C620

SIP Wireless Conference Phone
Administrator and Provisioning Manual

Rev. 3 12/24

CONTENTS

Preface 7

Text Conventions 8
Audience 8
Related Documents 8

Introducing the C620 9

About the C620 SIP Wireless Conference Phone 10
Quick Reference Guide 11
C620 Base Station 11
C620 Conference Phone 12
Network Requirements 13
C620 Configuration Methods 15
Customizing Soft Keys 16
Factory Reset the Base Station 18

Configuration Using the Phone Menus 19

Viewing the Main Menu 20
Using the Status menu 20
Viewing Line status 22
Using the Admin Settings Menu 23
Using the Network Setting menu 25
Using the Security menu 31
Using the Provisioning menu 31
Editing the conference phone PIN code 34

Using the WebUI 35

Using the Web User Interface (WebUI) 36
Status Page 39
System Status 39
Device Status 40
System Pages 41
SIP Account Management 41
General Account Settings 41
Dial Plan 44

SIP Server Settings 45
Registration Settings 45
Outbound Proxy Settings 45
Backup Outbound Proxy Settings 46
Caller Identity Settings 46
Audio Settings 46
Quality of Service 48
Signaling Settings 48
Voice Settings 49
Feature Access Codes Settings 49
Voicemail Settings 51
NAT Traversal 51
Music on Hold Settings 52
Network Conference Settings 52
Session Timer 52
Jitter Buffer 53
Keep Alive 53
XSI 54
Call Settings 55
General Call Settings 55
Do Not Disturb 55
Call Forward 55
User Preferences 57
General User Settings 57
Wireless Conference Phone 58
Soft Keys 58
Type 60
Server Application 61
Action URI Syntax 61
Action URI 63
XML Push Settings 65
Network Pages 66
Basic Network Settings 67
IPv4 67
IPv6 68
Advanced Network Settings 69
VLAN 69
LLDP-MED 70
802.1x 70
VPN 71
Contacts Pages 72
Base Directory 72
Create Base Directory Entry 75
Directory Import/Export 75
Blacklist 76
Create Blacklist Entry 78
Blacklist Import/Export 79
LDAP 80
LDAP Settings 80
Broadsoft Directory and CallLogs 82
Directory Type 83
CallLogs Type 83

Remote XML 84
Remote XML Directory Format 84
Servicing Pages 86
Reboot 86
Time and Date 86
Time and Date Format 87
Network Time Settings 87
Time Zone and Daylight Savings Settings 87
Manual Time Settings 88
Custom Language 89
Firmware Upgrade 90
Auto Upgrade 90
Base Firmware 90
Wireless Conf. Phone Firmware 91
Firmware Server Settings 91
Manual Firmware Update and Upload 92
Updating the base station 92
Updating the conference phone 92
Provisioning 94
Provisioning Server 95
Plug-and-Play Settings 95
DHCPv4 Settings 96
Resynchronization 96
Import Configuration 98
Export Configuration 98
Reset Configuration 99
Security 100
Passwords 100
Web Server 101
Trusted Servers 101
Trusted IP 102
Certificates 103
Device Certificate 103
Trusted Certificate 104
TR-069 Settings 106
System Logs 107
Syslog Settings 107
Network Trace 108
Download Log 108

Provisioning Using Configuration Files 111

The Provisioning Process 112
Resynchronization: configuration file checking 113
C620 restart 113
Configuration File Types 114
Data Files 115
Configuration File Tips and Security 116
Clearing parameters with %NULL in configuration file 116
Guidelines for the MAC-specific configuration file 116
Securing configuration files with AES encryption 117

Configuration File Parameter Guide 119

"sip_account" Module: SIP Account Settings 121
General configuration file settings 121
MAC-specific configuration file settings 132
"hs_settings" Module: Handset Settings 136
General configuration file settings 137
MAC-specific configuration file settings 141
“system” Module: System settings 143
MAC-specific configuration file settings 143
"network" Module: Network Settings 144
General configuration file settings 144
MAC-specific configuration file settings 146
"provisioning" Module: Provisioning Settings 149
General configuration file settings 149
MAC-specific configuration file settings 152
"time_date" Module: Time and Date Settings 154
"log" Module: Log Settings 159
"remoteDir" Module: Remote Directory Settings 160
"web" Module: Web Settings 165
“trusted_ip” Module: Trusted IP Settings 166
“trusted_servers” Module: Trusted Server Settings 167
"user_pref" Module: User Preference Settings 168
General configuration file settings 168
MAC-specific configuration file settings 168
"call_settings" Module: Call Settings 169
General configuration file settings 169
MAC-specific file settings 169
“audio” Module: Audio Settings 171
"file" Module: Imported File Settings 173
General configuration file settings 173
MAC-specific configuration file settings 175
“xml_app” Module: XML App Settings 177
“tr069” Module: TR-069 Settings 178
"tone" Module: Tone Definition Settings 180
"profile" Module: Password Settings 185
General configuration file settings 185
MAC-specific configuration file settings 185
"speed_dial" Module: Speed Dial Settings 187

Troubleshooting 189

Common Troubleshooting Procedures 189

Appendixes 191

Appendix A: Maintenance 191
Appendix B: GNU General Public License 192

PREFACE

Congratulations on your purchase of this Snom product. Please thoroughly read this manual for all the feature operations and troubleshooting information necessary to install and operate your new Snom product. You can also visit our website at *www.snomamericas.com*.

This administrator and provisioning manual contains detailed instructions for installing and configuring your C620 SIP Wireless Conference Phone with software version 1.0.5.17 or newer. See *"Using the Status menu" on page 20* for instructions on checking the software version on the C620. Please read this manual before installing the product.

Please print this page and record the following information regarding your product:

Model number: C620

Type: SIP Wireless Conference Phone

Serial number: _____

Purchase date: _____

Place of purchase: _____

Both the model and serial numbers of your Snom product can be found on the bottom of the device.

Save your sales receipt and original packaging in case it is necessary to return your telephone for warranty service.

Text Conventions

Table 1 lists text formats and describes how they are used in this guide.

Table 1. Description of Text Conventions

Text Format	Description
Screen	Identifies text that appears on a device screen or a WebUI page in a title, menu, or prompt.
HARD KEY or **DIAL-PAD KEY**	Identifies a hard key, including the dial-pad keys.
CallFwd	Identifies a soft key.
NOTE Notes provide important information about a feature or procedure.	Example of a Note.
CAUTION *A caution means that loss of data or unintended circumstances may result.*	Example of a Caution.

Audience

This guide is written for installers and system administrators. It assumes that you are familiar with networks and VoIP, both in theory and in practice. This guide also assumes that you have ordered your IP PBX equipment or service and selected which PBX features you want to implement. This guide references specific IP PBX equipment or services only for features or settings that have been designed for a specific service. Please consult your equipment supplier or service provider for recommended switches, routers, and firewall and NAT traversal settings, and so on.

As the C620 SIP Wireless Conference Phone becomes certified for IP PBX equipment or services, Snom may publish interop guides for those specific services. The interop guides will recommend second-party devices and settings, along with C620-specific configurations for optimal performance with those services. For the latest updates, visit our website at *www.snomamericas.com*.

Related Documents

The ***C620 Quick Installation Guide*** contains a quick reference guide to the C620 external features and brief instructions on connecting the C620 to a working IP PBX system.

The ***C620 User manual*** contains a quick reference guide, full installation instructions, instructions for making and receiving calls, and a guide to all user-configurable settings.

The documents are available from our website at *www.snomamericas.com*.

CHAPTER 1

INTRODUCING THE C620

This administrator and provisioning guide contains detailed instructions for configuring the C620 SIP Wireless Conference Phone. Please read this guide before attempting to configure the C620.

Some of the configuration tasks described in this chapter are duplicated in the Web User Interface (WebUI) described in the next chapter, but if you need to assign static IP addresses, they must be set at each device.

This chapter covers:

- *"About the C620 SIP Wireless Conference Phone" on page 10*
- *"Quick Reference Guide" on page 11*
- *"Network Requirements" on page 13*
- *"C620 Configuration Methods" on page 15*
- *"Customizing Soft Keys" on page 16.*

About the C620 SIP Wireless Conference Phone

The Snom C620 SIP Wireless Conference Phone is a designed to work with popular SIP telephone (IP PBX) equipment and services. Once you have ordered and configured your SIP equipment or service, the C620 enables you to make and receive calls as you would with any other business phone.

The C620 base station features include:

- Up to 3 SIP account registrations
- Up to 2 active SIP sessions
- 9 programmable soft key “slots”
- Power over Ethernet enabled
- 1,000-entry base directory

The C620 conference phone features include:

- Backlit Liquid Crystal Display
- Speakerphone, hold and mute capability
- 3-way conferencing
- 100-entry call history shared across Received and Missed calls
- 200-entry local directory

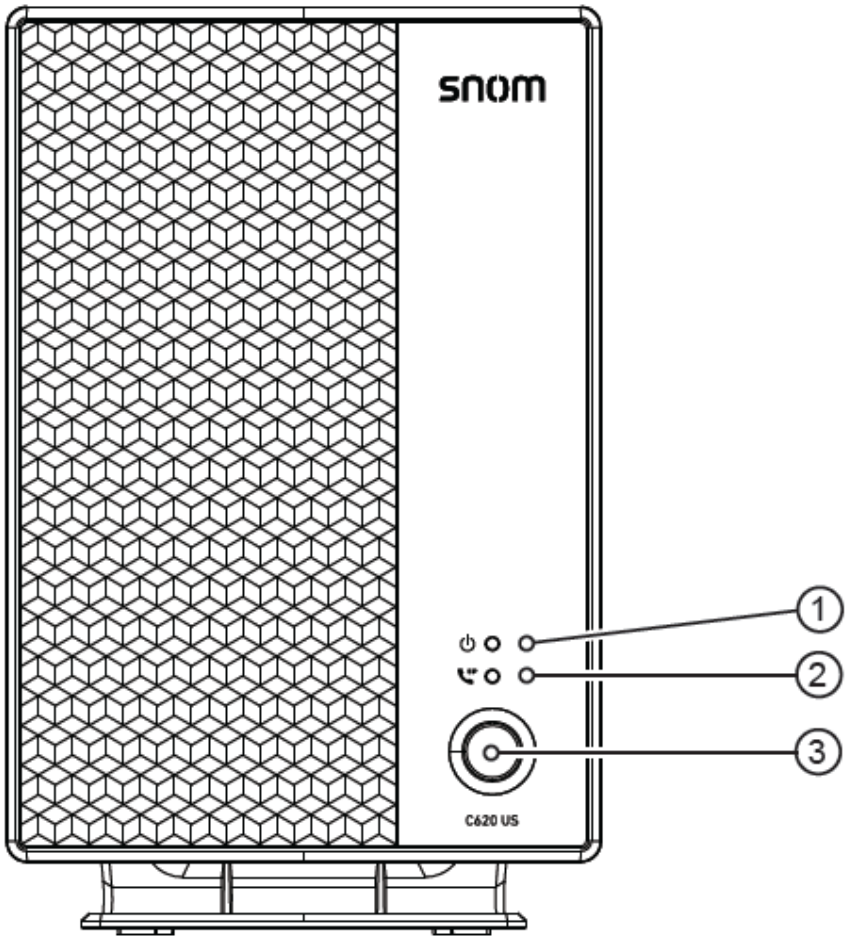
You can configure the C620 using the menus on the conference phone, a browser-based interface called the WebUI, or an automatic provisioning process (see *“Provisioning Using Configuration Files” on page 111*). The WebUI enables you to configure the C620 using a computer that is connected to the same Local Area Network. The WebUI resides on the C620, and may get updated with firmware updates.

The C620 has three programmable soft keys in three layers. You can program these soft keys for the Idle screen, Call Active screen, Call Held screen and Live Dial screen. For more details, see *“Customizing Soft Keys” on page 16*.

Quick Reference Guide

The external features of the C620 base station and conference phone are described below.

C620 Base Station

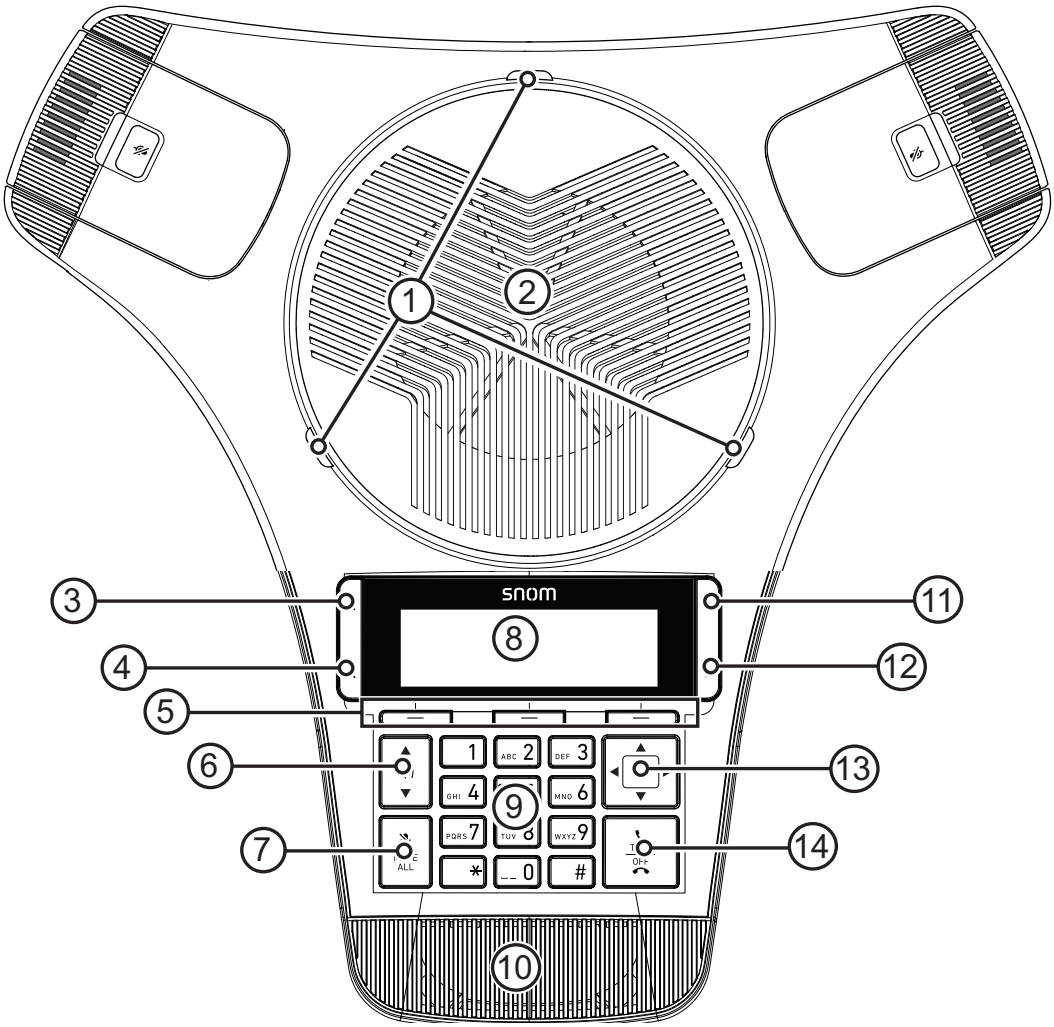


1. (Power LED)

2. SIP (VoIP LED)

3. LINK key

C620 Conference Phone



1. Status indicator
2. Speaker
3. (HOLD)
4. (CANCEL)
5. Soft Keys
6. Volume
7. **MUTE ALL**
8. LCD display screen
9. Dial pad keys
10. Front microphone
11. (Menu)
12. (OK)
13. Navigation Keys
14. **TALK / OFF**

Network Requirements

A simple C620 SIP Wireless Conference Phone installation example is shown in Figure 1. A switched network topology is recommended for your LAN (using standard 10/100 Ethernet switches that carry traffic at a nominal rate of 100 Mbit/s).

The office LAN infrastructure should use Cat.-5/Cat.-5e cable.

The C620 base station requires a wired connection to the LAN. However, wireless connections from your LAN to other devices (such as laptops) in your office will not impede performance.

A Dynamic Host Configuration Protocol (DHCP) server is recommended and must be on the same subnet as the C620 SIP Wireless Conference Phones so that IP addresses can be auto-assigned. In most cases, your network router will have a DHCP server. By default, the C620 has DHCP enabled for automatic IP address assignment.

NOTE Some DHCP servers have default settings that limit the number of network IP addresses assigned to devices on the network. You should log in to your server to confirm that the IP range is sufficient.

If no DHCP server is present, you can assign a static IP to the C620. You can assign a static IP address using the C620 menu.

To assign a static IP: On the handset Main menu, go to **Status & Settings > Admin settings > Network setting > IPv4 (or IPv6) > Set static IP**.
If you do not have a DHCP server or do not manually assign static IPs, you will not be able to access the WebUI.

A DNS server is recommended to resolve the path to the Internet and to a server for firmware and configuration updates. If necessary, the system administrator can also download upgrade files and use the WebUI to update the C620 firmware and/or configuration settings manually.

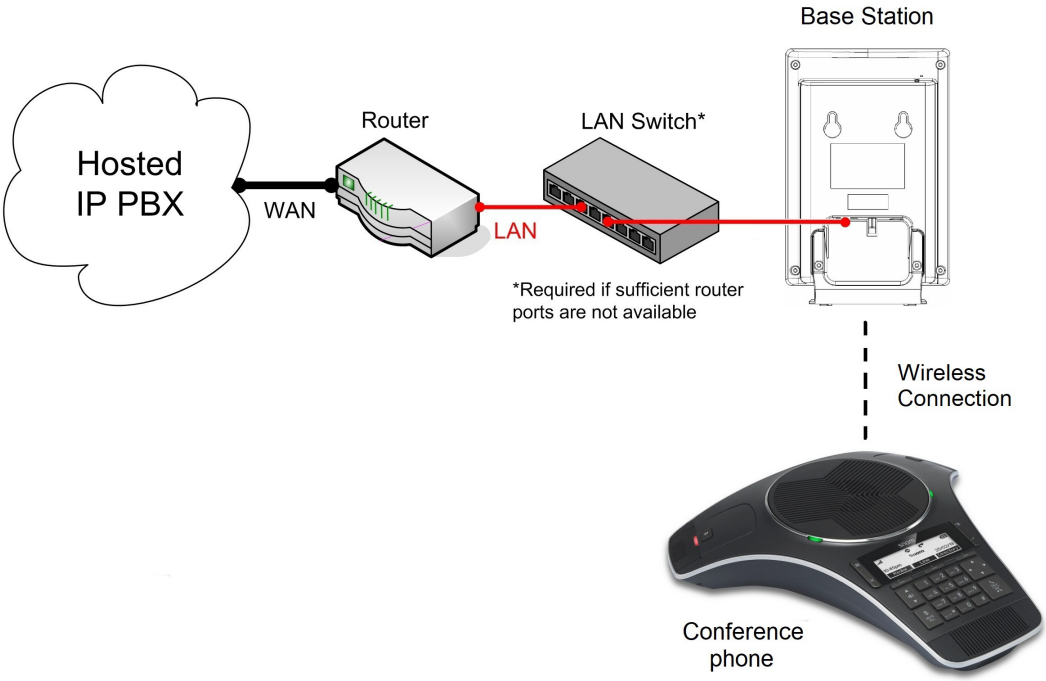


Figure 1. C620 Installation Example

C620 Configuration Methods

You can configure the C620 using one of the following methods:

- From the conference phone using the menus. The conference phone menus are best suited to configuring a few settings, perhaps after the initial setup has been done. For administrators, the settings available on the conference phone Admin Settings menu include network settings, account settings, and provisioning settings. See *"Using the Admin Settings Menu" on page 23*. Many of the user settings accessible on the conference phone are most useful for end users. Through the User Settings menu, they can customize the screen appearance, sounds, and manage calls. For more information, see the C620 User Manual.
- The Web User Interface, or WebUI, which can be accessed using an Internet browser. See *"Using the WebUI" on page 35*. The browser-based interface is easy to navigate and best suited to configuring a large number of C620 settings at once. The WebUI gives you access to every setting required for configuring a single device. You can enter service provider account settings on the WebUI, configure the soft keys, and set up provisioning, which will allow you to automatically and remotely update the C620 after initial configuration.
- Provisioning using configuration files. Working with configuration files enables you to configure the device at regular intervals. There are several methods available to enable the C620 to locate and upload the configuration file. For example, you can enable the C620, when it starts up or reboots, to check for the presence of a configuration file on a provisioning server. If the configuration file is new or has been modified in any way, the C620 automatically downloads the file and applies the new settings. For more information, see *"Provisioning Using Configuration Files" on page 111*.

Customizing Soft Keys

You can use the WebUI or parameters to customize the soft keys that appear on the Idle screen, Call Active screen, Call Held screen and Live Dial screen. For more details, see *"Soft Keys" on page 58* and *""hs_settings" Module: Handset Settings" on page 136*.

Table 2 shows the soft key options available for each screen. Each screen can have a maximum of nine soft keys.

Table 2. Custom Soft Keys

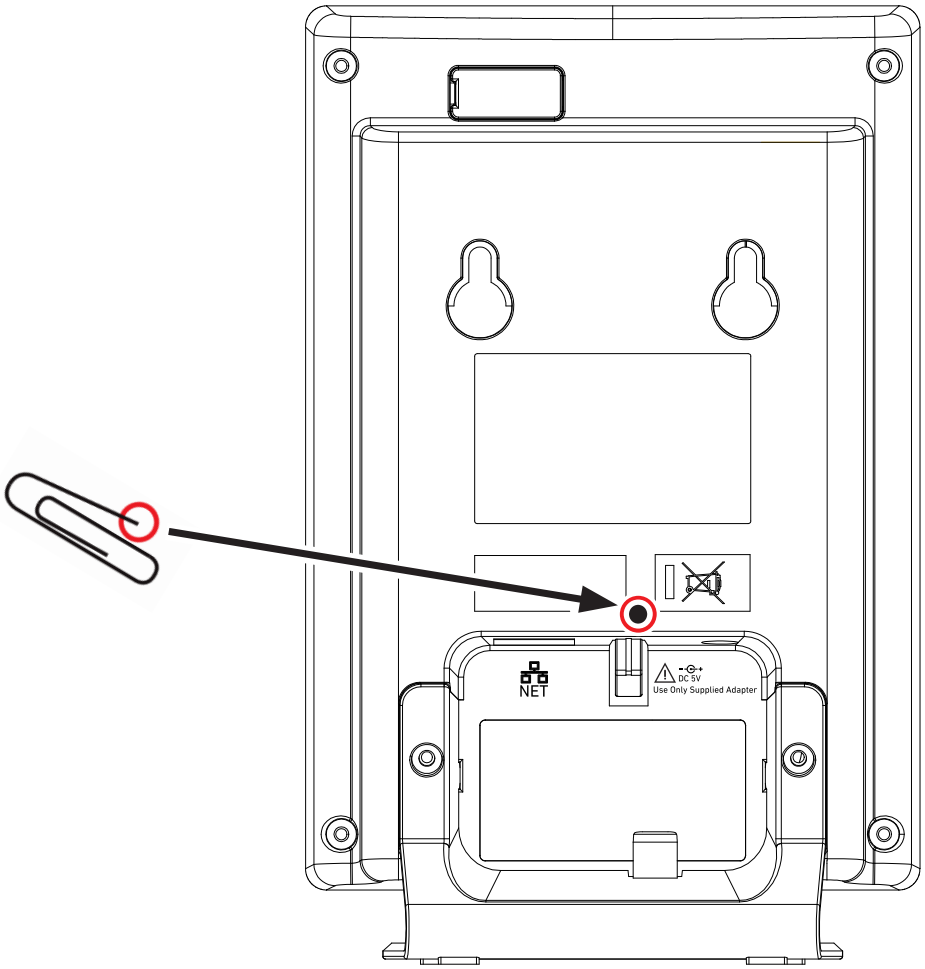
Screen	Available Soft Keys	Soft Key Text
Idle	Blank	
	Directory	Dir
	Call History	Call Hist
	Redial	Redial
	Messages	Message
	Do Not Disturb	DND
	Call Forward	CallFWD
	Call Forward All	FwdAll
	Call Forward No Answer	CFNA
	Call Forward Busy	cfwdB
	Call Return	CallBack
	Line (visible with more than one account assigned)	Line
	Settings	Settings
	Quick Dial	Qdial
Call Active	Blank	
	New	New
	End	End
	Hold	Hold
	Transfer	Transfer
	Conference	Conf.
	Private hold	Priv hold
Call Held	Blank	
	End	End
	New	New

Table 2. Custom Soft Keys

Screen	Available Soft Keys	Soft Key Text
	Resume	Resume
	Transfer	Transfer
	Conference	Conf.
	Quick Dial	Qdial
Live Dial	Blank	
	Directory	Dir
	Call History	Call Hist
	Redial	Redial
	Messages	Message
	End	End
	Dial	Dial
	Cancel	Cancel
	Backspc	Backspc
	Quick Dial	Qdial

Factory Reset the Base Station

1. Using a paperclip, or something similar, press and hold the reset button on the back of the base station for 15 seconds.
2. Release the reset button. During the next one to two minutes, the following occurs:
   - The conference phone displays “Please wait”.
   - The VoIP LED on the base station flashes quickly, then the Power LED and the VoIP LED flash alternatingly.
   - The conference phone beeps once and displays “Out of range or no power at base”.
   - The status indicators on the conference phone flash red quickly.
   - The conference phone displays the idle screen. This indicates the factory reset has completed.



CHAPTER 2

CONFIGURATION USING THE PHONE MENUS

The C620 Main Menu has the following sub-menus:

- **Directory**—view and dial entries in the Local directory, Base directory, Broadsoft directory, Blacklist and Speed dial list.
- **Call history**—view missed calls, received calls and dialed calls.
- **Message**—access the voice messages on each account.
- **Call Features**—set DND, call forward settings and other calling features.
- **Status & Settings**—display the Status & Settings menu with the following items:
  - **Status**—view the C620 network status, account registration status, and product information.
  - **User settings**—configure the language, date/time, programmable keys, display settings, audio settings, and register/deregister conference phones/wireless mics to the base station.
  - **Admin settings**—configure network settings (enter static IP addresses, for example), secure browsing, provisioning settings, edit PIN code, and perform firmware update.

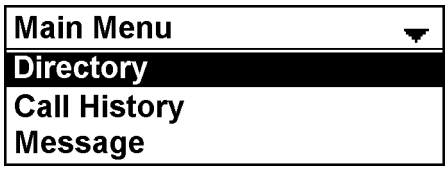
This chapter contains instructions for using the Admin Settings menu and for accessing the Status menu. See the C620 User Manual for more information about the other menus.

Viewing the Main Menu

To use the conference phone menu:

3. When the conference phone is idle, press .

   The **Main Menu** appears.



4. Press ▼ or ▲ to highlight the desired sub-menu, and then press .

   - Press to select a menu item.
   - Press to cancel an operation or return to the previous screen.

Using the Status menu

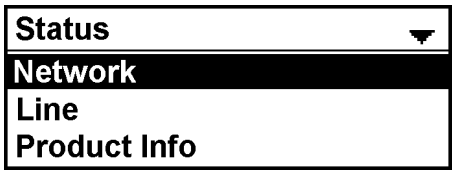
Use the **Status** menu to verify network settings and begin troubleshooting if network problems or account registration issues affect operation.

You can also find the software version of the C620 on the **Product Info** screen, available from the **Status** menu.

To view the Status menu:

1. When the conference phone is idle, press .
2. On the **Main Menu**, press ▲ or ▼ to highlight **Status & Settings**, and then press .
3. With **Status** highlighted, press .

   The **Status** menu appears.



4. On the **Status** menu, press ▲ or ▼ to highlight the desired menu item, and then press .

The available status menus are listed in Table 3.

Table 3. Status menu summary

Menu	Information listed
Network	Network status: ■ IPv4 or IPv6 ● IP Type (DCHP/Auto/Static IP/Disabled) ● IP address ● Subnet Mask ● Gateway IP address ● DNS Server 1 IP address ● DNS Server 2 IP address
Line	Lines and registration status. On the **Line** menu, highlight and select the desired line to view detailed line status information: ■ Line Status (Registered/Not registered) ■ Display name ■ User ID ■ Server
Product Info	Shows the product info for the speaker or base station. Select **Speaker** or **Base** to view the: ■ Model number (speaker only) ■ Serial number (speaker only) ■ Firmware version ■ V-Series ■ Hardware version

Viewing Line status

To view line status, from the **Status** menu, select **Line**. The **Line** menu lists the available lines, along with icons indicating each line's current registration status.

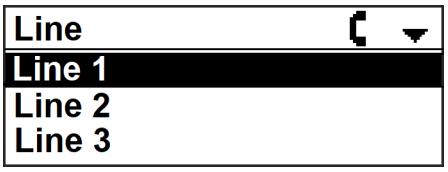
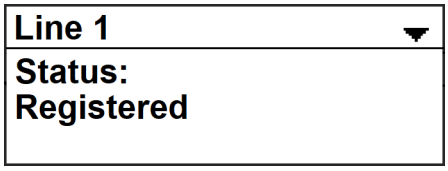


Table 4. Line status icons

Icon	Description
	Line registered
	Line unregistered

To view complete status information for a line:

On the Line menu, press ▲ or ▼ to highlight the desired line, and then press . The Line status screen appears.



Using the Admin Settings Menu

To access the Admin Settings menu:

1. When the conference phone is idle, press .
2. On the **Main Menu**, press ▲ or ▼ to highlight **Status & Settings**, and then press .

   The **Status & Settings** screen appears.

   Status & Settings
   Status
   User settings
   Admin settings

3. Press ▲ or ▼ to highlight **Admin settings**, and then press .
4. Use the dial pad to enter the admin password, and then press .
   The default password is **admin**.
   - To switch between entering uppercase letters, lowercase letters and numbers, press the middle soft key until its label displays **ABC** , **abc** or **123** .
   - With **ABC** or **abc** selected, press **1**, **0**, ✱ or **#** to enter symbols. The period and "@" symbols are available under the ✱ key.
   - Press **Backspc** to delete a character.

The Admin settings are listed in Table 5.

Password:
_
Backspc **ABC** **Next**

Table 5. Admin setting summary

Setting	Options
Network setting	IPv4 IPv6 VLAN ID
Security	Secure Browsing (Enabled, Disabled)
Provisioning	Server string Login ID Login PW

Table 5. Admin setting summary

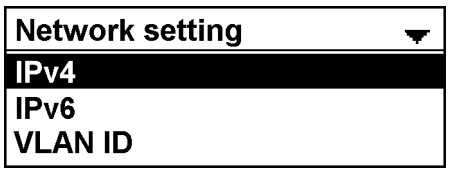
Setting	Options
Edit PIN code	Edit PIN code
Firmware update	Select **Firmware update** to have the handset check whether a firmware update is available. See *“Updating the conference phone” on page 92*.

Using the Network Setting menu

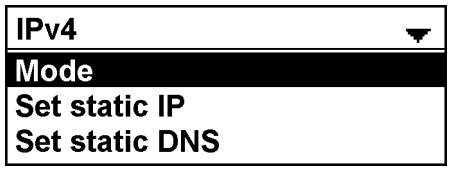
Use the Network setting menu to configure network-related settings for the C620. For more information about these settings, see *"Basic Network Settings" on page 67* and *"Advanced Network Settings" on page 69*.

To use the Network setting menu:

1. From the **Admin Settings** menu, press ▲ or ▼ to highlight **Network setting**, and then press ✓.
2. Press ▲ or ▼ to highlight **IPv4** or **IPv6**, and then press ✓.



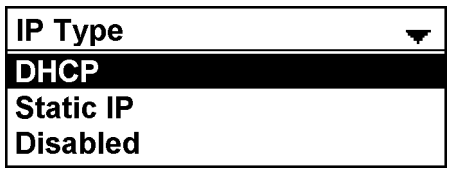
The **IPv4** or **IPv6** menu appears.



To enable or disable DHCP:

1. From the **IPv4** or **IPv6** menu, with **Mode** highlighted, press ✓.

   The **IP Type** screen appears.



2. Press ▲ or ▼ to select **DHCP** (for IPv4), **Auto** (for IPv6), **Static IP**, or **Disabled**, and then press ✓.

For IPv4, DHCP is enabled by default, which means the C620 will get its IP address from the network. When DHCP is disabled, you must enter a static IP address for the C620. For IPv6, DHCP is disabled by default.

NOTE You must be familiar with TCP/IP principles and protocols to configure static IP settings.

To set static IP for the C620:

1. From the **IPv4** or **IPv6** menu, menu, press ▲ or ▼ to highlight **Set static IP**, and then press ✓.

   If **Mode** is set to Static IP, the **Set static IP** menu appears. If **Mode** is not set to Static IP an error message appears briefly before returning you to the **Network setting** menu.

   Network setting
   DHCP in use.
   Static IP
   cannot be used

2. On the **Set static IP** menu, with **IP Address** highlighted, press ✓.

   Set static IP
   IP Address
   Subnet Mask
   Gateway

3. Enter the Static IP Address.

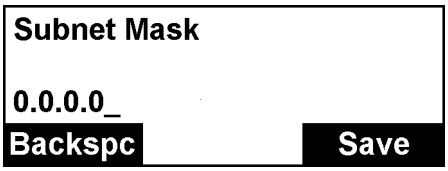
   IP Address
   0.0.0.0_
   Backspc **Save**

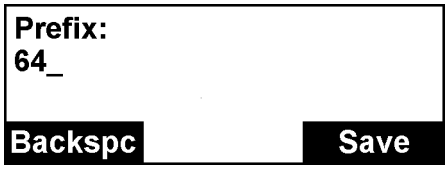
   - Press **Backspc** to delete numbers.
   - Use the dial pad to enter numbers.
   - For IPv6, press **2** or **3** repeatedly to select the letters printed on the key.
   - For IPv6, press the ✱ key to add a **:** symbol.
   - For IPv4, press the ✱ key to add a **.** symbol.

