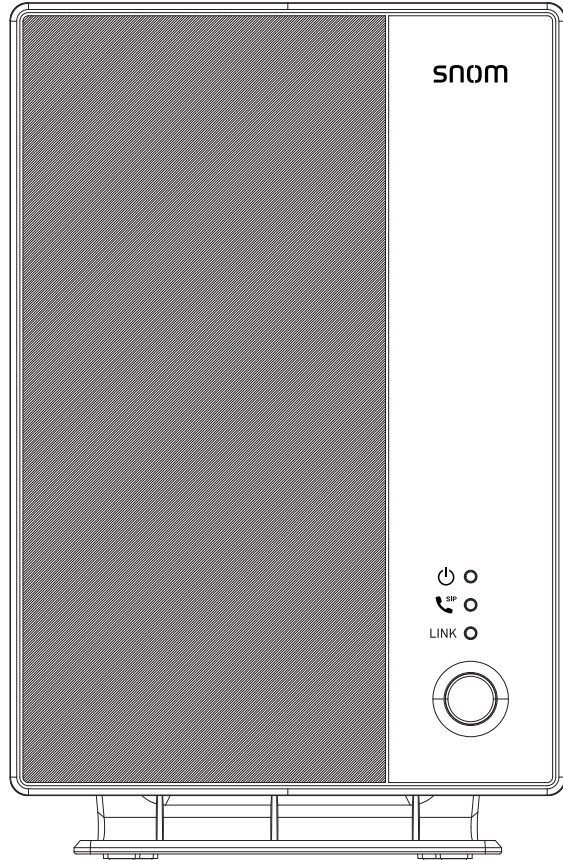


snom



M500

Dual-cell SIP DECT Base Station Administrator and Provisioning Manual

CONTENTS

Preface	7
Text Conventions	8
Audience.....	8
Related Documents	8
Introducing the M500	9
About the M500 Dual-cell SIP DECT Base Station	10
Quick Reference Guide	12
M500 Base station – Front view	12
M500 Base Station LEDs	13
M500 Base station – Rear view	16
M55 Handset	17
M56 Handset	18
M58 Deskset.....	20
Network Requirements	21
M500 Configuration Methods	22
How to set the base station operating mode or factory reset using the LINK button.....	23
How to configure site-wide vs. local settings in a M500 dual cell configuration.....	25
Site-wide vs. Local settings	25
WebUI	25
Provisioning.....	26
Exporting settings.....	27
Using Shared Calls	28
Configuration Using the Phone Menus	31
Viewing the Main Menu	32
Using the Status menu	32
Viewing Line status.....	35
Using the WebUI.....	37
Using the Web User Interface (WebUI)	38
How to identify the IP address of an M500 base station.....	39
How to access the WebUI	40
Status Page	42
System Status.....	42

Cordless Registrations.....	44
Register Handset	44
Manual Registration	44
Auto Registration.....	44
Cordless Registrations	45
Cordless Status	45
Base Status	46
Cordless Upgrade Status.....	47
System Pages	49
SIP Account Management	49
Registration tab	49
General Account Settings	49
SIP Server Settings	50
Registration Settings.....	51
Outbound Proxy Settings.....	51
Backup Outbound Proxy Settings.....	51
Features tab	52
Feature Access Codes Settings.....	52
Account Settings.....	53
Dial Plan	54
Voicemail Settings	55
Music On Hold Settings	56
XSI.....	56
Audio tab	57
Audio Settings.....	57
Voice Settings	58
Quality of Service.....	58
Jitter Buffer	58
Signaling tab	59
Signaling Settings	59
Caller Identity Settings.....	60
Session Timer	60
Keep Alive.....	60
NAT Traversal	61
Call Settings tab	61
General Call Settings.....	62
Do Not Disturb	62
Call Forward	62
Call Waiting.....	63
Base Preferences	64
General Base Settings	64
Audio	65
User Preferences.....	66
General User Settings.....	66
Device Preferences	66
Keys tab	67
PFK	67
M55 / M56 / M58 PFK.....	67
Type setting	68
Default PFK configuration.....	70
Speed dial.....	71
Wallpaper & Theme tab.....	72

Custom Wallpaper	72
Wallpaper & Theme on All Devices.....	73
Call Settings tab	73
Call Privacy for KeyLine.....	73
Paging Configuration	75
Group Members	75
Multicast	76
Alarm	76
Alarm.....	76
M56 Handset.....	78
Alarm Profiles	79
Network Pages	80
Basic Network Settings.....	81
IPv4	81
IPv6	82
Advanced Network Settings.....	83
VLAN.....	83
LLDP-MED	84
802.1x	84
Contacts Pages	86
Base Directory	86
Create Local Directory Entry	89
Directory Import/Export	89
Blocked List	90
Create Blocked List Entry.....	92
Blocked List/Blacklist Import/Export	93
LDAP	94
LDAP Settings.....	94
Broadsoft directory.....	97
Directory Type	97
Remote XML.....	98
Remote XML Directory Format.....	98
Servicing Pages.....	100
Reboot.....	100
Time and Date	100
Time and Date Format	102
Network Time Settings	102
Time Zone and Daylight Savings Settings	102
Custom Language	104
Firmware Upgrade	105
Auto Upgrade	105
Firmware Server Settings	105
Manual Firmware Update and Upload	107
Updating the base station	107
Updating handsets/desksets	108
Provisioning	110
Provisioning Server	111
Plug-and-Play Settings.....	111
DHCP Settings	112
Resynchronization.....	112
Import Configuration.....	115

- Export Configuration 115
- Reset Configuration 116
- Security 117
 - Passwords 117
 - Web Server 119
 - Cordless Pin Code 119
 - Trusted Servers 119
 - Trusted IP 120
- Certificates 121
 - Device Certificate 122
 - Trusted Certificate 122
- TR-369 Settings 124
- System Logs 125
 - Syslog Settings 125
 - Network Trace 126
 - Download Log 127
 - SIP Trace 128

Provisioning Using Configuration Files 129

- The Provisioning Process 130
 - Resynchronization: configuration file checking 131
 - M500 restart 131
- Configuration File 132
- Data Files 133
- Configuration File Tips and Security 134
 - Clearing parameters with %NULL in configuration file 134
 - Guidelines for the MAC-specific configuration file 134
 - Securing configuration files with AES encryption 135

Configuration File Parameter Guide 137

- "sip_account" Module: SIP Account Settings 139
 - Site-wide settings 139
- "cordless" Module: Cordless Settings 154
 - Site-wide settings 154
- "multicell" Module: Multicell Settings 158
 - Site-wide settings 158
 - Local settings 159
- "system" Module: System settings 161
 - Site-wide settings 161
 - Local settings 161
- "network" Module: Network Settings 163
 - Local settings 163
- "provisioning" Module: Provisioning Settings 168
 - Local settings 168
- "time_date" Module: Time and Date Settings 173
 - Site-wide settings 173
- "log" Module: Log Settings 178
 - Site-wide settings 178
- "remoteDir" Module: Remote Directory Settings 179
 - Site-wide settings 179

"web" Module: Web Settings	184
Site-wide settings.....	184
"trusted_ip" Module: Trusted IP Settings	185
Site-wide settings.....	185
"trusted_servers" Module: Trusted Server Settings	186
Site-wide settings.....	186
"user_pref" Module: User Preference Settings	187
Site-wide settings.....	187
"call_settings" Module: Call Settings	189
Site-wide settings.....	189
"audio" Module: Audio Settings.....	192
Site-wide settings.....	192
"page_zone" Module: Page Zone Settings	194
Site-wide settings.....	194
"ppversion" Module: PP Version Settings	196
Site-wide settings.....	196
"alarm" Module: Alarm settings	197
Site-wide settings.....	197
"file" Module: Imported File Settings.....	201
Site-wide settings.....	201
"tr369" Module: TR-369 Settings	205
Site-wide settings.....	205
"tone" Module: Tone Definition Settings.....	206
Site-wide settings.....	206
"profile" Module: Password Settings.....	211
Site-wide settings.....	211
"speeddial" Module : Speed Dial Settings	213
"XSI" Module: XSI Settings.....	214
Site-wide settings.....	214
Troubleshooting	217
Common Troubleshooting Procedures	217
Appendixes	219
Appendix A: Maintenance	219
Appendix B: GNU General Public License	221

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 M500 Dual-cell SIP DECT Base Station with software version 1.14.4 or newer. See [“Using the Status menu” on page 32](#) for instructions on checking the software version on the M500. Please read this manual before installing the product.

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

Model number: M500

Type: Dual-cell SIP DECT Base Station

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 <p>Notes provide important information about a feature or procedure.</p>	Example of a Note.
 CAUTION <p>A caution means that loss of data or unintended circumstances may result.</p>	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 M500 Dual-cell SIP DECT Base Station 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 M500-specific configurations for optimal performance with those services. For the latest updates, visit our website at www.snomamericas.com.

Related Documents

The **M500 Quick Installation Guide** contains a quick reference guide to the M500 external features and brief instructions on connecting the M500 to a working IP PBX system.

The **M500 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 M500

This administrator and provisioning guide contains detailed instructions for configuring the M500 Dual-cell SIP DECT Base Station. Please read this guide before attempting to configure the M500.

Some of the configuration tasks described in this chapter are duplicated in the Web User Interface (WebUI) described in the next chapter.

This chapter covers:

- [“About the M500 Dual-cell SIP DECT Base Station” on page 10](#)
- [“Quick Reference Guide” on page 12](#)
- [“Network Requirements” on page 21](#)
- [“M500 Configuration Methods” on page 22](#)

About the M500 Dual-cell SIP DECT Base Station

The Snom M500 Dual-cell SIP DECT Base Station with M55 cordless handset and M58 cordless deskset is a cordless business phone system designed to work with popular SIP telephone (IP PBX) equipment and services. Once you have ordered and configured your SIP equipment or service, the M500 and cordless accessories enable you to make and receive calls as you would with any other business phone.

The M500 Dual-cell SIP DECT Base Station features include:

- Up to 8 SIP account registrations per M500 base station
- Up to 8 concurrent calls per M500 base station
- Registration of up to 10 (narrowband) or 5 (wideband) DECT cordless handsets/desksets in single cell mode.
- Registration of up to 8 (narrowband) or 4 (wideband) DECT cordless handsets/desksets per M500 base station in dual cell mode.
- Shared call usage (held call pick up, call barge in to conference) on single SIP account among multiple users
- Power over Ethernet
- 1,000-entry base directory with entries shared on all registered handsets and desksets

The M55 handset features include:

- 2.4-inch color display
- 6 Programmable Feature Keys (PFKs) with LEDs (M55)
- 3 soft keys
- Speakerphone, hold, intercom and mute capability
- Integrated Bluetooth for headset support
- Corded headset support
- 3-way conferencing
- 400-entry local directory
- Antibacterial plastic

The M58 deskset features include:

- 5-inch color display
- Up to 3 pages of 8 Programmable Feature Keys (PFKs) with LEDs and dynamic labels with icons
- Programmable key for multicast paging

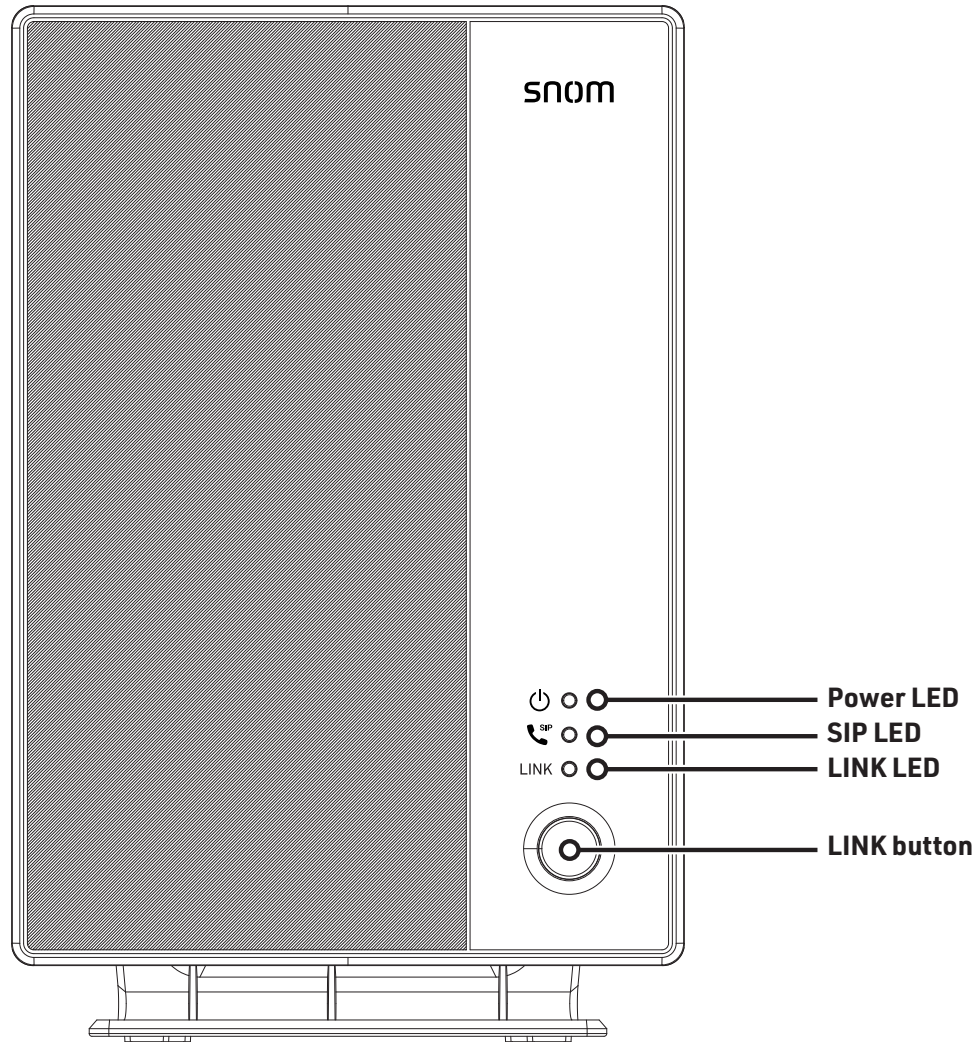
- Speakerphone, hold, intercom and mute capability
- Integrated Bluetooth for headset support
- Corded headset support
- 3-way conferencing
- 400-entry local directory
- Antibacterial plastic

You can configure the M500 using the menus on the handset/deskset, a browser-based interface called the WebUI, or an automatic provisioning process (see [“Provisioning Using Configuration Files” on page 129](#)). The WebUI enables you to configure the M500 using a computer that is connected to the same Local Area Network. The WebUI resides on the M500, and may get updated with firmware updates.

