UC-PHONE-S, UC-PHONE-S-PLUS, UC-PHONE-T, & UC-PHONE-T-PLUS Crestron Flex VoIP Desk Phones

Secure Deployment Guide

Crestron Electronics, Inc.

Contents

Introduction 1

Best Practices 2

Change the Default Password 2

Change the Default Username 2

Configure Strong Ciphers for TLS Connections (UC-PHONE-S and UC-PHONE-S-PLUS Only) 2

Configure Use of TLS1.2 Protocol for All SIP Connections (UC-PHONE-S and UC-PHONE-S-PLUS Only) 2

Disable Bluetooth® Feature 3

Configuration File 3
Phone User Interface Configuration 3
Web User Interface Configuration 3

Disable Cleartext HTTP Protocol 4

Configuration File 4
Web User Interface Configuration 4

Disable Wi-Fi® Feature (UC-PHONE-S and UC-PHONE-S-PLUS Only) 5

Configuration File 5
Phone User Interface Configuration 5

EAP-TLS Configuration on UC-PHONE with Free Radius Server (UC-PHONE-S and UC-PHONE-S-PLUS Only) 5

Prerequisites 5
Generate Self-Signed Set of Certificates 5
Free Radius Key Configuration Steps 6
Web User Interface Configuration 8

Enable Phone Lock 9

Configuration File 9
Web User Interface Configuration 9
Phone User Interface Configuration 10

Hardware Connection 10

Port Maps 11

UC-PHONE-S, UC-PHONE-S-PLUS, UC-PHONE-T, & UC-PHONE-T-PLUS Crestron Flex VoIP Desk Phones

Introduction

This guide describes best practices for securely installing UC-PHONE-S, UC-PHONE-S PLUS, UC-PHONE-T, and UC-PHONE-T-PLUS desk phones.

This guide assumes the reader has knowledge of configuring a desk phone. For information on configuring the phones, refer to the UC-PHONE-S and UC-PHONE-S-PLUS Supplemental Guide (Doc. 8412) and the UC-PHONE-T and UC-PHONE-T-PLUS Supplemental Guide (Doc. 8413) at www.crestron.com/manuals.

Best Practices

Change the Default Password

For enhanced security, change the phone's default password. This is configured in the phone's configuration file parameter "static.security.user_password" For example, the setting "static.security.user_password = crestronadmin:H6^788rty1$)" changes the password for login "crestronadmin" to "H6^788rty1$)".

Change the Default Username

For enhanced security, there are configuration parameters to change the default usernames for the phone. These can be configured in the phone's configuration file.

- **static.security.user_name.user = crestron #** changes the default user's username to **crestron**.
- **static.security.user_name.admin = crestronadmin #** changes the default admin's username to **crestronadmin**.

Configure Strong Ciphers for TLS Connections (UC-PHONE-S and UC-PHONE-S-PLUS Only)

To ensure that strong ciphers are used for all connectivity with the phone, configure the following cipher configuration parameters must set in configuration files.

- **sip.tls_cipher_list** configures ciphers for all SIP connections
- **security.tls_cipher_list** configures ciphers for all other types of TLS connections

The exact values are shown below:

- sip.tls_cipher_list = AES:!ADH:!LOW:!EXPORT:!aNULL:!eNULL
- security.tls_cipher_list = AES:!ADH:!LOW:!EXPORT:!aNULL:!eNULL

Configure Use of TLS1.2 Protocol for All SIP Connections (UC-PHONE-S and UC-PHONE-S-PLUS Only)

To ensure that phone uses TLS1.2 protocol for SIP connections, set the "security.default_ssl_method" to "5".

Disable Bluetooth® Feature

For enhanced security, the Bluetooth feature should be disabled if it is not needed.

Bluetooth is configured from the phone's configuration file parameter "features.bluetooth_enable", or from the phone interface.

Configuration File

In the phone's configuration file, set the value of parameter "features.bluetooth_enable" to "0".

