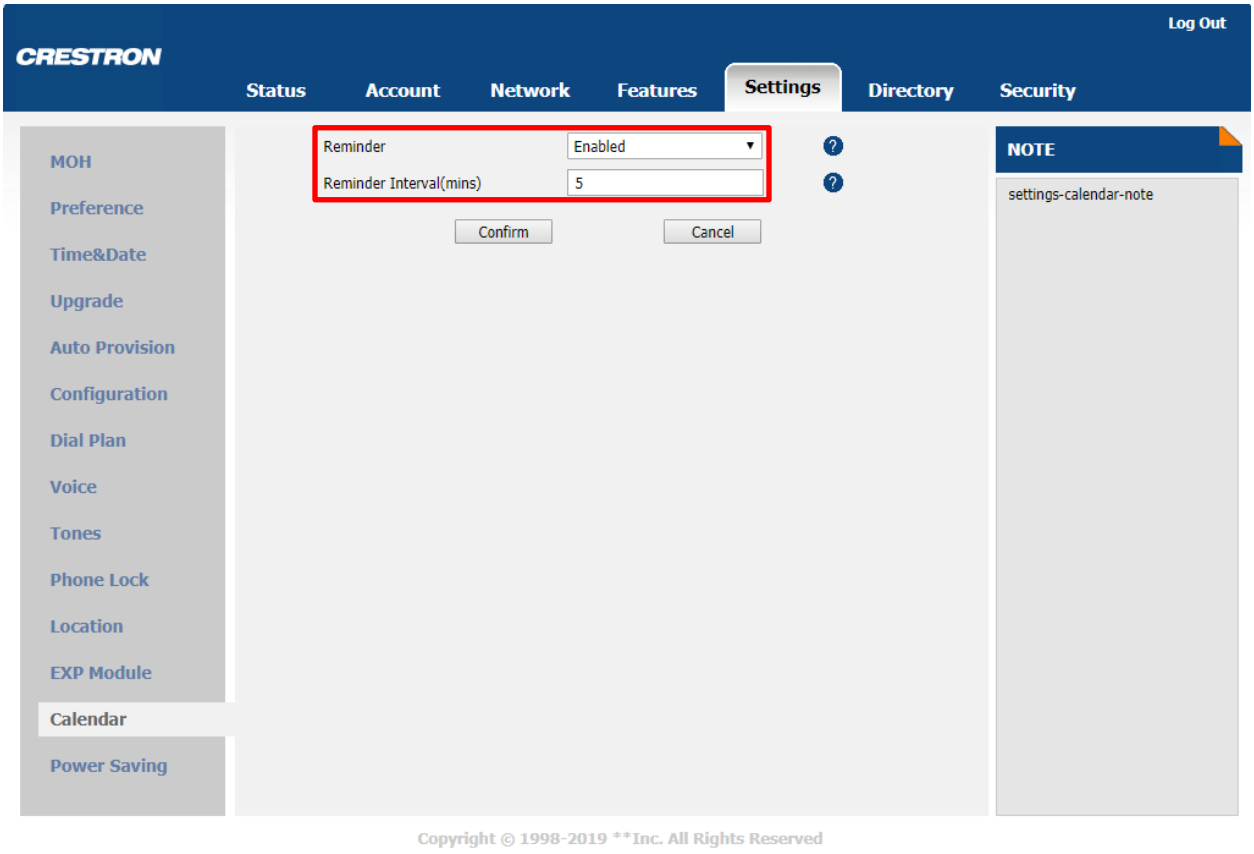
Parameter	Permitted Values	Default
sfb.calendar.enable	**0 or 1**	**1**
Description: Enables or disables the calendar feature. **0**- Disabled **1**- Enabled **Web User Interface:** None **Phone User Interface:** None		
phone_setting.calendar_reminder	**0 or 1**	**1**
Description: Enables or disables the meeting reminder. **0**- Disabled, the phone will not display reminders for any meeting. **1**- Enabled, the phone will display reminders for all meetings. **Web User Interface:** Settings > Calendar > Reminder **Phone User Interface:** Menu > Setting > Basic > Calendar Settings > Reminder		

Parameter	Permitted Values	Default
phone_settingcalendar_reminder.interval	Integer from 1 to 15	5
Description: Configures the interval (in minutes) for the phone to display the next meeting reminder after the reminder is temporarily removed. **Note:** This feature works only if the value of the parameter "phone_setting.calendar_reminder" is set to 1 (Enabled). **Web User Interface:** Settings > Calendar > Reminder Interval(mins) **Phone User Interface:** Menu > Setting > Basic > Calendar Settings > Reminder Interval		
phone_setting.calendar.update_time	Integer from 0 to 1000	300
Description: Configures the interval (in seconds) for the phone to automatically check if any calendar updates are available on Microsoft Exchange Server. If it is set to 300 (in seconds), the phone will check every 300 seconds to see if any calendar updates are available on the Microsoft Exchange Server. If an update is available, the phone will update the calendar. **Web User Interface:** None **Phone User Interface:** None		

Configure the Reminder via the Web User Interface

1. Click **Settings** > **Calendar**.

Settings > Calendar



2. Select **Enabled** from the **Reminder** drop-down list.
3. (Optional) Enter the reminder interval time (in minutes) in the **Reminder Interval(mins)** field.
4. Click **Confirm** to accept the changes.

Configure the Reminder via the Phone User Interface:

1. Tap **Setting** > **Basic** > **Calendar Settings**.
2. Select **Enabled** from the **Reminder** drop-down list.
3. Enter the reminder interval in the Reminder Interval(mins) field.
4. Tap **Save**.

View the Calendar

A user can view all schedules via the calendar on their phone. To view the calendar via phone user interface:

1. Tap **Menu** > **Calendar**. The calendar displays the day's schedule by default.
2. Tap **Back** to return to the previous screen.

Work with Schedule Reminders

If a user has an event scheduled, a reminder pop-up is displayed 15 minutes before it starts. The reminder shows the main information of the schedule, including subject, start time, end time and the rest time.

- Tap **Ignore** to permanently remove the reminder from the screen and stop all future reminders for the Skype conference.
- Tap **Snooze** to temporarily remove the reminder from the screen, until the next schedule reminder pops up. The reminder will appear every 5 minutes by default and also appear 1 minute before the schedule starts.
- Tap **Detail** to view specific information about the Skype conference, including the Skype conference's subject, participants, organizer, start and end time, location and content.
- If the user receives a Skype conference, tap **Join** to join the Skype conference.

NOTE: Tap ⊗ to ignore all reminders.

When the user receives a Skype conference reminder during a call, tap **Join** to join the Skype conference directly. The current call will be held and can be resumed after the Skype conference.

Configuring Advanced Settings

E911

E911 (Enhanced 911) is a location technology that enables the called party to identify the geographical location of the calling party. For example, if a caller makes an emergency call to E911, the feature extracts the caller's information so the police department can immediately identify the caller's location. For more information, refer to https://technet.microsoft.com/en- us/library/dn951423.aspx.

The system administrator can configure multiple emergency numbers via Skype for Business Server.

The phone sends the following attributes to the Location Information Server to get the location information:

- MAC address
- IP address

- Subnet
- SIP URI
- Chassis ID / Port ID of L2 switch (This information is obtained using LLDP)

During in-band provisioning, the following have been sent from the Frontend server to the phone.

- LIS URI
- Enhanced Emergency Enabled
- Location Required
- Emergency Dial String
- Emergency Dial String Mask
- Secondary Location Source
- Notify URI
- Conf URI
- Conf Mode

Sample

```
ms-subnet: 192.168.1.0.
<provisionGroup name="locationPolicy" >
<propertyEntryList >
<property name="EnhancedEmergencyServicesEnabled"
>true</property>
<property name="LocationPolicyTagID" >user-tagid</property>
<property name="LocationRequired" >yes</property>
<property name="UseLocationForE911Only" >true</property>
<property name="EmergencyDialString" >910086</property>
<property name="EmergencyDialMask" >911;912</property>
<property
name="NotificationUri"
>sip:7000@crestronuc.com,sip:80040@crestronuc.com</property>
<property name="ConferenceMode" >oneway</property>
```

When a user dials an emergency number, the location of the user and the phone number are sent out as a part of the INVITE message.

Sample

```
INVITE sip:+119@bor-ee.com;user=phone SIP/2.0
<location-info>
        <civicAddress xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
            <PC>361008</PC>
            <country>CN</country>
            <STS />
            <PRD />
            <HNS />
            <POD />
            <HNO />
            <RD>Wanghailu</RD>
            <A3>Xiamen</A3>
            <A1>Fujian</A1>
            <NAM />
            <LOC>63</LOC>
        </civicAddress>
    </location-info>
```

NOTE: If user's presence status is Do Not Disturb (**DND**) before dialing an emergency number, it will reset to **Available** from **DND** when an E911 number is dialed.

The E911 location tip provides geographical information. The network administrator configures user geographical location on the Skype for Business Server. After the user signs in, the geographical location is downloaded via in-band provisioning.

If geographical location is not provisioned by the server and the **LocationRequired** property of in-band LocationPolicy is set to **YES** or **DISCLAIMER** on the Skype for Business Server, a popup opens in the phone's LCD enabling the user to either ignore the notification or edit the location information.

E911 location tip can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the E911 location tip. **Parameters:** sfb.E911_location_tip
Local	Web User Interface	Configure the E911 location tip. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of the Configuration Parameter

Parameter	Permitted Values	Default
sfb.E911_location_tip	0 or 1	1

Description:

Enables or disables the idle screen to display the notification "Location is not set" when the location of the phone is not set.

0- Disabled

1- Enabled

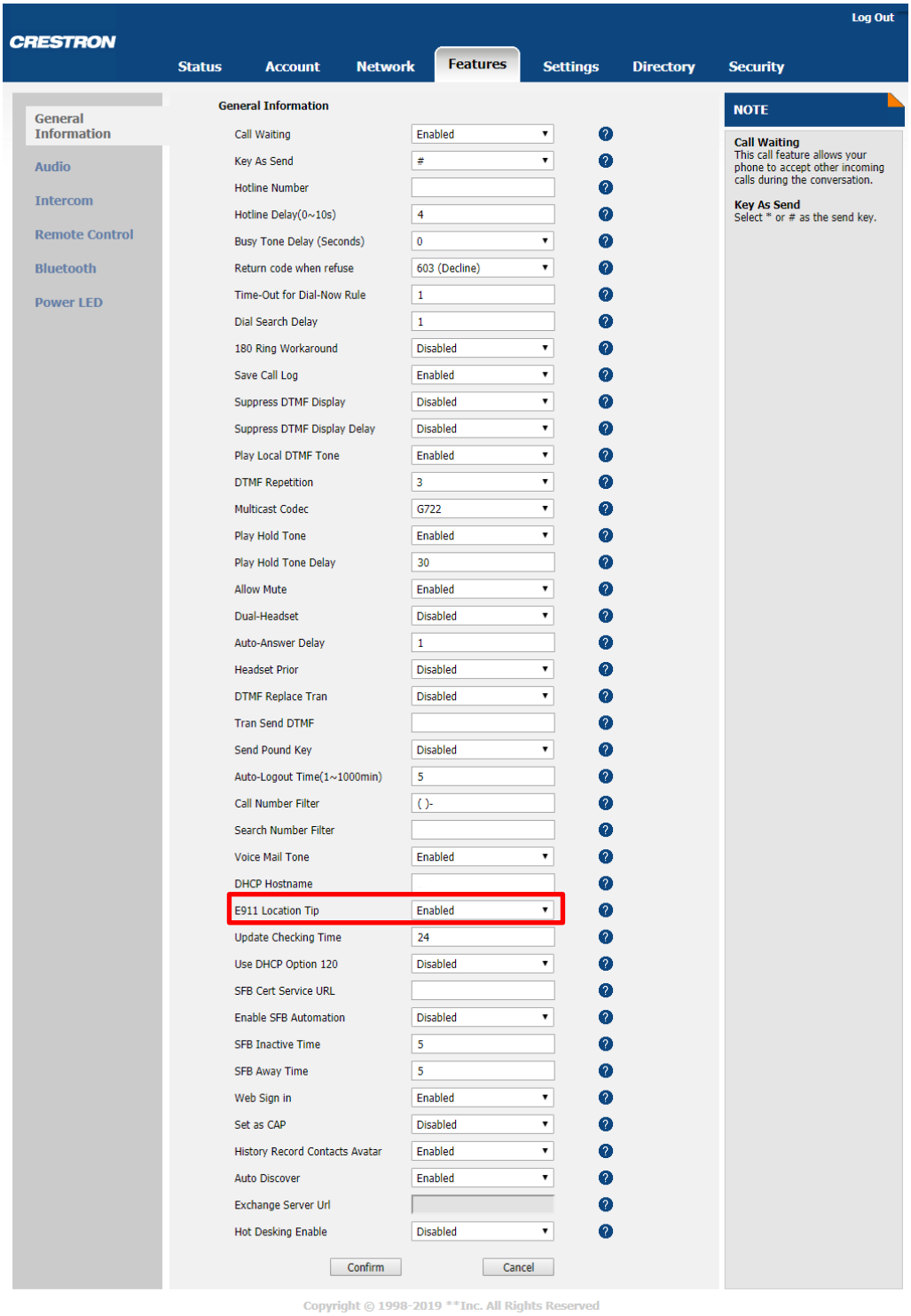
Web User Interface:
Features > General Information > E911 Location Tip

Phone User Interface:
None

Configure the E911 Location Tip via the Web User Interface

1. Click **Features** > **General Information.**

Features > General Information



2. Select **Enabled** or **Disabled** from the **E911 Location Tip** drop-down list.

3. Click **Confirm** to accept the change.

Add the Location Information

If the location is not set on the Skype for Business Server, the user can add the location information manually via the web user interface or the phone user interface.

Location information can be configured via web or phone user interface.

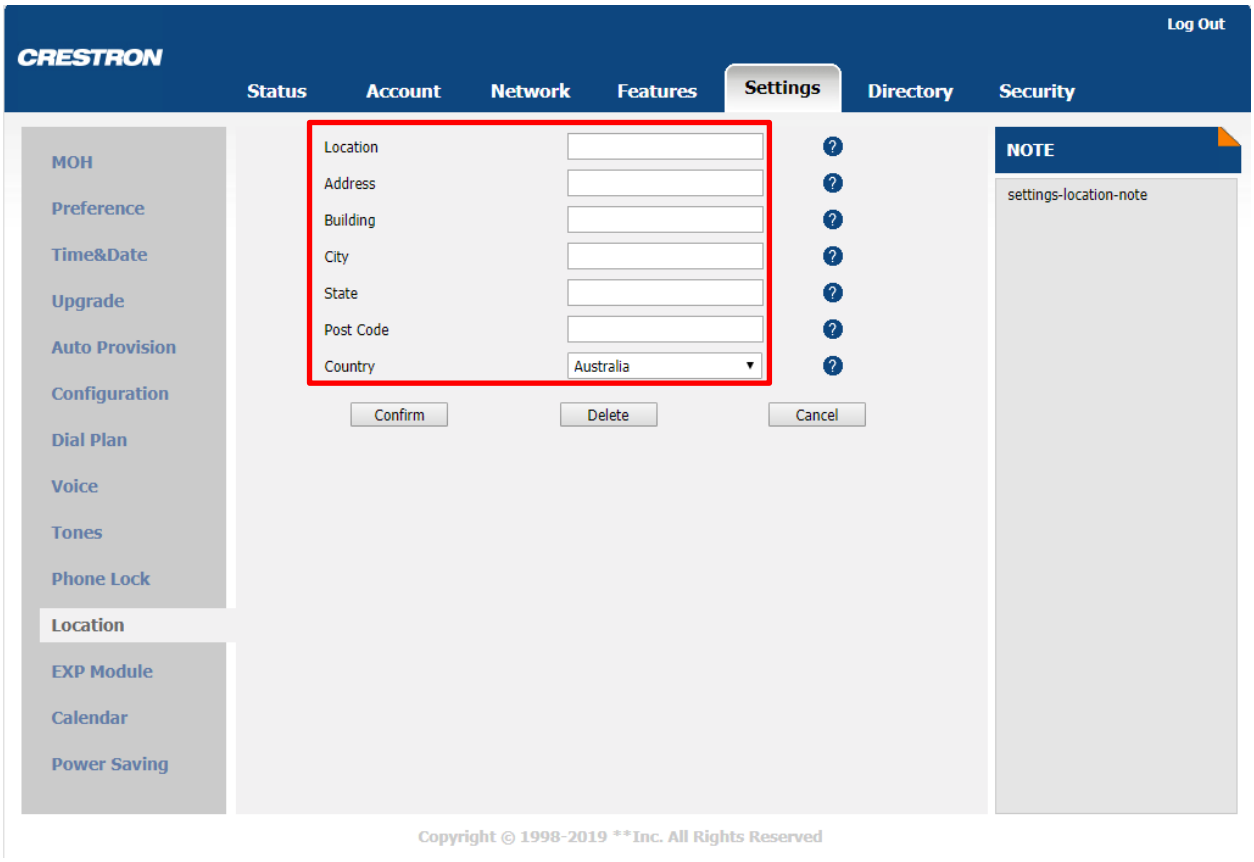
Configuration Methods

Local	Web User Interface	Configure location information. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-location&q=load
	Phone User Interface	Configure location information.

Add Location Information Manually via the Web User Interface

1. Click **Settings** > **Location**.

Settings > Location



2. Enter the location name in the **Location** field.

3. Enter the address in the **Address** field.
4. Enter the building name in the **Building** field.
5. Enter the city in the **City** field.
6. Enter the state in the **State** field.
7. Enter the post code in the **Post Code** field.
8. Select the country from the **Country** drop-down list.
9. Click **Confirm** to accept the changes.

Add Location Information Manually via the Phone User Interface

1. Tap **Setting** > **Basic** > **Location**.
2. Enter the location name in the **Set Location** field.
3. Enter the address in the **Set Address** field.
4. Enter the building name in the **Set Building** field.
5. Enter the city in the **Set City** field.
6. Enter the state in the **Set State** field.
7. Enter the post code in the **Set Postcode** field.
8. Select a country from the **Set Country** drop-down list.
9. Tap **Save**.

Multicast Paging

Multicast paging allows the phone to send/receive Real-time Transport Protocol (RTP) streams to/from the pre-configured multicast address(es) without involving SIP signaling. Up to 10 listening multicast addresses can be specified on the phone.

Send an RTP Stream

Send an RTP stream without involving SIP signaling by pressing a Paging soft key. A multicast address (IP: Port) should be assigned to the multicast paging key, which is configured to transmit an RTP stream to a group of designated phones. When the phone sends the RTP stream to a pre-configured multicast address, each phone preconfigured to listen to the multicast address can receive the RTP stream. When the originator stops sending the RTP stream, the subscribers stop receiving it.

Configuration changes can be made using the configuration files, the web, or the phone user interface.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Specify a multicast codec for the phone to use when sending an RTP stream. **Parameter:** multicast.codec
		Configure the multicast IP address and port number for a paging list key. **Parameter:** multicast.paging_address.X.ip_address
		Configure the multicast paging group name for a paging list key. **Parameter:** multicast.paging_address.X.label
Local	Web User Interface	Specify a multicast codec for the phone to use when sending an RTP stream. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load
		Configure the multicast IP address and port number for a paging list key. Configure the multicast paging group name for a paging list key. **Navigate to:** http://<phoneIPAddress>/servlet?p=contacts-multicastIP&q=load
	Phone User Interface	Configure the multicast IP address and port number for a paging list key. Configure the multicast paging group name for a paging list key.

Details of the Configuration Parameters

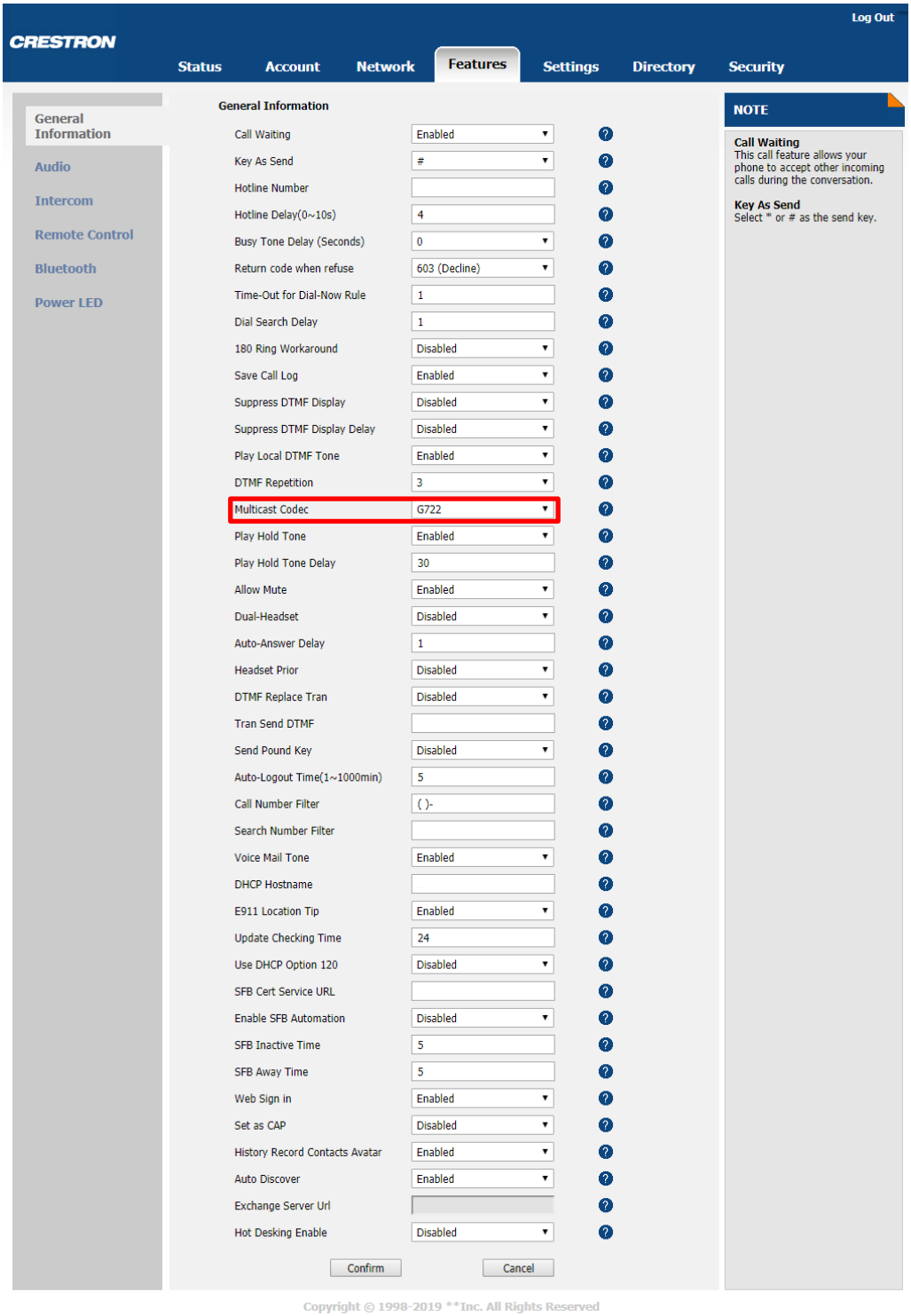
Parameter	Permitted Values	Default
multicast.codec	**PCMU, PCMA, G729, G722**	**G722**
Description: Configures the codec for multicast paging. **Example:** multicast.codec = G722 **Web User Interface:** Features > General Information > Multicast Codec **Phone User Interface:** None		

Parameter	Permitted Values	Default
multicast.paging_address.X.ip_address (X ranges from 1 to 10)	**String**	**Blank**
Description: Configures the IP address and port number of the multicast paging group in the paging list. It will be displayed on the LCD screen when placing the multicast paging call. **Example:** multicast.paging_address.1.ip_address = 224.5.6.20:10008 multicast.paging_address.2.ip_address = 224.1.6.25:1001 **Note:** Valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255. **Web User Interface:** Directory > Multicast IP > Paging List > Paging Address **Phone User Interface:** Menu > Setting > Features > Paging List > Option > Edit > Address		
multicast.paging_address.X.label (X ranges from 1 to 10)	**String**	**Blank**
Description: Configures the name of the multicast paging group to be displayed in the paging list. It will be displayed on the LCD screen when placing the multicast paging calls. **Example:** multicast.paging_address.1.label = Product multicast.paging_address.2.label = Sales **Web User Interface:** Directory > Multicast IP > Paging List > Label **Phone User Interface:** Menu > Setting > Features > Paging List > Option > Edit > Label		

Configure a Codec for Multicast Paging via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



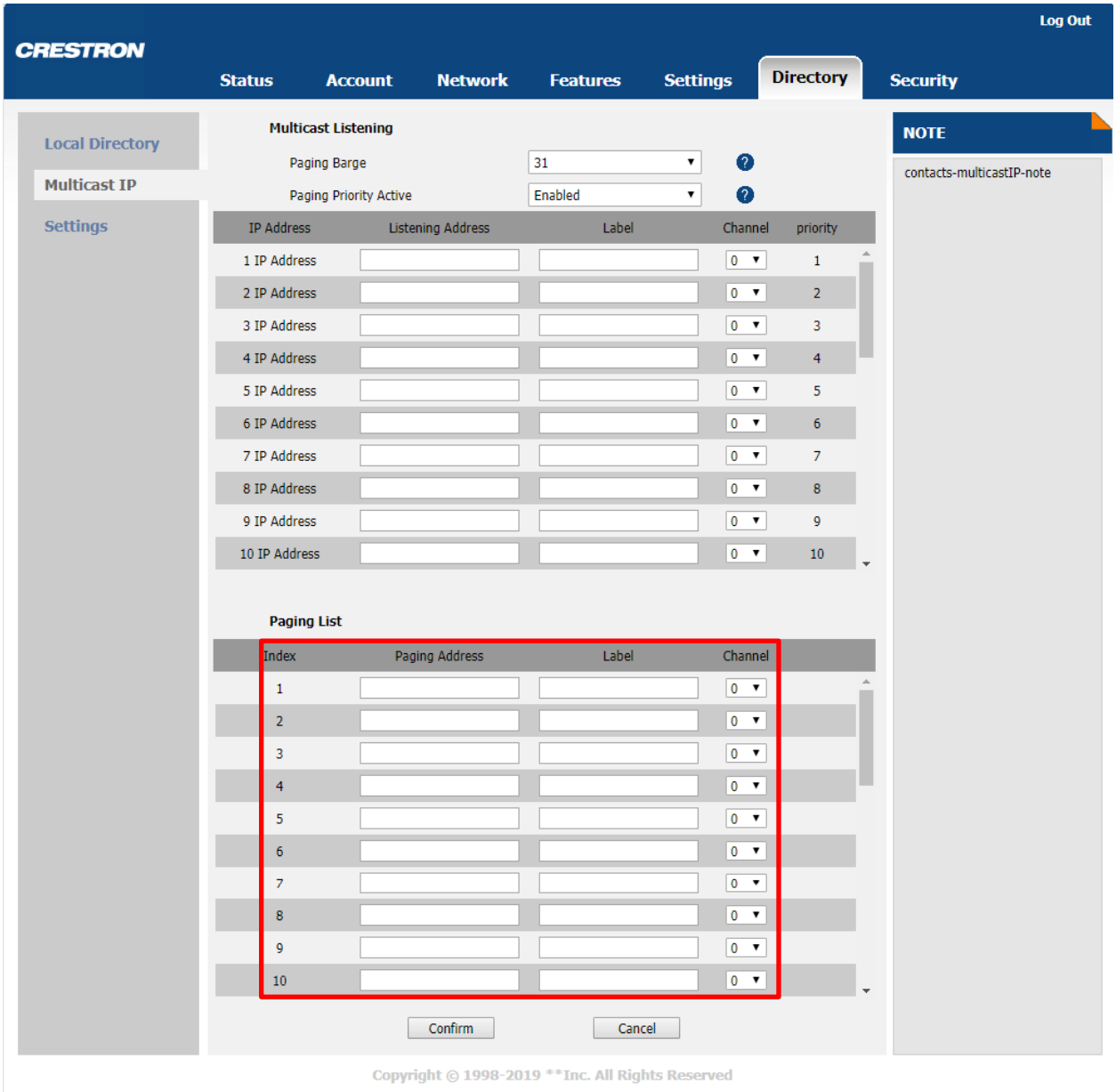
2. Select the codec from the **Multicast Codec** drop-down list.

3. Click **Confirm** to accept the change.

Configure Sending Multicast Addresses via the Web User Interface

1. Click **Directory** > **Multicast IP**.

Directory > Multicast IP



2. Enter the sending multicast address and port number in the **Paging Address** field.
3. Enter the label in the **Label** field. The label will appear on the phone display when sending an RTP multicast.
4. Click **Confirm** to accept the changes.

Configure the Paging List via the Phone User Interface

1. Tap **Setting** > **Features** > **Paging List**.
2. Tap the right side of an entry.
3. Enter the multicast IP address and port number (e.g., 224.5.6.20:10008) in the **Address** field. Valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255.
4. Enter the group name in the **Label** field.
5. Tap **Save**.
6. Repeat steps 2 to 6 to add more paging groups.

Receive an RTP Stream

Skype for Business phones can receive an RTP stream from the pre-configured multicast address(es) without SIP signaling, and can handle the incoming multicast paging calls differently depending on how Paging Barge and Paging Priority Active are configured.

The Paging Barge parameter defines the priority of the voice call in progress, and decides how the phone handles incoming multicast paging calls when there is already a voice call in progress. If the parameter is configured as **Disabled**, all incoming multicast paging calls will be automatically ignored. If the value of the parameter is the priority value, incoming multicast paging calls with higher or equal priority are automatically answered and the ones with lower priority are ignored.

The Paging Priority Active parameter determines how the phone handles incoming multicast paging calls when there is already a multicast paging call in progress. If the parameter is configured as **Disabled**, the phone will automatically ignore all incoming multicast paging calls. If the parameter is configured as **Enabled**, incoming multicast paging calls with equal or higher priority are automatically answered, and those with lower priority are ignored.

Configuration changes can be performed using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the listening multicast address. **Parameters:** multicast.listen_address.X.ip_address multicast.listen_address.X.label
		Configure Paging Barge and Paging Priority Active features. **Parameters:** multicast.receive_priority.enable multicast.receive_priority.priority
Local	Web User Interface	Configure the listening multicast address. Configure Paging Barge and Paging Priority Active features. **Navigate to**: http://<phoneIPAddress>/servlet?p=contacts-multicastIP&q=load

Details of the Configuration Parameters

Parameter	Permitted Values	Default
multicast.listen_address.X.ip_address (X ranges from 1 to 10)	**IP address: port**	**Blank**
Description: Configures the multicast address and port number the phone listens to. **Example:** multicast.listen_address.1.ip_address = 224.5.6.20:10008 **Web User Interface:** Directory > Multicast IP > Multicast Listening > Listening Address **Phone User Interface:** None		
multicast.listen_address.X.label (X ranges from 1 to 10)	**String within 99 characters**	**Blank**
Description: (Optional.) Configures the label to be displayed on the LCD screen when receiving multicast paging calls. **Example:** multicast.listen_address.1.label = Paging1 **Web User Interface:** Directory > Multicast IP > Multicast Listening > Label **Phone User Interface:** None		

Parameter	Permitted Values	Default
multicast.receive_priority.enable	0 or 1	1

Description:

Enables or disables handling incoming multicast paging calls when there is an active multicast paging call on the phone.

0- Disabled, the phone ignores the incoming multicast paging calls when there is an active multicast paging call on the phone.

1- Enabled, the phone receives incoming multicast paging calls with a equal or higher priority and ignores those with lower priority.

Web User Interface:
Directory > Multicast IP > Paging Priority Active

Phone User Interface:
None

multicast.receive_priority.priority	Integer from 0 to 10	10

Description:

Configures the priority of a voice call (a normal phone call rather than a multicast paging call) in progress.

1 is the highest priority, 10 is the lowest priority.

0- Disabled, all incoming multicast paging calls will be automatically ignored when a voice call is in progress.

1- 1

2- 2

3- 3

4- 4

5- 5

6- 6

7- 7

8- 8

9- 9

10-10

If it is set to other values, the phone will receive the incoming multicast paging call with equal or higher priority and ignore those with lower priority when a voice call is in progress.

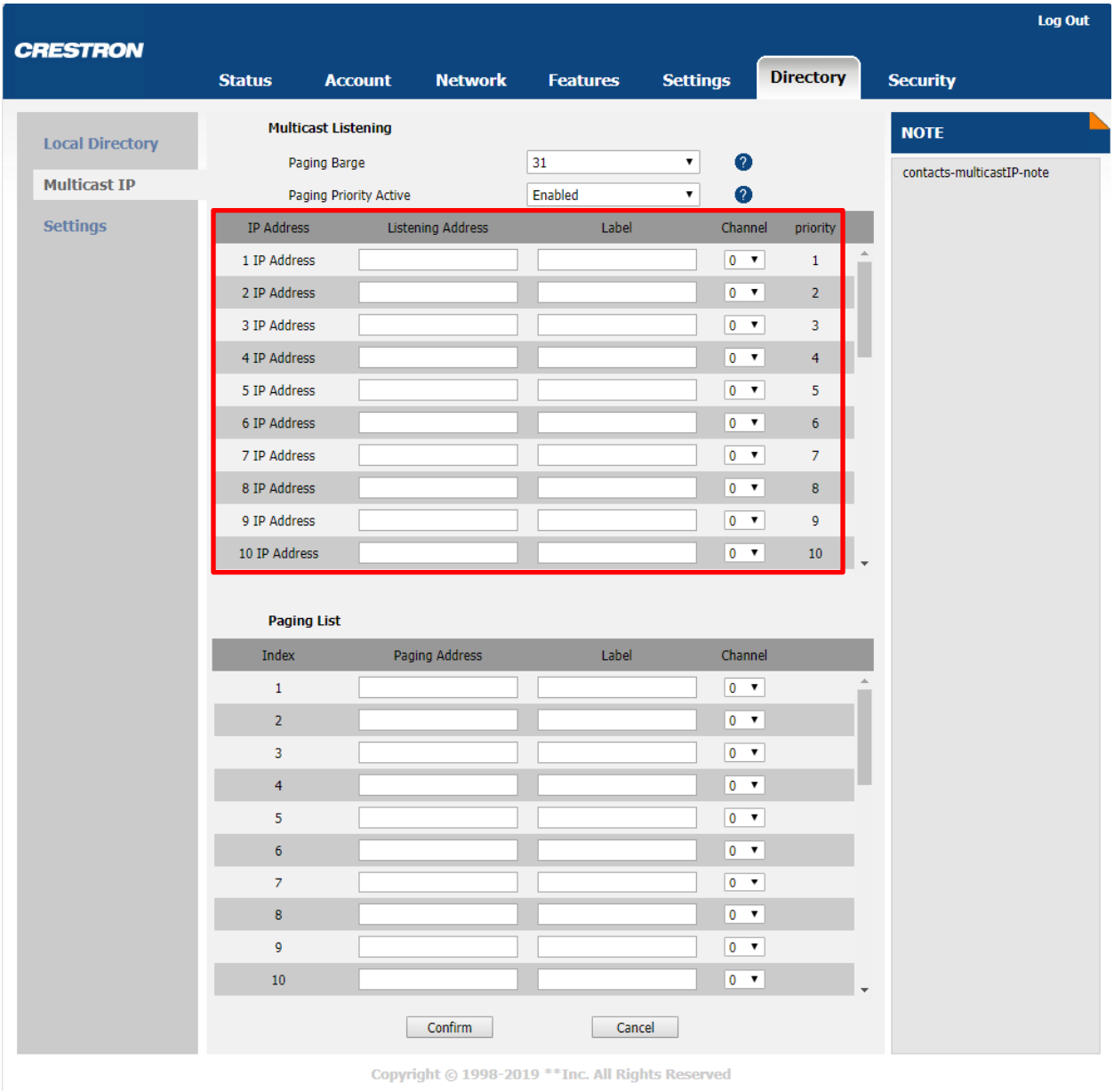
Web User Interface:
Directory->Multicast IP->Paging Barge

Phone User Interface:
None

Configure a Listening Multicast Address via the Web User Interface

1. Click **Directory** > **Multicast IP**.

Directory > Multicast IP

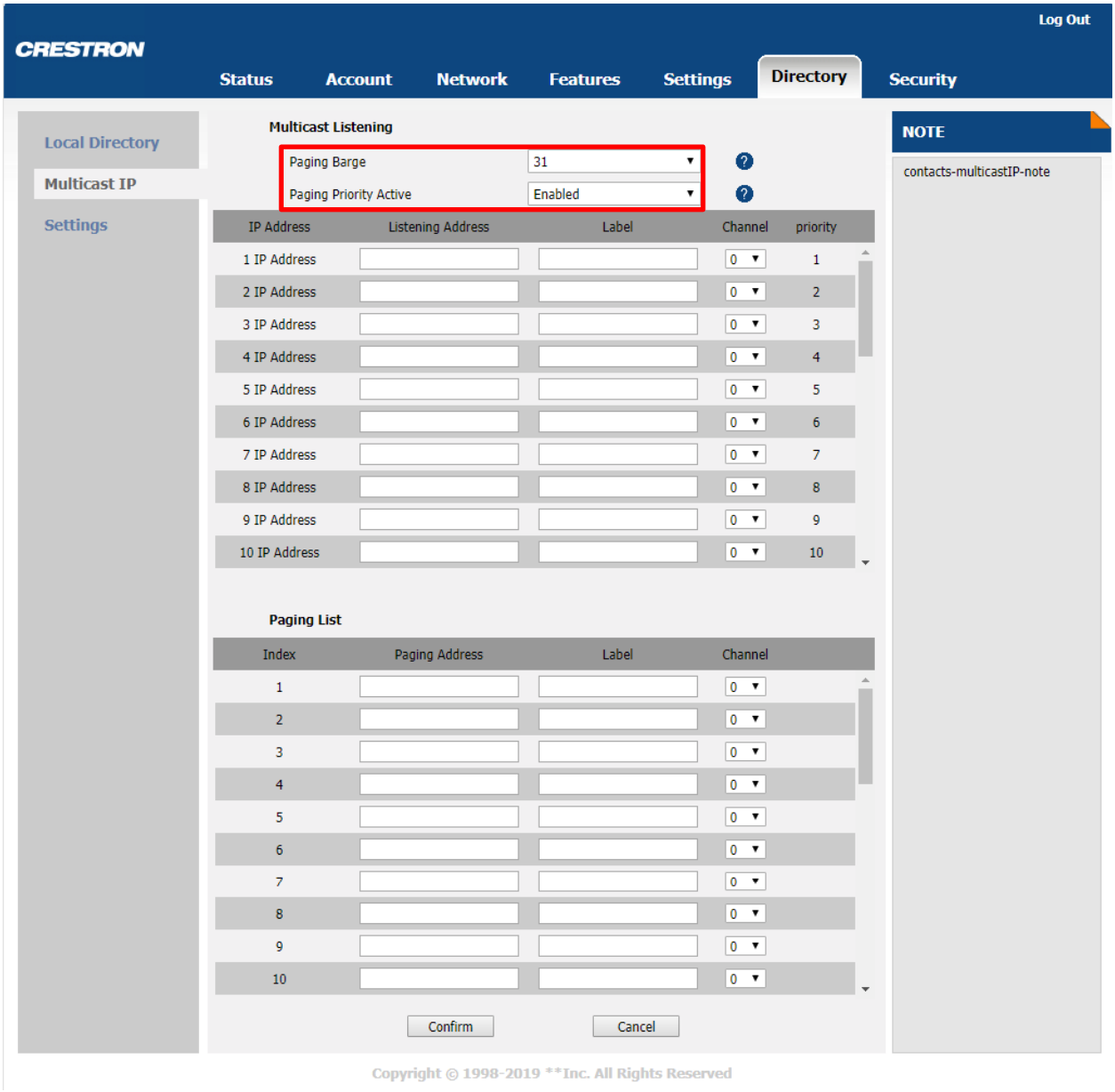


2. Enter the listening multicast address and port number in the **Listening Address** field. 1 is the highest priority and 10 is the lowest priority.
3. Enter the label in the **Label** field. The label will appear on the LCD screen when receiving an RTP multicast.
4. Click **Confirm** to accept the changes.

Configure Paging Barge and Paging Priority Active Features via the Web User Interface

1. Click **Directory** > **Multicast IP**.

Directory > Multicast IP



2. Select the desired value from the **Paging Barge** drop-down list.
3. Select **Enabled** or **Disabled** from the **Paging Priority Active** drop-down list.
4. Click **Confirm** to accept the changes.

Hot Desking

Hot desking allows a Guest to clear the Host's registration configurations on the phone, and then register his own account.

Hot desking feature can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the hot desking feature. **Parameters:** sfb.hot_desking.enable
Local	Web User Interface	Configure the hot desking feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure the hot desking feature.

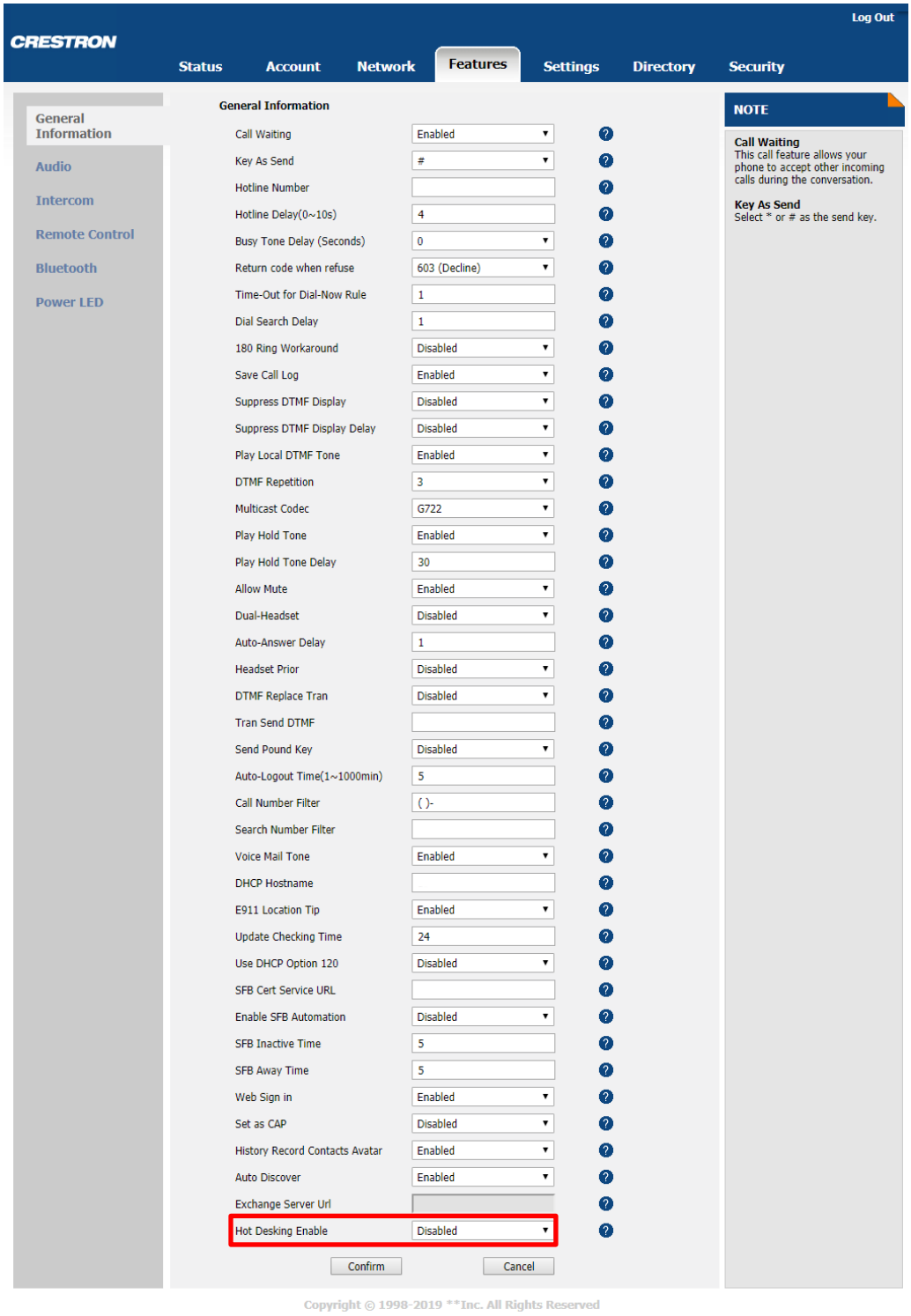
Details of the Configuration Parameter

Parameter	Permitted Values	Default
sfb.hot_desking.enable	**0 or 1**	**1**
Description: Enables or disables the hot desking feature. **0**- Disabled **1**- Enabled. **Web User Interface:** Features > General Information > Hot Desking Enable **Phone User Interface:** Menu > Setting > Features > Hot-Desking		

Configure Hot Desking Feature via the Web User Interface:

1. Click **Features** > **General Information**.

Features > General Information



2. Select **Enabled** or **Disabled** from the **Hot Desking Enable** drop-down list.

3. Click **Confirm** to accept.

Configure Hot Desking Feature via the Phone User Interface:

1. Tap **Setting** > **Features** > **Hot-Desking**.
2. Select **Enabled** or **Disabled** in the **Hot-Desking** field.
3. Tap **Save**

Common Area Phone.

Common Area Phones (CAPs) are those Skype for Business phones that are not associated with an individual user. Instead of being deployed in someone's office, CAPs are typically deployed in building lobbies, cafeterias, employee lounges, conference rooms, and other places where a large number of people are likely to gather. Unlike other phones on the Skype for Business server, which are typically maintained by using voice policies and dial plans that are assigned to individual users, CAPs do not have individual users assigned to them.

Common area phone can be configured using the following methods.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the Common Area Phone feature. **Parameters:** features.set_as_cap.enable features.voice_mail.enable features.cap_presence.enable features.redial.enable features.exchange_connect.enable features.sfb_directory.enable phone_setting.search_contacts.enable features.call_history.enable features.paging.enable
Local	Web User Interface	Configure the Common Area Phone feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load
	Phone User Interface	Configure the Common Area Phone feature.