Quick Reference Guide

The external features of the M500 Dual-cell SIP DECT Base Station, M55 handset, and M58 deskset are described below.

M500 Base station – Front view



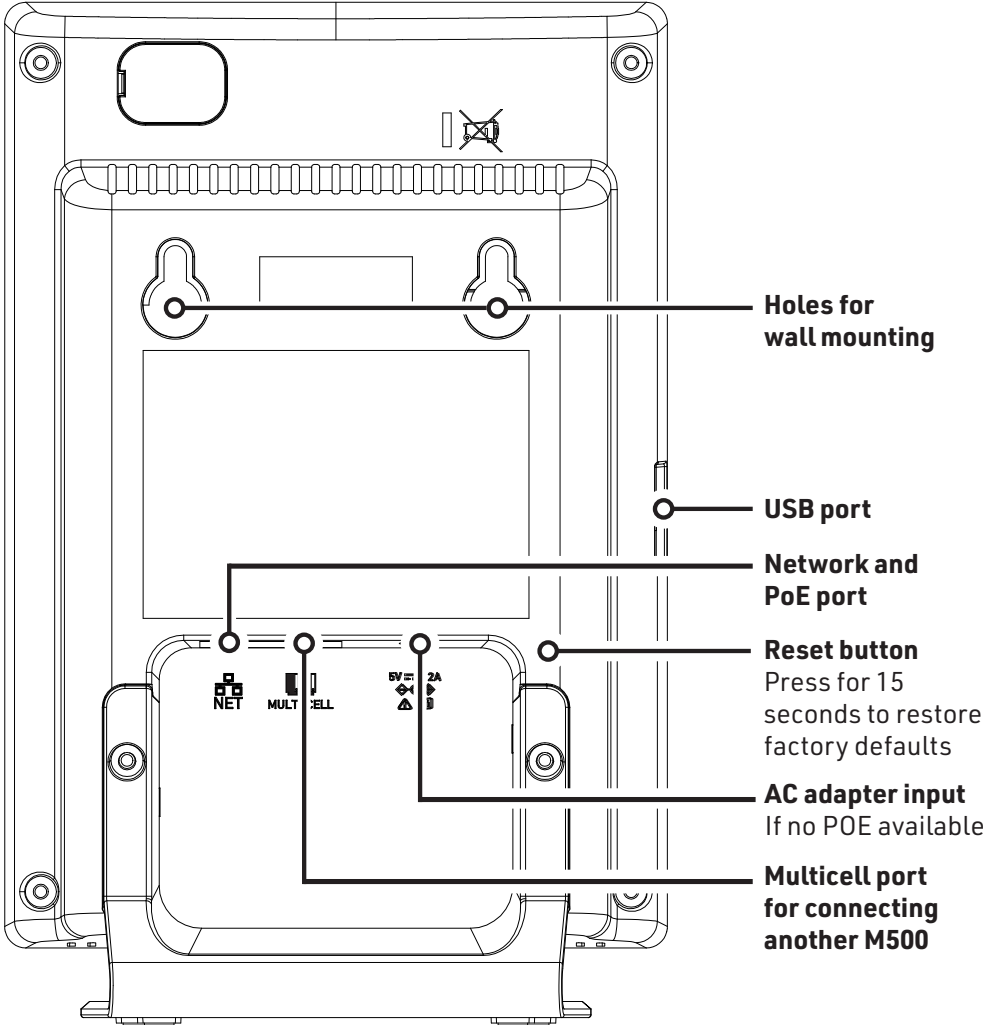
M500 Base Station LEDs

LED	Color	Pattern	Description
Power	Green	Steady	<ul style="list-style-type: none"> ■ Base station just powered ON and proceeding to IP retrieval ■ Power has been ON and IP is assigned to the base station ■ ON for five seconds after the confirmation of system deregistration
		OFF	<ul style="list-style-type: none"> ■ Base station is not powered up
		Slow Flash	<ul style="list-style-type: none"> ■ During deskset / handset registration, i.e. subscription mode ■ Power has been ON and DHCP has been enabled, but no IP is assigned to the base station ■ Toggles with the SIP LED for negotiating or checking with provisioning server
		Quick Flash	<ul style="list-style-type: none"> ■ Ready to deregister deskset / handset ■ Toggles with SIP LED for base station / deskset / handset firmware upgrade or configuration import in progress

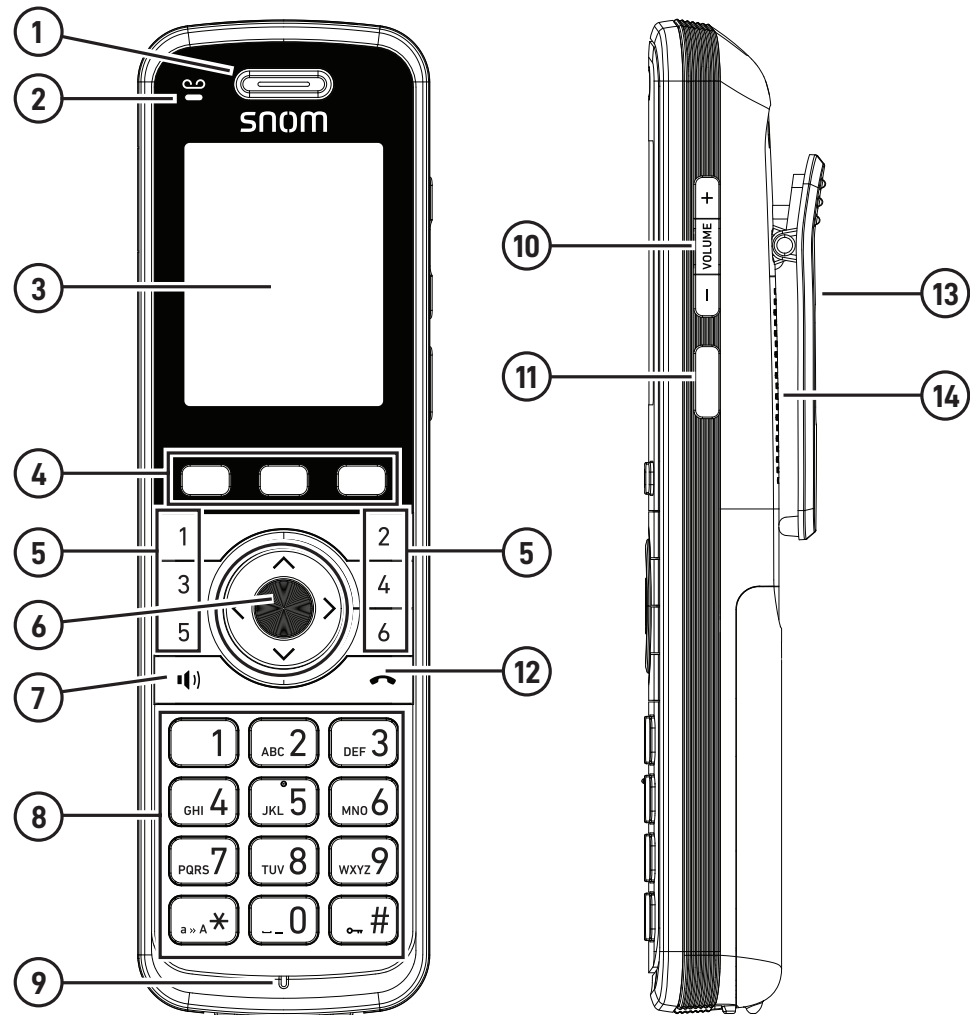
LED	Color	Pattern	Description
SIP	Green	Steady	<ul style="list-style-type: none"> All enabled SIP accounts are registered; displayed on a Primary or Single cell base station ON for five seconds after the confirmation of system deregistration
		Slow Flash	<ul style="list-style-type: none"> During deskset / handset registration, i.e. subscription mode Toggles with the power LED for negotiating or checking with provisioning server
		Quick Flash	<ul style="list-style-type: none"> Ready to deregister deskset / handset Toggles with the Power LED for base station / deskset / handset firmware upgrade or configuration import in progress
	Red	Slow Flash	<ul style="list-style-type: none"> At least one enabled SIP account is deregistered; displayed on a Primary or Single cell base station
	Red & Green	Slow Flash	<ul style="list-style-type: none"> Toggles red and green within the SIP LED for "Primary base" mode during base selection mode
	Orange	Steady	<ul style="list-style-type: none"> All enabled SIP accounts are registered; displayed on a Secondary base station
		Slow Flash	<ul style="list-style-type: none"> At least one enabled SIP account is deregistered; displayed on a Secondary base station


LED	Color	Pattern	Description
LINK	Green	Steady	<ul style="list-style-type: none"> ■ This base station is connected with deskset(s) / handset(s) and registered base stations (if any) ■ ON for five seconds after the confirmation of system deregistration
		Slow Flash	<ul style="list-style-type: none"> ■ During deskset/handset registration, i.e. subscription mode; ■ This base station is connected with registered base station(s) (if any), but not connected with any registered deskset / handset at the moment
		Quick Flash	<ul style="list-style-type: none"> ■ Ready to deregister deskset / handset
	Red	Steady	<ul style="list-style-type: none"> ■ This base station is registered and connected with other base stations, but the M500 system has no record of deskset / handset
		Slow Flash	<ul style="list-style-type: none"> ■ This base station cannot connected with other registered base station(s) in the same network, whether or not the base station is connected to deskset(s) / handset(s)
		Quick Flash	<ul style="list-style-type: none"> ■ This base station cannot find the master base unit; or the master base unit is down
	Red & Green	Slow Flash	<ul style="list-style-type: none"> ■ Toggles red and green within the LINK LED for “Secondary base” mode during base selection mode
	Orange	Slow Flash	<ul style="list-style-type: none"> ■ This base station is a standalone base unit that is not registered with any deskset / handset or base station
	Orange & Green	Slow Flash	<ul style="list-style-type: none"> ■ Toggles orange and green within the LINK LED for “Factory reset without reboot” during base selection mode