4. Press **Save** .

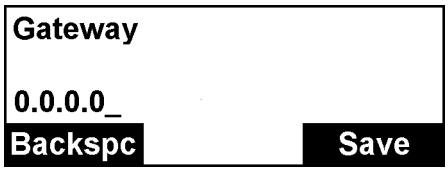
5. On the **Set static IP** menu, press ▲ or ▼ to highlight **Subnet Mask** for IPv4 or **Prefix** for IPv6, and then press ✓.

6. Enter the Subnet Mask for IPv4 or Prefix for IPv6.



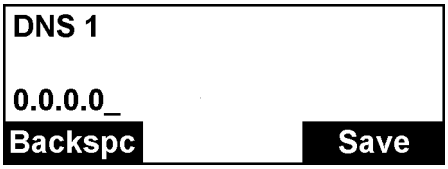


7. Press **Save** .
8. On the **Set static IP** menu, press ▲ or ▼ to highlight **Gateway**, and then press ✓.
9. Enter the Gateway.



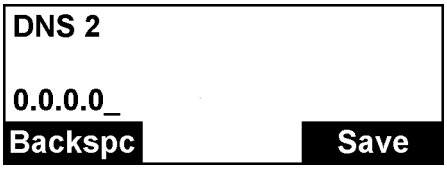
10. Press **Save** .
11. On the **Set static IP** menu, press ▲ or ▼ to highlight **DNS1**, and then press ✓.
12. Enter the IP address of the primary DNS server for your network.

    The value you enter will also be assigned to: **IPv4** or **IPv6** > **Set Static DNS** > **DNS1**.



13. Press **Save** .
14. On the **Set static IP** menu, press ▲ or ▼ to highlight **DNS2**, and then press ✓.
15. Enter the IP address of the secondary DNS server for your network.

    The value you enter will also be assigned to: **IPv4** or **IPv6** > **Set Static DNS** > **DNS2**.

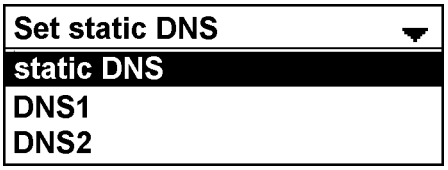


16. Press **Save** .

To set static DNS:

1. From the **IPv4** or **IPv6** menu, press ▲ or ▼ to highlight **Set static DNS**, and then press ✓.

   The **Set static DNS** menu appears.

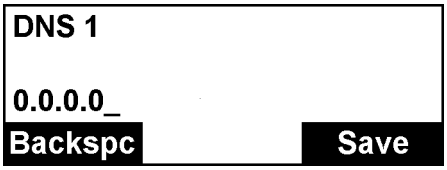
2. On the **Set static DNS** menu, with **static DNS** highlighted, press ✓.

3. Press ▲ or ▼ to select **Enabled** or **Disabled**, and then press ✓.

4. On the **Set Static DNS** menu, press ▲ or ▼ to highlight **DNS 1**, and then press ✓.

5. Enter the IP address for the primary DNS server.

   The value you enter will also be assigned to: **IPv4** or **IPv6** > **Set Static IP** > **DNS1**.

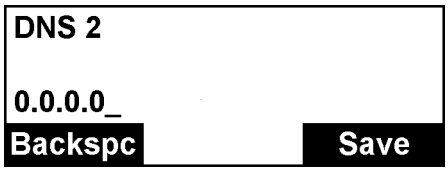
   - Press **Backspc** to delete numbers.
   - Use the dial pad to enter numbers.
   - For IPv6, press **2** or **3** repeatedly to select the letters printed on the key.
   - For IPv6, press the * key to add a **:** symbol.
   - For IPv4, press the * key to add a **.** symbol.

6. Press **Save** .

7. On the **Set static DNS** menu, press ▲ or ▼ to highlight **DNS 2**, and then press ✓.

8. Enter the IP address for the secondary DNS server. The C620 uses this server if the primary server does not respond.

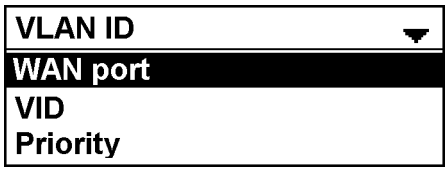
   The value you enter will also be assigned to: **IPv4** or **IPv6** > **Set Static IP** > **DNS2**.



9. Press **Save** .

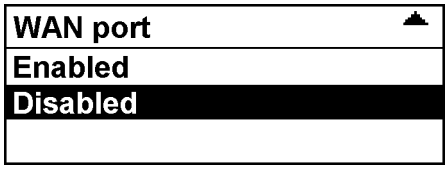
To set the VLAN ID for the C620:

1. From the **Network setting** menu, press ▲ or ▼ to highlight **VLAN ID**, and then press ✓.

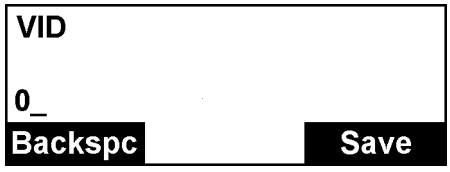


2. On the **VLAN ID** menu, with **WAN port** highlighted, press ✓.

   The WAN Port screen appears.



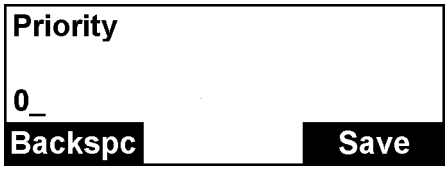
3. Press ▲ or ▼ to select **Enabled** or **Disabled**, and then press ✓.
4. On the **VLAN ID** menu, press ▲ or ▼ to highlight **VID**, and then press ✓.
5. Enter the WAN VID. The valid range is 0 to 4095.



   - Use the dial pad to enter numbers.
   - Press **Backspc** to delete numbers.

6. Press **Save** .
7. On the **VLAN ID** menu, press ▲ or ▼ to highlight **Priority**, and then press ✓.

8. Enter the WAN Priority. The valid range is 0 to 7.



9. Press **Save** .

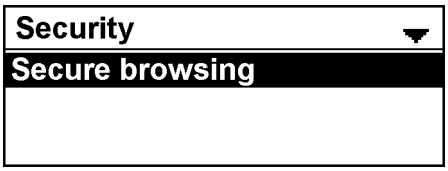
Using the Security menu

Use the Security menu to configure secure browsing settings.

To turn on/off secure browsing:

1. From the **Admin Settings** menu, press ▼ to highlight **Security**, and then press ✓.

   The Security menu appears.



2. With **Secure Browsing** selected, press ✓.
3. Press ▲ or ▼ to select **Enabled** or **Disabled**, and then press ✓.

   The message “Reboot Base to apply new Web server” appears.

4. Press **Ok**.

   After a few moments, the C620 will reboot.

Using the Provisioning menu

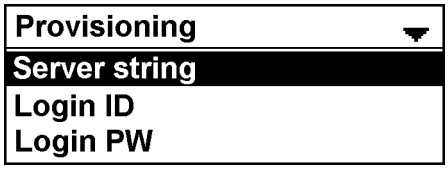
Use the Provisioning menu to configure auto-provisioning settings. For more information about auto-provisioning, see *“Provisioning” on page 94* and *“Provisioning Using Configuration Files” on page 111*.

On the Provisioning menu you can configure:

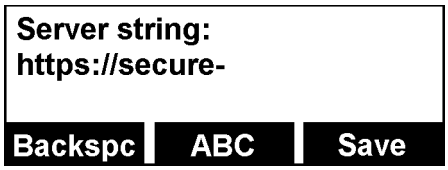
- Server string—the URL of the provisioning server. The URL can include a complete path to the configuration file.
- Login ID—the username the C620 will use to access the provisioning server.
- Login PW—the password the C620 will use to access the provisioning server.

To use the Provisioning menu:

1. From the **Admin Settings** menu, press ▼ to highlight **Provisioning**, and then press ✓.
   The **Provisioning** menu appears.



2. On the **Provisioning** menu, with **Server string** highlighted, press ✓.
3. Enter the URL of the provisioning server.
   - Press **Backspc** to delete a character.
   - Use the dial pad to enter characters.
   - To switch between entering uppercase letters, lowercase letters and numbers, press the middle soft key until its label displays **ABC** , **abc** or **123** .
   - With **ABC** or **abc** selected, press **1**, **0**, ✱ or **#** to enter symbols. The period and “@” symbols are available under the ✱ key.

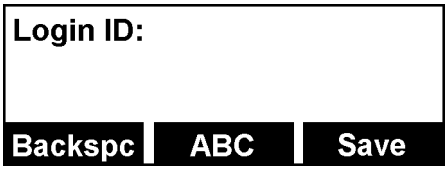


   The format of the URL must be RFC 1738 compliant, as follows:
   "<schema>://<user>:<password>@<host>:<port>/<url-path>"

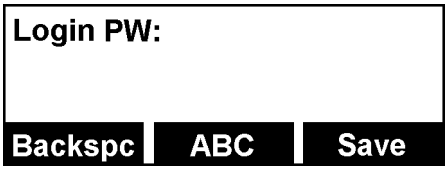
   "<user>:<password>@" may be empty.

   "<port>" can be omitted if you do not need to specify the port number.

4. Press **Save** .
5. On the **Provisioning** menu, press ▲ or ▼ to highlight **Login ID**, and then press ✓.
6. Enter the Login ID for access to the provisioning server if it is not part of the server string.



7. Press **Save** .
8. On the **Provisioning** menu, press ▲ or ▼ to highlight **Login PW**, and then press ✓.
9. Enter the Login password.



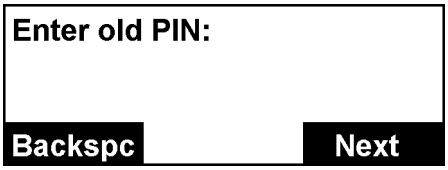
10. Press **Save** .

Editing the conference phone PIN code

The PIN code is a four-digit code that you use to deregister the conference phone from the base. The default PIN is **1590**.

To edit the PIN code:

1. From the Admin Settings menu, press ▼ to highlight **Edit PIN code**, and then press ✓.
   The **Enter old PIN** screen appears.

2. Enter the current PIN using the dial pad keys.
   - Press **Backspc** to delete a number.
3. Press **Next**.
4. Enter the new PIN, and then press **Next**.
5. Repeat entering the new PIN, and then press **Next**.

CHAPTER 3

USING THE WEBUI

The WebUI allows you to configure all aspects of C620 SIP Wireless Conference Phone operation, including account settings, soft keys, network settings, contact lists, and provisioning settings. The WebUI is embedded in the C620 operating system. When you access the WebUI, you are accessing it on the device, not on the Internet.

This chapter describes how to access the WebUI and configure C620 settings. This chapter covers:

- *"Using the Web User Interface (WebUI)" on page 36*
- *"Status Page" on page 39*
- *"System Pages" on page 41*
- *"Network Pages" on page 66*
- *"Contacts Pages" on page 72*
- *"Servicing Pages" on page 86*.

Using the Web User Interface (WebUI)

The Web User Interface (WebUI) resides on the C620 SIP Wireless Conference Phone's base station. You can access it using an Internet browser. After you log in to the WebUI, you can configure the C620 on the following pages:

System

- SIP Account Management (see *page 41*)
- Call Settings (see *page 55*)
- User Preferences (see *page 57*)
- Wireless Conference Phone (*page 58*)
- Server Application (see *page 61*)

Network

- Basic Network Settings (see *page 67*)
- Advanced Network Settings (see *page 69*)

Contacts

- Base Directory (see *page 72*)
- Blacklist (see *page 76*)
- LDAP (see *page 80*)
- Broadsoft (see *page 82*)
- Remote XML (see *page 84*)

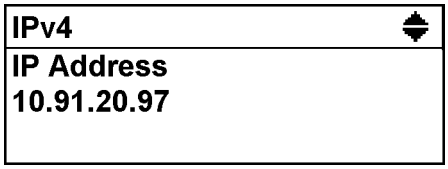
Servicing

- Reboot (see *page 86*)
- Time and Date (see *page 86*)
- Custom Language (see *page 89*)
- Firmware Upgrade (see *page 90*)
- Provisioning (see *page 94*)
- Security (see *page 100*)
- Certificates (see *page 103*)
- Tr069 (see *page 106*)
- System Logs (see *page 107*)

The WebUI also has a **System Status** and a **Device Status** page, where you can view network status and general information about the C620, wireless conference phone, wireless microphones, and expansion speaker. The information on the System Status page includes some of the same information as on the **Status** menu available on the conference phone.

To access the WebUI:

1. Ensure that your computer is connected to the same network as the C620.
2. Find the IP address of the C620:
   a. When the conference phone is idle, press .
   b. On the **Main Menu**, press ▼ to highlight **Status & Settings**, and then press .
   c. With **Status** highlighted, press .
   d. With **Network** highlighted, press .
   e. Press ▼ to highlight **IPv4** or **IPv6**, and then press .
   f. Press ▼ to scroll down the screen to display the IP address.



3. On your computer, open an Internet browser. (Depending on your browser, some of the pages presented here may look different and have different controls. Ensure that you are running the latest update of your preferred browser.)
4. Type the C620 IP address in the browser address bar and press **ENTER** on your computer keyboard.

   The browser displays a window asking for your user name and password.

   NOTE: If you have not yet changed the default administrator password and/or user password, you will be prompted to change the password(s) before you can use the WebUI functions.
5. Enter the username, and enter the password.
6. Click **OK**.

   The WebUI appears.

Click topics from the navigation bar along the top of the WebUI, and then click the links along the left to view individual pages. For your security, the WebUI times out after 10 minutes, so if it is idle for that time, you must log in again.

Most WebUI configuration pages have a Save button. Click Save to save changes you have made on the page. During a configuration session, click Save before you move on to the next WebUI page.

The remaining procedures in this chapter assume that you are already logged into the WebUI.

NOTE The settings tables in this section contain settings that appear in the WebUI and their equivalent settings in the configuration file template. You can use the configuration file template to create custom configuration files. Configuration files can be hosted on a provisioning server and used for automatically configuring phones. For more information, see *"Provisioning Using Configuration Files" on page 111*.

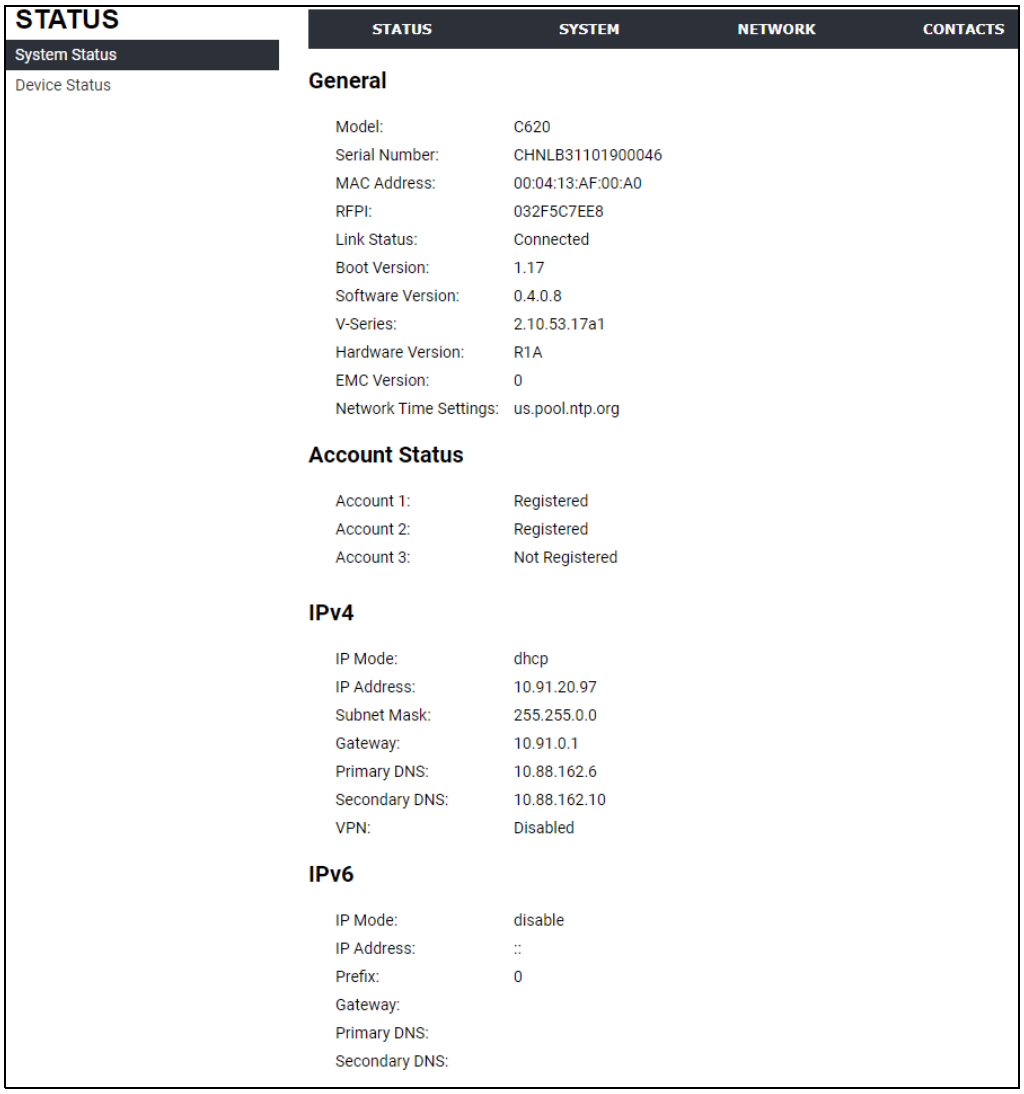
Status Page

On the Status pages, you can view network status and general information about the base station and conference phone. Some of the information on the Status pages is also available on the Status menu available on the conference phone.

System Status

The System Status page shows:

- **General** information about your device, including model, MAC address, and firmware version
- **Account Status** information about your SIP account registration
- **Network** information regarding your device's network address and network connection



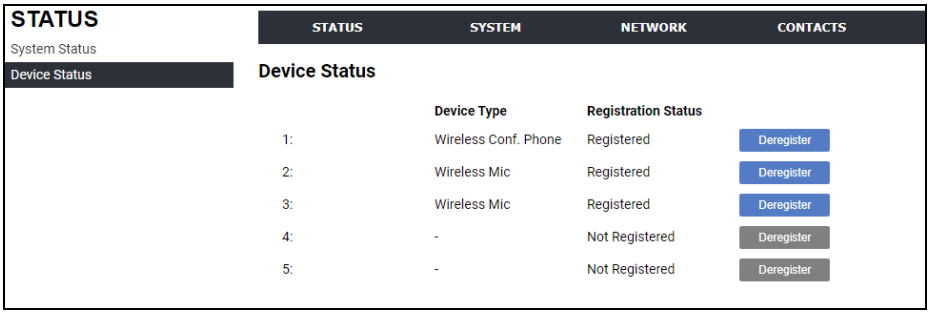
Device Status

The device status page shows the name and registration status of devices.

The devices that can be registered include:

- maximum of one conference phone
- up to two wireless microphones
- up to two C52-SP Expansion Speakerphones

The page lists the maximum of five devices, even if fewer devices are registered.



To deregister a device:

1. Click Deregister for the device you want to deregister.
2. Click OK at the confirmation prompt “Are you sure you want to deregister this device?”

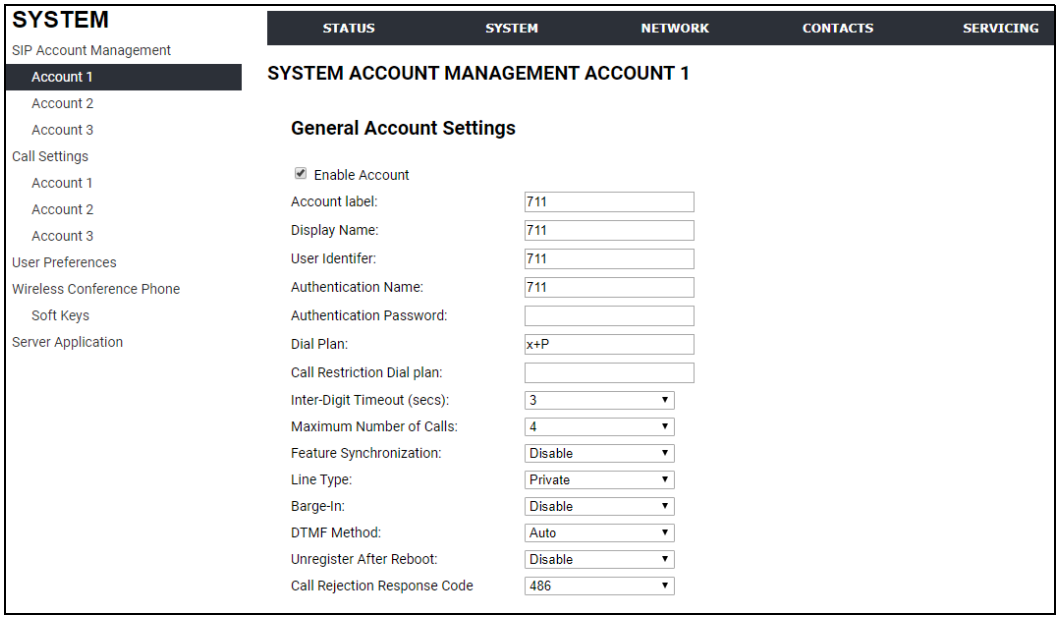
   After a few moments, the device is deregistered. It no longer appears on the Device Status page.

System Pages

SIP Account Management

On the SIP Account Management pages, you can configure each account you have ordered from your service provider.

The SIP Account settings are also available as parameters in the configuration file. See *""sip_account" Module: SIP Account Settings" on page 121*.



General Account Settings

In the tables on the following pages, click a setting to link to its matching configuration file parameter in Chapter 5, *Configuration File Parameter Guide*. Default values and ranges are listed there.

Setting	Description
Enable Account	Enable or disable the SIP account. Select to enable.
Account label	Enter the name that will appear on the conference phone display when account x is selected. The Account Label identifies the SIP account throughout the WebUI and on the handset Dialing Line menu.
Display Name	Enter the Display Name. The Display Name is the text portion of the caller ID that is displayed for outgoing calls using account x.

Setting	Description
User Identifier	Enter the User identifier supplied by your service provider. The User ID, also known as the Account ID, is a SIP URI field used for SIP registration. **Note**: Do not enter the host name (e.g. "@sipservice.com"). The WebUI automatically adds the default host name.
Authentication Name	If authentication is enabled on the server, enter the authentication name (or authentication ID) for authentication with the server.
Authentication Password	If authentication is enabled on the server, enter the authentication password for authentication with the server.
Dial Plan	Enter the dial plan, with dialing strings separated by a | symbol. See *"Dial Plan" on page 44*.
Call Restriction Dial plan	Used to restrict users from dialing out numbers through dial plan matching on a per-account basis.
Inter Digit Timeout (secs)	Sets how long the conference phone waits after any "P" (pause) in the dial string or in the dial plan.
Maximum Number of Calls	Select the maximum number of concurrent active calls allowed for that account.
Feature Synchronization	Enables the C620 to synchronize with BroadWorks Application Server. Changes to features such as DND, Call Forward All, Call Forward No Answer, and Call Forward Busy on the server side will also update the settings on the conference phone menu and WebUI. Similarly, changes made using the conference phone or WebUI will update the settings on the server.
Line Type	Select the line type to Private or Shared. A private line will be accessible only at the C620 you are configuring. Shared lines can be assigned to more than one SIP endpoint. For more information about using shared lines, see the C620 User Guide.
Barge-in	Not applicable.
DTMF method	Select the default DTMF transmission method. You may need to adjust this if call quality problems are triggering unwanted DTMF tones or you have problems sending DTMF tones in general.
Unregister after reboot	Enables the phone to unregister the account(s) after rebooting-before the account(s) register again as the phone starts up. If other phones that share the same account(s) unregister unexpectedly in tandem with the rebooting C620, disable this setting.

Setting	Description
Call Rejection Response Code	Select the response code for call rejection. This code applies to the following call rejection cases: ■ User presses **Reject** for an incoming call (except when Call Forward Busy is enabled) ■ DND is enabled ■ Phone rejects a second incoming call with Call Waiting disabled ■ Phone rejects an anonymous call with Anonymous Call Rejection enabled ■ Phone rejects call when the maximum number of calls is reached

Dial Plan

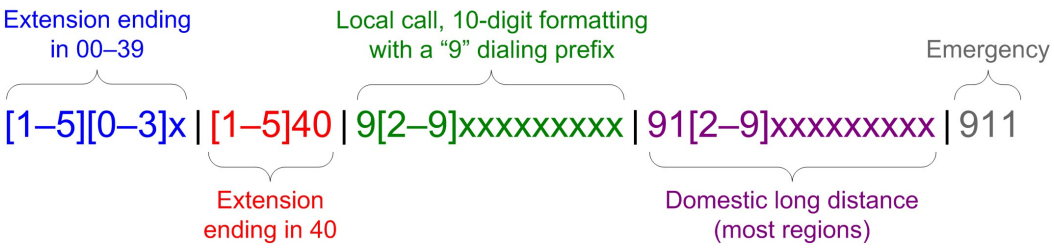
The dial plan consists of a series of dialing rules, or strings, that determine whether what the user has dialed is valid and when the conference phone should dial the number.

NOTE Numbers that are dialed when forwarding a call—when the user manually forwards a call, or a preconfigured number is dialed for Call Forward All, Call Forward–No Answer, or Call Forward Busy—always bypass the dial plan.

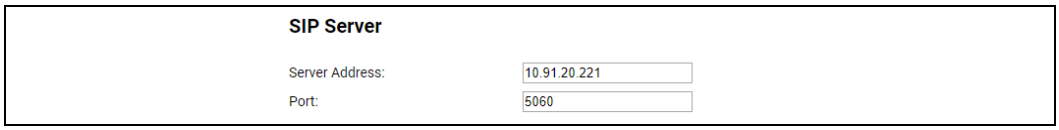
Dialing rules must consist of the elements defined in the table below.

Element	Description
x	Any dial pad key from 0 to 9, including # and *.
[0-9]	Any two numbers separated by a hyphen, where the second number is greater than the first. All numbers within the range or valid, excluding # and *.
x+	An unlimited series of digits.
,	This represents the playing of a secondary dial tone after the user enters the digit(s) specified or dials an external call prefix before the comma. For instance, "9,xxxxxxx" means the secondary dial tone is played after the user dials 9 until any new digit is entered. "9,3xxxxxx" means only when the digit 3 is hit would the secondary dial tone stop playing.
PX	This represents a pause of a defined time; X is the pause duration in seconds. For instance, "P3" would represent pause duration of 3 seconds. When "P" only is used, the pause time is the same as the Inter Digit Timeout (see *"SIP Account Management" on page 41*).
(0:9)	This is a substitution rule where the first number is replaced by the second. For example, "(4:723)xxxx" would replace "46789" with "723-6789". If the substituted number (the first number) is empty, the second number is added to the number dialed. For example, in "(:1)xxxxxxxxxx", the digit 1 is appended to any 10-digit number dialed.
|	This separator is used to indicate the start of a new pattern. Can be used to add multiple dialing rules to one pattern edit box.

A sample dial plan appears below.

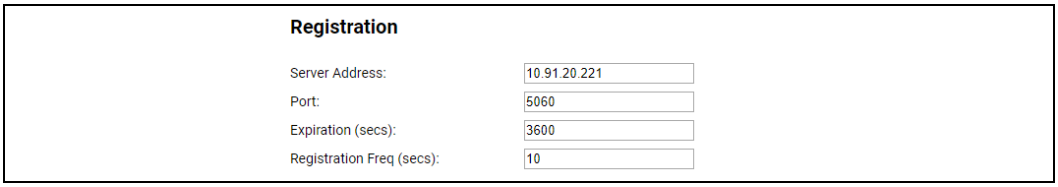


SIP Server Settings



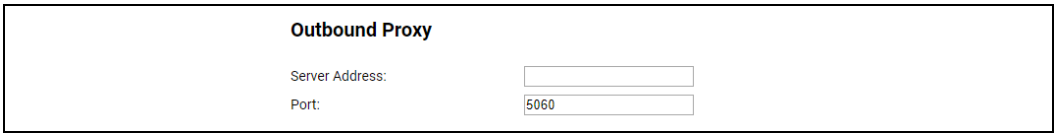
Setting	Description
Server address	Enter the IP address or domain name for the SIP server.
Port	Enter the port number that the SIP server will use.

Registration Settings



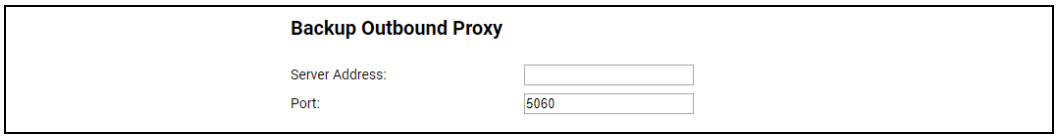
Setting	Description
Server address	Enter the IP address or domain name for the registrar server.
Port	Enter the port number that the registrar server will use.
Expiration (secs)	Enter the desired registration expiry time in seconds.
Registration Freq (secs)	Enter the desired registration retry frequency in seconds. If registration using the Primary Outbound Proxy fails, the Registration Freq setting determines the number of seconds before a registration attempt is made using the Backup Outbound Proxy.

Outbound Proxy Settings



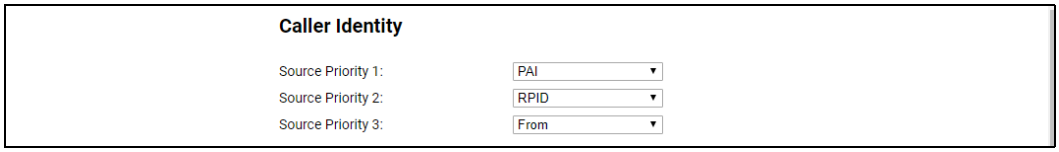
Setting	Description
Server Address	Enter the IP address or domain name for the proxy server.
Port	Enter the port number that the proxy server will use.

Backup Outbound Proxy Settings



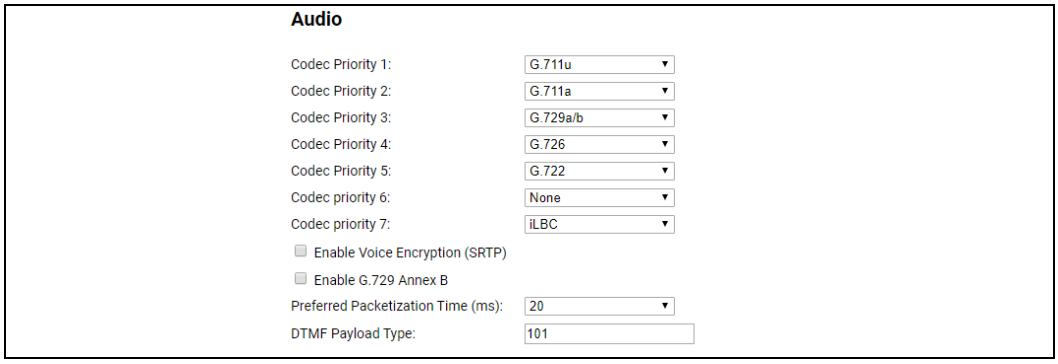
Setting	Description
Server address	Enter the IP address or domain name for the backup proxy server.
Port	Enter the port number that the backup proxy server will use.

Caller Identity Settings



Setting	Description
Source Priority 1	Select the desired caller ID source to be displayed on the incoming call screen: “From” field, RPID (Remote-Party ID) or PAI (P-Asserted Identity) header.
Source Priority 2	Select the lower-priority caller ID source.
Source Priority 3	Select the lowest-priority caller ID source.

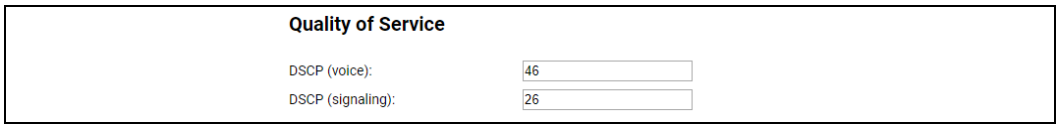
Audio Settings



Setting	Description
Codec priority 1	Select the codec to be used first during a call.
Codec priority 2	Select the codec to be used second during a call if the previous codec fails.

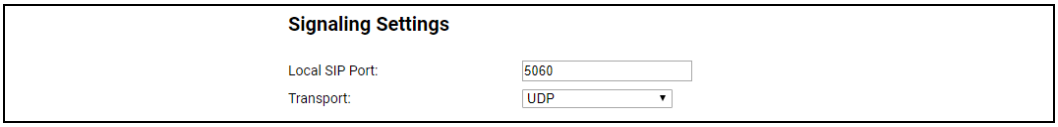
Setting	Description
Codec priority 3	Select the codec to be used third during a call if the previous codec fails.
Codec priority 4	Select the codec to be used fourth during a call if the previous codec fails.
Codec priority 5	Select the codec to be used fifth during a call if the previous codec fails.
Codec priority 6	Select the codec to be used sixth during a call if the previous codec fails.
Codec priority 7	Select the codec to be used seventh during a call if the previous codec fails.
Enable voice encryption (SRTP)	Select to enable secure RTP for voice packets.
Enable G.729 Annex B	When G.729a/b is enabled, select to enable G.729 Annex B, with voice activity detection (VAD) and bandwidth-conserving silence suppression.
Preferred Packetization Time (ms)	Select the packetization interval time.
DTMF Payload Type	Set the DTMF payload type for in-call DTMF from 96–127.