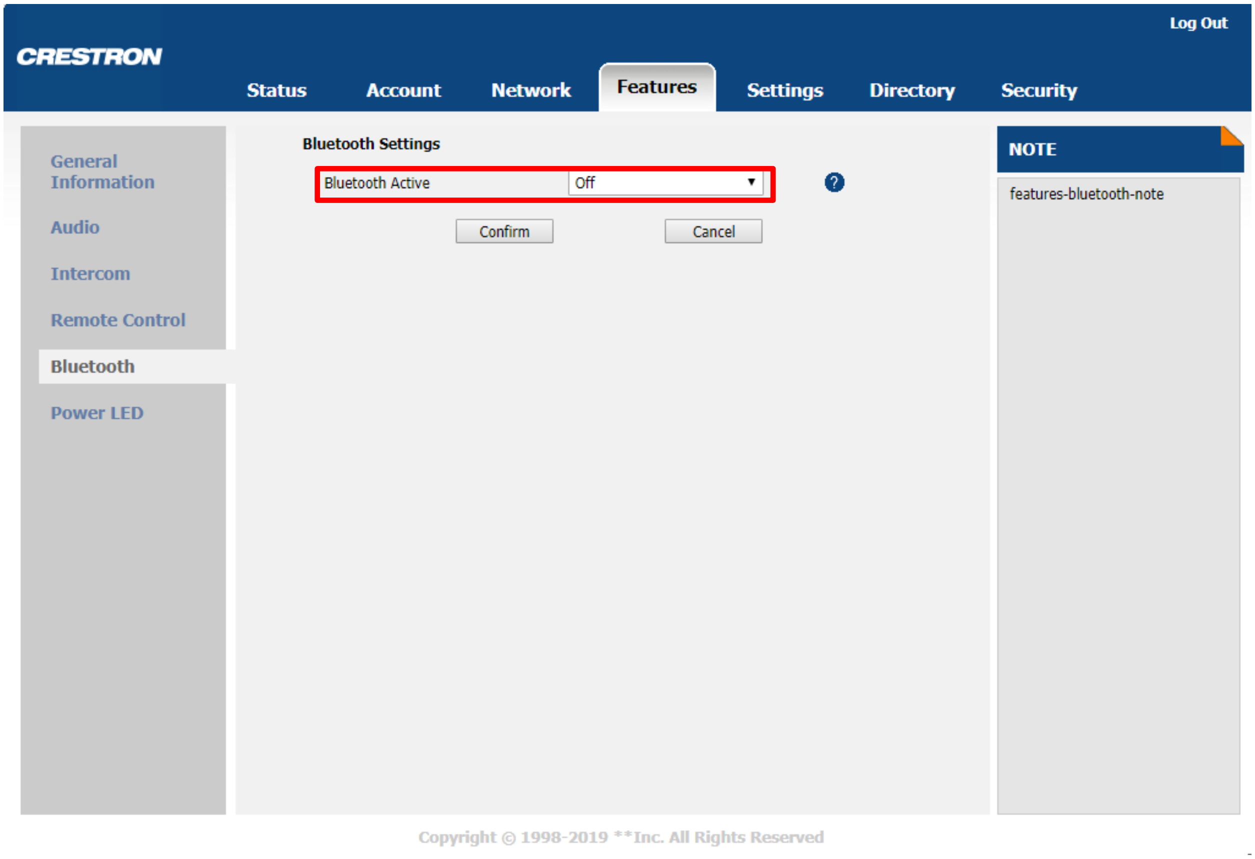
Phone User Interface Configuration

1. Tap **Menu** > **Setting** > **Basic** >**Bluetooth**.
2. Tap **Off**.

Web User Interface Configuration

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

Web user interface configuration (UC-PHONE-S shown)



Bluetooth Settings

Bluetooth Active: Off

2. Select **Off** from the **Bluetooth Active** drop-down list.

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

Disable Cleartext HTTP Protocol

The Cleartext HTTP Protocol can be disabled in the phone's configuration file or in the Web User Interface.