Details of the Configuration Parameters

Parameter	Permitted Values	Default
features.set_as_cap.enable	0 or 1	0
Description: Enables or disables the Common Area Phone feature. **0**- Disabled, the phone will work as an individual phone. **1**- Enabled, the phone will work as a common area phone (with limited features enabled). Note: If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Features > General Information > Set as CAP **Phone User Interface:** Menu > Setting > Advanced(default password: admin) > Common Area Phone > Set as CAP		
features.cap_presence.enable	0 or 1	1
Description: Enables or disables the display of presence status of the Skype for Business contacts. **0**- Disabled **1**- Enabled **Web User Interface:** None **Phone User Interface:** None		
features.voice_mail.enable	0 or 1	Refer to the following content
Description: Enables or disables the voice mail feature. **0**- Disabled **1**- Enabled **Default Values:** For individual phone: 1 For common area phone: 0 **Web User Interface:** None **Phone User Interface:** None		

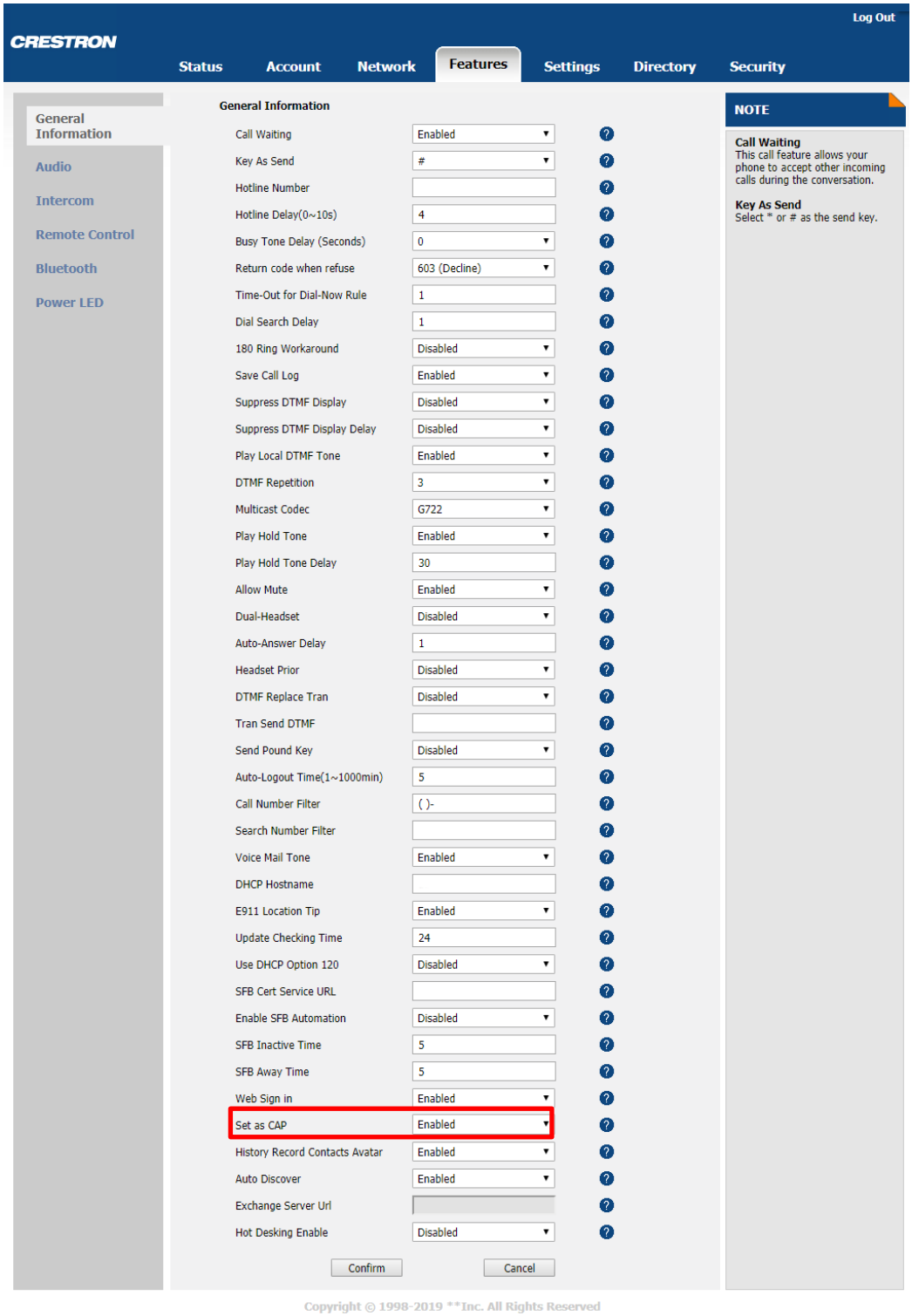
Parameter	Permitted Values	Default
features.redial.enable	0 or 1	Refer to the following content
Description: Enables or disables redialing the last dialed number. **0**- Disabled **1**- Enabled **Default Values:** For individual phone: 1 For common area phone: 0 **Web User Interface:** None **Phone User Interface:** None		
features.exchange_connect.enable	0 or 1	1
Description: Enables or disables the Microsoft Exchange integration feature. **0**- Disabled **1**- Enabled **Web User Interface:** None **Phone User Interface:** None		
features.sfb_directory.enable	0 or 1	Refer to the following content
Description: Enables or disables display of Skype for Business contacts. **0**- Disabled **1**- Enabled **Default Values:** For individual phone: 1 For common area phone: 0 **Web User Interface:** None **Phone User Interface:** None		

Parameter	Permitted Values	Default
phone_setting.search_contacts.enable	**0 or 1**	**Refer to the following content**
Description: Enables or disables searching contacts on the phone. **0**- Disabled **1**- Enabled **Default Values:** For individual phone: 1 For common area phone: 0 **Web User Interface:** None **Phone User Interface:** None		
features.call_history.enable	**0 or 1**	**Refer to the following content**
Description: Enables or disables display of call history. **0**- Disabled **1**- Enabled **Default Values:** For individual phone: 1 For common area phone: 0 **Web User Interface:** None **Phone User Interface:** None		
features.paging.enable	**0 or 1**	**Refer to the following content**
Description: Enables or disables configuring the multicast paging feature. **0**- Disabled, the phone hides multicast paging configurations. **1**- Enabled, the phone displays multicast paging configurations. **Default Values:** For individual phone: 1 For common area phone: 0 **Web User Interface:** None **Phone User Interface:** None		

Configure a Phone to be a CAP via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Select **Enabled** from the **Set as CAP** drop-down list.
3. Click **Confirm** to accept the change.

Configure a Phone to be a CAP via the Phone User Interface

1. Tap **Setting** > **Advanced** (default password: admin) > **Common Area Phone**.
2. Select **Enabled** from the **Set as CAP** field.
3. Tap **Save**. A dialog box pops up stating that the configuration will take effect after a reboot.

CAP Provisioning Sign-in Method

A web browser can be used to provision numerous CAPs quickly.

Branch Office Resiliency

Branch office resiliency is critical for multi site deployments of Skype for Business where the control servers are located at a central site or in data center. It allows branch site users to continue having Enterprise Voice service and voice mail (if voice mail rerouting settings are configured) when the branch site loses the connection with the central site.

When the WAN connection between the branch site and central site is unavailable, the phone goes into resiliency mode:

- The branch site user on the phone stays signed-in with an indication of "Limited service due to outage".
- The Presence icon on the phone LCD screen is displayed as .
- A call between branch site users is established successfully with 2-way audio.
- A conference between branch site users can be established successfully.
- The call history can not get modified. (Previously downloaded call log entries can not be deleted).
- Calls can be placed from the call history on the Skype for Business phone.
- The contact list is unavailable but the user can search for a contact on the Skype for Business phone.
- The user is not able to change the presence state manually.
- The user is not able to use the Calendar feature.
- The user is not able to receive voice mail as exchange is unreachable.
- Calls between branch office phones can be transferred to another branch site user.
- Call Forward settings cannot be changed.

When the WAN connection between the branch site and central site becomes available, the phone comes out of resiliency mode automatically. Notification of resiliency is automatically dismissed, and the user can use phone features as normal.

For more information on branch office resiliency, contact the system administrator.

Action URI

An Action URI allows phones to interact with the web server application by receiving and handling HTTP or HTTPS GET requests. When receiving a GET request, the phone performs the specified action and responds with a 200 OK message. A GET request may contain a variable named "key" along with a variable value, separated by "=". The valid URI format is: http(s)://<phoneIPAddress>/servlet?key=variable value. For example: http://10.3.20.10/servlet?key=OK.

For security reasons, phones do not handle HTTP/HTTPS GET requests by default. The trusted IP address for the Action URI must be specified. When the phone receives a GET request from the trusted IP address for the first time, the LCD screen displays "Allow Remote Control?". Tap **OK** on the phone to allow remote control. One or more trusted IP addresses can be specified on the phone, or the phone can be configured to receive and handle the URI from any IP address.

The Action URI feature can be used to capture the phone's current screen. For more information, refer to "Capture the Current Screen of the Phone" on page 261.

Specify the trusted IP address for an Action URI using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the phone to receive Action URI requests. **Parameter:** features.action_uri.enable
		Specify the trusted IP address(es) for sending the Action URI to the phone. **Parameter:** features.action_uri_limit_ip
Local	Web User Interface	Specify the trusted IP address(es) for sending an Action URI to the phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-remotecontrl&q=load

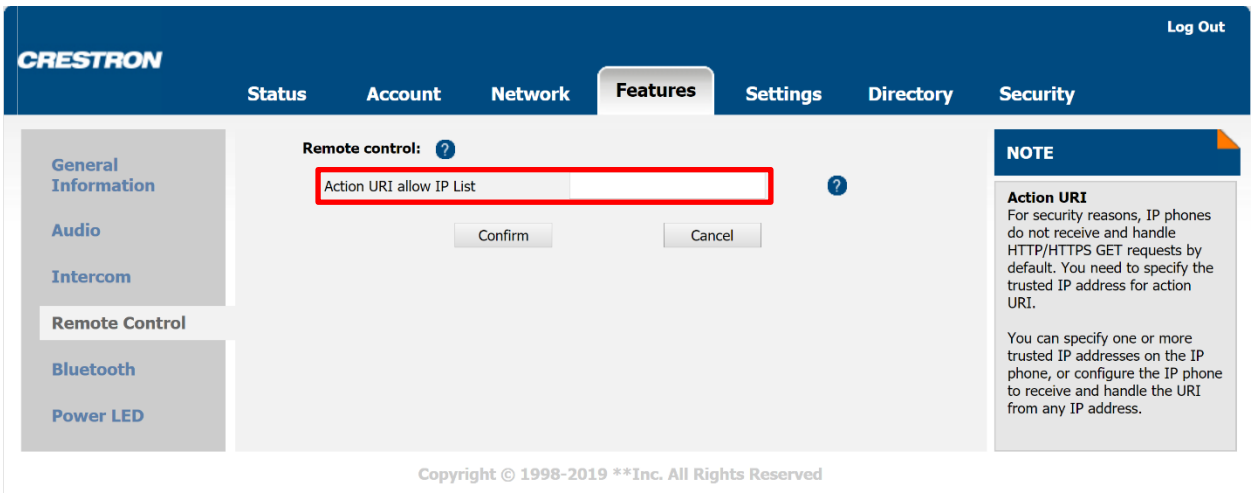
Details of the Configuration Parameters

Parameter	Permitted Values	Default
features.action_uri.enable	0 or 1	0
Description: Enables or disables receiving Action URI requests. **0**- Disabled **1**- Enabled **Web User Interface:** None **Phone User Interface:** None		
features.action_uri_limit_ip	IP address or any	Blank
Description: Configures the IP address of the server from which the phone receives Action URI requests. For discontinuous IP addresses, multiple IP addresses are separated by commas. For continuous IP addresses, the format likes *.*.*.* and the "*" stands for the values 0~255. For example: 10.10.*.* stands for the IP addresses that range from 10.10.0.0 to 10.10.255.255. If left blank, the phone will reject any HTTP GET request. If it is set to "any", the phone will accept and handle HTTP GET requests from any IP address. **Example:** features.action_uri_limit_ip = any **Note:** This feature works only if the value of the parameter "features.action_uri.enable" is set to 1 (Enabled). **Web User Interface:** Features > Remote Control > Action URI allow IP List **Phone User Interface:** None		

Configure the Trusted IP Address(es) for Action URI via the Web User Interface

1. Click **Features** > **Remote Control**.

Features > Remote Control



2. Enter the IP address or "any" in the **Action URI allow IP List** field.

   Multiple IP addresses are separated by commas. If "any" is entered in this field, the phone can receive and handle GET requests from any IP address. If the field is left blank, the phone cannot receive or handle any HTTP GET request.

3. Click **Confirm** to accept the change.

Capture the Current Screen of the Phone

The screen display of the phone can be captured using an Action URI. Skype for Business phones support handling HTTP or HTTPS GET requests. The URI format is http(s)://<phoneIPAddress>/screencapture. The captured picture can be saved as a BMP or JPEG file.

The URI "http(s)://<phoneIPAddress>/screencapture/download" can be used to capture the screen display first, and then download the image. The image is saved as a JPG file and named with the phone model and the capture time to the local system. Before capturing the phone's current screen, ensure the IP address of the PC is included in the trusted IP address for Action URIs on the phone.

When capturing the screen display, the phone may prompt the user to enter the user name and password of the administrator if the web browser does not remember the user name and password for the web user interface login.

NOTE: The old URI "http://<phoneIPAddress>/servlet?command=screenshot" can also be used to capture the screen display

To capture the current screen of the phone, enter the request URI (e.g., http://10.2.20.126/screencapture) in the browser's address bar and press the **Enter** key on the keyboard.

One of the following will occur:

- If it is the first time capturing the phone's current screen using the computer, the browser displays "Remote control forbidden", and the LCD screen displays an "Allow remote control?" message.

  Tap **OK** to allow remote control. The phone will return to the previous screen. Refresh the web page.

  The browser will display an image showing the phone's current screen. The image can be saved to the local computer.

- The browser will display an image showing the phone's current screen directly. The image can be saved to the local computer.

NOTE: Frequent capture may affect the Skype for Business phone performance. Crestron recommends an interval of at least four seconds between phone screen captures.

Quality of Experience

Quality of Experience (QoE) metrics track the quality of audio calls made in an organization, including how many network packets are lost, the amount of "jitter" (differences in packet delay), and the background noise.

The phone calculates QoE metrics and then sends them to a server for monitoring and diagnostics purposes.

The phone will send QoE metrics every 30 seconds during a call or once a call lasting more than 5 seconds ends.

QoE can be configured using the configuration files only.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the QoE feature. **Parameters:** phone_setting.qoe.enable features.report_qoe.when_bad_quality.enable

Details of the Configuration Parameters

Parameter	Permitted Values	Default
phone_setting.qoe.enable	0 or 1	1
Description: Enables or disables sending Quality of Experience (QoE) metrics to a server. **0**- Disabled **1**- Enabled **Web User Interface:** None **Phone User Interface:** None		
features.report_qoe.when_bad_quality.enable	0 or 1	1
Description: Enables or disables sending Quality of Experience (QoE) metrics to a server for monitoring and diagnostics when voice quality is poor. **0**- Disabled **1**- Enabled **Note:** This feature works only if the parameter "phone_setting.qoe.enable" is set to 1 (Enabled). **Web User Interface:** None **Phone User Interface:** None		

In QoE Metrics, the following formation will be reported:

Quality of Experience Metrics

Fields	Element	Attribute
VQReportEvent	VQSessionReport	
	VQSessionIntervalReport	
VQSessionReport		
	Endpoint	SessionId
	DialogInfo	
	MediaLine	
VQSessionReport:Endpoint		
		xmlns
		xmlns:v2
		xmlns:v3
		Name
		v2:OS
		v2:CPUName
		v2:CPUNumberOfCores

Fields	Element	Attribute
		v2:CPUProcessorSpeed (fixed value: 498)
		v2:VirtualizationFlag
VQSessionReport:DialogInfo		
	DialogCategory	CallId
	CorrelationID	FromTag
	FromURI	ToTag
	ToURI	Start
	Caller	End
	LocalContactURI	
	RemoteContactURI	
	LocalUserAgent	
	RemoteUserAgent	
	LocalPAI	
	RemotePAI	
	ConfURI	
	v2:CallPriority	
	v2:MediationServerBypassFlag	
	v2:TrunkingPeer	
	v2:MediaBypassWarningFlag	
	v2:RegisteredInside	
	CallId	
	FromTag	
	ToTag	
	Start	
	End	
VQSessionReport:MediaLine		
	Description	xmlns
	InboundStream	xmlns:v2
	OutboundStream	xmlns:v3
		Label
MediaLine:Description	Connectivity	
	Security	
	Offerer	
	Transport	
	NetworkConnectivityInfo	
	LocalAddr	
	RemoteAddr	
	CaptureDev	

Fields	Element	Attribute
	RenderDev	
	ReflexiveLocalIPAddress	
	v3:ReflexiveLocalIPAddress	
	v3:MidCallReport	
Description:Connectivity	Ice	
	IceWarningFlags	
	RelayAddress	
Connectivity:RelayAddress	IPAddr	
	Port	
Description:NetworkConnectivityInfo	NetworkConnection	
	VPN	
	LinkSpeed	
	v3:NetworkConnectionDetails	
Description:LocalAddr	IPAddr	
	Port	
	SubnetMask	
	v2:MACAddr	
Description:RemoteAddr	IPAddr	
	Port	
Description:CaptureDev	Name	
	Driver	
Description:RenderDev	Name	
	Driver	
Description:ReflexiveLocalIPAddress	IPAddr	
	Port	
MediaLine:InboundStream	Network	ID
	Payload	
	QualityEstimates	
InboundStream:Network	Jitter	
	PacketLoss	
	BurstGapLoss	
	Delay	
	Utilization	
Network:Jitter	InterArrival	
	InterArrivalSD	
	InterArrivalMax	
Network:PacketLoss	LossRate	
	LossRateMax	

Fields	Element	Attribute
Network:Delay	RelativeOneWay	
Delay:RelativeOneWay	Average	
	Max	
	Gap	
Delay:RelativeOneWay:Gap	Occurrences	
	Density	
	Duration	
Network:Utilization	Packets	
InboundStream:Payload:Audio	PayloadType	
	PayloadDescription	
	SampleRate	
	Signal	
	v4:JitterBufferSizeAvg	
	v4:JitterBufferSizeMax	
	v4:JitterBufferSizeMin	
	v4:NetworkJitterAvg	
	v4:NetworkJitterMax	
	v4:NetworkJitterMin	
Audio:Signal	SignalLevel	
	NoiseLevel	
	SpeakerGlitchRate	
	v2:RxAvgAGCGain	
	v3:RecvSignalLevelCh1	
	v3:RecvNoiseLevelCh1	
	v4:RenderSignalLevel	
	v4:RenderNoiseLevel	
	v4:RenderLoopbackSignalLevel	
QualityEstimates:Audio	RecvListenMOS	
	RecvListenMOSMin	
	RecvListenMOSAlg (fixed value for device: P.564)	
	NetworkMOS	
Audio:NetworkMOS	OverallAvg	
	OverallMin	
MediaLine:OutboundStream	Network	ID
	Payload	
	QualityEstimates	
OutboundStream:Network	Jitter	
	PacketLoss	

Fields	Element	Attribute
	Delay	
	Utilization	
Network:Jitter	InterArrival	
	InterArrivalMax	
Network:PacketLoss	LossRate	
	LossRateMax	
Network:Delay	RoundTrip	
	RoundTripMax	
Network:Utilization	Packets	
	BandwidthEst	
OutboundStream:Payload:Audio	PayloadType	
	PayloadDescription	
	SampleRate	
	Signal	
Audio:Signal	SignalLevel	
	NoiseLevel	
	MicGlitchRate	
	EchoPercentMicIn	
	EchoPercentSend	
	SendSignalLevelCh1	
	SendNoiseLevelCh1	

An administrator can log into the QoE Monitoring Server to view QoE information.

Configuring Audio Features

Predial Tone

Predial Tone allows phones to play a key tone in following situations:

- Enter phone numbers without picking up the handset
- Tap (Search icon) to enter the predialing screen, and then enter phone numbers without picking up the handset

Predial Tone can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure predial tone feature. **Parameters:** sfb.pre_dial_tone.enable
Local	Web User Interface	Configure predial tone feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-audio&q=load

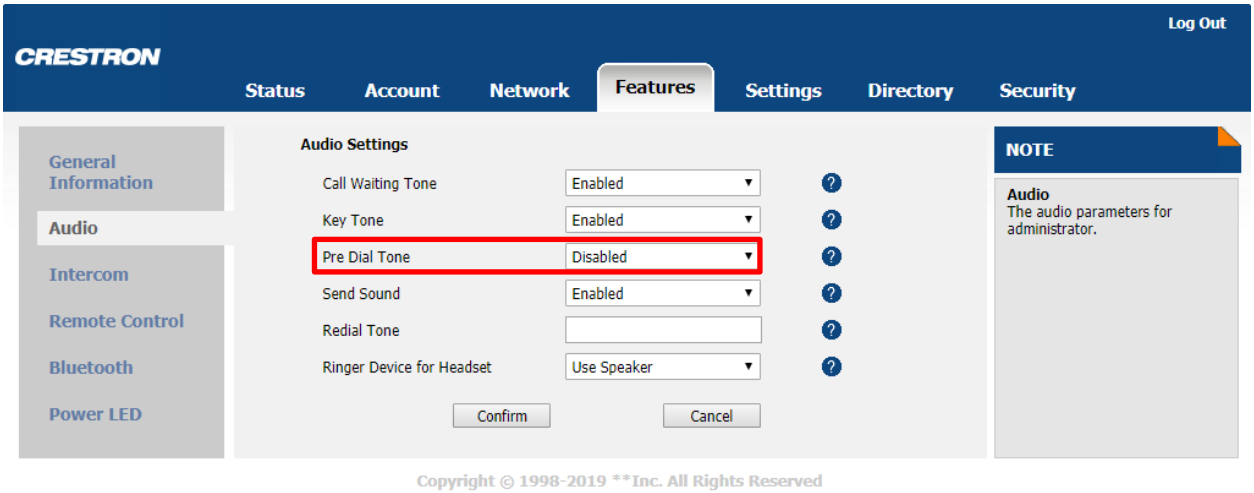
Details of the Configuration Parameter

Parameter	Permitted Values	Default
sfb.pre_dial_tone.enable	**0 or 1**	**0**
Description: Enables or disables playing a key tone in the following situations: • Enter phone numbers without picking up the handset. • Tap (**Search** icon) to enter the predialing screen, and then enter phone numbers without picking up the handset. **Web User Interface:** Features > Audio > Pre Dial Tone **Phone User Interface:** None		

Configure Predial Tone via the Web User Interface

1. Click **Features** > **Audio**.

Features > Audio



2. Select **Enabled** or **Disabled** from the **Predial Tone** drop-down list.
3. Click **Confirm** to accept the change.

Phone Ring Tones

Phone ring tones indicate incoming calls. The user can select a built-in system ring tone or a custom ring tone for the phone or a registered account. To set the custom ring tones, the ring tones must be uploaded to the phone in advance.

The ring tone must be a .wav file in CMU/PCMA audio format, mono, 8 kHz sample rate and 16-bit resolution. The file size must be less than 8 MB. 2 MB should be reserved for the phone.

Ring tones can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure a ring tone for the phone. **Parameter:** phone_setting.ring_type
		Specify the access URL of the custom ring tone. **Parameter:** phone_setting.ringtone.url
		Delete all custom ring tone files. **Parameter:** ringtone.delete
	<MAC>.cfg	Configure a ring tone on a per line basis. **Parameter:** account.1.ringtone.ring_type
Local	Web User Interface	Upload the custom ring tones. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-preference&q=load
		Configure a ring tone for the phone. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-preference&q=load
	Phone User Interface	Configure a ring tone for the phone.

Details of the Configuration Parameters

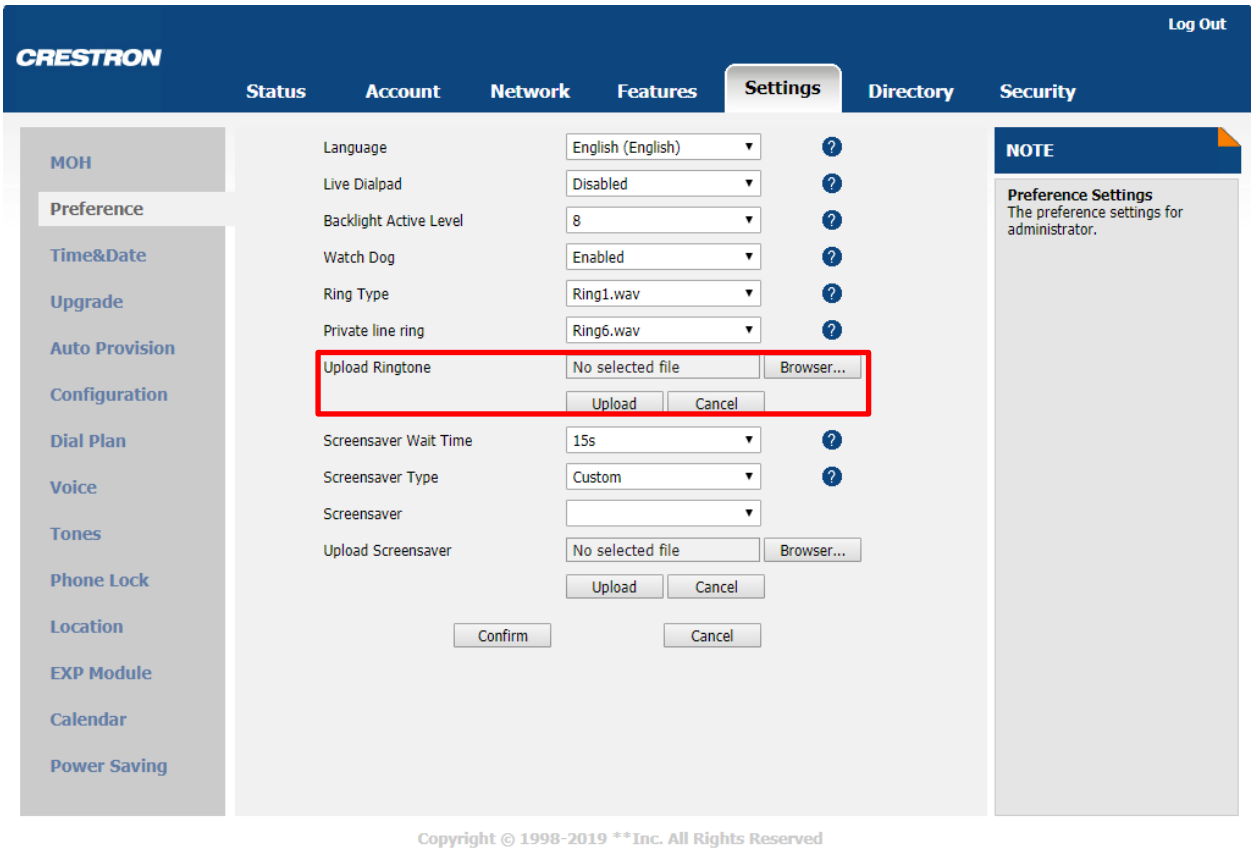
Parameter	Permitted Values	Default
phone_setting.ring_type	Refer to the following content	Ring1.wav
Description: Configures a ring tone for the phone. **Permitted Values:** Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav, Splash.wav or custom ring tone name (e.g., Customring.wav). **Example:** • **To configure a phone built-in ring tone (e.g., Ring1.wav):** phone_setting.ring_type = Ring1.wav • **To configure a custom ring tone (e.g., Customring.wav):** phone_setting.ring_type = Customring.wav **Web User Interface:** Settings > Preference > Ring Type **Phone User Interface:** Menu > Setting > Basic > Sounds > Ring Tones > Normal		
account.1.ringtone.ring_type	Refer to the following content	Common
Description: Configures a ring tone for Account 1. **Example**: **account.1.ringtone.ring_type = Ring3.wav** It means configuring Ring3.wav for the account. It means that Ring3 is specified as the ringtone to account1. **account.1.ringtone.ring_type = Common** It means the account will use the ring tone selected for the phone configured by the parameter "phone_setting.ring_type". **Permitted Values:** Common, Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav, Splash.wav or custom ring tone name (e.g., Customring.wav). **Web User Interface:** None **Phone User Interface:** None		
phone_setting.ringtone.url	URL within 511 characters	Blank
Description: Configures the access URL of the custom ring tone file. **Example:** phone_setting.ringtone.url = tftp://192.168.1.100/Customring.wav **Web User Interface:** Settings > Preference > Upload Ringtone **Phone User Interface:** None		

Parameter	Permitted Values	Default
ringtone.delete	http://localhost/all	Blank
Description: Deletes all custom ring tone files. **Example:** ringtone.delete = http://localhost/all **Web User Interface:** None **Phone User Interface:** None		

Upload a Custom Ring Tone via the Web User Interface

1. Click **Settings** > **Preference**.

Settings > Preference

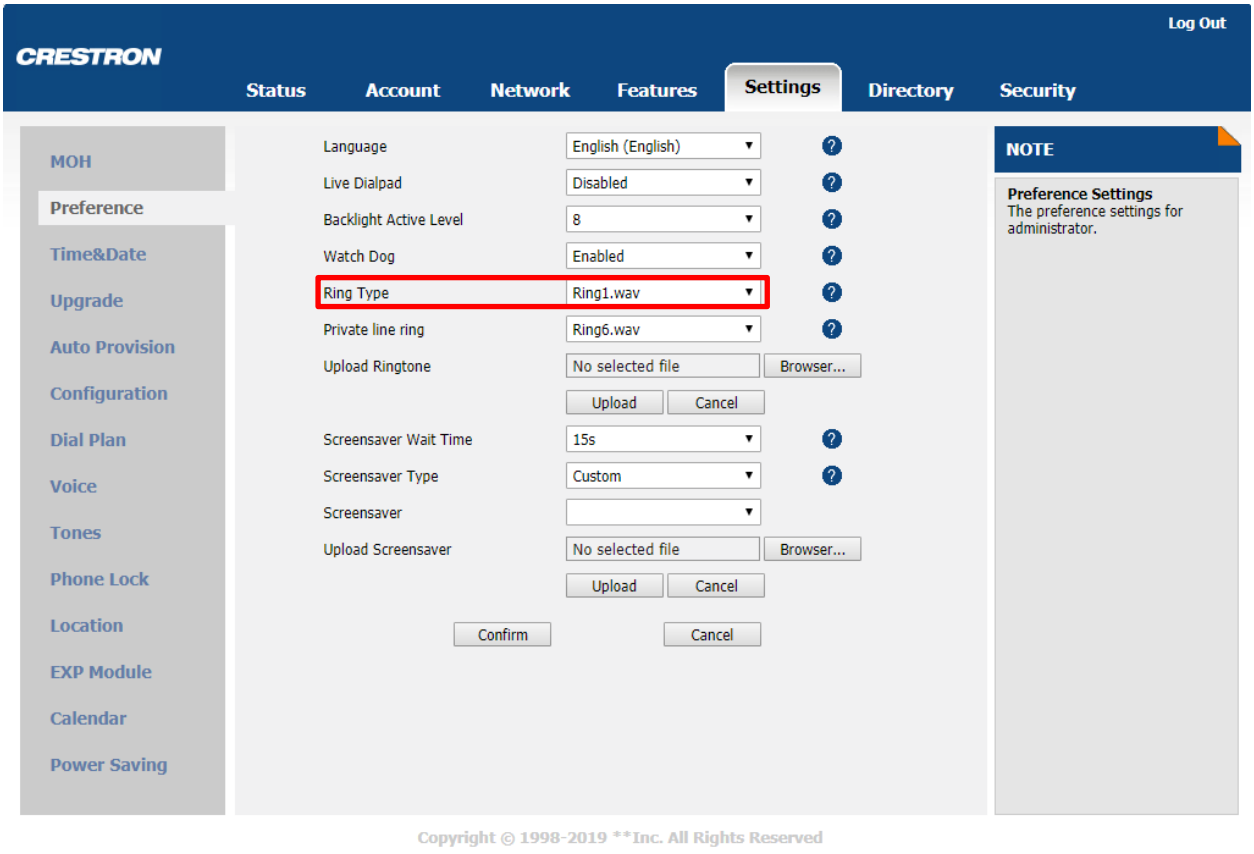


2. In the **Upload Ringtone** field, click **Browser** to locate a ring tone file from the local computer. The file must be WAV format.
3. Click **Upload** to upload the file. The custom ring tone appears in the **Ring Type** drop-down list.

Change the Ring Tone for the Phone via the Web User Interface

1. Click **Settings** > **Preference**.

Settings > Preference



2. Select the ring tone from the **Ring Type** drop-down list.
3. Click **Confirm** to accept the change.

Select a Ring Tone for the Phone via the Phone User Interface

1. Tap **Setting** > **Basic** > **Sounds** > **Ring Tones**.
2. Tap the type of call where the ring tone will be assigned (**Normal**, **Private Line**, **Team Call**, **Response Group**).
3. Tap a ring tone.
4. Tap **Save**.

Mute the Ringtone

Set the account status to Busy (in a call) or Do Not Disturb so as not to be disturbed by the phone ringing.

Muting the ringtone can be configured using the configuration files only.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the phone to mute the ringtone. **Parameters:** phone_setting.soundsmin.busy_enable phone_setting.soundsmin.dnd_enable

Details of the Configuration Parameters

Parameter	Permitted Values	Default
phone_setting.soundsmin.busy_enable	0 or 1	0
Description: Enables or disables muting the ringtone when account status is busy (in a call). **0**- Disabled, the phone plays a ringtone for incoming calls when account status is busy (in a call). **1**- Enabled, the phone does not play a ringtone for incoming calls when account statusis busy (in a call). **Web User Interface:** None **Phone User Interface:** None		
phone_setting.soundsmin.dnd_enable	0 or 1	1
Description: Enables or disables muting the ringtone when account status is Do Not Disturb. **0**- Disabled, the phone plays a ringtone for incoming calls from working group when account status is Do Not Disturb. **1**- Enabled, the phone does not play a ringtone for incoming calls from working group when account status is Do Not Disturb. **Web User Interface:** None **Phone User Interface:** None		

Private Line Tones

The Skype for Business Server allows the system administrator to give users a second, but private telephone line in addition to their primary telephone line. A private line is often assigned to the boss, who wants an unlisted telephone number at which they can be reached directly.

When the boss receives a private call, the private line will bypass call delegation and only the boss's phone rings. A private line can only be configured via Skype for Business Server.

The Private Line Tones feature allows the phone to play a distinct ring tone when receiving a private call.

Private Line Tones can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure a ring tone for the private line. **Parameters:** phone_setting.private_line_ring.enable phone_setting.private_line_ring_type
Local	Web User Interface	Configure a ring tone for the private line. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-preference&q=load
	Phone User Interface	Configure a ring tone for the private line.

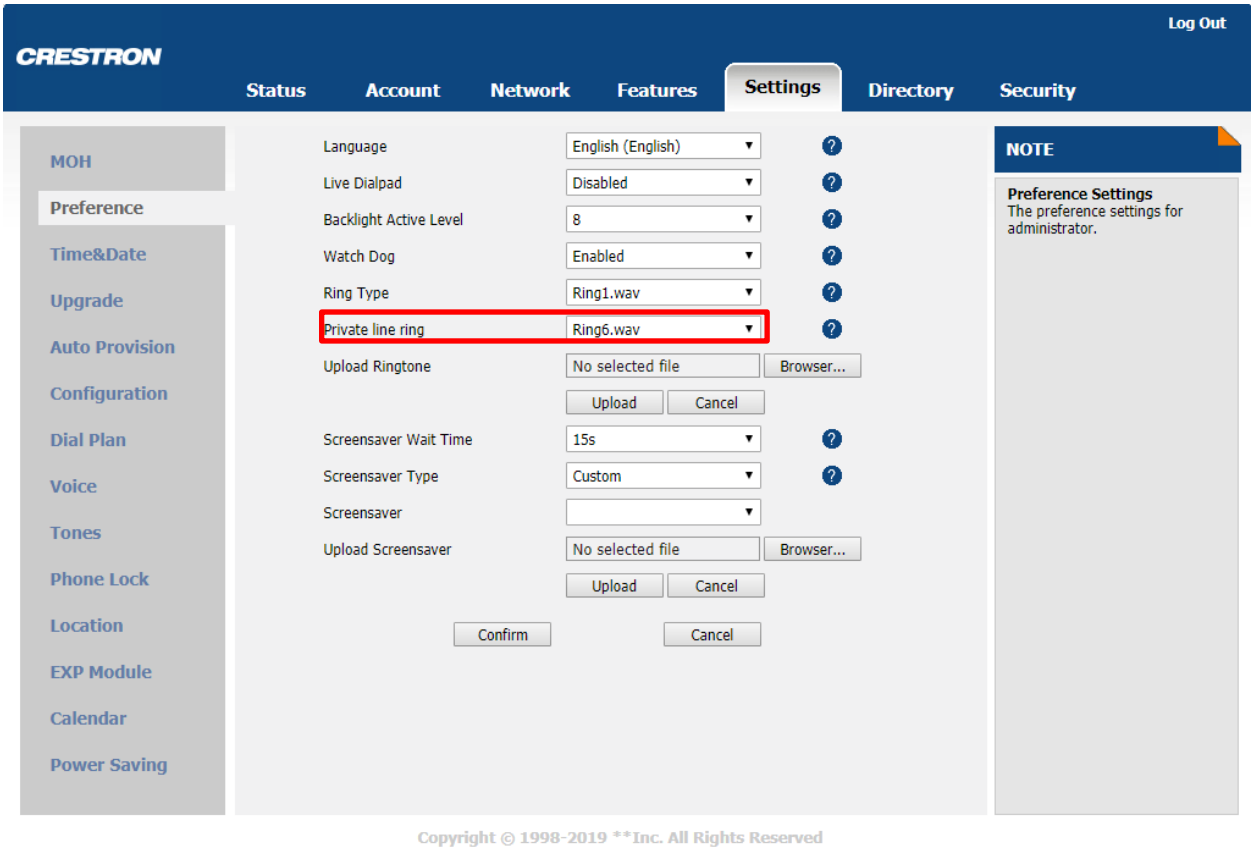
Details of the Configuration Parameters

Parameter	Permitted Values	Default
phone_setting.private_line_ring.enable	**0 or 1**	**1**
Description: Enables or disables a distinct ring tone for the private line. **0**- Disabled, private call will use the phone's ring tone. The phone's ring tone is configured by the parameter "phone_setting.ring_type". **1**- Enabled, a distinct ring tone can be assigned to the private line. **Web User Interface:** None **Phone User Interface:** None		
phone_setting.private_line_ring_type	**Refer to the following content**	**Ring6.wav**
Description: Configures a ring tone for the private line. **Permitted Values:** Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav, Splash.wav or custom ring tone name (e.g., Customring.wav). **Example:** • **To configure a phone built-in ring tone (e.g., Ring6.wav):** phone_setting.private_line_ring_type = Ring6.wav • **To configure a custom ring tone (e.g., Customring.wav):** phone_setting.private_line_ring_type = Customring.wav **Web User Interface:** Settings > Preference > Private line ring **Phone User Interface:** Menu > Setting > Basic > Sounds > Ring Tones > Private Line		

Change the Ring Tone for the Private Line via the Web User Interface:

1. Click **Settings** > **Preference**.

Settings > Preference



2. Select the ring tone from the **Private line ring** drop-down list.
3. Click **Confirm** to accept the change.

Select a Ring Tone for the Private Line via the Phone User Interface

1. Tap **Setting** > **Basic** > **Sounds** > **Ring Tones** > **Private Line**.
2. Tap a ring tone.
3. Tap **Save**.

Redial Tone

The Redial Tone feature allows the phone to continue to play the dial tone after the preset numbers are input on the predialing screen.

Redial Tone can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure Redial Tone feature. **Parameters:** features.redial_tone
Local	Web User Interface	Configure Redial Tone feature. **Navigate to:** http://<phoneIPAddress>/servlet?p =features-audio&q=load

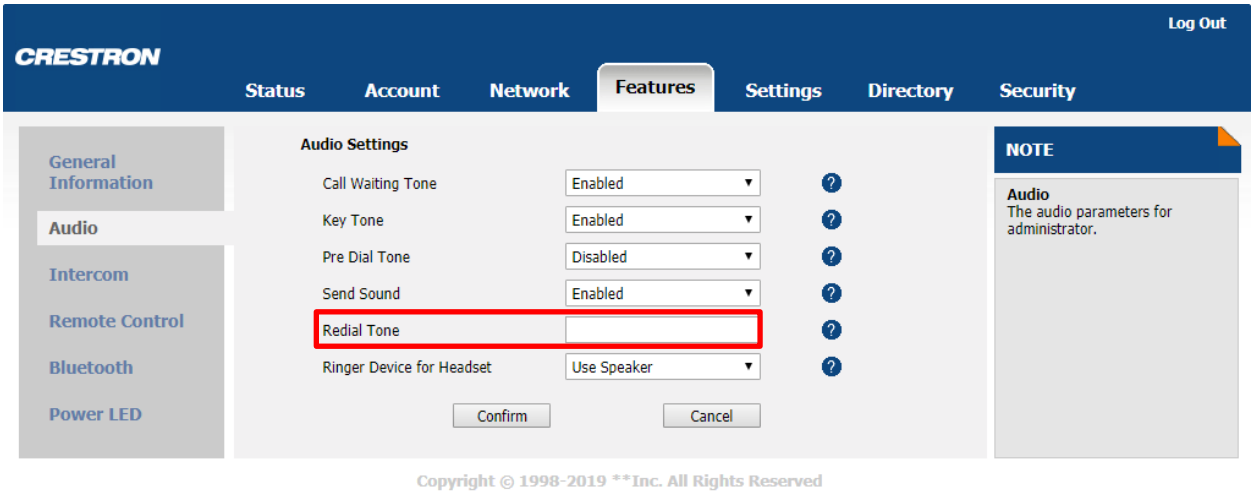
Details of the Configuration Parameter

Parameter	Permitted Values	Default
features.redial_tone	**Integer within 6 digits**	**Blank**
Description: Configures the phone to continue to play the dial tone after the preset numbers are input on the predialing screen. **Example:** features.redial_tone = 125 The phone will continue to play the dial tone after inputting "125" on the predialing screen. If it is left blank, the phone will not play the dial tone after inputting numbers on the predialing screen. **Web User Interface:** Features > Audio > Redial Tone **Phone User Interface:** None		

Configure Redial Tone via the Web User Interface

1. Click **Features** > **Audio**.

Features > Audio



2. Enter the redial tone in the **Redial Tone** field.
3. Click **Confirm** to accept the change.

Tones

When receiving a message, the phone will play a warning tone. Customized tones or select specialized tone sets (vary from country to country) can be used to indicate different conditions of the phone. The default tones used on phones are the US tone sets. Available tone sets for phones:

- Australia
- Austria
- Brazil
- Belgium
- Chile
- China
- Czech
- Czech ETSI
- Denmark
- Finland
- France
- Germany
- Great Britain
- Greece
- Hungary
- Lithuania
- India
- Italy
- Japan
- Mexico
- New Zealand
- Netherlands
- Norway
- Portugal
- Spain

- Switzerland
- Sweden
- Russia
- United States

Configured tones can be heard on phones for the following conditions.

Phone Conditions

Condition	Description
Dial	When in the predialing interface
Ringback	Ringback tone
Busy	When the callee is busy
Congestion	When the network is congested
Call Waiting	Call waiting tone (For more information on call waiting, refer to "Call Waiting" on page 194)
Dial Recall	When receiving a call back
Info	When receiving a special message
Stutter	When receiving a voice mail
Auto Answer	When automatically answering a call (For more information on auto answer, refer to "Auto Answer" on page 197)

Tones can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the tones for the phone. **Parameters:** voice.tone.country voice.tone.dial voice.tone.ring voice.tone.busy voice.tone.congestion voice.tone.callwaiting voice.tone.dialrecall voice.tone.info voice.tone.stutter voice.tone.autoanswer
Local	Web User Interface	Configure the tones for the phone. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-tones&q=load

Details of the Configuration Parameters

PARAMETER	Permitted Values	Default
voice.tone.country	**Refer to the following content**	**Custom**
Description: Configures the country tone for the phone. **Permitted Values:** Custom, Australia, Austria, Brazil, Belgium, Chile, China, Czech, Czech ETSI, Denmark, Finland, France, Germany, Great Britain, Greece, Hungary, Lithuania, India, Italy, Japan, Mexico, New Zealand, Netherlands, Norway, Portugal, Spain, Switzerland, Sweden, Russia, United States. **Example:** voice.tone.country = Custom **Web User Interface:** Settings > Tones > Select Country **Phone User Interface:** None		
voice.tone.dial	**String**	**Blank**
Description: Customizes the dial tone. tonelist = element[,element] [,element]... **Where** • **element** = [!]Freq1[+Freq2][+Freq3][+Freq4] /Duration • **Freq**: the frequency of the tone (ranges from 200 to 4000Hz). If it is set to 0Hz, 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. Eight different tones can be configured for one condition, and must be separated by commas. (e.g., 250/200,0/1000,200+300/500,200+500+800+1500/1000). To have the phone to play tones once, add an exclamation mark "!" before tones (i.e., !250/200,0/1000,200+300/500,200+500+800+1500/1000). **Note:** This feature works only if the value of the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings > Tones > Dial **Phone User Interface:** None		

PARAMETER	Permitted Values	Default
voice.tone.ring	String	Blank
Description: Customizes the ringback tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note:** This feature works only if the value of the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings > Tones > Ring Back **Phone User Interface:** None		
voice.tone.busy	String	Blank
Description: Customizes the tone when the callee is busy. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note:** This feature works only if the value of the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings > Tones > Busy **Phone User Interface:** None		
voice.tone.congestion	String	Blank
Description: Customizes the tone when the network is congested. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note:** This feature works only if the value of the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings > Tones > Congestion **Phone User Interface:** None		
voice.tone.callwaiting	String	Blank
Description: Customizes the call waiting tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note:** This feature works only if the value of the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings > Tones > Call Waiting **Phone User Interface:** None		

PARAMETER	Permitted Values	Default
voice.tone.dialrecall	String	Blank
Description: Customizes the call back tone. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note:** This feature works only if the value of the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings > Tones > Dial Recall **Phone User Interface:** None		
voice.tone.info	String	Blank
Description: Customizes the info tone. The phone will play the info tone with the special information, for example, "The number you are calling is not in service." The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note:** This feature works only if the value of the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings > Tones > Info **Phone User Interface:** None		
voice.tone.stutter	String	Blank
Description: Customizes the tone when the phone receives a voice mail. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note:** This feature works only if the value of the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings > Tones > Stutter **Phone User Interface:** None		

PARAMETER	Permitted Values	Default
voice.tone.autoanswer	String	Blank

Description:

Customizes the warning tone for auto answer.

The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial".

Note: This feature works only if the value of the parameter "voice.tone.country" is set to Custom.

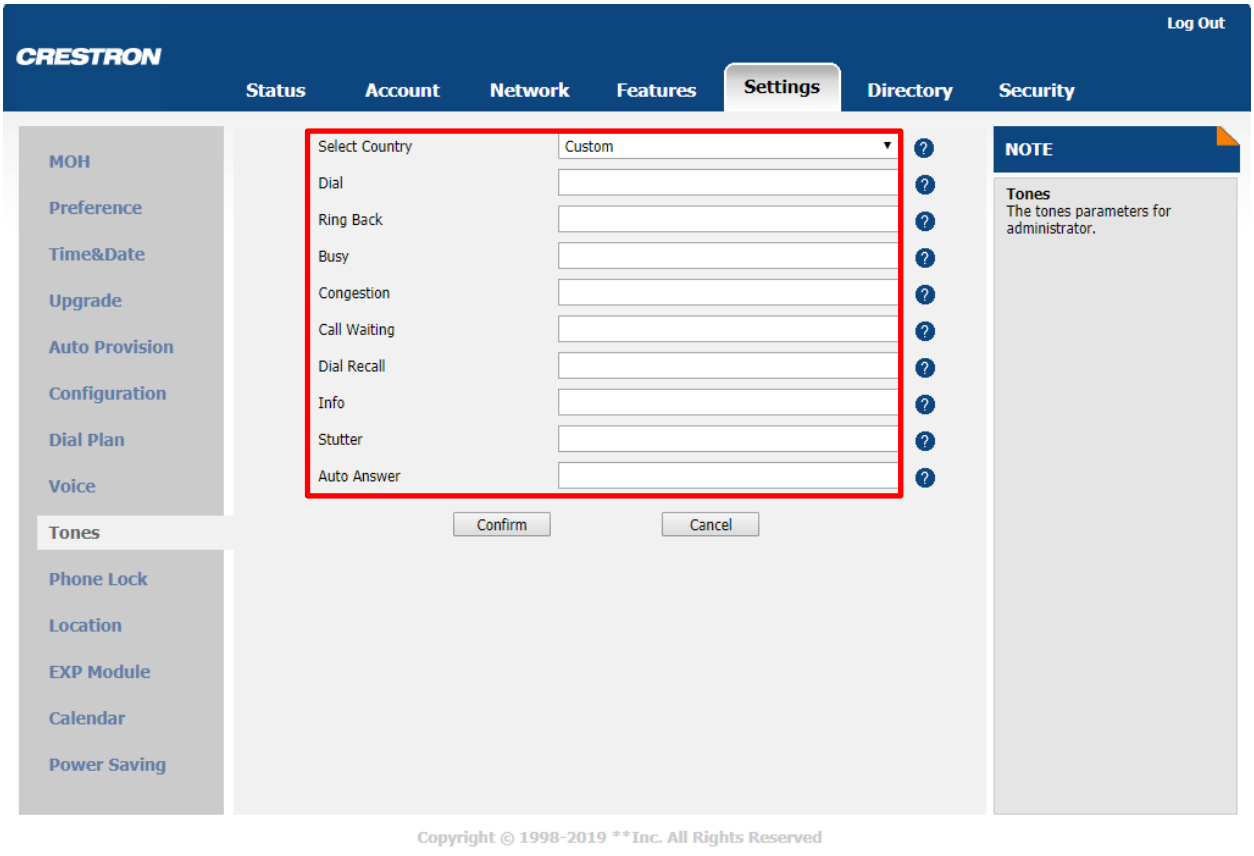
Web User Interface:
Settings > Tones > Auto Answer

Phone User Interface:
None

Configure Tones via the Web User Interface

1. Click **Settings** > **Tones**.

Settings > Tones



2. Select the country from the **Select Country** drop-down list.

   If **Custom** is selected, a tone can be customized for each condition of the phone.

3. Click **Confirm** to accept the change.

Voice Mail Tone

The Voice Mail Tone feature allows the phone to play a warning tone when receiving a new voice mail. The warning tone can be customized or specialized tone sets (vary from country to country) can be selected for the phone.