Quality of Service



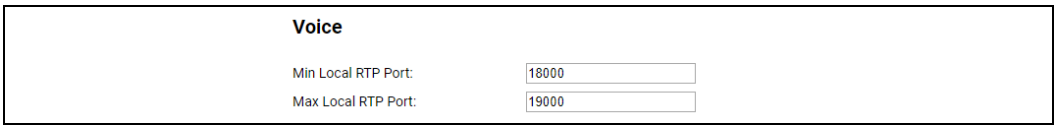
Setting	Description
DSCP (voice)	Enter the Differentiated Services Code Point (DSCP) value from the Quality of Service setting on your router or switch.
DSCP (signalling)	Enter the Differentiated Services Code Point (DSCP) value from the Quality of Service setting on your router or switch.

Signaling Settings



Setting	Description
Local SIP port	Enter the local SIP port.
Transport	Select the SIP transport protocol: ■ TCP (Transmission Control Protocol) is the most reliable protocol and includes error checking and delivery validation. ■ UDP (User Datagram Protocol) is generally less prone to latency, but SIP data may be subject to network congestion. ■ TLS (Transport Layer Security)—the C620 supports secured SIP signalling via TLS. Optional server authentication is supported via user-uploaded certificates. TLS certificates are uploaded using the configuration file. See *""file" Module: Imported File Settings" on page 173* and consult your service provider.

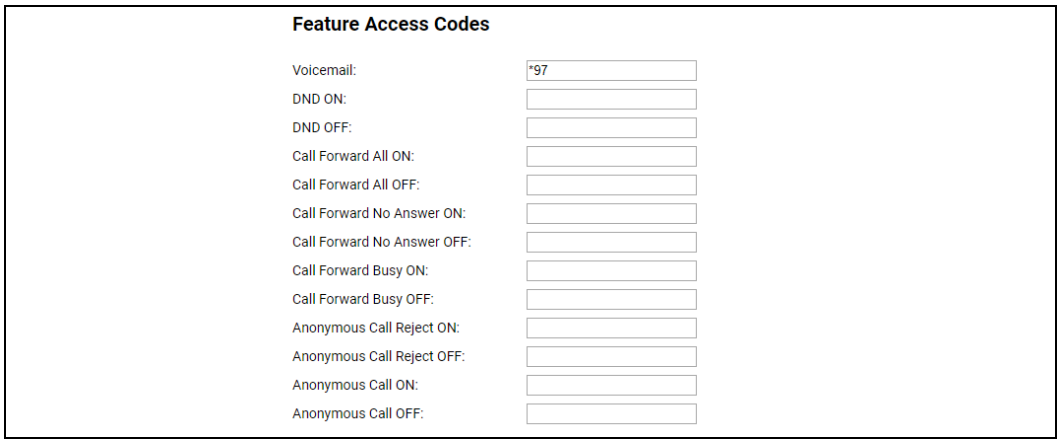
Voice Settings



Setting	Description
Min Local RTP Port	Enter the lower limit of the Real-time Transport Protocol (RTP) port range. RTP ports specify the minimum and maximum port values that the phone will use for RTP packets.
Max Local RTP Port	Enter the upper limit of the RTP port range.

Feature Access Codes Settings

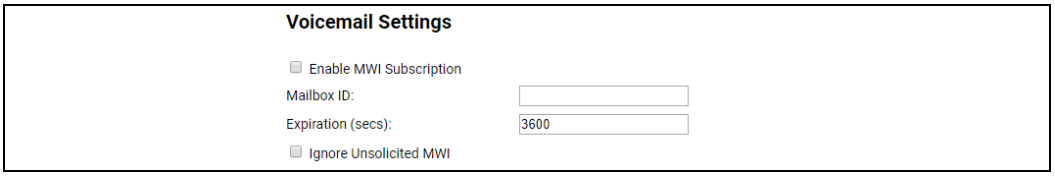
If your IP PBX service provider uses feature access codes, then enter the applicable codes here.



Setting	Description
Voicemail	Enter the voicemail access code. The code is dialed when the user selects a line from the Message menu.
DND ON	Enter the Do Not Disturb ON access code.
DND OFF	Enter the Do Not Disturb OFF access code.
Call Forward All ON	Enter the Call Forward All ON access code.
Call Forward All OFF	Enter the Call Forward All OFF access code.
Call Forward No Answer ON	Enter the Call Forward No Answer ON access code.
Call Forward No Answer OFF	Enter the Call Forward No Answer OFF access code.

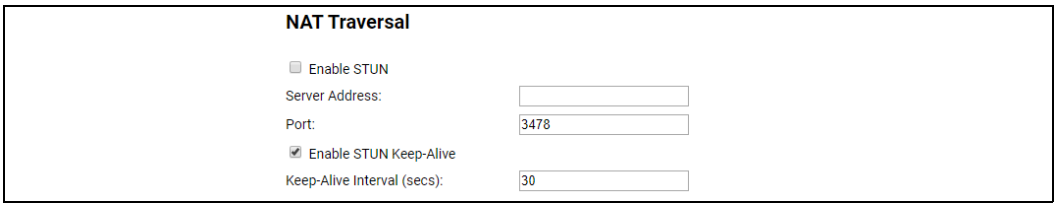
Setting	Description
Call Forward Busy ON	Enter the Call Forward Busy ON access code.
Call Forward Busy OFF	Enter the Call Forward Busy OFF access code.
Anonymous Call Reject ON	Enter the Anonymous Call Reject ON access code.
Anonymous Call Reject OFF	Enter the Anonymous Call Reject OFF access code.
Anonymous Call ON	Enter the Anonymous Call ON access code.
Anonymous Call OFF	Enter the Anonymous Call OFF access code.

Voicemail Settings



Setting	Description
Enable MWI Subscription	When enabled, the account subscribes to the "message summary" event package. The account may use the User ID or the service provider's "Mailbox ID".
Mailbox ID	Enter the URI for the mailbox ID. The phone uses this URI for the MWI subscription. If left blank, the User ID is used for the MWI subscription.
Expiration (secs)	Enter the MWI subscription expiry time (in seconds) for account x.
Ignore unsolicited MWI	When selected, unsolicited MWI notifications—notifications in addition to, or instead of SUBSCRIBE and NOTIFY methods—are ignored for account x. If the C620 receives unsolicited MWI notifications, the Message Waiting LED will not light to indicate new messages. Disable this setting if: ■ MWI service does not involve a subscription to a voicemail server. That is, the server supports unsolicited MWI notifications. ■ you want the Message Waiting LED to indicate new messages when the C620 receives unsolicited MWI notifications.

NAT Traversal



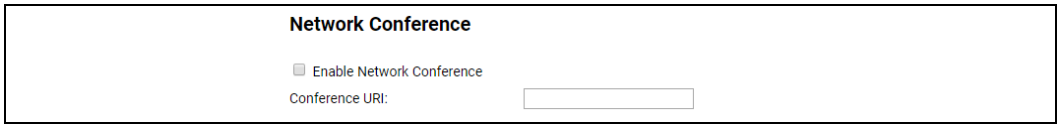
Setting	Description
Enable STUN	Enables or disables STUN (Simple Traversal of UDP through NATs) for account x. The Enable STUN setting allows the C620 to identify its publicly addressable information behind a NAT via communicating with a STUN server.

Setting	Description
Server Address	Enter the STUN server IP address or domain name.
Port	Enter the STUN server port.
Enable STUN Keep-Alive	Enables or disables UDP keep-alives. Keep-alive packets are used to maintain connections established through NAT.
Keep-Alive Interval (secs)	Enter the interval (in seconds) for sending UDP keep-alives.

Music on Hold Settings

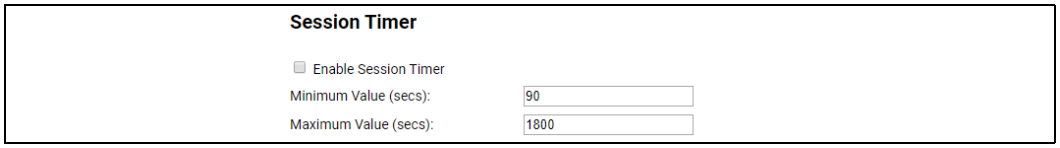
Setting	Description
Enable Local MoH	Enables or disables a hold-reminder tone that the user hears when a far-end caller puts the call on hold.

Network Conference Settings



Setting	Description
Enable Network Conference	Enables or disables network conferencing for account x.
Conference URI	Enter the URI for the network bridge for conference handling on account x.

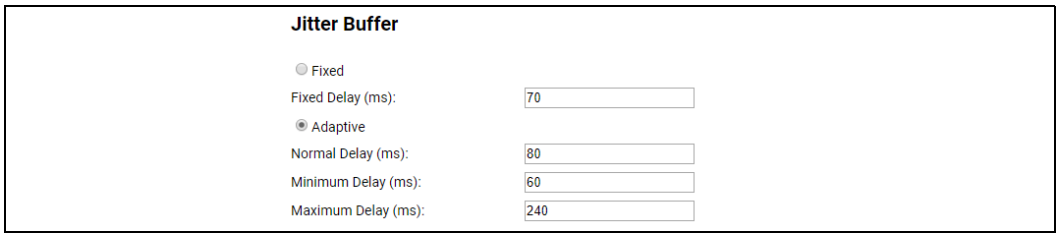
Session Timer



Setting	Description
Enable Session Timer	Enables or disables the SIP session timer. The session timer allows a periodic refreshing of a SIP session using the RE-INVITE message.

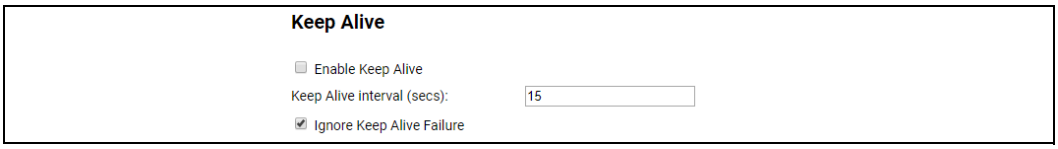
Setting	Description
Minimum Value (secs)	Sets the session timer minimum value (in seconds) for account x.
Maximum Value (secs)	Sets the session timer maximum value (in seconds) for account x.

Jitter Buffer



Setting	Description
Fixed	Enable fixed jitter buffer mode.
Fixed Delay (ms)	If Fixed is selected, enter the fixed jitter delay.
Adaptive	Enable adaptive jitter buffer mode.
Normal Delay (ms)	If Adaptive is selected, enter the normal or “target” delay.
Minimum Delay (ms)	Enter the minimum delay.
Maximum Delay (ms)	Enter the maximum delay. This time, in milliseconds, must be at least twice the minimum delay.

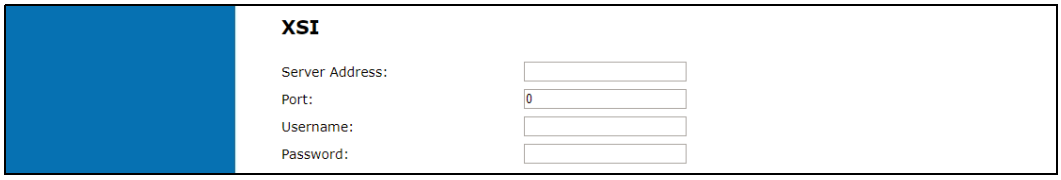
Keep Alive



Setting	Description
Enable Keep Alive	Enable SIP keep alive in service of NAT traversal and as a heartbeat mechanism to audit the SIP server health status. Once enabled, OPTIONS traffic should be sent whenever the account is registered. OPTIONS traffic will occur periodically according to the keep-alive interval.
Keep Alive interval (secs)	Set the interval at which the OPTIONS for the keep-alive mechanism are sent.

Setting	Description
Ignore Keep Alive Failure	Enable the phone to ignore keep-alive failure, if the failure can trigger account re-registration and re-subscription (and active calls are dropped).

XSI

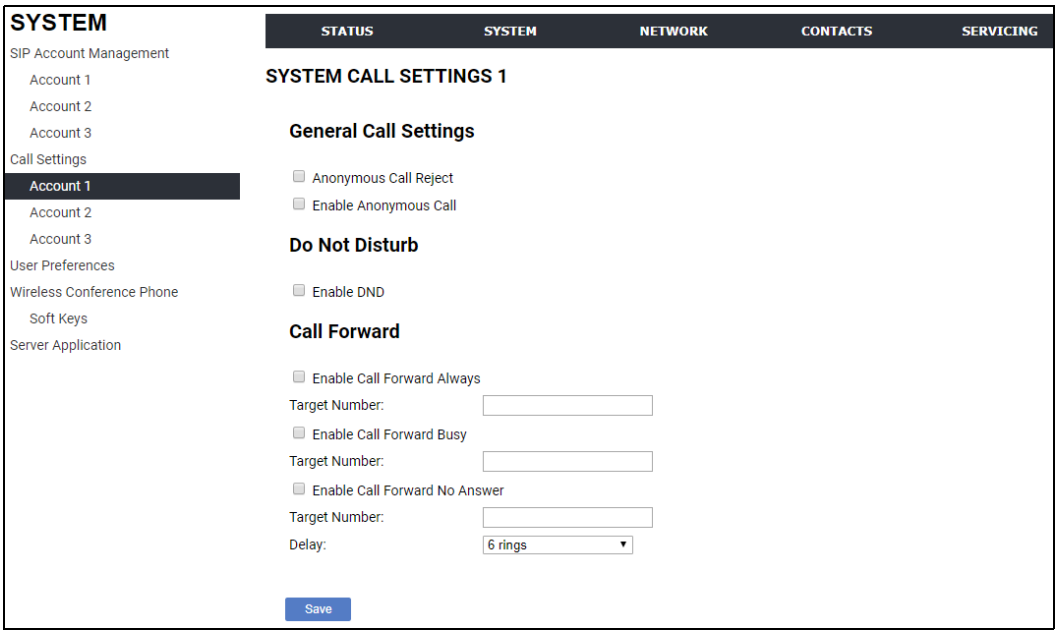


Setting	Description
Server Address	Specifies the Broadsoft XSI server.
Port	Specifies the port used for all XSI services.
Username	The Broadsoft XSI account name.
Password	The password of the Broadsoft XSI account.

Call Settings

You can configure call settings for each account. Call Settings include Do Not Disturb and Call Forward settings.

The call settings are also available as parameters in the configuration file. See *“"call_settings" Module: Call Settings” on page 169*.



General Call Settings

Setting	Description
Anonymous Call Reject	Enables or disables rejecting calls indicated as "Anonymous."
Enable Anonymous Call	Enables or disables outgoing anonymous calls. When enabled, the caller name and number are indicated as "Anonymous."

Do Not Disturb

Setting	Description
Enable DND	Turns Do Not Disturb on or off.

Call Forward

Setting	Description
Enable Call Forward Always	Enables or disables call forwarding for all calls on that line. Select to enable.
Target Number	Enter a number to which all calls will be forwarded.

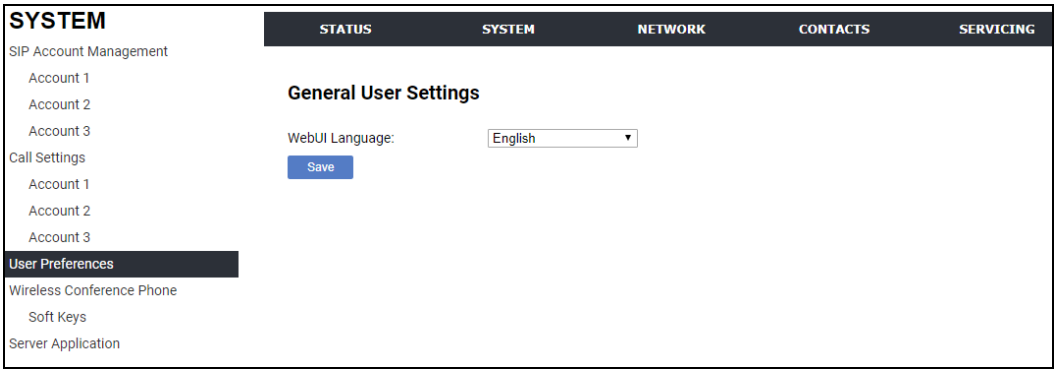
Setting	Description
Enable Call Forward Busy	Enables or disables forwarding incoming calls to the target number if: ■ the number of active calls has reached the maximum number of calls configured for account x ■ Call Waiting Off is selected.
Target Number	Enter a number to which calls will be forwarded when Call Forward Busy is enabled.
Enable Call Forward No Answer	Enables or disables call forwarding for unanswered calls on that line.
Target Number	Enter a number to which unanswered calls will be forwarded.
Delay	Select the number of rings before unanswered calls are forwarded.

User Preferences

On the User Preferences page, you can set the language that appears on the WebUI. The User Preferences page is also available to phone users when they log on to the WebUI.

The preference settings are also available as parameters in the configuration file. See *""user_pref" Module: User Preference Settings" on page 168*.

The WebUI Language setting is also available as a parameter in the configuration file. See *"**`user_pref.web_language`**" on page 168*.



General User Settings

In the table below, click a setting to link to its matching configuration file parameter in Chapter 5, *Configuration File Parameter Guide*. Default values and ranges are listed there.

Setting	Description
WebUI Language	Sets the language that appears on the WebUI.

Wireless Conference Phone

The Wireless Conference Phone settings enable you to configure soft keys for the conference phones that are registered to the base station.

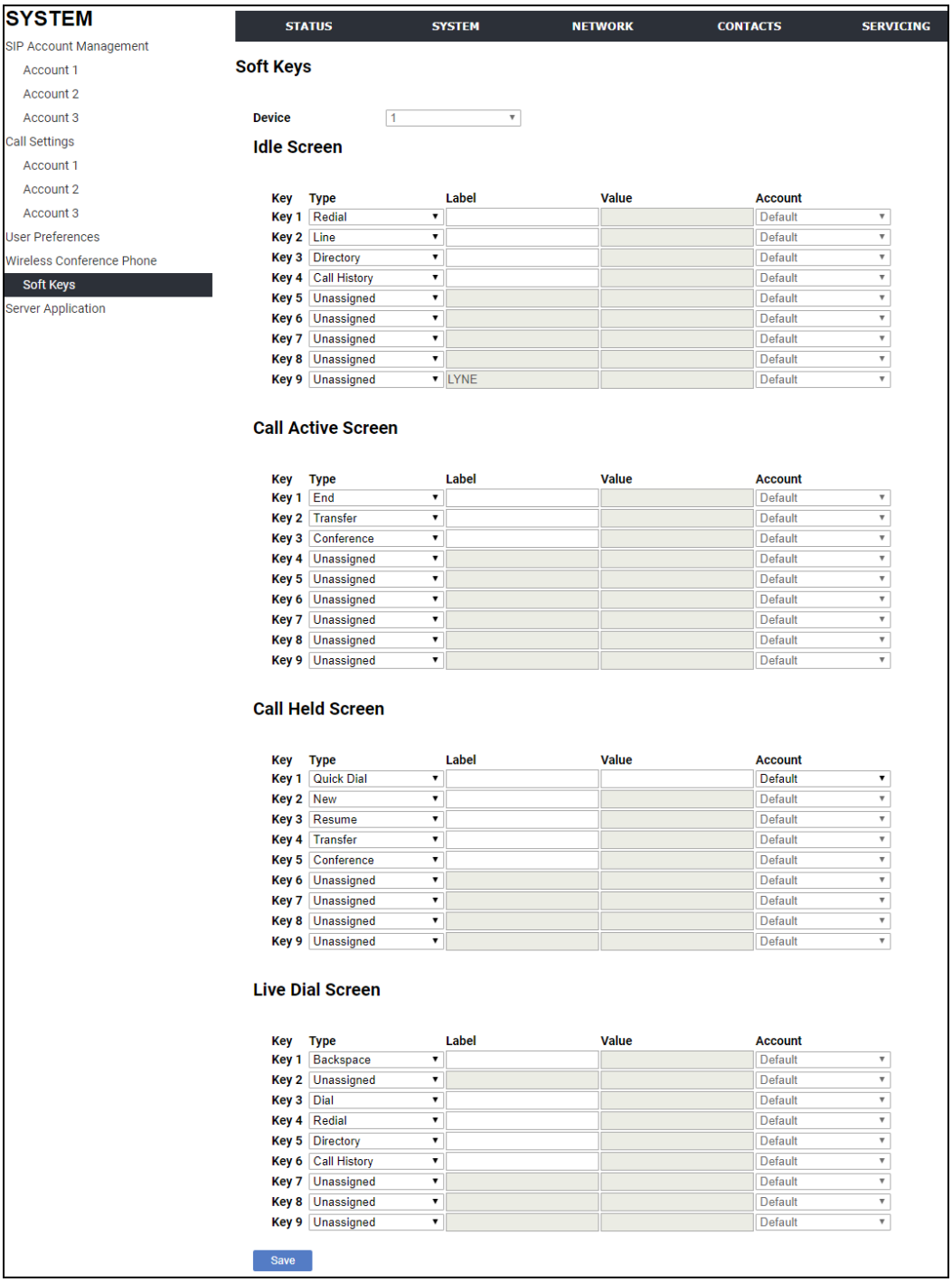
Soft Keys

On the Soft Keys page, you can select which soft keys can appear on the Idle screen, the Call Active screen, the Call Held screen and the Live Dial screen. You can also specify the position of each soft key.

Some soft keys appear only under certain conditions. For example, the Line soft key on the Idle screen appears only if there is more than one registered SIP account. When a "conditional" soft key is not visible, the soft key's position is left empty.

Soft key levels with no soft keys will not be shown if there are multiple soft key levels (as indicated by the ◀ and ▶ icons). Any soft key level where all soft keys are invisible will be dynamically skipped when the user navigates through the available levels. On the C620, a soft key level consists of three soft keys (populated or blank) in a row.

The soft key settings are also available as parameters in the configuration file.
See *""hs_settings" Module: Handset Settings" on page 136*



In the **Device** setting, select the device number of the conference phone.

The **Type** setting defines the function of the soft key. The following table lists the available selections for Type.

The **Label** setting defines the label text displayed for the soft key. If left blank, the soft key will display the default text for the specified **Type**.

The **Value** and **Account** fields are only applicable for certain **Type**s, as described in the following table.

Type

Setting	Description
Backspace	Configures the key to delete a character on the dial screen.
Call Forward	Configures the key to access the Call Forward menu.
Call Forward All	Configures the key to turn Call Forward All on or off. In the **Account** setting, select the desired account number for which Call Forward All will apply. Make sure to also configure Call Forward settings on the Call Settings page for the desired account.
Call Forward Busy	Configures the key to turn Call Forward Busy on or off. In the **Account** setting, select the desired account number for which Call Forward Busy will apply. Make sure to also configure Call Forward settings on the Call Settings page for the desired account.
Call Forward No Answer	Configures the key to turn Call Forward No Answer on or off. In the **Account** setting, select the desired account number for which Call Forward No Answer will apply. Make sure to also configure Call Forward settings on the Call Settings page for the desired account.
Call History	Configures the key to access the Call History menu.
Call Return	Configures the key to dial the number of the most recently missed call.
Cancel	Configures the key to cancel dialing and exit the live dial screen.
Conference	Configures the key to initiate a conference call.
Dial	Configures the key to dial the number entered on the dial screen.
Directory	Configures the key to access the Directory menu.
Do Not Disturb	Configures the key to turn Do Not Disturb on or off. In the **Account** setting, select the desired account number.
End	Configures the key to end the call.
Hold	Configures the key to put the call on hold.
Line	Configures the key for accessing a line. This soft key is only visible if more than one account is enabled on the C620.
Messages	Configures the key to access the Message menu. In the **Account** setting, select the desired account number.

Setting	Description
New	Configures the key to access the dialing screen for making a new call during a call.
Private Hold	Configures the key to put the call on private hold.
Quick Dial	Configures the key to dial the number specified in the **Value** setting. In the **Account** setting, select the desired account number.
Redial	Configures the key to access the Dialed Calls menu.
Resume	Configures the key to resume the held call.
Settings	Configures the key to access the User Settings menu.
Transfer	Configures the key to transfer the call.
Unassigned	Configures the key so it does not have a function. If you press the key, nothing will happen.

Server Application

On the Server Application page, you can enter Action URIs to allow the C620 to interact with a server application by using an HTTP GET request. The action URI triggers a GET request when a specified event occurs. Action URIs allow an external application to take control of the display when an event occurs. These predefined events are listed under “Action URI” on the Server Application page.

Action URIs are typically used in conjunction with the XML Browser, which can be customized to deliver an appropriate user experience.

The C620 supports both push and pull server applications. Note that Action URI events are not “push” events as it is the phone that requests a URI when triggered by certain states. You can enable push server applications under “XML Push Settings”.

Action URI Syntax

To access an XML application, the phone performs an HTTP GET on a URL.

An HTTP GET request may contain a variable name and variable value, which are separated by "=". Each variable value starts and ends with "$$" in the query part of the URL.

Action URI variables pass dynamic data to the server. The valid URL format is:
`http://host[:port]/dir/file name?variable name=$$variable value$$`

where:

- host is the hostname or IP address of the server supporting the XML application
- port is the port number the phones are using for the HTTP request

At the time of the HTTP call, the variable value field is populated with the appropriate data. For example, the following URL passes the SIP Account User Identifier to the server:
`http://10.50.10.140/script.pl?name=$$SIPUSERNAME$$`

A GET request then passes along the following information:
`http://10.50.10.140/script.pl?name=42512`

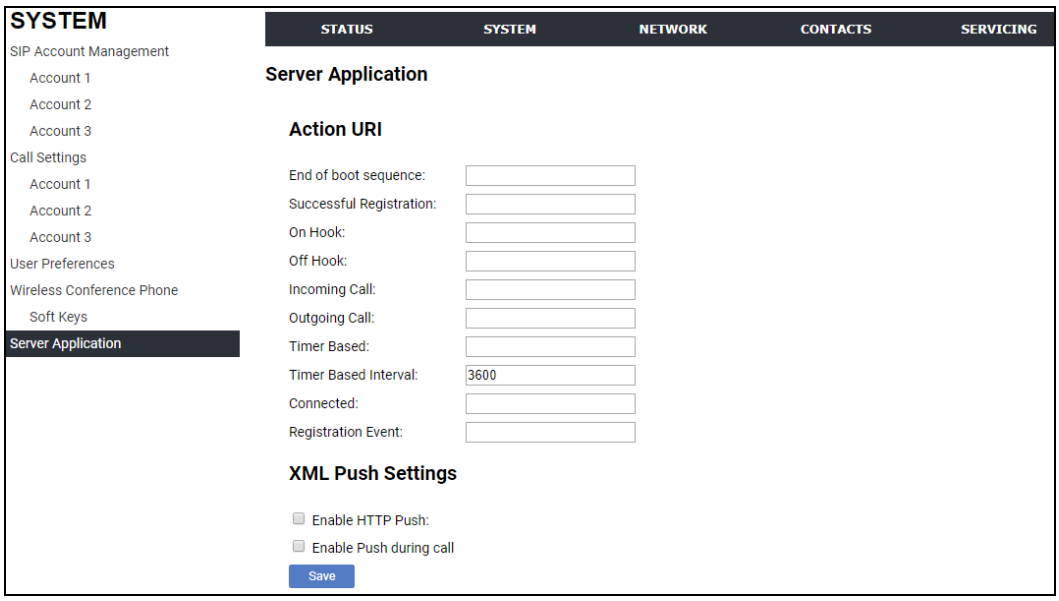
Assuming that the User Identifier is 42512.

Variable names are defined by the particular XML application being called.

Variable values are predefined and depend on the status of the phone. If the variable has no meaning in the current status, then the phone sends an empty string.

The table below lists all possible variable values. Note that variables applicable during an Incoming or Active Call (such as INCOMINGNAME and REMOTENUMBER) are initialized at the beginning and at the end of the call.

Variable value	Description
SIPUSERNAME	SIP Account User Identifier
DISPLAYNAME	SIP Account Display Name
LOCALIP	Phone's local IP Address
INCOMINGNAME	Caller ID name of the current Incoming Call
REMOTENUMBER	Remote party phone number (Incoming or Outgoing)
REGISTRATIONSTATE	Registration state available from the Registration event. Values are: ■ REGISTERED ■ DEREGISTERED ■ FAIL
MAC	The phone's MAC Address
MODEL	The phone's model number: C620.



Action URI

Setting	Description
End of boot sequence	The End of boot sequence URI is triggered at the end of the phone boot sequence. Using the End of boot sequence URI, it is possible to develop self-provisioning on the phone. For example, an XML application can identify the phone and generate a MAC-specific file on the fly.
Successful Registration	The Successful Registration URI is triggered the first time the phone registers successfully to a SIP Account. If the phone registers to multiple SIP Accounts, then the Successful Registration URI is triggered for each line.
On Hook	The On Hook URI is triggered when the phone transitions from Active to Idle (or from Paging to Idle). For example, when: ■ The user presses the **End** soft key ■ The user hangs up the handset during a call ■ A transfer is completed and the user returns to idle ■ The far end hangs up ■ The call was not answered ■ The call fails.

Setting	Description
Off Hook	The Off Hook URI is triggered when the user goes to Dial mode by: ■ Pressing the TALK/OFF hard key ■ Pressing the [New] soft key during a held call. Note that the Off Hook URI will NOT be triggered when calling a predefined number and going immediately to Dialling mode—this event triggers the Outgoing Call URI instead.
Incoming Call	The Incoming Call URI is triggered for each Incoming Ring event or Call Waiting event. Using the Incoming Call URI, it is possible to display extra information on the phone for an Incoming Call. For example, the XML application that is called when there is an Incoming Call can do a database lookup and display information on the caller. Note that this Action URI will not be triggered if DND or Call Forward All is enabled or if Call Waiting is disabled (i.e., the call is rejected).
Outgoing Call	The Outgoing Call URI is triggered each time a SIP INVITE message is sent (Dialling mode). For example, after: ■ Pressing the **Dial** key in Pre-Dial with populated number ■ Using the dial pad to speed dial a call ■ Dialling a Directory number by going off-hook.
Timer Based	The Timer Based URI will be triggered when the configured timeout expires. The timer starts at the end of the phone boot sequence.
Timer Based Interval	Enter the interval before the Timer Based URI is triggered.
Connected	The Connected URI is triggered each time the phone is in an Active Call or is Paging.
Registration Event	The Registration Event URI is triggered every time there is a registration state change. For example: ■ Registered ■ Deregistered ■ Fail (Registration timed out, refused, or expired) The Registration Event URI is not triggered when the same event is repeated.

XML Push Settings

Setting	Description
Enable HTTP Push	Select to enable HTTP push, which enables the phone to display XML objects that are “pushed” to the phone from the server via http/https POST or SIP NOTIFY.
Enable Push during call	Select to enable the phone to display pushed XML objects during a call. Otherwise, the XML application is displayed after the call is over.

Network Pages

You can set up the C620 for your network configuration on the Network pages. Your service provider may require you to configure your network to be compatible with its service, and the C620 settings must match the network settings.

The network settings are grouped into Basic and Advanced Settings. IPv4 and IPv6 protocols are supported.

When both IPv4 and IPv6 are enabled and available, the following guidelines apply when determining which stack to use:

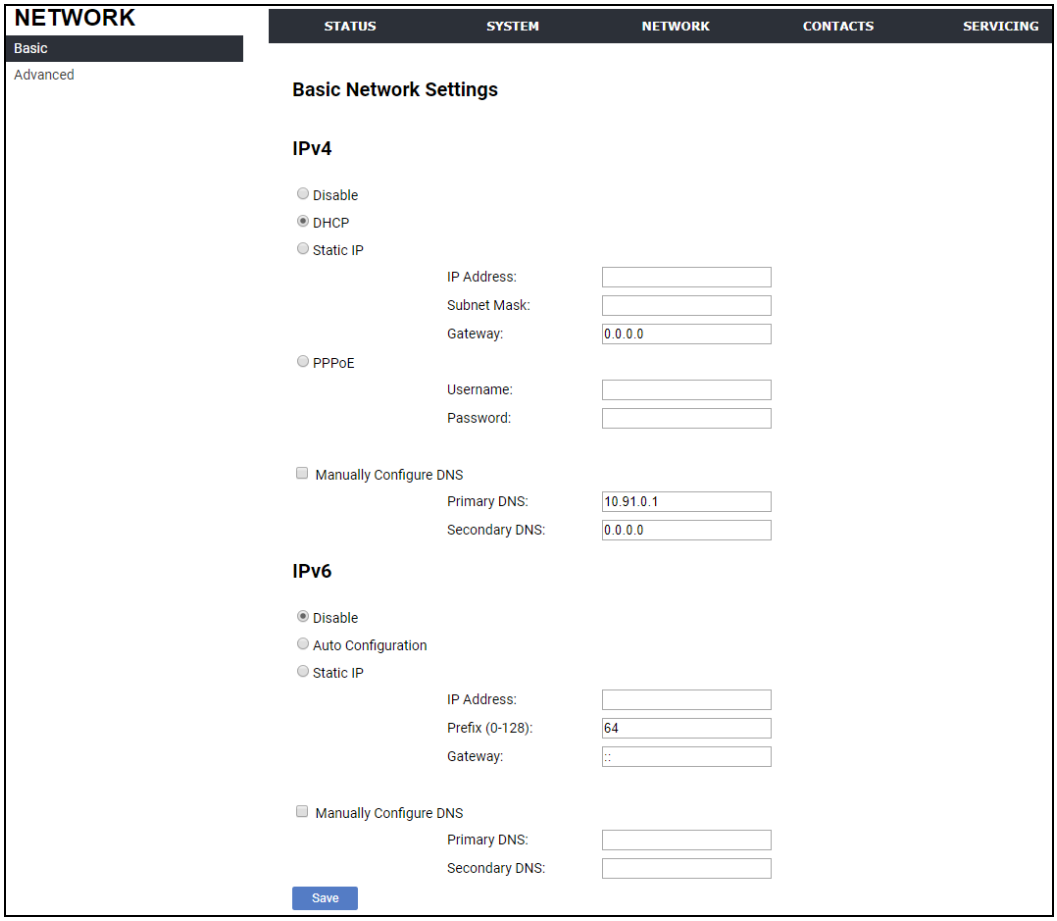
- For outgoing traffic, the IP address (or resolved IP) in the server field—either IPv4 or IPv6—will determine which stack to be used.
- DNS entries with both IPv4 and IPv6 settings can be used to resolve FQDN entries. There are no preferences with the order of the DNS queries.
- Pcap should include traffic for both stacks.
- Dual stack operations should be transparent to PC port traffic.