M500 Base station – Rear view

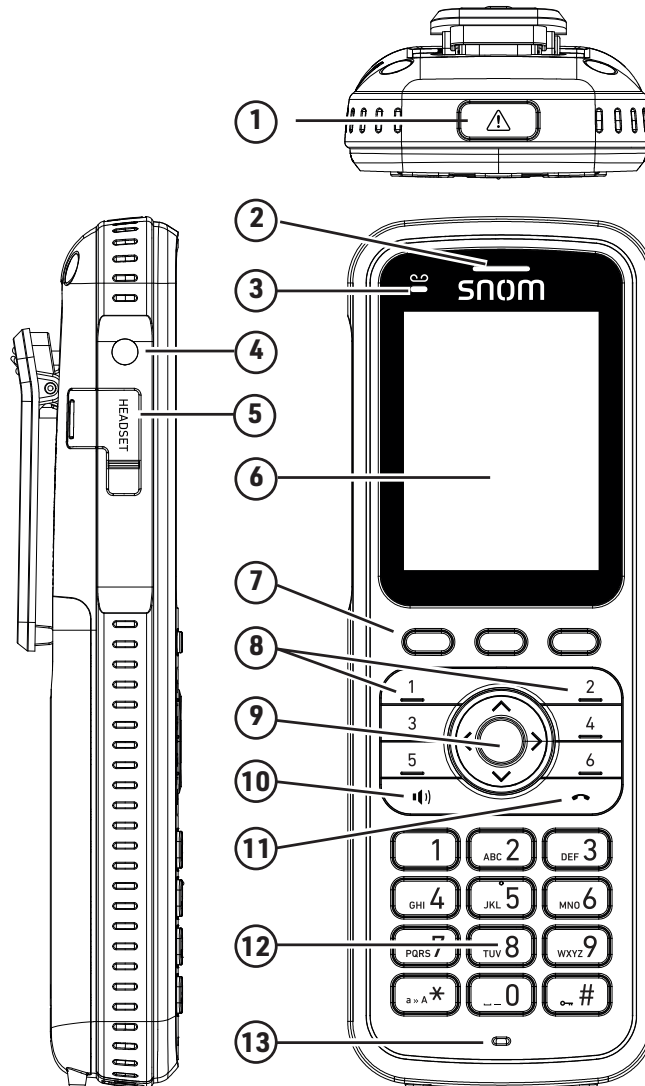



M55 Handset



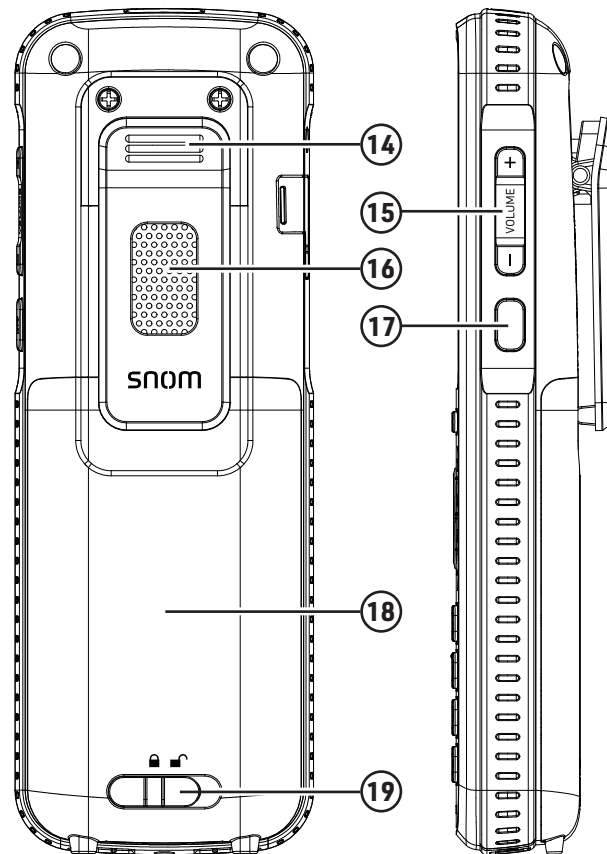
- | | |
|---|---------------------------|
| 1. Earpiece | 8. Alphanumeric keypad |
| 2. MESSAGE LED | 9. Microphone |
| 3. Color screen | 10. – VOLUME + key |
| 4. Soft keys | 11. Programmable key |
| 5. Programmable Feature Keys (PFKs) 1-6 | 12. OFF/Cancel key |
| 6. ○ MENU/Confirm key and
 navigation keys | 13. Belt clip |
| 7. SPEAKER key | 14. Speaker |

M56 Handset



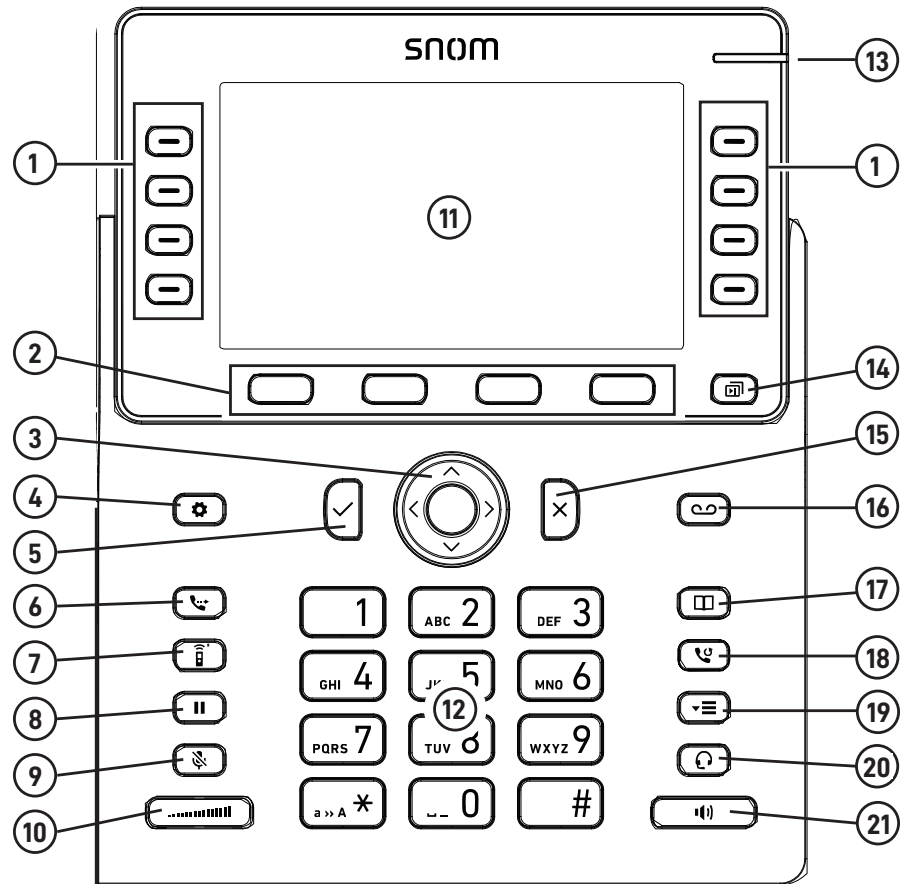
- | | |
|-----------------------|--|
| 1. Alarm button | 8. Programmable Feature Keys (PFKs) 1-6 |
| 2. Earpiece | 9. ○ MENU/Confirm key and
 navigation keys |
| 3. MESSAGE LED | 10. SPEAKER key |
| 4. Flashlight LED | 11. OFF/Cancel key |
| 5. Headset jack | 12. Alphanumeric keypad |
| 6. Color screen | 13. Microphone |
| 7. Soft keys | |


M56 Handset (continued)



- 14. Belt clip
- 15. – **VOLUME** + key
- 16. Speaker
- 17. Programmable key
- 18. Battery cover
- 19. Lock/unlock battery cover

M58 Deskset



- | | |
|---|-------------------------------|
| 1. Programmable Feature Keys (PFKs) | 12. Alphanumeric keypad |
| 2. Soft keys | 13. Message waiting indicator |
| 3. ○ MENU/Confirm key and
 navigation keys | 14. Next page key |
| 4. Settings key | 15. Cancel key |
| 5. OK key | 16. Message key |
| 6. Transfer key | 17. Directory key |
| 7. Intercom key | 18. Redial key |
| 8. Hold key | 19. Call History key |
| 9. Mute key | 20. Headset key |
| 10. Volume key | 21. Speaker key |
| 11. Color screen | |

Network Requirements

A simple M500 single cell configuration 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 M500 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 M500 Dual-cell SIP DECT Base Station so that IP addresses can be auto-assigned. In most cases, your network router will have a DHCP server. By default, the M500 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.

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 M500 firmware and/or configuration settings manually.

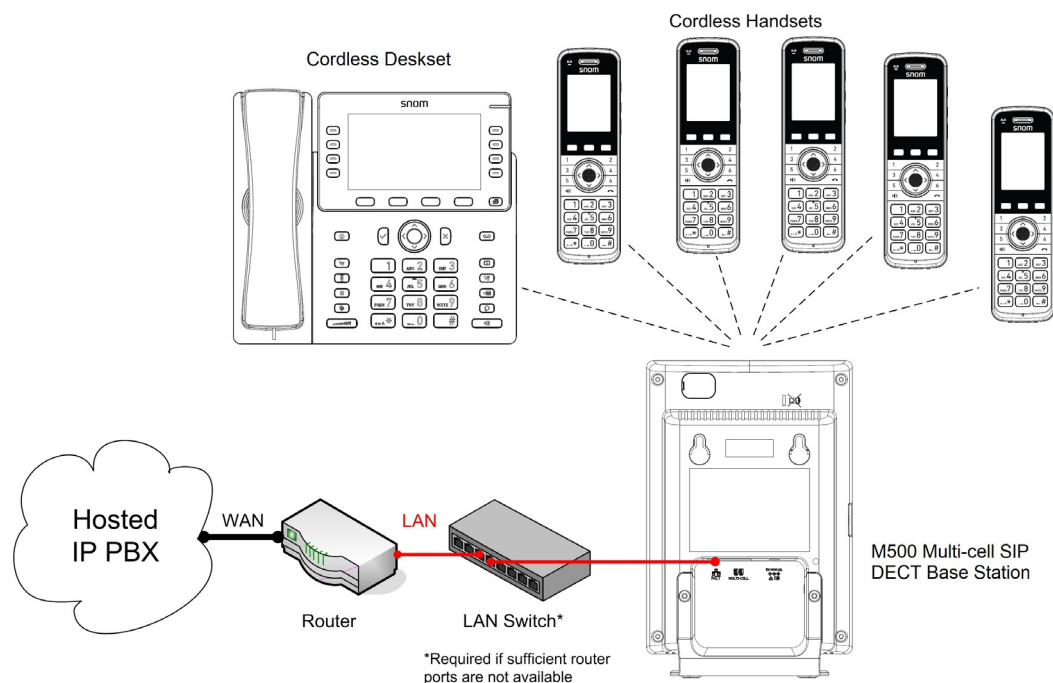


Figure 1. M500 Installation Example (single cell configuration)

M500 Configuration Methods

You can configure the M500 using one of the following methods:

- From the M55 handset / M56 handset / M58 deskset using the handset/deskset menus. The handset/deskset menus are best suited to configuring a few settings, perhaps after the initial setup has been done.

The **User settings** menu enables phone users to:

- Customize display settings (language, backlight, screensaver, wallpaper)
- Customize audio settings (ringers, volume, advisory tones)
- Edit speed dial entries
- Register or deregister handsets/desksets

For more information about the User Menu, refer to the M55 / M56 / M58 User Manual.

- The Web User Interface, or WebUI, which can be accessed using an Internet browser. See [“Using the WebUI” on page 37](#). The browser-based interface is easy to navigate and best suited to configuring a large number of M500 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, assign accounts to handsets and set up provisioning, which will allow you to automatically and remotely update the M500 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 M500 to locate and upload the configuration file. For example, you can enable the M500, 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 M500 automatically downloads the file and applies the new settings. For more information, see [“Provisioning Using Configuration Files” on page 129](#).

How to set the base station operating mode or factory reset using the LINK button

When an M500 base station is brand new out of the box, its default operating mode is **Single**. You can use the LINK button on the base station to change its mode to **Primary** or **Secondary**. You can also change a base station's mode back to **Single** by performing a factory reset. Follow the steps below.

1. Press and hold the LINK button on the base station for at least 20 seconds. All LEDs turn off.



NOTE

If all three LEDs are flashing green, then you did not hold the LINK key long enough. Wait 5 seconds for the three LEDs to stop flashing green, and then try step 1 again.

2. Press the LINK button (for less than 2 seconds) to activate the sub-menu.

The SIP or LINK LEDs flash in alternating colors to indicate the currently selected sub-menu option.

Sub-menu option	SIP LED	LINK LED
Change operating mode to Primary	Flashing green/red 	Off
Change operating mode to Secondary	Off	Flashing green/red
<empty> Reserved for future use	Flashing orange/red 	Off
<empty> Reserved for future use	Off	Flashing orange/red
<empty> Reserved for future use	Flashing orange/green 	Off
Factory Reset AND change operating mode to Single	Off	Flashing orange/green

3. To move to the next sub-menu option, press the LINK button (for less than 2 seconds). Repeat until the desired sub-menu option is indicated by the flashing SIP or LINK LEDs.

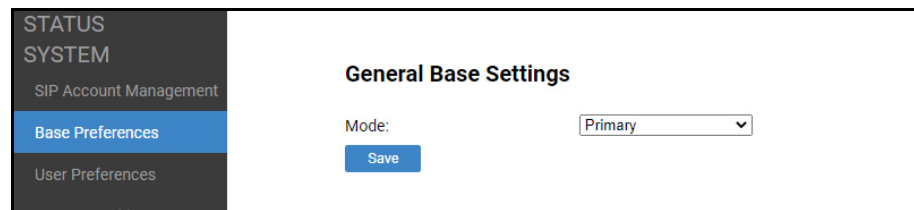


NOTE

If 10 seconds has elapsed without pressing the LINK button, the sub-menu will time out and the base station LEDs will display their normal status indications.

4. To select the sub-menu option indicated by the flashing SIP or LINK LEDs, press and hold the LINK button for at least 2 seconds.