Voice Mail Tone can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure whether to play a warning tone when the phone receives a new voice mail. **Parameter:** features.voice_mail_tone_enable
Local	Web User Interface	Configure whether to play a warning tone when the phone receives a new voice mail. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

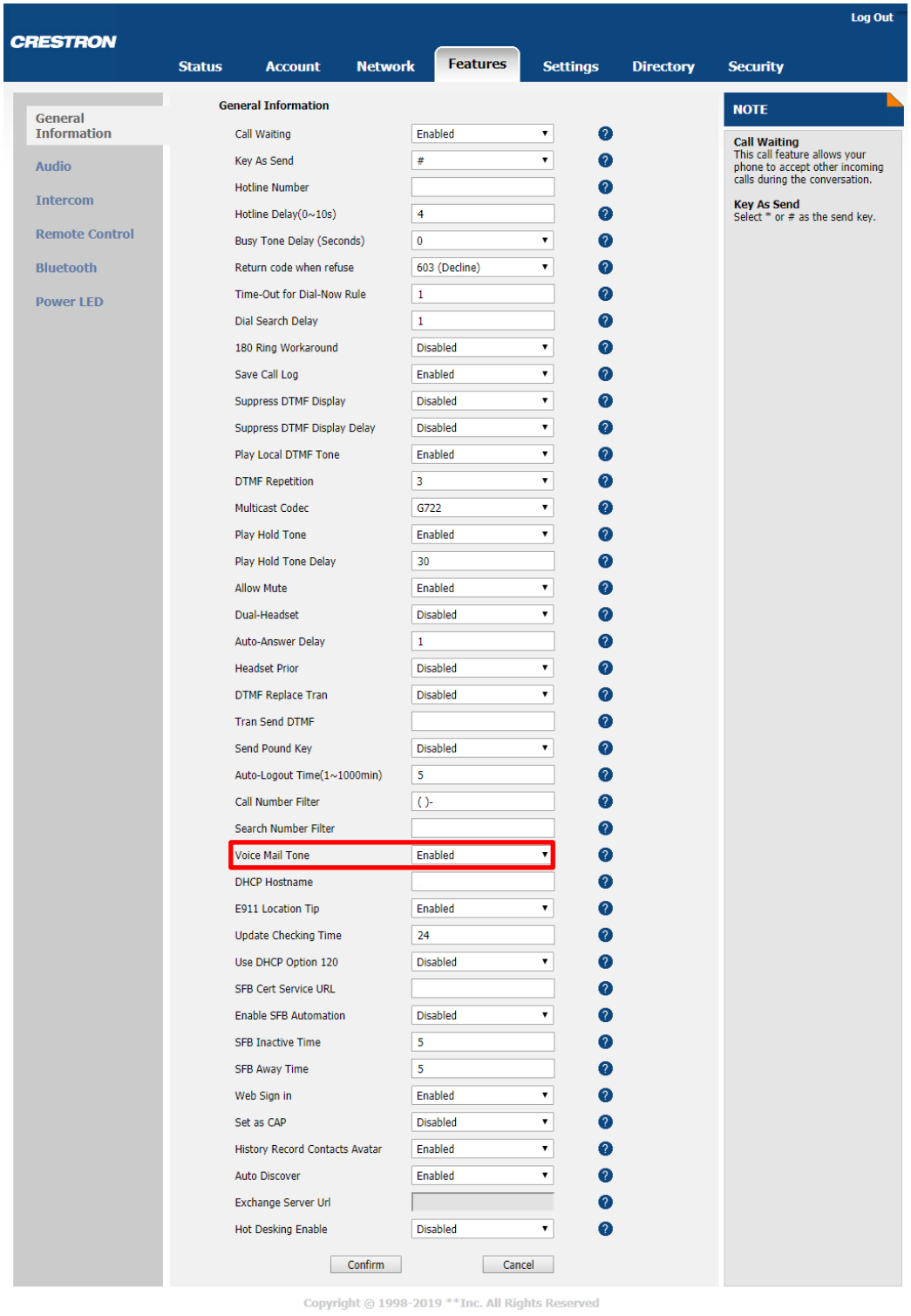
Details of the Configuration Parameter

Parameter	Permitted Values	Default
features.voice_mail_tone_enable	**0 or 1**	**1**
Description: Enables or disables playing a warning tone when the phone receives a new voice mail. **0**- Disabled **1**- Enabled **Web User Interface:** Features > General Information > Voice Mail Tone **Phone User Interface:** None		

Configure Voice Mail Tone via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Select **Enabled** or **Disabled** from the **Voice Mail Tone** drop-down list.
3. Click **Confirm** to accept the change.

Headset Prior

The Headset Prior feature allows users to use headset preferentially if a headset is physically connected to the phone. This feature is especially useful for permanent or full-time headset users.

Headset prior can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure headset prior. **Parameter:** features.headset_prior
Local	Web User Interface	Configure headset prior. **Navigate to**: http://<phoneIPAddress>/servlet?p=features- general&q=load

Details of the Configuration Parameter

Parameter	Permitted Values	Default
features.headset_prior	**0 or 1**	**0**

Description:

Enables or disables preferential use of headset mode for all incoming calls and outgoing calls.

0- Disabled, the headset mode can be deactivated by pressing the speakerphone key or the HEADSET key except the HANDSET key.

1- Enabled, the headset mode will not be deactivated until the user presses the HEADSET key again.

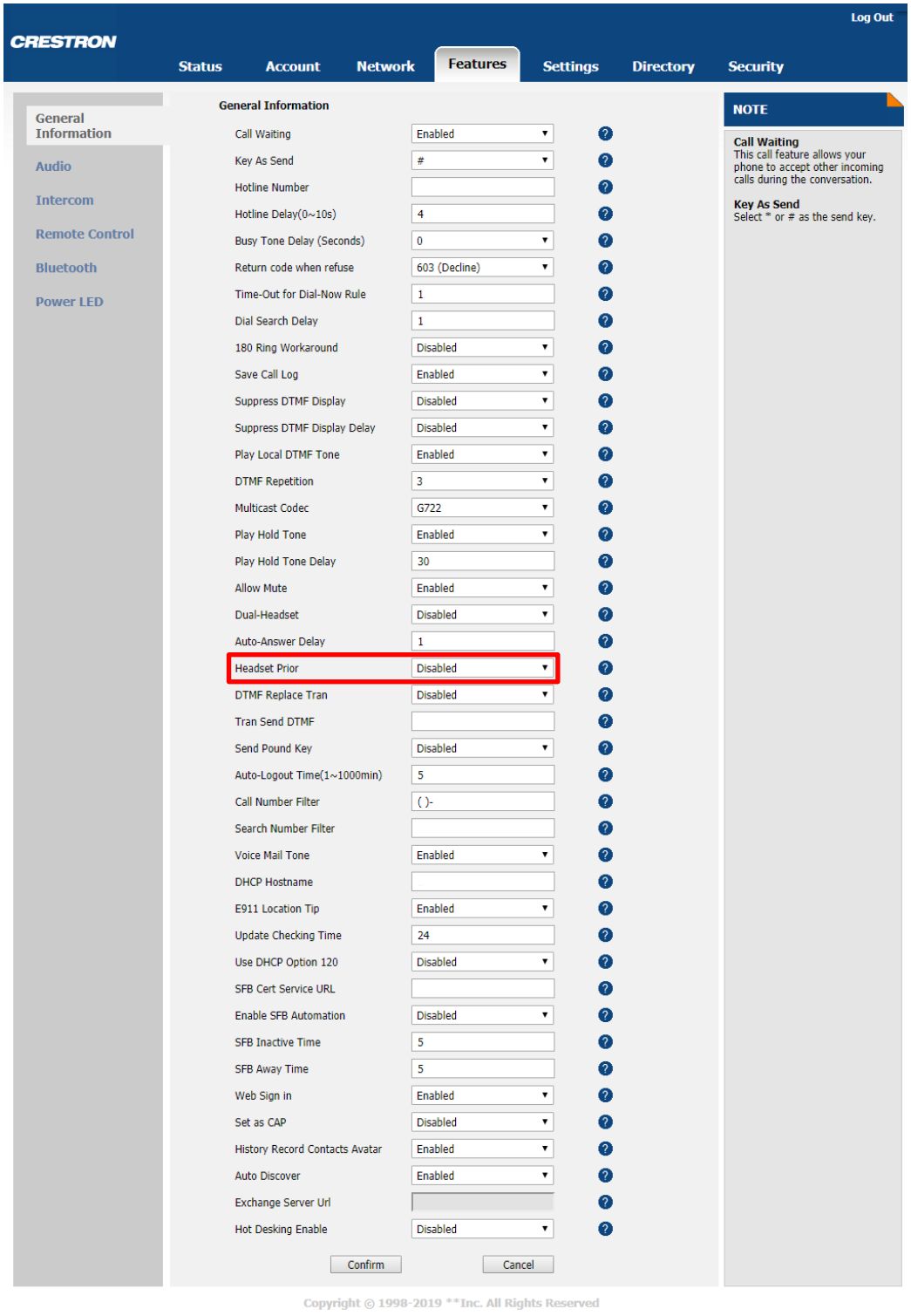
Web User Interface:
Features > General Information > Headset Prior

Phone User Interface:
None

Configure Headset Prior via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Select **Enabled** or **Disabled** from the **Headset Prior** drop-down list.
3. Click **Confirm** to accept the change.

Ringer Device for Headset

The Skype for Business phones support speaker and headset ringer devices. The phone can be configured to specify which ringer device is to be used when receiving an incoming call. For example, if the ringer device is set to **Headset**, the ring tone will be played through the headset.

If the ringer device is set to **Headset** or **Headset&Speaker**, the headset should be connected to the phone and headset mode should be activated in advance. Press the **HEADSET** key to activate headset mode.

Ringer device for headset can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the ringer device for the phone. **Parameter:** features.ringer_device.is_use_headset
Local	Web User Interface	Configure the ringer device for the phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-audio&q=load

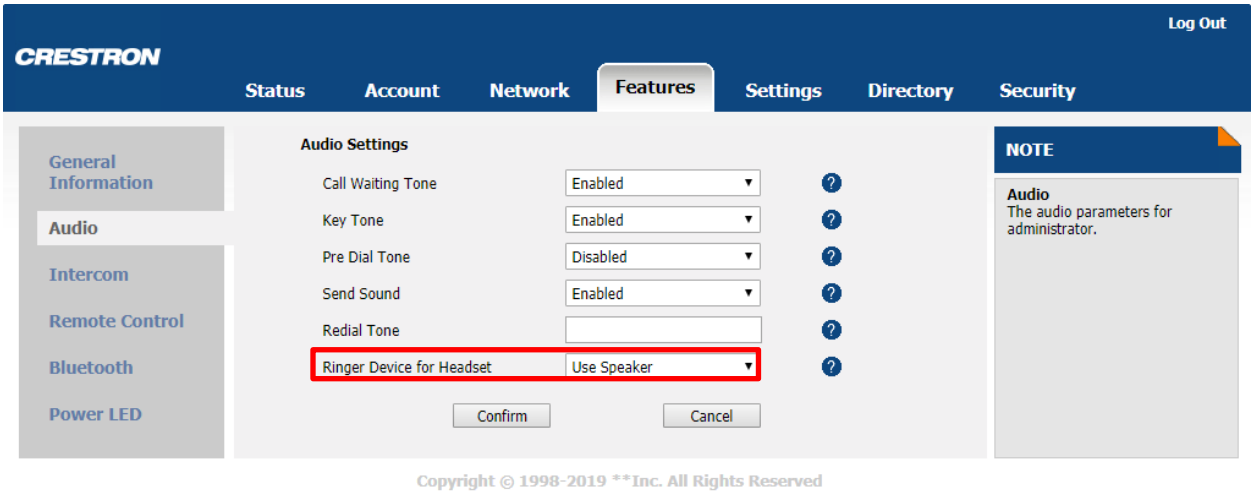
Details of the Configuration Parameter

Parameter	Permitted Values	Default
features.ringer_device.is_use_headset	**0, 1 or 2**	**0**
Description: Configures the ringer device for the phone. **0**- Use Speaker **1**- Use Headset **2**- Use Headset & Speaker If the ringer device is set to Headset or Headset&Speaker, the headset should be connected to the phone and headset mode should be activated in advance. **Web User Interface:** Features > Audio > Ringer Device for Headset **Phone User Interface:** None		

Configure Ringer Device for Headset via the Web User Interface

1. Click **Features > Audio**.

Features > Audio



2. Select the ringer device for the headset from the **Ringer Device for Headset** drop-down list.
3. Click **Confirm** to accept the change.

Dual Headset

The Dual Headset featureallows the use of two headsets on one phone. To use this feature, two headsets must be physically connected to the headset and handset jacks respectively. Once the phone connects to a call, the user with the headset connected to the headset jack has full-duplex capabilities, while the user with the headset connected to the handset jack is only able to listen.

Dual headset can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure dual headset. **Parameter:** features.headset_training
Local	Web User Interface	Configure dual headset. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of the Configuration Parameter

Parameter	Permitted Values	Default
features.headset_training	0 or 1	0

Description:

Enables or disables dual headset feature.

0- Disabled

1- Enabled, users can use two headsets on one phone. When the phone joins in a call, the users with the headset connected to the headset jack have a full-duplex conversation, while the users with the headset connected to the handset jack are only allowed to listen to.

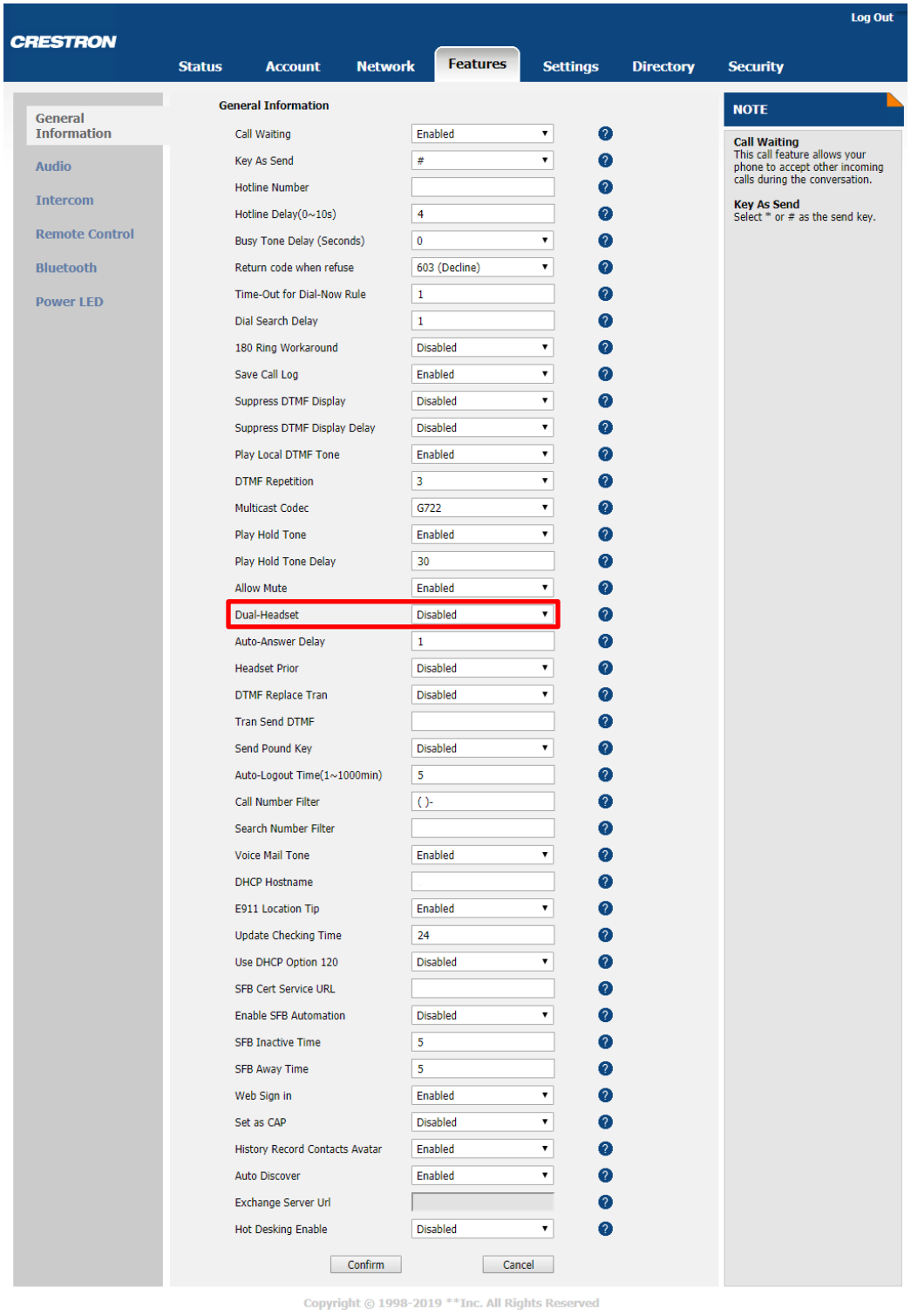
Web User Interface:
Features > General Information > Dual-Headset

Phone User Interface:
None

Configure Dual Headset via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Select **Enabled** or **Disabled** from the **Dual Headset** drop-down list.
3. Click **Confirm** to accept.

Sending Volume

Configure the sending volume of currently engaged audio devices (handset, speakerphone, or headset) when the phone is in use.

Sending volume can be configured using the configuration files only.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the sending volume of the speaker. **Parameter:** voice.handfree_send
		Configure the sending volume of the handset. **Parameter:** voice.handset_send
		Configure the sending volume of the headset. **Parameter:** voice.headset_send

Details of the Configuration Parameters

Parameter	Permitted Values	Default
voice.handfree_send	**Integer from -50 to 50**	**0**
Description: Configures the sending volume of the speaker. **Note:** We recommend that this parameter be modified cautiously. An unreasonable value may render the voice quality bad. If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** None		

Parameter	Permitted Values	Default
voice.handset_send	Integer from -50 to 50	0
Description: Configures the sending volume of the handset. **Note:** We recommend that this parameter be modified cautiously. An unreasonable value may render the voice quality bad. If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** None		
voice.headset_send	Integer from -50 to 50	0
Description: Configures the sending volume of the headset. **Note:** We recommend that this parameter be modified cautiously. An unreasonable value may render the voice quality bad. If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** None		

Audio Codecs

CODEC is an abbreviation of COder-DECoder, capable of encoding or decoding a digital data stream or signal by implementing an algorithm. The object of the algorithm is to represent a high-fidelity audio signal with a minimum number of bits. This can effectively reduce the frame size and the bandwidth required for audio transmission.

The audio codec the phone uses to establish a call should be supported by the SIP server. When placing a call, the phone will offer the enabled audio codec list to the server and then use the audio codec negotiated with the called party according to the priority.

The following table lists the audio codecs supported:

Supported Audio Codecs

Supported Audio Codecs	Default Audio Codecs
G722, PCMA, PCMU, G729, G726-16, G726-24, G726-32, G726-40, iLBC, G723_53, G723_63, SILK_NB, SILK_WB	G722, PCMA, PCMU, G729

The following table summarizes the supported audio codecs on phones:

Audio Codec Details

Codec	Algorithm	Reference	Bitrate	Sample Rate	Packetization Time
G722	G.722	RFC 3551	64 Kbps	16	20ms
PCMA	G.711 a-law	RFC 3551	64 Kbps	8 Ksps	20ms
PCMU	G.711 u-law	RFC 3551	64 Kbps	8 Ksps	20ms

Codec	Algorithm	Reference	Bitrate	Sample Rate	Packetization Time
G729	G.729	RFC 3551	8 Kbps	8 Ksps	20ms
G726-16	G.726	RFC 3551	16 Kbps	8 Ksps	20ms
G726-24	G.726	RFC 3551	24 Kbps	8 Ksps	20ms
G726-32	G.726	RFC 3551	32 Kbps	8 Ksps	20ms
G726-40	G.726	RFC 3551	40 Kbps	8 Ksps	20ms
G723_53/ G723_63	G.723.1	RFC 3551	5.3kbps 6.3kbps	8 Ksps	30ms
iLBC	iLBC	RFC 3952	15.2 Kbps 13.33 Kbps	8 Ksps	20ms 30ms
SILK_NB	SILK_NB	draft-vos-silk-01	12 Kbps	8 Ksps	20ms
SILK_WB	SILK_WB	draft-vos-silk-01	20 Kbs	16 Ksps	20ms

Packetization Time

Ptime (Packetization Time) is a measurement of the duration (in milliseconds) of the audio data in each RTP packet sent to the destination, and defines how much network bandwidth is used for the RTP stream transfer. Before establishing a conversation, codec and ptime are negotiated through SIP signaling. The valid values of ptime range from 10 to 60, in increments of 10 milliseconds. The default ptime is 20ms. Ptime negotiation can also be disabled.

The attribute "rtpmap" is used to define a mapping from RTP payload codes to a codec, clock rate and other encoding parameters.

The corresponding attributes of the codec are:

Codec Attributes

Codec	Configuration	Priority	RTPmap
G722	Configuration Files Web User Interface	1	9
PCMU	Configuration Files Web User Interface	2	0
PCMA	Configuration Files Web User Interface	3	8
G729	Configuration Files Web User Interface	4	18
G723_53	Configuration Files Web User Interface	0	4
G723_63	Configuration Files Web User Interface	0	4
G726-16	Configuration Files Web User Interface	0	103
G726-24	Configuration Files Web User Interface	0	104
G726-32	Configuration Files Web User Interface	0	102

Codec	Configuration	Priority	RTPmap
G726-40	Configuration Files Web User Interface	0	105
iLBC	Configuration Files Web User Interface	0	106
SILK_WB	Configuration Files Web User Interface	0	119
SILK_NB	Configuration Files Web User Interface	0	120

Configuration changes can be performed using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<MAC>.cfg**	Configure the codecs to be used. **Parameters:** static.account.1.codec.Y.enable static.account.1.codec.Y.payload_type
		Configure the priority and rtpmap for the enabled codec. **Parameters:** static.account.1.codec.Y.priority static.account.1.codec.Y.rtpmap
Local	Web User Interface	Configure the codecs to be used. Configure the priority for the enabled codec. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-codec&q=load&acc=0

Details of the Configuration Parameters

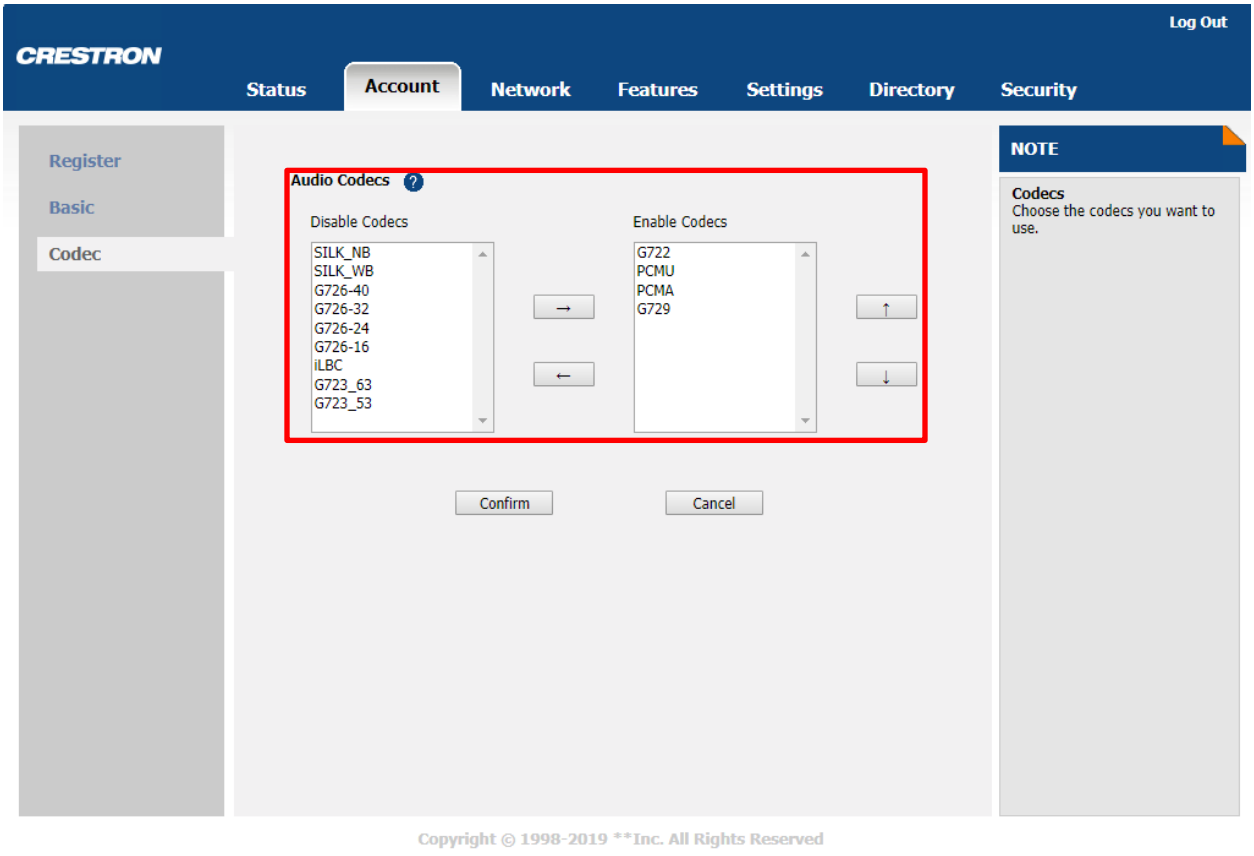
Parameter	Permitted Values	Default
static.account.1.codec.Y.enable (Y ranges from 1 to 13)	**0 or 1**	**Refer to the following content**
Description: Enables or disables the specified codec for the account. **0**- Disabled **1**- Enabled **Default**: When Y=1, the default value is 1; When Y=2, the default value is 1; When Y=3, the default value is 0; When Y=4, the default value is 0; When Y=5, the default value is 1; When Y=6, the default value is 1; When Y=7, the default value is 0; When Y=8, the default value is 0; When Y=9, the default value is 0; When Y=10, the default value is 0; When Y=11, the default value is 0; When Y=12, the default value is 0; When Y=13, the default value is 0; **Example:** static.account.1.codec.1.enable = 1 It means that the codec PCMU is enabled on the account. **Web User Interface:** Account > Codec **Phone User Interface:** None		
static.account.1.codec.Y.payload_type (Y ranges from 1 to 13)	**Refer to the following content**	**Refer to the following content**
Description: Configures the codec for the account. **Permitted Values:** G722, PCMU, PCMA, G729, G726-16, G726-24, G726-32, G726-40, iLBC, G723_53, G723_63, SILK_NB, SILK_WB **Default:** When Y=1, the default value is PCMU; When Y=2, the default value is PCMA; When Y=3, the default value is G723_53;When Y=4, the default value is G723_63; When Y=5, the default value is G729; When Y=6, the default value is G722; When Y=7, the default value is iLBC; When Y=8, the default value is G726-16; When Y=9, the default value is G726-24; When Y=10, the default value is G726-32; When Y=11, the default value is G726-40; When Y=12, the default value is SILK_WB; When Y=13, the default value is SILK_NB; **Example:** static.account.1.codec.1.payload_type = PCMU **Web User Interface:** Account > Codec **Phone User Interface:** None		

Parameter	Permitted Values	Default
static.account.1.codec.Y.priority (Y ranges from 0 to 13)	**Integer from 0 to 12**	**Refer to the following content**
Description: Configures the priority of the codec enabled for the account. **Default:** When Y=1, the default value is 2; When Y=2, the default value is 3; When Y=3, the default value is 0; When Y=4, the default value is 0; When Y=5, the default value is 4; When Y=6, the default value is 1; When Y=7, the default value is 0; When Y=8, the default value is 0; When Y=9, the default value is 0; When Y=10, the default value is 0; When Y=11, the default value is 0; When Y=12, the default value is 0; When Y=13, the default value is 0; **Example:** static.account.1.codec.1.priority = 2 **Web User Interface:** Account > Codec **Phone User Interface:** None		
static.account.1.codec.Y.rtpmap (Y ranges from 1 to 13)	**Integer from 0 to 127**	**Refer to the following content**
Description: Configures the rtpmap of the audio codec for the account. **Default:** When Y=1, the default value is 0; When Y=2, the default value is 8; When Y=3, the default value is 4; When Y=4, the default value is 4; When Y=5, the default value is 18; When Y=6, the default value is 9; When Y=7, the default value is 106; When Y=8, the default value is 103; When Y=9, the default value is 104; When Y=10, the default value is 102; When Y=11, the default value is 105; When Y=12, the default value is 119; When Y=13, the default value is 120; **Example:** static.account.1.codec.1.rtpmap = 0 **Web User Interface:** None **Phone User Interface:** None		

Configure the Codecs to be Used and Adjust the Priority of the Enabled Codecs via the Web User Interface

1. Click **Account** > **Codec**.

Account > Codec



2. Select the codec to be enabledfrom the **Disable Codecs** column andthen click → The selected codec appears in the **Enable Codecs** column.
3. Repeat the step 3 to add more codecs to the **Enable Codecs** column.
4. To remove the codec from the **Enable Codecs** column, select the codec to be removed and then click ←.
5. To adjust the priority of codecs, select the codec to reprioritize and then click ↑ or ↓.
6. Click **Confirm** to accept the changes.

Acoustic Clarity Technology

Acoustic Echo Cancellation (AEC)

Skype for Business phones employ advanced AEC for hands-free operation. The AEC feature can be configured to remove the echo of the local loudspeaker from the local microphone without removing the near-end speech.

AEC is not normally required for calls via the handset. In some cases, where echo is experienced by the remote party, AEC may be used to reduce or avoid echo when the user employs the handset.

NOTE: Utilizing Acoustic Echo Cancellation will introduce a small delay into the audio path which might cause lower voice quality.

AEC can be configured using the configuration files or via web user interface.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure AEC. **Parameter:** voice.echo_cancellation
Local	Web User Interface	Configure AEC. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings- voice&q=load

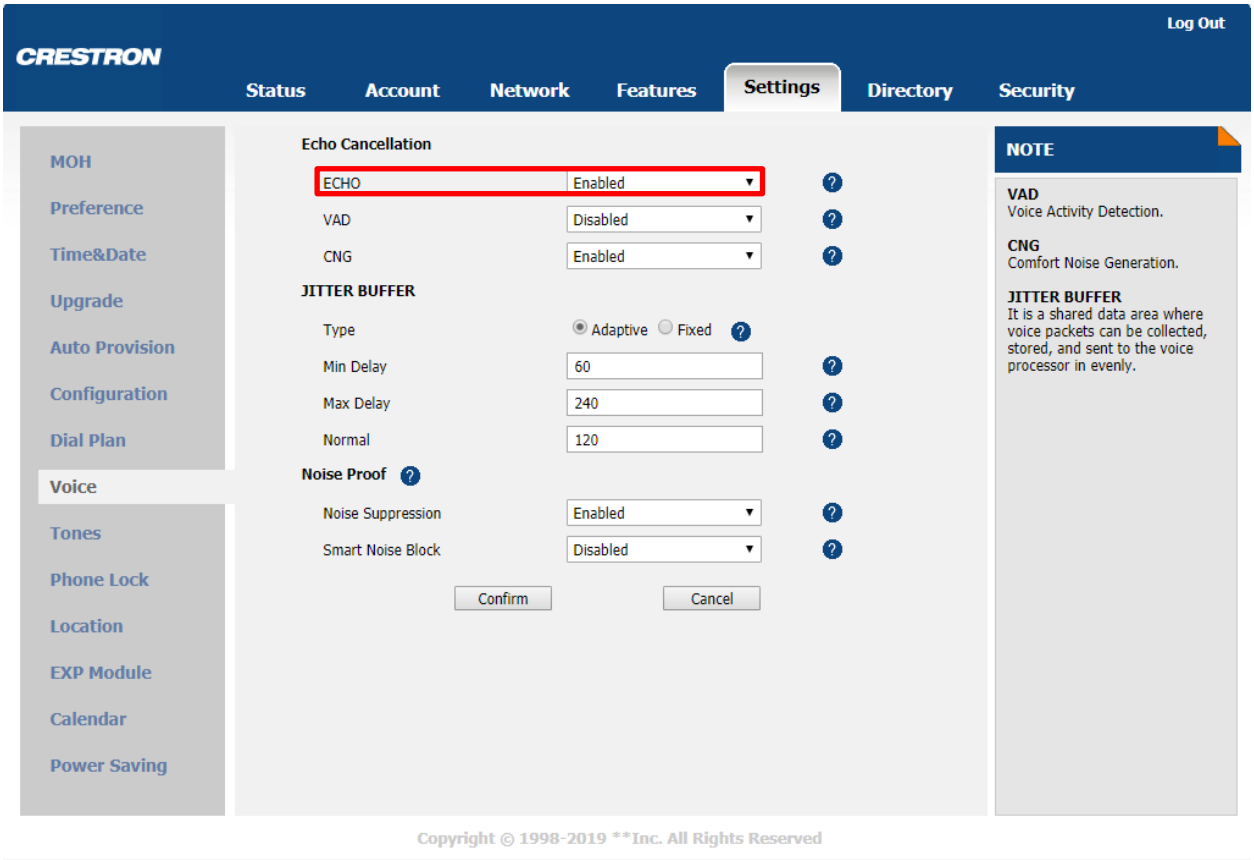
Details of the Configuration Parameter

Parameter	Permitted Values	Default
voice.echo_cancellation	**0 or 1**	**1**
Description: Enables or disables the AEC (Acoustic Echo Canceller) feature on the phone. **0**- Disabled **1**- Enabled **Web User Interface:** Settings > Voice > Echo Cancellation > ECHO **Phone User Interface:** None		

Configure AEC via the Web User Interface

1. Click **Settings** > **Voice**.

Settings > Voice



2. Select **Enabled** or **Disabled** from the **ECHO** drop-down list.
3. Click **Confirm** to accept the change.

Voice Activity Detection

Voice Activity Detection (VAD) can avoid unnecessary coding or transmission of silence packets in VoIP applications, saving on computation and network bandwidth.

VAD can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure VAD. **Parameter:** voice.vad
Local	Web User Interface	Configure VAD. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-voice&q=load

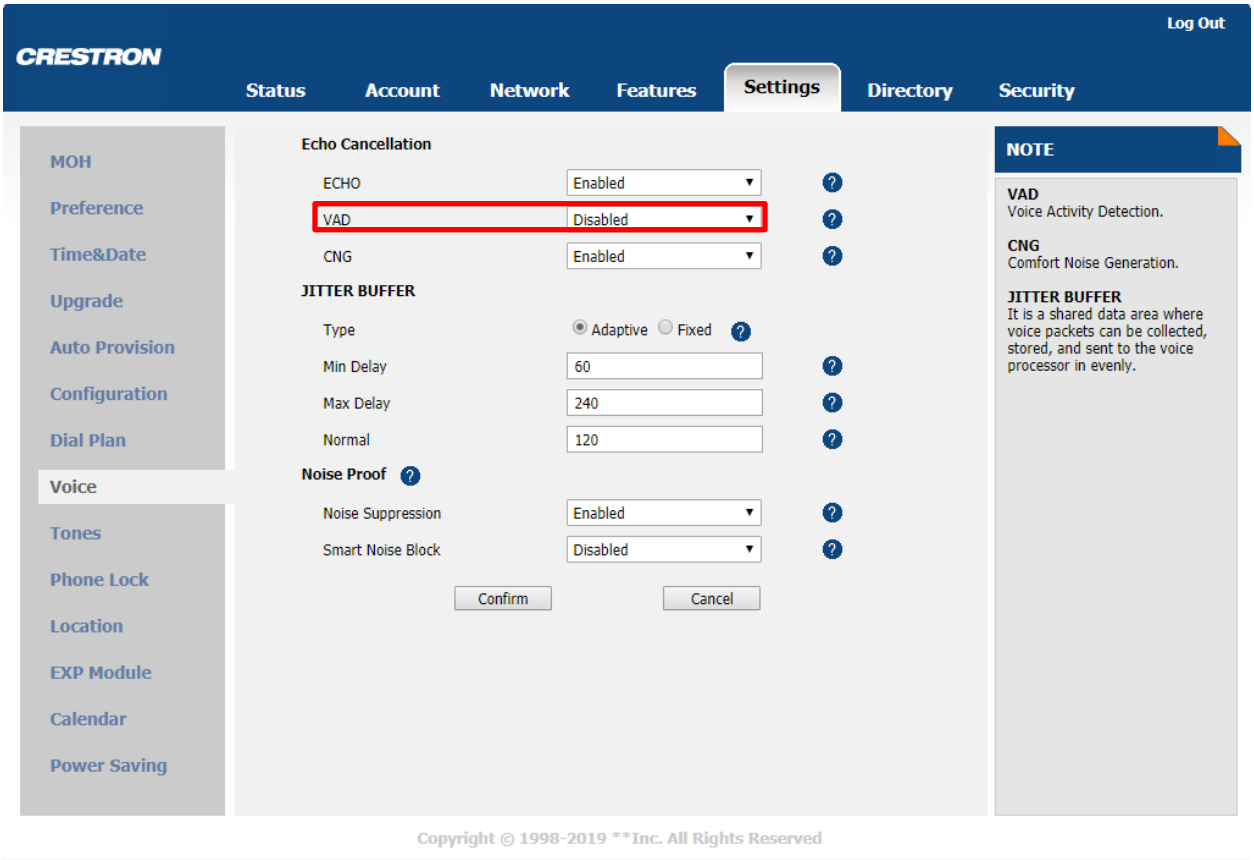
Details of the Configuration Parameter

Parameter	Permitted Values	Default
voice.vad	**0 or 1**	**0**
Description: Enables or disables the VAD (Voice Activity Detection) feature on the phone. **0**- Disabled **1**- Enabled **Web User Interface**: Settings > Voice > Echo Cancellation > VAD **Phone User Interface:** None		

Configure VAD via the Web User Interface

1. Click **Settings** > **Voice**.

Settings > Voice



2. Select **Enabled** or **Disabled** from the **VAD** drop-down list.
3. Click **Confirm** to accept the change.

Comfort Noise Generation

Comfort Noise Generation (CNG) is used to generate background noise for voice communications during periods of silence in a conversation.

NOTE: VAD is used to send CN packets when the phone detect silence; CNG is used to generate comfortable noise when the phone receives CN packets from the other side.

For example, A is talking with B. A: VAD=1, CNG=1

B: VAD=0, CNG=1

If A mutes the call, since VAD=1, A will send CN packets to B. When receiving CN packets, B will generate comfortable noise.

If B mutes the call, since VAD=0, B will not send CN packets to A. So even if CNG=1 (B), A will not hear comfortable noise.

CNG can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure CNG. **Parameter:** voice.cng
Local	Web User Interface	Configure CNG. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-voice&q=load

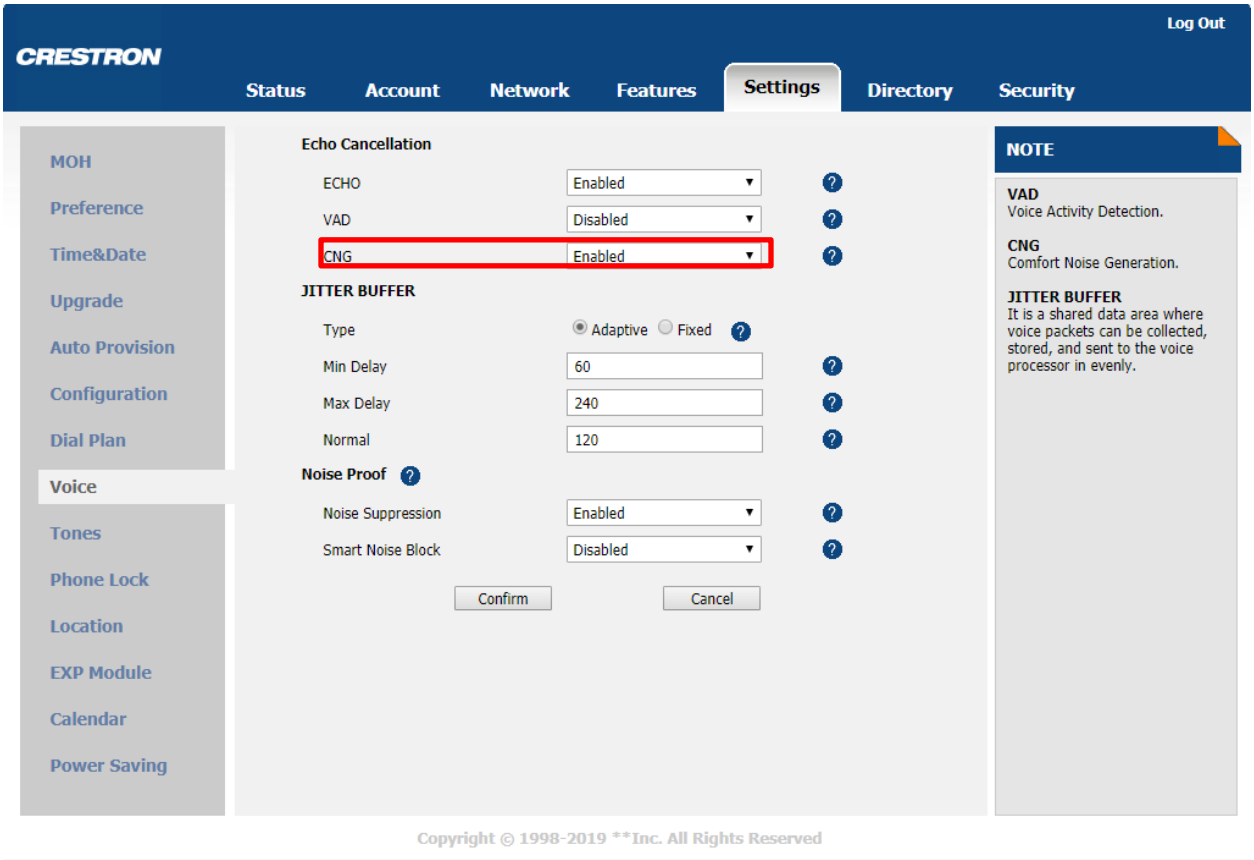
Details of the Configuration Parameter

Parameter	Permitted Values	Default
voice.cng	**0 or 1**	**1**
Description: Enables or disables the CNG (Comfortable Noise Generation) feature on the phone. **0**- Disabled **1**- Enabled **Web User Interface**: Settings > Voice > Echo Cancellation > CNG **Phone User Interface:** None		

Configure CNG via the Web User Interface

1. Click **Settings** > **Voice**.

Settings > Voice



2. Select **Enabled** or **Disabled** from the **CNG** drop-down list.
3. Click **Confirm** to accept the change.

Jitter Buffer

Configure the mode and the delay time for the jitter buffer in the wired network or wireless network.

The jitter buffer can be configured using the configuration files or via web user interface.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the mode of the jitter buffer and the delay time for the jitter buffer. **Parameters:** voice.jib.adaptive voice.jib.min voice.jib.max voice.jib.normal
Local	Web User Interface	Configure the mode of the jitter buffer and the delay time for the jitter buffer. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-voice&q=load

Details of the Configuration Parameters

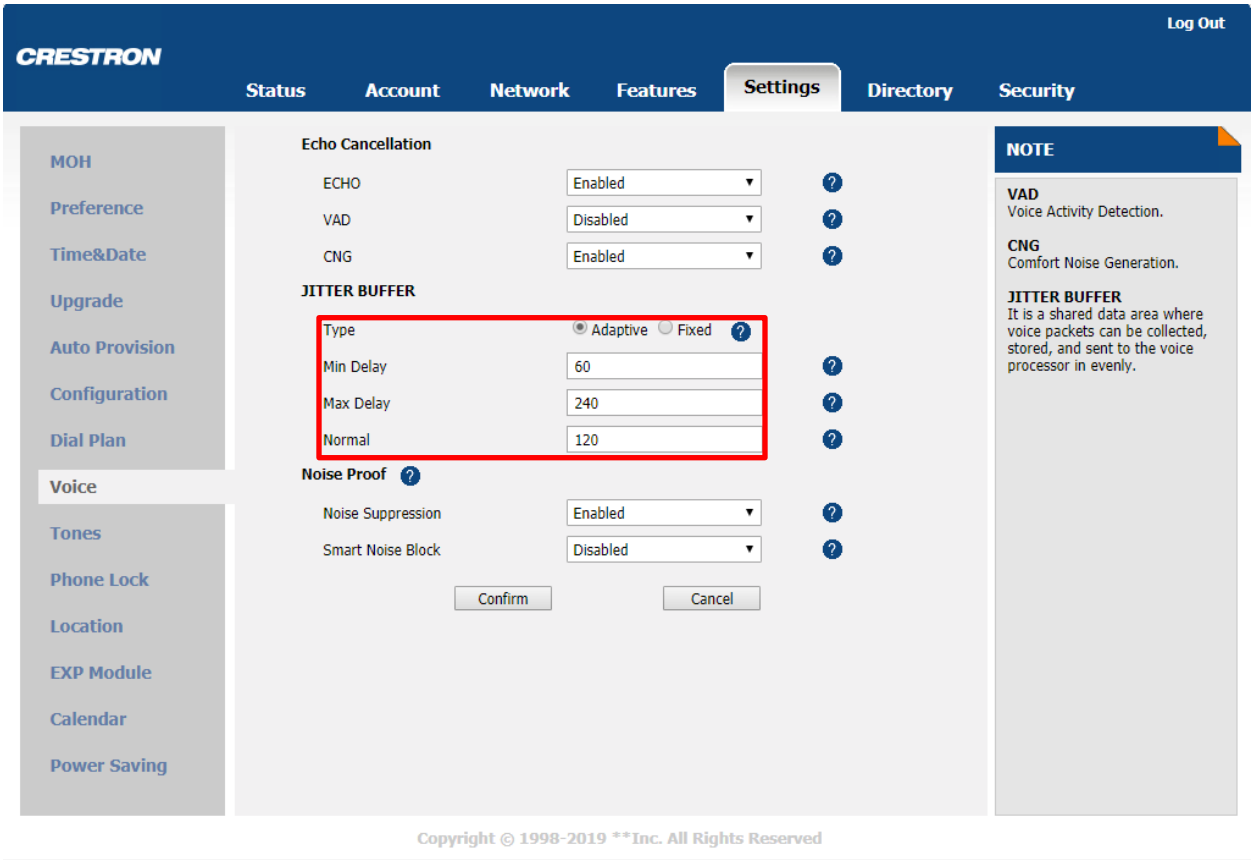
Parameter	Permitted Values	Default
voice.jib.adaptive	**0 or 1**	**1**
Description: Configures the type of jitter buffer. **0**- Fixed **1**- Adaptive **Web User Interface:** Settings > Voice > JITTER BUFFER > Type **Phone User Interface:** None		
voice.jib.min	**Integer from 0 to 400**	**60**
Description: Configures the minimum delay time (in milliseconds) for the jitter buffer. **Note:** This feature works only if the value of the parameter "voice.jib.adaptive" is set to 1 (Adaptive). **Web User Interface:** Settings > Voice > JITTER BUFFER > Min Delay **Phone User Interface:** None		

Parameter	Permitted Values	Default
voice.jib.max	Integer from 0 to 400	240
Description: Configures the maximum delay time (in milliseconds) for the jitter buffer. **Note:** This feature works only if the value of the parameter "voice.jib.adaptive" is set to 1 (Adaptive). **Web User Interface:** Settings > Voice > JITTER BUFFER > Max Delay **Phone User Interface:** None		
voice.jib.normal	Integer from 0 to 400	120
Description: Configures the normal delay time (in milliseconds) for the jitter buffer. **Note:** This feature works only if the value of the parameter "voice.jib.adaptive" is set to 0 (Fixed). **Web User Interface:** Settings > Voice > JITTER BUFFER > Normal **Phone User Interface:** None		

Configure Jitter Buffer via the Web User Interface

1. Click **Settings** > **Voice**.

Settings > Voice



2. Select **Adaptive** or **Fixed** in the **Type** field.
3. Enter the minimum delay time for adaptive jitter buffer in the **Min Delay** field. The valid value ranges from 0 to 300.
4. Enter the maximum delay time for adaptive jitter buffer in the **Max Delay** field. The valid value ranges from 0 to 300.
5. Enter the fixed delay time for fixed jitter buffer in the **Normal** field. The valid value ranges from 0 to 300.
6. Click **Confirm** to accept the changes.

Noise Suppression

Extraneous noises, when transmitted to remote participants, can be very distracting. Enable the Noise Suppression feature to suppress these.