NOTE
- PnP is not supported on IPv6.
- VPN is not supported in IPv6 or PPPoE.

The network settings are also available as parameters in the configuration file. See *“"network" Module: Network Settings” on page 144*.

After entering information on this page, click Save to save it.

Basic Network Settings



NOTE You must be familiar with TCP/IP principles and protocols to configure static IP settings.

In the tables on the following pages, click a setting to link to its matching configuration file parameter in Chapter 5, *Configuration File Parameter Guide*. Default values and ranges are listed there.

IPv4

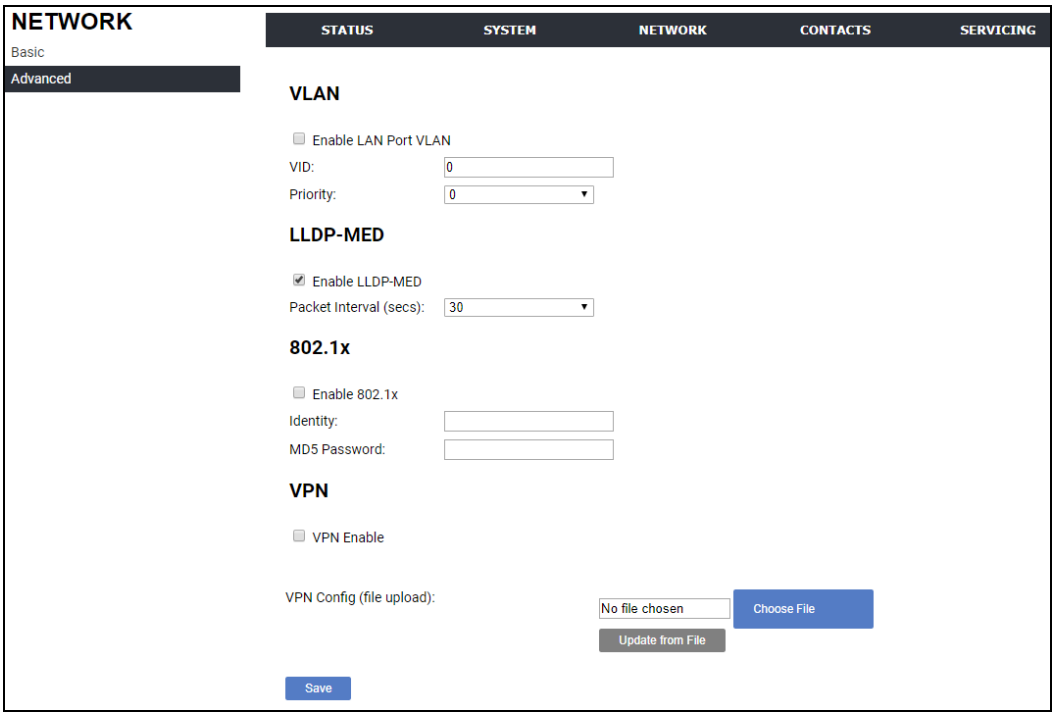
Setting	Description
Disable	Disables all related IPv4 settings.
DHCP	DHCP is selected (enabled) by default, which means the C620 will get its IP address, Subnet Mask, Gateway, and DNS Server(s) from the network. When DHCP is disabled, you must enter a static IP address for the C620, as well as addresses for the Subnet Mask, Gateway, and DNS Server(s).

Setting	Description
Static IP	When Static IP is selected, you must enter a static IP address for the C620, as well as addresses for the Subnet Mask, Gateway, and DNS Server(s).
IP Address	If DHCP is disabled, enter a static IP address for the C620.
Subnet Mask	Enter the subnet mask.
Gateway	Enter the address of the default gateway (in this case, your router).
PPPoE	Select to enable PPPoE (Point-to-Point Protocol over Ethernet) mode.
Username	Enter your PPPoE account username.
Password	Enter your PPPoE account password.
Manually Configure DNS	Select to enable manual DNS configuration.
Primary DNS	If DHCP is disabled, enter addresses for the primary and secondary DNS servers.
Secondary DNS	

IPv6

Setting	Description
Disable	Disables all related IPv6 settings.
Auto Configuration	Auto configuration is selected (enabled) by default, which means the C620 will get its IP address, Gateway, and DNS Server(s) from the network. When Auto Configuration is disabled, you must enter a static IP address for the C620, as well as addresses for the Gateway and DNS Server(s).
Static IP	When Static IP is selected, you must enter a static IP address for the C620, as well as an IPv6 address prefix, Gateway, and DNS Server(s).
IP Address	If Auto Configuration is disabled, enter a static IP address for the C620.
Prefix (0–128)	Enter the IPv6 address prefix length (0 to 128 bits).
Gateway	Enter the address of the default gateway (in this case, your router).
Manually Configure DNS	Select to enable manual DNS configuration.
Primary DNS	If Auto Configuration is disabled, enter addresses for the primary and secondary DNS servers.
Secondary DNS	

Advanced Network Settings



VLAN

You can organize your network and optimize VoIP performance by creating a virtual LAN for phones and related devices.

In the tables on the following pages, click a setting to link to its matching configuration file parameter in Chapter 5, *Configuration File Parameter Guide*. Default values and ranges are listed there.

Setting	Description
Enable LAN Port VLAN	Enable if the phone is part of a VLAN on your network. Select to enable.
VID	Enter the VLAN ID (vlan 5, for example).
Priority	Select the VLAN priority that matches the Quality of Service (QOS) settings that you have set for that VLAN ID. Outbound SIP packets from the LAN port (labeled “NET” on the C620) will be marked and sent according to their priority. 7 is the highest priority. **Note**: Configuring QOS settings for your router or switch is a subject outside the scope of this document.

LLDP-MED

Setting	Description
Enable LLDP-MED	Enables or disables Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED). LLDP-MED is a standards-based discovery protocol supported on some network switches. It is required for auto-configuration with VLAN settings.
Packet Interval (secs)	Sets the LLDP-MED packet interval (in seconds).

802.1x

Setting	Description
Enable 802.1x	Enables or disables the 802.1x authentication protocol. This protocol allows the phone to attach itself to network equipment that requires device authentication via 802.1x.
Identity	Enter the 802.1x EAPOL identity.
MD5 Password	Enter the 802.1x EAPOL MD5 password.

VPN

You can operate the C620 SIP Wireless Conference Phone over a Virtual Private Network (VPN). VPN enables remote users and remote sites to connect to a main corporate network and SIP server with a high level of performance and security.

Configuring VPN using the WebUI consists of enabling VPN and uploading a VPN configuration file. The VPN configuration file (**openvpn_client.tar**) must contain the following files:

- **client.conf**
- a **keys** folder containing
  - **ca.crt**
  - **client.crt**
  - **client.key**

The filename of the VPN client configuration file and certificates must match the names provided above. For more information about configuring VPN, visit our website at *www.snomamericas.com*.

NOTE Ensure that NTP or manual time is configured correctly so that the C620 is using the correct date and time before VPN setup. Mismatched time between sites and servers may invalidate the initial TLS handshake.

Setting	Description
VPN Enable	Enables or disables the phone to connect using the OpenVPN client. If VPN is enabled, but not connected, all SIP traffic will continue to route via the LAN IP. If VPN is enabled and connected, all SIP traffic will route via the VPN tunnel. The exception is the web server, which will still be accessible via the LAN IP.
VPN Config (file upload)	Browse to and upload the VPN configuration file **openvpn_client.tar**.

Contacts Pages

Base Directory

On the Base Directory page, you can manage directory entries that will be available on all conference phones. You can sort, edit, delete, and add contact information for up to 1,000 entries. In order to back up your contacts or import another local directory file, the page also enables you to export and import the base directory.

The Base Directory lists up to 20 entries per page. Click Next, Last, First, or a page number to view the desired page of entries.

NOTE The conference phone also has its own Local directory. You can add entries to the Local directory using the conference phone. For more information, see the C620 User Guide.

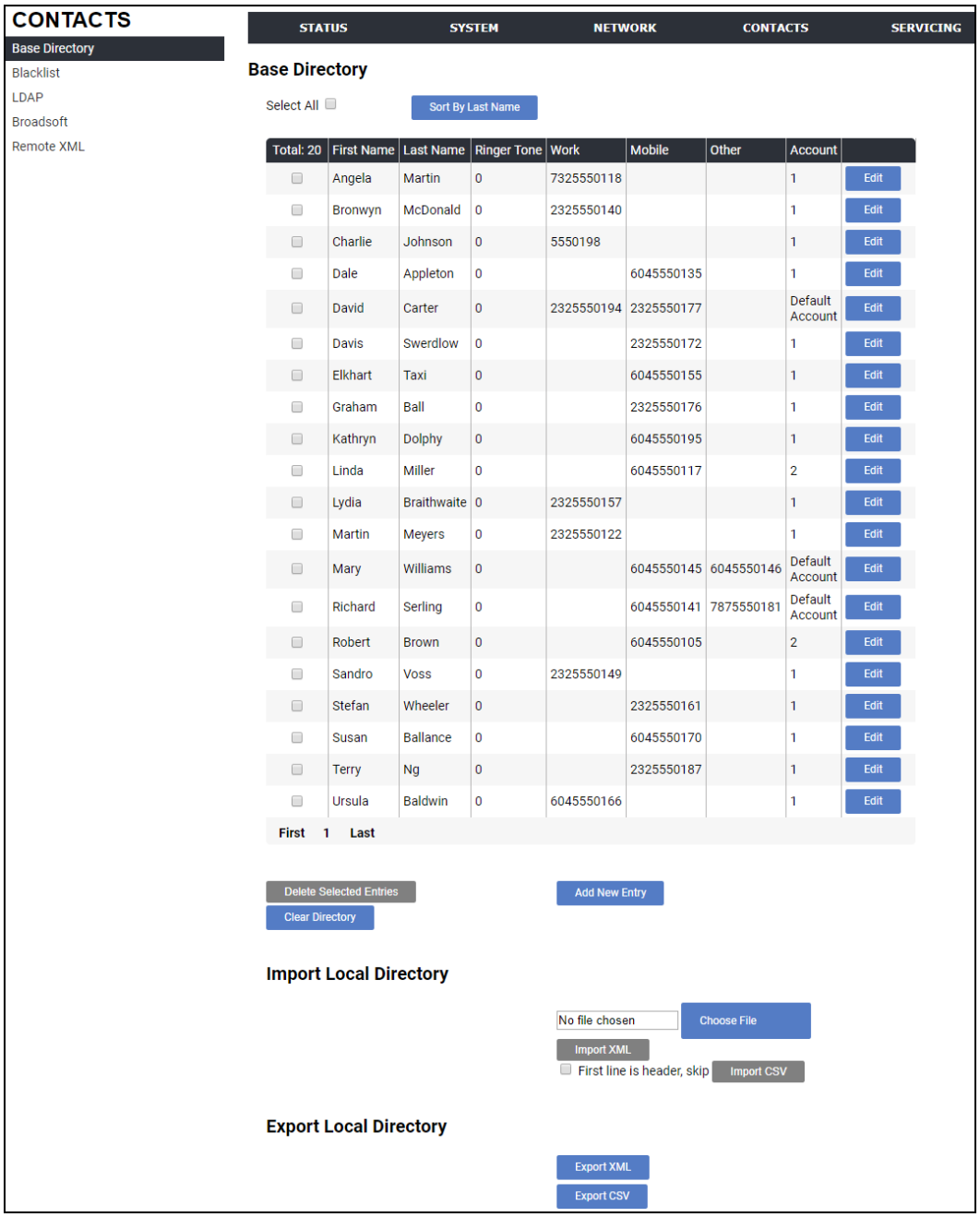


Table 6 describes the buttons available on the Base Directory page.

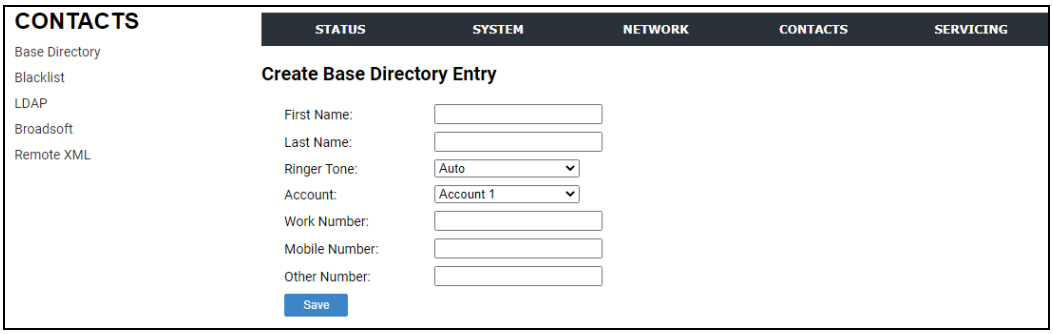
Table 6. Base Directory commands

Click	To...
Sort By Last Name	Sort the list by last name
Sort By First Name	Sort the list by first name

Click	To...
Edit	Edit information for an entry
Next	View the next page of entries
Last	View the last page of entries
First	View the first page of entries
Delete Selected Entries	Delete selected entries from the directory. Click **Select All** to select every entry on the page you are viewing.
Add New Entry	Add a new directory entry
Clear Directory	Delete all Directory entries
Choose File	Choose a directory file to import
Import XML Import CSV	Import a directory file in XML or CSV format
Export XML Export CSV	Export the directory in XML or CSV format

To add a new directory entry:

1. Click Add New Entry .
   The **Create Base Directory Entry** page appears.



2. Enter the required information as described in the following table.

Create Base Directory Entry

Setting	Description	Range	Default
First Name	Enter the appropriate names in these fields. The maximum length of the first name and last name fields is 15 characters.	n/a	Blank
Last Name			
Ringer Tone	Sets a unique ringer tone for calls from this directory entry.	Auto, Tone 1–10	Tone 1
Account	Sets the account used when you dial this directory entry.	Default Account, Account 1–3	Default Account
Work	Enter the appropriate telephone numbers in these fields.	n/a	Blank
Mobile			
Other			

Directory Import/Export

For a brand new C620 conference phone out of the box, the Base Directory will be empty. The best way to create an import file of directory entries is to first add a new entry to be used as a placeholder. Then export the Base Directory in either CSV or XML format. Open the file in a CSV or XML editor, and then add or modify entries. When you are finished editing, import the file to the Base Directory.

Importing a directory file adds the imported directory entries to existing entries. Therefore, it is possible to have duplicate entries after importing a directory file. If you are importing a "complete" directory file with the aim of replacing the entire current directory, select the **Select All** checkbox and click Delete Selected Entries to clear the directory before importing the file.

NOTE You can also import a directory file via provisioning. With provisioning, you can control whether the imported directory file adds to or replaces existing Base Directory entries. In the provisioning configuration file, enter the URI of the imported directory file in one of the following parameters:

- *"file.contact.directory.append" on page 175* – adds to existing entries
- *"file.contact.directory.overwrite" on page 175* – replaces existing entries

Directory files in XML format have the following tags:

Base Directory WebUI field	Directory file XML tag
First Name	<DIR_ENTRY_NAME_FIRST>
Last Name	<DIR_ENTRY_NAME_LAST>

Base Directory WebUI field	Directory file XML tag
Work Number	<DIR_ENTRY_NUMBER_WORK>
Mobile Number	<DIR_ENTRY_NUMBER_MOBILE>
Other Number	<DIR_ENTRY_NUMBER_OTHER>
Account	<DIR_ENTRY_LINE_NUMBER>
Call Block (not on WebUI)	<DIR_ENTRY_BLOCK>
Ringer Tone	<DIR_ENTRY_RINGER>

Blacklist

On the Blacklist page, you can manage local blacklist entries. The C620 rejects calls from numbers that match blacklist entries. You can sort, edit, delete, and add up to 200 blacklist entries. In order to back up your blacklist entries or import another local blacklist file, the page also enables you to export and import the blacklist.

The blacklist displays entries on up to 10 pages, with 20 entries per page. Click Next , Last , First , or a page number to view the desired page of entries.

NOTE
You can also use the C620 menu to manage blacklist entries.
For more information, see the C620 User Guide.

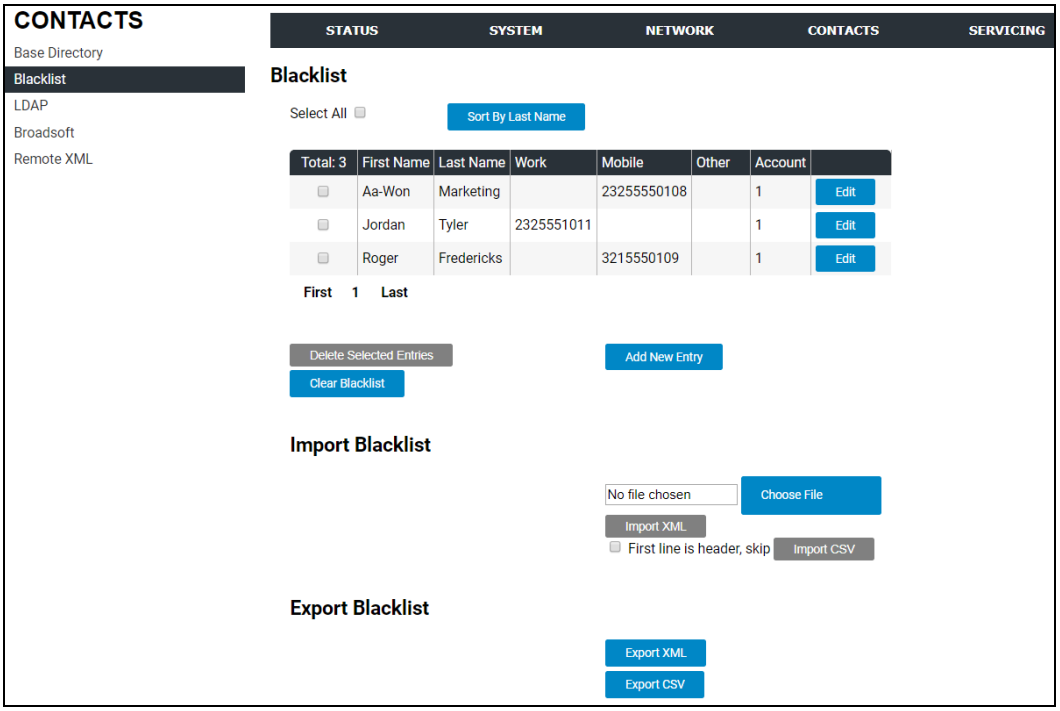


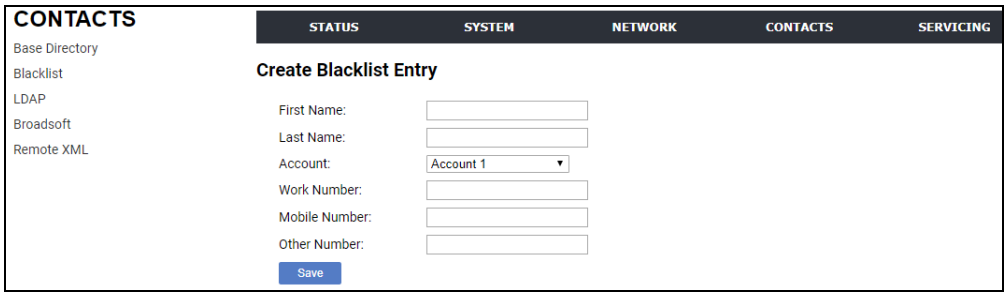
Table 7 describes the buttons available on the Blacklist page.

Table 7. Blacklist commands

Click	To...
Sort By Last Name	Sort the list by last name
Sort By First Name	Sort the list by first name
Edit	Edit information for an entry
Next	View the next page of entries
Last	View the last page of entries
First	View the first page of entries
Delete Selected Entries	Delete selected entries. Click **Select All** to select every entry on the page you are viewing.
Add New Entry	Add a new entry
Clear Directory	Delete all entries
Choose File	Choose a blacklist file to import
Import XML Import CSV	Import a blacklist file in XML or CSV format
Export XML Export CSV	Export the blacklist file in XML or CSV format

To add a new blacklist entry:

1. Click Add New Entry .
   The **Create Blacklist Entry** page appears.



2. Enter the required information as described in the following table.

Create Blacklist Entry

Setting	Description	Range	Default
First Name	Enter the appropriate names in these fields. The maximum length of the first name and last name fields is 15 characters.	n/a	Blank
Last Name			
Account	Sets the account used when you dial this directory entry.	Default Account, Account 1–3	Account 1
Work	Enter the appropriate telephone numbers in these fields.	n/a	Blank
Mobile			
Other			

Blacklist Import/Export

For a brand new C620 conference phone out of the box, the Blacklist will be empty. The best way to create an import file of blacklist entries is to first add a new entry to be used as a placeholder. Then export the Blacklist in either CSV or XML format. Open the file in a CSV or XML editor, and then add or modify entries. When you are finished editing, import the file to the Blacklist.

Importing a blacklist file adds the imported blacklist entries to existing entries. Therefore, it is possible to have duplicate entries after importing a blacklist file. If you are importing a "complete" blacklist file with the aim of replacing the entire current blacklist, select the **Select All** checkbox and click Delete Selected Entries to clear the blacklist before importing the file.

NOTE You can also import a blocked list file via provisioning. With provisioning, you can control whether the imported blocked list file adds to or replaces existing Blocked List entries. In the provisioning configuration file, enter the URI of the imported blocked list file in one of the following parameters:

- *"file.contact.blacklist.append" on page 175* – adds to existing entries
- *"file.contact.blacklist.overwrite" on page 176* – replaces existing entries

Blacklist files in XML format have the following tags:

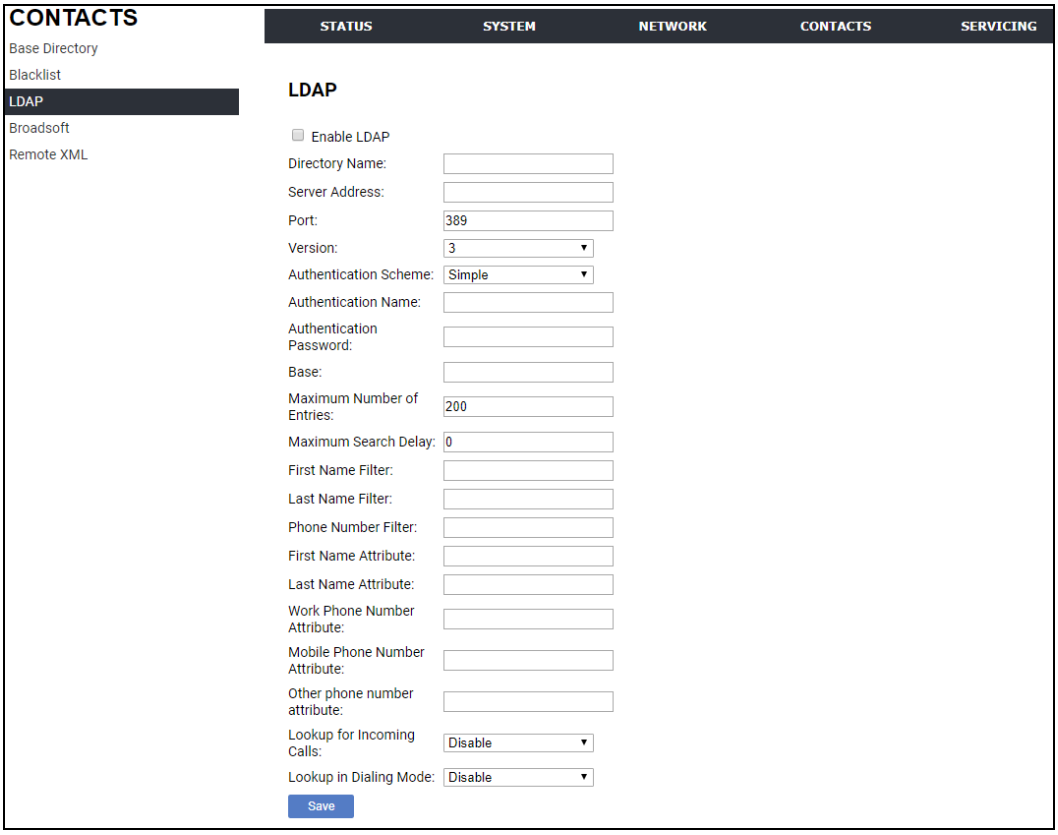
Blacklist WebUI field	Blacklist file XML tag
First Name	<BLACKLIST_ENTRY_NAME_FIRST>
Last Name	<BLACKLIST_ENTRY_NAME_LAST>
Work Number	<BLACKLIST_ENTRY_NUMBER_WORK>
Mobile Number	<BLACKLIST_ENTRY_NUMBER_MOBILE>
Other Number	<BLACKLIST_ENTRY_NUMBER_OTHER>
Account	<BLACKLIST_ENTRY_LINE_NUMBER>

LDAP

The phone supports remote Lightweight Directory Access Protocol (LDAP) directories. An LDAP directory is hosted on a remote server and may be the central directory for a large organization spread across several cities, offices, and departments. You can configure the phone to access the directory and allow users to search the directory for names and telephone numbers.

The LDAP settings are also available as parameters in the configuration file.
See *""remoteDir" Module: Remote Directory Settings" on page 160*.

After entering information on this page, click Save to save it.



LDAP Settings

In the tables on the following pages, click a setting to link to its matching configuration file parameter in Chapter 5, *Configuration File Parameter Guide*. Default values and ranges are listed there.

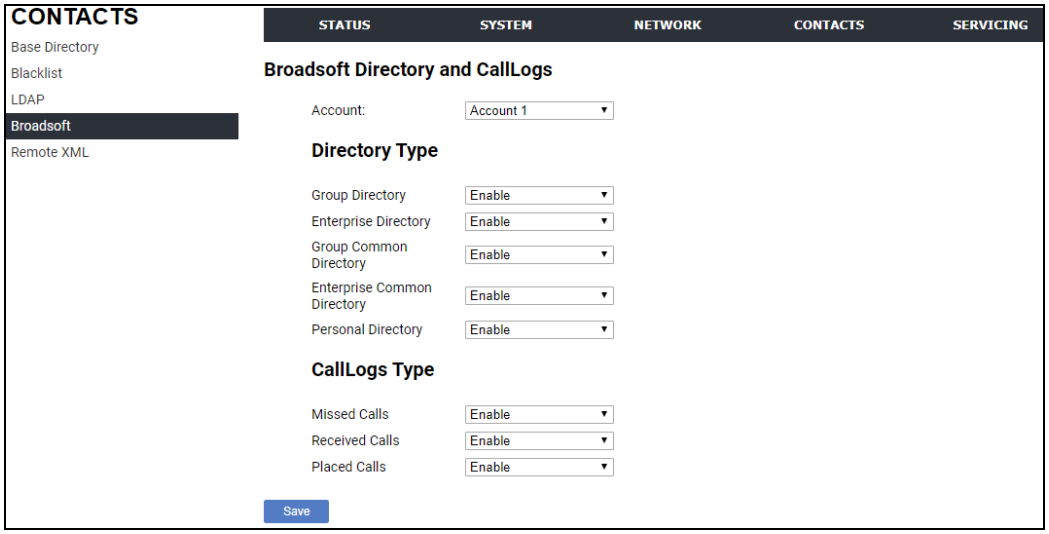
Setting	Description
Enable LDAP	Enables or disables the phone's access to the LDAP directory.
Directory Name	Enter the LDAP directory name.

Setting	Description
Server Address	Enter the LDAP server domain name or IP address.
Port	Enter the LDAP server port.
Version	Select the LDAP protocol version supported on the phone. Ensure the protocol value matches the version assigned on the LDAP server.
Authentication Scheme	Select the LDAP server authentication scheme.
Authentication Name	Enter the user name or authentication name for LDAP server access.
Authentication Password	Enter the authentication password for LDAP server access.
Base	Enter the LDAP search base. This sets where the search begins in the directory tree structure. Enter one of more attribute definitions, separated by commas (no spaces). Your directory may include attributes like "cn" (common name) or "ou" (organizational unit) or "dc" (domain component). For example: ou=accounting,dc=snom,dc=com
Maximum Number of Entries	Sets the maximum number of entries returned for an LDAP search. Limiting the number of hits can conserve network bandwidth.
Maximum Search Delay	Enter the delay (in seconds) before the phone starts returning search results.
First Name Filter	Enter the first name attributes for LDAP searching. The format of the search filter is compliant to the standard string representations of LDAP search filters (RFC 2254).
Last Name Filter	Enter the last name attributes for LDAP searching. The format of the search filter is compliant to the standard string representations of LDAP search filters (RFC 2254).
Phone Number Filter	Enter the number attributes for LDAP searching. The format of the search filter is compliant to the standard string representations of LDAP search filters (RFC 2254).
First Name Attribute	Sets the attribute for first name. What you enter here should match the first name attribute for entries on the LDAP server (gn for givenName, for example). This helps ensure that the phone displays LDAP entries in the same format as the Base Directory.
Last Name Attribute	Sets the attribute for last name. What you enter here should match the last name attribute for entries on the LDAP server (sn for surname, for example). This helps ensure that the phone displays LDAP entries in the same format as the Base Directory.

Setting	Description
Work Phone Number Attribute	Sets the attribute for the work number. What you enter here should match the work number attribute for entries on the LDAP server (telephoneNumber, for example). This helps ensure that the phone displays LDAP entries in the same format as the Base Directory.
Mobile Phone Number Attribute	Sets the attribute for the mobile number. What you enter here should match the mobile number attribute for entries on the LDAP server (mobile, for example). This helps ensure that the phone displays LDAP entries in the same format as the Base Directory.
Other phone number attribute	Sets the attribute for the other number. What you enter here should match the other number attribute for entries on the LDAP server (otherPhone, for example). This helps ensure that the phone displays LDAP entries in the same format as the Base Directory.
Lookup for Incoming Calls	Enables or disables LDAP incoming call lookup. If enabled, the phone searches the LDAP directory for the incoming call number. If the number is found, the phone uses the LDAP entry for CID info.
Lookup in Dialing Mode	Enables or disables LDAP outgoing call lookup. If enabled, numbers entered in predial or live dial are matched against LDAP entries. If a match is found, the LDAP entry is displayed for dialing.

Broadsoft Directory and CallLogs

The C620 supports the display of Broadsoft directories and call logs.



Setting	Description
Account	Select the desired account number.

Directory Type

Setting	Description
Group Directory	Enables or disables the display of the Broadsoft Group Directory on the phone for the specified account.
Enterprise Directory	Enables or disables the display of the Broadsoft Enterprise Directory on the phone for the specified account.
Group Common Directory	Enables or disables the display of the Broadsoft Group Common Directory on the phone for the specified account.
Enterprise Common Directory	Enables or disables the display of the Broadsoft Enterprise Common Directory on the phone for the specified account.
Personal Directory	Enables or disables the display of the Broadsoft Personal Directory on the phone for the specified account.

CallLogs Type

Setting	Description
Missed Calls	Enables or disables the display of Missed Calls.
Received Calls	Enables or disables the display of Received Calls.
Placed Calls	Enables or disables the display of Placed Calls.

Remote XML

The C620 supports three server-hosted Remote XML directories, with a maximum of 5,000 entries shared across the three directories.