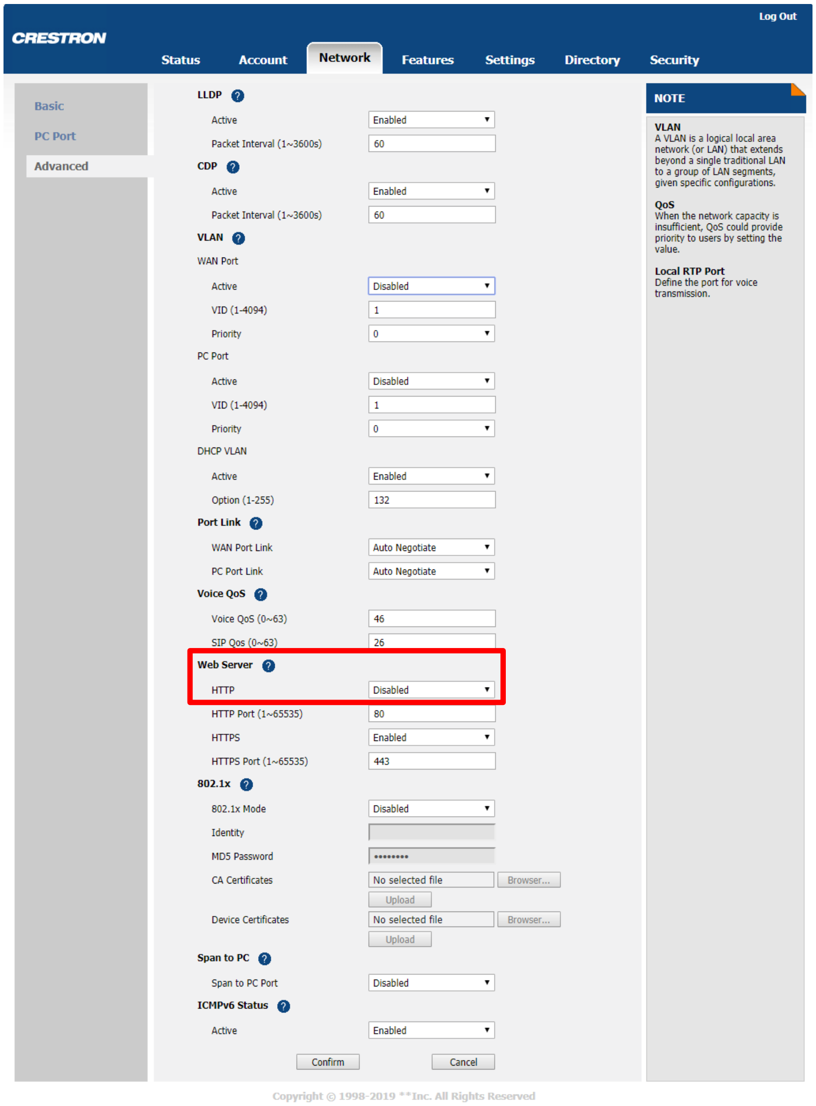
Configuration File

In the phone's configuration file, set the value of parameter "static.wui.http_enable" to "0" .

Web User Interface Configuration

1. From the Web User Interface, click **Network** > **Advanced**.

Web user interface configuration (UC-PHONE-S shown)



LLDP	
Active	Enabled
Packet Interval (1~3600s)	60
CDP	
Active	Enabled
Packet Interval (1~3600s)	60
VLAN	
WAN Port	
Active	Disabled
VID (1-4094)	1
Priority	0
PC Port	
Active	Disabled
VID (1-4094)	1
Priority	0
DHCP VLAN	
Active	Enabled
Option (1-255)	132
Port Link	
WAN Port Link	Auto Negotiate
PC Port Link	Auto Negotiate
Voice QoS	
Voice QoS (0~63)	46
SIP Qos (0~63)	26
Web Server	
HTTP	Disabled
HTTP Port (1~65535)	80
HTTPS	Enabled
HTTPS Port (1~65535)	443
802.1x	
802.1x Mode	Disabled
Identity	
MD5 Password	••••••••
CA Certificates	No selected file
Device Certificates	No selected file
Span to PC	
Span to PC Port	Disabled
ICMPv6 Status	
Active	Enabled

NOTE

VLAN
A VLAN is a logical local area network (or LAN) that extends beyond a single traditional LAN to a group of LAN segments, given specific configurations.