Noise Suppression can be configured using the following methods:

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure Noise Suppression. **Parameter:** voice.tns.enable
Local	Web User Interface	Configure the Noise Suppression. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-voice&q=load

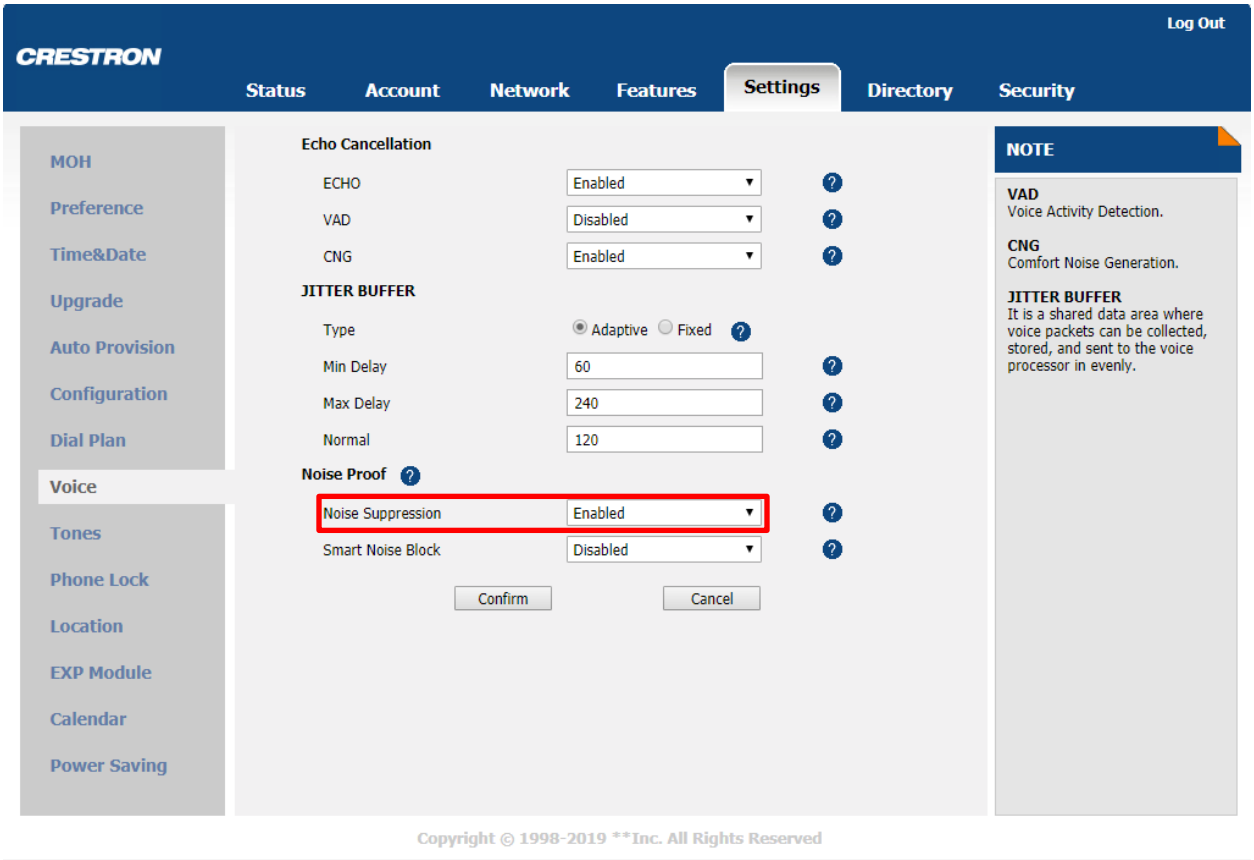
Details of the Configuration Parameter

Parameter	Permitted Values	Default
voice.tns.enable	**0 or 1**	**1**
Description: Enables or disables the Noise Suppression feature on the IP phones. **0**- Disabled **1**- Enabled **Web User Interface:** Settings > Voice > Noise Proof > Noise Suppression **Phone User Interface:** None		

Configure Noise Suppression via the Web User Interface

1. Click **Settings** > **Voice**.

Settings > Voice



2. Select **Enabled** or **Disabled** from the **Noise Suppression** drop-down list.
3. Click **Confirm** to accept the change.

Smart Noise Block

Use the Smart Noise Block feature to block out noises when there is no speech in a call.

Smart Noise Block can be configured using the following methods.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure Smart Noise Block. **Parameter:** voice.ans_nb.enable
Local	Web User Interface	Configure Smart Noise Block. **Navigate to:** http://<phoneIPAddress>/servlet?m=mod_data&p=settings-voice&q=load

Details of the Configuration Parameter

Parameter	Permitted Values	Default
voice.ans_nb.enable	0 or 1	0

Description:

Enables or disables the Smart Noise Block feature on the IP phones.

0- Disabled

1- Enabled

Note: This feature works only if the value of the parameter "voice.tns.enable" is set to 1 (Enabled).

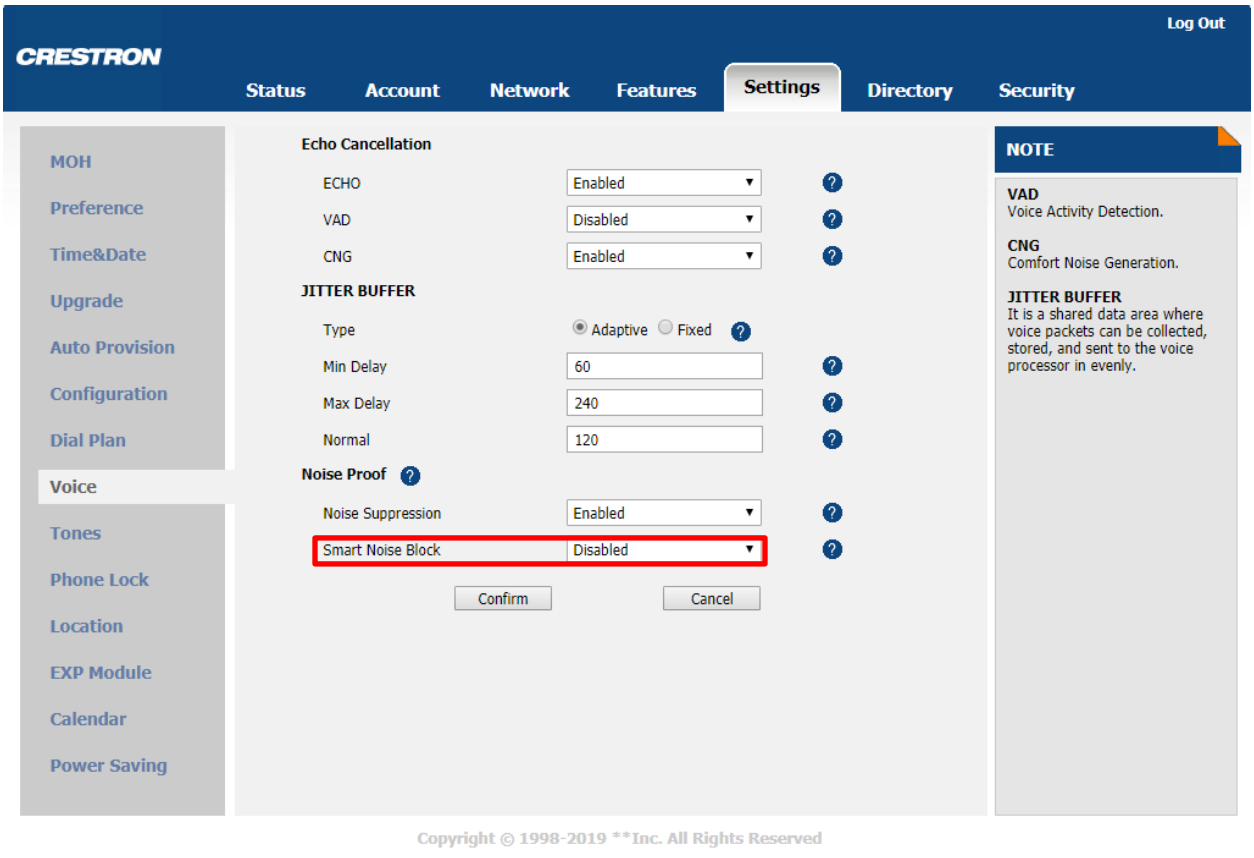
Web User Interface:
Settings > Voice > Noise Proof > Smart Noise Block

Phone User Interface:
None

Configure Smart Noise Block via the Web User Interface

1. Click **Settings** > **Voice**.

Settings > Voice



2. Select **Enabled** or **Disabled** from the **Smart Noise Block** drop-down list.
3. Click **Confirm** to accept the change.

DTMF

DTMF is the signal sent from the phone to the network, generated when pressing the phone's keypad during a call. Each key pressed on the phone generates a tone comprised of two frequencies: a high frequency and a low frequency.

The DTMF keypad is laid out in a 4×4 matrix, with each row representing a low frequency, and each column representing a high frequency. Pressing a digit key (such as '1') will generate a tone for each of two frequencies (697 and 1209 hertz (Hz)).

DTMF Keypad Frequencies

	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

Methods of Transmitting a DTMF Digit

DTMF digits are transmitted by RTP Events compliant with RFC 2833. The payload type and sending times of the end RTP Event packet can be configured. The RTP Event packet contains 4 bytes. The 4 bytes are distributed over several fields denoted as Event, End bit, R-bit, Volume and Duration. If the End bit is set to 1, the packet contains the end of the DTMF event. The sending times of the end RTP Event packet can be configured.

Configuration changes can be performed using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the number of times for the phone to send the end RTP Event packet. **Parameter:** features.dtmf.repetition
Local	Web User Interface	Configure the number of times for the phone to send the end RTP Event packet. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

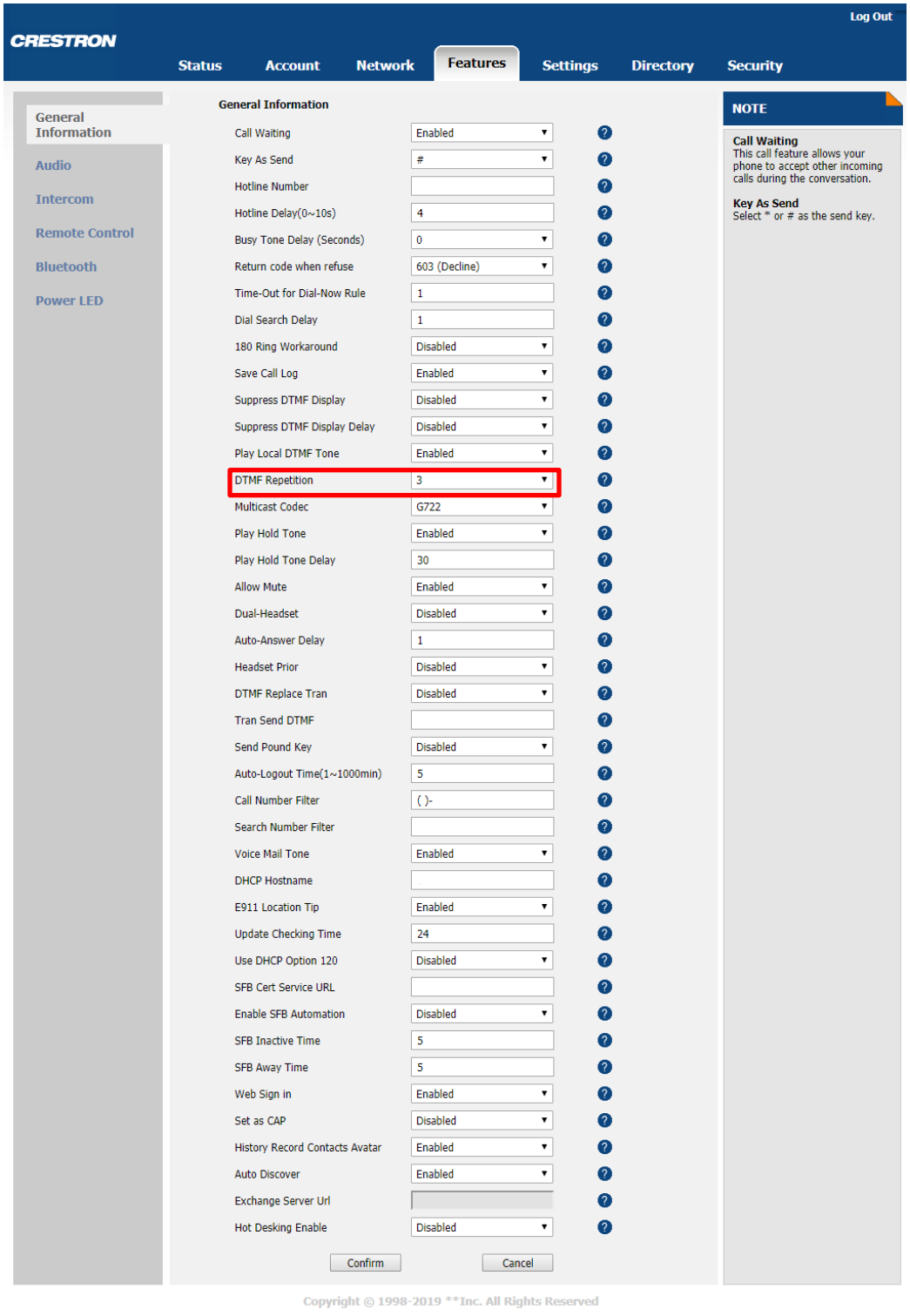
Details of the Configuration Parameter

Parameter	Permitted Values	Default
features.dtmf.repetition	1, 2 or 3	3
Description: Configures the repetition times for sending the end RTP Event packet during an active call. **Web User Interface:** Features > General Information > DTMF Repetition **Phone User Interface:** None		

Configure the Number of Times to Send the End RTP Event packet via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Select the amount of repetition (**1**-**3**) from the **DTMF Repetition** drop-down list.
3. Click **Confirm** to accept the change.

Suppress DTMF Display

The Suppress DTMF Display feature allows phones to suppress the display of DTMF digits during an active call. DTMF digits are displayed as "*" on the LCD screen. The Suppress DTMF Display delay defines whether to display the DTMF digits for a short period of time before displaying as "*".

Configuration changes can be performed using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure Suppress DTMF Display and Suppress DTMF Display delay. **Parameters:** **f**eatures.dtmf.hide features.dtmf.hide_delay
Local	Web User Interface	Configure Suppress DTMF Display and Suppress DTMF Display delay. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of the Configuration Parameters

Parameter	Permitted Values	Default
features.dtmf.hide	**0 or 1**	**0**
Description: Enables or disables the phone to suppress the display of DTMF digits during an active call. **0**- Disabled **1**- Enabled, the DTMF digits are displayed as asterisks. **Web User Interface:** Features > General Information > Suppress DTMF Display **Phone User Interface:** None		

Parameter	Permitted Values	Default
features.dtmf.hide_delay	0 or 1	0

Description:

Enables or disables the phone to display the DTMF digits for a short period before displaying asterisks during an active call.

0- Disabled

1- Enabled

Note: This feature works only if the value of the parameter "features.dtmf.hide" is set to 1 (Enabled).

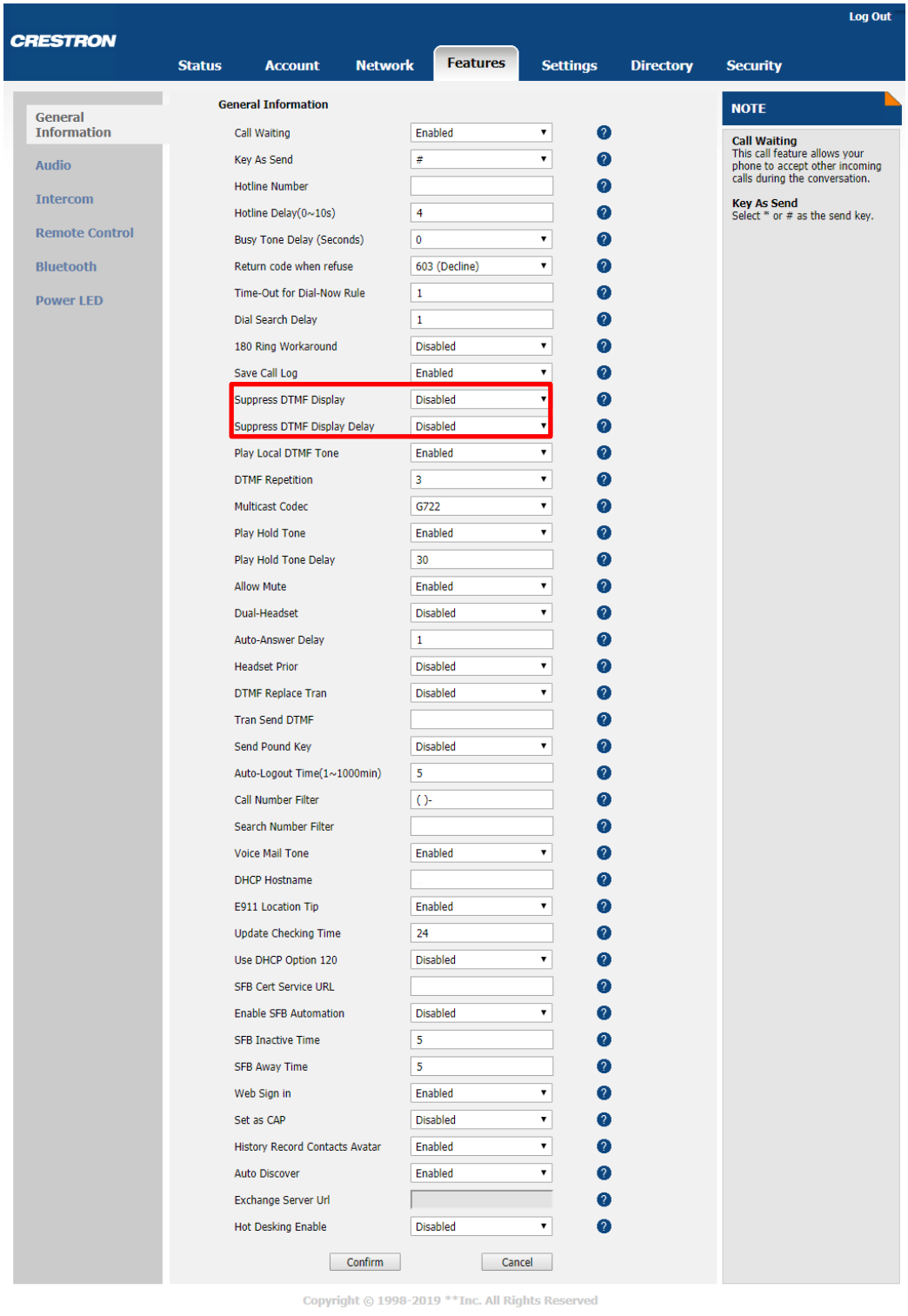
Web User Interface:
Features > General Information > Suppress DTMF Display Delay

Phone User Interface:
None

Configure Suppress DTMF Display and Suppress DTMF Display Delay via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Select **Enabled** or **Disabled** from the **Suppress DTMF Display** drop-down list.
3. Select **Enabled** or **Disabled** from the **Suppress DTMF Display Delay** drop-down list.
4. Click **Confirm** to accept the changes.

Transfer via DTMF

Call transfer is implemented via DTMF on some traditional servers. The phone sends specified DTMF digits to the server for transferring calls to third parties.

Configuration changes can be performed using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure transfer via DTMF. **Parameters:** features.dtmf.replace_tran features.dtmf.transfer
Local	Web User Interface	Configure transfer via DTMF. **Navigate to:** http://<phoneIPAddress>/servlet?p=features-general&q=load

Details of the Configuration Parameters

Parameter	Permitted Values	Default
features.dtmf.replace_tran	**0 or 1**	**0**
Description: Enables or disables the sending of DTMF sequences for transfer function when pressing a Transfer/Bind Transfer soft key or TRANSFER key. **0**- Disabled, the phone will perform the transfer as normal when pressing a Transfer/Bind Transfer soft key or TRANSFER key during a call. **1**- Enabled, the phone will transmit the designated DTMF digits to the server for performing call transfer when pressing a Transfer/Bind Transfer soft key or TRANSFER key during a call. **Web User Interface:** Features > General Information > DTMF Replace Tran **Phone User Interface:** None		

Parameter	Permitted Values	Default
features.dtmf.transfer	String within 32 characters	Blank

Description:

Configures the DTMF digits to be transmitted to perform call transfer. Valid values are: 0-9, *, #, and A-D.

Example:
features.dtmf.transfer = 123

Note: This feature works only if the value of the parameter "features.dtmf.replace_tran" is set to 1 (Enabled).

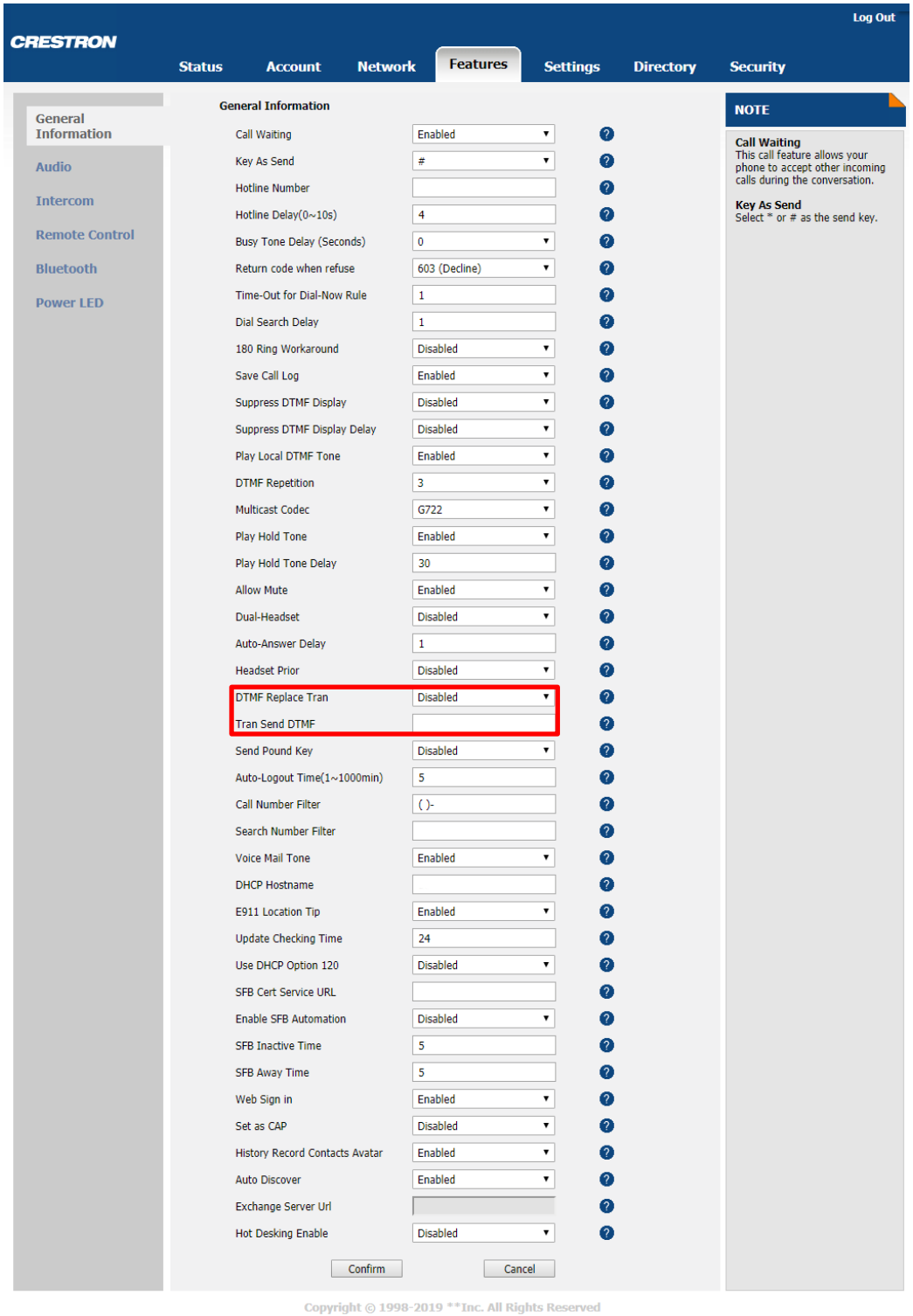
Web User Interface:
Features > General Information > Tran Send DTMF

Phone User Interface:
None

Configure Transfer via DTMF via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Select **Enabled** or **Disabled** from the **DTMF Replace Tran** drop-down list.
3. Enter the specified DTMF digits in the **Tran Send DTMF** field.
4. Click **Confirm** to accept the changes.

Play Local DTMF Tone

The Play Local DTMF Tone feature allows phones to play a local DTMF tone during an active call. If this feature is enabled, the user can hear the DTMF tone when pressing the phone's keypad during a call.

Configuration changes can be performed using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure play local DTMF tone. **Parameter:** features.play_local_dtmf_tone_enable
Local	Web User Interface	Configure play local DTMF tone. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

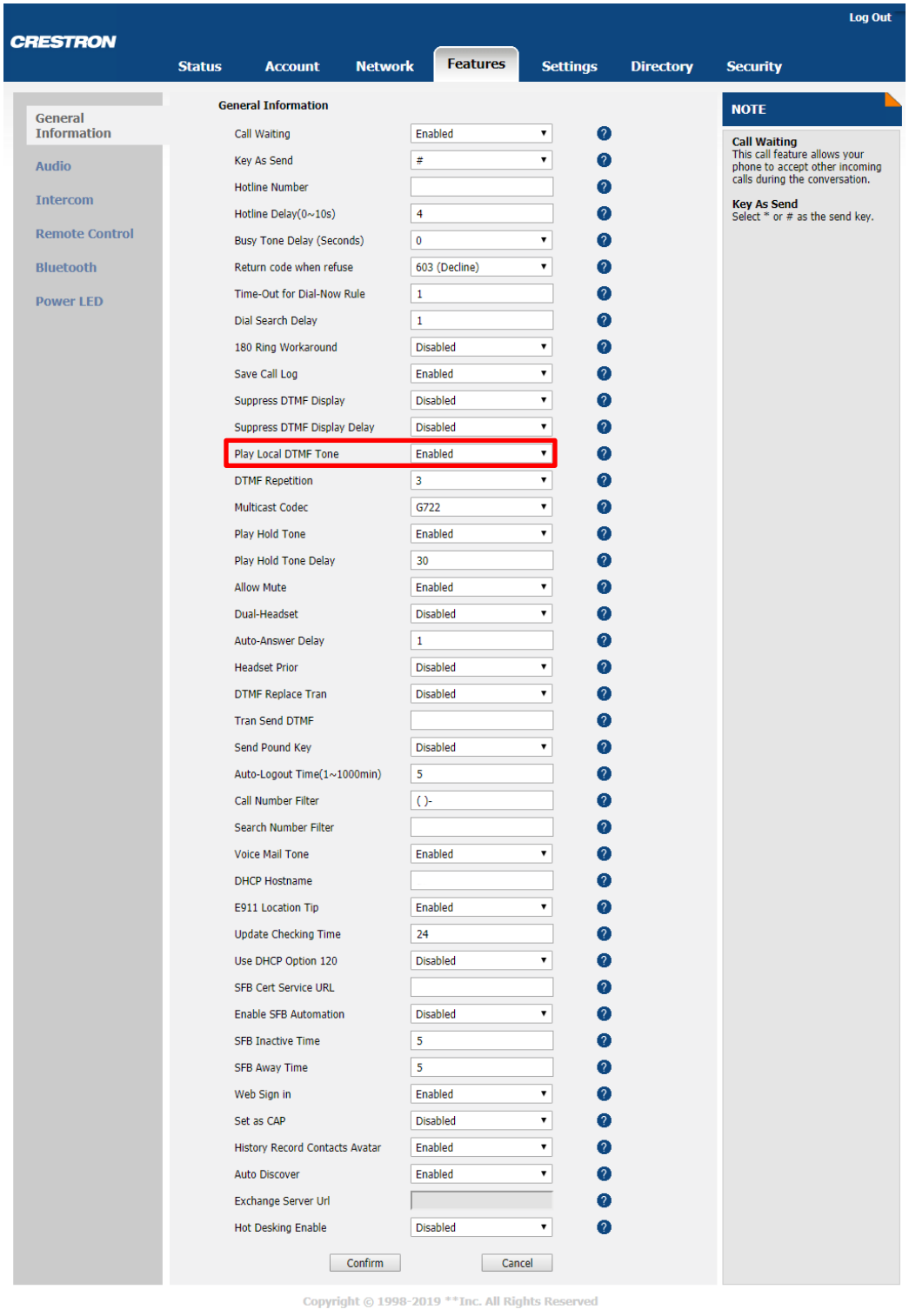
Details of the Configuration Parameter

Parameter	Permitted Values	Default
features.play_local_dtmf_tone_enable	**0 or 1**	**1**
Description: Enables or disables playing a local DTMF tone during a call. **0**- Disabled **1**- Enabled, the user can hear the DTMF tone when pressing the phone's keypad during a call. **Web User Interface:** Features > General Information > Play Local DTMF Tone **Phone User Interface:** None		

Configure Play Local DTMF Tone via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Select **Enabled** or **Disabled** from the **Play Local DTMF Tone** drop-down list.
3. Click **Confirm** to accept the change.

Configure Security Features

Skype for Business Feature License

By default, the phone has a built-in Skype for Business feature license, which allows the user to use phones with Skype for Business features directly.

If a phone that is not running Skype for Business firmware is to be upgraded to Skype for Business firmware, a Skype for Business feature license must be uploaded to the phone.

The Skype for Business feature license can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Specify the access URL of Skype for Business feature license. **Parameter:** lync_license_dat.url
Local	Web User Interface	Specify the access URL of Skype for Business feature license. **Navigate to:** http://<phoneIPAddress>/servlet?p=security-license&q=load

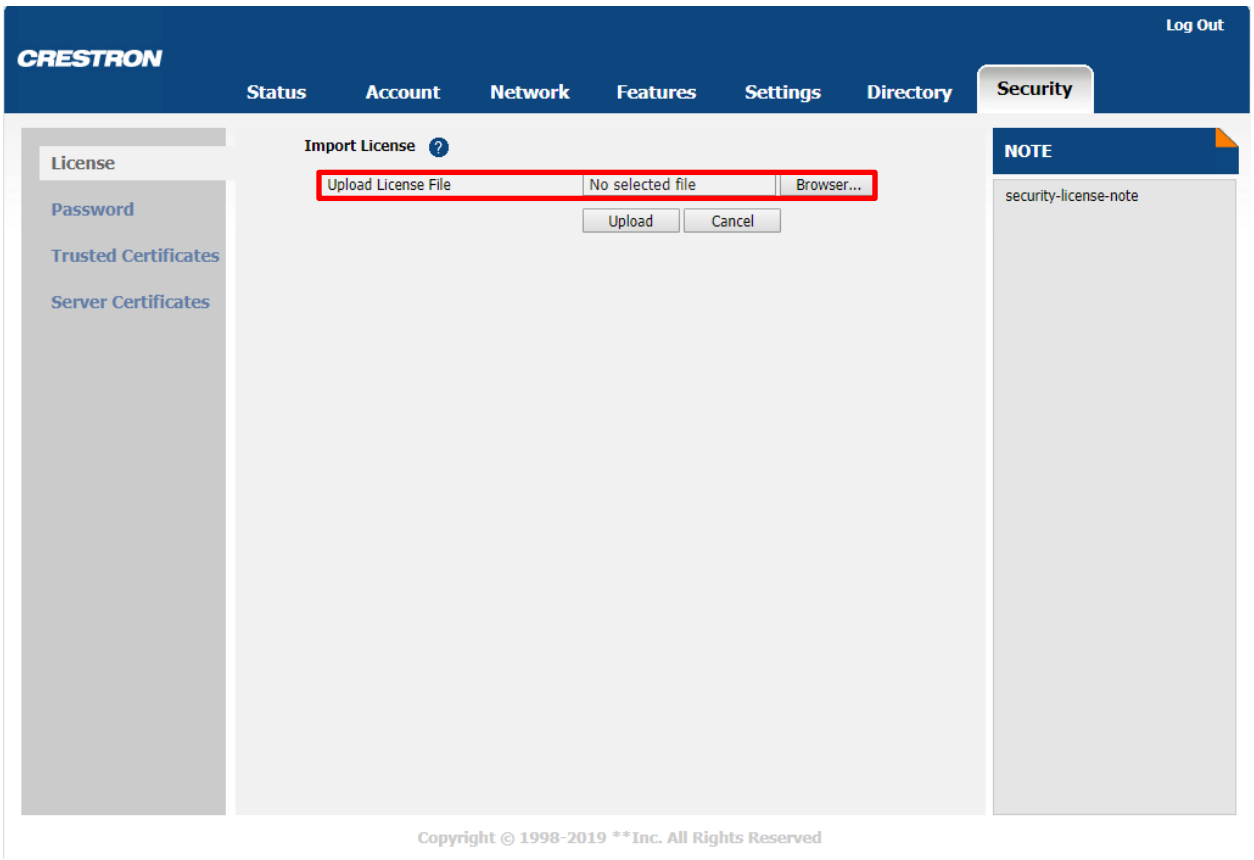
Details of the Configuration Parameter

Parameter	Permitted Values	Default
lync_license_dat.url	**String within 99 characters**	**Blank**
Description: Configures the access URL of the Skype for Business feature license. **Example:** lync_license_dat.url = http://192.168.1.20/License_$MAC.dat **Example:** The phone will replace the characters "$MAC" with its MAC address during auto provisioning. For example, the MAC address of one Skype for Business phone is 00156543EC97. When performing auto provisioning, the phone will request the License_00156543ec97.dat file from the provisioning server address "http://192.168.1.20". **Web User Interface:** Security > License **Phone User Interface:** None **Note:** If the parameter is changed, the phone will reboot to make the change take effect.		

Upload the Skype for Business Feature License via the Web User Interface

1. Click **Security** > **License**.

Security > License



2. Click **Browser** to select the license from the local system.
3. Click **Upload** to upload the certificate.

For instructions on viewing the Skype for Business Server license status via the web user interface, refer to "Skype for Business Status" on page 342.

User and Administrator Passwords

Some menu options are protected by two privilege levels: user and administrator, each with its own password. When logging into the web user interface, the user must enter the user name and password to access various menu options. The default user password is "user" and the default administrator password is "admin".

For security reasons, the user or administrator should change the default user or administrator password as soon as possible. The user can be changed by both the user and the administrator, while the administrator password can only be changed by the administrator.

Advanced menu options are strictly used by administrators. Users can configure them only if they have administrator privileges.

User or administrator password can be changed using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Change the user or administrator password of the phone. **Parameter:** static.security.user_password
Local	Web User Interface	Change the user or administrator password of the phone. **Navigate to**: http://<phoneIPAddress>/servlet?p=security&q=load
	Phone User Interface	Change the administrator password of the phone.

Details of the Configuration Parameter

Parameter	Permitted Values	Default
static.security.user_password	**String within 32 characters**	**user**

Description:

Configures the password of the user or administrator for the phone's web user interface access.

The phone uses "user" as the default user password and "admin" as the default administrator password.

The valid value format is username:new password.

Example:
static.security.user_password = user:123 means setting the password of user (current user name is "user") to 123.
static.security.user_password = admin:456 means setting the password of administrator (current user name is "admin") to 456.

Note: Phones support ASCII characters 32-126(0x20-0x7E) in passwords. The password can be set to be empty via web user interface only.

Web User Interface:
Security > Password

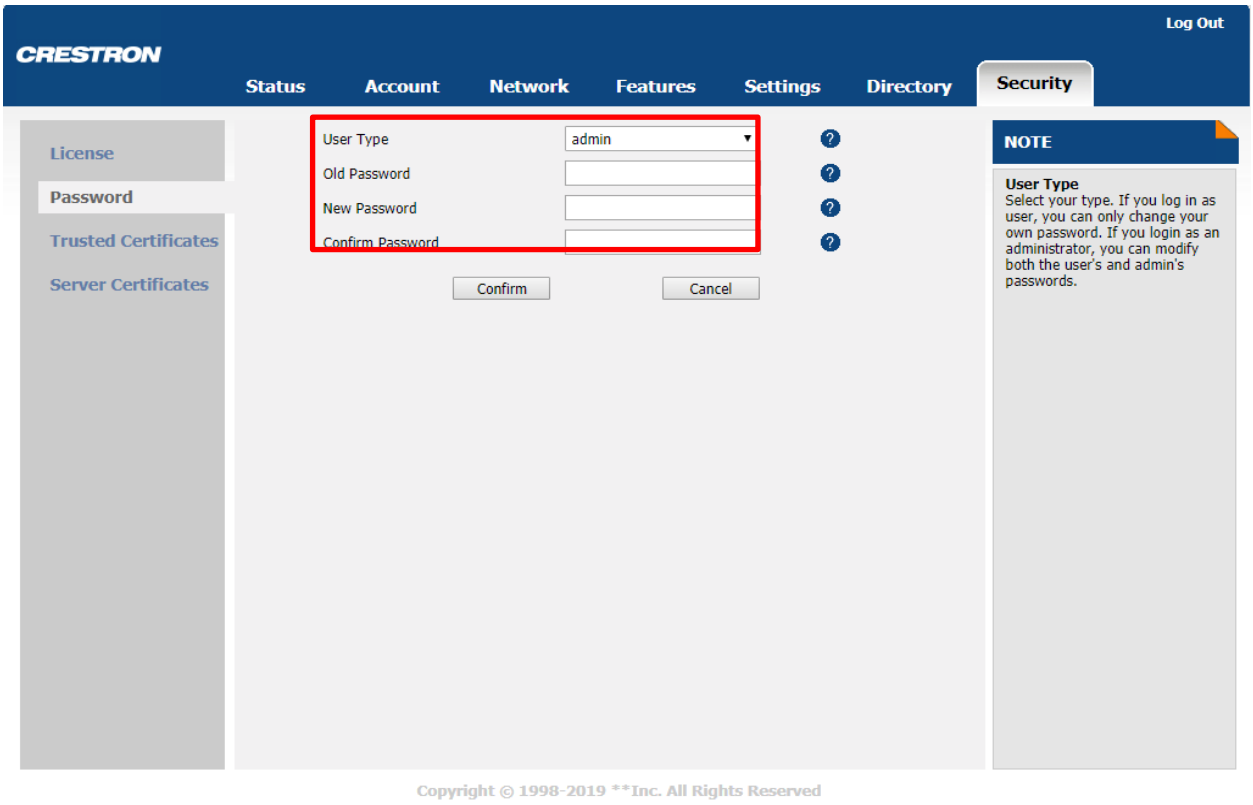
Phone User Interface:
Menu > Setting > Advanced (default password: admin) > Set Password

Note: The user password cannot be changed via the Phone User Interface.

Change the User or Administrator Password via the Web User Interface

1. Click **Security** > **Password**.

Security > Password



2. Select **user** or **admin** from the **User Type** drop-down list.
3. Enter the new password in the **New Password** and **Confirm Password** fields. Valid characters are ASCII characters 32-126(0x20-0x7E) except 58(3A).

   NOTE: If logging into the web user interface of the phone with the user credential, the old user password must be entered in the **Old Password** field.

4. Click **Confirm** to accept the changes.

Change the Administrator Password via the Phone User Interface

1. Tap **Setting** > **Advanced** (default password: admin) > **Set Password**.
2. Enter the current administrator password in the **Current Password** field.
3. Enter new password in the **New Password** field and **Confirm Password** field. Valid characters are ASCII characters 32-126(0x20-0x7E).
4. Tap **Save** to accept the changes.

Auto Logout Time

Auto logout time defines a specific period of time after which the phones will automatically log out if the web user interface has not been used. Once logged out, the username and password must be entered for web access authentication.

Auto-logout time can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure auto-logout time. **Parameter**: features.relog_offtime
Local	Web User Interface	Configure auto-logout time. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

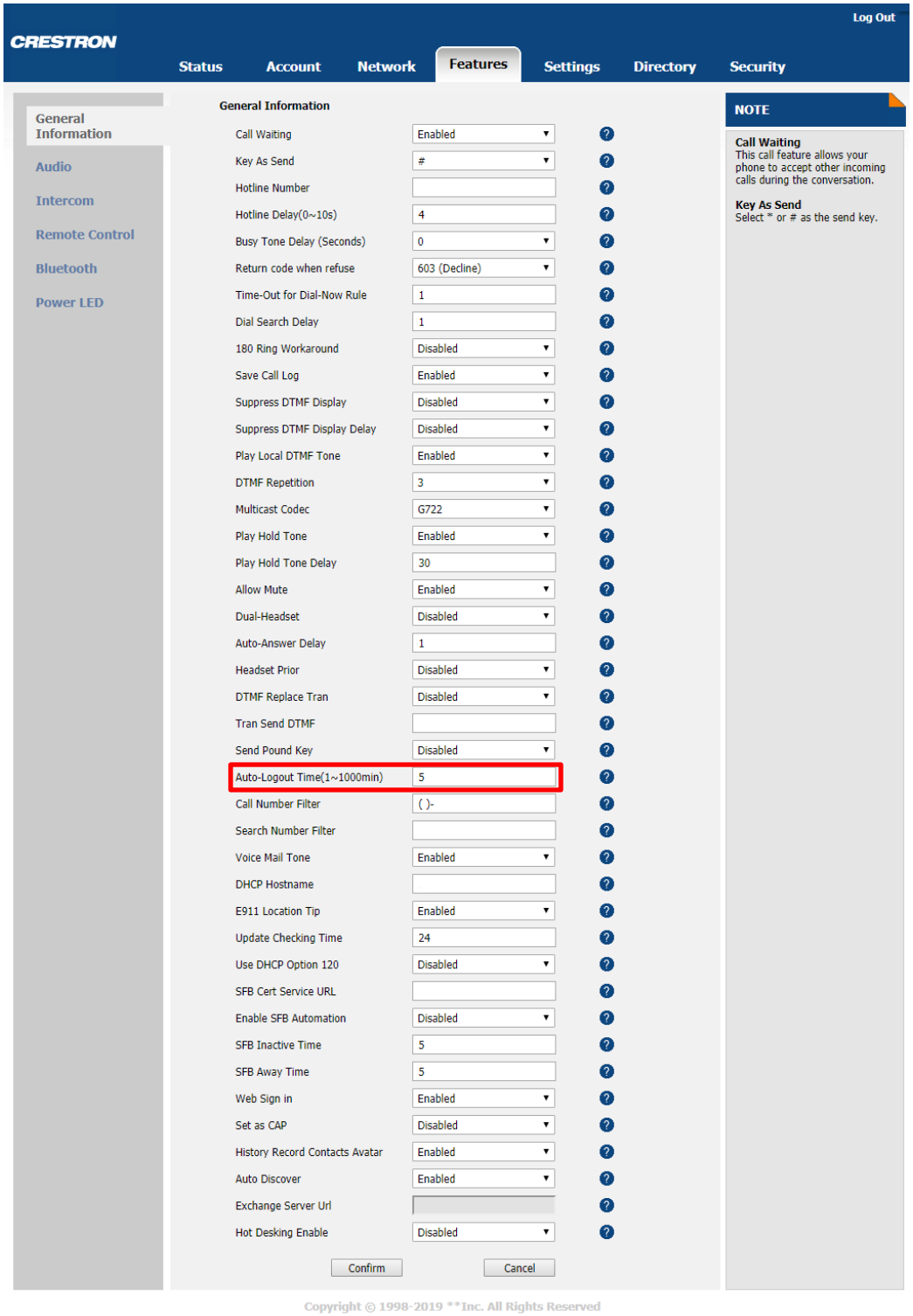
Details of the Configuration Parameter

Parameter	Permitted Values	Default
features.relog_offtime	**Integer from 1 to 1000**	**5**
Description: Configures the timeout interval (in minutes) for web access authentication. **Example**: features.relog_offtime = 5 If a user logs into the web user interface and leave it idle for 5 minutes, the user will be automatically logged out. **Note:** If the parameter is changed, the phone will reboot to make the change take effect. **Web User Interface:** Features > General Information > Auto-Logout Time(1~1000min) **Phone User Interface:** None		

Configure the Auto-Logout Time via the Web User Interface

1. Click **Features** > **General Information**.

Features > General Information



2. Enter the auto-logout time (in minutes) in the **Auto-Logout Time(1~1000min)** field.
3. Click **Confirm** to accept the change.

Phone Lock

If the system administrator sets the policy "ucEnforcePinLock" = true on the Skype for Business Fronted Server, the user can use the phone lock feature to lock the phone to prevent unauthorized use. The phone will prompt the user to configure a n-digit lock PIN at the initial sign-in.

Phone lock can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configures the phone lock feature. **Parameter**: phone_setting.phone_lock.enable
		Configures the time (in minutes) the phone is idle before it automatically locks. **Parameter:** phone_setting.phone_lock.lock_time_out
		Configures the unlock attempts. **Parameter:** sfb.phone_lock.max_attempts
		Configures the phone to be locked and unlocked automatically along with the paired PC. **Parameter:** sfb.phone_lock_with_pc.enable
		Configures the phone to automatically sign out when a user does not enter the lock Pin within 5 minutes. **Parameter:** sfb.phone_lock.sign_out_auto.enable
Local	Web User Interface	Configures the phone lock feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-phonelock&q=load
	Phone User Interface	Configures the phone lock feature.

Details of the Configuration Parameters

Parameter	Permitted Values	Default
phone_setting.phone_lock.enable	0 or 1	0
Description: Enables or disables the phone lock feature. **0**- Disabled **1**- Enabled, the phone will prompt the user to configure a n-digit unlock PIN at the initial sign-in. **Web User Interface:** Settings > Phone Lock > Phone Lock **Phone User Interface:** Menu > Setting > Basic > Phone Lock > Lock Enable		
phone_setting.phone_lock.lock_time_out	1 to 1440	10
Description: Configures the period of time (in minutes) the phone is idle before it automatically locks. **Web User Interface:** Settings > Phone Lock > Idle time-out(1~1440mins) **Phone User Interface:** Menu > Setting > Basic > Phone Lock > Idle time-out		
sfb.phone_lock.max_attempts	3 to 10	5
Description: Configures the maximum number of unsuccessful unlock attempts for a locked phone that is not in a call. The user will be automatically signed out of the phone when the unsuccessful unlock attempts exceed the limit. **Web User Interface:** Settings > Phone Lock > Max attempts of unlock **Phone User Interface:** Menu > Setting > Basic > Phone Lock > Unlock attempts		
sfb.phone_lock_with_pc.enable	0 or 1	1
Description: Enables or disables automatic locking and unlocking when the computer is locked and unlocked. **0**- Disabled **1**- Enabled **Web User Interface:** Settings > Phone Lock > Phone Lock with PC **Phone User Interface:** Menu > Setting > Basic > Phone Lock > Phone Lock with PC		

Parameter	Permitted Values	Default
sfb.phone_lock.sign_out_auto.enable	0 or 1	0

Description:

Enables or disables automatic sign out when the user does not create a lock PIN within 5 minutes of prompt.

0- Disabled

1- Enabled

Note: If this parameter is changed, the phone will reboot to effect the change.

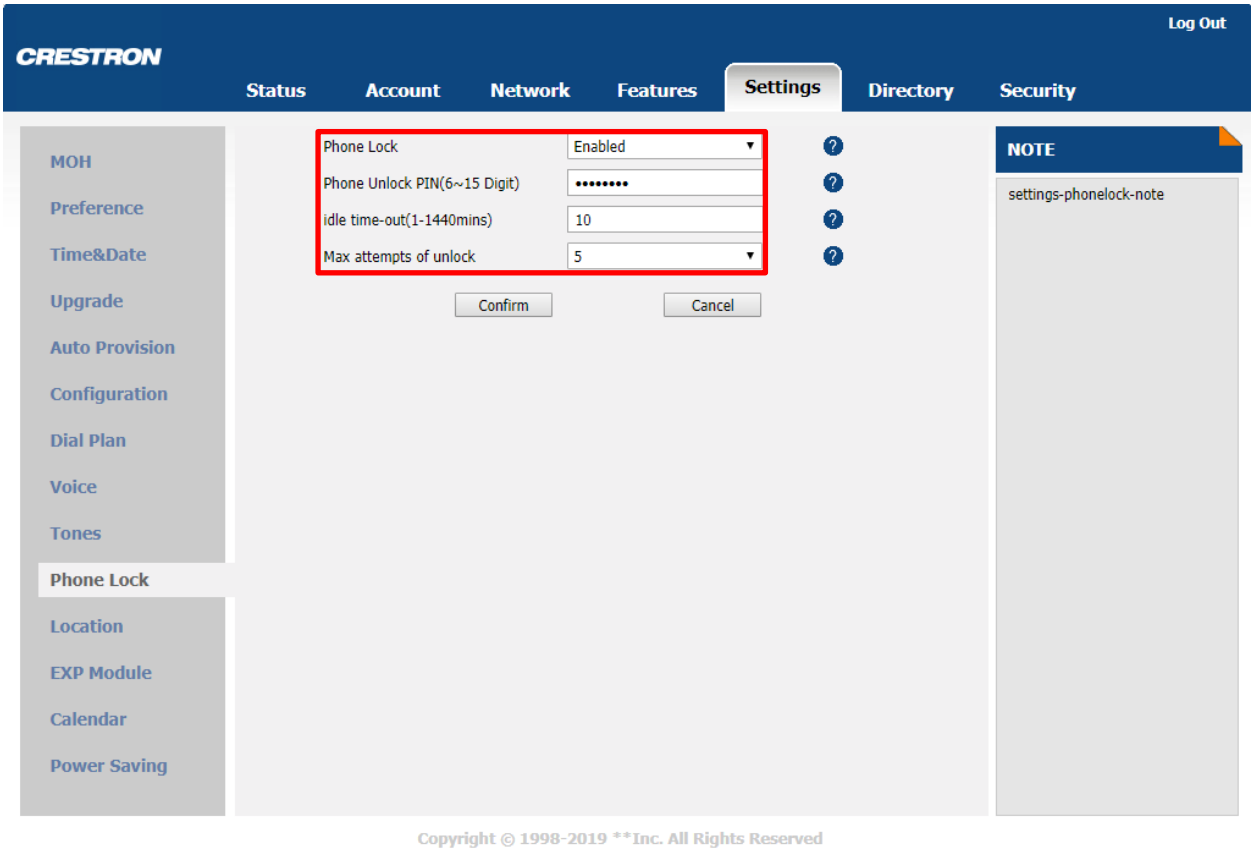
Web User Interface:
None

Phone User Interface:
None

Configure Phone Lock via the Web User Interface

1. Click **Settings** > **Phone Lock**.

Settings > Phone Lock



2. Select the **Enabled** from the **Phone Lock** drop-down list.
3. Enter the lock PIN in the **Phone Unlock PIN(6~15 Digit)** field.
4. Enter the time-out value (in minutes) in the **Idle time-out(1~1440mins)** field.