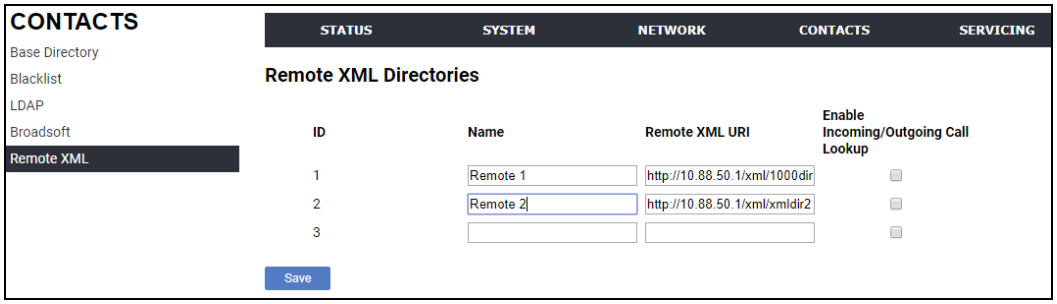
When the user selects a remote directory to view, the C620 will sync with the directory server. The conference phone will display **Sync failed** if any of the following failing conditions is encountered:

- Server not reachable
- Remote XML directory file is not available
- Invalid XML directory file

Remote XML Directory Format

The following shows a sample single-entry file which can be used in a remote XML directory. Note that the default tags are the same as those defined for the Local Directory.

```
<?xml version="1.0" encoding="utf-8"?>

<DIR_ENTRY>

<DIR_ENTRY_NAME_FIRST>John</DIR_ENTRY_NAME_FIRST>

<DIR_ENTRY_NAME_LAST>Smith</DIR_ENTRY_NAME_LAST>

<DIR_ENTRY_NUMBER_OTHER>3333</DIR_ENTRY_NUMBER_OTHER>

<DIR_ENTRY_NUMBER_WORK>1111</DIR_ENTRY_NUMBER_WORK>

<DIR_ENTRY_NUMBER_MOBILE>2222</DIR_ENTRY_NUMBER_MOBILE>

</DIR_ENTRY>
```



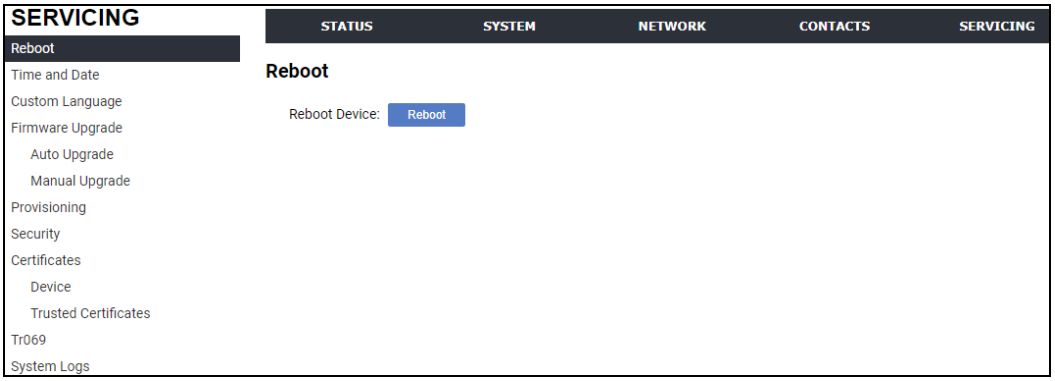
In the tables on the following pages, click a setting to link to its matching configuration file parameter in Chapter 5, *Configuration File Parameter Guide*. Default values and ranges are listed there.

Setting	Description
Name	Sets the name of the directory as it will appear on the C620 Directory list. The following order applies to the Directory list when multiple server-based directories are enabled: 1. Local 2. Blacklist 3. LDAP 4. Broadsoft 5. Remote XML directory 1 6. Remote XML directory 2 7. Remote XML directory 3 Any Remote XML directories will move up the list if LDAP and/or Broadsoft directories are not enabled.
Remote XML URI	Enter the location of the XML directory file, from which the phone will sync and retrieve directory entries.
Enable Incoming/ Outgoing Call Lookup	Enables/disables the call lookup feature for incoming and outgoing calls.

Servicing Pages

Reboot

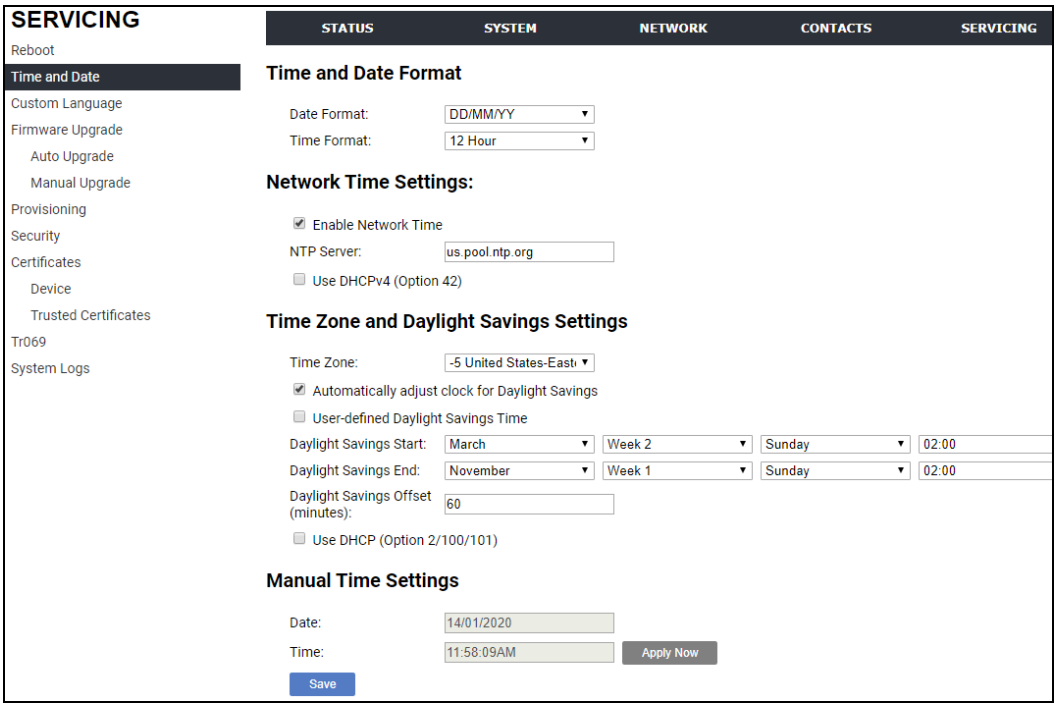
To manually reboot the C620 conference phone and apply settings that you have updated, click Reboot .



Time and Date

On the Time and Date page, you can manually set the time and date, and the time and date formats. You can also set the system time to follow a Network Time Protocol (NTP) Server (recommended) or you can set the time and date manually.

The time and date settings are also available as parameters in the configuration file. See *""time_date" Module: Time and Date Settings" on page 154*.



Time and Date Format

In the tables on the following pages, click a setting to link to the matching configuration file parameter in Chapter 5, *Configuration File Parameter Guide*. Default values and ranges are listed there.

Setting	Description
Date Format	Sets the date format.
Time Format	Sets the clock to a 24-hour or 12-hour format.

Network Time Settings

Setting	Description
Enable Network Time	Enables or disables getting time and date information for your phone from the Internet.
NTP Server	If Enable Network Time is selected, enter the URL of your preferred time server.
Use DHCPv4 (Option 42)	If Enable Network Time is selected, select to use DHCP to locate the time server. Option 42 specifies the NTP server available to the phone. When enabled, the phone obtains the time in the following priority: 1. Option 42 2. NTP Server 3. Manual time.

Time Zone and Daylight Savings Settings

Setting	Description
Time Zone	Select your time zone from the list.
Automatically adjust clock for Daylight Savings	Select to adjust the clock for daylight savings time according to the NTP server and time zone setting. To disable daylight savings adjustment, disable both this setting and User-defined Daylight Savings Time.
User-defined Daylight Savings Time	Select to set your own start and end dates and offset for Daylight Savings Time. To disable daylight savings adjustment, disable both this setting and Automatically adjust clock for Daylight Savings.

Setting	Description
Daylight Savings Start: ■ Month ■ Week ■ Day ■ Hour	If User-defined DST is enabled, set the start date and time for daylight savings: Month, week, day, and hour.
Daylight Savings End: ■ Month ■ Week ■ Day ■ Hour	If User-defined DST is enabled, set the end date and time for daylight savings: Month, week, day, and hour.
Daylight Savings Offset (minutes)	If User-defined DST is enabled, this specifies the daylight savings adjustment (in minutes) to be applied when the current time is between Daylight Savings Start and Daylight Savings End.
Use DHCP (Option 2/100/101)	If Enable Network Time is selected, select to use DHCP to determine the time zone offset. Options 2, 100 and 101 determine time zone information.

Manual Time Settings

If Enable Network Time is disabled or if the time server is not available, use Manual Time Settings to set the current time.

Setting	Description
Date	Select the current year, month, and day. Click the **Date** field and select the date from the calendar that appears.
Time	Sets the current hour, minute, and second. Click the Time field, and enter the current time. You can also refresh the page to update the manual time settings.

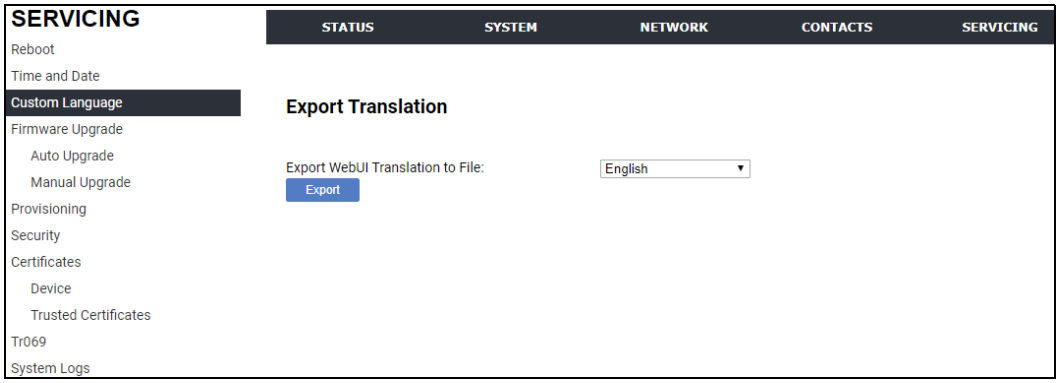
Click Apply Now to start the C620 using the manual time settings.

Custom Language

On the Export Translation page, you can export WebUI language strings. After exporting language strings, you can use the resulting file as the basis for a custom language translation file (.tpk file).

You can import one custom language for use on the WebUI. The custom language adds to the existing languages available with the firmware.

Importing a custom language can only be done using the configuration file. See *“"file" Module: Imported File Settings” on page 173*.



The available languages for export are identical to the WebUI Language list described in *“User Preferences” on page 57*.

The filename of the exported language file will be:

- WebUI: <Model Number>-<Display Name>-webui.tpk

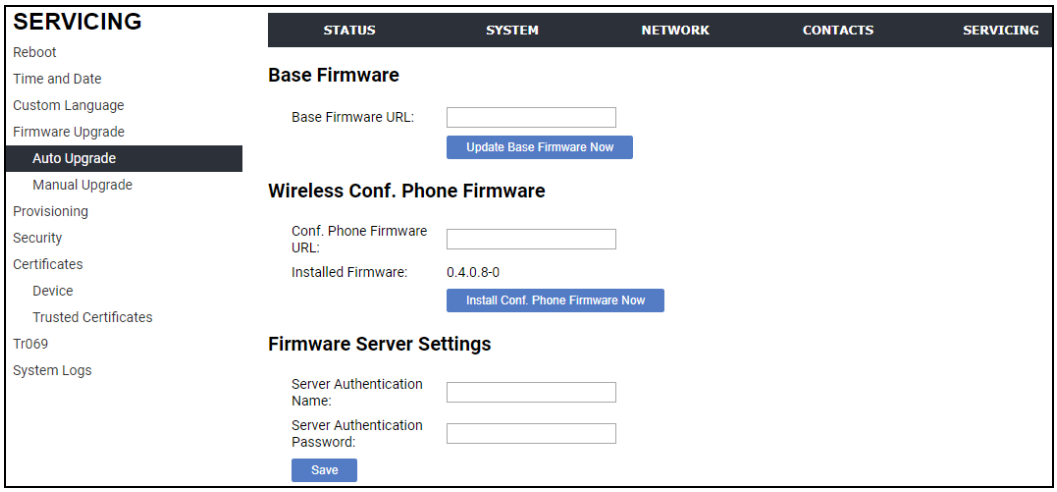
Firmware Upgrade

You can update the C620 with new firmware using the following methods:

- **Auto Upgrade** – Retrieving a firmware update file from a remote host computer and accessed via a URL. This central location may be arranged by you, an authorized dealer, or your SIP service provider. the URL under **Base Firmware** or **Wireless Conf. Phone Firmware**.
- **Manual Upgrade** – Using a file located on your computer or local network. No connection to the Internet is required. Consult your dealer for access to firmware update files. Click **Manual Upgrade** to view the page where you can manually upgrade the C620 firmware.

The firmware upgrade settings are also available as parameters in the configuration file. See *""provisioning" Module: Provisioning Settings" on page 149*.

Auto Upgrade



Base Firmware

Setting	Description
Base Firmware URL	The URL where the C620 Base Station firmware update file resides. This should be a full path, including the filename of the firmware file.

Wireless Conf. Phone Firmware

Setting	Description
Conf. Phone Firmware URL	The URL where the conference phone firmware update file resides. This should be a full path, including the filename of the firmware file.
Installed Firmware	The version number of conference phone firmware currently installed.

Firmware Server Settings

Setting	Description
Server authentication name	Authentication username for the firmware server.
Server authentication password	Authentication password for the firmware server.

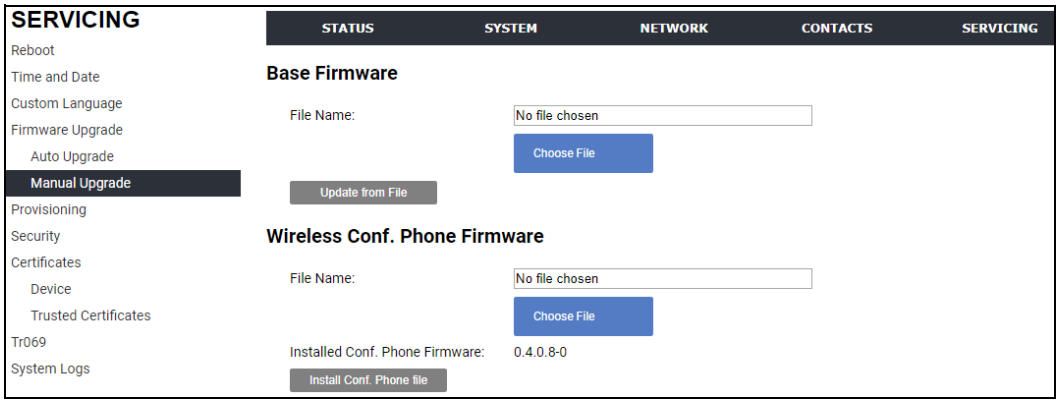
To update the firmware immediately:

- Click Update Base Firmware Now or Install Conf. Phone Firmware Now.

NOTE You can also configure the C620 to check for firmware updates at regular intervals. See *"Provisioning" on page 94*.

Manual Firmware Update and Upload

On the Manual Firmware Update Settings page, you can upgrade the C620 base station and conference phone firmware using a file located on your computer or local network.



Updating the base station

To update the firmware using a file on your computer or local network:

1. Under **Base Firmware**, click Choose File to locate and open the firmware update file.
2. Click Update from File.

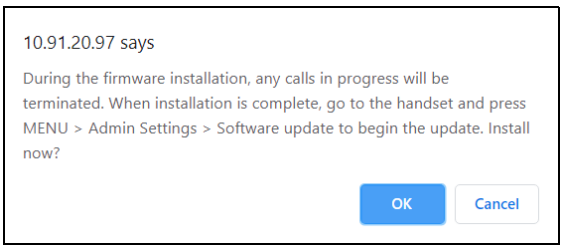
   After clicking Update from File, the C620 will update its firmware and restart.

Updating the conference phone

Updating conference phone firmware using the WebUI is a two-step process. First you must download the conference phone firmware and install it on the base station. Second, you must install the conference phone firmware on the conference phone. The conference phone downloads the firmware over the air from the base station.

To install the conference phone firmware on the base station:

1. Under **Wireless Conf. Phone Firmware**, click Choose File to locate and open the firmware update file.
2. Click Install Conf. Phone file.
   The confirmation dialog box shown below appears.



3. To begin installing the conference phone firmware, click OK. The message **Installing handset firmware. Please wait...** appears. To cancel the download, click Cancel.

After clicking OK, the message **System update in progress. Please wait...** appears on the conference phone.

After a successful update, the message **Firmware installation successful** appears on the WebUI.

An error message appears if:

- the conference phone firmware is already up to date.
- the conference phone firmware URL is incorrect, or the file cannot be retrieved for any other reason.
- the conference phone firmware file is corrupted.
- the conference phone doesn't recognize the firmware file. For example, the firmware file may belong to a different ErisTerminal product.

To install the firmware on the conference phone:

NOTE Your conference phone will automatically initiate the firmware update after a short period of time, as long as there are no active calls on the base station. If you wish to manually start the firmware update, perform the steps below.

1. On the conference phone, press , and then select **Status & Settings**.
2. Select **Admin settings**.
3. Enter the admin password. The default is **admin**. To switch between entering uppercase letters, lowercase letters and numbers, press the middle soft key until its label displays **ABC** , **abc** or **123** .
4. On the Admin settings menu, select **Firmware update**.
   The conference phone checks for new firmware. If new firmware is found, the conference phone screen asks you to proceed with the update.

Provisioning

Provisioning refers to the process of acquiring and applying new settings for the C620 using configuration files retrieved from a remote computer. After a C620 is deployed, subsequent provisioning can update the C620 with new settings; for example, if your service provider releases new features. See also *"Provisioning Using Configuration Files" on page 111*.

With automatic provisioning, you enable the C620 to get its settings automatically—the process occurs in the background as part of routine system operation. Automatic provisioning can apply to multiple devices simultaneously.

With manual provisioning on the WebUI, you update the C620 settings (configuration and/or firmware) yourself via **SERVICING > Provisioning > Import Configuration** and/or **SERVICING > Firmware Upgrade > Manual Upgrade**. Manual provisioning can only be performed on one C620 at a time.

On the Provisioning page, you can enter settings that will enable the C620 to receive automatic configuration and firmware updates. The Provisioning page also allows you to manually update C620 configuration from a locally stored configuration file using an Import function. You can also export the C620 configuration—either to back it up or apply the configuration to another C620 in the future—to a file on your computer.

The provisioning process functions according to the Resynchronization settings and Provisioning Server Settings. The C620 checks for the provisioning URL from the following sources in the order listed below:

1. PnP—Plug and Play Subscribe and Notify protocol

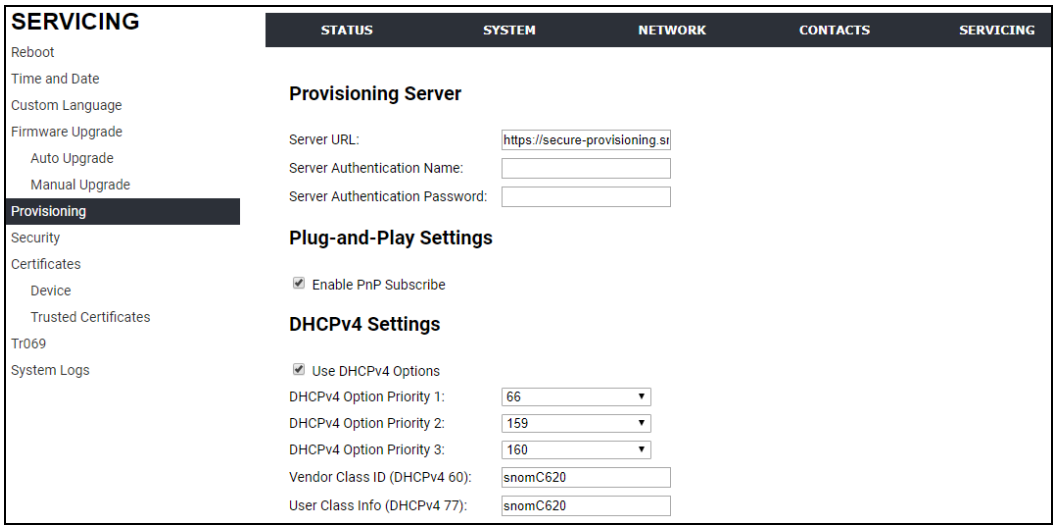
2. DHCP Options

3. Preconfigured URL—Any C620 updated to the latest firmware release will have the Redirection Server URL available as the default Provisioning Server URL (see *"`provisioning.server_address`" on page 153*).

NOTE Using the Redirection Service requires contacting the Snom support team for an account.

If one of these sources is disabled, not available, or has not been configured, the C620 proceeds to the next source until reaching the end of the list.

The provisioning settings are also available as parameters in the configuration file. See *""provisioning" Module: Provisioning Settings" on page 149*.



Provisioning Server

In the tables on the following pages, click a setting to link to the matching configuration file parameter in Chapter 5, *Configuration File Parameter Guide*. Default values and ranges are listed there.

Setting	Description
Server URL	URL of the provisioning file(s). The format of the URL must be RFC 1738 compliant, as follows: "<schema>://<user>:<password>@<host>:<port>/<url-path>" ■ "<user>:<password>@" may be empty. ■ "<port>" can be omitted if you do not need to specify the port number.
Server Authentication Name	User name for access to the provisioning server
Server Authentication Password	Password for access to the provisioning server

Plug-and-Play Settings

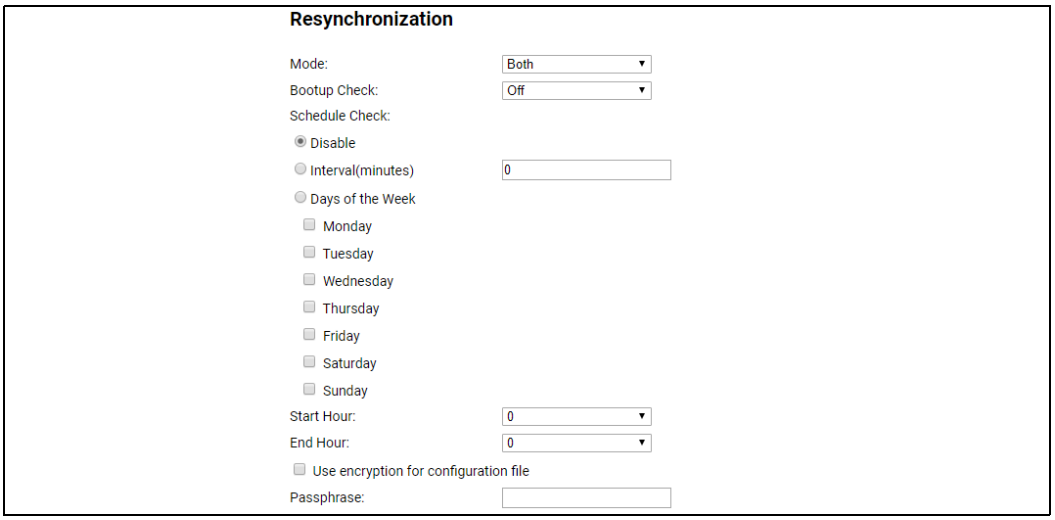
Setting	Description
Enable PnP Subscribe	Select to enable the C620 to search for the provisioning URL via a SUBSCRIBE message to a multicast address (224.0.1.75). The C620 expects the server to reply with a NOTIFY that includes the provisioning URL. The process times out after five attempts.

DHCPv4 Settings

Setting	Description
Use DHCPv4 Options	Enables the C620 to use DHCP options to locate and retrieve the configuration file. When selected, the C620 automatically attempts to get a provisioning server address, and then the configuration file. If DHCP options do not locate a configuration file, then the server provisioning string is checked. **Note**: Ensure that DHCP is also enabled on the "Basic Network Settings" page (see *"Basic Network Settings" on page 67*).
DHCPv4 Option Priority 1	If DHCP is enabled, sets the DHCP Option priority. Select the highest priority option.
DHCPv4 Option Priority 2	If DHCP is enabled, sets the DHCP Option priority. Select the second highest priority option.
DHCPv4 Option Priority 3	If DHCP is enabled, sets the DHCP Option priority. Select the third highest priority option.
Vendor Class ID (DHCPv4 60)	DHCP Option 60 is available to send vendor-specific information to the DHCP Server.
User Class Info (DHCPv4 77)	DHCP Option 77 is available to send vendor-specific information to the DHCP Server.

Resynchronization

In the Resynchronization section, you can select how and when the phone checks for updated firmware and/or configuration files.



Setting	Description
Mode	Sets which files for which the C620 checks. It can check for configuration files, firmware update files (from the URL entered on the Firmware Server Settings page), or both. **Note**: When checking for both configuration and firmware files, the firmware URL can be within the config file. This firmware URL takes take precedence over the URL on the Firmware Server Settings page. It will also update the URL on the Firmware Server Settings page. This enables you to change the firmware URL automatically.
Bootup Check	Sets the C620 to check the provisioning URL for new configuration and/or firmware files upon bootup. The update is applied as part of the reboot process.
Schedule Check: Disable	When selected, disables regularly scheduled file checking.
Schedule Check: Interval(minutes)	Sets an interval for checking for updates. After selecting Interval, enter the interval in minutes between update checks.
Schedule Check: Days of the Week	Select to enable weekly checking for updates on one or more days. After selecting Days of the Week, select the day(s) on which the C620 checks for updates.
Start Hour	Select the hour of the day on which the C620 checks for updates.
End Hour	Select the hour of the day on which the C620 stops checking for updates.
Use encryption for configuration file	Enables an AES-encrypted configuration file to be decrypted before being applied to the C620. Select if the configuration file has been secured using AES encryption. See *“Securing configuration files with AES encryption” on page 117*.
Passphrase	If the configuration file has been secured using AES encryption, enter the 16-bit key.

Import Configuration

You can configure the C620 by importing a configuration file from your computer or your local network. For information about configuration file types and configuration file formatting, see *"Provisioning Using Configuration Files" on page 111*.

To import a configuration file:

1. Click Choose File to locate and open the configuration file.
2. Click Update from File.

The C620 will update its configuration.

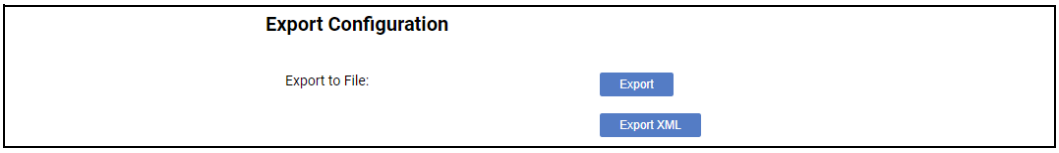
Manually importing a configuration file differs from the auto-provisioning process in that:

- The C620 does not check whether the file has been loaded before. The configuration file is processed whether or not it is different from the current version.
- The C620 will restart immediately after importing the configuration file, without waiting for one minute of inactivity.

Export Configuration

You can export all the settings you have configured on the WebUI and save them as a configuration file on your computer. You can then use this configuration file as a backup, or use it to update other phones.

Under **Reset Configuration**, you can also reset the phone to its default configuration.



NOTE

The exported configuration file will contain the following passwords in plain text:

- SIP account authentication password
- EAPOL password
- Firmware server password
- Provisioning server password
- Encryption passphrase
- LDAP server password
- Broadsoft directory server password.

Please ensure that you save the exported configuration file in a secure location. You can also disable passwords from being exported as plain text. See *"provisioning.pwd_export_enable" on page 152*.

To export the configuration file:

- Click **Export**.

The format of the exported file is **<model name>_<mac address>.cfg**. For example, **C620_0011A0CF489.cfg**.

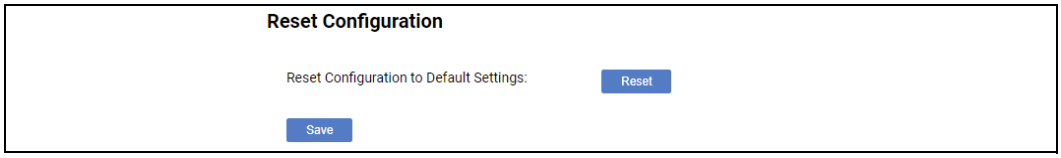
Exporting a configuration file generates two header lines in the configuration file. These header lines provide the model number and software version in the following format:

```
#Model Number = xxxxxxx

#SW Version = xxxxxxx
```

You can use the exported file as a general configuration file, and duplicate the settings across multiple units. However, ensure that you edit the file to remove any MAC-specific SIP account settings before applying the general configuration file to other units.

Reset Configuration

You can reset the phone to its default settings.



To reset the C620 to its default configuration:

1. Under **Reset Configuration**, click **Reset**.
2. When the confirmation box appears, click **OK**.

Security

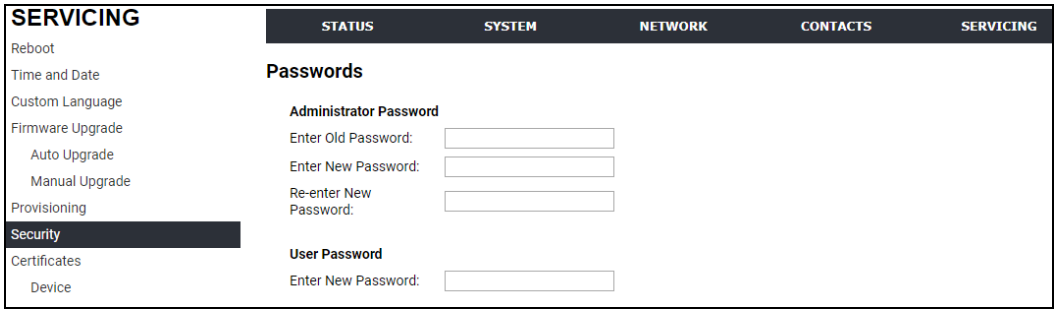
On the **Security** page, you can:

- Reset the admin password and user password
- Configure web server settings
- Reset the Cordless PIN for registering cordless devices
- Enable the system to only accept SIP traffic from trusted sources and IPs.

These security settings are also available as parameters in the configuration file. See *""web" Module: Web Settings" on page 165*.

Passwords

You can set the administrator password and user password on the WebUI or by using provisioning. For more information on using provisioning to set passwords, see *""profile" Module: Password Settings" on page 185*.



To change the admin password:

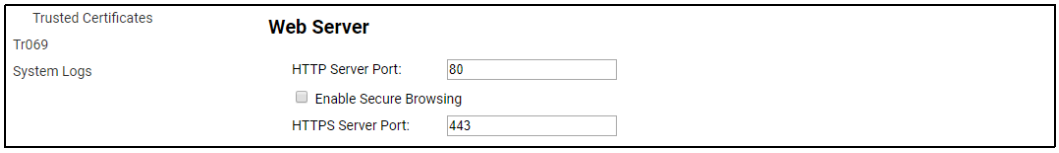
1. Enter the old password.
2. Enter and re-enter a new password. The password is case sensitive and can consist of both numbers and letters (to a maximum of 15 characters).
3. Click Save .

To change the user password:

1. Enter the new password.

   The password is case sensitive and can consist of both numbers and letters (to a maximum of 15 characters).
2. Click Save .

Web Server



In the tables on the following pages, click a setting to link to the matching configuration file parameter in Chapter 5, *Configuration File Parameter Guide*. Default values and ranges are listed there.

Setting	Description
HTTP Server port	Port used by the HTTP server.
Enable Secure Browsing	Sets the server to use the HTTPS protocol.
HTTPS Server port	Port used by the HTTPS server.

To configure Web Server Settings:

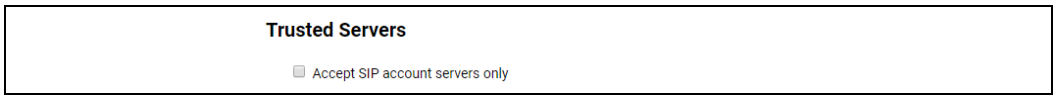
1. Enter the HTTP Server port number. The default setting is 80.
2. Enable or Disable Secure Browsing. When enabled, the HTTPS protocol is used, and you must select the HTTPS server port in the next step.
3. Enter the HTTPS server port number. The default setting is 443.

NOTE Changing the Web Server settings will reboot the C620.

Trusted Servers

The Trusted Servers setting provides a means of blocking unauthorized SIP traffic. When enabled, each account's Registration server, SIP server, Outbound Proxy server and Backup Outbound Proxy server will be used as sources for trusted SIP traffic. All unsolicited SIP traffic (for example, INVITE, NOTIFY, unsolicited MWI, OPTIONS) will be blocked unless it is from one of the trusted servers with the enabled accounts.

If additional trusted sources are required beyond what has been specified with the enabled accounts (for example, if IP dialing or other types of server traffic need to be secured), use the Trusted IP settings on the Security page.



Setting	Description
Accept SIP account servers only	Enable or disable using the account servers as sources for trusted SIP traffic.

Trusted IP

In addition to the Trusted Servers setting, incoming IP traffic can be filtered using an "Allowed IP" list of IP addresses. When this is enabled, all unsolicited IP traffic will be blocked unless it is from one of the trusted IP addresses on the "Allowed IP" list.

You can enter the "Allowed IP" list in the 10 fields on the "Trusted IP" section. Entries on the "Allowed IP" list must be specified as IP addresses (IPv4 or IPv6).

Three formats are supported for entries on the "Allowed IP" list:

1. IP range specified using CIDR notation (defined in rfc4632). IPv4 or IPv6 address followed by a prefix; for example, 192.168.0.1/24.
2. IP range specified with a pair of starting and ending IPv4 or IPv6 addresses, separated by '-' (for example, 192.168.0.1-192.168.5.6).
   - No space before or after '-'
   - Both starting IP & ending IP have to be with the same IP version
   - Starting IP has to be smaller than the ending IP; otherwise, all traffic will be dropped.
3. Single IP address in IPv4 or IPv6.

NOTE To ensure WebUI access after configuring Trusted IP, you must include the IP of the Web Browser on the “Allowed IP” list.