QoS
When the network capacity is insufficient, QoS could provide priority to users by setting the value.

Local RTP Port
Define the port for voice transmission.

2. Set **HTTP** to **Disabled**.
3. Click **Confirm** to save the setting.

Disable Wi-Fi® Feature (UC-PHONE-S and UC-PHONE-S-PLUS Only)

For enhanced security, the Wi-Fi feature should be disabled.

NOTE: Wi-Fi is not available on all phone models.

Wi-Fi is configured from the phone's configuration file parameter "static.wifi.enable", or from the phone user interface.

Configuration File

In the phone's configuration file, set the value of parameter "static.wifi.enable" to "0".

Phone User Interface Configuration

1. Tap **Menu** > **Setting** > **Basic** >**Wi-Fi**.
2. Tap **Off**.

EAP-TLS Configuration on UC-PHONE with Free Radius Server (UC-PHONE-S and UC-PHONE-S-PLUS Only)

Prerequisites

- Radius supplicant configured and pointed at the radius server.
- FreeRADIUS Version 3.0.13
- CA certificate from an in-house certificate authority.
- Server certificate issued by our in-house CA for radius server to operate.
- Client certificate(PEM format) with unencrypted private key issued by an in-house certificate authority for UC phone.

Generate Self-Signed Set of Certificates

Following are sample steps to generate a self-signed set of certificates.

NOTE: The steps shown are for example only. Consult with the network administrator for a detailed procedure for setting up of root, server and client certificate sets.

```
###### Certificate Authority Creation ######
▪   openssl genrsa -out ca.key 1024
▪   openssl req -new -x509 -days 365 -key CA.key -out ca.crt

###### Server certificate creation ######
▪   openssl genrsa -out server.key 2048
▪   openssl req -new -key server.key -out server.csr
▪   openssl x509 -days 365 -CA ca.crt –Cakey ca.key -req  -CAcreateserial -CAserial
    ca.srl -in server.csr -out server.pem
▪   cat server.pem server.key > server.pem

######  Client certificate creation ######
▪   openssl genrsa -out client.key 2048
▪   openssl req -new -key client.key -out client.csr
▪   openssl x509 -days 365 -CA ca.crt –Cakey ca.key -req  -CAserial ca.srl -in
    client.csr -out client.pem
▪   cat client.pem client.key > client.pem
```

Free Radius Key Configuration Steps

1. Navigate to the /etc/raddb directory.

2. Edit clients.conf as shown below. Only one client function should be active. The custom function named cisco3750, which has been included to match radius supplicant details is shown below.

   NOTE: "–" denotes lines to be modified and "+" denotes changes made on the respective parameters. All others parameters are not to be changed or uncommented.

```
-         nas_type          = localhost
+         nas_type          = cisco
+ client cisco3750 {
+         ipaddr = <switch/supplicant IP address>
+         netmask = <subnetmask>
+         secret = <your switch radius secret key>
+         shortname = <switch name>
+         }
```

3. Navigate to /etc/raddb/certs/ and copy the CA certificate, server certificate, and client certificates.

4. Navigate to /etc/raddb/mods-enabled/ directory, and open eap.conf file.

```
- default_eap_type = md5
+ default_eap_type = tls
-         #tls-config tls-common {
-                 private_key_password = whatever
-                 private_key_file = ${certdir}/server.pem
-                 certificate_file = ${certdir}/server.pem
-                 ca_file = ${cadir}/ca.pem
-                                 #}
-                 #tls    {
-                         #tls=tls-common
-                         #}
+         tls-config tls-common {
+                 private_key_password = <server certificate password>
+                 private_key_file = ${certdir}/<your server certificate name>
+                 certificate_file = ${certdir}/<your server certificate name>
+                 ca_file = ${cadir}/<your CA certificate name>
+                                 }
+                 tls     {
+                         tls = tls-common
+                         }
```