5. Select the maximum amount of unlock attempts from the **Max attempts of unlock** drop-down list.
6. Click **Confirm** to accept the changes.

Configure Phone Lock via the Phone User Interface

1. Tap **Setting** > **Basic** > **Phone Lock**.
2. Configure the fields as needed.
3. Tap **Save**.

Transport Layer Security (TLS)

TLS is a commonly-used protocol for providing communications privacy and managing the security of message transmission, allowing Skype for Business phones to communicate with other remote parties and connect to the HTTPS URL for provisioning in a way that is designed to prevent eavesdropping and tampering.

TLS protocol is composed of two layers: TLS Record Protocol and TLS Handshake Protocol. The TLS Record Protocol completes the actual data transmission and ensures the integrity and privacy of the data. The TLS Handshake Protocol allows the server and client to authenticate each other and negotiate an encryption algorithm and cryptographic keys before data is exchanged.

The TLS protocol uses asymmetric encryption for authentication of key exchange, symmetric encryption for confidentiality, and message authentication codes for integrity.

- **Symmetric encryption**: For symmetric encryption, the encryption key and the corresponding decryption key can be told by each other. In most cases, the encryption key is the same as the decryption key.
- **Asymmetric encryption**: For asymmetric encryption, each user has a pair of cryptographic keys – a public encryption key and a private decryption key. The information encrypted by the public key can only be decrypted by the corresponding private key and vice versa. Usually, the receiver keeps its private key. The public key is known by the sender, so the sender sends the information encrypted by the known public key, and then the receiver uses the private key to decrypt it.

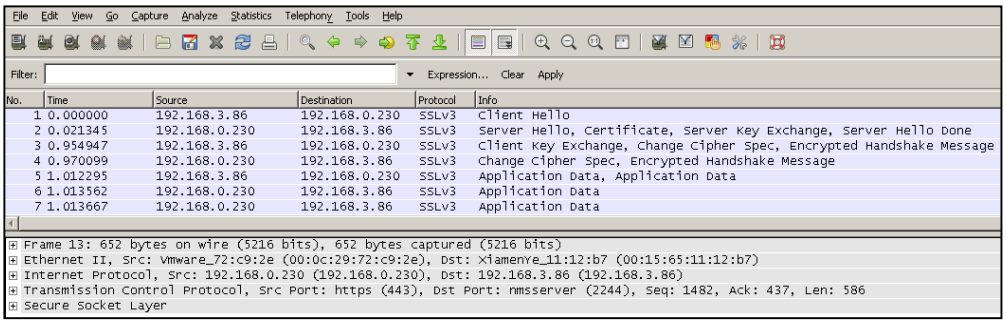
Skype for Business phones support TLS version 1.0, 1.1 and 1.2. A cipher suite is a named combination of authentication, encryption, and message authentication code (MAC) algorithms used to negotiate the security settings for a network connection using the TLS/SSL network protocol. IP phones support the following cipher suites:

- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA
- AES256-SHA
- EDH-RSA-DES-CBC3-SHA

- EDH-DSS-DES-CBC3-SHA
- DES-CBC3-SHA
- DES-CBC3-MD5
- DHE-RSA-AES128-SHA
- DHE-DSS-AES128-SHA
- AES128-SHA
- RC2-CBC-MD5
- IDEA-CBC-SHA
- DHE-DSS-RC4-SHA
- RC4-SHA
- RC4-MD5
- RC4-64-MD5
- EXP1024-DHE-DSS-DES-CBC-SHA
- EXP1024-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-DSS-DES-CBC-SHA
- DES-CBC-SHA
- DES-CBC-MD5
- EXP1024-DHE-DSS-RC4-SHA
- EXP1024-RC4-SHA
- EXP1024-RC4-MD5
- EXP-EDH-RSA-DES-CBC-SHA
- EXP-EDH-DSS-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP-RC2-CBC-MD5
- EXP-RC4-MD5

The following figure illustrates the TLS messages exchanged between the Skype for Business phone and TLS server to establish an encrypted communication channel:

TLS Messages



1. Skype for Business phone sends a "Client Hello" message proposing SSL options.
2. Server responds with a "Server Hello" message selecting the SSL options, sends its public key information in a "Server Key Exchange" message and concludes its part of the negotiation with a "Server Hello Done" message.
3. Skype for Business phone sends session key information (encrypted by the server's public key) in the "Client Key Exchange" message.
4. Server sends a "Change Cipher Spec" message to activate the negotiated options for all future messages it will send.

Skype for Business phones can encrypt SIP with TLS, which is called SIPS. When TLS is enabled for an account, the SIP message of this account will be encrypted, and a lock icon appears on the LCD screen after the successful TLS negotiation.

Certificates

The Skype for Business phone can serve as a TLS client or a TLS server. The TLS requires the following security certificates to perform the TLS handshake:

- **Trusted Certificate**: When the Skype for Business phone requests a TLS connection with a server, the Skype for Business phone should verify the certificate sent by the server to decide whether it is trusted based on the trusted certificates list. The Skype for Business phone has 51 built-in trusted certificates. Up to 51 custom certificates can be uploaded. The format of the trusted certificate files must be *.pem,*.cer,*.crt and *.der and the maximum file size is 5MB. For more information on 51 trusted certificates, refer to "Appendix C: Trusted Certificates" on page 385.

- **Server Certificate**: When clients request a TLS connection with the Skype for Business phone, the Skype for Business phone sends the server certificate to the clients for authentication. The Skype for Business phone has two types of built-in server certificates: a unique server certificate and a generic server certificate. Only one server certificate can be uploaded to the Skype for Business phone. The old server certificate will be overridden by the new one. The format of the server certificate files must be *.pem and *.cer and the maximum file size is 5MB.
  - A unique server certificate: It is unique to a Skype for Business phone (based on the MAC address) and issued by the Certificate Authority (CA).
  - A generic server certificate: It is issued by the Certificate Authority (CA). Only if no unique certificate exists, the Skype for Business phone may send a generic certificate for authentication.

The Skype for Business phone can authenticate the server certificate based on the trusted certificates list. The trusted certificates list and the server certificates list contain the default and custom certificates. The type of certificates the Skype for Business phone accepts can be specified: default certificates, custom certificates, or all certificates.

The Common Name Validation feature enables the phone to require validation of the common name of the certificate sent by the connecting server. The Security verification rules are compliant with RFC 2818.

NOTES:

- In the TLS feature, we use the terms "trusted" and "server" certificates. These are also known as CA and device certificates.
- Resetting the Skype for Business phone to factory defaults will delete custom certificates by default. This feature is configurable by the parameter "static.phone_setting.reserve_certs_enable" using the configuration files.

Configuration changes can be performed using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the trusted certificates feature. **Parameters:** static.security.trust_certificates static.security.ca_cert static.security.cn_validation
		Configure the server certificates feature. **Parameters:** static.security.dev_cert
		Upload the trusted certificates. **Parameter:** static.trusted_certificates.url

		Delete all uploaded trusted certificates. **Parameter:** static.trusted_certificates.delete
		Upload the server certificates. **Parameter:** static.server_certificates.url
		Delete all uploaded server certificates. **Parameter:** static.server_certificates.delete
		Configure the custom certificates. **Parameter:** static.phone_setting.reserve_certs_enable
Local	Web User Interface	Configure the trusted certificates feature. Upload the trusted certificates. **Navigate to:** http://<phoneIPAddress>/servlet?p=trusted-cert&q=load
		Configure the server certificates feature. Upload the server certificates. **Navigate to:** http://<phoneIPAddress>/servlet?p=server-cert&q=load

Details of the Configuration Parameters

Parameter	Permitted Values	Default
static.security.trust_certificates	0 or 1	1

Description:

Enables or disables trusting only the server certificates in the Trusted Certificates list.

0- Disabled, the phone will trust the server no matter whether the certificate sent by the server is valid or not.

1- Enabled, the phone will authenticate the server certificate based on the trusted certificates list. The phone will only trust the server when authentication succeeds.

Note: If the parameter is changed, the phone will reboot to effect the change.

Web User Interface:
Security > Trusted Certificates > Only Accept Trusted Certificates

Phone User Interface:
None

Parameter	Permitted Values	Default
static.security.ca_cert	**0, 1 or 2**	**2**
Description: Configures the type of certificates in the Trusted Certificates list for the Skype for Business phone to authenticate for TLS connection. **0**- Default Certificates **1**- Custom Certificates **2**- All Certificates **Note:** If the parameter is changed, the phone will reboot to effect the change. **Web User Interface:** Security > Trusted Certificates > CA Certificates **Phone User Interface:** None		
static.security.cn_validation	**0 or 1**	**0**
Description: Enables or disables mandatory validation of the CommonName or SubjectAltName of the certificate sent by the server. **0**- Disabled **1**- Enabled **Note:** If the parameter is changed, the phone will reboot to effect the change. **Web User Interface:** Security > Trusted Certificates > Common Name Validation **Phone User Interface:** None		
static.security.dev_cert	**0 or 1**	**0**
Description: Configures the type of the device certificates for the Skype for Business phone to send for TLS authentication. **0**- Default Certificates **1**- Custom Certificates **Note:** If the parameter is changed, the phone will reboot to effect the change. **Web User Interface:** Security > Server Certificates > Device Certificates **Phone User Interface:** None		

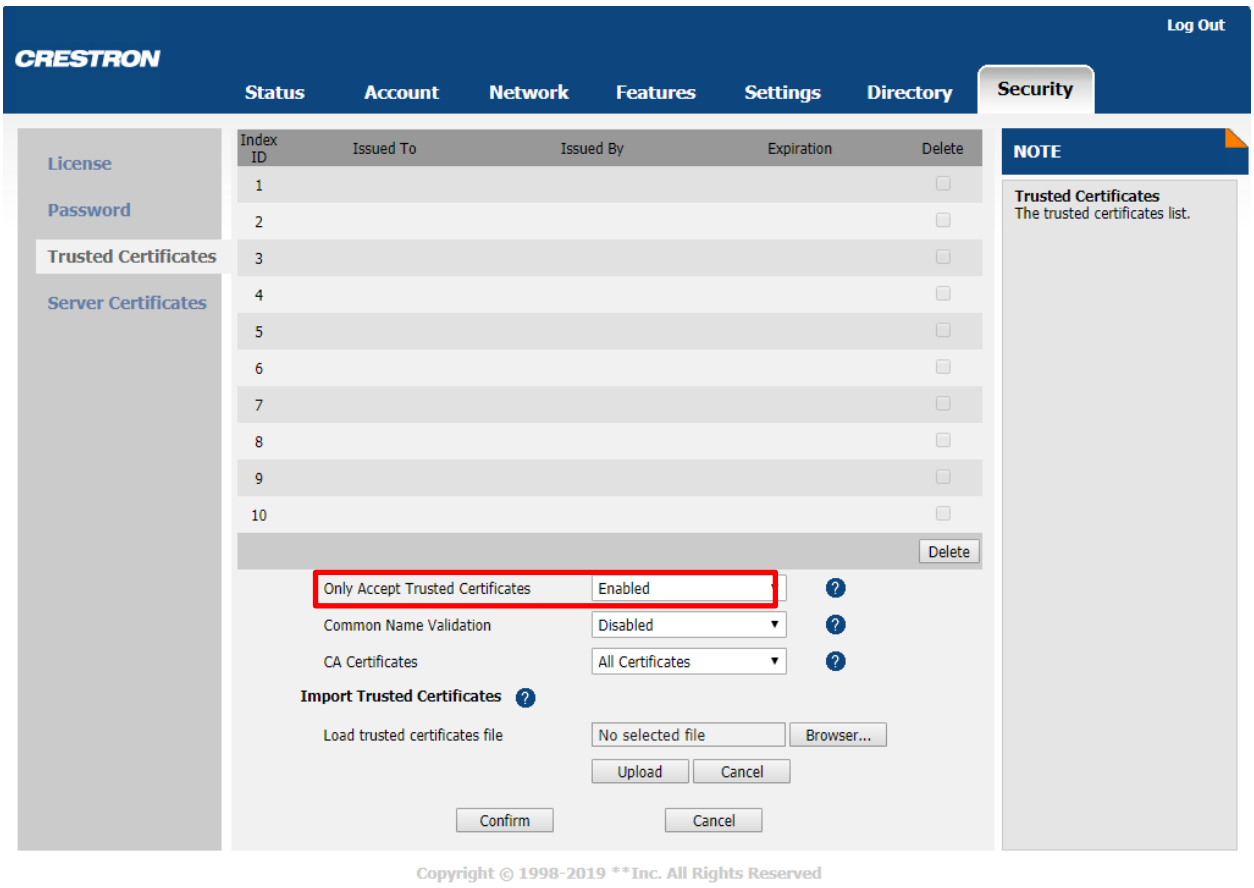
Parameter	Permitted Values	Default
static.trusted_certificates.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom trusted certificate used to authenticate the connecting server. **Example:** static.trusted_certificates.url = http://192.168.1.20/tc.crt **Note:** The certificate must be in *.pem, *.crt, *.cer or *.der format. **Web User Interface:** Security > Trusted Certificates > Load trusted certificates file **Phone User Interface:** None		
static.trusted_certificates.delete	**http://localhost/all**	**Blank**
Description: Deletes all uploaded trusted certificates. **Example:** static.trusted_certificates.delete = http://localhost/all **Web User Interface:** None **Phone User Interface:** None		
static.server_certificates.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the certificate the phone sends for authentication. **Example:** static.server_certificates.url = http://192.168.1.20/ca.pem **Note:** The certificate must be in *.pem or *.cer format. **Web User Interface:** Security > Server Certificates > Load server cer file **Phone User Interface:** None		
static.server_certificates.delete	**http://localhost/all**	**Blank**
Description: Deletes all uploaded server certificates. **Example:** static.server_certificates.delete = http://localhost/all **Web User Interface:** None **Phone User Interface:** None		

Parameter	Permitted Values	Default
static.phone_setting.reserve_certs_enable	0 or 1	0
Description: Enables or disables reserving custom certificates after the phone is reset to factory defaults. **0**- Disabled **1**- Enabled **Web User Interface:** None **Phone User Interface:** None		

Configure the Trusted Certificates via the Web User Interface

1. Click **Security** > **Trusted Certificates**.

Security > Trusted Certificates

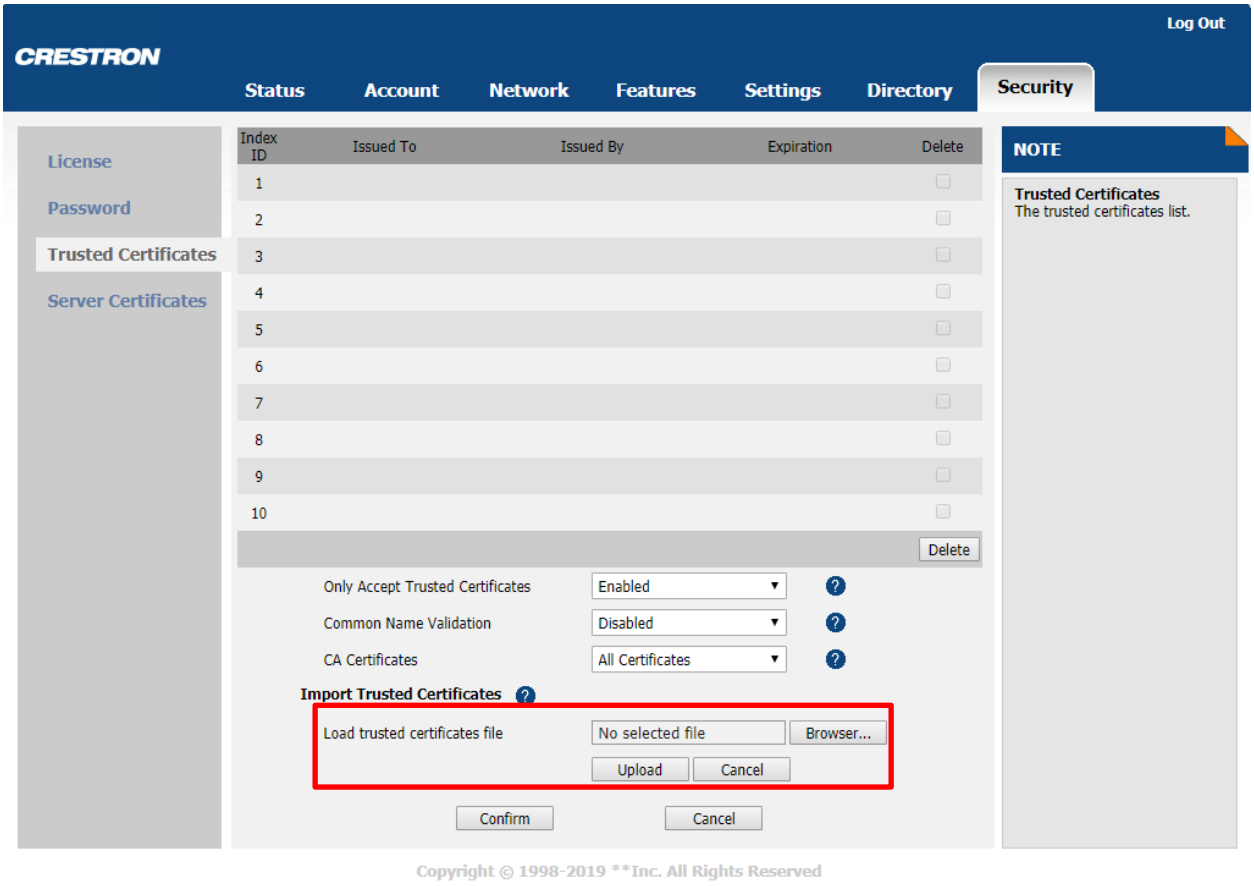


2. Select **Enabled** or **Disabled** from the **Only Accept Trusted Certificates**, **Common Name Validation** drop-down lists and the types of certificates from the **CA Certificates** drop-down list.
3. Click **Confirm** to accept the changes.

Upload a Trusted Certificate via the Web User Interface

1. Click **Security** > **Trusted Certificates**.

Security > Trusted Certificates

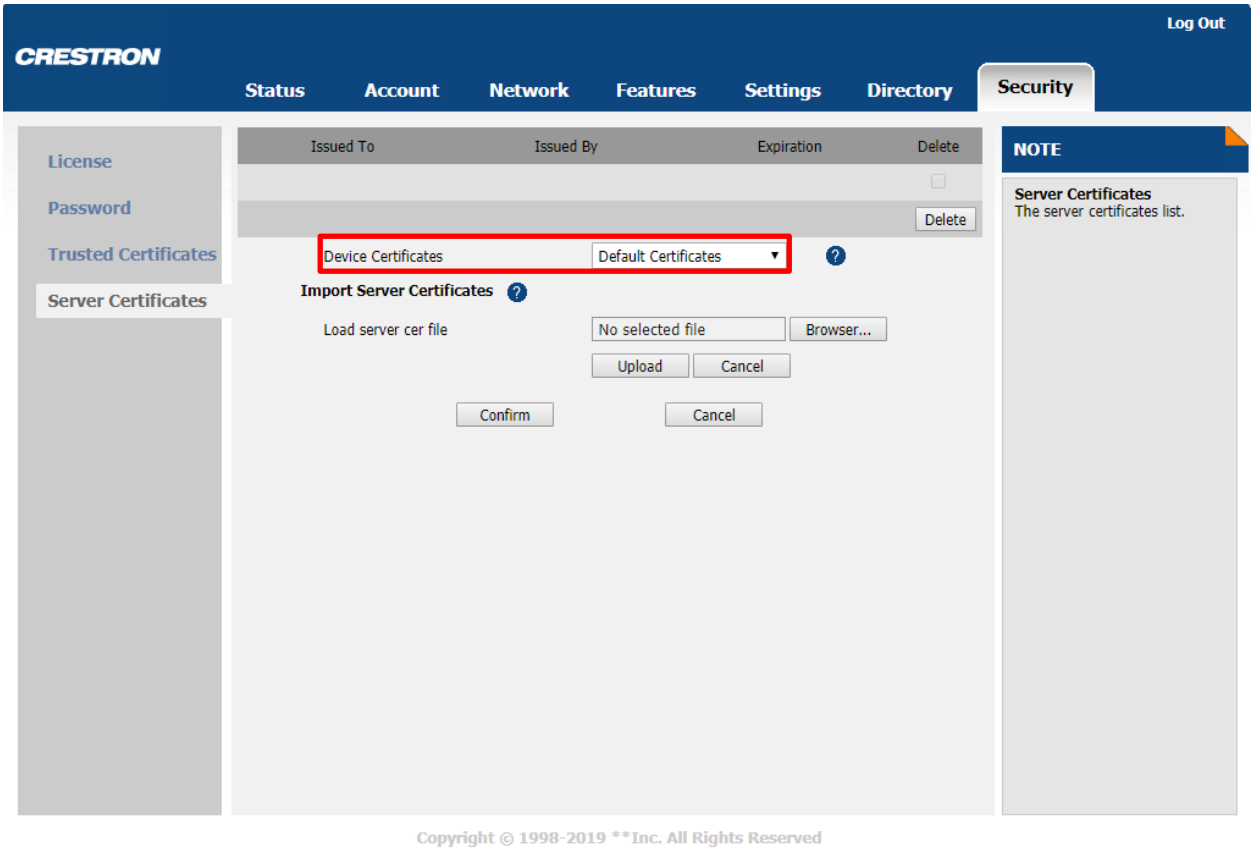


2. Click **Browser** to select the certificate (*.pem, *.crt, *.cer or *.der) from the local system.
3. Click **Upload** to upload the certificate.

Configure the Server Certificates via the Web User Interface

1. Click **Security** > **Server Certificates**.

Security > Server Certificates

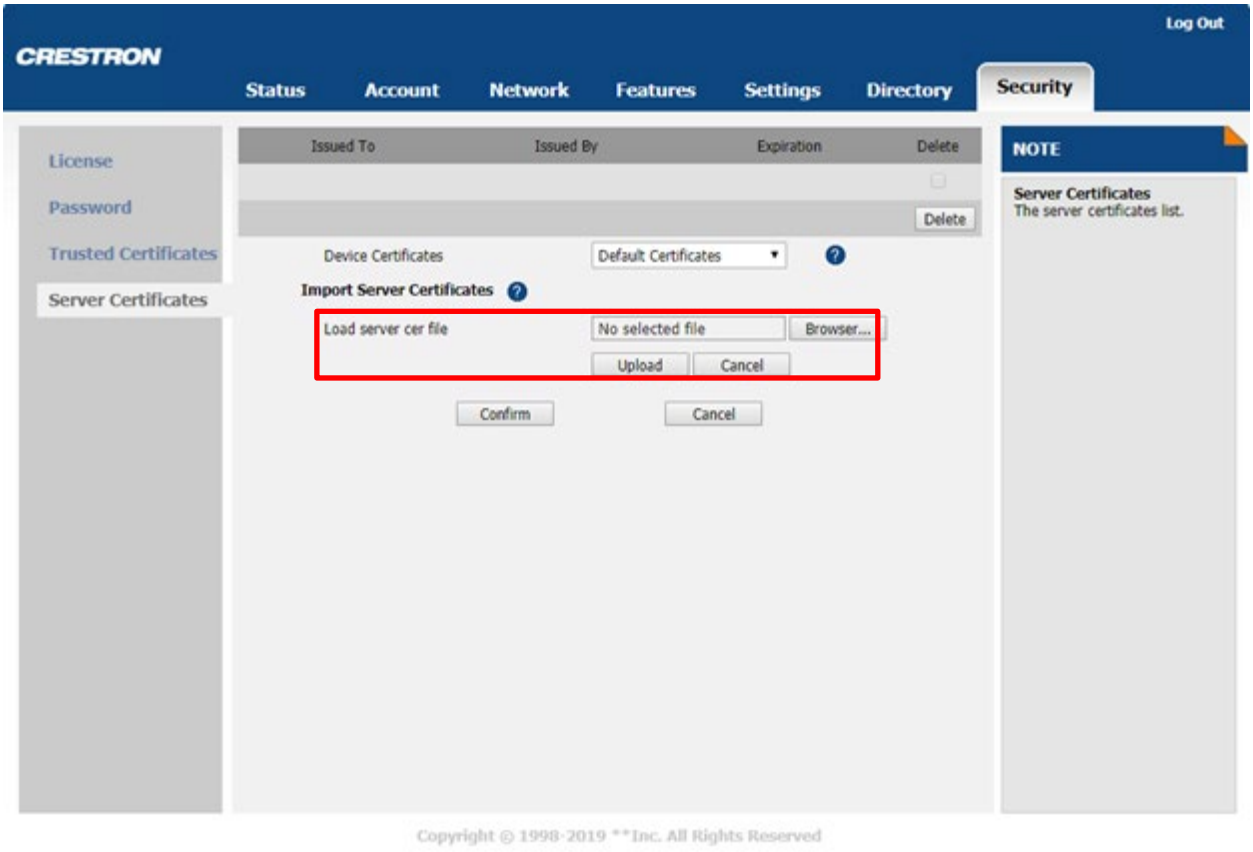


2. Select the types of certificates from the **Device Certificates** drop-down list.
3. Click **Confirm** to accept the change.

Upload a Server Certificate via the Web User Interface

1. Click **Security** > **Server Certificates**.

Security > Server Certificates



2. Click **Browser** to select the certificate (*.pem and *.cer) from the local system.
3. Click **Upload** to upload the certificate. A dialog box pops up to prompt "Success: The Server Certificate has been loaded! Rebooting, please wait..."

Troubleshooting

This section provides an administrator with general information for troubleshooting some common issues they may encounter during use.

Skype for Business phones can provide feedback in a variety of forms such as log files, packets, status indicators, etc., which can help an administrator more easily find a system problem and fix it.

Memory Information

Configure phone process, memory occupancy, and CPU utility via the web user interface.

Memory information can be configured locally.

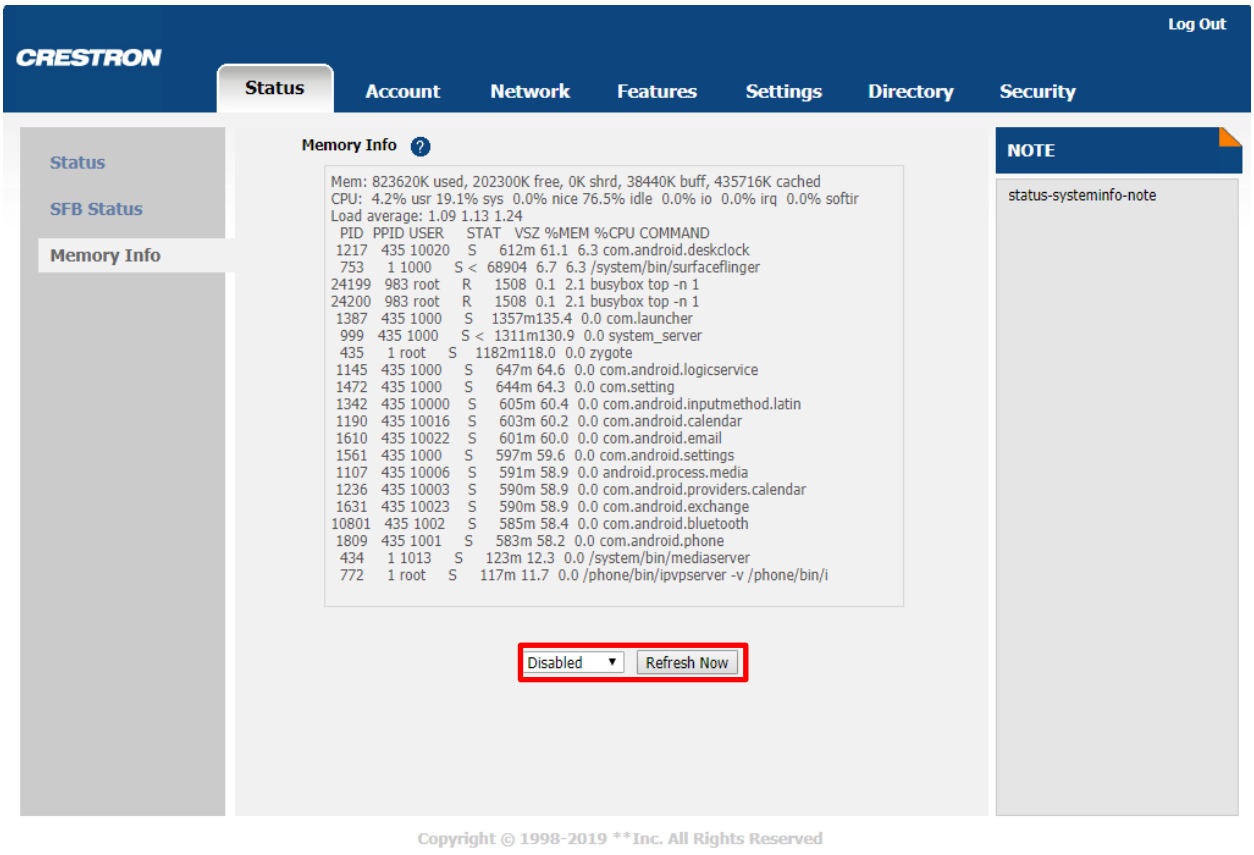
Configuration Methods

Local	Web User Interface	Configure memory information feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=status- systeminfo&q=load

Configure Memory Information via the Web User Interface

1. Click **Status** > **Memory Info**.

Status > Memory Info



2. Select the refresh interval from the drop-down list. If **Disabled** is selected, the page will not be refreshed.
3. Click **Refresh Now** to refresh the page and accept the change

Skype for Business Status

Troubleshoot phone issues by viewing the Skype for Business status.

To view Skype for Business status via the Web User Interface, click **Status** > **SFB Status**.

Skype for Business Status Definitions

Status	Display Name	Description
License	License Status	Indicates whether the Skype for Business feature license is imported to the phone. Values: • Installed • None
	License Validity	Term of validity of the license (in days).
Authentication info	User Type	Indicates the account type. Values: • UNKNOW • PIN • ONPREM • MANAGED • FEDERATED
	SIP Authentication	Indicates the SIP authentication type. Values: • UNSET • NTLM • KERBEROS • NEGOTIATE • TLS_DSK
	Sign-in Authentication Type	Indicates the Sign-in authentication type. Values: • NONE • ORG_ID • OAUTH • NTLM • DEV_PAIRING • BASIC • CACHE • CERT • ALL_METHOD
	Exchange Authentication Type	Indicates the Exchange authentication type. Values: • NONE • ORG_ID • OAUTH • NTLM

Status	Display Name	Description
		• DEV_PAIRING • BASIC • CACHE • CERT • ALL_METHOD
Server Status	Update Server URL	Indicates the Updates Server URL.
	Edge Server	Indicates the Edge Server address.
	Voice Mail URL	Indicates the Voice Mail URI of the account
	Email URI	Indicates the Email URI of the account
	ABS URL	Indicates the ABS (Address Book Server) URL
	LIS URL	Indicates the LIS URL for obtaining address information
	STS URI	Indicates the URI of the Security token service.
	Focus Factory URI	Indicates the URI of the Focus Factory.
	Home Server URL	Indicates the URL of the Home server.
	MRAS URL	Indicates the URL of the Media Relay Authentication Service.
	Call Park Server URI	Indicates the Call Park Server URI.
QoE	QoE Status	Indicates the QOE status
	QoE URI	Indicates the address where to send Quality of Experience (QoE) report.
	In-Call QoE Status	Indicates the QOE status during a call.
	In-Call QoE Interval	Indicates the interval the phone sends a Quality of Experience (QoE) report to the server during a call.
Hot desking	Hot desking Status	Indicates whether the phone is in hot-desking mode.
	Hot desking Time out	Indicates the idle time (in seconds) before the phone automatically exits the Hot Desking mode.
	CAP Status	Indicates whether the phone is in CAP (common area phone) mode.
Features Status	Simultaneous ringing	Indicates whether the simultaneous ringing feature is enabled
	Call forwarding	Indicates whether the call forwarding feature is enabled
	Call Park	Indicates whether the call park feature is enabled
	Call transfer	Indicates whether the call transfer feature is enabled
	Delegation	Indicates whether the Delegation (assign a delegate or being assigned to be a delegate) feature is enabled.

Status	Display Name	Description
	Teamcall	Indicates whether the Teamcall (the supervisor's phone and the team-call group will ring simultaneously when the supervisor receives a call) feature is enabled
Data	Calendar Number	Indicates the total number of calendars downloaded from the server.
	Contact Number	Indicates the total number of the user's Skype for Business contacts.
	Outlook Contacts Number	Indicates the total number of the user's Outlook contacts.
	Call logs Number	Indicates the total number of call logs downloaded from the server.
	Visual Voicemail Number	Indicates the total number of voice mails downloaded from the server.
Exchange	Calendar Status	Indicates whether the Exchange calendar feature is enabled. If it is enabled, the calendar on the phone is synchronized with the Exchange server.
	Contact Status	Indicates whether to download Outlook contact from the Exchange server to the phone.
	Calllog Status	Indicates whether the Exchange call log feature is enabled. If it is enabled, call logs on the phone are synchronized with the Exchange server.
	VoiceMail Status	Indicates whether the Exchange voice mail feature is enabled.
		If it is enabled, the user can retrieve voicemails stored on the Exchange server
	EWS URL	Indicates the Microsoft Exchange server address.

Log Files

Log files are essential when troubleshooting phone issues. Log files contain information about phone activities and the phone's configuration profile.

The log files can be generated on the phone or syslog messages can be sent to the syslog server in real time.

Local Log

The log can be kept on the phone or the local log files can be uploaded to the provisioning server. The severity level of the local log can be configured. By default, the local log level is normal.

The Local log can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the Local log feature. **Parameter:** static.local_log.enable
		Configure the severity level of the logs to be reported to the sys.log file. **Parameter:** static.local_log.level
		Configure the maximum size of the log files to be stored on the phone. **Parameter:** static.local_log.max_file_size
		Configure the maximum size of the local log files to be stored on the server. **Parameter:** static.auto_provision.local_log.backup.append .max_fil e_size
		Configure the phone to upload local log files to the server. **Parameter:** static.auto_provision.local_log.backup.enable
		Configure the period of the local log file uploads to the server. **Parameter:** static.auto_provision.local_log.backup.upload _period
		Configure the behavior when local log files on the server reach the maximum size. **Parameter:** static.auto_provision.local_log.backup.append .limit_ mode
		Configure whether the local log files on the server are overwritten or appended. **Parameter:** static.auto_provision.local_log.backup.append
		Configure the waiting time after bootup before the phone uploads the boot.log file to the server. **Parameter:** static.auto_provision.local_log.backup.bootlo g.uploa d_wait_time

		Configure the upload path for the local log files. **Parameter:** static.auto_provision.local_log.backup.path
Local	**Web User Interface**	Configure the Local log feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-config&q=load

Details of the Configuration Parameters

Parameter	Permitted Values	Default
static.local_log.enable	**0 or 1**	**1**
Description: Enables or disables recording the log files locally. **0**- Disabled, the phone will not record log files locally. Previously recorded log files are still kept on the phone. **1**- Enabled, the phone will record log files locally. The local log files can be uploaded to the provisioning server, or a specific server, or they can be exported to the local PC. **Note**: Do not disable this feature. **Web User Interface:** Settings > Configuration > Local Log Switch **Phone User Interface:** None		
static.local_log.level	**5 or 6**	**Refer to the following content**
Description: Configures the level of local log information to be reported to the sys.log file and sipsignal.log file. **5**- Normal **6**- Debug **Default Value**: 6 **Web User Interface:** Settings > Configuration > Local Log Level **Phone User Interface:** None		

Parameter	Permitted Values	Default
static.local_log.max_file_size	1 kb to 5120 kb	Refer to the following content

Description:

Configures the maximum size (in KB) of the log files to be stored on the phone.

1- If the local log files are configured to be uploaded to the server by the parameter "static.auto_provision.local_log.backup.enable", the phone will clear all the local log files on the phone once the local log files are backed up successfully.

2- If the value of the parameter "static.auto_provision.local_log.backup.enable" is set to 0 (Disabled), the phone will erase half of the logs starting from the oldest log information on the phone.

Permitted Values:
Integer from 1 kb to 5120 kb

Default Value:
5120 kb

Example: static.local_log.max_file_size = 1024

Web User Interface:
Settings > Configuration > Max Log File Size (1024-2048KB)

Phone User Interface:
None

static.auto_provision.local_log.backup.enable	0 or 1	0

Description:

Enables or disables uploading the local log files to the provisioning server or to a specific server.

0- Disabled

1- Enabled, the phone will upload the local log files to the provisioning server or to the specific server to back up these files when one of the following happens:

- Auto provisioning is triggered;
- The size of the local log files reaches the maximum limit configured by the parameter "static.local_log.max_file_size";
- Local log files are uploaded according to the upload period configured by the parameter "static.auto_provision.local_log.backup.upload_period".

Note: The upload path is configured by the parameter "static.auto_provision.local_log.backup.path".

Web User Interface:
Settings > Configuration > Enable log backup

Phone User Interface:
None

Parameter	Permitted Values	Default
static.auto_provision.local_log.backup.path	URL within 1024 characters	Blank
Description: Configures the upload path for the local log files. If left blank, the phone will upload the local log files to the provisioning server. If a relative URL (e.g., /upload) is configured, the phone will upload the local log files by extracting the root directory from the access URL of the provisioning server. If an absolute URL with protocol (e.g., tftp) is configured, the phone will upload the local log files using the desired protocol. If no protocol is specified+, the phone will use the same protocol with auto provisioning for uploading files. **Example:** static.auto_provision.local_log.backup.path = tftp://10.3.6.133/upload/ **Note**: This feature works only if the value of the parameter "static.auto_provision.local_log.backup.enable" is set to 1 (Enabled). **Web User Interface:** Settings > Configuration > Backup Server URL **Phone User Interface:** None		
static.auto_provision.local_log.backup.upload_period	Integer from 30 to 86400	180
Description: Configures the period (in seconds) of the local log file uploads to the provisioning server or to a specific server. **Example:** static.auto_provision.local_log.backup.upload_period = 180 **Note**: This feature works only if the value of the parameter "static.auto_provision.local_log.backup.enable" is set to 1 (Enabled). **Web User Interface:** Settings > Configuration > Log backup interval **Phone User Interface:** None		
static.auto_provision.local_log.backup.append	0 or 1	0
Description: Configures whether the local log files on the provisioning server or on a specific server are overwritten or appended. **0**- Overwrite **1**- Append (not applicable to TFTP Server) **Web User Interface:** Settings > Configuration > Backup Mode **Phone User Interface:** None		

Parameter	Permitted Values	Default
static.auto_provision.local_log.backup.append.max_file_size	**Integer from 200 to 65535**	**1024**
Description: Configures the maximum size (in KB) of the local log files to be stored on the provisioning server or a specific server. **Example:** static.auto_provision.local_log.backup.append.max_file_size = 1024 **Web User Interface:** Settings > Configuration > Max size for backup log **Phone User Interface:** None		
static.auto_provision.local_log.backup.append.limit_mode	**0 or 1**	**0**
Description: Configures the behavior when local log files on the provisioning server or a specific server reach the maximum size limit. **0**- Delete, the server will delete the old log and the phone will continue to uploading log files. **1**- Stet, the phone will stop uploading log files. **Web User Interface:** Settings > Configuration > Backup limit mode **Phone User Interface:** None		
static.auto_provision.local_log.backup.bootlog.uploa d_wait_time	**Integer from 1 to 86400**	**120**
Description: Configures the waiting time (in seconds) before the phone uploads the boot.log file to the provisioning server or to a specific server after startup. **Example:** static.auto_provision.local_log.backup.bootlog.upload_wait_time = 121 **Web User Interface:** Settings > Configuration > Bootlog backup time **Phone User Interface:** None		

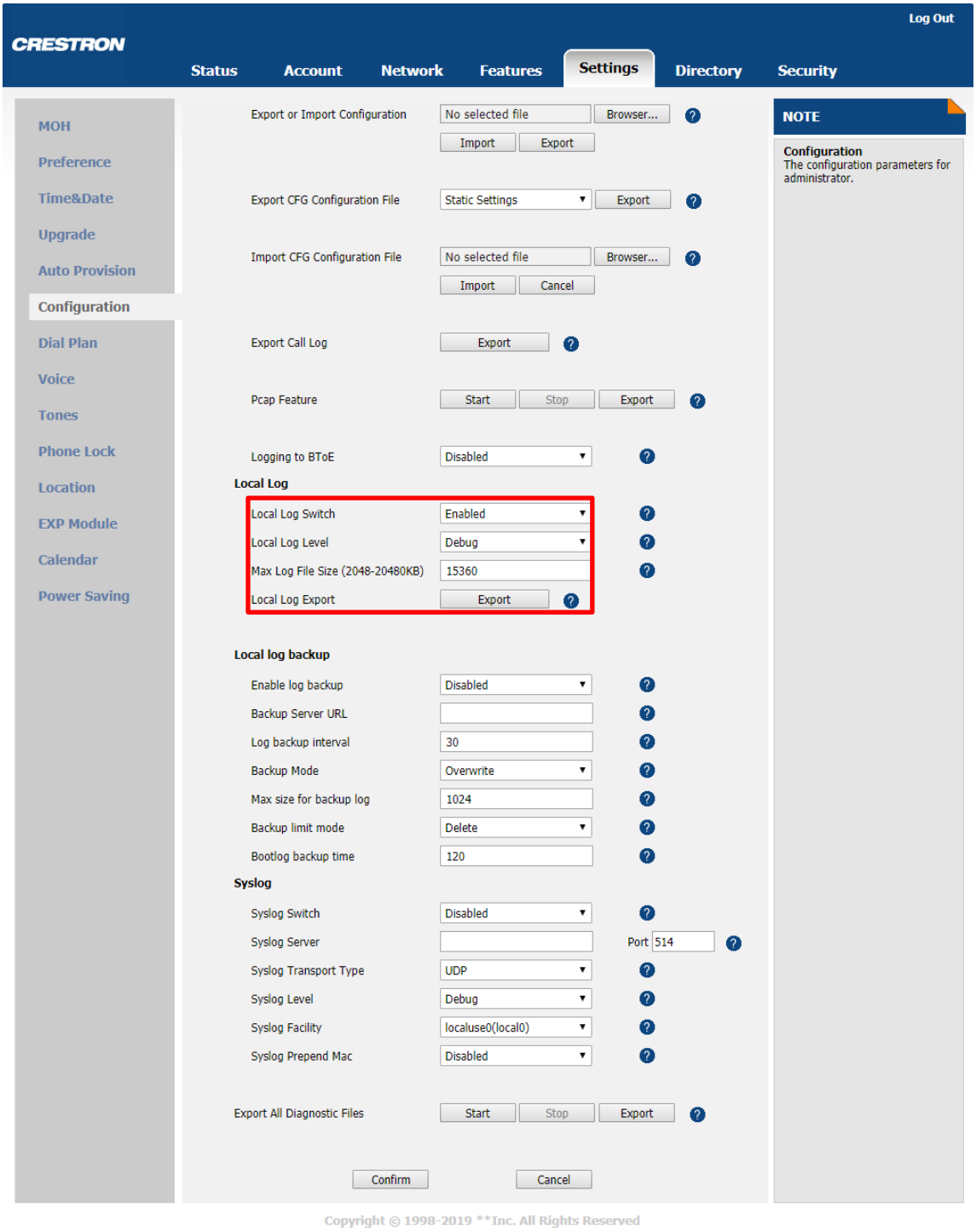
Export the Log Files to a Local PC

Local log files can be exported to a computer via the Web User Interface. The exported local log files include three types: boot.log, sys.log, and sipsignal.log. The sipsignal.log appears only when the local log level is adjusted to debug and the phone receives or sends SIP message. These three local log files can be exported via the Web User Interface simultaneously.

Export the Local Log File to a Local PC via the Web User Interface:

1. Click **Settings** > **Configuration**.

Settings > Configuration



2. Select **Enabled** from the **Local Log Switch** drop-down list.

3. Select **Debug** from the **Local Log Level** drop-down list of. The default local log level is **Normal**.
4. Limit size of the log files in the **Max Log File Size (1024-2048KB)** field.
5. Click **Confirm** to accept the change.
6. Reproduce the issue.
7. Click **Export** to open the file download window, and then save the file to the local system.

Export the Log File to the Skype for Business Server

The log file can be uploaded to the Skype for Business Server via the Phone User Interface only. When uploading a log, the HTTP POST sent from phone has the following headers:

- UCDevice_Type: "with a value of "3PIP".
- UCDevice_ID: containing a unique string identifying the phone. The UCDevice_ID contains at minimum the following entries:
  - VendorName-phone manufacturer name
  - DeviceModel-phone model
  - Firmware version
  - MAC address

  Example:

  UCDevice_ID: Crestron_UC-PHONE-S_66.9.0.30_00156574B1D6E\r\n

  UCDevice_Type: 3PIP\r\n

To export a log file to the Skype for Business Server via phone user interface:

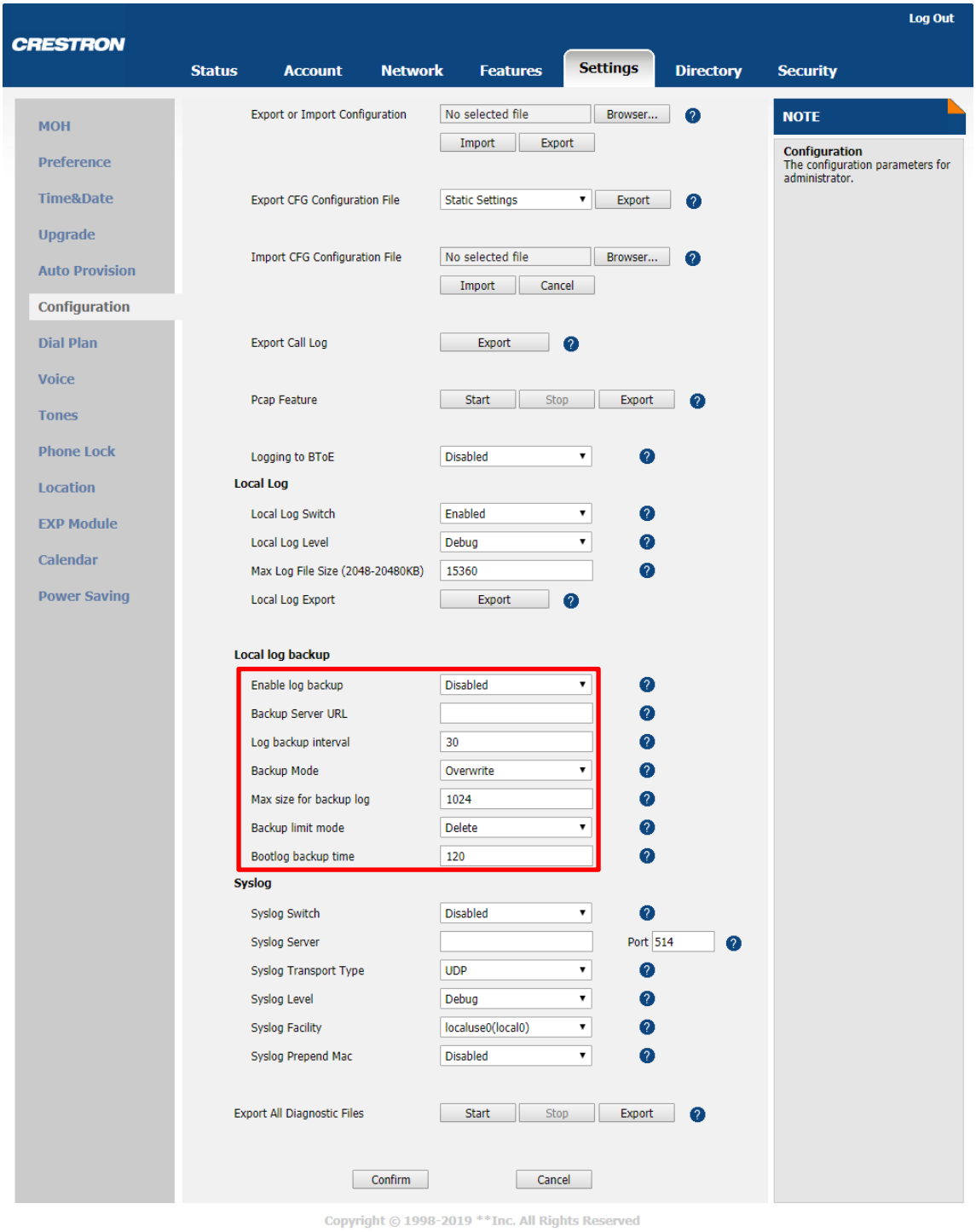
1. Tap **Setting** > **Basic** > **Log Upload**.
2. Tap **Log Upload**. A dialog box displays "Log Uploaded Successfully!".