5. Wait for the base station to reboot. This takes approximately 70 seconds. During this time, the LED indications will change.
6. To confirm the operating mode has been set correctly:
 - a. Open an Internet browser and enter the base station's IP address in the address bar.
If you do not know the IP address, refer to [“How to identify the IP address of an M500 base station” on page 39](#).
 - b. For the user name, enter **admin**. For the password, enter the default password **admin**.
 - c. On the left sidebar, click **System**, and then click **Base Preferences**.
 - d. The **Mode** value shows the currently assigned operating mode (Single, Primary or Secondary).



The screenshot displays the web interface for the snom M500 base station. On the left is a dark sidebar with the following menu items: STATUS, SYSTEM, SIP Account Management, Base Preferences (highlighted in blue), and User Preferences. The main content area is titled 'General Base Settings'. It contains a 'Mode:' label followed by a dropdown menu currently set to 'Primary'. Below the dropdown is a blue 'Save' button.

How to configure site-wide vs. local settings in a M500 dual cell configuration

This section describes how to configure site-wide vs. local settings in a M500 dual cell configuration.

Site-wide vs. Local settings

Site-wide settings are applicable to all base stations in a dual cell configuration. When you update a site-wide setting via provisioning, the setting will be automatically updated for all base stations in the system.

Local settings are applicable to a specific base station in a dual cell configuration. When you update a local setting via provisioning, the setting will only be updated for the specified base station.

WebUI

On the primary base station, the WebUI displays both site-wide settings and local settings:

- Changes to the site-wide settings will be automatically applied to all base stations.
- Changes to the local settings will only be applied to the primary base station.

On the secondary base station, the WebUI displays local settings only:

- Changes to the local settings will be only be applied to the secondary base station.

Below are some examples of WebUI pages that display local settings:

System > Base Preferences

General Base Settings

Mode:

Network > Advanced

VLAN

Enable LAN Port VLAN

VID:

Priority:

LLDP-MED

Enable LLDP-MED

Packet Interval (secs):

802.1x

Enable 802.1x

Identity:

MD5 Password:

Servicing > Provisioning

Provisioning Server

Server URL:

Server Authentication Name:

Server Authentication Password:

Plug-and-Play Settings

Enable PnP Subscribe

DHCP Settings

Use DHCP Options

DHCP Option Priority 1:

DHCP Option Priority 2:

DHCP Option Priority 3:

Vendor Class ID (DHCP 60):

User Class Info (DHCP 77):

Resynchronization

Mode:

Bootup Check:

Schedule Check:

Disable

Interval(minutes)

Days of the Week

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

Start Hour:

End Hour:

Use encryption for configuration file

Passphrase:

The following local settings are not available on the WebUI, and must be configured via provisioning:

- multicell.multicast_address
- multicell.site_id
- network.dhcpv6_vendor_class_id
- network.ip.pppoe.service_name
- provisioning.pnp_response_timeout
- provisioning.remote_check_sync_enable

Provisioning

The file fetching rules described in [“provisioning.server_address” on page 172](#) are in effect, but the way that imported settings are applied depends on the operating **Mode** of the base station (see [“General Base Settings” on page 64](#)).

Mode	Import behavior
Single	All settings will be self applied.
Primary	<ul style="list-style-type: none"> ■ Site-wide settings will be self applied and also broadcast to all secondary base(s) within the site. ■ Local settings will only be self applied.
Secondary	<ul style="list-style-type: none"> ■ Site-wide settings will be discarded. ■ Local settings will be self applied. <p>Note: Before it joins a site, a secondary base will self apply all settings.</p>

Suggested practice for importing configuration files in a dual cell operation:

Have one MAC-specific file (e.g. snomM500-000413A11FA7.htm) for each individual base.

- Include local settings for each base to its associated MAC file for both primary base and secondary base(s).
- Include site-wide settings to the MAC file of the primary base. Alternatively, site-wide settings can be included in a separate generic file (e.g. snomM500.htm) if separating local and site-wide settings into different files is the preferred approach.

Exporting settings

The export behavior of settings is determined by the operating **Mode** of the base station (Single, Primary or Secondary – see [“General Base Settings” on page 64](#)).

Mode	Export behavior
Single	All settings will be exported.
Primary	Both site-wide settings and local settings will be exported.
Secondary	Only local settings will be exported. Note: Before it joins a site, a secondary base will export all settings.

Using Shared Calls

Your system allows shared calls usage among multiple handset/deskset users on a SIP account.

Shared calls support brings traditional key system behavior to the SIP environment. Incoming calls on an account can alert multiple handsets/desksets, and be answered by any one of them. Multiple handsets/desksets can share an account for outgoing calls. Typical call sharing operations like held call pick up and barge-in conference among handset/deskset users can be achieved via Programmable Feature Keys (PFKs). For more details, see [“Device Preferences” on page 66](#).

Each "KeyLine" number, when assigned to a shared call, behaves as a virtual "Line" number allowing easy, yet unique reference across multiple handset/deskset users.

Using our default configuration for KeyLine as an example, any incoming/outgoing call on account 1 will get assigned a KeyLine number. The lowest unoccupied KeyLine number will typically be assigned first.

Please see the following scenarios to see how the KeyLine number can be used among users via the PFKs.

Example - picking up a held shared call:

	Alice's handset	Bob's handset
1. Alice is on a call.		
2. Alice presses Hold to put the call on hold.		
3. Alice dials Bob's extension or uses paging to contact Bob. 4. Alice says, "Bob, can you pick up call 2?" 5. Alice ends the call/page with Bob.		
	Alice's handset	Bob's handset
6. Bob presses PFK 2 to pick up the call. The call is now on Bob's handset.		

Example - barging in a shared call:

	Alice's handset	Bob's handset
1. Alice is on a call.		
2. Alice presses Hold to put the call on hold. 3. Alice dials Bob's extension or uses paging to contact Bob. 4. Alice says, "Bob, can you join me on call 3?" 5. Alice ends the call/page with Bob and presses PFK 3 to resume the original call.		
6. Bob presses PFK 3 to barge in the call. Bob is now in a 3-way call with Alice and the caller on call 3.		

CHAPTER 2

CONFIGURATION USING THE PHONE MENUS

The M500 Main Menu has the following sub-menus:

- **Directory**—view and dial local and shared directory entries.
- **Call History**—view missed calls, received calls and dialed calls.
- **Message**—access the voice messages on each account.
- **Call Features**—set Bluetooth and call waiting features
- **Intercom Call**—make an intercom call or page to other handsets/desksets.
- **Settings**—display the Status & Settings menu with the following items:
 - **Status**—view the M500 network status, account registration status, and product information.
 - **User settings**—configure the language, date/time, display settings, audio settings, handset keypad light, speed dial, lift handset to answer, missed call alert and register/deregister conference handsets/desksets to the base station.

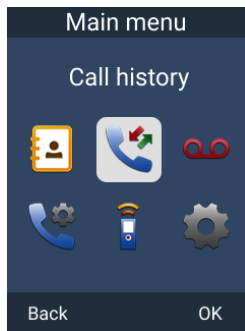
This chapter contains instructions for accessing the Status menu. See the M55, M56 or M58 User Manual for more information about the User settings menu.

Viewing the Main Menu

To use the handset/deskset menu:

1. When the handset/deskset is idle, press the **MENU/Confirm** key.

The **Main Menu** appears.



2. Press **^** **v** **<** **>** to highlight the desired sub-menu, and then press **OK**.
 - Press **OK** or **Enter** to select a menu item.
 - Press **Back** to cancel an operation or return to the previous screen.

Using the Status menu

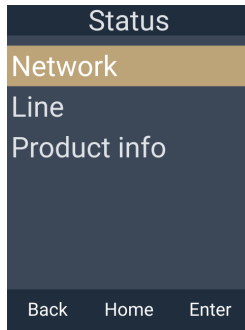
Use the **Status** menu to verify network settings and begin troubleshooting if network problems or account registration issues affect operation.



You can also find the software version of the M500 on the **Product Info** screen, available from the **Status** menu.

To view the Status menu:

1. When the handset/deskset is idle, press the **MENU/Confirm** key.
2. On the **Main Menu**, press **v** and **>** to highlight **Settings**, and then press the **MENU/Confirm** key.
3. With **Status** highlighted, press the **MENU/Confirm** key.

The **Status** menu appears.



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

The available status menus are listed in Table 2.

Table 2. Status menu summary

Menu	Information listed
Network	<p>Network status:</p> <ul style="list-style-type: none"> ■ IPv4 or IPv6 <ul style="list-style-type: none"> ● IP Mode ● IP address ● Subnet Mask ● Gateway IP address ● DNS server 1 IP address ● DNS server 2 IP address
Line	<p>Lines and registration status. On the Line menu, highlight and select the desired line to view detailed line status information:</p> <ul style="list-style-type: none"> ■ Line Status (Registered/Not registered) ■ Display name ■ User ID ■ Server

Table 2. Status menu summary

Menu	Information listed
Product Info	<p>Select This device to view information about the handset/deskset:</p> <ul style="list-style-type: none"> ■ Model number ■ IPEI ■ Serial number ■ Firmware version ■ Hardware version ■ RFPI ■ Bluetooth version <p>Select Base/Cell to view information about the base to which the handset/deskset is connected.</p> <ul style="list-style-type: none"> ■ RFPI ■ Firmware version ■ V-series ■ Hardware version ■ MAC address ■ Boot version ■ EMC version ■ NTP URL

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.

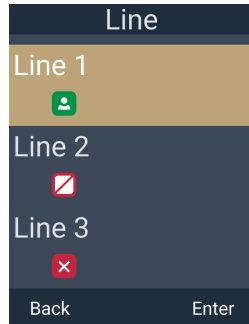





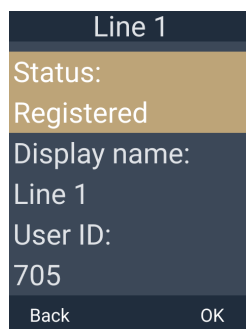


Table 3. Line status icons

Icon	Description
	Line registered
	Line unregistered
	Line disabled

To view complete status information for a line:

On the **Line** menu, press  or  to highlight the desired line, and then press the **MENU/Confirm** key. The Line status screen appears.



CHAPTER 3

USING THE WEBUI

The WebUI allows you to configure all aspects of M500 Dual-cell SIP DECT Base Station operation, including account settings, network settings, contact lists, and provisioning settings. The WebUI is embedded in the M500 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 M500 settings. This chapter covers:

- [“Using the Web User Interface \(WebUI\)” on page 38](#)
- [“Status Page” on page 42](#)
- [“System Pages” on page 49](#)
- [“Network Pages” on page 80](#)
- [“Contacts Pages” on page 86](#)
- [“Servicing Pages” on page 100.](#)

Using the Web User Interface (WebUI)

The Web User Interface (WebUI) resides on the M500 Dual-cell SIP DECT Base Station. You can access it using an Internet browser. After you log in to the WebUI, you can configure the M500 on the following pages:

System

- SIP Account Management (see [page 49](#))
- Base Preferences (see [page 64](#))
- User Preferences (see [page 66](#))
- Device Preferences (see [page 66](#))
- Paging Configuration (see [page 75](#))

Contacts

- Base Directory (see [page 86](#))
- Blocked List (see [page 90](#))
- LDAP (see [page 94](#))
- Remote XML (see [page 98](#))

Network

- Basic Network Settings (see [page 81](#))
- Advanced Network Settings (see [page 83](#))

Servicing

- Reboot (see [page 100](#))
- Time and Date (see [page 100](#))
- Custom Language (see [page 104](#))
- Firmware Upgrade (see [page 105](#))
- Provisioning (see [page 110](#))
- Security (see [page 117](#))
- Certificates (see [page 121](#))
- Tr369 (see [page 124](#))
- System Logs (see [page 125](#))
- SIP Trace (see [page 128](#))

The WebUI also has a **System Status** page, where you can view network status and general information about the M500 and handsets/desksets. The information on the System Status page includes some of the same information as on the **Status** menu available on the handsets/desksets.

How to identify the IP address of an M500 base station

You need to know the IP address of the base station in order to access the WebUI. In a dual cell configuration, each base station has its own IP address. This section describes how to identify the IP address of an M500 base station.

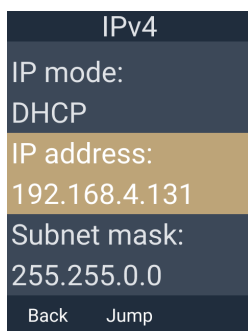
1. On a handset/deskset registered to the base station, press the **MENU/Confirm** key. The Main Menu appears.



NOTE

If you do not have any handsets/desksets registered to the base station, you can register a handset/deskset. Follow the instructions in “Manually registering via the LINK key on base station” in the M55 / M56 / M58 User Manual.

2. On the **Main Menu**, press **▼** and **▶** to highlight **Settings**, and then press **OK**.
3. With **Status** highlighted, press **Enter**.
4. With **Network** highlighted, press **Enter**.
5. Press **▲** or **▼** to highlight **IPv4** or **IPv6**, and then press **Enter**.
6. Press **▼** to highlight the **IP Address**.



7. On your computer, open an Internet browser.
8. Type the **IP address** in the browser address bar, and press **ENTER** on your computer keyboard. The browser displays a window asking for your username 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.