5. Navigate to /etc/raddb/sites-enabled/ and open the default file for editing.

6. Under the authorize function, uncomment the eap function. All other functions such as PAP, MSCHAP, etc. under authorize are to be commented as changes are not needed on the authentication function.

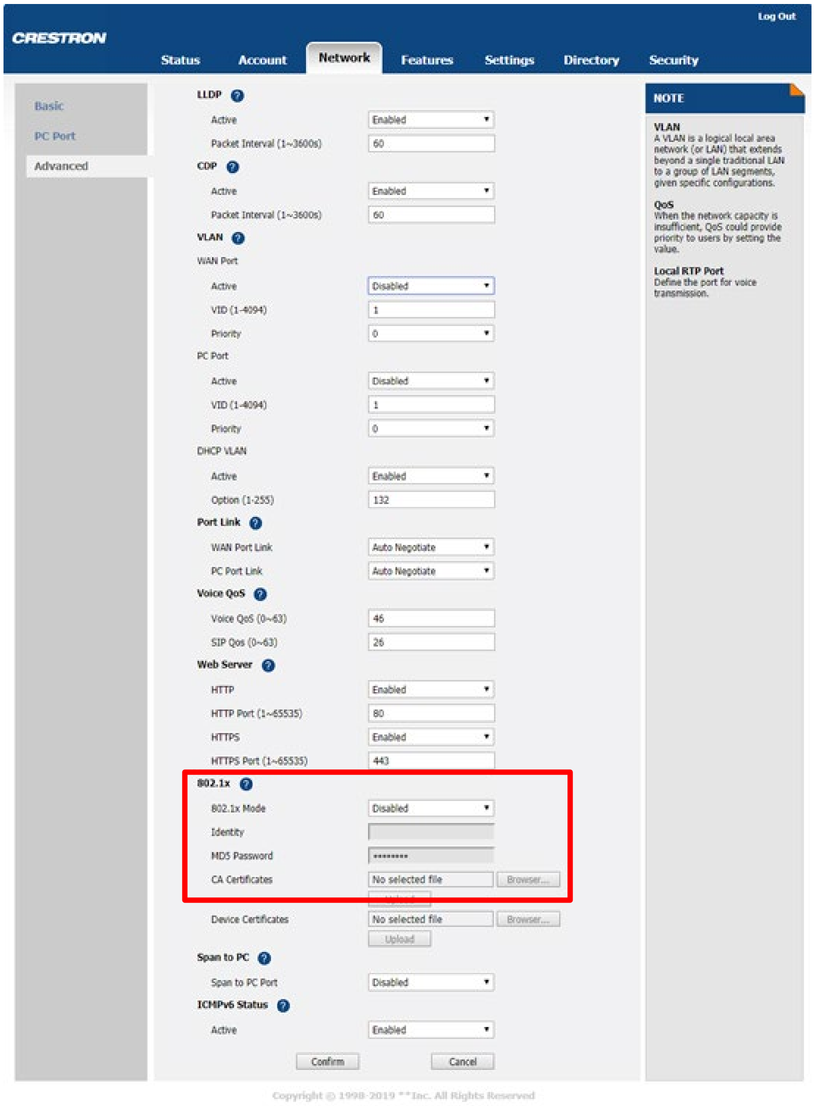
```
+         eap {
+                 ok = return
+                 updated = return
+         }
```

The FreeRADIUS service can be configured to start on boot. EAP-TLS authentication will be handled by the FreeRADIUS server.