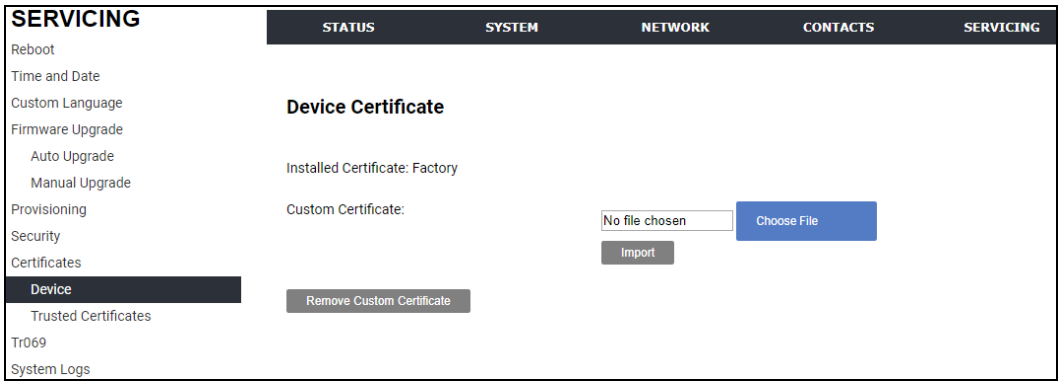
Setting	Description
Accept only allowed IP for incoming requests	Enable or disable using the “Allowed IP” list to filter all IP traffic.
Allowed IP 1–10	Enter IP addresses or address ranges to be used as sources of authorized IP traffic.

Certificates

You can add two types of certificates using the WebUI or the provisioning file (see *“"file" Module: Imported File Settings” on page 173*). The two types of certificates are:

- Device—A single Device Certificate can be uploaded so that other parties can authenticate the phone in the following cases:
  - When the phone acts as a web server for the user to manage configurations.
  - When the phone acts as a client for applications where HTTP is supported.
- Trusted—Trusted Certificates are for server authentication with secured HTTP transaction in the following applications: SIP signaling, Provisioning, Firmware, and LDAP directory service. Up to 20 trusted certificates can be installed.

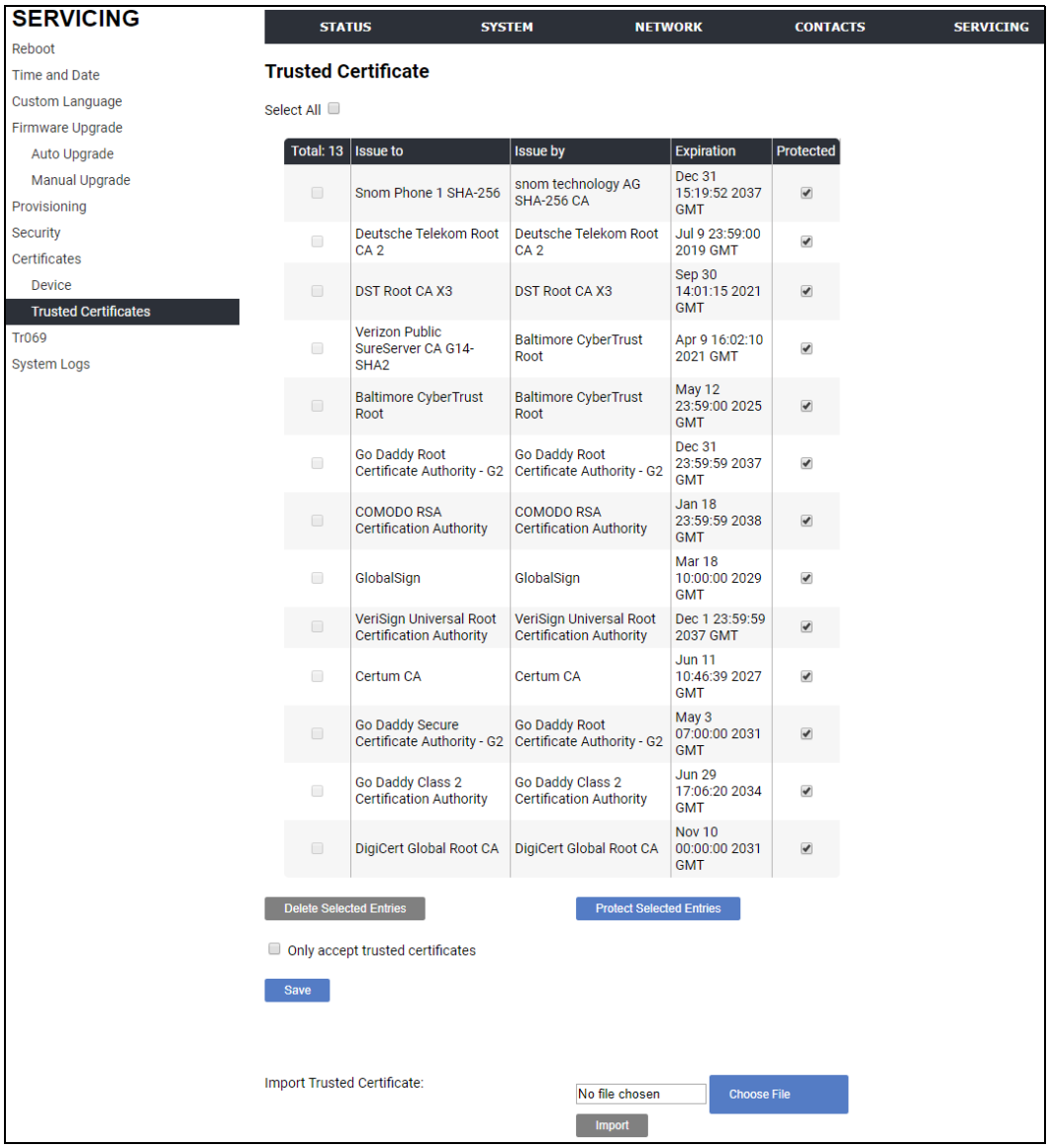
Device Certificate



To import a device certificate:

1. On the Device Certificate page, click Choose File.
2. Locate the certificate file and click **Open**.
3. Click Import.

Trusted Certificate



On the **Trusted Certificate** page, you can:

- import up to 20 trusted certificates.
- delete individual (or all) certificates.
- protect certificates by selecting them in the **Protected** column, and then clicking Protect Selected Entries. Protected certificates cannot be selected for deletion and are not removed during a reset to factory defaults.

Select **Only accept trusted certificates** to enable server authentication. Deselecting this option disables server authentication.

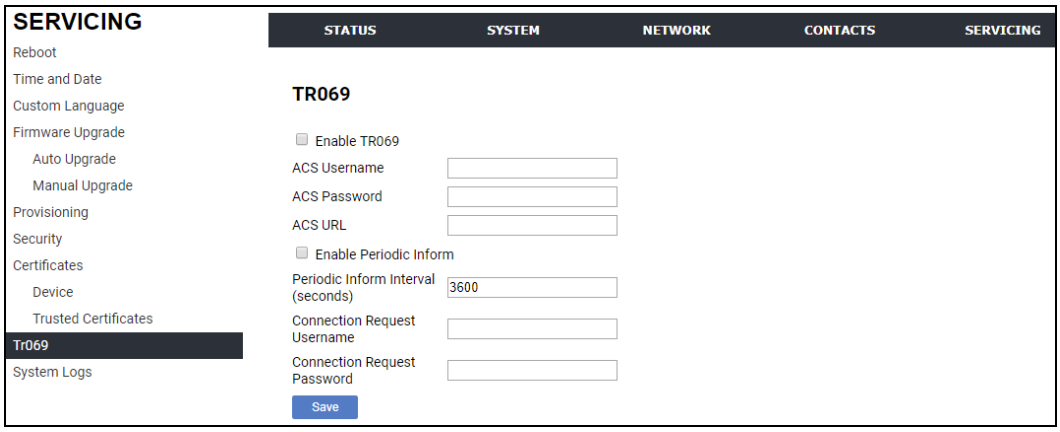
To import a trusted certificate:

1. On the Trusted Certificate page, click Choose File.
2. Locate the certificate file and click **Open**.
3. Click Import.

TR-069 Settings

The Broadband Forum's Technical Report 069 (TR-069) defines a protocol for remote management and secure auto-configuration of compatible devices. On the **Tr069** page, you can enable TR-069 and configure access to an auto-configuration server (ACS).

The provisioning settings are also available as parameters in the configuration file. See *""tr069" Module: TR-069 Settings" on page 178*.



In the table below, click a setting to link to the matching configuration file parameter in Chapter 5, *Configuration File Parameter Guide*. Default values and ranges are listed there.

Setting	Description
Enable TR069	Enable/Disable TR-069 subsystem.
ACS Username	User name used for ACS authentication.
ACS Password	Password used for ACS authentication.
ACS URL	URL used to contact the ACS (for example, http://my.acs:9675/path/to/somewhere/).
Enable Period Inform	Enable/Disable periodic inform method calls.
Periodic Inform Interval (seconds)	Periodic inform method calls interval.
Connection Request Username	If the ACS wants to communicate with the device, it must offer the matching Connection Request user name. When the device sends the report to ACS for the first time, it contains information for this.
Connection Request Password	If the ACS wants to communicate with the device, it must offer the matching Connection Request password. When the device sends the report to ACS for the first time, it contains information for this.

System Logs

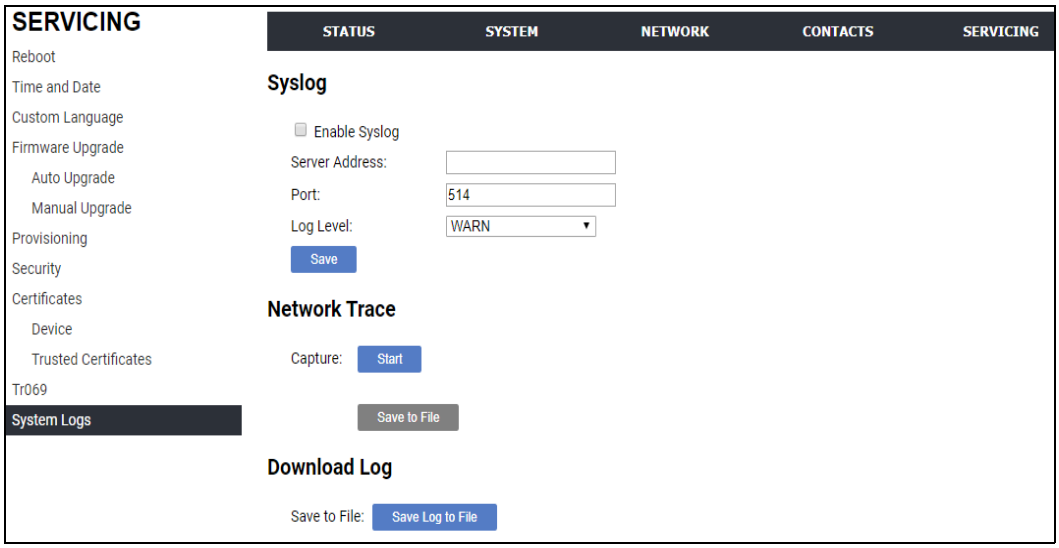
On the **Syslog Settings** page, you can enter settings related to system logging activities. It supports the following logging modes:

- Syslog server
- Volatile file

Under **Network Trace**, you can capture network traffic related to the phone's activity and save the capture as a .pcap file. The file can be used for diagnostic and troubleshooting purposes.

Under **Download Log**, you can save the system log to a file.

The Syslog settings are also available as parameters in the configuration file. See *""log" Module: Log Settings" on page 159*.



Syslog Settings

In the table below, click a setting to link to the matching configuration file parameter in Chapter 5, *Configuration File Parameter Guide*. Default values and ranges are listed there.

Setting	Description
Enable Syslog	Enable log output to syslog server.
Server Address	Syslog server IP address.
Port	Syslog server port.

Setting	Description
Log Level	Select the log level from the list (displayed in order of highest to lowest level). The higher the level selected, the larger the debug output. ■ ALL ■ DEBUG ■ INFO ■ WARN ■ ERROR ■ CRIT

The logging levels are:

- ALL: Activity is logged for all of the logging levels.
- DEBUG: Developer messages for troubleshooting/debugging purposes.
- INFO: Normal operational messages.
- WARN (Warning): An indication that an error or critical condition can occur if action is not taken. This is the default log level.
- ERROR: Non-urgent failures—unexpected conditions that won't cause the device to malfunction.
- CRIT (Critical): Operating conditions to be reported or corrected immediately (for example, an internal component failure or file system error).

Network Trace

To perform a network trace:

1. Start a network trace by clicking Start . The button changes to Stop .
2. Stop the network trace by clicking Stop .
3. Save the trace by clicking Save to file . Your browser should prompt you to save the **capture.pcap** file.

Download Log

To download the system log:

1. Click Save Log to file .
2. After your browser prompts you to save the **system.log** file, save the file in the desired location.

CHAPTER 4

PROVISIONING USING CONFIGURATION FILES

Provisioning using configuration files is the quickest way to configure multiple C620 SIP Wireless Conference Phones. You can place configuration files on a provisioning server, where the C620 SIP Wireless Conference Phones retrieve the files and update their configuration automatically.

Configuration files have the extension **.htm** and contain settings that will apply to C620 SIP Wireless Conference Phones. To edit a configuration file, open it with a text editor such as Notepad.

The settings within a configuration file are grouped into modules. Most of the modules group their settings in the same way that settings are grouped on the C620 WebUI. For example, the "time_date" module in the configuration file contains the same settings that are on the **Time and Date** WebUI page. For a complete list of C620 configuration file modules and their associated parameters, see *"Configuration File Parameter Guide" on page 119*.

Using the WebUI, you can also import a configuration file and apply the configuration file settings to the C620. For more information, see *"Import Configuration" on page 98*.

This chapter covers:

- *"The Provisioning Process" on page 112*
- *"Configuration File Types" on page 114*
- *"Data Files" on page 115*
- *"Configuration File Tips and Security" on page 116*.

The Provisioning Process

The automatic provisioning process is as follows:

1. Check for new or updated configuration files. For file-checking options, see *"Provisioning" on page 94* and *"Resynchronization: configuration file checking" on page 113*. The C620 maintains a list of the last loaded provisioning files. The C620 compares its current configuration against the files it finds on the provisioning server.

   If provisioning has been triggered by the resync timer expiring or by remote check-sync, the C620 checks for updated files after one minute of inactivity.

2. Download the configuration files.

   If any file on the provisioning server has changed, the C620 treats it as a new file and downloads it.

   If the provisioning URL specifies a path only with no filename, then by default the C620 looks for and retrieves the following two files:

   - General file: **<model>.cfg**.
   - MAC-specific file: **<model>_<MAC Address>.cfg**.

   The <model> variable is the Snom product model: C620, for example.

   If the provisioning URL specifies both a path and filename, then the C620 retrieves only the configuration file specified.

3. The C620 restarts after one minute of inactivity.

During provisioning, the C620 reads the configuration file and validates each module and setting. The C620 considers a setting valid if it is:

- a valid data type
- formatted as a valid setting
- within a valid data range
- part of a module that passes an integrity check. That is, the module's settings are consistent and logical. For example, in the "network" module, if DHCP is disabled, but no static IP address is specified, the module will fail the integrity check and none of the settings will apply.

Invalid modules or invalid settings are skipped and logged as ERROR messages in the system log, but will not interrupt the provisioning process. The system log will include the module parameters that have not been applied. A recognized module with unrecognized settings will cause all other settings in that module to be skipped.

A successful configuration or firmware update is reported as an INFO message in the system log.

See *"Configuration File Parameter Guide" on page 119* for the options and value ranges available for each configuration file setting.

Resynchronization: configuration file checking

You can select a number of options that determine when the C620 checks for new configuration files. This process of checking for configuration files is called Resynchronization. Resynchronization options are available on the WebUI **Provisioning** page, but you can also include them in a configuration file.

The resynchronization options are:

- Mode—sets the C620 to check for a configuration file only, a firmware update file only, or both types of file.
- Never—configuration file checking is disabled
- Bootup—the C620 checks for new configuration files when it boots up. Any updates are applied during the boot-up process.
- Remote check-sync—enables you to start a resynchronization remotely using your hosted server's web portal. The Remote check-sync settings are available only in the configuration file, not the WebUI.
- Repeatedly, at a defined interval from 60 to 65535 minutes (45 days).

C620 restart

If the C620 needs to restart after an auto-update, the restart happens only after the device has been idle for one minute.

To prevent users from delaying the update process (auto-updates cannot begin until the C620 has been idle for one minute), or to avoid device restarts that might interfere with incoming calls:

- set the resynchronization interval to a suitable period
- upload any new configuration file(s) to your provisioning server after work hours so that the C620 will download the file(s) when there is no call activity.

When you update the C620 by importing a configuration file using the WebUI, the device restarts immediately after applying the new settings, regardless of whether the C620 is idle.

Configuration File Types

The C620 is able to retrieve and download two types of configuration file. Depending on your requirements, you may want to make both types of configuration file available on your provisioning server.

The two configuration file types are a general configuration file and a MAC-specific configuration file. The types differ in name only. The formatting of the files' content is the same.

The general configuration file contains settings that are required by every C620 in the system.

The MAC-specific configuration file is a file that only a single C620 can retrieve. The MAC-specific configuration file name contains a C620 MAC address and can only be retrieved by the device with a matching MAC address.

The filename formats for both files are:

- General file: **<model>.cfg**
- MAC-specific file: **<model>_<MAC Address>.cfg**

The <model> variable is the Snom product model; for example, **C620**. For more information about the MAC-specific configuration file, see *"Guidelines for the MAC-specific configuration file" on page 116*.

If the provisioning URL specifies a path only with no filename, then by default the C620 will fetch both files.

However, if the provisioning URL specifies both a path and filename, then the C620 will only fetch the single configuration file specified.

Both the general and MAC-specific files can contain any of the available configuration settings. A setting can appear in the general configuration file or the MAC-specific configuration file, or both files, or neither file. If a setting appears in both files, the setting that is read last is the one that applies.

When the C620 fetches both a general and a MAC-specific configuration file, the general file is processed first. You can configure a setting for most of your C620 SIP Wireless Conference Phones in the general file, and then overwrite that setting for just a few C620 SIP Wireless Conference Phones using the MAC-specific file.

Data Files

The configuration file can also include links to data files for product customization. Allowed data types include the following:

- Directory (contacts, blacklist) in .xml format
- Certificates (server, provisioning) in pem format

Links to data files are in the configuration file's "file" module. This is where you enter any URLs to the data files that the C620 SIP Wireless Conference Phone may require.

None of the data files are exported when you export a configuration file from the C620. However, you can export a Directory or Blacklist .xml file using the WebUI. After modifying the .xml file, you can use the configuration file "file" module to have the C620 import the new file. For a complete list of data file parameters, see *""file" Module: Imported File Settings" on page 173*.

Configuration File Tips and Security

All configuration settings are initially stored in a configuration template file. Copy, rename, and edit the template file to create a general configuration file and the MAC-specific configuration files you will need. You can store the general configuration file and the MAC-specific files on your provisioning server.

Do not modify the configuration file header line that includes the model and firmware version.

To save yourself time and effort, consider which settings will be common to all (or the majority of) C620 SIP Wireless Conference Phones. Such settings might include call settings, language, and NAT settings. You can then edit those settings in the configuration template and save it as the general configuration file. The remaining settings will make up the MAC-specific configuration file, which you will have to copy and edit for each C620.

Clearing parameters with %NULL in configuration file

For configuration file parameters that can have a text string value, you can clear the value of the parameter by applying the value %NULL in the configuration file.

For example: `sip_account.1.display_name = %NULL`

Guidelines for the MAC-specific configuration file

The C620 downloads the MAC-specific configuration file after the general configuration file. You must create a MAC-specific configuration file for each C620 in your organization's telephone system. The file name must contain the C620 MAC address, which is printed on a label on the back of the device. For example, a Snom C620 SIP Wireless Conference Phone with the MAC address of 00:11:A0:10:6F:2D would download the **C620_0011A0106F2D.cfg** file.

NOTE When renaming a MAC-specific configuration file, ensure the filename is all upper case.

The MAC-specific configuration file contains settings intended exclusively for that C620 SIP Wireless Conference Phone. Such settings will include SIP account settings such as display name, user ID, and authentication ID.

Securing configuration files with AES encryption

You can encrypt your configuration files to prevent unauthorized users modifying the configuration files. The C620 firmware decrypts files using the AES 256 algorithm. After encrypting a file and placing it on your provisioning server, you can enable the C620 to decrypt the file after fetching it from the server.

The procedures in this section use OpenSSL for Windows for file encryption, as shown in Figure 2.

To decrypt a configuration file, you will need a 16-character AES key that you specified when you encrypted the file. The key (or passphrase) is limited to 16 characters in length and supports special characters **~ ^ ` % ! & - _ + = | . @ * : ; , ? ( ) [ ] { } < > / \ #** as well as spaces.

NOTE The encryption of configuration files is supported only for the auto provisioning process. Encrypt files only if you intend to store them on a provisioning server. Do not encrypt files that you intend to manually import to the C620. You cannot enable decryption for manually imported configuration files.

To encrypt a configuration file:

1. (Optional) Place your configuration file in the same folder as the openssl executable file. If the configuration file is not in the same folder as the openssl executable file, you can enter a relative pathname for the [infile] in the next step.
2. Double-click the **openssl.exe** file.
3. On the openssl command line, type:

```
enc -aes-256-cbc -pass pass:[passphrase123456] -in [infile] -out [outfile]
-nosalt -p
```

Elements in brackets are examples—do not enter the brackets. Enter a 16-character passphrase and the unencrypted configuration file filename (the "infile") and a name for the encrypted file ("outfile") that will result.

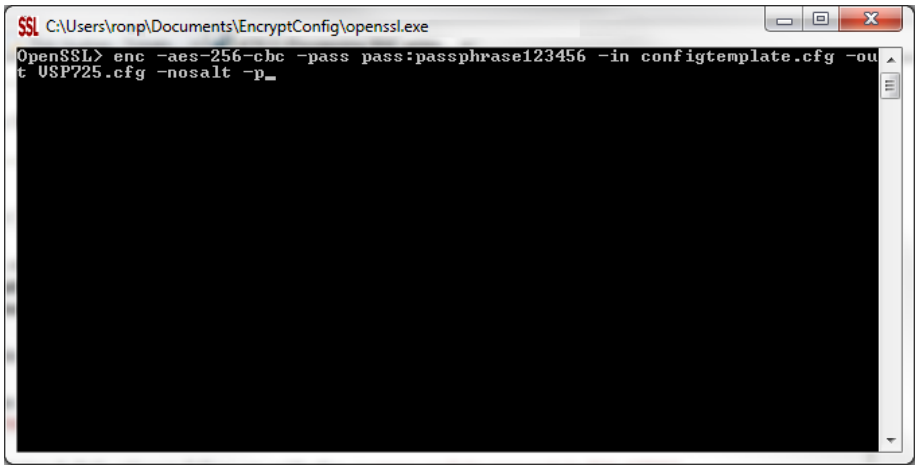
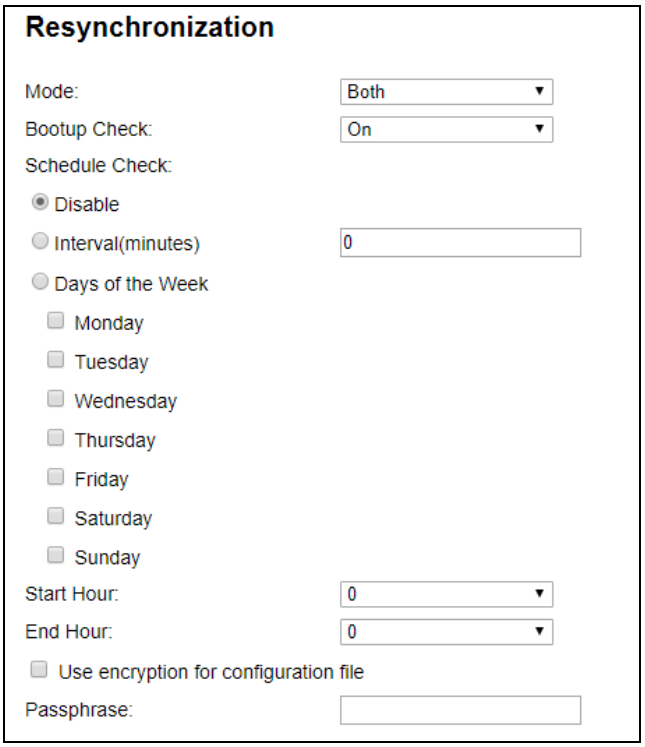


Figure 2. OpenSSL command line

To enable configuration file decryption:

1. On the WebUI, click **Servicing > Provisioning**.
2. On the Provisioning page under **Resynchronization**, select **Use Encryption for configuration file**.



3. Enter the 16-character passphrase that you created when you encrypted the configuration file.
4. Click Save .

NOTE You must ensure that configuration files are encrypted when enabling AES Encryption. Decrypting an unencrypted file will result in a garbage file that is not processed. This will also be logged as an error in the system log.

CHAPTER 5

CONFIGURATION FILE PARAMETER GUIDE

This chapter lists the available options for all the settings within the C620 configuration file. Most settings in the configuration file have an equivalent in the WebUI (see the settings tables in *“Using the WebUI” on page 35*). However, the options you must enter when editing the configuration file have a different syntax and format.

The settings are divided into modules. Most modules correspond to a page on the C620 WebUI. You may wish to reorganize the modules within the configuration file itself. The configuration file settings can be listed in any order, and the configuration file will still be valid.

The modules included in the configuration file are:

- *“"sip_account" Module: SIP Account Settings” on page 121*
- *“"hs_settings" Module: Handset Settings” on page 136*
- *“"network" Module: Network Settings” on page 144*
- *““system” Module: System settings” on page 143*
- *“"provisioning" Module: Provisioning Settings” on page 149*
- *“"time_date" Module: Time and Date Settings” on page 154*
- *“"log" Module: Log Settings” on page 159*
- *“"remoteDir" Module: Remote Directory Settings” on page 160*
- *“"web" Module: Web Settings” on page 165*
- *““trusted_ip” Module: Trusted IP Settings” on page 166*
- *““trusted_servers” Module: Trusted Server Settings” on page 167*
- *“"user_pref" Module: User Preference Settings” on page 168*

- *“"call_settings" Module: Call Settings” on page 169*
- *“"speed_dial" Module: Speed Dial Settings” on page 187*
- *““audio” Module: Audio Settings” on page 171*
- *“"file" Module: Imported File Settings” on page 173*
- *““xml_app” Module: XML App Settings” on page 177*
- *““tr069” Module: TR-069 Settings” on page 178*
- *“"tone" Module: Tone Definition Settings” on page 180*
- *“"profile" Module: Password Settings” on page 185*

"sip_account" Module: SIP Account Settings

The SIP Account settings enable you to set up individual accounts for each user. Each account requires you to configure the same group of SIP account settings. The SIP account settings for each account are identified by the account number, from 1 to 3 for the C620.

For example, for account 1 you would set:

```
sip_account.1.sip_account_enable = 1
sip_account.1.label = Line 1
sip_account.1.display_name = 1001
sip_account.1.user_id = 2325551001
```

and so on.

For account 2, you would set:

```
sip_account.2.sip_account_enable = 1
sip_account.2.label = Line 2
sip_account.2.display_name = 1002
sip_account.2.user_id = 2325551002
```

and so on, if you have additional accounts to configure.

The SIP account settings follow the format: sip_account.x.[element], where x is an account number ranging from 1 to 3 for the C620.

All these settings are exported when you manually export the configuration from the C620.

General configuration file settings

Setting:	**`sip_account.x.dial_plan`**		
Description:	Sets the dial plan for account x. See *"Dial Plan" on page 44*.		
Values:	Text string	**Default:**	x+P

Setting:	**`sip_account.x.call_restrict_dial_plan`**		
Description:	Enter call restriction dial plan, to prevent users from completing calls to certain numbers for this account.		
Values:	text string (dial plan syntax)	**Default:**	Blank

Setting:	`sip_account.x.inter_digit_timeout`		
Description:	Sets the inter-digit timeout (in seconds) for account x. The inter-digit timeout sets how long the C620 waits after the last digit is entered before dialing the number.		
Values:	1–10	**Default:**	3

Setting:	`sip_account.x.maximum_call_number`		
Description:	Sets the maximum number of concurrent active calls allowed for that account.		
Values:	1–4	**Default:**	4

Setting:	`sip_account.x.dtmf_transport_method`		
Description:	Sets the transport method for DTMF signaling for account x.		
Values:	auto, rfc2833, inband, info	**Default:**	auto

Setting:	`sip_account.x.unregister_after_reboot_enable`		
Description:	Enables or disables the C620 to unregister account x after rebooting.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`sip_account.x.primary_sip_server_address`		
Description:	Sets the SIP server IP address for account x.		
Values:	IPv4, IPv6 or FQDN	**Default:**	Blank

Setting:	`sip_account.x.primary_sip_server_port`		
Description:	Sets the SIP server port for account x.		
Values:	1–65535	**Default:**	5060

Setting:	`sip_account.x.primary_registration_server_address`		
Description:	Sets the registration server IP address for account x.		
Values:	IPv4, IPv6 or FQDN	**Default:**	Blank

Setting:	`sip_account.x.primary_registration_server_port`		
Description:	Sets the registration server port for account x.		
Values:	1–65535	**Default:**	5060

Setting:	`sip_account.x.primary_registration_expires`		
Description:	Sets the expiration time (in seconds) of the current registration for account x.		
Values:	30–7200	**Default:**	3600

Setting:	`sip_account.x.registration_retry_time`		
Description:	Sets the retry frequency of the current registration for account x.		
Values:	1–1800	**Default:**	10

Setting:	`sip_account.x.reliable_provisional_response_option`		
Description:	Sets the 100rel/PRACK option. Indicates if the reliable provisional responses are disabled, supported, or required. 1 (supported): ■ We will include "100rel" in "Supported" header. ■ This triggers the remote side (server or remote client) to include "Requires:100rel" in their response (180 or 183). Server may choose not to do so. But if it does, we need to respond with PRACK. ■ We will NOT include a "Requires: 100rel" in our requests (INVITE). i.e. we won't force anyone to use 100rel, but we will do if we were asked to do. 2 (required): ■ Everything as described for supported, plus our outgoing INVITE also includes "Requires: 100rel". ■ This forces the remote party must support 100rel.		
Values:	0 (disabled), 1 (supported), 2 (required)	**Default:**	0

Setting:	`sip_account.x.primary_outbound_proxy_server_address`		
Description:	Sets the outbound proxy server IP address for account x.		
Values:	IPv4, IPv6 or FQDN	**Default:**	Blank

Setting:	`sip_account.x.primary_outbound_proxy_server_port`		
Description:	Sets the outbound proxy server port for account x.		
Values:	1–65535	**Default:**	5060

Setting:	`sip_account.x.backup_outbound_proxy_server_address`		
Description:	Sets the backup outbound proxy server IP address for account x.		
Values:	IPv4, IPv6 or FQDN	**Default:**	Blank

Setting:	`sip_account.x.backup_outbound_proxy_server_port`		
Description:	Sets the backup outbound proxy server port for account x.		
Values:	1–65535	**Default:**	5060

Setting:	`sip_account.x.codec_priority.1`		
Description:	Sets the highest-priority codec for account x.		
Values:	g711u, g711a, g729, g726, g722, g723_1, ilbc	**Default:**	g711u

Setting:	`sip_account.x.codec_priority.2`		
Description:	Sets the second highest-priority codec for account x.		
Values:	none, g711u, g711a, g729, g726, g722, g723_1, ilbc	**Default:**	g711a

Setting:	`sip_account.x.codec_priority.3`		
Description:	Sets the third highest-priority codec for account x.		
Values:	none, g711u, g711a, g729, g726, g722, g723_1, ilbc	**Default:**	g729

Setting:	`sip_account.x.codec_priority.4`		
Description:	Sets the fourth highest-priority codec for account x.		
Values:	none, g711u, g711a, g729, g726, g722, g723_1, ilbc	**Default:**	g726

Setting: `sip_account.x.codec_priority.5`

Description: Sets the fifth highest-priority codec for account x.

Values: none, g711u, g711a, g729, g726, g722, g723_1, ilbc **Default:** g722

Setting: `sip_account.x.codec_priority.6`

Description: Sets the highest-priority codec for account x.

Values: none, g711u, g711a, g729, g726, g722, g723_1, ilbc **Default:** g723_1

Setting: `sip_account.x.codec_priority.7`

Description: Sets the highest-priority codec for account x.

Values: none, g711u, g711a, g729, g726, g722, g723_1, ilbc **Default:** ilbc

Setting: `sip_account.x.voice_encryption_enable`

Description: Enables or disables SRTP voice encryption for account x.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `sip_account.x.g729_annexb_enable`

Description: Enables G.729 Annex B, with voice activity detection (VAD) and bandwidth-conserving silence suppression. This setting applies only when G.729a/b is selected in a `sip_account.x.codec_priority` parameter.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `sip_account.x.ilbc_payload_type`

Description: Set the default payload type for the ilbc codec.

Values: 96-127 **Default:** 98

Setting: `sip_account.x.dscp`

Description: Sets the Voice Quality of Service Layer 3 - DSCP for account x.