9. Enter **admin** for the username, and enter the password.
10. Click **Sign in**.
11. On the left sidebar of the web page, click **Status**, and then click **Base Status**. The Base Status page appears.

- If you see a **Mode** column, it indicates the base station's mode in a dual cell configuration. Look up the base station's **Mode** to find its corresponding IP address in the **IP** column. Use this IP address to access the WebUI. See [“How to access the WebUI” on page 40](#).

In the example below, the Primary base station's IP address is 10.91.20.11 and the Secondary base station's IP address is 10.91.20.109.

Base Status							
Base	IP	MAC	Version	Mode	Air Sync	Connection Status	No. of Localized Handsets
1	10.91.20.11	00:04:13:BB:02:E0	1.14.3	Primary	-	Connected	3
2	10.91.20.109	00:04:13:BB:04:C7	1.14.3	Secondary 1	Synced	Connected	1

- If you do not see a **Mode** column, it indicates a single cell configuration. The **IP** column shows the base station's IP address (which will match the IP address displayed on the handset/deskset). Use this IP address to access the WebUI. However, at this point you have already accessed the WebUI (in Step 8).

In the example below, the base station's IP address is 10.91.20.71.

Base Status					
Base	IP	MAC	Version	Connection Status	No. of Localized Handsets
1	10.91.20.71	00:04:13:BB:00:99	1.14.3	Connected	0

How to access the WebUI

- Ensure that your computer is connected to the same network as the M500.
- 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.)
- Type the M500 base station IP address in the browser address bar and press **ENTER** on your computer keyboard.

If you do not know what IP address to use, see [“How to identify the IP address of an M500 base station” on page 39](#).

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.

- Enter **admin** for the username, and enter the password. You can change the password later on the WebUI **Security** page, available under **Servicing**.
- Click **OK**.

The WebUI appears.

Click topics from the navigation bar along the left 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  button. Click  to save changes you have made on the page. During a configuration session, click  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 129](#).

Status Page

On the Status pages, you can view network status and general information about the base station and handsets/desksets. Some of the information on the Status pages is also available on the Status menu available on the handset/deskset. You can also view information about cordless registrations, cordless status, base status, and cordless upgrade status.

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 of enabled accounts
- **Network** information regarding your device's network address and network connection

STATUS	
System Status	
Cordless Registrations	
Cordless Status	
Base Status	
Cordless Upgrade Status	
SYSTEM	
NETWORK	
CONTACTS	
SERVICING	

General	
Model:	M500
Serial Number:	CHNLB28122100154
MAC Address:	00:04:13:BB:02:E0
RFPI:	1038C42D00
Link Status:	Connected
Boot Version:	
Software Version:	1.14.3
Hardware Version:	
Hardware Revision:	01
EMC Version:	0
Network Time Settings:	us.pool.ntp.org
Account Status	
Account 1:	Registered
Account 3:	Registered
Account 4:	Registered
IPv4	
IP Mode:	dhcp
IP Address:	10.91.20.11
Subnet Mask:	255.255.0.0
Gateway:	10.91.0.1
Primary DNS:	10.88.162.6
Secondary DNS:	10.88.162.10
VPN:	Disabled
IPv6	
IP Mode:	disable
IP Address:	::
Prefix:	0
Gateway:	
Primary DNS:	
Secondary DNS:	

Cordless Registrations

The Cordless Registrations page shows a list of registered handsets/desksets, and enables you to register or deregister handsets/desksets.



In a dual cell configuration, registration must be done on the primary base station. This affects both manual registration and auto registration.

Handset ID	Name	Registration Status	IPEI	Firmware
1:	Handset 1	Registered	032F53FF74	1.14.3
2:	Deskset 2	Registered	032F53FBD7	1.14.3
3:	Handset 3	Registered	032F54711D	1.14.3
4:	Handset 4	Registered	032F53F90A	1.14.3
5:	Handset 5	Not Registered		
6:	Handset 6	Not Registered		
7:	Handset 7	Not Registered		
8:	Handset 8	Not Registered		
9:	Handset 9	Not Registered		
10:	Handset 10	Not Registered		
11:	Handset 11	Not Registered		
12:	Handset 12	Not Registered		
13:	Handset 13	Not Registered		
14:	Handset 14	Not Registered		
15:	Handset 15	Not Registered		
16:	Handset 16	Not Registered		
17:	Handset 17	Not Registered		
18:	Handset 18	Not Registered		
19:	Handset 19	Not Registered		
20:	Handset 20	Not Registered		
21:	Handset 21	Not Registered		
22:	Handset 22	Not Registered		
23:	Handset 23	Not Registered		
24:	Handset 24	Not Registered		
25:	Handset 25	Not Registered		
26:	Handset 26	Not Registered		
27:	Handset 27	Not Registered		
28:	Handset 28	Not Registered		
29:	Handset 29	Not Registered		
30:	Handset 30	Not Registered		
31:	Handset 31	Not Registered		
32:	Handset 32	Not Registered		
33:	Handset 33	Not Registered		
34:	Handset 34	Not Registered		
35:	Handset 35	Not Registered		
36:	Handset 36	Not Registered		
37:	Handset 37	Not Registered		
38:	Handset 38	Not Registered		
39:	Handset 39	Not Registered		
40:	Handset 40	Not Registered		
41:	Handset 41	Not Registered		
42:	Handset 42	Not Registered		
43:	Handset 43	Not Registered		
44:	Handset 44	Not Registered		
45:	Handset 45	Not Registered		
46:	Handset 46	Not Registered		
47:	Handset 47	Not Registered		
48:	Handset 48	Not Registered		

Register Handset

Enables you to manually register a handset/deskset by entering the IPEI. Enter an available **Handset ID** and the **IPEI** of the handset/deskset, and then click **Register**. For more details, see “Registering by entering the handset’s IPEI on the Web UI” in the M55 or M58 User Guide.

Manual Registration

Enables you to start manual registration of a handset/deskset from the WebUI instead of pressing the LINK key on the base station. You must also trigger manual registration on the handset/deskset. For more details, see “Manually registering via the Web UI” in the M55 or M58 User Guide.

To start registration, press **Start**. To stop registration, press **Stop**.

Auto Registration

Indicates if Auto Registration is enabled or disabled. This is set by the parameter **cordless.autoreg_enable**. For more details, see “[cordless.autoreg_enable](#)” on [page 154](#).

Cordless Registrations

Displays a list of registered cordless handsets/desksets and their Handset ID, Name, Registration Status, IPEI, and currently installed firmware version. The M500 supports a maximum of 16 cordless registrations in dual cell mode.

To deregister a handset/deskset, click [Deregister](#).

To deregister all handsets/desksets, click [Deregister All](#).

Setting	Description
Handset ID	Device number of the cordless handset/deskset.
Name	Device name of the cordless handset/deskset.
Registration Status	Indicates the device registration status (Registered or Not Registered).
IPEI	IPEI of the cordless handset/deskset.
Firmware	Firmware version currently installed on the cordless handset/deskset.

Cordless Status

The Cordless Status page shows information about registered cordless handsets/desksets.

STATUS		Cordless Status									
System Status		Base: <input type="text" value="All"/>									
Cordless Registrations											
Cordless Status											
Base Status											
Cordless Upgrade Status											
SYSTEM											
Cordless ID	Name	IPEI	Firmware	Shared Directory	In Range	Signal	Battery	In Cradle	Localized at Base		
1	Handset 1	032F53FF74	1.14.3	27	Yes	4	93	No	Secondary 1		
2	Deskset 2	032F53FBD7	1.14.3	27	Yes	4	100	Yes	Primary		
3	Handset 3	032F54711D	1.14.3	27	Yes	4	99	No	Primary		
4	Handset 4	032F53F90A	1.14.3	27	Yes	4	99	No	Primary		

Setting	Description
Base (drop down list)	Displayed only in a dual cell configuration. Enables you to filter the list to show the primary base station, a specific secondary base station or all base stations.
Cordless ID	Device number of the cordless handset/deskset.
Name	Device name of the cordless handset/deskset.
IPEI	IPEI of the cordless handset/deskset
Firmware	Firmware version currently installed on the cordless handset/deskset.
Shared Directory	Version number of the Base Directory contacts list.

Setting	Description
In Range	Indicates if handset/deskset is in range of the base station.
Signal	Signal strength (number of bars)
Battery	Battery charge level (percentage)
In Cradle	Indicates if the handset is in the cradle
Localized at Base	Displayed only in a dual cell configuration. Indicates to which base station the cordless handset/deskset is connected when roaming between multiple base stations.

Base Status

The Base Status page shows information about the base station(s).

STATUS	Base Status							
	Base	IP	MAC	Version	Mode	Air Sync	Connection Status	No. of Localized Handsets
System Status	1	10.91.20.11	00:04:13:BB:02:E0	1.14.3	Primary	-	Connected	3
Cordless Registrations	2	10.91.20.109	00:04:13:BB:04:C7	1.14.3	Secondary 1	Synced	Connected	1
Cordless Status								
Base Status								

Setting	Description
Base	ID number of the base station
IP	IP Address of the base station
MAC	MAC ID of the base station
Version	Firmware version currently installed on the base station.
Mode	Displayed only in a dual cell configuration. Indicates the base station is a primary or secondary base station.
Air Sync	Displayed only in a dual cell configuration. Indicates if the secondary base station is Synced or Unsynced to the primary base station.
Connection Status	Indicates the connection status of the base station.
No. of Localized Handsets	The number of cordless handsets/desksets localized to the base station.

Cordless Upgrade Status

The Cordless Upgrade Status page shows the version numbers of the firmware, shared directory and custom wallpaper installed on the base station(s) and handsets/desksets. It also shows the upgrade status of each base station and handset/deskset.

Base	M58 Version	Handset Version	Shared Directory	Handset Wallpaper	Deskset Wallpaper	Upgrading
1	1.14.3	1.14.3 (16%)	27	255	255	Idle
2	1.14.3	1.14.3 (8%)	27	255	255	Idle

Cordless ID	Localized at Base	Type	Software Version	Shared Directory	Wallpaper Version	Upgrade Status
1	2	Handset	1.12.2	27	-1	Pending
2	2	Deskset	1.12.2	27	255	Idle
3	1	Handset	1.12.2	27	-1	Pending
4	1	Handset	1.12.2	27	-1	Pending

Setting	Description
Base	ID number of the base station
M58 Version	Version number of the M58 firmware most recently downloaded to the base station. When a firmware upgrade is in progress, a percentage indicates how much of the firmware file is downloaded to the base station.
Handset Version	Version number of the M55/M56 firmware most recently downloaded to the base station. When a firmware upgrade is in progress, a percentage indicates how much of the firmware file is downloaded to the base station.
Shared Directory	Version number of the Base Directory contacts list. When you update the Base Directory on the WebUI, this number increases.
Handset Wallpaper	Version number of the handset custom wallpaper uploaded to the base station.
Deskset Wallpaper	Version number of the deskset custom wallpaper uploaded to the base station.
Upgrading	Indicates what type of upgrade is currently in progress - Handset (firmware), Handset Wallpaper, Deskset (firmware), Deskset Wallpaper or Idle (no upgrade is in progress).

Setting	Description
Cordless ID	ID number of the cordless handset/deskset
Localized at Base	Indicates the ID number of the base station to which the handset/deskset is localized.

Setting	Description
Type	Indicates the type of device - Handset or Deskset.
Software Version	Version number of the handset/deskset firmware most recently downloaded
Shared Directory	Version number of the Base Directory contacts list. If this number matches the Shared Directory value for the Base station, it means the Base Directory on the handset is in sync with the Base Directory on the base station.
Wallpaper Version	Version number of the wallpaper assigned to the device.
Upgrade Status	Indicates the status of a firmware upgrade - Idle, Pending, Updating or Failed.

System Pages

SIP Account Management

On the SIP Account Management page, you can configure each account you have ordered from your service provider. In the **Account** list, select the account number you want to configure.



In a dual cell configuration, the SIP Account Management page is only displayed in the WebUI of the **Primary** base station.

The SIP Account settings are organized by category in tabs – **Registration**, **Features**, **Audio**, **Signaling** and **Call Settings**. Click a tab to display the settings for that category.

The SIP Account settings are also available as parameters in the configuration file. See [“sip_account” Module: SIP Account Settings](#) on page 139.

Registration tab

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.