The log file can be found on the Skype for Business Server at %ocsfilestore%\%domain%- WebServices-1\DeviceUpdateLogs\Cient.

Back Up the Local Log Files to a Server via the Web User Interface

1. Click **Settings** > **Configuration**.

Settings > Configuration



2. Select **Enabled** from the **Enable log backup** drop-down list.
3. Enter the path in the **Backup Server URL** field.

4. Enter the interval (in seconds) in the **Log backup interval** field. The local log files (boot.log and sys.log) will be uploaded to the server at intervals.
5. Select the mode from the **Backup Mode** drop-down list.
   - Select **Overwrite**, to overwrite the old local log files with the new uploaded local log files.
   - Select **Append** (not applicable to TFTP Server) to append the new uploaded local log files to the existing local log files.
6. Enter the maximum size of the local log files that can be stored on the server in the **Max size for backup log** field.
7. Select mode from the **Backup limit mode** drop-down list.
   - Select **Delete** to delete the old local log and start over when the server reaches its capacity.
   - Select **Stet** to have the phone stop uploading the local log when the server reaches its capacity.
8. Enter the time (in seconds) in the **Bootlog backup** time field. It configures the waiting time (in seconds) before the phone uploads the <MAC>- boot.log file to the server after startup.
9. Click **Confirm** to accept the changes.

Syslog

The phone can be configured to send syslog messages to a syslog server in real time.

Syslog logging can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the syslog feature. **Parameter:** static.syslog.enable
		Configure the syslog server. **Parameter:** static.syslog.server
		Configure the syslog level. **Parameter:** static.syslog.level
Local	Web User Interface	Configure the syslog feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=seettings-config&q=load

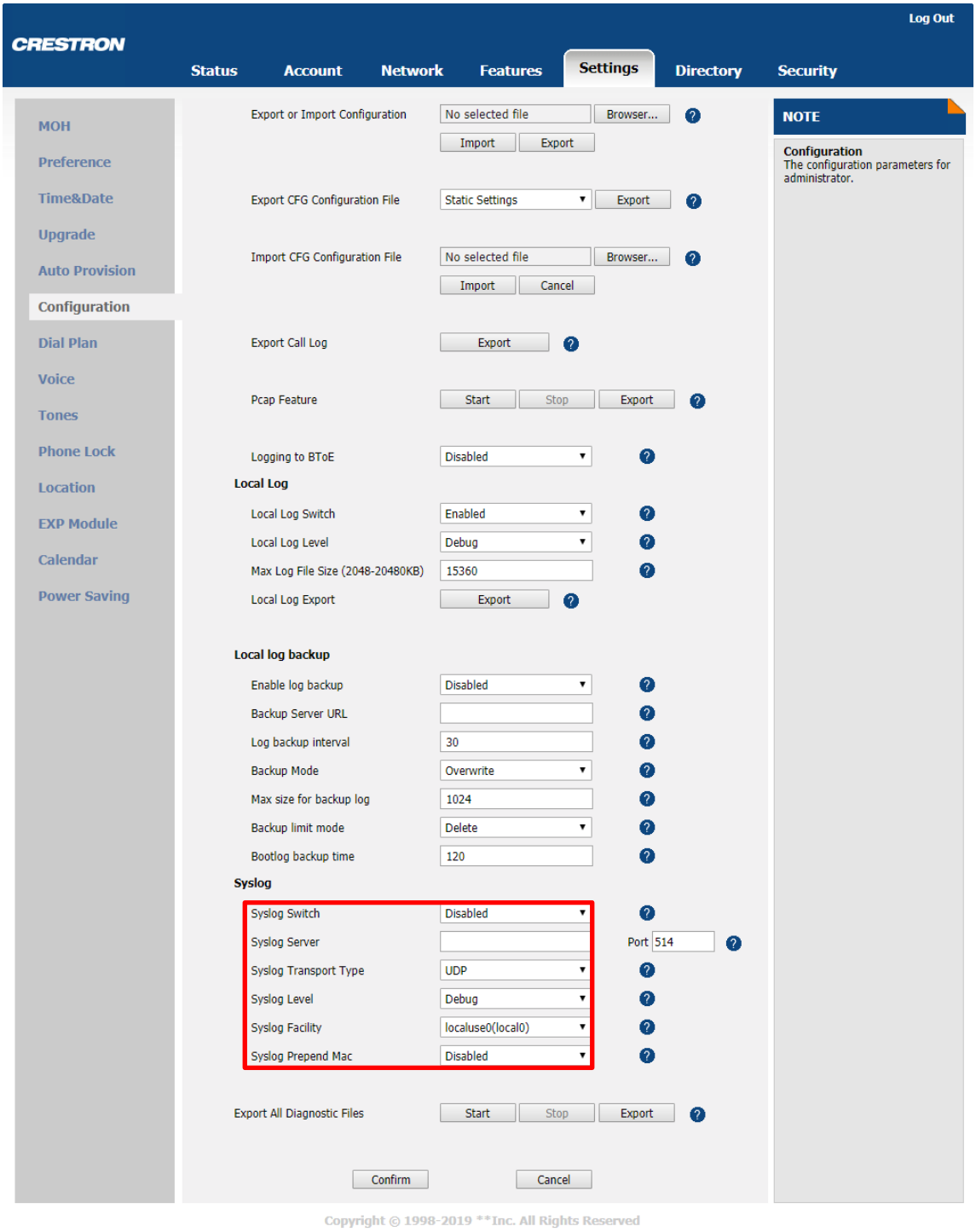
Details of the Configuration Parameters

Parameter	Permitted Values	Default
static.syslog.enable	0 or 1	0
Description: Enables or disables uploading log messages to the syslog server. **0**- Disabled **1**- Enabled **Web User Interface:** Settings > Configuration > Syslog Switch **Phone User Interface:** None		
static.syslog.server	IP address or domain name	Blank
Description: Configures the IP address or domain name of the syslog server. **Example:** static.syslog.server = 192.168.1.100 **Web User Interface:** Settings > Configuration > Syslog Server **Phone User Interface:** None		
static.syslog.level	5 or 6	5
Description: Configures the level of syslog information displayed in the syslog. **5**- Normal **6**- Debug **Web User Interface:** Settings > Configuration > Syslog Level **Phone User Interface:** None		

Export the Log Files to a Syslog Server via the Web User Interface

1. Click **Settings** > **Configuration**.

Settings > Configuration



2. Select **Enabled** or **Disabled** from the **Syslog Switch** drop-down list.
3. Enter the syslog server address in the **Syslog Server** field.

4. Enter the syslog server port in the **Port** field.
5. Select the transport type from the **Syslog Transport Type** drop-down list. It configures the transport protocol the phone uses when exporting log messages to the syslog server.
6. Select the log level from the **Syslog Level** drop-down list. When choosing a log level, all events of an equal or higher severity level are included and events of a lower severity level are excluded.
7. Select the facility from the **Syslog Facility** drop-down list. It configures the facility that generates the log messages.
8. Select **Enabled** or **Disabled** from the **Syslog Prepend Mac** drop-down list. It configures whether the uploaded log messages have the phone MAC address or not.
9. Click **Confirm** to accept the changes.

View the Syslog Message

The syslog file stored in the specified folder on the syslog server can be viewed. The location of the folder may differ from the syslog server. For more information, refer to the network resources.

The following figure shows a portion of the syslog:

Syslog

```
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek read (0,256) ret 256 [sgfc]
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek read (0,256) ret 256 [sgfc]
Jul 14 03:38:48 cfg [451]: CFG <4+warnin> write all 0, len 40960, offset 8346, changed 4, used 124, node_set 1021 to 1021
Jul 14 03:38:48 cfg [451]: CFG <4+warnin> 1462 buf remain 667054
Jul 14 03:38:48 cfg [451]: CFG <4+warnin> 1489 buf remain 667054
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write cnt 4
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write [3363,44] [syslog.log_level]
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write [4942,49] [syslog.server]
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write [5158,40] [syslog.level]
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write [6884,41] [syslog.enable]
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write [0,256] [sgfc]
Jul 14 03:38:48 cfg [451]: CFG <4+warnin> backup cfg
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write [0,256] [sgfc]
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write cnt 4
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write [3363,44] [syslog.log_level]
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write [4942,49] [syslog.server]
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write [5158,40] [syslog.level]
Jul 14 03:38:48 cfg [451]: CFG <5+notice> seek write [6884,41] [syslog.enable]
```

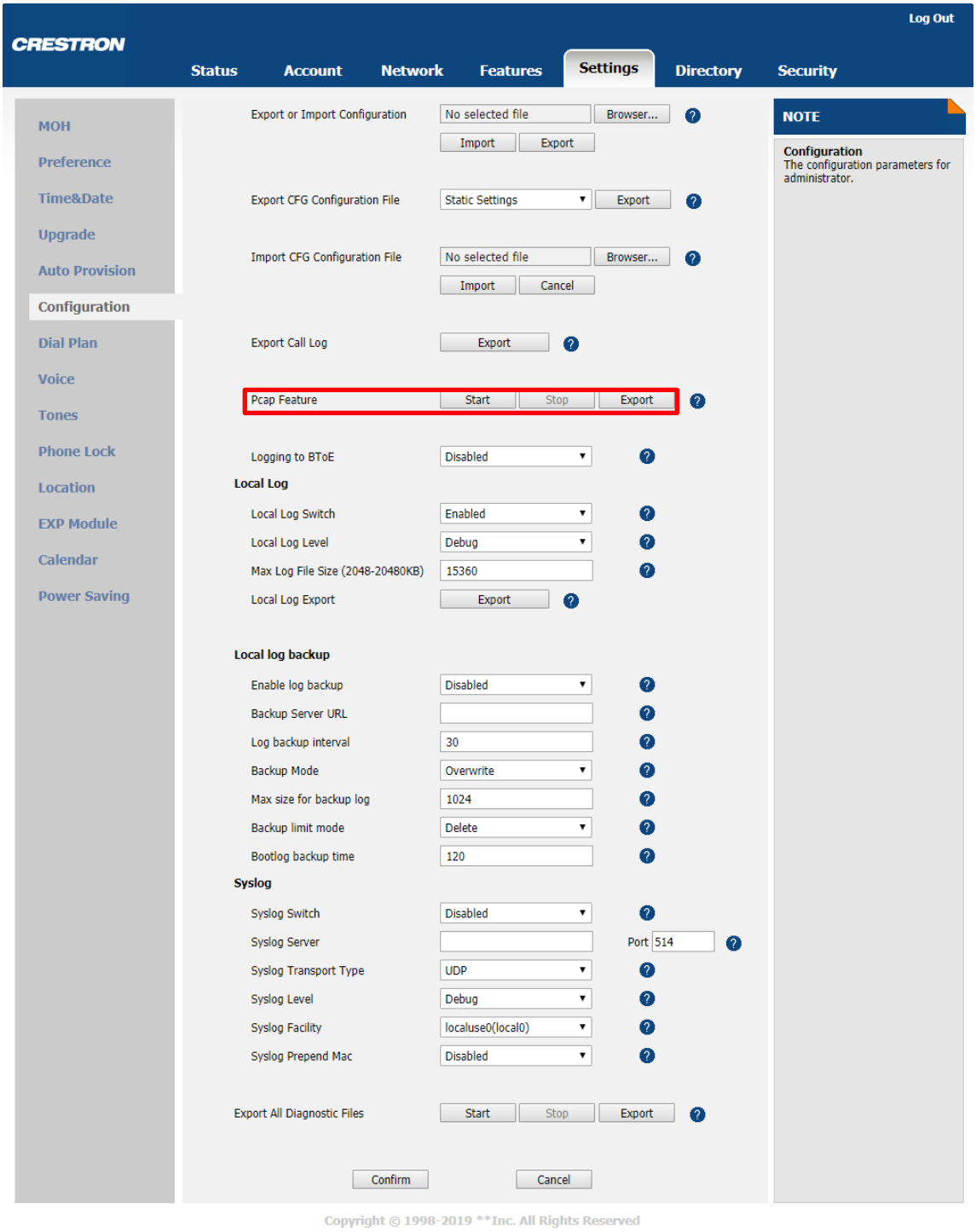
Capture Packets

Packets can be captured in two ways: via the Web User Interface or using the Ethernet software. The captured packets can be analyzed for troubleshooting purposes.

Capture Packets via the Web User Interface

1. Click **Settings** > **Configuration**.

Settings > Configuration



2. In the **Pcap Feature** field, click **Start** to start capturing signal traffic.
3. Reproduce the issue to get stack traces.

4. Click **Stop** to stop capturing.
5. Click **Export** to open the file download window, and then save the file to the local system.

Capture the Packets with the Ethernet Software

Data packets can be received from the network hub, or from the phone's PC port.

To receive data packets from the hub, connect the Internet port of the phone and the PC to the same hub, and then use packet analyzer software to capture the signal traffic.

To receive data packets from the PC port, connect the Internet port of the phone to the Internet and the PC port of the phone to a PC. Before capturing the signal traffic, make sure the data packets can be received from the WAN (Internet) port to the PC (LAN) port.

The span to PC Port can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the span to PC Port. **Parameter:** static.network.span_to_pc_port
Local	Web User Interface	Configure the span to PC Port. **Navigate to:** http://<phoneIPAddress/servlet?p=network-adv&q=load

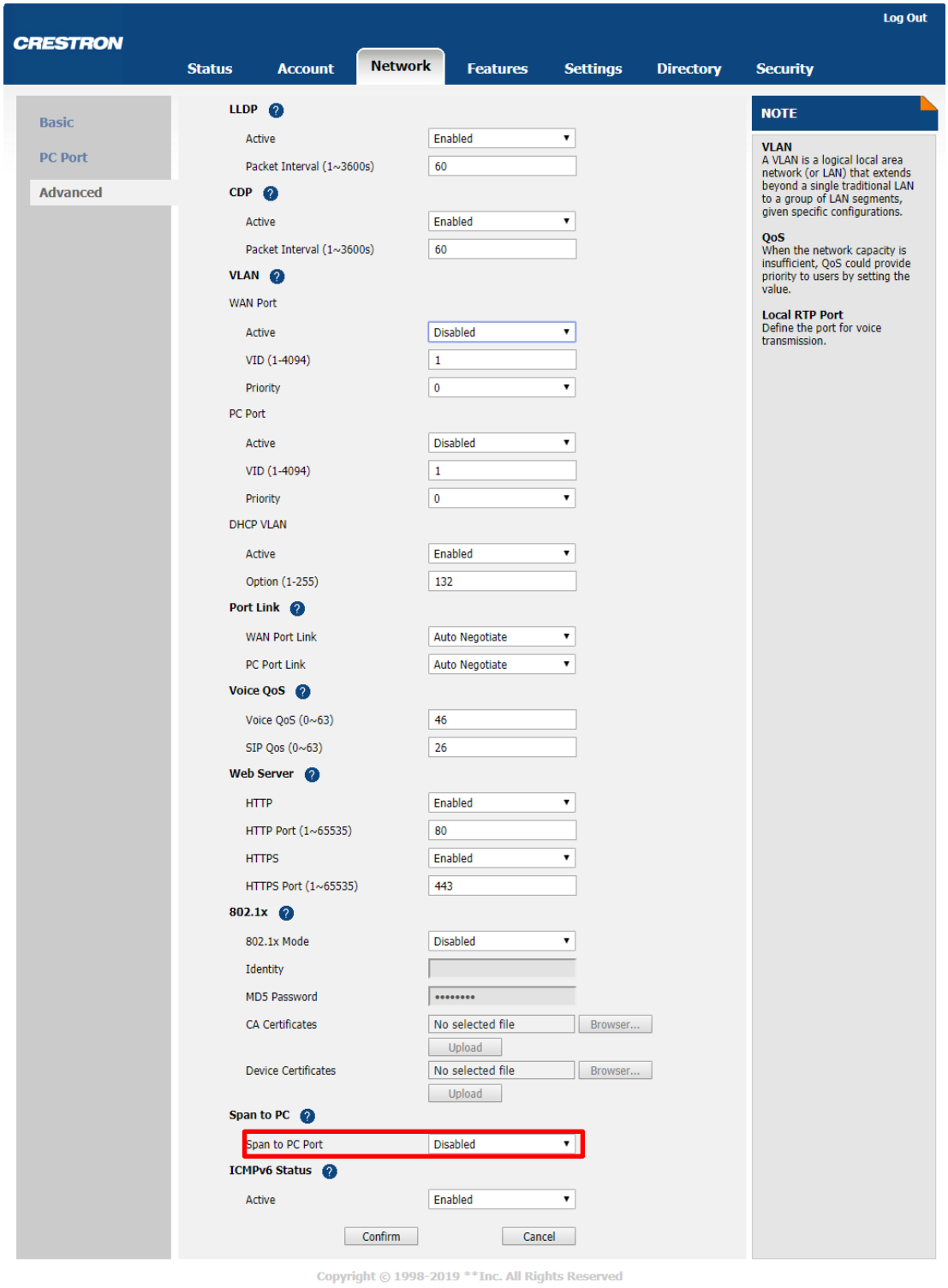
Details of the Configuration Parameter

Parameter	Permitted Values	Default
static.network.span_to_pc_port	**0 or 1**	**0**
Description: Enables or disables spanning data packets received from the WAN (Internet) port to the PC (LAN) port. **0**- Disabled **1**- Enabled, all data packets from WAN (Internet) port can be received by the PC port. **Note:** This feature works only if the value of the parameter "static.network.pc_port.enable" is set to 1 (Auto Negotiate). If the parameter is changed, the phone will reboot to effect the change. **Web User Interface:** Network > Advanced > Span to PC > Span to PC Port **Phone User Interface:** None		

Enable the Span to PC Port via the Web User Interface

1. Click **Network** > **Advanced**.

Network > Advanced



2. Select **Enabled** from the **Span to PC Port** drop-down list.
3. Click **Confirm** to accept the change. A dialog box pops up to prompt that settings will take effect after a reboot.
4. Click **OK** to reboot the phone.
5. Use packet analyzer software to capture the signal traffic.

Enable Watch Dog Feature

The Skype for Business phone provides a troubleshooting feature called Watch Dog, which helps monitor the phone status and get stack traces from the last time the phone failed. If the Watch Dog feature is enabled, the phone will automatically reboot when it detects a fatal failure. This feature can be configured using the configuration files or via web user interface.

Watch dog can be configured using the configuration files or locally.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the Watch Dog feature. **Parameter:** static.watch_dog.enable
Local	Web User Interface	Configure the Watch Dog feature. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-preference&q=load

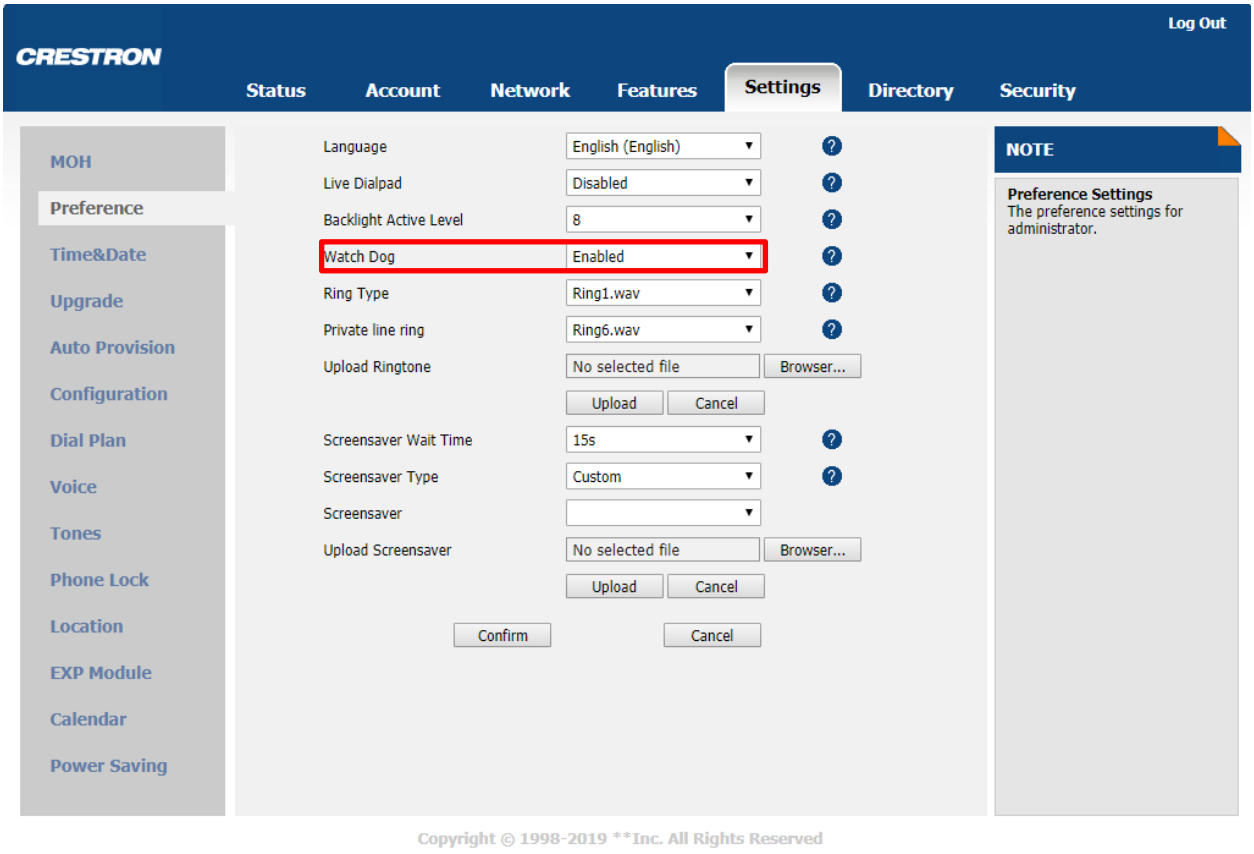
Details of the Configuration Parameter

Parameter	Permitted Values	Default
static.watch_dog.enable	**0 or 1**	**1**
Description: Enables or disables the Watch Dog feature. **0**- Disabled **1**- Enabled, the phone will reboot automatically when the system crashed. **Web User Interface:** Settings > Preference > Watch Dog **Phone User Interface:** None		

Configure the Watch Dog feature via the Web User Interface

1. Click **Settings** > **Preference**.

Settings > Preference



2. Select **Enabled** or **Disabled** from the pull-down list of **Watch Dog**.
3. Click **Confirm** to accept the change.

Get Information from Status Indicators

Status indicators may consist of the power LED, MESSAGE key LED, line key indicator, headset key indicator, and the on-screen icon.

The following shows two examples of obtaining the phone information from status indicators on Skype for Business phones:

- If a LINK failure of the phone is detected, a prompting message "Network unavailable" is displayed on the LCD screen.
- If a voice mail is received, the Power LED Indicator slowly flashes red.
- If a Skype for Business favorite is during a call, the line key LED indicator glows red.

Analyze Configuration Files

Configuration file(s) can be exported in order to check the current configuration of the phone and troubleshoot if necessary. Configuration files can also be imported for quick and easy configuration.

Seven types of configuration files can be exported to the local system:

- config.bin
- <MAC>-local.cfg
- <MAC>-inband.cfg
- <MAC>-config.cfg
- <MAC>-static.cfg
- <MAC>-non-static.cfg
- <MAC>-all.cfg

BIN Configuration Files

The config.bin file is an encrypted file. For more information on config.bin file, contact Crestron True Blue Support at www.crestron.com/support.

Configuration changes can be performed using the following methods.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Specify the access URL for the custom configuration files. **Parameter:** static.configuration.url
Local	Web User Interface	Export or import the custom configuration files. **Navigate to**: http://<phoneIPAddress>/servlet?p=settings-config&q=load

Details of the Configuration Parameter

Parameter	Permitted Values	Default
static.configuration.url	URL within 511 characters	Blank

Description:

Configures the access URL for the custom configuration files.

Note: The file format of the custom configuration file must be *.bin. If the parameter is changed, the phone will reboot to make the change take effect.

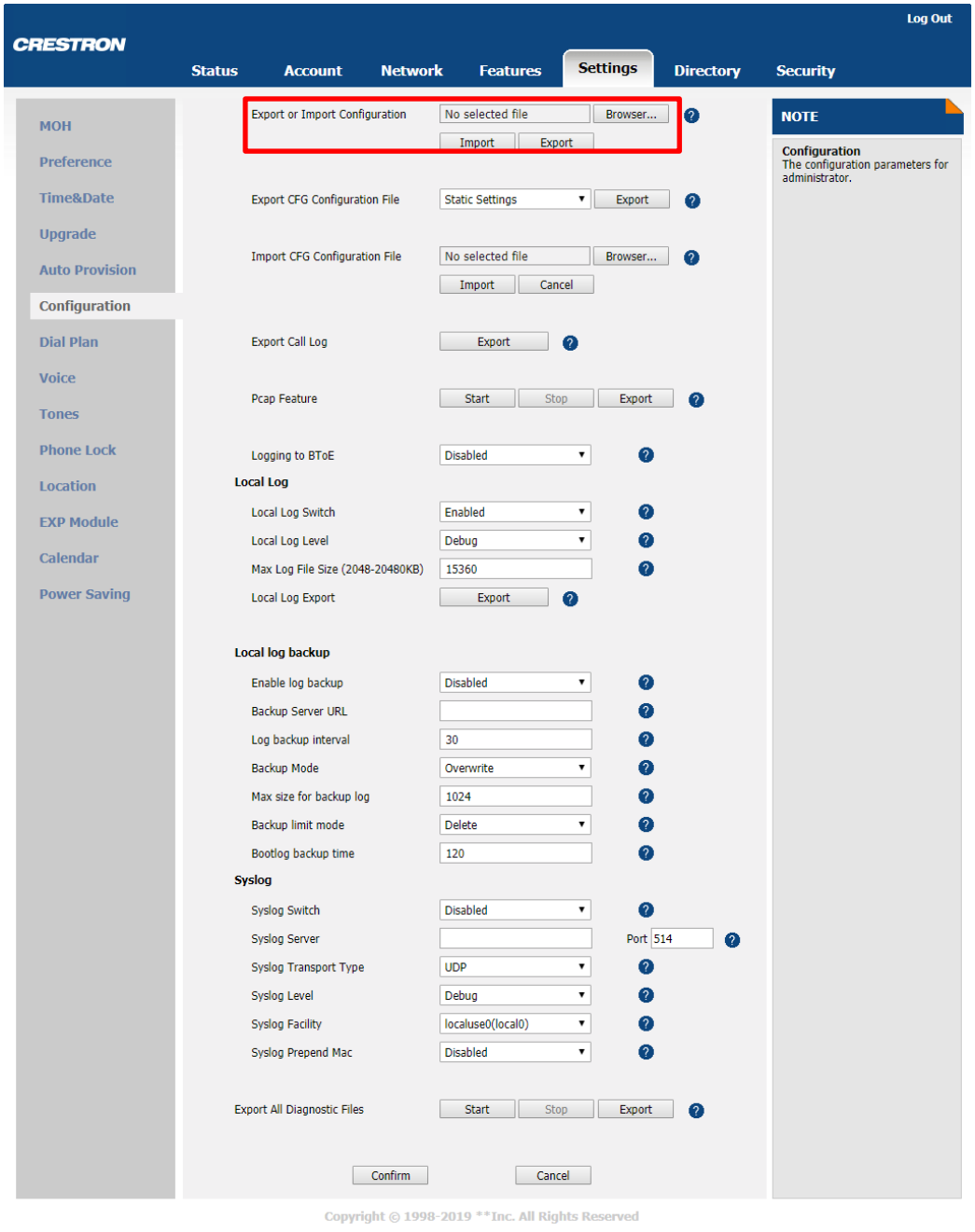
Web User Interface:
Settings > Configuration > Export or Import Configuration

Phone User Interface:
None

Export a BIN Configuration File via the Web User Interface

1. Click **Settings** > **Configuration**.

Settings > Configuration

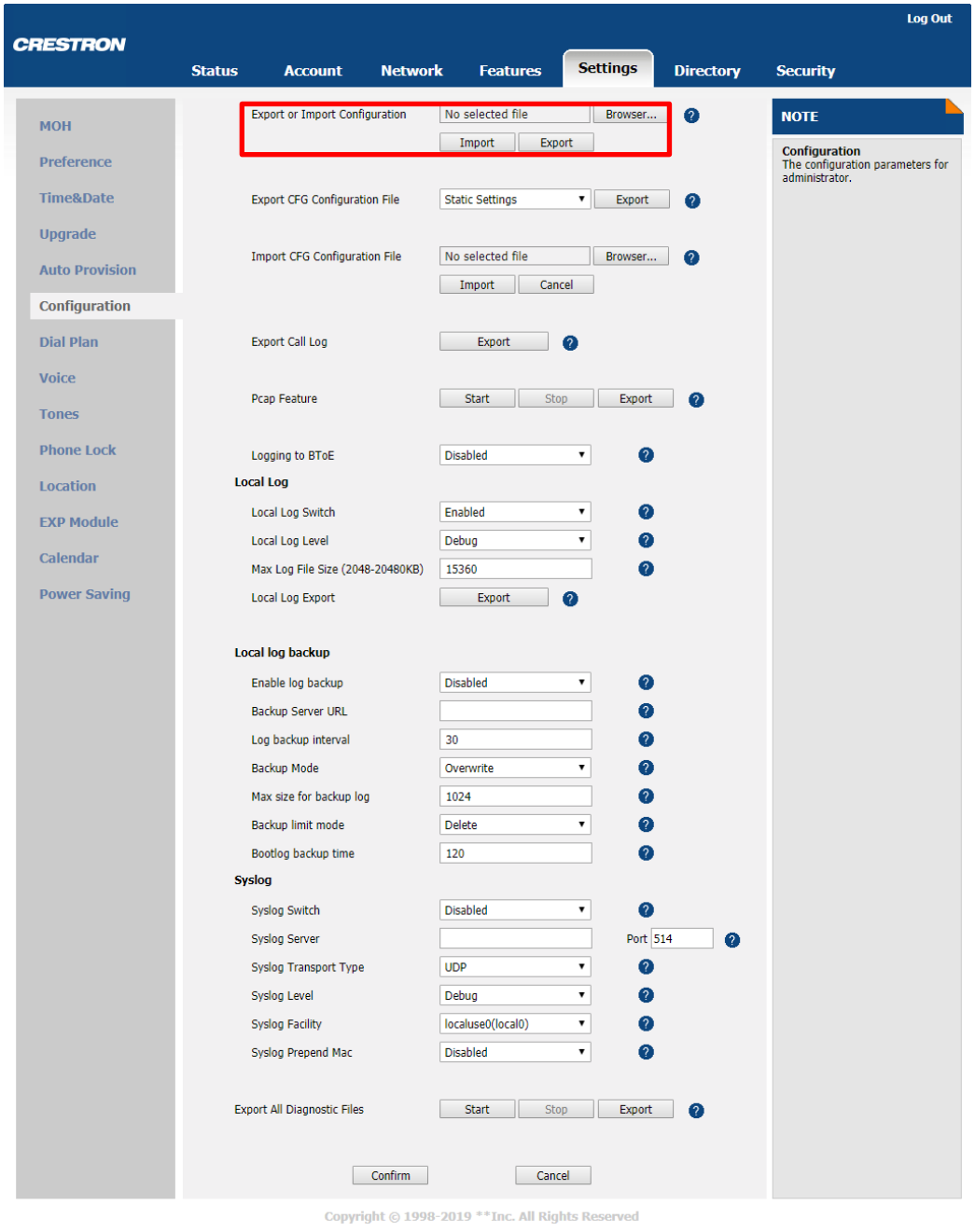


2. In the **Export or Import Configuration** section, click **Export** to open the file download window, and then save the file to the local system.

Import a BIN Configuration File via the Web User Interface

1. Click **Settings** > **Configuration**.

Settings > Configuration



2. In the **Export or Import Configuration** section, click **Browser** to locate a BIN configuration file from the local system.
3. Click **Import** to import the configuration file.

CFG Configuration Files

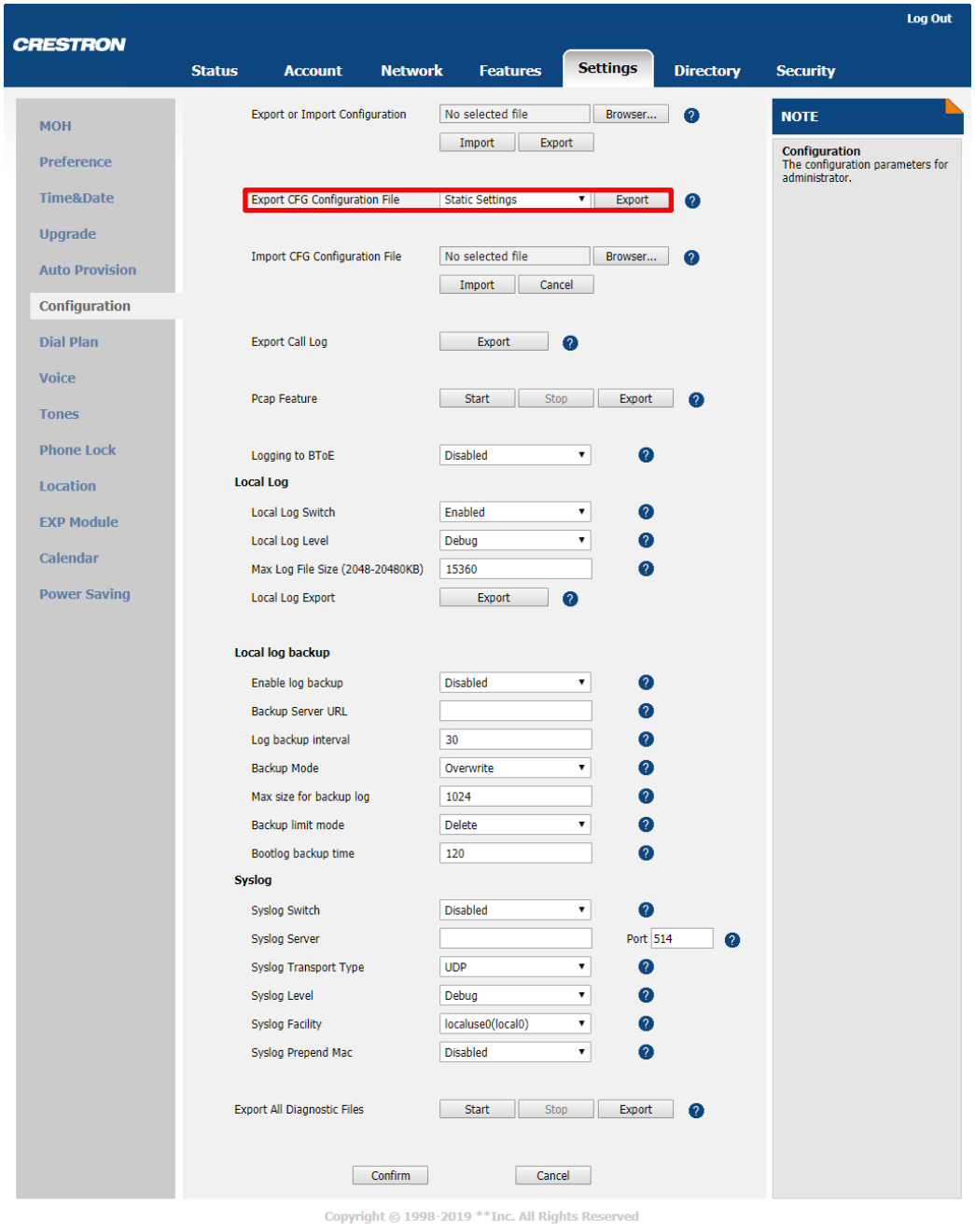
The following CFG configuration files can be exported:

- **<MAC>-local.cfg**: This file contains changes associated with non-static settings made via the Phone User Interface and the Web User Interface. It can be exported only if the value of the parameter "static.auto_provision.custom.protect" is set to 1.
- **<MAC>-inband.cfg:** This file contains configurations sent from the Skype for Business server. It can be exported only if the value of the parameter "static.auto_provision.custom.protect" is set to 1.
- **<MAC>-config.cfg**: This file contains changes associated with non-static settings made using configuration files. It can be exported only if the value of the parameter "static.auto_provision.custom.protect" is set to 1.
- **<MAC>-static.cfg**: This file contains all changes associated with static settings (for example, network settings).
- **<MAC>-non-static.cfg**: This file contains all changes associated with non-static settings.
- **<MAC>-all.cfg**: This file contains all changes made via the Phone User Interface, the Web User Interface, configuration files, and in-band provisioning.

Export a CFG Configuration File via the Web User Interface

1. Click **Settings** > **Configuration**.

Settings > Configuration



2. Select the CFG configuration file from the **Export CFG Configuration File** drop-down list.
3. Click **Export** to open the file download window, and then save the file to the local system.

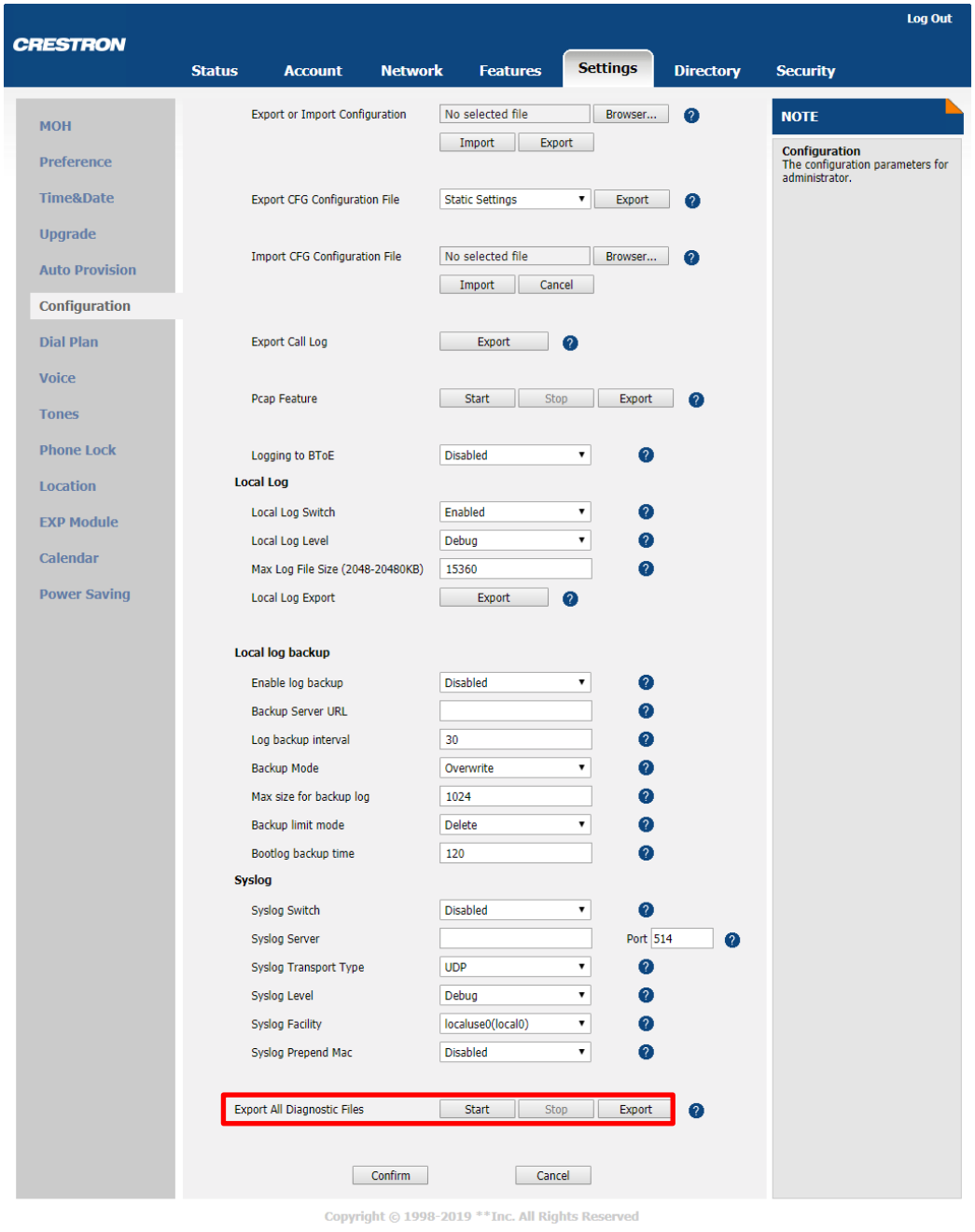
Export All Diagnostic Files via the Web User Interface

The phones support three types of diagnostic files (including Pcap trace, log files (boot.log and sys.log), and BIN configuration files) to help analyze problems. These files can be exported. The file format of exported diagnostic file is *.tar.

To export the files:

1. Click **Settings** > **Configuration**.

Settings > Configuration



2. Click **Start** in the **Export All Diagnostic Files** field to begin capturing signal traffic. The local log level will be automatically set to 6.
3. Reproduce the issue.
4. Click **Stop** in the **Export All Diagnostic Files** field to stop the capture. The local log level will be automatically set to the previous setting.
5. Click **Export** to open file download window, and then save the diagnostic file to the local system. A diagnostic file named **allconfig.tgz** is successfully exported to the local system.

NOTE: If the issue cannot be reproduced, simply click **Export** to export all diagnostic files.

To view the diagnostic files on the local system:

1. Extract the combined diagnostic files to the local system.
2. Open the folder to which the files were extracted and identify the files to view.

The Pcap trace, log files (boot.log and sys.log), and BIN configuration files be selected for export.

For more information, refer to "Capture Packets" on page 356, "Log Files" on page 344, and "Analyze Configuration Files" on page 362.

Troubleshooting Solutions

This section describes solutions to common issues that may occur while using the phone. Upon encountering a scenario not listed in this section, contact Crestron True Blue Support at www.crestron.com/support.

IP Address Issues

The Phone Does Not Get an IP Address

Do one of the following:

- Ensure the Ethernet cable is plugged into the Internet port on the phone and the cable is not loose or damaged.
- Ensure the IP address and related network parameters are set correctly.
- Ensure the network switch or hub is good condition.

Solve an IP conflict

Do one of the following:

- Set another available IP address for the phone.

- Check the network configuration via the Phone User Interface at **Menu** > **Setting** > **Advanced** > **Network** > **WAN Port** > **IPv4** (or **IPv6**). If **Static IP** is selected, select **DHCP** instead.

Time and Date Issues

The Phone Does Not Display Time and Date Correctly

Check the phone to see if it is configured to obtain the time and date from the NTP server automatically. If the phone is unable to access the NTP server, configure the time and date manually.

Display Issues

The LCD Screen is Blank

Ensure that a PoE-compliant switch or hub is used.

Directory Issues

Difference Between a Skype for Business Directory and a Local Directory

The Skype for Business directory on the phone displays all Skype for Business contacts on the Skype for Business client. A local directory is written to the phone's flash memory. When signing into different phones using the same account, each phone displays the same Skype for Business contacts, while a local directory can only be viewed on a specific phone.

Audio Issues

Increase or Decrease the Volume

Press the volume key to increase or decrease the ringer volume when the phone is idle or ringing, or to adjust the volume of the active audio device (handset, speakerphone or headset) when a call is in progress.

Poor Sound Quality During a Call

Some possible reasons for poor sound quality/acoustics such as intermittent voice, low volume, echo, or other noises:

- Users are seated too far out of recommended microphone range and sound faint, or are seated too close to sensitive microphones and cause echo.
- Intermittent voice is mainly caused by packet loss, due to network congestion, and jitter, due to message recombination of transmission or receiving equipment (e.g., timeout handling, retransmission mechanism, buffer under run).

- Noisy equipment, such as a PC or a fan, may cause voice interference. Turn off any noisy equipment.
- Line issues can also cause this problem. Disconnect the old line and redial the call to check whether another line provides a better connection.

No Sound When the Other Party Answers the Call

If the caller and receiver cannot hear anything - there is no sound when the other party picks up, the possible reason could be the phone cannot send the real-time transport protocol (RTP) streams, in which audio data is transmitted, to the connected call.

Try to disable the 180 ring workaround feature. For more information, refer to "180 Ring Workaround" on page 204.

When Placing a Long-Distance Call Without Plus 0, the Phone Plays the Local Ringback Tone Instead of Media

Ensure that the 180 Ring Workaround feature is disabled. For more information, refer to "180 Ring Workaround" on page 204.

Bluetooth Issues

Phone Does Not Always Connect with Bluetooth Device

Delete the registration information of the Bluetooth device on both the phone and the Bluetooth device, and then pair and connect them again. Contact Crestron or the Bluetooth device manufacturer for more information.

Bluetooth Headset Affects Voice Quality

Bluetooth voice quality can be affected while the 2.4 GHz band is enabled or when used in an environment with many other Bluetooth devices. This possible loss in voice quality is due to the inherent limitations with Bluetooth technology.

Firmware and Upgrading Issues

Phone Does Not Update Firmware Successfully

Do one of the following:

- Ensure the target firmware is not the same as the current firmware.
- Ensure the target firmware is applicable to the phone model.
- Ensure the current or the target firmware is not protected.
- Ensure the power is on and the network is available during upgrade.
- Ensure the web browser is not closed or refreshed when upgrading firmware via the Web User Interface.

- Ensure the target firmware is available on the Skype for Business Server.

Phone Does Not Update the Configuration

Do one of the following:

- Ensure the configuration is set correctly.
- Reboot the phone. Some configurations require a reboot to take effect.
- Ensure the configuration is applicable to the phone model.
- The configuration may depend on support from a server.

Auto Provisioning

Auto provisioning refers to the update of phones, including updating configuration parameters, the local phone book, firmware, and so on. Auto provisioning can be used for a single phone, but it makes more sense in mass deployment.

System Log Issues

Can Not Export Log to a Syslog Server

Do one of the following:

- Ensure the syslog server supports saving the syslog files exported from phone.
- Ensure the syslog server address was configured correctly via the phone's Web User Interface.

Resetting Issues

If troubleshooting suggestions don't solve a problem, the phone can be reset to its factory default settings. Resetting the phone to factory default clears the flash parameters, removes log files, user data, and cached data, and resets the administrator password to admin. All custom settings will be overwritten.

NOTE: If the value of the parameter "static.auto_provision.custom.protect" is set to 1 in central provisioning, the phone supports five ways to reset the phone. If the value of the parameter "static.auto_provision.custom.protect" is set to 0 in central provisioning, the phone only supports Reset to factory to reset all configurations on the phone.