Web User Interface Configuration

1. From the Web User Interface, click **Network** > **Advanced**.

   Web user interface configuration (UC-PHONE-S shown)



LLDP	
Active	Enabled
Packet Interval (1~3600s)	60
CDP	
Active	Enabled
Packet Interval (1~3600s)	60
VLAN	
WAN Port	
Active	Disabled
VID (1-4094)	1
Priority	0
PC Port	
Active	Disabled
VID (1-4094)	1
Priority	0
DHCP VLAN	
Active	Enabled
Option (1-255)	132
Port Link	
WAN Port Link	Auto Negotiate
PC Port Link	Auto Negotiate
Voice QoS	
Voice QoS (0~63)	46
SIP Qos (0~63)	26
Web Server	
HTTP	Enabled
HTTP Port (1~65535)	80
HTTPS	Enabled
HTTPS Port (1~65535)	443
802.1x	
802.1x Mode	Disabled
Identity	
MD5 Password	********
CA Certificates	No selected file Browser... Upload
Device Certificates	No selected file Browser... Upload
Span to PC	
Span to PC Port	Disabled
ICMPv6 Status	
Active	Enabled

NOTE

VLAN
A VLAN is a logical local area network (or LAN) that extends beyond a single traditional LAN to a group of LAN segments, given specific configurations.

QoS
When the network capacity is insufficient, QoS could provide priority to users by setting the value.

Local RTP Port
Define the port for voice transmission.

Copyright © 1998-2019 **Inc. All Rights Reserved

2. From the **802.1x Mode** drop-down list, select **EAP-TLS**.

3. Upload the CA and client certificates.

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

   b. In the **Device Certificates** field, click **Browser** to select the desired client (*.pem or *.cer) certificate from your local system.

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

4. **Identity** can be provided based on the CN name of the certificate was issued to.

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

Enable Phone Lock

To prevent unauthorized use, the phone lock feature should be enabled and configured.

Phone lock is configured from the phone's configuration file parameter "phone_setting.phone_lock.enable", the web user interface, or the phone user interface.