Setting	Description
Account Type	<p>Determines the call sharing nature among devices that share the usage of a SIP account.</p> <ul style="list-style-type: none"> Standard: Established call with one device remains private and will not be shared with other devices sharing the SIP account Key Line Emulation: Established call with one device will be visible to other devices sharing the SIP account. Shared device can interact with the call via Line keys or Call list.
Account label	<p>Enter the name that will appear on the M55 / M56 / M58 display when account x is selected. The Account Label identifies the SIP account on the handset/deskset screens and Line menu.</p>
Display Name	<p>Enter the Display Name. The Display Name is the text portion of the caller ID that is displayed for outgoing calls using account x.</p>
User Identifier	<p>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.</p>
Authentication Name	<p>If authentication is enabled on the server, enter the authentication name (or authentication ID) for authentication with the server.</p>
Authentication Password	<p>If authentication is enabled on the server, enter the authentication password for authentication with the server.</p>

SIP Server Settings

SIP Server	
Server Address:	<input type="text"/>
Port:	<input type="text" value="5060"/>

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

Registration	
Server Address:	<input type="text"/>
Port:	<input type="text" value="5060"/>
Expiration (secs):	<input type="text" value="3600"/>
Registration Freq (secs):	<input type="text" value="10"/>

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

Outbound Proxy	
Server Address:	<input type="text"/>
Port:	<input type="text" value="5060"/>

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

Backup Outbound Proxy	
Server Address:	<input type="text"/>
Port:	<input type="text" value="5060"/>

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.

Features tab

Feature Access Codes Settings

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

Feature Access Codes

Voicemail:

DND ON:

DND OFF:

Call Forward All ON:

Call Forward All OFF:

Call Forward No Answer ON:

Call Forward No Answer OFF:

Call Forward Busy ON:

Call Forward Busy OFF:

Anonymous Call Reject ON:

Anonymous Call Reject OFF:

Anonymous Call ON:

Anonymous Call OFF:

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.
Call Forward Busy ON	Enter the Call Forward Busy ON access code.
Call Forward Busy OFF	Enter the Call Forward Busy OFF access code.

Setting	Description
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.

Account Settings

Account	
Dial Plan:	<input type="text" value="x+P"/>
Inter-Digit Timeout (secs):	<input type="text" value="3"/>
Maximum Number of Calls:	<input type="text" value="10"/>
Feature Synchronization:	<input type="text" value="Disable"/>
DTMF Method:	<input type="text" value="Auto"/>
Unregister After Reboot:	<input type="text" value="Disable"/>
Call Rejection Response Code	<input type="text" value="486"/>

Setting	Description
Dial Plan	Enter the dial plan, with dialing strings separated by a symbol. See “Dial Plan” on page 54 .
Inter Digit Timeout (secs)	Sets how long the M55 / M56 / M58 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 M500 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 M55 / M56 / M58 menu and WebUI. Similarly, changes made using the M55 / M56 / M58 or WebUI will update the settings on the server.
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.

Setting	Description
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 M500, disable this setting.
Call Rejection Response Code	<p>Select the response code for call rejection. This code applies to the following call rejection cases:</p> <ul style="list-style-type: none"> ■ 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 M55 / M56 / M58 should dial the number.



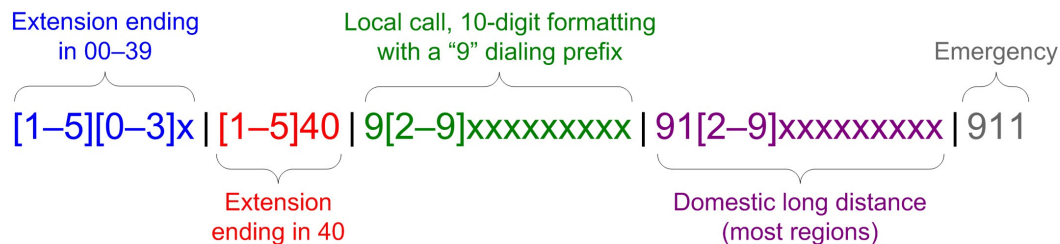
Numbers that are dialed when forwarding a call—when the user manually forwards a call, or a preconfigured number is dialed for Call Forward All, Call Forward–No Answer, or Call Forward Busy—always bypass the dial plan.

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 are 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,xxxxxx" 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.

Element	Description
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 <i>"Inter Digit Timeout (secs)" on page 53</i>).
(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)xxxxxxxxx", 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.



Voicemail Settings

Voicemail Settings

Enable MWI Subscription

Mailbox ID:

Expiration (secs):

Ignore Unsolicited MWI

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.

Setting	Description
Ignore unsolicited MWI	<p>When selected, unsolicited MWI notifications—notifications in addition to, or instead of SUBSCRIBE and NOTIFY methods—are ignored for account x. If the M500 receives unsolicited MWI notifications, the Message Waiting LED will not light to indicate new messages.</p> <p>Disable this setting if:</p> <ul style="list-style-type: none"> ■ 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 M500 receives unsolicited MWI notifications.

Music On Hold Settings

Music On Hold

Enable Local MoH

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.

XSI

XSI

Server Address:

Port:

Username:

Password:

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.

Audio tab

Audio Settings

Audio

Codec Priority 1: ▼

Codec Priority 2: ▼

Codec Priority 3: ▼

Codec Priority 4: ▼

Codec Priority 5: ▼

Codec priority 6: ▼

Codec priority 7: ▼

Enable Voice Encryption (SRTP)

Enable G.729 Annex B

Preferred Packetization Time (ms): ▼

DTMF Payload Type:

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.
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.

Voice Settings

Voice	
Min Local RTP Port:	<input type="text" value="18000"/>
Max Local RTP Port:	<input type="text" value="19000"/>

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.

Quality of Service

Quality of Service	
DSCP (voice):	<input type="text" value="46"/>
DSCP (signaling):	<input type="text" value="26"/>

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

Jitter Buffer

Jitter Buffer	
<input type="radio"/> Fixed	
Fixed Delay (ms):	<input type="text" value="70"/>
<input checked="" type="radio"/> Adaptive	
Normal Delay (ms):	<input type="text" value="80"/>
Minimum Delay (ms):	<input type="text" value="60"/>
Maximum Delay (ms):	<input type="text" value="240"/>

Setting	Description
Fixed	Enable fixed jitter buffer mode. NOTE: you can select either the Fixed option or the Adaptive option, but not both.
Fixed Delay (ms)	If Fixed is selected, enter the fixed jitter delay.

Setting	Description
Adaptive	Enable adaptive jitter buffer mode. NOTE: you can select either the Fixed option or the Adaptive option, but not both.
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.

Signaling tab

Signaling Settings

Signaling Settings

Local SIP Port:

Transport: ▼

Setting	Description
Local SIP port	Enter the local SIP port.
Transport	<p>Select the SIP transport protocol:</p> <ul style="list-style-type: none"> ■ 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 M500 supports secured SIP signaling 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 201 and consult your service provider.

Caller Identity Settings

Caller Identity

Source Priority 1: ▼

Source Priority 2: ▼

Source Priority 3: ▼

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.

Session Timer

Session Timer

Enable Session Timer

Minimum Value (secs):

Maximum Value (secs):

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.
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.

Keep Alive

Keep Alive

Enable Keep Alive

Keep Alive interval (secs):

Ignore Keep Alive Failure

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.
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).

NAT Traversal

NAT Traversal

Enable STUN

Server Address:

Port:

Enable STUN Keep-Alive

Keep-Alive Interval (secs):

Setting	Description
Enable STUN	Enables or disables STUN (Simple Traversal of UDP through NATs) for account x. The Enable STUN setting allows the M500 to identify its publicly addressable information behind a NAT via communicating with a STUN server.
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.

Call Settings tab

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

The call settings are also available as parameters in the configuration file. See ["call_settings" Module: Call Settings](#) on page 189.

General Call Settings

Anonymous Call Reject

Enable Anonymous Call

Do Not Disturb

Enable DND

Call Forward

Enable Call Forward Always

Target Number:

Enable Call Forward Busy

Target Number:

Enable Call Forward No Answer

Target Number:

Delay:

Call Waiting

Enable Call Waiting

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: <ul style="list-style-type: none"> ■ 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.

Call Waiting

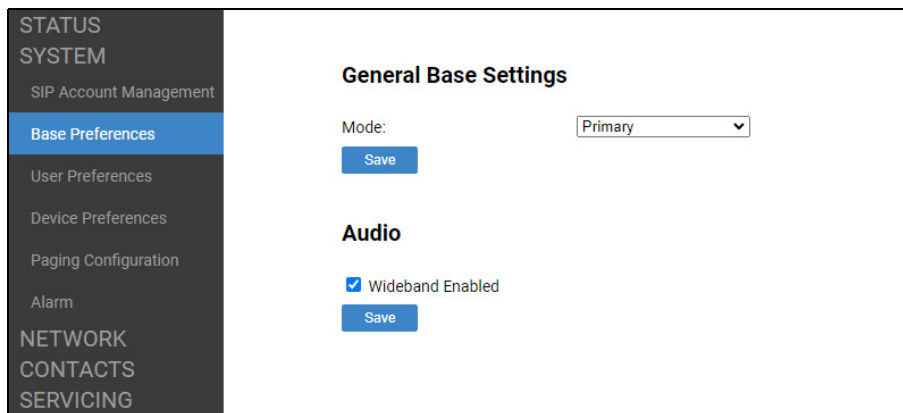
Setting	Description
Enable Call Waiting	Enables or disables Call Waiting for the account.

Base Preferences

On the Base Preferences page, you can configure the operating mode for the base station as single, primary or secondary.

If you are using the WebUI on the primary base station of a dual cell configuration, you can enable/disable wideband audio.

These settings are also available as parameters in the configuration file. See the parameters [“multicell.role” on page 159](#) and [“cordless.wideband_enabled” on page 155](#).



General Base 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
Mode	<p>Select the operating mode of a base station, which can be one of the following:</p> <ul style="list-style-type: none"> ■ “single” for single cell operation ■ “primary” for acting as a primary base within a dual cell site ■ “secondary” for acting as a secondary base within a dual cell site <p>Note that changing a base's role may trigger reset of selected parameters and auto reboot to prepare the base for new mode of operation.</p> <p>In a dual cell configuration, configure this setting for each specific base station. This is NOT a site-wide setting.</p>

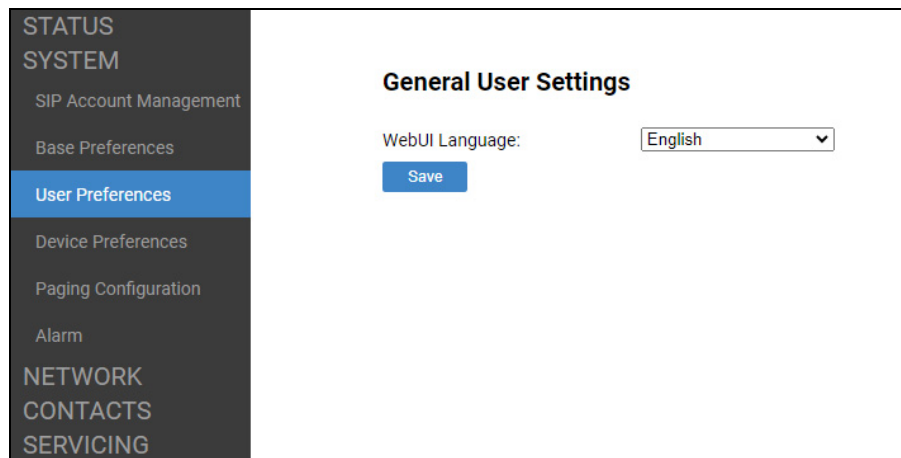
Audio

Setting	Description
Wideband Enabled	<p>Select the checkbox to enable wideband for DECT audio.</p> <p>This setting is only visible on the WebUI of a primary base station in a dual cell configuration.</p> <p>NOTE: When wideband is enabled, the system calling capacity is lowered to four devices per base unit. A reboot is also required, and all calls in progress will be terminated.</p>

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 WebUI Language setting is also available as a parameter in the configuration file. See [“user_pref.web_language” on page 188](#).



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.

Device Preferences

On the Device Preferences page, you can:

- Assign additional functions to the Programmable Feature Keys (PFKs) on handsets/desksets
- Assign the speed dial keys on handsets/desksets
- Enable or disable barge-in of shared calls on handsets/desksets
- Upload a custom wallpaper for handsets/desksets
- Select a wallpaper and theme for all handsets/desksets



In a dual cell configuration, the Device Preferences page is only displayed in the WebUI of the **Primary** base station.

The Device Preferences settings are organized by category in tabs – **Keys**, **Custom Wallpaper** and **Call Settings**. Click a tab to display the settings for that category.

Keys tab

	Type	Account	Value	
PFK 1	KeyLine	Account 3	1	
	KeyLine	Account 3	2	PFK 2
PFK 3	KeyLine	Account 3	3	
	KeyLine	Account 3	4	PFK 4
PFK 5	KeyLine	Account 3	716	
	Line	Account 4	1	PFK 6

In the **Select Device** box, select the handset/deskset whose PFKs you want to assign functions.

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
Device Name	Enter a name for the cordless handset/deskset. The default name is according to the device type—“Handset x” for cordless handset and “Deskset x” for cordless deskset, where x is the device number (1-16).
Default Account	Select the default account for cordless handset/deskset. The cordless handset/deskset attempts to use this account first when going off hook.

PFK

M55 / M56 / M58 PFK

The M55 / M56 / M58 PFK settings are also available as parameters in the configuration file. See the parameters named **cordless.x.pfk.y.____** on page 157-157.

Each row represents a numbered PFK (for example, PFK 1, PFK 2, etc.)