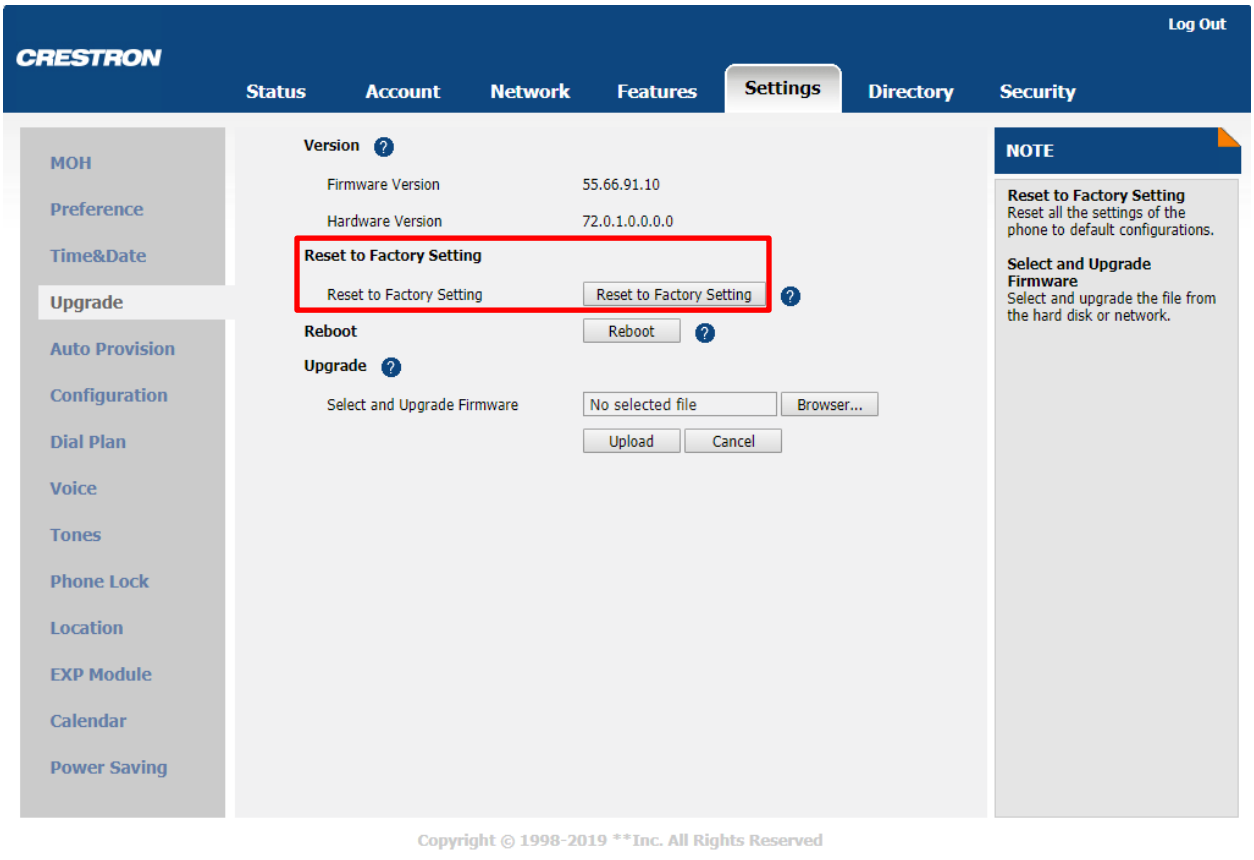
- **Reset Local settings**: All configurations saved in the <MAC>-local.cfg file on the phone will be reset. Changes associated with non-static settings made via the Web User Interface and the Phone User Interface are saved in the <MAC>-local.cfg file.
- **Reset Non-static Settings**: All non-static settings on the phone will be reset.
- **Reset StaticSettings**: All static settings on the phone will be reset.

- **Reset Userdata & Local config**: All the local cache data (for example, userdata, history, local directory) will be cleared, and all configurations saved in the <MAC>-local.cfg configuration file on the phone will be reset.
- **Reset To Factory**: Reset the phone to factory default settings.

Reset the Phone via the Web User Interface

1. Click **Settings** > **Upgrade**.

Settings > Upgrade



2. Click **Reset to Factory Setting**.

Reset the Phone to a Custom Factory Configuration

The phone can be reset to a custom factory configuration if required.

Some values in the default factory configuration file can be changed to generate a custom factory configuration file, which can then be imported to the phone. As a result, the custom factory configurations can be kept even if the phone is reset.

A custom factory configuration can be set using the following methods.

Configuration Methods

Central Provisioning (Configuration File)	**<y0000000000xx>.cfg**	Configure the Custom Factory Configuration feature. **Parameter:** static.features.custom_factory_config.enable
		Configure the access URL of the custom factory configuration file. **Parameter:** static.custom_factory_configuration.url
Local	Web User Interface	Configure the access URL of the custom factory configuration file. **Navigate to:** http://<phoneIPAddress>/servlet?p=settings-config&q=load

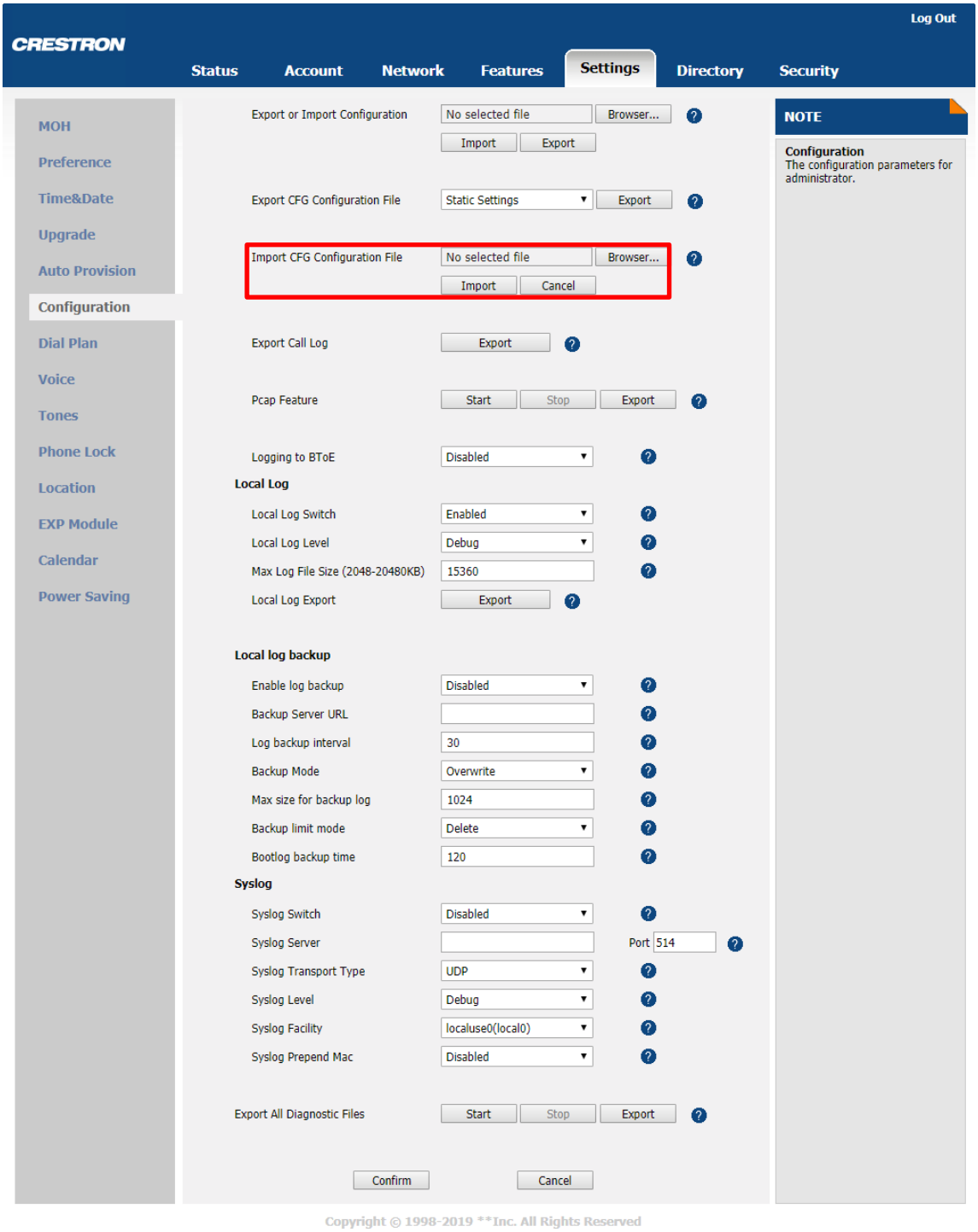
Details of the Configuration Parameters

Parameter	Permitted Values	Default
static.features.custom_factory_config.enable	**0 or 1**	**0**
Description: Enables or disables importing a custom factory configuration file. **0**- Disabled **1**- Enabled, **Import Factory Configuration** item will be displayed on the phone's Web User Interface at **Settings**->**Configuration**. A custom factory configuration file can be imported or deleted via the Web User Interface. **Web User Interface:** None **Phone User Interface:** None		
static.custom_factory_configuration.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom factory configuration file. **Note**: This feature works only if the value of the parameter "static.features.custom_factory_config.enable" is set to 1 (Enabled) and the custom factory configuration file is a .bin file. If the parameter is changed, the phone will reboot to effect the change. **Web User Interface:** Settings->Configuration->Import Factory Config **Phone User Interface:** None		

Import the Custom Factory Configuration Files via the Web User Interface

1. Click **Settings** > **Configuration**.

Settings > Configuration



2. Click **Browser** to locate the custom factory configuration file.

3. Click **Import**.

When the custom factory configuration file is imported successfully, the phone can be reset to the custom factory configuration. For more information on how to reset to factory configuration via the web user interface, refer to "Reset the Phone to a Custom Factory Configuration" on page 373.

User-defined factory configurations can be deleted via the Web User Interface.

Rebooting Issues

Reboot the Phone via the Web/Phone User Interface

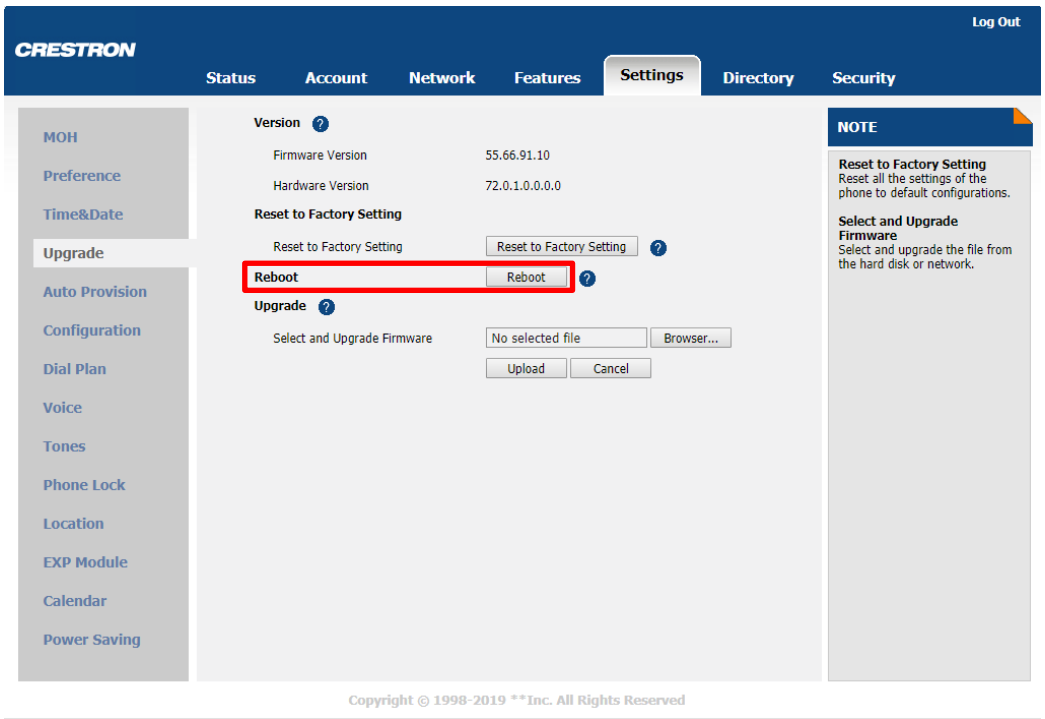
Reboot the Phone via the Phone User Interface:

1. Tap **Menu** > **Setting** > **Advanced** (default password: admin) > **Reboot**.
2. Tap **Reboot**.
3. Tap **OK**.

Reboot the Phone via the Web User Interface:

1. Click **Settings** > **Upgrade**.

Settings > Upgrade



2. Click **Reboot** to reboot the phone. Any reboot of the phone may take a few minutes.

Protocol and Port Issues

Supported Communication Protocols and Ports

Skype for Business Phones, Supported Protocols and Ports

Source Device	Source IP	Source Port	Destination Device	Destination IP	Destination Port (Listening port)	Protocol	Description of destination port
Skype for Business phones	IP address of Skype for Business phones	2~65535	Skype for Business phone or voice gateway	IP address of Skype for Business phone or voice gateway	Determined by destination device.	UDP	RTP protocol port, it is used to send or receive audio stream.
		1024~65535	File server	IP address of file server	Determined by destination device.	TCP	HTTP protocol port, it is used to download file.
		1024~65535	AA	IP address of AA	Determined by destination device.	TCP	HTTP protocol port, it is used for AA communi-cation.
		68	DHCP Server	IP address of DHCP server	67	UDP	DHCP protocol port, it is used to obtain the IP address from DHCP server.
		1024~65535	NTP Server	IP address of NTP server	123	UDP	NTP protocol port, it is used to synchronize time from NTP time server.

Source Device	Source IP	Source Port	Destination Device	Destination IP	Destination Port (Listening port)	Protocol	Description of destination port
		1024~65535	Syslog Server	IP address of syslog server	514	UDP	Syslog protocol port, it is used for Skype for Business phones to upload syslog information to syslog server.
PC	IP address of PC	Determined by the destination device.	Skype for Business phones	IP address of Skype for Business phones	1~65535	TCP	HTTP port (default value: 80)
					1~65535	TCP	HTTP port (default value: 443)
Skype for Business phone of voice gateway	Skype for Business phone or voice gateway				2~65535	UDP	RTP protocol port, it is used by destination device to send or receive audio stream.

Password Issues

Restore the Administrator Password

Performing a factory reset restores the original administrator password. All custom settings will be overwritten.

Power and Startup Issues

The Phone Has No Power

If no lights appear on the phone when it is powered up, do one of the following:

- Reboot the phone.
- Verify the connection to a PoE power source.

The LCD Screen is Black

If the Power LED Indicator is on and the keypad is usable but the LCD screen is black, reboot the phone.

Other Issues

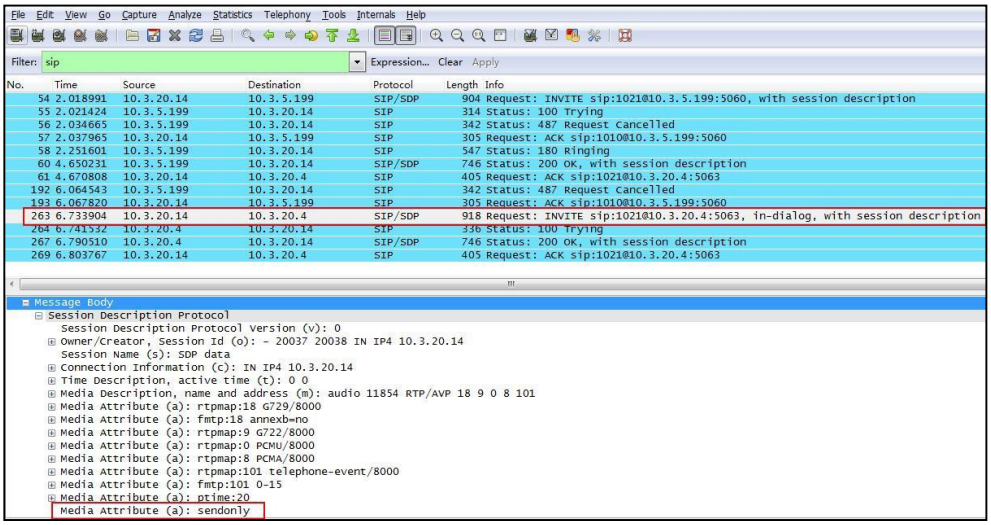
Find Basic Phone Information

Tap **Status** when the phone is idle to check the basic information (e.g., IP address, MAC address, and firmware version).

Difference Between Enabling and Disabling the RFC2453 Hold Feature

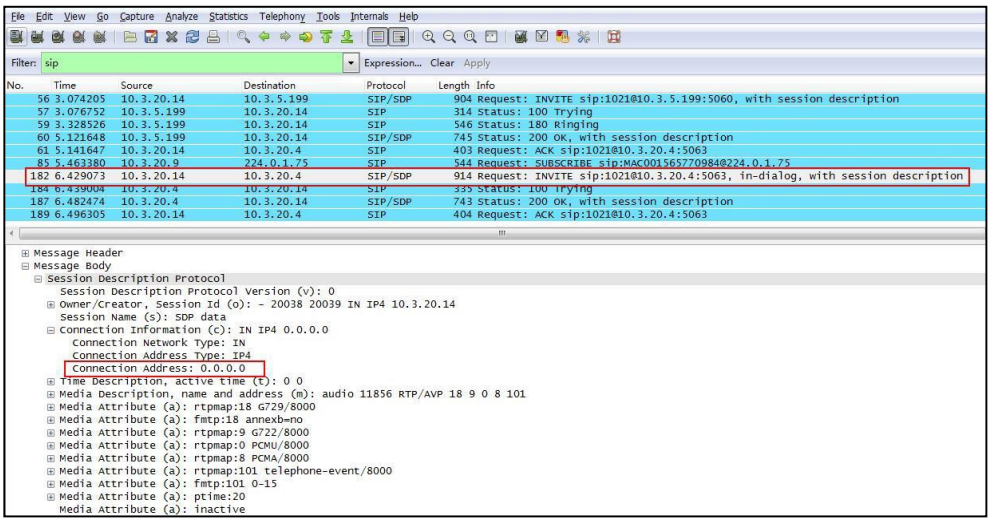
With the RFC2453 Hold feature enabled, SDP media direction attributes (such as a=sendonly) per RFC 2543 are used in the INVITE message when placing a call on hold.

Packets



With the RFC2453 Hold feature disabled, SDP media connection address c=0.0.0.0 per RFC 3264 is used in the INVITE message when placing a call on hold.

Packets



For more information on RFC 2543 hold feature, refer to "Call Hold" on page 206. For more information on capturing packets, refer to "Capture Packets" on page 356.

Appendix A: Glossary

802.1x
An IEEE Standard for port-based Network Access Control (PNAC). It is a part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to join a LAN or WLAN.

ACS (Auto Configuration Server)
The server responsible for autoconfiguration of the Central Processing Element (CPE).

Cryptographic Key
A piece of variable data that is fed as input into a cryptographic algorithm to perform operations such as encryption and decryption, or signing and verification.

DHCP (Dynamic Host Configuration Protocol)
A network management protocol built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts.

DHCP Option
A configuration for specific values, and enabled for assignment and distribution to DHCP clients based on server, scope, class, or client-specific levels.

DNS (Domain Name System)
A hierarchical distributed naming system for PC, services, or any resource connected to the Internet or a private network.

EAP-MD5 (Extensible Authentication Protocol-Message Digest Algorithm 5)
An algorithm provides authentication of the EAP peer to the EAP server but not mutual authentication.

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security)
A protocol that provides for mutual authentication, integrity-protected cipher suite negotiation between two endpoints.

PEAP-MSCHAPv2 (Protected Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol version 2)
A protocol that provides for mutual authentication, but does not require a client certificate on the phone.

FAC (Feature Access Code)
Special patterns of characters that are dialed from a phone keypad to invoke particular features.

HTTP (Hypertext Transfer Protocol)
Used to request and transmit data on the World Wide Web.

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer)
A widely-used communications protocol for secure communication over a network.

IEEE (Institute of Electrical and Electronics Engineers)
A non-profit professional association headquartered in New York City that is dedicated to advancing technological innovation and excellence.

LAN (Local Area Network)
A computer network used to connect devices in a limited area such as a home, school, PC laboratory, or office building.

MIB (Management Information Base)
A virtual database used for managing the entities in a communications network.

OID (Object Identifier)
An identifier mechanism signed to an individual object within a MIB.

ROM (Read-only Memory)
A class of storage medium used in PC and other electronic devices.

RTP (Real-time Transport Protocol)
A network protocol that provides end-to-end service for real-time data.

TCP (Transmission Control Protocol)
A transport layer protocol used by applications that require guaranteed delivery.

UDP (User Datagram Protocol)
A protocol offering non-guaranteed datagram delivery.

URI (Uniform Resource Identifier)
A compact sequence of characters that identifies an abstract or physical resource.

URL (Uniform Resource Locator)
A reference that specifies the address of an Internet resource.

VLAN (Virtual LAN)
A group of hosts with a common set of requirements, which communicate as if they were attached to the same broadcast domain, regardless of their physical location.

VoIP (Voice over Internet Protocol)
A family of technologies used for the delivery of voice communications and multimedia sessions over IP networks.

WLAN (Wireless Local Area Network)
A type of local area network that uses high-frequency radio waves rather than wires to communicate between nodes.

XML-RPC (Remote Procedure Call Protocol)
A protocol that uses XML to encode its calls and HTTP as a transport mechanism.

Appendix B: Time Zones

Time Zones

Time Zone	Time Zone Name
-11	Samoa
-10	United States-Hawaii-Aleutian, United States-Alaska-Aleutian
-9:30	French Polynesia
-9	United States-Alaska Time
-8	Canada (Vancouver,Whitehorse), Mexico (Tijuana,Mexicali), United States-Pacific Time
-7	Canada (Edmonton,Calgary), Mexico (Mazatlan,Chihuahua), United States-MST no DST, United States-Mountain Time
-6	Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica, Belize, Canada-Manitoba (Winnipeg), Chile (Easter Islands), Mexico (Mexico City,Acapulco), United States-Central Time
-5	Peru, Bahamas (Nassau), Canada (Montreal,Ottawa,Quebec), Cuba (Havana), United States-Eastern Time
-4:30	Venezuela (Caracas)
-4	Canada (Halifax,Saint John), Chile (Santiago), Paraguay (Asuncion), United Kingdom-Bermuda (Bermuda), United Kingdom (Falkland Islands), Trinidad&Tobago
-3:30	Canada-Newfoundland (St. Johns)
-3	Argentina (Buenos Aires), Brazil (DST), Brazil (no DST), Denmark- Greenland (Nuuk)
-2:30	Newfoundland and Labrador
-2	Brazil (no DST)
-1	Portugal (Azores)
0	Denmark-Faroe Islands (Torshavn), GMT, Greenland, Ireland (Dublin), Morocco, Portugal (Lisboa,Porto,Funchal), Spain-Canary Islands (Las Palmas), United Kingdom (London)
+1	Albania (Tirane), Austria (Vienna), Belgium (Brussels), Caicos, Chad, Croatia (Zagreb), Czech Republic (Prague), Denmark (Kopenhagen), France (Paris), Germany (Berlin), Hungary (Budapest), Italy (Rome), Luxembourg (Luxembourg), Macedonia (Skopje), Namibia (Windhoek), Netherlands (Amsterdam), Spain (Madrid), Switzerland (Bern), Sweden (Stockholm)
+2	Estonia (Tallinn), Finland (Helsinki), Gaza Strip (Gaza), Greece (Athens), Israel (Tel Aviv), Jordan (Amman), Latvia (Riga), Lebanon (Beirut), Moldova (Kishinev), Romania (Bucharest), Russia (Kaliningrad), Syria (Damascus), Turkey (Ankara), Ukraine (Kyiv, Odessa)
+3	East Africa Time, Iraq (Baghdad), Russia (Moscow)
+3:30	Iran (Tehran)
+4	Armenia (Yerevan), Azerbaijan (Baku), Georgia (Tbilisi), Abu Dhabi, Kazakhstan (Aktau), Russia (Samara)
+4:30	Afghanistan (Kabul)
+5	Kazakhstan (Aqtobe), Kyrgyzstan (Bishkek), Pakistan (Islamabad), Russia (Chelyabinsk)
+5:30	India (Calcutta)
+5:45	Nepal (Katmandu)
+6	Kazakhstan (Astana, Almaty), Russia (Novosibirsk,Omsk)
+6:30	Myanmar (Naypyitaw)

Time Zone	Time Zone Name
+7	Russia (Krasnoyarsk), Thailand (Bangkok)
+8	Australia (Perth), China (Beijing), Russia (Irkutsk, Ulan-Ude), Singapore (Singapore)
+8:45	Eucla
+9	Japan (Tokyo), Korea (Seoul), Russia (Yakutsk,Chita)
+9:30	Australia (Adelaide), Australia (Darwin)
+10	Australia (Brisbane), Australia (Hobart), Australia (Sydney,Melboume,Canberra), Russia (Vladivostok)
+10:30	Australia (Lord Howe Islands)
+11	New Caledonia (Noumea), Russia (Srednekolymsk Time)
+11:30	Norfolk Island
+12	New Zealand (Wellington,Auckland), Russia (Kamchatka Time)
+12:45	New Zealand (Chatham Islands)
+13	Tonga (Nukualofa)
+13:30	Chatham Islands
+14	Kiribati

Appendix C: Trusted Certificates

Skype for Business phones trust the following CAs by default:

- DigiCert High Assurance EV Root CA
- Deutsche Telekom AG Root CA-2
- Equifax Secure Certificate Authority
- Equifax Secure eBusiness CA-1
- Equifax Secure Global eBusiness CA-1
- GeoTrust Global CA
- GeoTrust Global CA2
- GeoTrust Primary CA
- GeoTrust Primary CA G2 ECC
- GeoTrust Universal CA
- GeoTrust Universal CA2
- Thawte Personal Freemail CA
- Thawte Premium Server CA
- Thawte Primary Root CA - G1 (EV)
- Thawte Primary Root CA - G2 (ECC)
- Thawte Primary Root CA - G3 (SHA256)
- Thawte Server CA
- VeriSign Class 1 Public Primary Certification Authority
- VeriSign Class 1 Public Primary Certification Authority - G2
- VeriSign Class 1 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority - G2
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority
- VeriSign Class 3 Public Primary Certification Authority - G2
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G4
- VeriSign Class 3 Public Primary Certification Authority - G5
- VeriSign Class 4 Public Primary Certification Authority - G2
- VeriSign Class 4 Public Primary Certification Authority - G3

- VeriSign Universal Root Certification Authority
- Microsoft_IT_SSL_SHA2.cer
- CNNIC_Root.cer
- BaltimoreCyberTrust.cer
- UserTrust.cer
- AAA Certificate Services.cer
- DigiCert Assured ID Root CA.cer
- Entrust.net Certification Authority (2048).cer
- Entrust Root Certification Authority
- Entrust.net Secure Server Certification Authority
- GTE CyberTrust Global Root.cer
- Starfield Class 2 Certification Authority.cer
- AddTrust External CA Root
- Go Daddy Class 2 Certification Authority
- StartCom Certification Authority
- DST Root CA X3
- ISRG Root X1 (intermediate certificates: Let's Encrypt Authority X1 and Let's Encrypt Authority X2 are signed by the root certificate ISRG Root X1.)
- Baltimore CyberTrust Root
- DigiCert Cloud Services CA-1
- D-Trust Root Class 3 CA 2 2009
- AddTrust External CA Root
- Starfield Root Certificate Authority - G2

NOTE: Crestron maintains a built-in list of most common CA Certificates. Due to memory constraints, we cannot ensure a complete set of certificates. If using a certificate from a commercial Certificate Authority not in the list above, send a request to your local distributor. Otherwise, a particular CA certificate can be uploaded into the phone. For more information on uploading custom CA certificate, refer to "Transport Layer Security (TLS)" on page 330.

Appendix D: Static Settings

There are differences between the parameter names that start with "static." and other common parameters:

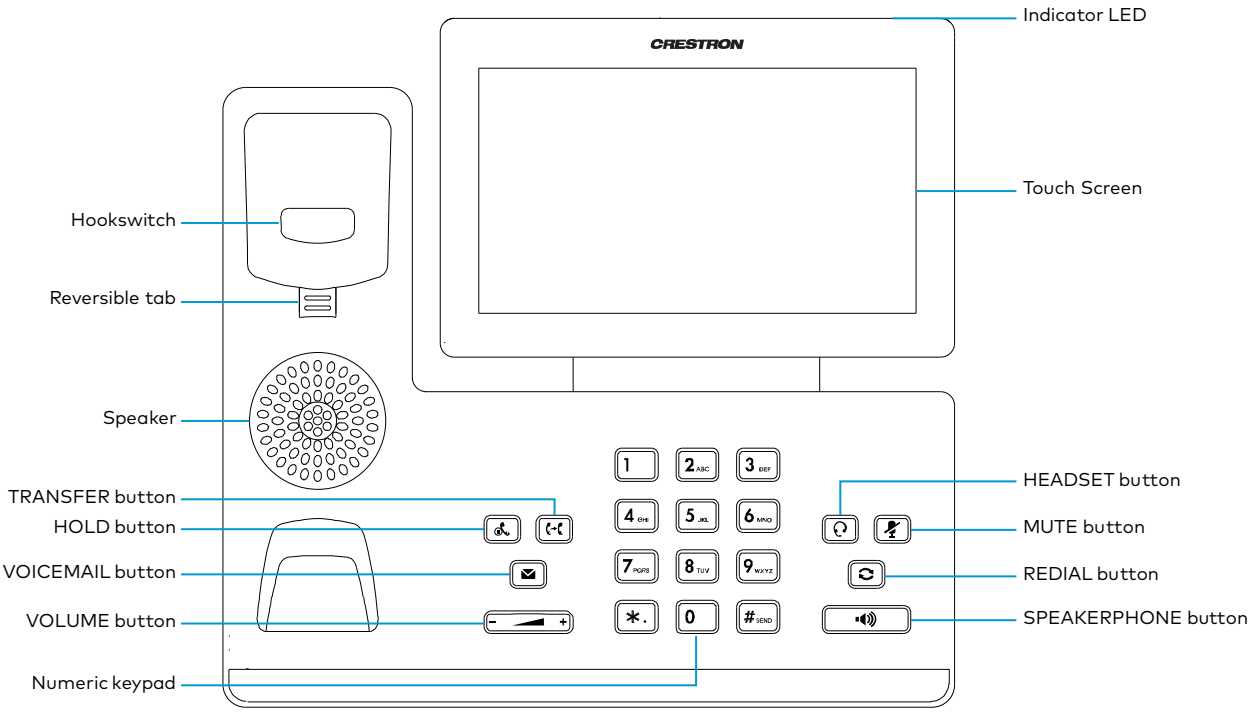
- All static settings have no priority. They take effect no matter what method (Web User Interface, Phone User Interface, configuration files, or In-band provisioning) is used for provisioning.
- All static settings are never saved to the <MAC>-local.cfg file.

All static settings are not affected by the overwrite mode. Even if the parameters associated with static settings are deleted, the values of the parameters associated with static settings in the configuration file are cleared.

Appendix E: Phone Operation

Hardware

Buttons and Indicators



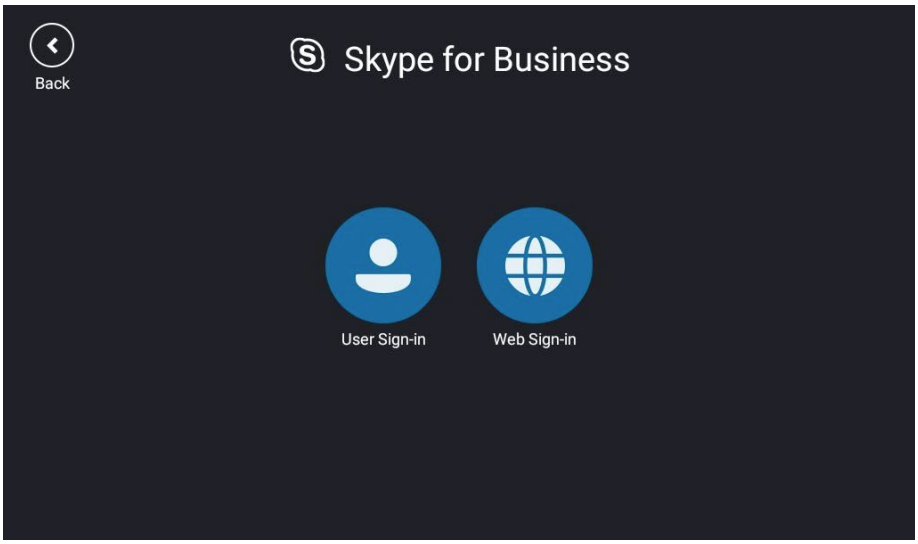
- Hookswitch: Connects or disconnects the phone from the phone line. The hookswitch is automatically activated when the handset is lifted from the phone.
- Reversible Tab: Secures the handset in the handset cradle when the phone is mounted vertically.
- Speaker: Used for speakerphone functions.
- TRANSFER: 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 is receiving a voicemail or missing 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, the user is prompted to sign in to the Skype for Business application. A user can sign in to the phone from the phone or the web. Tap **User Sign-in** or **Web Sign-in**.

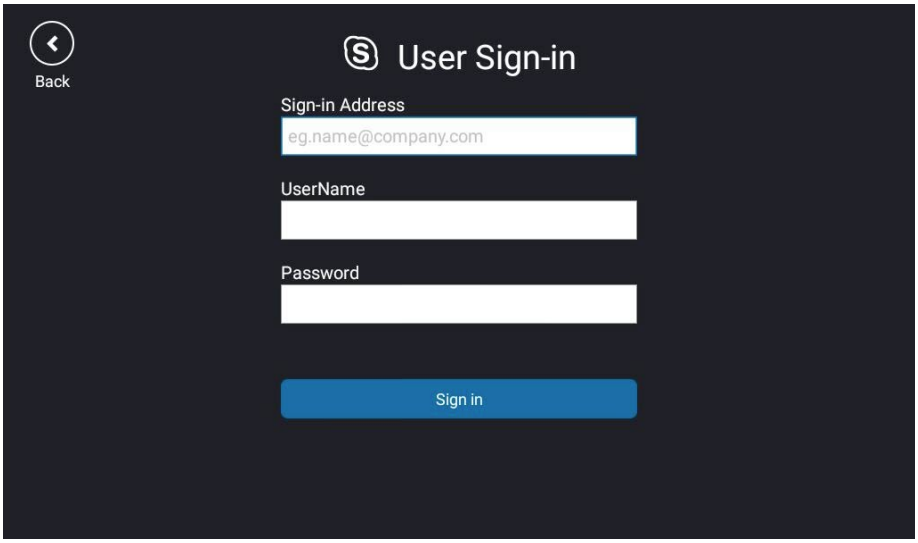
Sign-in Options



User Sign-in

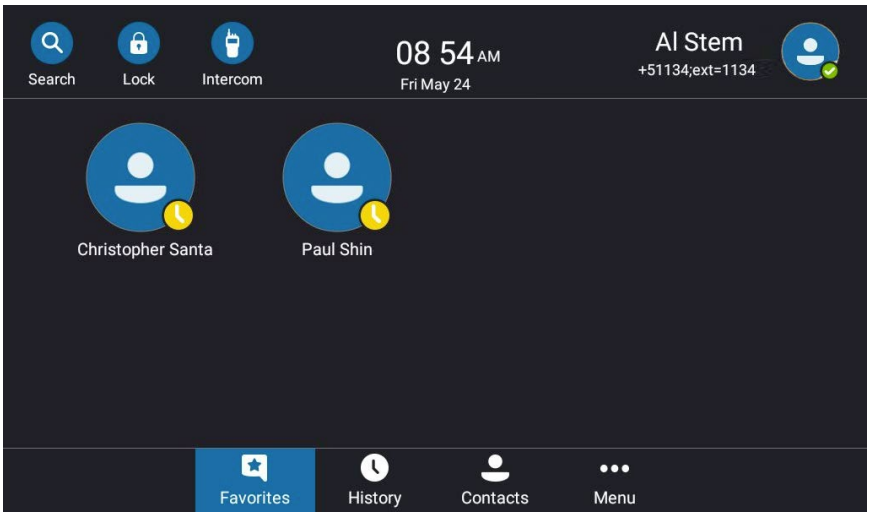
Select the **User Sign-in** option to sign in with a sign-in address, user name, and password.

User Sign-in



1. Tap **User Sign-in**.
2. Enter the sign-in address, user name, and password in the respective fields, and tap **Sign in**.
3. Follow the on-screen instructions for creating a lock PIN and tap **Save**. The Favorites screen is displayed.

Favorites Screen

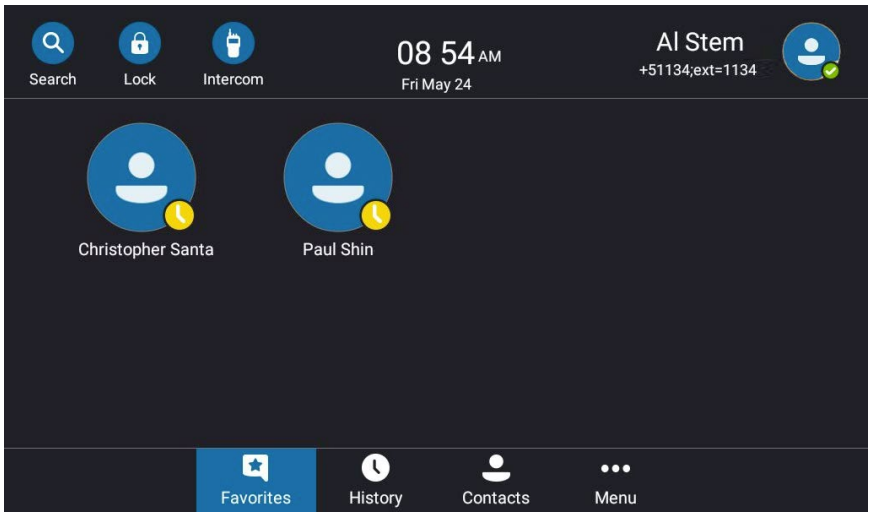


Web Sign-in

Select the **Web Sign-in** option to sign in from a web browser.

1. Tap **Web Sign-in.**
2. Follow the instructions shown on the phone display.
3. Follow the on-screen instructions for creating a lock PIN and tap **Save**. The Favorites screen is displayed.

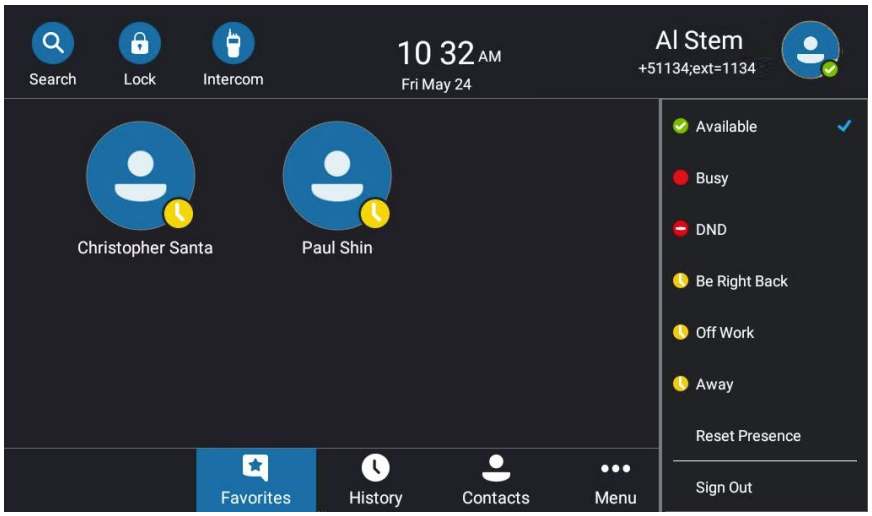
Favorites Screen



Sign Out from the Skype for Business Service

1. Tap the user icon on the upper-right corner of the screen to manage the Skype for Business presence. A list of options is displayed.

Sign Out



2. Tap **Sign Out.**

Getting Started

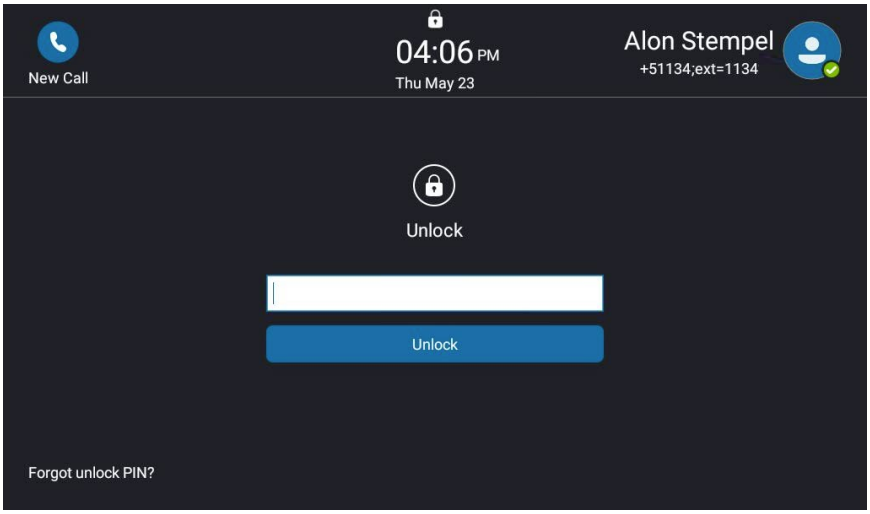
Unlock the Phone

If the phone is locked, type the lock PIN on the keypad and tap **Unlock**. The Favorites screen is displayed.

Lock the Phone

To lock the phone, tap **Lock**. The Lock screen is displayed.

Lock Screen



NOTE: The phone can be set to lock after a set amount of time has elapsed. Refer to "Configure Phone Lock via the Phone User Interface" on page 330.

Overview of the Touch Screen

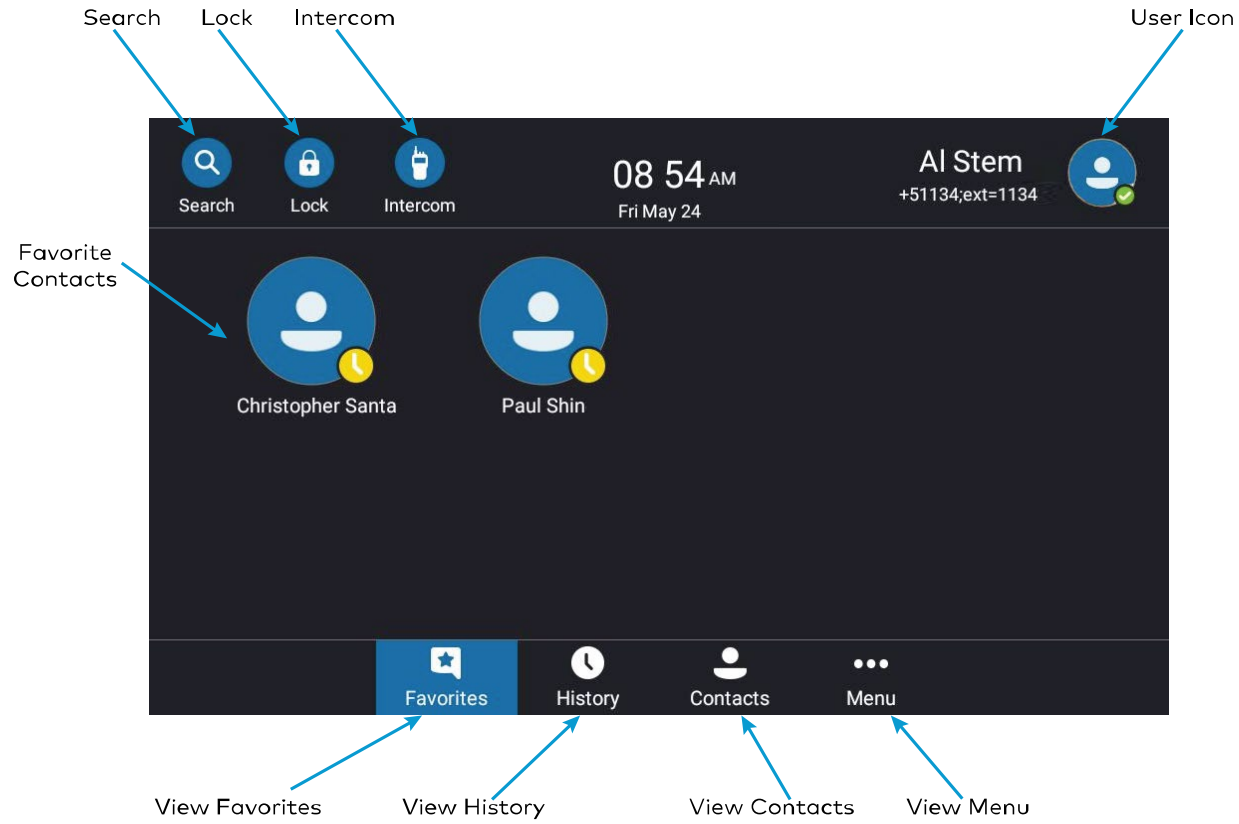
The following screens can be accessed on the phone.

- The Favorites Screen
- The History Screen
- The Contacts Screen
- The Menu Screen

The Favorites Screen

The Favorites screen provides access to all of the Skype for Business phone functions.

Favorites Screen



From the Favorites screen, the following functions are available:

- Search for a contact
- Lock the phone
- Use the intercom
- Manage the Skype for Business presence
- Sign out from the Skype for Business service
- Call a favorite contact
- View call history
- View contact groups
- Jump to a menu to view the calendar, call a Skype for Business meeting, check voice mail, view the phone's status, and adjust settings.

NOTE: The features listed above are only available when configured as such. Contact the administrator regarding these features if they are not present on the phone.

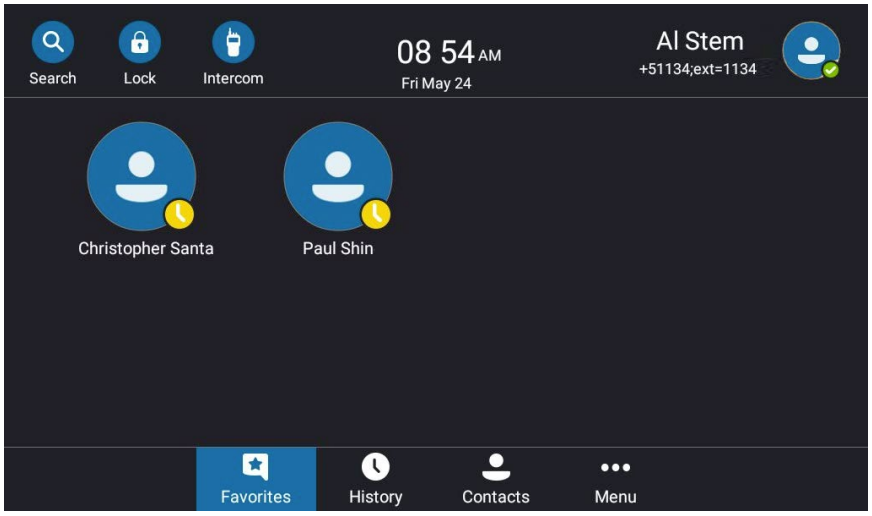
Access the Favorites Screen

Local favorites and Skype for Business favorites are displayed on the Favorites screen. By default, local favorites are displayed before the Skype for Business favorites. Skype for Business contacts also have an icon to indicate their presence status.

To access the Favorites screen:

1. Tap **Favorites**. The Favorites screen is displayed.

Favorites Screen



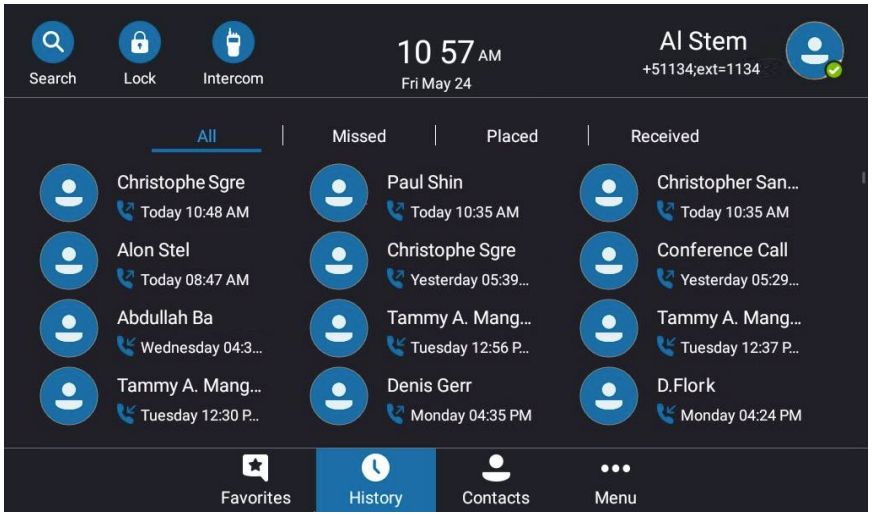
2. Slide up and down to view more favorites.

Access the History Screen

Missed, placed, received, and forwarded calls can be viewed in the History screen.