Values: 0–63 **Default:** 46

Setting:	`sip_account.x.sip_dscp`		
Description:	Sets the Signalling Quality of Service Layer 3 - DSCP for account x.		
Values:	0–63	**Default:**	26

Setting:	`sip_account.x.local_sip_port`		
Description:	Sets the Local SIP port for account x.		
Values:	1–65535	**Default:**	Account 1: 5060 Account 2: 5070 Account 3: 5080

Setting:	`sip_account.x.transport_mode`		
Description:	Sets the Signalling Transport Mode for account x.		
Values:	udp, tcp, tls	**Default:**	udp

Setting:	`sip_account.x.mwi_enable`		
Description:	Enables or disables message waiting indicator subscription for account x. Enable if SUBSCRIBE and NOTIFY methods are used for MWI.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`sip_account.x.mwi_subscription_expires`		
Description:	Sets the MWI subscription expiry time (in seconds) for account x.		
Values:	15–65535	**Default:**	3600

Setting:	`sip_account.x.mwi_ignore_unsolicited`		
Description:	Enables or disables ignoring of unsolicited MWI notifications—notifications in addition to, or instead of, SUBSCRIBE and NOTIFY methods—for account x. Disable if MWI service is configured on the voicemail server and does not involve a subscription to a voicemail server.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`sip_account.x.nat_traversal_stun_enable`		
Description:	Enables or disables STUN (Simple Traversal of UDP through NATs) for account x. STUN enables clients, each behind a firewall, to establish calls via a service provider hosted outside of either local network.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`sip_account.x.nat_traversal_stun_server_address`		
Description:	Sets the STUN server IP address.		
Values:	IPv4, IPv6 or FQDN	**Default:**	Blank

Setting:	`sip_account.x.nat_traversal_stun_server_port`		
Description:	Sets the STUN server port.		
Values:	1–65535	**Default:**	3478

Setting:	`sip_account.x.nat_traversal_stun_keep_alive_enable`		
Description:	Enables or disables UDP keep-alives. Keep-alive packets are used to maintain connections established through NAT.		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

Setting:	`sip_account.x.nat_traversal_stun_keep_alive_interval`		
Description:	Sets the interval (in seconds) for sending UDP keep-alives.		
Values:	0–65535	**Default:**	30

Setting:	`sip_account.x.keep_alive_enable`		
Description:	Enable SIP keep alive for NAT traversal and monitoring SIP server status.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`sip_account.x.keep_alive_interval`		
Description:	Sets the interval (in seconds) for sending keep-alives.		
Values:	1-3600	**Default:**	15

Setting: `sip_account.x.keep_alive_ignore_failure`

Description: Enable the phone to ignore keep-alive failure, if failure triggers re-subscription (and calls are dropped).

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `sip_account.x.music_on_hold_enable`

Description: Enables or disables a hold-reminder tone that a far-end caller hears when put on hold during a call on account x.

Values: 0 (disabled), 1 (enabled) **Default:** 1

Setting: `sip_account.x.sip_session_timer_enable`

Description: Enables or disables the SIP session timer.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `sip_account.x.sip_session_timer_min`

Description: Sets the session timer minimum value (in seconds) for account x.

Values: 90–65535 **Default:** 90

Setting: `sip_account.x.sip_session_timer_max`

Description: Sets the session timer maximum value (in seconds) for account x.

Values: 90–65535 **Default:** 1800

Setting: `sip_account.x.check_trusted_certificate`

Description: Enables or disables accepting only a trusted TLS certificate for account x.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `sip_account.x.preferred_ptime`

Description: Enter the packetization interval time in milliseconds.

Values: 10, 20, 30, 40, 50, 60 **Default:** 20

Setting: `sip_account.x.cid_src_priority.1`

Description: Sets the first priority of the caller ID source to be displayed on the incoming call screen.

Values: from, pai, rpid **Default:** pai

Setting: `sip_account.x.cid_src_priority.2`

Description: Sets the second priority of the caller ID source to be displayed on the incoming call screen.

Values: none, from, pai, rpid **Default:** rpid

Setting: `sip_account.x.cid_src_priority.3`

Description: Sets the third priority of the caller ID source to be displayed on the incoming call screen.

Values: none, from, pai, rpid **Default:** from

Setting: `sip_account.x.call_rejection_response_code`

Description: Select the response code for call rejection. This code applies to the following call rejection cases:

- User presses **Reject** for an incoming call
- DND is enabled
- Phone rejects a second incoming call with Call Waiting disabled
- Phone rejects an anonymous call with Anonymous Call Rejection enabled
- Phone rejects call when the maximum number of calls is reached

Values: 480, 486, 603 **Default:** 486

Setting: `sip_account.x.dtmf_payload_type`

Description: Set the configurable RTP payload type for in-call DTMF.

Values: 96-127 **Default:** 101

Setting: `sip_account.x.use_register_route_header`

Description: Use Route header for REGISTER

Values: 0 (disabled), 1 (enabled) **Default:** 1

Setting: `sip_account.dirty_host_ttl`

Description: Specify the “Time to Live” (TTL) for dirty hosts in seconds. This means that, when a phone was unable to reach a host, the phone will not try to reach this host again until the time specified in this field has elapsed.
If this setting is 0 or empty, it has no effect (the host is set as "dirty" but only for 0 seconds, which means it will have no effect on future requests).

Values: 0-7200 **Default:** 0

Setting: `sip_account.mac_info_in_every_sip_message`

Description: Extends the User Agent Header by the MAC address in all SIP messages. When enabled, the MAC address is added to *every* SIP message (all IDs), in the following way:
User-Agent: *model /firmware version* (MAC=*MAC address*)
e.g. User-Agent: snomC620/1.0.5.17 (MAC=000413BB0634)

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `sip_account.pnp_local_sip_port`

Description: Local SIP port for the purpose of checking ua-profile event to process provisioning PnP upon received notification.

Values: 1-65535 **Default:** 5170

Setting: `sip_account.service_unavailable_handling_option`

Description: Configuration option to handle two modes of failover.
1 = failover triggered by unresponsive server
0 = failover triggered by network received 503 sip response.
We can only parse Retry-After if value=1. So if we need to honor Retry-After, we need to set value=1.

Values: 0, 1 **Default:** 1

Setting: `sip_account.dns_query_option`

Description: Select DNS query option for SIP traffic only:
0 (DNS query with A record only)
1 (DNS query with NAPTR/SRV/A)

DNS query for all other traffic (e.g. HTTP) should always perform A record only.

Values: 0, 1 **Default:** 1

Setting:	`sip_account.shared_local_sip_port_enable`
Description:	Allow the same SIP local port for multiple accounts. If enabled, the SIP local port defined in parameter **sip_account.shared_local_sip_port** will be used instead of the SIP local ports defined for the accounts, parameter: **sip_account.x.local_sip_port**.
Values:	0 (disabled), 1 (enabled) **Default:** 0

Setting:	`sip_account.shared_local_sip_port`
Description:	Defines the local SIP port to be used by all accounts, if enabled by parameter **sip_account.shared_local_sip_port_enable**.
Values:	1-65535 **Default:** 5060

Setting:	`sip_account.sips_uri_enable`
Description:	Defines whether to use SIPS URI or SIP URI with TLS encryption. 1 = sips uri generated 0 = sip uri generated with “transport=tls”. This was the deprecated method of doing tls, which was replaced by sips uri. sips uri is our default setting.
Values:	0, 1 **Default:** 1

MAC-specific configuration file settings

Setting: `sip_account.x.sip_account_enable`

Description: Enables account x to be used by the device.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `sip_account.x.label`

Description: Sets the text that identifies the account on the device LCD. The account label appears on the dialing screen and other call appearance screens.

Values: Text string **Default:** Blank

Setting: `sip_account.x.display_name`

Description: Sets the text portion of the caller ID that is displayed for outgoing calls using account x.

Values: Text string **Default:** Blank

Setting: `sip_account.x.user_id`

Description: Sets the account ID for account x. Depending on your service provider's specifications, this could be an extension number.
Note: Do not enter the host name (e.g. "@sipservice.com"). The configuration file automatically adds the default host name.

Values: Text string **Default:** Blank

Setting: `sip_account.x.authentication_name`

Description: Sets the authentication name for account x. Depending on your service provider's specifications, this could be identical to the user ID.

Values: Text string **Default:** Blank

Setting: `sip_account.x.authentication_access_password`

Description: Sets the authentication password for account x.
The parameter **provisioning.pwd_export_enable** enables/disables this password from being exported in plain text.

Values: Text string **Default:** Blank

Setting: `sip_account.x.feature_sync_enable`

Description: Enables or disables feature synchronization for account x. When enabled, features configured on the service provider's web portal will automatically be updated on the device's WebUI.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `sip_account.x.access_code_retrieve_voicemail`

Description: Sets the voicemail retrieval feature access code for account x.

Values: Text string **Default:** Blank

Setting: `sip_account.x.access_code_dnd_on`

Description: Sets the do not disturb (DND) ON feature access code for account x.

Values: Text string **Default:** Blank

Setting: `sip_account.x.access_code_dnd_off`

Description: Sets the do not disturb (DND) OFF feature access code for account x.

Values: Text string **Default:** Blank

Setting: `sip_account.x.access_code_cfa_on`

Description: Sets the Call Forward All ON feature access code for account x.

Values: Text string **Default:** Blank

Setting: `sip_account.x.access_code_cfa_off`

Description: Sets the Call Forward All OFF feature access code for account x.

Values: Text string **Default:** Blank

Setting: `sip_account.x.access_code_cfna_on`

Description: Sets the Call Forward No Answer ON feature access code for account x.

Values: Text string **Default:** Blank

Setting:	`sip_account.x.access_code_cfna_off`		
Description:	Sets the Call Forward No Answer OFF feature access code for account x.		
Values:	Text string	**Default:**	Blank

Setting:	`sip_account.x.access_code_cfb_on`		
Description:	Sets the Call Forward Busy ON feature access code for account x.		
Values:	Text string	**Default:**	Blank

Setting:	`sip_account.x.access_code_cfb_off`		
Description:	Sets the Call Forward Busy OFF feature access code for account x.		
Values:	Text string	**Default:**	Blank

Setting:	`sip_account.x.access_code_anonymous_call_block_on`		
Description:	Sets the Anonymous Call Block ON feature access code for account x.		
Values:	Text string	**Default:**	Blank

Setting:	`sip_account.x.access_code_anonymous_call_block_off`		
Description:	Sets the Anonymous Call Block OFF feature access code for account x.		
Values:	Text string	**Default:**	Blank

Setting:	`sip_account.x.access_code_outgoing_call_anonymous_on`		
Description:	Sets the Anonymous Outgoing Call ON feature access code for account x.		
Values:	Text string	**Default:**	Blank

Setting:	`sip_account.x.access_code_outgoing_call_anonymous_off`		
Description:	Sets the Anonymous Outgoing Call OFF feature access code for account x.		
Values:	Text string	**Default:**	Blank

Setting:	`sip_account.x.share_line_enable`		
Description:	Enable shared line for account x.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`sip_account.x.mwi_uri`		
Description:	Sets the MWI URI that will be used for MWI subscription. If this setting is left blank, the C620 uses the account x user ID for MWI subscription.		
Values:	SIP URI text string	**Default:**	Blank

Setting:	`sip_account.x.network_conference_enable`		
Description:	Enables or disables network conferencing for account x.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`sip_account.x.network_bridge_uri`		
Description:	Sets the URI for the network conferencing bridge on account x.		
Values:	Text string (SIP URI)	**Default:**	Blank

"hs_settings" Module: Handset Settings

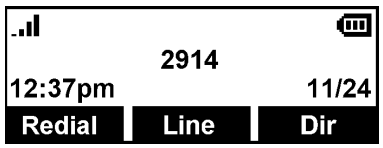
The Handset Settings allow you to configure account assignments and names for the devices that are registered to the base station. For more information on registering devices, see the C620 User Guide.

The following parameters are used to customize the soft keys.

```
hs_settings.x.pfk.softkey.y.idle.feature
hs_settings.x.pfk.softkey.y.idle.label
hs_settings.x.pfk.softkey.y.idle.value
hs_settings.x.pfk.softkey.y.idle.account

hs_settings.x.pfk.softkey.y.call_active.feature
hs_settings.x.pfk.softkey.y.call_active.label
hs_settings.x.pfk.softkey.y.call_active.value
hs_settings.x.pfk.softkey.y.call_active.account

hs_settings.x.pfk.softkey.y.call_held.feature
hs_settings.x.pfk.softkey.y.call_held.label
hs_settings.x.pfk.softkey.y.call_held.value
hs_settings.x.pfk.softkey.y.call_held.account

hs_settings.x.pfk.softkey.y.live_dial.feature
hs_settings.x.pfk.softkey.y.live_dial.label
hs_settings.x.pfk.softkey.y.live_dial.value
hs_settings.x.pfk.softkey.y.live_dial.account
```

Soft keys appear on the phone screen in the same order as the y index of the soft key parameters. For example, the following parameter/value combination will result in the Idle screen shown below.

```
hs_settings.1.pfk.softkey.1.idle.feature = redial
hs_settings.1.pfk.softkey.1.idle.label = (blank)
hs_settings.1.pfk.softkey.1.idle.value = (blank)
hs_settings.1.pfk.softkey.1.idle.account = 0
hs_settings.1.pfk.softkey.2.idle.feature = select_line
hs_settings.1.pfk.softkey.2.idle.label = (blank)
hs_settings.1.pfk.softkey.2.idle.value = (blank)
hs_settings.1.pfk.softkey.2.idle.account = 0
hs_settings.1.pfk.softkey.3.idle.feature = dir
hs_settings.1.pfk.softkey.3.idle.label = (blank)
hs_settings.1.pfk.softkey.3.idle.value = (blank)
hs_settings.1.pfk.softkey.3.idle.account = 0
```



General configuration file settings

Setting: `hs_settings.x.pfk.softkey.y.idle.feature`

Description: Sets the features assigned to the soft keys on the idle screen, where x = 1 to 6 (device number of the conference phone), and y = 1 to 9 (soft key number).

Values: blank, dir, call_log, redial, message, dnd, cfwd, cfwd_all, cfna, cfwd_busy, callback, select_line, settings, quick_dial

Default:
y = 1: redial
y = 2: select_line
y = 3: dir
y = 4: call_log
y = 5-9: blank

Setting: `hs_settings.x.pfk.softkey.y.idle.label`

Description: Sets the label of the soft keys on the idle screen, where x = 1 to 6 (device number of the conference phone), and y = 1 to 9 (soft key number).
If left blank, the phone will display the default label for the selected feature (e.g. label “Dir” for the feature “dir”).

Values: text string

Default: blank

Setting: `hs_settings.x.pfk.softkey.y.idle.value`

Description: Sets the value for the soft key on the idle screen, where x = 1 to 6 (device number of the conference phone), and y = 1 to 9 (soft key number).
If the feature is quick_dial, this is the phone number that is dialed when you press the soft key.

Values: text string

Default: blank

Setting: `hs_settings.x.pfk.softkey.y.idle.account`

Description: Sets the account number to which the soft key feature applies, where x = 1 to 6 (device number of the conference phone), and y = 1 to 9 (soft key number).

Values: 0-3

Default: 0 (default account)

Setting:	`hs_settings.x.pfk.softkey.y.call_active.feature`		
Description:	Sets the features assigned to the soft keys on the call active screen, where x = 1 to 6 (device number of the conference phone), and y = 1 to 9 (soft key number).		
Values:	blank, new, end, hold, transfer, conf, pri_hold	**Default:**	y = 1: end y = 2: transfer y = 3: conf y = 4-9: blank

Setting:	`hs_settings.x.pfk.softkey.y.call_active.label`		
Description:	Sets the label of the soft keys on the call active screen, where x = 1 to 6 (device number of the conference phone), and y = 1 to 9 (soft key number). If left blank, the phone will display the default label for the selected feature (e.g. label “End” for the feature “end”)		
Values:	text string	**Default:**	blank

Setting:	`hs_settings.x.pfk.softkey.y.call_active.value`		
Description:	Sets the value for the soft key on the call active screen, where x = 1 to 6 (device number of the conference phone), and y = 1 to 9 (soft key number).		
Values:	text string	**Default:**	blank

Setting:	`hs_settings.x.pfk.softkey.y.call_active.account`		
Description:	Sets the account number to which the soft key feature applies, where x = 1 to 6 (device number of the conference phone), and y = 1 to 9 (soft key number).		
Values:	0-3	**Default:**	0 (default account)

Setting:	`hs_settings.x.pfk.softkey.y.call_held.feature`		
Description:	Sets the features assigned to the soft keys on the call held screen, where x = 1 to 6 (device number of the conference phone), and y = 1 to 9 (soft key number).		
Values:	blank, new, end, resume, transfer, conf, quick_dial	**Default:**	y = 1: end y = 2: new y = 3: resume y = 4: transfer y = 5: conf y = 6-9: blank

Setting:	`hs_settings.x.pfk.softkey.y.call_held.label`		
Description:	Sets the label of the soft keys on the call held screen, where x = 1 to 6 (device number of the conference phone), and y = 1 to 9 (soft key number). If left blank, the phone will display the default label for the selected feature (e.g. label “End” for the feature “end”)		
Values:	text string	**Default:**	blank

Setting:	`hs_settings.x.pfk.softkey.y.call_held.value`		
Description:	Sets the value for the soft key on the call held screen, where x = 1 to 6 (device number of the conference phone), and y = 1 to 9 (soft key number). If the feature is quick_dial, this is the phone number that is dialed when you press the soft key.		
Values:	text string	**Default:**	blank

Setting:	`hs_settings.x.pfk.softkey.y.call_held.account`		
Description:	Sets the account number to which the soft key feature applies, where x = 1 to 6 (device number of the conference phone), and y = 1 to 9 (soft key number).		
Values:	0-3	**Default:**	0 (default account)

Setting:	`hs_settings.x.pfk.softkey.y.live_dial.feature`		
Description:	Sets the features assigned to the soft keys on the live dial screen, where x = 1 to 6 (device number of the conference phone), and y = 1 to 9 (soft key number).		
Values:	blank, dir, call_log, redial, message, end, dial, select_line, cancel, backspc, quick_dial	**Default:**	y = 1: backspc y = 2: blank y = 3: dial y = 4: redial y = 5: dir y = 6-9: blank

Setting:	`hs_settings.x.pfk.softkey.y.live_dial.label`		
Description:	Sets the label of the soft keys on the live dial screen, where x = 1 to 6 (device number of the conference phone), and y = 1 to 9 (soft key number). If left blank, the phone will display the default label for the selected feature (e.g. label “Backspc” for the feature “backspc”)		
Values:	text string	**Default:**	blank

Setting:	`hs_settings.x.pfk.softkey.y.live_dial.value`		
Description:	Sets the value for the soft key on the live dial screen, where x = 1 to 6 (device number of the conference phone), and y = 1 to 9 (soft key number). If the feature is quick_dial, this is the phone number that is dialed when you press the soft key.		
Values:	text string	**Default:**	blank

Setting:	`hs_settings.x.pfk.softkey.y.live_dial.account`		
Description:	Sets the account number to which the soft key feature applies, where x = 1 to 6 (device number of the conference phone), and y = 1 to 9 (soft key number).		
Values:	0-3	**Default:**	0 (default account)

Setting: `hs_settings.autoreg_enable`

Description: Enable/disable HS auto registration

- If enabled, device with IPEI matching with **hs_settings.x.ipei** will be allowed to register without going through manual DECT registration
- Otherwise, device have to be registered through manual DECT registration
- See also parameters **hs_settings.x.ipei**, **system.x.registered_ipei**

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `hs_settings.handset_us_pin_code`

Description: Sets the new 4-digit PIN for device registration/deregistration.

Values: 4-digit number **Default:** 1590

Setting: `hs_settings.statistics_enable`

Description: Enable device use statistics gathering.

Values: 0 (disabled), 1 (enabled) **Default:** 1

Setting: `hs_settings.statistics_timer`

Description: Device statistics reporting interval.

Values: integer **Default:** 900

MAC-specific configuration file settings

Setting: `hs_settings.x.handset_name`

Description: Sets the name for device x. You can use up to 11 letters and/or numbers. Use alphanumeric characters only—no symbol characters are allowed.

Values: Text string **Default:** SPEAKER BOX (only if the device is a conference phone)

Setting:	`hs_settings.x.ipei`		
Description:	(where x ranges from 1-6) ■ Registration slot reserved for device with the same IPEI as the configured one. ■ Device with the same IPEI as the configured IPEI can register as Device x without going through manual DECT registration ■ See also parameters **hs_settings.autoreg_enable**, **system.x.registered_ipei**.		
Values:	String (IPEI)	**Default:**	blank

“system” Module: System settings

The system settings enables you to configure DECT related settings for the C620 SIP Wireless Conference Phone.

MAC-specific configuration file settings

Setting: `system.x.registered_ipei`

Description: This setting is **READ-ONLY**, and indicates handset/deskset registration status (for both auto & manual registration), where x ranges from 1-6 (device number).

- [blank] if no handset/deskset is registered to the slot

See also parameters **hs_settings.autoreg_enable** and **hs_settings.x.ipei**.

Values: N/A **Default:** N/A

"network" Module: Network Settings

The network settings follow the format: network.[element].

General configuration file settings

Setting:	`network.vlan.wan.enable`		
Description:	Enables or disables the WAN VLAN .		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`network.vlan.wan.id`		
Description:	Sets the WAN VLAN ID.		
Values:	0–4095	**Default:**	0

Setting:	`network.vlan.wan.priority`		
Description:	Sets the WAN port VLAN priority.		
Values:	0–7	**Default:**	0

Setting:	`network.lldp_med.enable`		
Description:	Enables or disables LLDP-MED.		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

Setting:	`network.lldp_med.interval`		
Description:	Sets the LLDP-MED packet interval (in seconds).		
Values:	1–30	**Default:**	30

Setting:	`network.dhcpv6_vendor_class_id`		
Description:	Sets the vendor ID for DHCPv6 option 16.		
Values:	Text string	**Default:**	C620

Setting:	`network.eapol.enable`		
Description:	Enables or disables 802.1x EAPOL.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`network.eapol.identity`		
Description:	Sets the 802.1x EAPOL identity.		
Values:	Text string	**Default:**	Blank

Setting:	`network.eapol.access_password`		
Description:	Sets the 802.1x EAPOL MD5 password. The parameter **provisioning.pwd_export_enable** enables/disables this password from being exported in plain text.		
Values:	Text string	**Default:**	Blank

Setting:	`network.vendor_class_id`		
Description:	Sets the vendor ID for DHCP option 60.		
Values:	Text string	**Default:**	snomC620

Setting:	`network.user_class`		
Description:	Sets the user class for DHCP option 77.		
Values:	Text string	**Default:**	snomC620

MAC-specific configuration file settings

Setting: `network.ip.mode`

Description: Sets the IPv4 network mode.

Values: disable, dhcp, static, pppoe **Default:** dhcp

Setting: `network.ip.static_ip_addr`

Description: Sets a static IP address for the network.

Values: Text string (IPv4) **Default:** Blank

Setting: `network.ip.subnet_mask`

Description: Sets the subnet mask for the network.

Values: Text string (IPv4) **Default:** Blank

Setting: `network.ip.gateway_addr`

Description: Sets the Gateway IP address.

Values: Text string (IPv4) **Default:** Blank

Setting: `network.ip.dns1`

Description: Sets the primary DNS server IP address.

Values: Text string (IPv4) **Default:** Blank

Setting: `network.ip.dns2`

Description: Sets the secondary DNS server IP address.

Values: Text string (IPv4) **Default:** Blank

Setting: `network.ip.manually_configure_dns`

Description: Enable or disable manual DNS configuration.

Values: 0 (disable), 1 (enable) **Default:** 0

Setting:	`network.ip.pppoe.service_name`		
Description:	If IPv4 mode is PPPoE, enter the name of the applicable PPPoE provider, in case more than one is available.		
Values:	Text string	**Default:**	Blank

Setting:	`network.ip.pppoe.username`		
Description:	If IPv4 mode is PPPoE, enter your PPPoE account username.		
Values:	Text string	**Default:**	Blank

Setting:	`network.ip.pppoe.access_password`		
Description:	If IPv4 mode is PPPoE, enter your PPPoE account password. The parameter **provisioning.pwd_export_enable** enables/disables this password from being exported in plain text.		
Values:	Text string	**Default:**	Blank

Setting:	`network.ip6.mode`		
Description:	Set the IPv6 network mode, depending on how the device will be assigned an IP address.		
Values:	disable, auto, static	**Default:**	disable

Setting:	`network.ip6.static_ip_addr`		
Description:	When IPv6 mode is static, enter the static IP address for the network.		
Values:	Text string (IPv6)	**Default:**	Blank

Setting:	`network.ip6.prefix`		
Description:	When IPv6 mode is static, enter the IPv6 address prefix length.		
Values:	0–128	**Default:**	64

Setting:	`network.ip6.gateway_addr`		
Description:	When IPv6 mode is static, enter the default gateway address.		
Values:	Text string (IPv6)	**Default:**	Blank

Setting:	`network.ip6.dns1`		
Description:	If manual DNS configuration is enabled, enter the address for the primary DNS server.		
Values:	Text string (IPv6)	**Default:**	Blank

Setting:	`network.ip6.dns2`		
Description:	If manual DNS configuration is enabled, enter the address for the secondary DNS server.		
Values:	Text string (IPv6)	**Default:**	Blank

Setting:	`network.ip6.manually_configure_dns`		
Description:	Enable or disable manual DNS configuration for IPv6.		
Values:	0 (disable), 1 (enable)	**Default:**	0

Setting:	`network.vpn.enable`		
Description:	Enables or disables the phone to connect using the OpenVPN client. For more information, see *"VPN" on page 71*.		
Values:	0 (disable), 1 (enable)	**Default:**	0

"provisioning" Module: Provisioning Settings

The provisioning settings follow the format: provisioning.[element].

All these settings are exported when you manually export the configuration from the C620.

General configuration file settings

Setting:	`provisioning.dhcp_option_enable`		
Description:	Enables or disables using DHCP options for locating the configuration and firmware files.		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

Setting:	`provisioning.dhcp_option_priority_1`		
Description:	Sets the first priority DHCP option for the provisioning/firmware file check.		
Values:	0, 66, 159, 160	**Default:**	66

Setting:	`provisioning.dhcp_option_priority_2`		
Description:	Sets the second priority DHCP option for the provisioning/firmware file check.		
Values:	0, 66, 159, 160	**Default:**	159

Setting:	`provisioning.dhcp_option_priority_3`		
Description:	Sets the third priority DHCP option for the provisioning/firmware file check.		
Values:	0, 66, 159, 160	**Default:**	160

Setting:	`provisioning.resync_mode`		
Description:	Sets the mode of the device's provisioning/firmware file check. This determines which files the device retrieves when the resync process begins.		
Values:	config_only, firmware_only, config_and_firmware	**Default:**	config_and_firmware

Setting:	`provisioning.bootup_check_enable`		
Description:	Enables or disables bootup check for configuration and firmware files.		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

Setting:	`provisioning.schedule_mode`		
Description:	Sets the type of schedule check for configuration and firmware files.		
Values:	disable, interval, weekday	**Default:**	disable

Setting:	`provisioning.resync_time`		
Description:	Sets the interval (in minutes) between checks for new firmware and/or configuration files.		
Values:	0–65535	**Default:**	0 (OFF)

Setting:	`provisioning.weekdays`		
Description:	Sets the day(s) when the device checks for new firmware and/or configuration files. Enter a comma-delimited list of weekdays from 0 (Sunday) to 6 (Saturday). For example, 5,6,0 means the provisioning check will be performed on Friday, Saturday and Sunday.		
Values:	text string	**Default:**	Blank

Setting:	`provisioning.weekdays_start_hr`		
Description:	Sets the hour when the device checks for new firmware and/or configuration files.		
Values:	0–23	**Default:**	0

Setting:	`provisioning.weekdays_end_hr`		
Description:	Sets the hour when the device stops checking for new firmware and/or configuration files.		
Values:	0–23	**Default:**	0

Setting: `provisioning.remote_check_sync_enable`

Description: Enables or disables remotely triggering the device to check for new firmware and/or configuration files. The file checking is triggered remotely via a SIP Notify message from the server containing the **check-sync** event.

Values: 0 (disabled), 1 (enabled) **Default:** 1

Setting: `provisioning.crypto_enable`

Description: Enables or disables encryption check for the configuration file(s). Enable if you have encrypted the configuration file(s) using AES encryption.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `provisioning.crypto_passphrase`

Description: Sets the AES encryption passphrase for decrypting the configuration file(s). Enter the key that was generated when you encrypted the file.

Values: Text string **Default:** Blank

Setting: `provisioning.check_trusted_certificate`

Description: Enables or disables accepting only a trusted TLS certificate for access to the provisioning server.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `provisioning.pnp_enable`

Description: Enables or disables the C620 checking for the provisioning URL using the Plug-and-Play Subscribe and Notify protocol.

Values: 0 (disabled), 1 (enabled) **Default:** 1

Setting: `provisioning.pnp_response_timeout`

Description: Sets how long the C620 repeats the SUBSCRIBE request if there is no reply from the PnP server.

Values: 1–60 **Default:** 10

Setting: `provisioning.pwd_export_enable`

Description: Enables or disables passwords from being exported in plain text. This parameter is not available on the WebUI. The passwords affected are:

- network.eapol.access_password
- network.ip.pppoe.access_password
- provisioning.fw_server_access_password
- provisioning.server_access_password
- profile.admin.access_password
- profile.user.access_password
- sip_account.x.authentication_access_password
- remoteDir.ldap_access_password

Values: 0 (disabled), 1 (enabled) **Default:** 0

MAC-specific configuration file settings

Setting: `provisioning.firmware_url`

Description: Sets the URL for the server hosting the firmware file.

Values: URI **Default:** Blank

Setting: `provisioning.handset_firmware_url`

Description: Sets the URL for the server hosting the handset firmware file.

Values: URI **Default:** Blank

Setting: `provisioning.fw_server_username`

Description: Sets the authentication name for the server hosting the firmware file.

Values: Text string **Default:** Blank

Setting: `provisioning.fw_server_access_password`

Description: Sets the authentication password for the server hosting the firmware file. The parameter **provisioning.pwd_export_enable** enables/disables this password from being exported in plain text.

Values: Text string **Default:** Blank

Setting: `provisioning.server_address`

Description: Sets the provisioning server IP address.

File fetching rules:

- If the provisioning server address is without a filename, e.g. http://<path>/ , the files to be retrieved by the base are:

  http://<path>/snomC620.htm
  http://<path>/snomC620-{mac}.htm

- If the provisioning server address is with a filename but without replacement variable, e.g. http://<path>/test.htm , the files to be retrieved by the base are:

  http://<path>/test.htm
  http://<path>/test-{mac}.htm

- If the provisioning server address is with a filename but with replacement variable, e.g. http://<path>/{mac}.htm , the files to be retrieved by the base are:

  http://<path>/{mac}.htm

Values: Text string **Default:** https://et.vtechphones.com/rg2/

Setting: `provisioning.server_username`

Description: Sets the authentication name for the provisioning server.

Values: Text string **Default:** Blank

Setting: `provisioning.server_access_password`

Description: Sets the authentication password for the provisioning server.
The parameter **provisioning.pwd_export_enable** enables/disables this password from being exported in plain text.

Values: Text string **Default:** Blank

"time_date" Module: Time and Date Settings

The time and date settings follow the format: time_date.[element].

All these settings are exported when you manually export the configuration from the C620.

All the time and date settings are included in the general configuration file.

Setting:	`time_date.date_format`		
Description:	Sets the format for displaying the date.		
Values:	DD/MM/YY, MM/DD/YY, YY/MM/DD	**Default:**	DD/MM/YY

Setting:	`time_date.24hr_clock`		
Description:	Enables or disables 24-hour clock.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`time_date.ntp_server`		
Description:	Enables or disables NTP server to set time and date.		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

Setting:	`time_date.ntp_server_addr`		
Description:	Sets the URL for the NTP server.		
Values:	IPv4, IPv6 or FQDN	**Default:**	us.pool.ntp.org

Setting:	`time_date.ntp_dhcp_option`		
Description:	Enables or disables DHCP option 42 to find the NTP server.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`time_date.selected_timezone`
Description:	Sets the local time zone.