For M55 and M56 handsets, you can configure six PFKs.

For M58 desksets, you can configure three pages of eight PFKs. In the box next to **PFK**, select the page number.

Setting	Description
Type	Select a programmable feature type to assign to the PFK. For more details, see the “Type setting” section below.
Account	If applicable, select an account number to assign to the PFK.
Value	<p>If applicable, enter a numeric value or text string to assign to the PFK. For example, a speed dial phone number.</p> <p>Applicable only if Type is set to one of the following:</p> <ul style="list-style-type: none"> ■ Speed Dialing ■ Intercom Call ■ Paging ■ In-Call DTMF ■ Dect Busy Monitoring <p>For a description of what to enter for Value, see the table entries for these Type settings on page 70.</p>

Type setting

The following table lists the available selections for the **Type** setting.

Type setting	Description
N/A	Configures the PFK so it does not have a function. If you press the PFK while the handset/deskset is idle, nothing will happen.
KeyLine	Configures the PFK to use the specified Account for shared call operation. Please refer to “Using Shared Calls” on page 28 for typical shared call usage. Note that the specified account has to be configured as “Key Line Emulation” for the Account Type . The PFK LED will change according to call activity.
Line	Configures the PFK to use the specified Account for private call operation. With private call operation, established calls remain private to the user until being transferred to or conferenced with other parties. Note that the specified account has to be configured as “Standard” for the Account Type . The PFK LED will change according to call activity.
Call List	Configures the PFK to access the Call list. The Call List displays a list of shared calls (held and active) and private calls (held) that can be accessed by the handset/deskset.

Type setting	Description
Dialing Line	Configures the PFK to access the Select line menu.
Directory	Configures the PFK to access the Directory menu.
Call History	Configures the PFK to access the Call history menu.
Redial	Configures the PFK to access the Dialed calls list.
Messages	Configures the PFK to access the Message menu for the specified Account .
Torch	Configures the PFK to turn the handset flashlight on/off. Only applicable to M56 handsets.
Do Not Disturb	Configures the PFK to turn Do Not Disturb on or off for the specified Account .
Call Forward All	<p>Configures the PFK to turn Call Forward All on or off for the specified Account.</p> <p>Make sure to also configure the Call Forward Always Target Number via SYSTEM > SIP Account Management > Call Settings > Call Forward (see page 62).</p> <p>The PFK will control the Enable Call Forward All setting on this page.</p>
Call Forward Busy	<p>Configures the PFK to turn Call Forward Busy on or off for the specified Account.</p> <p>Make sure to also configure the Call Forward Busy Target Number via SYSTEM > SIP Account Management > Call Settings > Call Forward (see page 63).</p> <p>The PFK will control the Enable Call Forward Busy setting on this page.</p>
Call Forward No Answer	<p>Configures the PFK to turn Call Forward No Answer on or off for the specified Account.</p> <p>Make sure to also configure the Call Forward No Answer Target Number and Delay via SYSTEM > SIP Account Management > Call Settings > Call Forward (see page 63).</p> <p>The PFK will control the Enable Call Forward No Answer setting.</p>
User Settings	Configures the PFK to access the User settings menu.
Speed Dial List	Configures the PFK to access the Speed dial list
Intercom Call List	Configures the PFK to access the Intercom Call list
Silent Ringer	Configures the PFK to turn Silent Ringer on or off. If turned on, the ringer will be silent for incoming phone calls.

Type setting	Description
Silent Mode	Configures the PFK to turn Silent Mode on or off. If turned on, the following tones will not be played: <ul style="list-style-type: none"> ■ Ringer tone ■ Confirmation tone ■ Notification tone ■ Key tone ■ End of list tone
Callback	Configures the PFK to call back the number of the most recently missed call.
Speed Dialing	Configures the PFK to call the number specified in the Value setting from the specified Account .
Intercom Call	Configures the PFK to make an intercom call to the handset/deskset device number specified in the Value setting.
Paging	Configures the PFK to page the paging group number specified in the Value setting. For example, if Value=2, the phone will page the handsets/desksets defined in the 2nd entry of the Select Page Group list on the Paging Configuration page. See “Paging Configuration” on page 75 .
Paging List	Configures the PFK to access the Paging list.
In-Call DTMF	Configures the PFK to dial an in-call DTMF string when pressed during an active call. Enter the DTMF string in the Value setting.
Dect Busy Monitoring	Configures the PFK to perform DECT Busy Monitoring of the Device number specified in the Value setting.
L1-L6 Overview	For M55 handsets only. Configures the PFK to display all of the handset’s Programmable Key assignments.

Default PFK configuration

The default PFK configuration is PFK1-4 set up as KeyLine.

WebUI:

M55 PFK			
	Type	Account	Value
PFK 1	KeyLine	Account 1	1
	KeyLine	Account 1	2
PFK 3	KeyLine	Account 1	3
	KeyLine	Account 1	4
PFK 5	N/A	Account 3	4
	N/A	Account 4	1

Provisioning:

```

cordless.1.pfk.1.account = 1
cordless.1.pfk.1.feature = keyline
cordless.1.pfk.1.value = 1
cordless.1.pfk.2.account = 1
cordless.1.pfk.2.feature = keyline
cordless.1.pfk.2.value = 2
cordless.1.pfk.3.account = 1
cordless.1.pfk.3.feature = keyline
cordless.1.pfk.3.value = 3
cordless.1.pfk.4.account = 1
cordless.1.pfk.4.feature = keyline
cordless.1.pfk.4.value = 4
    
```

For more information about these parameters, see page 157-157.

Speed dial

The speed dial settings are also available as parameters in the configuration file. See the parameters named **speeddial.x.y._____** on page 213.

Speed dial			
Speed dial Key	Name	Account	Number
Key 0	Tango	Account 1	11223344
Key 1	Echo	Account 1	999292
Key 2	Foxtrot	Account 1	32433
Key 3	Oscar	Account 1	712
Key 4		Account 1	
Key 5		Account 1	
Key 6		Account 1	
Key 7		Account 1	
Key 8		Account 1	
Key 9		Account 1	

Each row represents the speed dial key (0-9) of the selected device.

Setting	Description
Name	Enter the name used by the speed dial entry.
Account	Enter the account used by the speed dial entry
Number	Enter the phone number of the speed dial entry.

Wallpaper & Theme tab

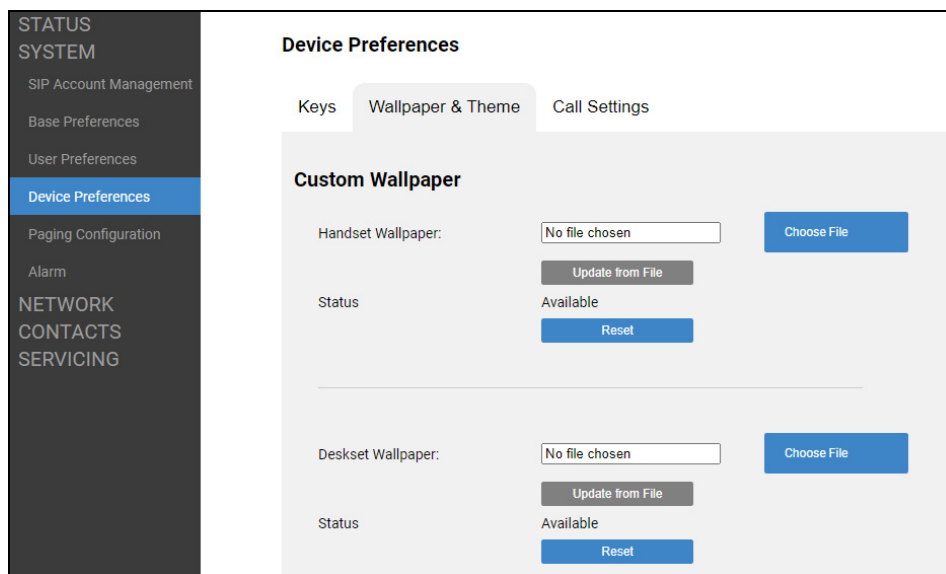
Custom Wallpaper

You can install your own custom wallpaper on the handsets/desksets.

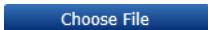

The wallpaper file should be in bitmap format (.BMP) with color depth 24-bit or lower. Supported bitmap color depths: 24-bit, 16-bit, 8-bit, 4-bit, 1-bit and monochrome.


Handset wallpaper: 240x320 pixels

Deskset wallpaper: 480x272 pixels



To install custom wallpaper:

1. Under **Handset Wallpaper** or **Deskset Wallpaper**, click  and select the wallpaper file you want to install.
2. Click .
3. To monitor the progress of the wallpaper update, open the WebUI page **Status > Cordless Upgrade Status**.
 - The wallpaper file is uploaded to the base station.
 - In a dual-cell system, it is sent from the primary base station to the secondary base station.

- The base station(s) download the wallpaper file to the handsets/desksets.
- The  icon will flash on the handsets/desksets while the wallpaper is being downloaded.

The **Status** field displays “Available” if a custom wallpaper is currently installed, and displays “Not Available” if there is no custom wallpaper installed.

You can also install custom wallpaper via provisioning of the file.deskset_wallpaper and file.handset_wallpaper parameters.

To remove custom wallpaper:

- Under **Handset Wallpaper** or **Deskset Wallpaper**, click .

You can also remove custom wallpaper via provisioning of the file.action parameter with the value removewallpaper_handset or removewallpaper_deskset.


Wallpaper & Theme on All Devices

You can select the wallpaper and theme to be displayed on all handsets/desksets.

Wallpaper & Theme on All Devices

Wallpaper:

Theme:



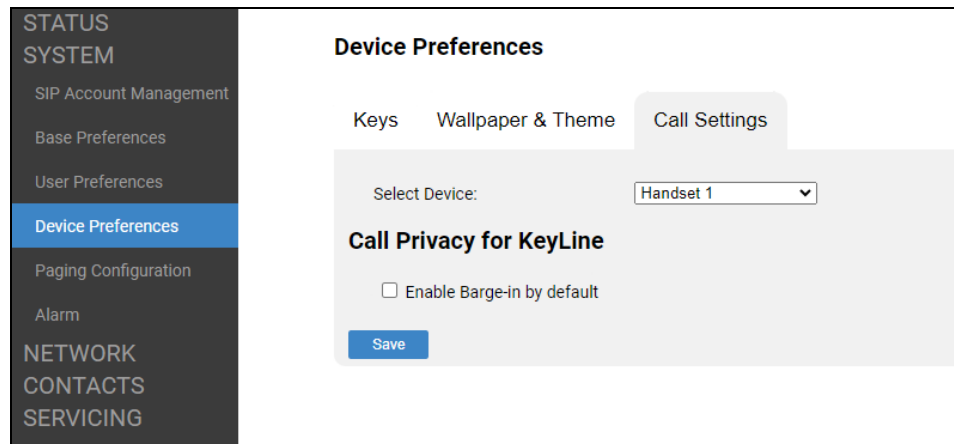
Setting	Description
Wallpaper	<p>Select the desired wallpaper.</p> <ul style="list-style-type: none"> ■ Select “Custom” to choose a custom wallpaper. ■ If you select “Custom”, but there is no custom wallpaper installed, the handset/deskset will display the “None” wallpaper until you install the custom wallpaper.
Theme	Select the desired display theme.

Call Settings tab

In the **Select Device** box, select the handset/deskset whose call privacy you want to set.

Call Privacy for KeyLine

The Enable Barge-in by default setting is also available as a parameter in the configuration file. See the parameter named *“cordless.x.allow_barge_in”* on page 156.



Setting	Description
Enable Barge-in by default	Configures the default Call Privacy setting for the selected device. If enabled, barge-in will be allowed for shared calls by default when a call is dialed out, answered or resumed from held on the selected device. During a call, user can override the barge-in default via the PUI.

Paging Configuration

On the Paging Configuration page, you can configure up to six paging groups. A paging group is a list of registered handsets/desksets that can receive a page. For example, you can set up paging group “Sales” for handsets 1 and 2, and paging group “Warehouse” for handsets 3, 4 and 5.



NOTE

In a dual cell configuration, the Paging Configuration page is only displayed in the WebUI of the **Primary** base station.

The paging configuration settings are also available as parameters in the configuration file. See “page_zone.group.x.members” and “page_zone.group.x.name” on page 194.

Handset ID	Name	
1:	Handset 1	<input checked="" type="checkbox"/>
2:	Deskset 2	<input type="checkbox"/>
3:	Handset 3	<input checked="" type="checkbox"/>
4:	Handset 4	<input checked="" type="checkbox"/>

In the **Select Page Group** box, select the paging group you want to configure.

In the **Page Group Name** box, enter a name for the paging group (maximum 15 characters).

Group Members

Select the checkboxes of the handsets/desksets to be included in the paging group.