1. Tap **History**. The Call Log screen is displayed.

Call Log Screen



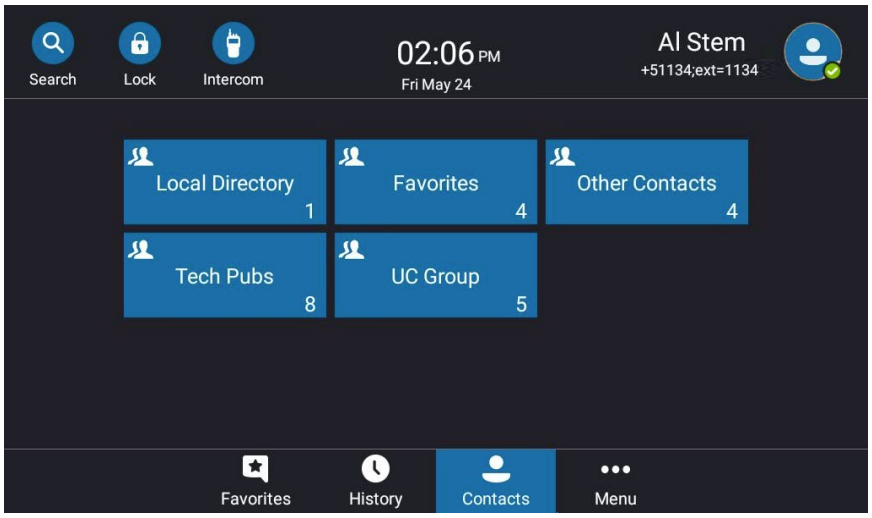
2. Slide up and down to view more history records.

Access the Contacts Screen

The Contacts screen includes the local directory and Skype for Business directory.

1. Tap **Contacts**. The Contacts screen is displayed.

Contacts Screen



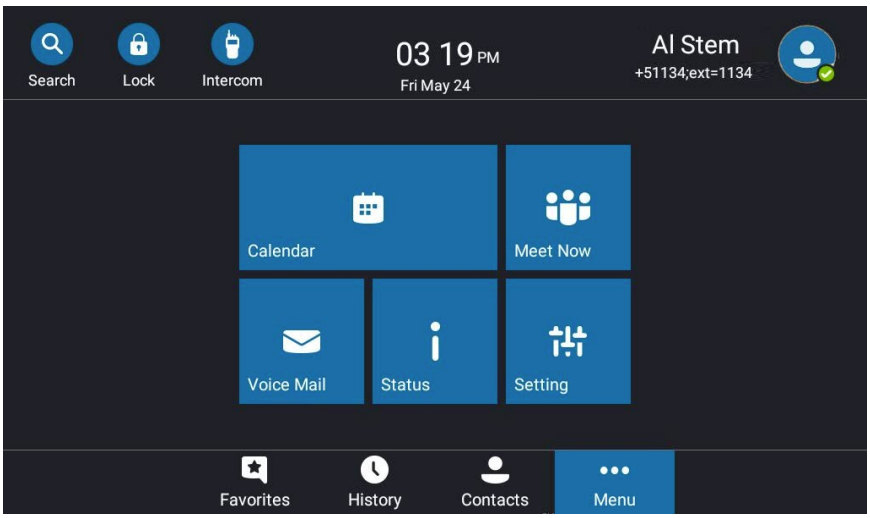
2. Slide up and down to view more groups.

Access the Menu Screen

The menu screen provides access to phone features, settings, and information. Tap **Menu** to display the Menu screen.

Tap **Menu**. The Menu screen is displayed.

Menu Screen

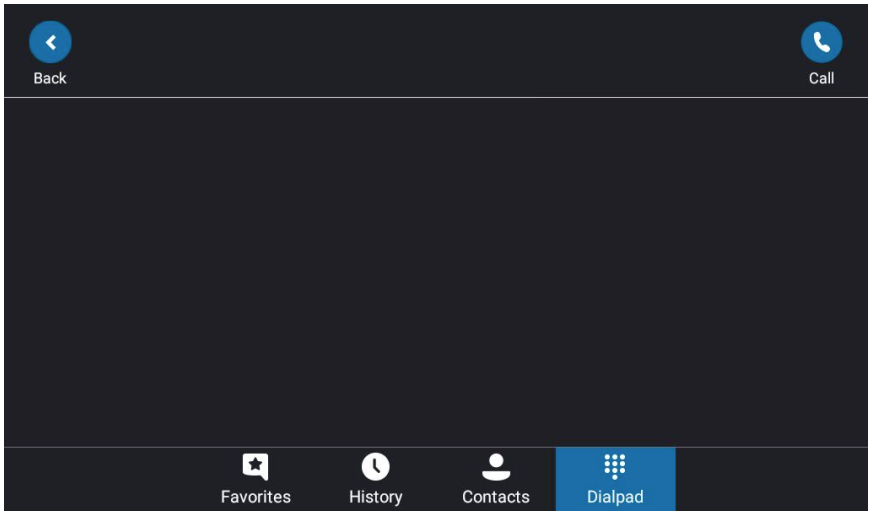


Search for a Contact

Use the touch screen to search for local and Skype for Business contacts.

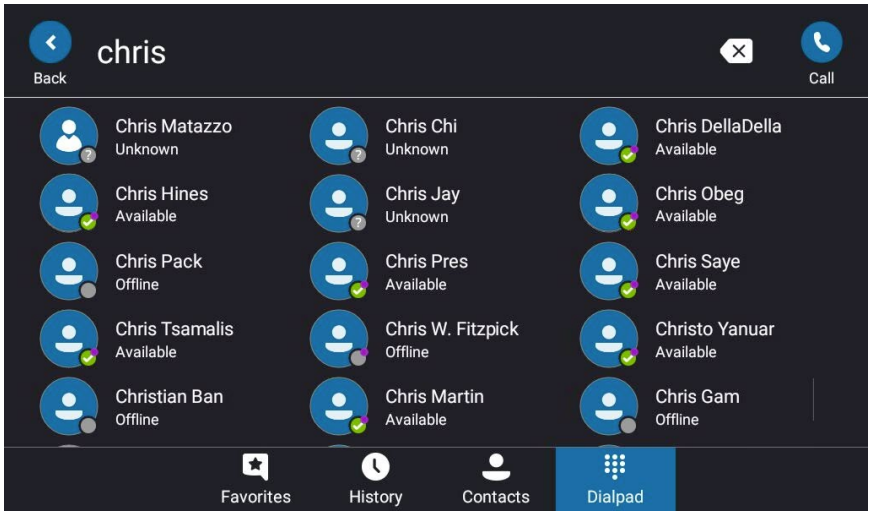
1. Tap **Search** to display the search screen.

Search Screen



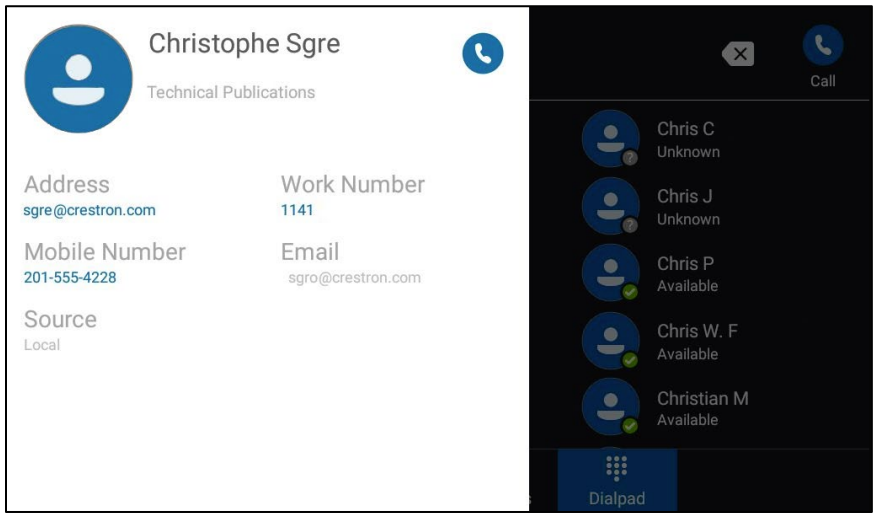
2. Enter the phone number with the keypad or tap the cursor on the screen to use an on-screen keyboard to enter the name to search for. Search results are displayed as letters are typed.

Search Results



3. Tap the contact to view their details.

Contact Details



- Tap a blue email address or number to contact the person. Email address entries will call their Skype for Business account. Digit entries will call a number.
- Tap **Add to Local** to add the contact to the local contact list.
- Tap **Add to SFB** to add the contact to the Skype for Business contact list.

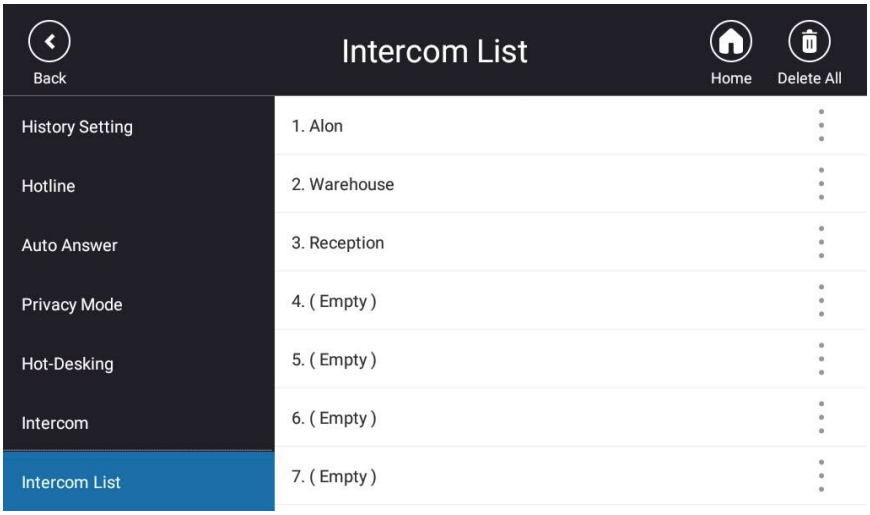
Lock the Phone

Tap **Lock** to lock the phone from unauthorized use. For directions on unlocking the phone, refer to "Unlock the Phone" on page 392.

Intercom

The intercom function allows direct calling a contact. Tap **Intercom** to use the intercom function. The Intercom List screen is displayed.

Intercom List

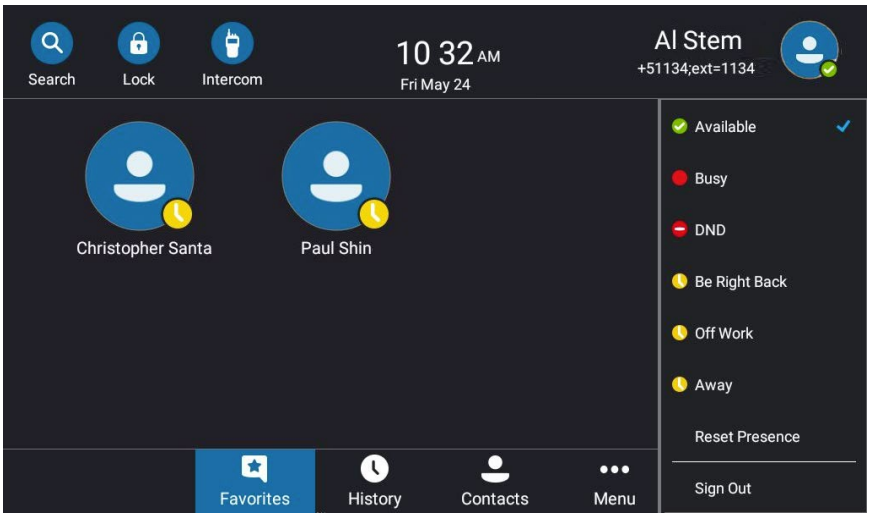


To use the intercom, tap an entry in the intercom list.

Manage Skype for Business Presence

1. Tap the user icon to manage the Skype for Business presence. A list of options is displayed.

Skype for Business Presence



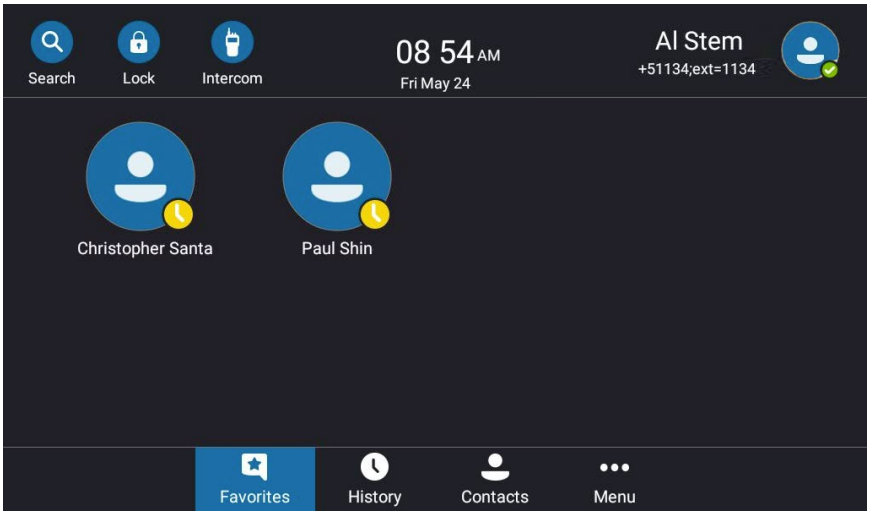
2. Tap the desired presence setting.

NOTE: A user can also sign out from the Skype for Business service. For details, refer to "Sign Out from the Skype for Business Service" on page 391.

Call a Favorite Contact

Tap **Favorites** to view a list of favorite contacts.

Favorites Screen



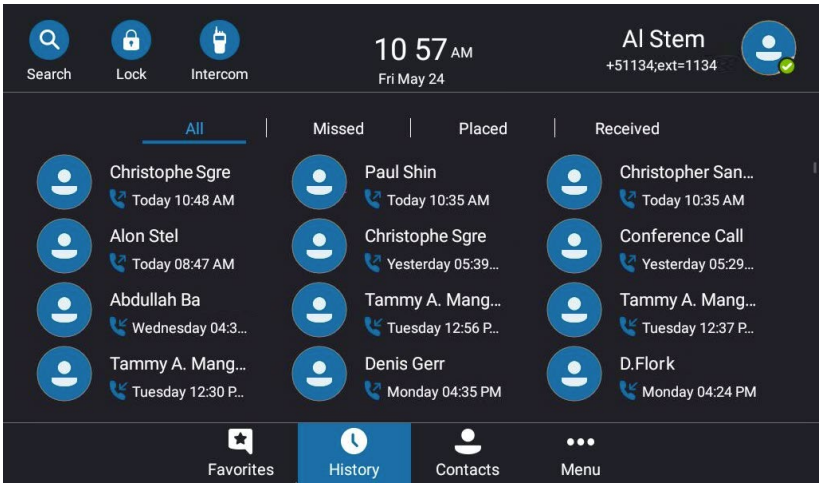
Tap a favorite contact to call them.

NOTE: If the contact has a Skype for Business account and a regular telephone number, the phone will dial the Skype for Business account.

View Call History

Tap **History** to view the call logs.

Call Logs



Filters

Different filters can be applied to the call logs.

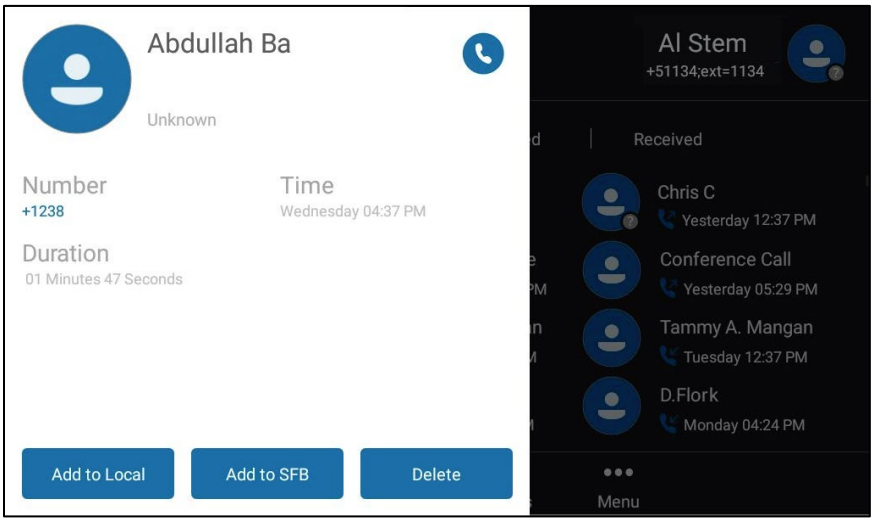
- Tap **All** to view all of the calls in the call log.

- Tap **Missed** to view a list of missed calls.
- Tap **Placed** to view a list of calls made from the phone.
- Tap **Received** to view a list calls received on the phone.

Entry Details

While viewing the logs, tap an entry to view details.

Log Entry Detail



While viewing the details, a user can add the contact to the local directory, add the contact to the Skype for Business directory, or delete the entry from the call log.

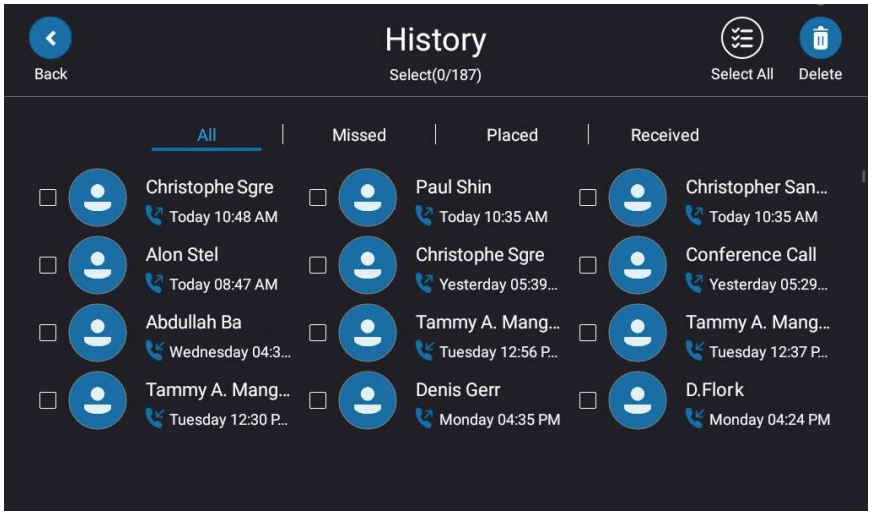
- Tap **Add to Local** to add the contact to the local directory.
- Tap **Add to Sfb** to add the contact to the Skype for Business directory.
- Tap **Delete** the delete the entry from the call log.

Delete Entries from the Call Log

To delete entries from the call log:

1. Press anywhere in the call log and hold until the History Select screen is displayed.

History Select Screen

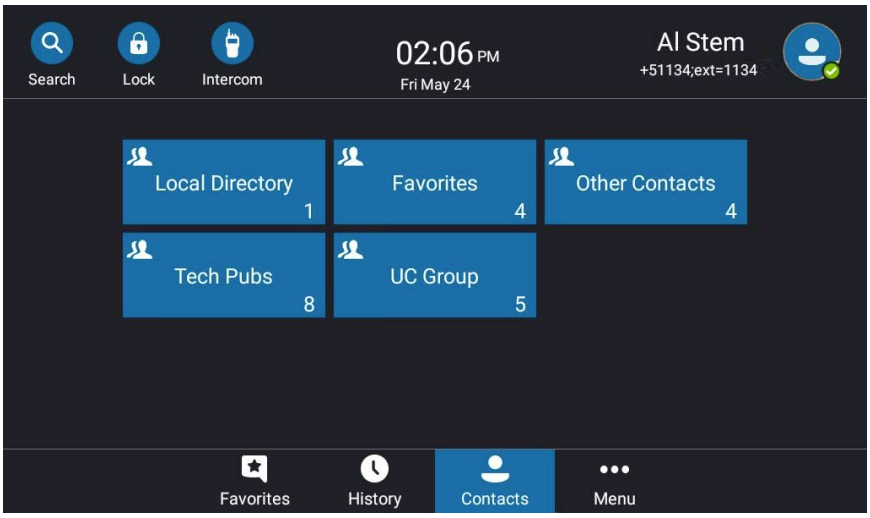


2. A checkbox is shown next to each entry.Tap the checkboxes of each entry to be deleted or tap **Select All** to select all of the entries in the log.
3. Tap **Delete** to delete the selected entries.

View Contact Groups

Tap **Contacts** to view contact groups. A list of contact groups is displayed.

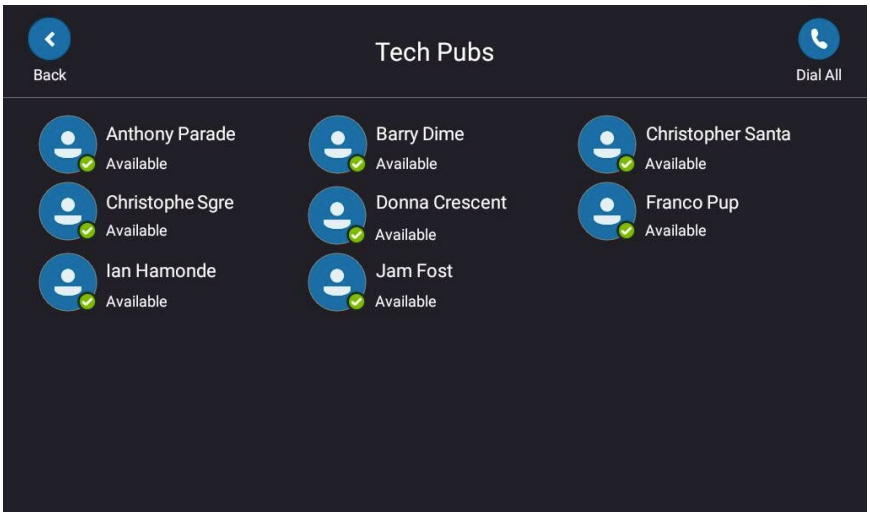
Contact Groups



NOTE: Contact groups are managed in the Skype for Business software.

Tap a contact group to view the group members.

Contact Group Members



Tap a contact to view their contact details and contact options, or tap **Dial All** to call all of the members in the group.

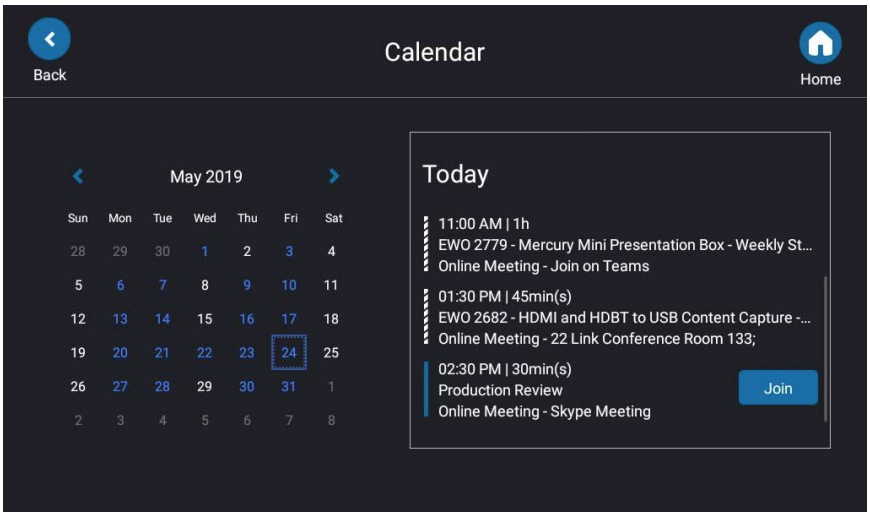
Additional Functions

Tap **Menu** to access the calendar, call a meeting, access voice mail, view phone status, and adjust seetings.

View the Calendar

Tap **Calendar** to view the calendar of scheduled events.

Calendar



Navigate the calendar by tapping **<** or **>**. When the date to be viewed is visible, tap it to display the day's scheduled events.

Upcoming Skype for Business meetings will have a button labeled **Join**. Tap it to join a Skype for Business meeting. For details on joining a meeting, refer to "Join a Skype for Business Meeting" on page 404.

Tap **Back** to return to the previous screen, or tap **Home** to jump to the Favorites screen.

Start a Skype for Business Meeting

A user can start a Skype for Business meeting by tapping **Meet Now**. For details, refer to "Create a Skype for Business Meeting" on page 404.

Access Voice Mail

Tap **Voice Mail** to display the Voice Mail screen. Refer to "Use Voice Mail" on page 411 for details.

View Phone Information

Tap **Status** to view information about the phone, its network connection details, location, and license information.

Change and View Phone Settings

Tap **Setting** to configure features, basic settings, and advanced settings.

NOTE: An administrative password is required to review and/or change advanced settings.

For details, refer to "Set Up a System" on page 9, "Configure Basic Features" on page 98, and "Configuring Advanced Settings" on page 235.

Make Phone Calls

Phone calls can be made from the keypad, call log, contact list, or voice mail using the handset, built-in speakerphone, or a connected USB headset.

Call from the Keypad

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

To send the dialed number and speed up the process, press **# SEND**. Otherwise, the phone will call the dialed number after a short delay.

Call from the Call Log, Contact List, or Voice Mail

When viewing a call log entry, a contact, or a voice mail message, tap **Call** to call the displayed contact.

Create or Join a Skype for Business Meeting

From the phone, a user can create a create an immediate Skype for Business meeting, or join a Skype for Business meeting to which they are invited.

NOTES:

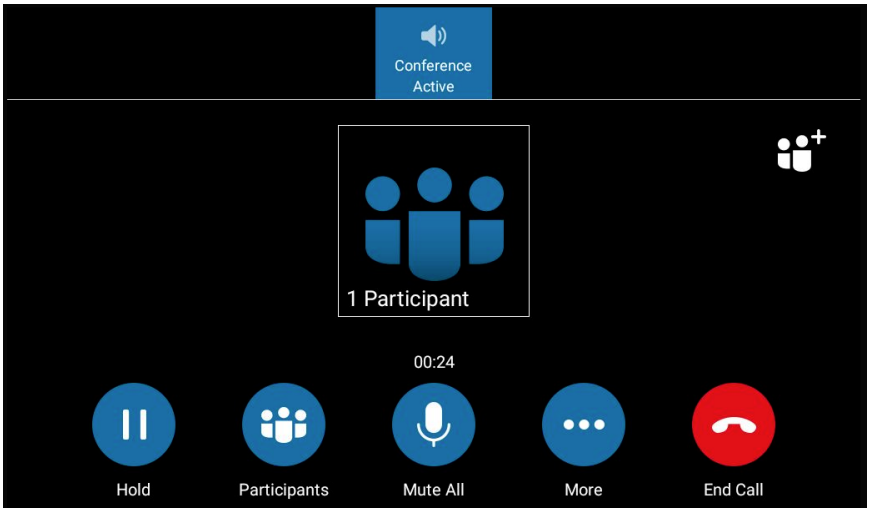
- Skype for Business meetings cannot be scheduled for a future time from the phone. To schedule a Skype for Business meeting, Microsoft Outlook or some other scheduling software that is compatible with Skype for Business software must be used.
- To join a Skype for Business meeting, the user must accept the meeting using Microsoft Outlook or some other scheduling software that is compatible with Skype for Business software.

Create a Skype for Business Meeting

A user can create an immediate Skype for Business meeting using the Meet Now function. To do so:

Tap **Menu**, and then tap **Meet Now**.

Meeting Screen

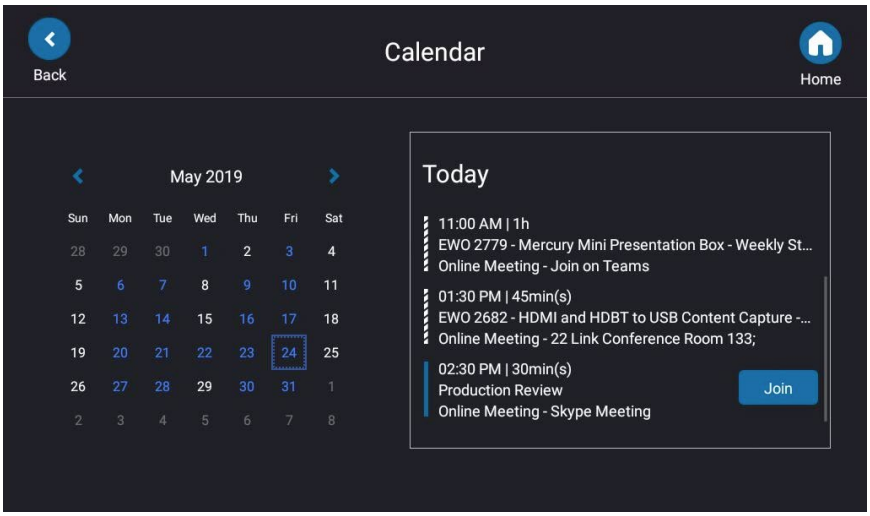


Join a Skype for Business Meeting

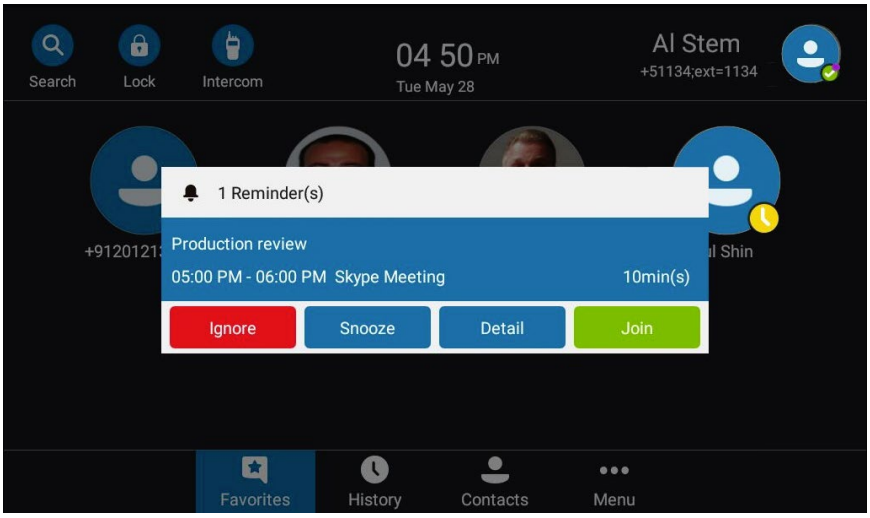
Users can join a Skype for Business meeting to which they were invited using the Join function.

The Join function is available from the calendar view (refer to "View the Calendar" on page 402) or from a Skype for Business meeting reminder.

Join Function, Calendar View

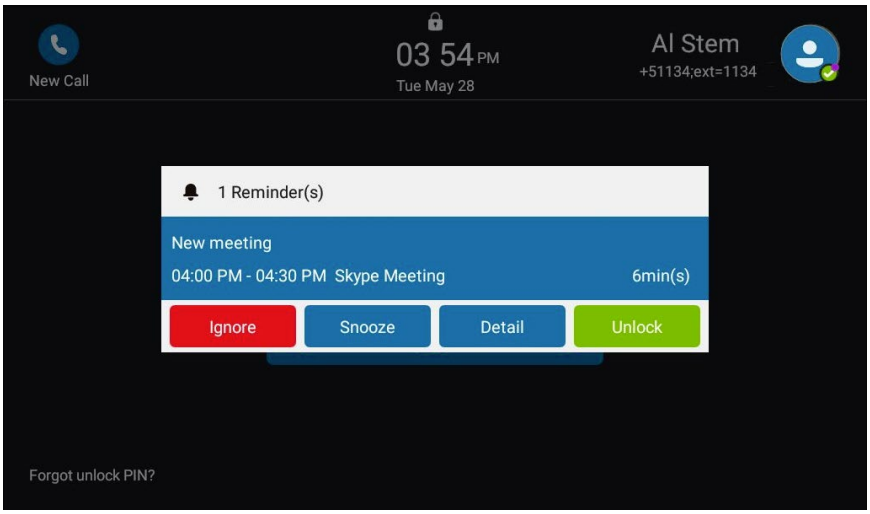


Join Function, Skype for Business Meeting Reminder



NOTE: If the phone is locked, a Skype for Business meeting reminder will display the following image.

Meeting Reminder

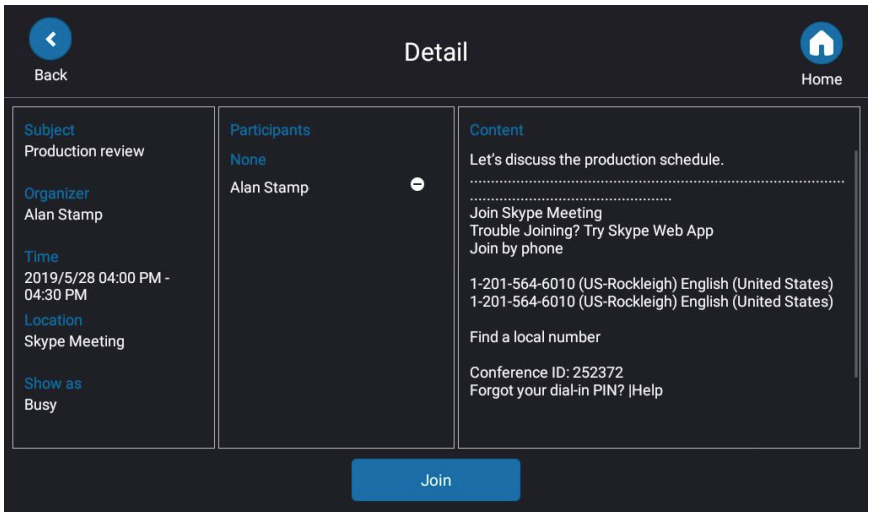


Tap **Unlock,** enter the unlock PIN, and then tap **Unlock**, to view the reminder.

When a Skype for Business meeting reminder is displayed, do one of the following:

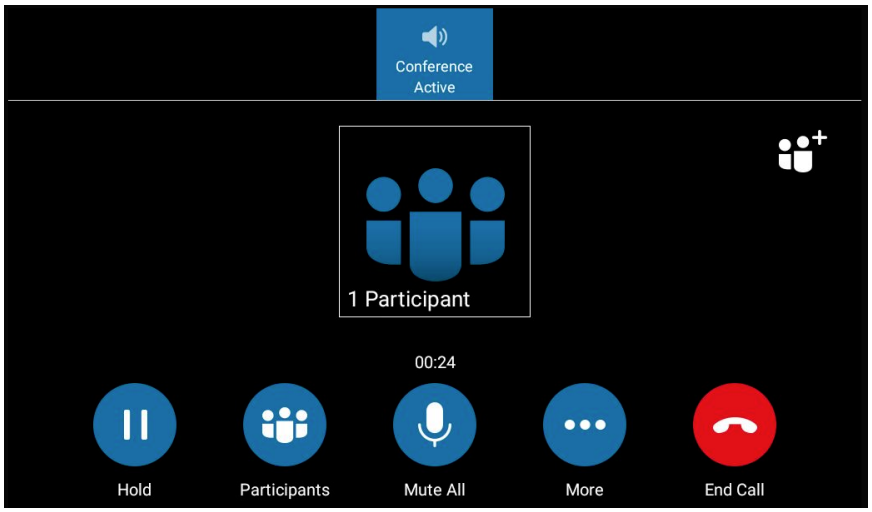
- Tap **Ignore** to ignore the Skype for Business meeting reminder. The Skype for Business meeting reminder will disappear and no further notifications will be displayed.
- Tap **Snooze** to snooze the Skype for Business meeting reminder. The Skype for Business meeting reminder will display again at the meeting's start time.
- Tap **Detail** to view meeting details. The Detail screen is displayed.

Meeting Detail



- Tap **Join** to join the Skype for Business meeting. The Skype for Business meeting screen is displayed.

Meeting Screen



Skype for Business Meeting Functions

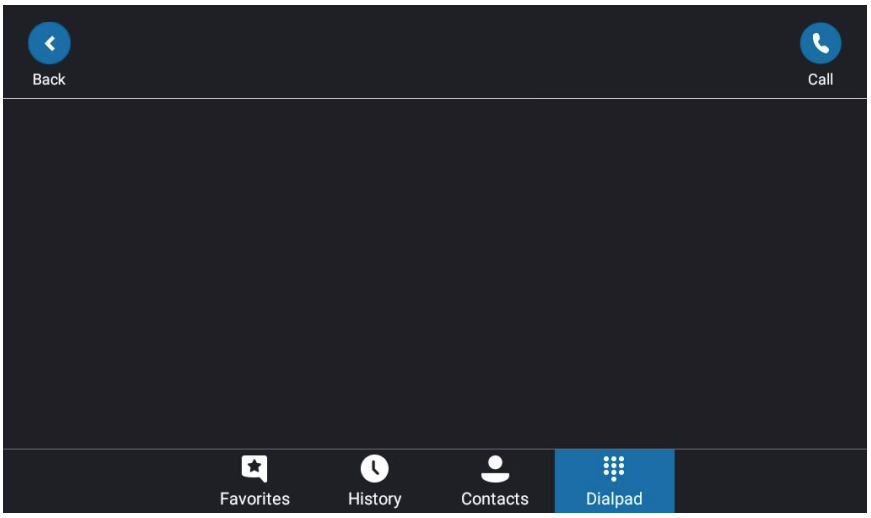
During a Skype for Business meeting, the following functions are available:

- Add participants (Organizer and Presenter only)
- Place a call on hold
- Manage participants
- Mute and/or unmute all participants

Add Participants to the Skype for Business Meeting (Organizer & Presenter Only)

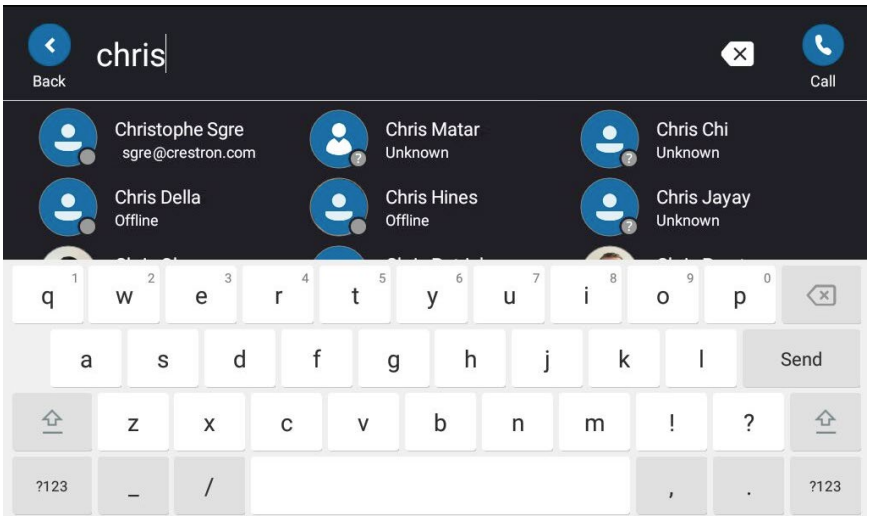
1. Tap  to add participants. The contact search screen is displayed.

Add Participants



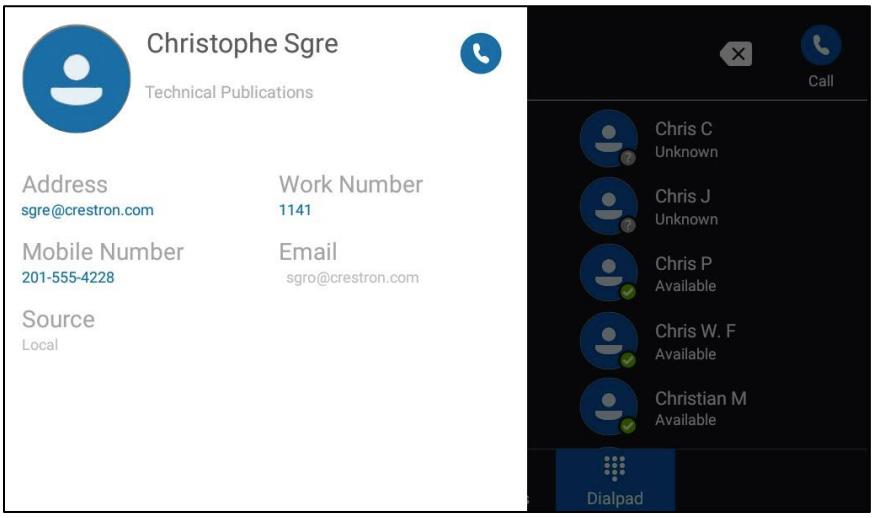
2. Tap the cursor on the top of the screen for an on-screen keyboard to use for entering the name to search. Search results are displayed as letters are typed.

Search Results



3. Tap the contact to view their details.

Contact Details



4. Tap the contact method to use for the Skype for Business meeting.
5. Repeat steps 1 through 4 for each participant to be added.

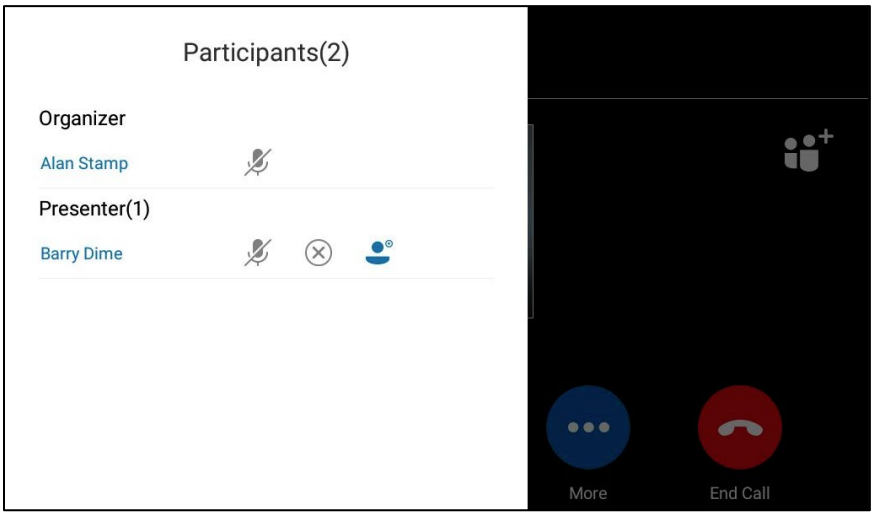
Place a Call on Hold

Tap **Hold** to place a call on hold.

Manage Participants (Organizer and Presenter Only)

Tap **Participants** to view and manage Skype for Business meeting participants. A list of participants is displayed on the Participants screen.

Manage Participants



Meeting participants are:

- **Organizer**: The organizer is the user who creates the Skype for Business meeting. An Organizer can manage the presenters and attendees.
- **Presenter**(): A participant who is invited to the conference will be a presenter by default. A presenter can only manage other presenters and attendees.
- **Attendee** (): A user who is invited to a conference but who is not authorized to act as a presenter. The attendee cannot manage call participants.

The following functions can be administered for each participant.

- Tap the  to mute or unmute a participant.
- Tap  to unmute a participant.
- Tap **X** to remove the participant from the conference call.
- Tap  to demote a presenter to an attendee.
- Tap  to promote an attendee to a presenter.

Mute or Unmute All Participants

Tap **Mute All** to mute all participants. Tap **UnMute All** to unmute all of the participants.

Additional Skype for Business Meeting Functions

Tap **More** to view additional controls. Repeatedly tapping **More** will display other controls.

- **Enable and/or Disable Conference Attendance Announcements:** Tap **E.Anc** to enable Skype for Business meeting attendance announcements. Tap **U.Anc** to disable announcements.
- **Lock and/or Unlock a Skype for Business meeting:** Tap **ConfLock** to lock a Skype for Business meeting to prevent other people from joining the conference call without approval. When the Skype for Business meeting is locked, contacts must wait for the organizer or presenters to admit them to the Skype for Business meeting. Tap **ConfUnLock** to unlock the Skype for Business meeting.
- **Display Dial-In Information:** Tap **ConfInfo** to view the Skype for Business meeting dial-in number and conference ID number.
- **Make an Intercom Call:** Tap **Intercom** to use the intercom function. Refer to "Intercom" on page 398 for details.

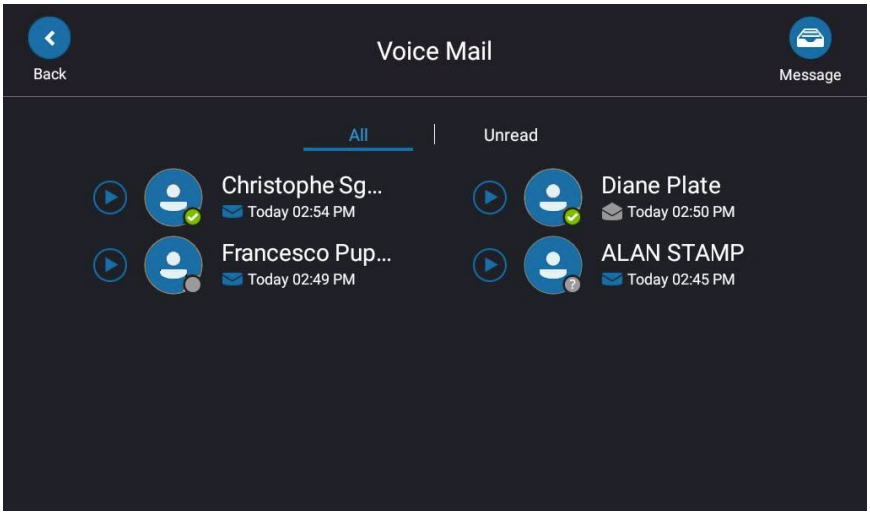
End the Skype for Business Meeting

Tap **End Call** to end the Skype for Business meeting.

Use Voice Mail

Tap **Voice Mail** to display voice mail messages.

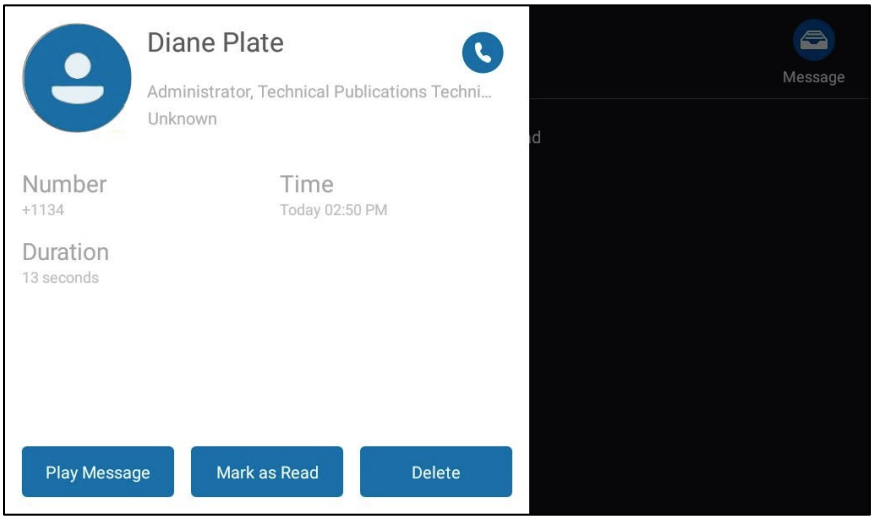
Voice Mail Messages



New messages are shown with a blue envelope icon, while read messages are indicated with a grey envelope icon.

Tap a message to display information about it and display the message options.

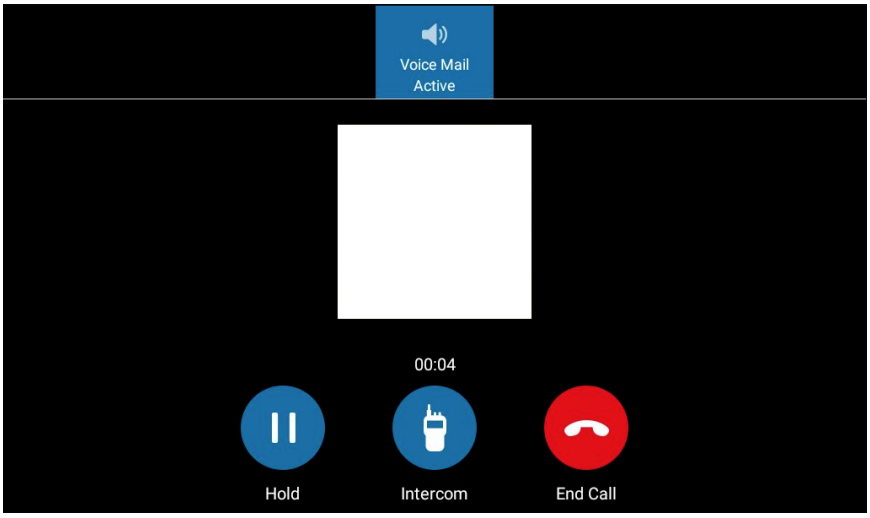
Contact Details



Listen to a Message

Tap **Play Message** to listen to a message. The message plays and playback controls are displayed.

Voice Mail Playback



Call Back

Tap the phone icon on the upper-right corner to call back a person who left a message.

Mark a Message as Read

To mark a message as read, tap **Mark as Read**.

Delete a Message

Tap **Delete** to delete a message.

This page is intentionally left blank.

Crestron Electronics, Inc.
15 Volvo Drive, Rockleigh, NJ 07647
Tel: 888.CRESTRON
Fax: 201.767.7576
www.crestron.com

Supplemental Guide – DOC. 8412A
(2052763)
09/13/19