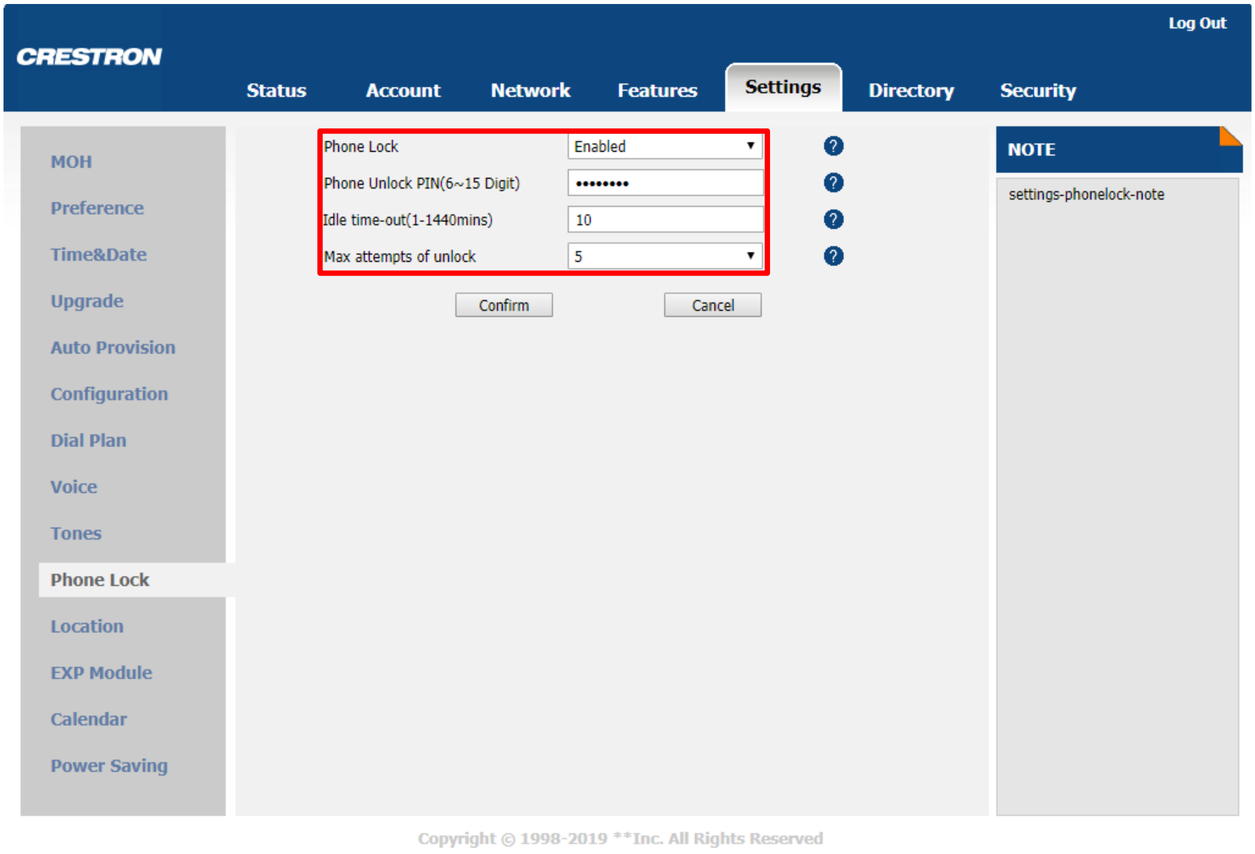
Configuration File

To enable the phone lock in the phone's configuration file, set the value of parameter "phone_setting.phone_lock.enable" to "1". Additional parameters are used to configure the feature.

Web User Interface Configuration

1. Click **Settings** > **Phone Lock** (UC-PHONE-S and UC-PHONE-S-PLUS) or **Features > Phone Lock** (UC-PHONE-T and UC-PHONE-T-PLUS).

Web user interface configuration (UC-PHONE-S shown)



Phone Lock	Enabled
Phone Unlock PIN(6~15 Digit)	••••••••
Idle time-out(1-1440mins)	10
Max attempts of unlock	5

2. Select **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 desired time in the **Idle time-out(1~1440mins)** field.
5. Select the desired value from the **Max attempts of unlock** drop-down list.
6. Click **Confirm** to accept the change.

Phone User Interface Configuration

1. Tap **Menu** > **Setting** > **Basic** > **Phone Lock**.
2. Configure the desired fields.
3. Tap **Save**.

Hardware Connection

The PC port on the bottom of the phone can provide unauthorized access to 802.1x protected networks if the network switch is not set for MAC-based access control.

Port Maps

The following tables show the port maps for the UC-PHONE-S, UC-PHONE-S-PLUS, UC-PHONE-T, and UC-PHONE-T-PLUS.

UC-PHONE-S and UC-PHONE-S-PLUS

PORT	TYPE	DIRECTION	FUNCTION	OPEN	NOTES
80	TCP	Both	Website http server	Open	The default port used when accessing the web user interface by http protocol
443	TCP	Both	Website https server	Open	The default port used when accessing the web user interface by https protocol
5061	TCP	Both	SIP-TLS connection	Open	The default port used when using SIP-TLS connection

UC-PHONE-T and UC-PHONE-T-PLUS

PORT	TYPE	DIRECTION	FUNCTION	OPEN	NOTES
80	TCP	Both	Website http server	Open	The default port used when accessing the web user interface by http protocol
443	TCP	Both	Website https server	Open	The default port used when accessing the web user interface by https protocol

Crestron Electronics, Inc.
15 Volvo Drive, Rockleigh, NJ 07647
Tel: 888.CRESTRON
Fax: 201.767.7576
www.crestron.com

Secure Deployment Guide – DOC. 8457A
(2052763)
9/11/19
Specifications subject to
change without notice.