Values:	Pacific/Pago_Pago, Pacific/Honolulu, America/Adak, America/Anchorage, America/Vancouver, America/Tijuana, America/Los_Angeles, America/Edmonton, America/Chihuahua, America/Denver, America/Phoenix, America/Winnipeg, Pacific/Easter, America/Mexico_City, America/Chicago, America/Nassau, America/Montreal, America/Grand_Turk, America/Havana, America/New_York, America/Caracas, America/Halifax, America/Santiago, America/Asuncion, Atlantic/Bermuda, Atlantic/Stanley, America/Port_of_Spain, America/St_Johns, America/Godthab, America/Argentina/Buenos_Aires, America/Fortaleza, America/Sao_Paulo, America/Noronha, Atlantic/Azores, GMT, America/Danmarkshavn, Atlantic/Faroe, Europe/Dublin, Europe/Lisbon, Atlantic/Canary, Europe/London, Africa/Casablanca, Europe/Tirane, Europe/Vienna, Europe/Brussels, Europe/Zagreb, Europe/Prague, Europe/Copenhagen, Europe/Paris, Europe/Berlin, Europe/Budapest, Europe/Rome, Europe/Luxembourg, Europe/Skopje, Europe/Amsterdam, Africa/Windhoek, Europe/Tallinn, Europe/Helsinki, Asia/Gaza, Europe/Athens, Asia/Jerusalem, Asia/Amman, Europe/Riga, Asia/Beirut, Europe/Chisinau, Europe/Kaliningrad, Europe/Bucharest, Asia/Damascus, Europe/Istanbul, Europe/Kiev, Africa/Djibouti, Asia/Baghdad, Europe/Moscow, Asia/Tehran, Asia/Yerevan, Asia/Baku, Asia/Tbilisi, Asia/Aqtau, Europe/Samara, Asia/Aqtobe, Asia/Bishkek, Asia/Karachi, Asia/Yekaterinburg, Asia/Kolkata, Asia/Almaty, Asia/Novosibirsk, Asia/Krasnoyarsk, Asia/Bangkok, Asia/Shanghai, Asia/Singapore, Australia/Perth, Asia/Seoul, Asia/Tokyo, Australia/Adelaide, Australia/Darwin, Australia/Sydney, Australia/Brisbane, Australia/Hobart, Asia/Vladivostok, Australia/Lord_Howe, Pacific/Noumea, Pacific/Auckland, Pacific/Chatham, Pacific/Tongatapu	**Default:**	America/New_York

Setting:	`time_date.daylight_saving_auto_adjust`		
Description:	Sets the device to automatically adjust clock for daylight savings.		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

Setting:	`time_date.daylight_saving_user_defined`		
Description:	Enables or disables manual daylight savings configuration.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`time_date.daylight_saving_start_month`		
Description:	Sets the month that daylight savings time starts.		
Values:	January, February, March, April, May, June, July, August, September, October, November, December	**Default:**	March

Setting:	`time_date.daylight_saving_start_week`		
Description:	Sets the week that daylight savings time starts.		
Values:	1–5	**Default:**	2

Setting:	`time_date.daylight_saving_start_day`		
Description:	Sets the day that daylight savings time starts.		
Values:	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday	**Default:**	Sunday

Setting:	`time_date.daylight_saving_start_hour`		
Description:	Sets the hour that daylight savings time starts.		
Values:	00:00, 01:00, 02:00, 03:00, 04:00, 05:00, 06:00, 07:00, 08:00, 09:00, 10:00, 11:00, 12:00, 13:00, 14:00, 15:00, 16:00, 17:00, 18:00, 19:00, 20:00, 21:00, 22:00, 23:00	**Default:**	02:00

Setting:	`time_date.daylight_saving_end_month`		
Description:	Sets the month that daylight savings time ends.		
Values:	January, February, March, April, May, June, July, August, September, October, November, December	**Default:**	November

Setting:	`time_date.daylight_saving_end_week`		
Description:	Sets the week that daylight savings time ends.		
Values:	1–5	**Default:**	1

Setting:	`time_date.daylight_saving_end_day`		
Description:	Sets the day that daylight savings time ends.		
Values:	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday	**Default:**	Sunday

Setting:	`time_date.daylight_saving_end_hour`		
Description:	Sets the hour that daylight savings time ends.		
Values:	00:00, 01:00, 02:00, 03:00, 04:00, 05:00, 06:00, 07:00, 08:00, 09:00, 10:00, 11:00, 12:00, 13:00, 14:00, 15:00, 16:00, 17:00, 18:00, 19:00, 20:00, 21:00, 22:00, 23:00	**Default:**	02:00

Setting:	`time_date.daylight_saving_amount`		
Description:	Sets the daylight savings time offset in minutes.		
Values:	0–255	**Default:**	60

Setting:	`time_date.timezone_dhcp_option`		
Description:	Enables or disables DHCP option 2/100/101 for determining time zone information.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`time_date.ntp_server_update_interval`		
Description:	Sets the delay between NTP server updates, in seconds.		
Values:	0–4294967295	**Default:**	1000

Setting:	`time_date.time_and_date`		
Description:	Manually sets the date and time. Use the format <year>-<month>-<day>T<hour>:<minute>:<second>		
Values:	<year>-<month>-<day>T <hour>:<minute>:<second>	**Default:**	2016-03-01T12:00:00

"log" Module: Log Settings

The log settings control system logging activities. System logging may be required for troubleshooting purposes. The following logging modes are supported:

- Serial/Console—system log output to an external console using a serial/RS-232 cable
- Syslog server—output to a log file on a separate server
- Volatile file

The log settings follow the format: log.[element].

All the log settings are included in the general configuration file.

Setting:	`log.syslog_enable`		
Description:	Enables or disables log output to syslog server.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`log.syslog_server_address`		
Description:	Sets the syslog server IP address.		
Values:	Text string (IPv4 or IPv6)	**Default:**	Blank

Setting:	`log.syslog_server_port`		
Description:	Sets the syslog server port.		
Values:	1–65535	**Default:**	514

Setting:	`log.syslog_level`		
Description:	Sets the log level. The higher the level, the larger the debug output. 5—all 4—debug 3—info 2—warning 1—error 0—critical		
Values:	0–5	**Default:**	2

"remoteDir" Module: Remote Directory Settings

The remote directory settings follow the format: remoteDir.[element].

All these settings are exported when you manually export the configuration from the C620.

All the remote directory settings are included in the general configuration file.

Setting:	`remoteDir.ldap_enable`		
Description:	Enables or disables the C620 SIP Wireless Conference Phone's access to the LDAP directory.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`remoteDir.ldap_directory_name`		
Description:	Sets the LDAP directory name.		
Values:	Text string	**Default:**	Blank

Setting:	`remoteDir.ldap_server_address`		
Description:	Sets the LDAP server IP address.		
Values:	Text string	**Default:**	Blank

Setting:	`remoteDir.ldap_port`		
Description:	Sets the LDAP server port.		
Values:	1–65535	**Default:**	389

Setting:	`remoteDir.ldap_protocol_version`		
Description:	Sets the LDAP protocol version.		
Values:	version_2, version_3	**Default:**	version_3

Setting:	`remoteDir.ldap_authentication_type`		
Description:	Sets the LDAP authentication type.		
Values:	simple, ssl	**Default:**	simple

Setting: `remoteDir.ldap_user_name`

Description: Sets the LDAP authentication user name.

Values: Text string **Default:** Blank

Setting: `remoteDir.ldap_access_password`

Description: Sets the LDAP authentication password.
The parameter **provisioning.pwd_export_enable** enables/disables this password from being exported in plain text.

Values: Text string **Default:** Blank

Setting: `remoteDir.ldap_base`

Description: Sets the LDAP search base. This sets where the search begins in the directory tree structure. Enter one or more attribute definitions, separated by commas (no spaces). Your directory may include attributes like "cn" (common name) or "ou" (organizational unit) or "dc" (domain component). For example, ou=accounting,dc=snom,dc=com

Values: Text string **Default:** Blank

Setting: `remoteDir.ldap_max_hits`

Description: Sets the maximum number of entries returned for an LDAP search. Limiting the number of hits can conserve network bandwidth.

Values: 0–32000 **Default:** 200

Setting: `remoteDir.ldap_search_delay`

Description: Sets the LDAP maximum search delay in seconds.

Values: 0–500 **Default:** 0

Setting: `remoteDir.ldap_firstname_filter`

Description: Sets the LDAP first name attribute filter.

Values: Text string **Default:** Blank

Setting: `remoteDir.ldap_lastname_filter`

Description: Sets the LDAP last name attribute filter.

Values: Text string **Default:** Blank

Setting: `remoteDir.ldap_number_filter`

Description: Sets the LDAP number filter.

Values: Text string **Default:** Blank

Setting: `remoteDir.ldap_firstname_attribute`

Description: Sets the name attributes. Enter the name attributes that you want the C620 to display for each entry returned after an LDAP search. Separate each attribute with a space. For example, givenName sn will display the first name and surname for each entry.

Values: Text string **Default:** Blank

Setting: `remoteDir.ldap_lastname_attribute`

Description: Sets the last name attributes.

Values: Text string **Default:** Blank

Setting: `remoteDir.ldap_work_number_attributes`

Description: Sets the number attributes. Enter the number attributes that you want the C620 to display for each entry returned after an LDAP search. Separate each attribute with a space. For example, telephoneNumber mobile will display the work phone number and mobile phone number for each entry.

Values: Text string **Default:** Blank

Setting: `remoteDir.ldap_mobile_number_attributes`

Description: Sets the mobile number attributes.

Values: Text string **Default:** Blank

Setting: `remoteDir.ldap_other_number_attributes`

Description: Sets the “other” number attributes.

Values: Text string **Default:** Blank

Setting: `remoteDir.ldap_incall_lookup_enable`

Description: Enables or disables LDAP incoming call lookup. If enabled, the C620 searches the LDAP directory for the incoming call number. If the number is found, the C620 uses the LDAP entry for CID info.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `remoteDir.ldap_outcall_lookup_enable`

Description: Enables or disables LDAP outgoing call lookup. If enabled, numbers entered in pre-dial or live dial are matched against LDAP entries. If a match is found, the LDAP entry is displayed for dialing.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `remoteDir.ldap_check_certificate`

Description: Enables or disables accepting only a trusted LDAP certificate.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `remoteDir.xml.x.name`

Description: Sets the name of the directory as it will appear on the phone‘s Directory list. For this and following parameters, x is the number of the XML directory (1–3).

Values: Text string **Default:** Blank

Setting: `remoteDir.xml.x.uri`

Description: The location of the XML directory file, from which the phone will sync and retrieve directory entries.

Values: URI **Default:** Blank

Setting: `remoteDir.xml.x.call_lookup_enable`

Description: Enables/disables the call lookup feature for incoming and outgoing calls.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `remoteDir.xml.x.contact_entry_tag`

Description: Sets the tag name for directory entry.

Values: Text string **Default:** DIR_ENTRY

Setting:	`remoteDir.xml.x.first_name_tag`		
Description:	Sets the first name tag for a directory entry.		
Values:	Text string	**Default:**	DIR_ENTRY_NAME_FIRST

Setting:	`remoteDir.xml.x.last_name_tag`		
Description:	Sets the last name tag for a directory entry.		
Values:	Text string	**Default:**	DIR_ENTRY_NAME_LAST

Setting:	`remoteDir.xml.x.work_number_tag`		
Description:	Sets the work number tag for a directory entry.		
Values:	Text string	**Default:**	DIR_ENTRY_NUMBER_WORK

Setting:	`remoteDir.xml.x.mobile_number_tag`		
Description:	Sets the mobile number tag for a directory entry.		
Values:	Text string	**Default:**	DIR_ENTRY_NUMBER_MOBILE

Setting:	`remoteDir.xml.x.other_number_tag`		
Description:	Sets the other number tag for a directory entry.		
Values:	Text string	**Default:**	DIR_ENTRY_NUMBER_OTHER

"web" Module: Web Settings

The web settings control the web server IP, port, and security settings.

The web settings follow the format: web.[element].

All the Web settings are included in the general configuration file.

Setting:	`web.server_enable`		
Description:	Enables or disables the availability of the phone's embedded WebUI.		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

Setting:	`web.http_port`		
Description:	Sets the http port when http is enabled.		
Values:	1–65535	**Default:**	80

Setting:	`web.https_enable`		
Description:	Sets server to use the https protocol.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`web.https_port`		
Description:	Sets the https port when https is enabled.		
Values:	1–65535	**Default:**	443

“trusted_ip” Module: Trusted IP Settings

The trusted_ip settings provide enhanced security for the C620. When enabled, these settings can filter network traffic and reject any traffic from unauthorized sources.

The trusted_ip settings follow the format: trusted_ip.[element].

All the trusted_ip settings are included in the general configuration file.

Setting:	`trusted_ip.only_accept_allowed_ip`		
Description:	Enables or disables using the Allowed IP list to filter network traffic. When enabled, all unsolicited IP traffic will be blocked unless it is from one of the trusted IP addresses on the "Allowed IP" list.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`trusted_ip.x.allow_ip`		
Description:	Enter an IP address or address range for one instance of the “Allowed IP” list. x ranges from 1 to 10. See *“Trusted IP” on page 102* for more information.		
Values:	Text string (IPv4 or IPv6, IP range in IPv4 or IPv6)	**Default:**	Blank

“trusted_servers” Module: Trusted Server Settings

The trusted_servers settings provide enhanced security for the C620. When enabled, these settings can filter network traffic and reject any traffic from unauthorized sources.

The trusted_servers settings follow the format: trusted_servers.[element].

All the trusted_servers settings are included in the general configuration file.

Setting:	`trusted_servers.only_accept_sip_account_servers`		
Description:	Enables or disables using each enabled account's Registration server, SIP server, Outbound Proxy server and Backup Outbound Proxy server as sources for trusted SIP traffic.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

"user_pref" Module: User Preference Settings

The user preference settings are accessible to the C620 user. These settings are useful for initial setup. You may wish to remove these settings from auto-provisioning update files so that users do not have their own settings overwritten.

The user preference settings follow the format: user_pref.[element].

General configuration file settings

Setting: `user_pref.account.x.diversion_display`

Description: Enables or disables the display of diversion <name-addr> info (if available) for calls forwarded to account x.

Values: 0 (disabled), 1 (enabled) **Default:** 1

Setting: `user_pref.feature_access_code_on_sip_registered_enable`

Description: Enables or disables Feature Access Code (FAC) call sending out after registration succeeded. If enabled, then allow FAC call to be sent only if user changes corresponding status locally.

Values: 0 (disabled), 1 (enabled) **Default:** 0

MAC-specific configuration file settings

Setting: `user_pref.web_language`

Description: Sets the language that appears on the WebUI.

Values: en (English),
fr (French),
es (Spanish),
it (Italian),
pt (Portuguese),
nl (Dutch),
de (German),
el (Greek),
ru (Russian),
tr (Turkish),
pl (Polish),
en-GB (English-United Kingdom),
fr-CA (French-Canada),
es-MX (Spanish-Mexico).

Default: en

"call_settings" Module: Call Settings

The call settings configure data related to a user's call preferences. The data is stored internally at /mnt/flash/CallSettings.xml.

All the call settings (except one) follow the format: call_settings.account.x.[element] where x is an account number ranging from 1 to 3.

General configuration file settings

Setting: `call_settings.early_media_preferred`

Description: Controls what to do when 180 Ringing message is received after 183 Session Progress message (SDP): ignore it and continue with early media (1), or switch to local RBT (0).

- when set to 1, after 183 is received, early media will be played on handset even if 180 is received afterward.
- when set to 0, local ringback tone will be played if 180 is received after 183.

Values: 0, 1 **Default:** 0

MAC-specific file settings

Setting: `call_settings.account.x.block_anonymous_enable`

Description: Enables or disables anonymous call blocking.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `call_settings.account.x.outgoing_anonymous_enable`

Description: Enables or disables outgoing anonymous calls.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `call_settings.account.x.dnd_enable`

Description: Enables or disables Do Not Disturb for account x.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting:	`call_settings.account.x.call_fwd_always_enable`		
Description:	Enables or disables Call Forward Always for account x.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`call_settings.account.x.call_fwd_always_target`		
Description:	Sets the Call Forward Always target number for account x.		
Values:	Text string	**Default:**	Blank

Setting:	`call_settings.account.x.call_fwd_busy_enable`		
Description:	Enables or disables Call Forward Busy for account x.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`call_settings.account.x.call_fwd_busy_target`		
Description:	Sets the Call Forward Busy target number for account x.		
Values:	Text string	**Default:**	Blank

Setting:	`call_settings.account.x.cfna_enable`		
Description:	Enables or disables Call Forward No Answer for account x.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`call_settings.account.x.cfna_target`		
Description:	Sets the Call Forward No Answer target number for account x.		
Values:	Text string	**Default:**	Blank

Setting:	`call_settings.account.x.cfna_delay`		
Description:	Sets the Call Forward No Answer delay (in number of rings) for account x.		
Values:	1–10	**Default:**	6

“audio” Module: Audio Settings

The audio settings include jitter buffer parameters and RTP port settings.

All the audio settings are included in the general configuration file.

Setting:	`audio.x.jitter_mode`		
Description:	Select the desired mode for the jitter buffer: fixed (static) or adaptive. This setting depends on your network environment and conditions.		
Values:	fixed, adaptive	**Default:**	adaptive

Setting:	`audio.x.fixed_jitter.delay`		
Description:	When in fixed jitter buffer mode, set the delay (in ms) desirable to provide good audio quality with the minimal possible delay.		
Values:	30–500	**Default:**	70

Setting:	`audio.x.adaptive_jitter.min_delay`		
Description:	When in adaptive jitter buffer mode, set the minimum delay (in ms) desirable to maintain data packet capture and audio quality.		
Values:	20–250	**Default:**	60

Setting:	`audio.x.adaptive_jitter.target_delay`		
Description:	When in adaptive jitter buffer mode, set the target delay (in ms) desirable to provide good audio quality with the minimal possible delay.		
Values:	20–500	**Default:**	80

Setting:	`audio.x.adaptive_jitter.max_delay`		
Description:	When in adaptive jitter buffer mode, set the maximum delay (in ms) desirable to maintain data packet capture and audio quality.		
Values:	180–500	**Default:**	240

Setting:	`audio.x.rtp.port_start`		
Description:	Sets the Local RTP port range start.		
Values:	1–65535	**Default:**	18000

Setting:	`audio.x.rtp.port_end`		
Description:	Sets the Local RTP port range end.		
Values:	1–65535	**Default:**	19000

Setting:	`audio.rtcp_xr.enable`		
Description:	Enables or disables reporting of RTCP XR via SIP to a collector server. RTP Control Protocol Extended Reports (RTCP XR) are used for voice quality assessment and diagnostics.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

"file" Module: Imported File Settings

The "file" parameters enable the provisioning file to import additional configuration files of various types, including:

- Contact lists
- Security certificates

The following certificates are supported:

- Per-account TLS certificate (you can choose to use the Account 1 certificate for all accounts)
- LDAP
- Web server (the C620 has a default self-signed web server certificate)
- Provisioning
- Languages

File parameter values are URLs that direct the C620 to the location of the file to be imported.

None of these settings are exported when you manually export the configuration from the C620.

General configuration file settings

Setting:	`file.certificate.x.url`		
Description:	URL to upload a trusted certificate file in pem or crt. It will be given index x and marked as unprotected. x ranges from 1 to 20. This parameter is **NON-EXPORTABLE**.		
Values:	URI	**Default:**	Blank

Setting:	`file.protected_certificate.x.url`		
Description:	URL to upload a trusted certificate file in pem or crt. It will be given index x and marked as protected. x ranges from 1 to 20. This parameter is **NON-EXPORTABLE**.		
Values:	URI	**Default:**	Blank

Setting: `file.certificate.trusted.url`

Description: URL to upload a trusted certificate file in pem or crt. It will be given the first available index and marked as unprotected. For example, <protocol>://<user>:<password>@<host>:<port>/<url-path>
This parameter is **NON-EXPORTABLE**.

Values: URI **Default:** Blank

Setting: `file.protected_certificate.trusted.url`

Description: URL to upload a trusted certificate file in pem or crt. It will be given the first available index and marked as protected. For example, <protocol>://<user>:<password>@<host>:<port>/<url-path>
This parameter is **NON-EXPORTABLE**.

Values: URI **Default:** Blank

Setting: `file.protected_certificate.custom_device.url`

Description: URL to upload a custom device certificate to override the factory installed device certificate. For example, <protocol>://<user>:<password>@<host>:<port>/<url-path>
This parameter is **NON-EXPORTABLE**.

Values: URI **Default:** Blank

Setting: `file.action`

Description: Enables you to delete certain certificates.

- removecertificate_customdevice: remove the custom device certificate and resume the use of the factory installed device certificate
- removecertificate_allnonprotected: remove all non-protected trusted certificates
- removecertificate_all: remove the custom device certificate and all protected or non-protected trusted certificates

Enables you to delete a custom language from the WebUI, the deskset screens, or both.
This parameter is **NON-EXPORTABLE**.

Values: removecertificate_customdevice, removecertificate_allnonprotected, removecertificate_all removecustomlanguage_all, removecustomlanguage_webui **Default:** Blank

Setting:	`file.vpn.advanced_config`		
Description:	URL of OpenVPN client configuration file. For more information, see *"VPN" on page 71*. This parameter is **NON-EXPORTABLE**.		
Values:	URI	**Default:**	Blank

Setting:	`file.language.desksetui.url`		
Description:	Sets the custom WebUI language. This parameter is **NON-EXPORTABLE**.		
Values:	URI	**Default:**	blank

MAC-specific configuration file settings

Setting:	`file.contact.directory.append`		
Description:	URL of contact directory to be imported. Entries in the imported file will be added to existing directory entries. This parameter is **NON-EXPORTABLE**.		
Values:	URI	**Default:**	Blank

Setting:	`file.contact.directory.overwrite`		
Description:	URL of contact directory to be imported. Entries in the imported file will replace all existing directory entries. This parameter is **NON-EXPORTABLE**.		
Values:	URI	**Default:**	Blank

Setting:	`file.contact.blacklist.append`		
Description:	URL of contact blacklist to be imported. Entries in the imported file will be added to existing blacklist entries. This parameter is **NON-EXPORTABLE**.		
Values:	URI	**Default:**	Blank

Setting:	`file.contact.blacklist.overwrite`		
Description:	URL of contact blacklist to be imported. Entries in the imported file will replace all existing blacklist directory entries. This parameter is **NON-EXPORTABLE**.		
Values:	URI	**Default:**	Blank

“xml_app” Module: XML App Settings

The C620 supports both push and pull server applications. The XML app settings allow you to enable “push” events and how they interact with the phone during calls.

The XML app settings are included in the general configuration file.

Setting:	`xml_app.http_push_enable`		
Description:	Enable or disable HTTP push, which enables the phone to display XML objects that are “pushed” to the phone from the server via http/https POST or SIP NOTIFY.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`xml_app.push_during_call_enable`		
Description:	Enable or disable the phone to display pushed XML objects during a call. Otherwise, the XML application is displayed after the call is over.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

“tr069” Module: TR-069 Settings

The Broadband Forum’s Technical Report 069 (TR-069) defines a protocol for remote management and secure auto-configuration of compatible devices. The TR-069 settings allow you to enable TR-069 and configure access to an auto-configuration server (ACS).

All the TR-069 settings are included in the general configuration file.

Setting:	`tr069.enable`		
Description:	Enable/disable the TR-069 subsystem.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`tr069.acs.url`		
Description:	Enter the URL to the auto configuration server (ACS).		
Values:	Text string	**Default:**	Blank

Setting:	`tr069.acs.username`		
Description:	Enter user name for ACS authentication.		
Values:	Text string	**Default:**	Blank

Setting:	`tr069.acs.access_password`		
Description:	Enter password for ACS authentication.		
Values:	Text string	**Default:**	Blank

Setting:	`tr069.periodic_inform.enable`		
Description:	Enable/disable the phone sending Inform messages to the server.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`tr069.periodic_inform.interval`		
Description:	Set the interval (in seconds) between sending Inform messages.		
Values:	1–65535	**Default:**	3600

Setting:	`tr069.connection_request.username`		
Description:	Set the user name for authenticating the connection sent from the ACS.		
Values:	Text string	**Default:**	Blank

Setting:	`tr069.connection_request.access_password`		
Description:	Set the password for authenticating the connection sent from the ACS.		
Values:	Text string	**Default:**	Blank

"tone" Module: Tone Definition Settings

The Tone Definition settings configure data for various tones for the purpose of localization. The Audio Manager component uses the data from this model to populate the mcu on bootup.

Each tone definition must be a string of 12 elements separated by a space:

```
"<num of freq> <freq1> <amp1> <freq2> <amp2> <freq3> <amp3> <freq4> <amp4>
<on duration> <off duration> <repeat count>"
```

Where:

```
<num of freq>: 0-4

<freq1>: 0-65535

<amp1>: -32768-32767

<freq2>: 0-65535

<amp2>: -32768-32767

<freq3>: 0-65535

<amp3>: -32768-32767

<freq4>: 0-65535

<amp4>: -32768-32767

<on duration>: 0-2^32

<off duration>: 0-2^32

<repeat count>: 0-65535
```

All the tone definition settings are included in the general configuration file.

Setting:	`tone.inside_dial_tone.num_of_elements`		
Description:	Sets the number of tone elements for the dial tone.		
Values:	1–5	**Default:**	1

Setting:	`tone.inside_dial_tone.element.1`		
Description:	Defines the inside dial tone element 1.		
Values:	Tone element string	**Default:**	2 440 -22 350 -22 0 0 0 0 65535 0 65535

Setting:	`tone.inside_dial_tone.element.x`		
Description:	Defines the inside dial tone element x (x = 2–5).		
Values:	Tone element string	**Default:**	Blank

Setting:	`tone.inside_dial_tone.num_of_repeat_all`		
Description:	Sets the number of repeats of all elements in sequence; that is, repeating back to the first element.		
Values:	0–65535	**Default:**	0

Setting:	`tone.stutter_dial_tone.num_of_elements`		
Description:	Sets the number of tone elements for the stutter dial tone.		
Values:	1–5	**Default:**	2

Setting:	`tone.stutter_dial_dial_tone.element.1`		
Description:	Defines the stutter dial tone element 1.		
Values:	Tone element string	**Default:**	2 440 -22 350 -22 0 0 0 0 100 100 10

Setting:	`tone.stutter_dial_dial_tone.element.2`		
Description:	Defines the stutter dial tone element 2.		
Values:	Tone element string	**Default:**	2 440 -22 350 -22 0 0 0 0 65535 065535

Setting:	`tone.stutter_dial_tone.element.x`		
Description:	Defines the stutter dial tone element x (x = 3–5).		
Values:	Tone element string	**Default:**	Blank

Setting:	`tone.stutter_dial_tone.num_of_repeat_all`		
Description:	Sets the number of repeats of all elements in sequence; that is, repeating back to the first element.		
Values:	0–65535	**Default:**	0

Setting:	`tone.busy_tone.num_of_elements`		
Description:	Sets the number of tone elements for the busy tone.		
Values:	1–5	**Default:**	1

Setting:	`tone.busy_tone.element.1`		
Description:	Defines the busy tone element 1.		
Values:	Tone element string	**Default:**	2 480 -22 620 -22 0 0 0 0 375 375 65535

Setting:	`tone.busy_tone.element.x`		
Description:	Defines the busy tone element x (x = 2–5).		
Values:	Tone element string	**Default:**	Blank

Setting:	`tone.busy_tone.num_of_repeat_all`		
Description:	Sets the number of repeats of all elements in sequence; that is, repeating back to the first element.		
Values:	0–65535	**Default:**	0

Setting:	`tone.ring_back_tone.num_of_elements`		
Description:	Sets the number of tone elements for the ringback tone.		
Values:	1–5	**Default:**	2

Setting:	`tone.ring_back_tone.element.1`		
Description:	Defines the ringback tone element 1.		
Values:	Tone element string	**Default:**	2 440 -22 480 -22 0 0 0 0 400 200 1

Setting:	`tone.ring_back_tone.element.2`		
Description:	Defines the ringback tone element 2.		
Values:	Tone element string	**Default:**	2 440 -22 480 -22 0 0 0 0 400 2000 1

Setting: `tone.ring_back_tone.element.x`

Description: Defines the ringback tone element x (x = 3–5).

Values: Tone element string **Default:** Blank

Setting: `tone.ring_back_tone.num_of_repeat_all`

Description: Sets the number of repeats of all elements in sequence; that is, repeating back to the first element.

Values: 0–65535 **Default:** 65535

Setting: `tone.congestion_tone.num_of_elements`

Description: Sets the number of tone elements for the congestion tone.

Values: 1–5 **Default:** 3

Setting: `tone.congestion_tone.element.1`

Description: Defines the dial tone element 1.

Values: Tone element string **Default:** 1 950 -22 0 0 0 0 0 0 330 0 1

Setting: `tone.congestion_tone.element.2`

Description: Defines the dial tone element 2.

Values: Tone element string **Default:** 1 1400 -22 0 0 0 0 0 0 330 0 1

Setting: `tone.congestion_tone.element.3`

Description: Defines the dial tone element 3.

Values: Tone element string **Default:** 1 1800 -22 0 0 0 0 0 0 330 1000 1

Setting: `tone.congestion_tone.element.x`

Description: Defines the dial tone element x (x = 4–5).

Values: Tone element string **Default:** Blank

Setting:	`tone.congestion_tone.num_of_repeat_all`		
Description:	Sets the number of repeats of all elements in sequence; that is, repeating back to the first element.		
Values:	0–65535	**Default:**	65535

Setting:	`tone.dial_tone.num_of_elements`		
Description:	Sets the number of tone elements for the dial tone.		
Values:	1–5	**Default:**	1

Setting:	`tone.dial_tone.element.1`		
Description:	Defines the dial tone element 1.		
Values:	Tone element string	**Default:**	2 440 -22 350 -22 0 0 0 0 65535 0 65535

Setting:	`tone.dial_tone.element.x`		
Description:	Defines the dial tone element x (x = 2–5).		
Values:	Tone element string	**Default:**	Blank

Setting:	`tone.dial_tone.num_of_repeat_all`		
Description:	Sets the number of repeats of all elements in sequence; that is, repeating back to the first element.		
Values:	0–65535	**Default:**	0

"profile" Module: Password Settings

The password settings allow you to set the default administrator and user passwords in the configuration file. The administrator password is usually included in the general configuration file, while the user password is usually included in the MAC-specific configuration file. The passwords can also be set using the WebUI. Be aware that scheduled provisioning configuration file updates may reset these passwords.

General configuration file settings

Setting: `profile.admin.access_password`

Description: Sets the administrator password for accessing the admin menus on the conference phone and the WebUI.
The parameter **provisioning.pwd_export_enable** enables/disables this password from being exported in plain text.

Values: Text string (15 characters maximum) **Default:** admin

Setting: `profile.support.access_password`

Description: Sets the support password for accessing the DECT Statistics page on the WUI: http(s)://<host:port>/dect_statistics.kl1. This password can only be set via provisioning.
The parameter **provisioning.pwd_export_enable** enables/disables this password from being exported in plain text.

Values: Text string (15 characters maximum) **Default:** support

MAC-specific configuration file settings

Setting: `profile.user.access_password`

Description: Sets the user password for logging on to the WebUI and editing user-accessible settings.
The parameter **provisioning.pwd_export_enable** enables/disables this password from being exported in plain text.

Values: Text string (15 characters maximum) **Default:** user

Setting: `profile.enable_password_strength_check`

Description: If enabled, the C620 will enforce password strength criteria when the admin, support and/or user passwords are changed.

Passwords must have at least 8 characters, including at least one of each:

- uppercase letter (A-Z)
- lowercase letter (a-z)
- special character (!%&*()_+|~-=\`{}[]:";'<>?,/)
- number (0-9)

NOTE: This parameter is ONLY for enforcing password strength when a password is changed. This parameter is not applied to existing passwords that do not fulfill the password strength criteria.

This parameter is **NON-EXPORTABLE**.

Values: 0 (disabled), 1 (enabled) **Default:** 0

"speed_dial" Module: Speed Dial Settings

The custom speed dial settings enable you to program up to 10 numbers that the phone user dials frequently.

The speed dial settings follow the format speed_dial.x.[element] , where x is the speed dial entry number that matches the dial pad key (0-9).

All the speed dial settings are included in the general configuration file.

Setting:	`speed_dial.x.account`		
Description:	Sets the account that the speed dial key uses to dial the number. 0 = default account. 1-3 = account number.		
Values:	0-3	**Default:**	0

Setting:	`speed_dial.x.name`		
Description:	Sets the name of the speed dial entry.		
Values:	text string	**Default:**	blank

Setting:	`speed_dial.x.number`		
Description:	Sets the number to be dialed.		
Values:	text string	**Default:**	blank

CHAPTER 6

TROUBLESHOOTING

If you have difficulty with your C620 SIP Wireless Conference Phone, please try the suggestions below.

NOTE For customer service or product information, contact the person who installed your system. If your installer is unavailable, visit our website at *www.snomamericas.com*.

Common Troubleshooting Procedures

Follow these procedures to resolve common issues. For more troubleshooting information, see the user's manual for your product.

The firmware upgrade or configuration update isn't working.

- Before using the WebUI, ensure you have the latest version of your web browser installed. Some menus and controls in older browsers may operate differently than described in this manual.
- Ensure you have specified the correct path to the firmware and configuration files on the **SERVICING > Firmware Upgrade > Auto Upgrade** page and the **SERVICING > Provisioning** page.
- If the phone is not downloading a MAC-specific configuration file, ensure the filename is all upper case.
- Ensure you are using the correct firmware version for the correct device.

Provisioning: "Use DHCP Option" is enabled, but the C620 is not getting a provisioning URL from the DHCP Server.

- Ensure that DHCP is enabled in Network settings.

APPENDIXES

Appendix A: Maintenance

Taking care of your products

- Your C620 SIP Wireless Conference Phone contains sophisticated electronic parts, so you must treat it with care.
- Avoid rough treatment.
- Place the conference phone in the charging dock gently.
- Save the original packing materials to protect your C620 SIP Wireless Conference Phone if you ever need to ship it.

Avoid water

- You can damage your C620 SIP Wireless Conference Phone if it gets wet. Do not install the C620 SIP Wireless Conference Phone near a sink, bathtub or shower.

Electrical storms

- Electrical storms can sometimes cause power surges harmful to electronic equipment. For your own safety, take caution when using electric appliances during storms.

Cleaning your products

- Your C620 SIP Wireless Conference Phone has a durable plastic casing that should retain its luster for many years. Clean it only with a soft cloth slightly dampened with water or a mild soap.
- Do not use excess water or cleaning solvents of any kind.

Remember that electrical appliances can cause serious injury if used when you are wet or standing in water. If the C620 SIP Wireless Conference Phone should fall into water, DO NOT RETRIEVE IT UNTIL YOU UNPLUG THE POWER CORD AND NETWORK CABLE FROM THE WALL, then pull the unit out by the unplugged cords.

Appendix B: GNU General Public License

COPYRIGHT NOTICE AND WARRANTY DISCLAIMER

I.

This Product contains Software applicable to GNU General Public License, Version 2 which can be used freely.

II.

Towards the licensor of this Software the following liability is disclaimed:

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

III.

The GNU General Public License is as follows:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330
Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author‘s protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone‘s free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program‘s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range

of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR

A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program‘s name and a brief idea of what it does>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

IV.

If requested by you, the complete corresponding source code of the Software can be sent by Snom Technology GmbH on a standard data storage medium against the reimbursement of the manufacturing costs of EUR 10.- per unit.

The complete corresponding source code of the Software can also be downloaded from our web site
https://www.snom.com/en/footer/discover-snom/gtc/source-code-gpl-open-source/.

V.

For further information see *http://www.snom.com*.