Multicast

Setting	Description
Enable External Page	<p>Enables multicast paging to/from external parties.</p> <p>If enabled (check box is selected):</p> <ul style="list-style-type: none"> ■ Multicast paging by an external party on the configured IP address and port will reach all configured members of the page group. ■ Paging initiated by any handset/deskset will reach the configured members of the page group and the external parties listening to the configured multicast IP address and port. <p>If disabled (check box is cleared):</p> <ul style="list-style-type: none"> ■ Multicast paging by the external party on the configured IP address and port will not be accepted by the M500. ■ Multicast paging is only for internal paging to configured members of the page group.
IP Address	Multicast IP address for multicast paging with external parties. Can be left blank if the Enable External Page check box is cleared.
Port	Multicast port for multicast paging with external parties. Can be left blank if the Enable External Page check box is cleared.

Alarm

On the Alarm page, you can define alarm profiles and assign them to selected M56 handsets.



In a dual cell configuration, the Alarm page is only displayed in the WebUI of the **Primary** base station.

The alarm settings are also available as parameters in the configuration file. See [“alarm” Module: Alarm settings](#) on page 197.

Alarm

Each row represents an alarm profile (1-8).

Setting	Description
Label	Optional: Assigns a name to the alarm profile.

Setting	Description
Alarm type	<p>Defines the method that is used to trigger the M56 alarm for the specified alarm profile.</p> <ul style="list-style-type: none"> ■ Disable - alarm profile is disabled ■ Alarm button - Press and hold the alarm key on the top of the M56 handset for 1.5 seconds + Trigger Delay. ■ Man down <ul style="list-style-type: none"> ● M56 handset lay down in horizontal position: 0-15 degrees ● Continuous no movement time > Trigger Delay + 5 seconds (Note: If M56 handset is in horizontal position and steady, it will trigger No movement alarm first. If pre-alarm is disregarded then it will trigger Man down alarm.) <p>OR</p> ● Continuous movement (in horizontal direction) time > Trigger Delay + 5 seconds (This case is assumed an injured person laying down but can move slowly.) ■ No movement <ul style="list-style-type: none"> ● M56 handset in a steady position (any angle) ● Continuous no movement time > M56 handset in a steady position (any angle) ● Continuous no movement time > Trigger Delay (e.g. if the user is sleeping or forgot to bring the handset) (e.g. if the user is sleeping or forgot to bring the handset) ■ Running <ul style="list-style-type: none"> ● Swing or shake the M56 handset with frequency > 1.5 Hz in any direction ● Continuous action > Trigger Delay + 3 seconds

Setting	Description
Alarm Signal (channel to send alarm)	<p>Defines the way an alarm is signaled for the specified alarm profile.</p> <ul style="list-style-type: none"> ■ Call: the M56 handset calls the telephone number defined in Alarm Number. ■ Intercom: the M56 handset makes an intercom call to the device defined in Intercom Call Alarm Recipient. ■ Paging: the M56 handset pages the paging group defined in Paging Alarm Group.
Trigger Delay (sec)	Enter the time delay (in seconds) that the M56 handset will wait before making a call/intercom call/page to the alarm recipient or, if Delay to send triggered alarm has also been configured, before the pre-alarm delay is triggered.
Stop Pre-Alarm (cancel triggered but unsent alarm)	If this setting is enabled, the pre-alarm can be canceled from the M56 handset.
Delay to send triggered alarm (sec)	Enter the number of seconds from the moment the M56 handset's alarm is activated that the handset will wait before calling the alarm number. The display will show the "Pre-alarm triggered" message. If Howling is enabled, the M56 handset plays a continuous loud alarm sound.
Stop Alarm (cancel set alarm)	If this setting is enabled, the call/intercom call/page to the alarm recipient can be canceled from the M56 handset.
Howling (play siren if alarm is not answered)	If this setting is enabled, the M56 handset will emit an alarm sound until it has established a call/intercom call/page with the alarm recipient.

M56 Handset

This section of the page enables you to define alarm settings for a specified M56 handset.

Setting	Description
Select M56 HS	Select the M56 for which you want to configure the alarm.
Alarm Line	Specifies which line to use on the selected M56 handset when making a call, intercom call or page to the alarm recipient.
Alarm Number	Sets the telephone number the selected M56 handset will call when the alarm is signaled. Used when Alarm Signal is set to "Call".
Intercom Call Alarm Recipient	Sets the device number the selected M56 handset will intercom call when the alarm is signaled. Used when Alarm Signal is set to "Intercom".

Setting	Description
Paging Alarm Group	Sets the paging group the selected M56 handset will page when the alarm is signaled. Used when Alarm Signal is set to "Paging".

Alarm Profiles

This section of the page enables you to assign alarm profiles to the selected M56 handset.

Setting	Description
Profile	Profile number and Label in parentheses (if applicable).
Alarm type	The Alarm Type for the alarm profile.
Checkbox	Select this checkbox to assign the alarm profile to the specified M56 handset.

Network Pages

You can set up the M500 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 M500 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 163.

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

Basic Network Settings

STATUS
SYSTEM
NETWORK

Basic

Advanced

CONTACTS
SERVICING

Basic Network Settings

IPv4

Disable
 DHCP
 Static IP

PPPoE

Manually Configure DNS

IP Address:
 Subnet Mask:
 Gateway:
 Username:
 Password:
 Primary DNS:
 Secondary DNS:

IPv6

Disable
 Auto Configuration
 Static IP

Manually Configure DNS

IP Address:
 Prefix (0-128):
 Gateway:
 Primary DNS:
 Secondary DNS:

[Save](#)



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



NOTE

In a dual cell configuration, the settings listed below must be configured for each specific base station. These are NOT site-wide settings.

Setting	Description
Disable	Disables all related IPv4 settings.

Setting	Description
DHCP	DHCP is selected (enabled) by default, which means the M500 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 M500, as well as addresses for the Subnet Mask, Gateway, and DNS Server(s).
Static IP	When Static IP is selected, you must enter a static IP address for the M500, 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 M500.
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



In a dual cell configuration, the settings listed below must be configured for each specific base station. These are NOT site-wide settings.

Setting	Description
Disable	Disables all related IPv6 settings.
Auto Configuration	Auto configuration is selected (enabled) by default, which means the M500 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 M500, 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 M500, 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 M500.

Setting	Description
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

STATUS
 SYSTEM
 NETWORK
 Basic
Advanced
 CONTACTS
 SERVICING

VLAN

Enable LAN Port VLAN

VID:

Priority:

Enable PC Port VLAN

VID:

Priority:

LLDP-MED

Enable LLDP-MED

Packet Interval (secs):

802.1x

Enable 802.1x

Identity:

MD5 Password:

Save

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.



In a dual cell configuration, the settings listed below must be configured for each specific base station. These are NOT site-wide settings.

Setting	Description
Enable LAN Port VLAN	Enable if the LAN port (labeled “NET” on the M500) is part of a VLAN on your network. Select to enable.

Setting	Description
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 M500) 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.
Enable PC Port VLAN	Enable if the PC port (labeled "MULTI-CELL" on the M500) 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 PC port (labeled "MULTI-CELL" on the M500) 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



NOTE

In a dual cell configuration, the settings listed below must be configured for each specific base station. These are NOT site-wide settings.

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



NOTE

In a dual cell configuration, the settings listed below must be configured for each specific base station. These are NOT site-wide settings.

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.

Contacts Pages

Base Directory

On the Base Directory page, you can manage directory entries that will be available on all handsets/desksets. 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**

Each handset/deskset also has its own Local directory. You can add entries to the Local directory using the handset/deskset. For more information, see the M55 / M56 / M58 User Guide.

**NOTE**

In a dual cell configuration, the Base Directory page is only displayed in the WebUI of the **Primary** base station.

STATUS
SYSTEM
NETWORK
CONTACTS

Base Directory

Blocked List

LDAP

Broadsoft

Remote XML

SERVICING

Local Directory

Select All Sort By Last Name

Total: 26	First Name	Last Name	Ringer Tone	Work	Mobile	Other	Account	
<input type="checkbox"/>	Angela	Martin	0	7325550118			3	Edit
<input type="checkbox"/>	Bronwyn	McDonald	0	2325550140			3	Edit
<input type="checkbox"/>	Charlie	Johnson	0	5550198			3	Edit
<input type="checkbox"/>	Dale	Appleton	0		6045550135		3	Edit
<input type="checkbox"/>	David	Carter	3	2325550194	2325550177		4	Edit
<input type="checkbox"/>	Davis	Swerdlow	0		232555172		3	Edit
<input type="checkbox"/>	Elkhart	Taxi	0		6045550155		3	Edit
<input type="checkbox"/>	Graham	Ball	0		2325550176		3	Edit
<input type="checkbox"/>	Kathryn	Dolphy	0		6045550195		3	Edit
<input type="checkbox"/>	Linda	Miller	0		6045550117		4	Edit
<input type="checkbox"/>	Lydia	Braithwaite	0	2325550157			3	Edit
<input type="checkbox"/>	Martin	Meyers	0	2325550122			3	Edit
<input type="checkbox"/>	Mary	Williams	0		6045550145	6045550146	3	Edit
<input type="checkbox"/>	Richard	Serling	0		6045550141	7875550181	4	Edit
<input type="checkbox"/>	Robert	Brown	2		6045550105		4	Edit
<input type="checkbox"/>	Sandro	Voss	0	2325550149			3	Edit
<input type="checkbox"/>	Stefan	Wheeler	0		2325550161		3	Edit
<input type="checkbox"/>	Susan	Balance	0		6045550170		3	Edit
<input type="checkbox"/>	Terry	Ng	0		2325550187		3	Edit
<input type="checkbox"/>	Ursula	Baldwin	0	6045550166			3	Edit

First 1 Next Last

Delete Selected Entries
Add New Entry
Clear Directory

Import Local Directory

Choose File

Import XML
 First line is header, skip Import CSV

Export Local Directory

Export CSV
Export XML (Simple)
Export XML (Tbook)

Table 4 describes the buttons available on the Base Directory page.

Table 4. Base Directory commands

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

Click	To...
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 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 a directory file in simple XML format or tbook format ("OLD XML FORMAT")
Import CSV	Import a directory file in CSV format
Export CSV	Export the directory in CSV format
Export XML (Simple)	Export the directory in simple XML format
Export XML (Tbook)	Export the directory in tbook XML format ("NEW XML FORMAT")

To add a new directory entry:

1. Click [Add New Entry](#) .
The **Create Local Directory Entry** page appears.

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

Create Local 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 1–48	Default Account
Work	Enter the appropriate telephone numbers in these fields.	n/a	Blank
Mobile			
Other			

Directory Import/Export

For a brand new M500 base station 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 (Simple) 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 will delete any existing entries in the Base Directory. The system will display a warning prompt, “All Directory entries will be deleted. Do you want to continue?”



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 204](#) – adds to existing entries
- [“file.contact.directory.overwrite” on page 204](#) – replaces existing entries

Directory files in simple 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>
Work Number	<DIR_ENTRY_NUMBER_WORK>
Mobile Number	<DIR_ENTRY_NUMBER_MOBILE>

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

For a description of directory files in tbook XML format ("NEW XML FORMAT") or tbook format ("OLD XML FORMAT"), visit <https://service.snom.com/display/wiki/Local+Directory>.

Blocked List

On the Blocked List page, you can manage blocked list entries. The M500 rejects calls from numbers that match blocked list entries. You can sort, edit, delete, and add up to 200 blocked list entries. In order to back up your blocked list entries or import another blocked list file, the page also enables you to export and import the blocked list.

The blocked list 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.



In a dual cell configuration, the Blocked List page is only displayed in the WebUI of the **Primary** base station.

STATUS

SYSTEM

NETWORK

CONTACTS

Base Directory

Blocked List

LDAP

Remote XML

SERVICING

Blocked List

Select All Sort By Last Name

Total: 3	First Name	Last Name	Work	Mobile	Other	Account	
<input type="checkbox"/>	Aa-Won	Marketing			2325550108	1	Edit
<input type="checkbox"/>	Jordan	Tyler		2325551011		1	Edit
<input type="checkbox"/>	Roger	Fredricks			3215550109	1	Edit

First **1** Last

[Delete Selected Entries](#)
[Add New Entry](#)

[Clear Blocked List](#)

Import Blocked List

[Choose File](#)

[Import XML](#)

First line is header, skip [Import CSV](#)

Export Blocked List

[Export XML](#)
[Export CSV](#)

Table 5 describes the buttons available on the Blocked List page.

Table 5. Blocked List 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 blocked list file to import
Import XML Import CSV	Import a blocked list file in XML or CSV format
Export XML Export CSV	Export the blocked list file in XML or CSV format

To add a new blocked list entry:

1. Click [Add New Entry](#) .
The **Create Blocked List Entry** page appears.

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

Create Blocked List 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 1–48	Account 1
Work	Enter the appropriate telephone numbers in these fields.	n/a	Blank
Mobile			
Other			

Blocked List/Blacklist Import/Export

For a brand new M500 base station out of the box, the Blocked List will be empty. The best way to create an import file of blocked list entries is to first add a new entry to be used as a placeholder. Then export the Blocked List 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 Blocked List.

Importing a blocked list file will delete any existing entries in the Blocked List. The system will display a warning prompt, “All Blocked List entries will be deleted. Do you want to continue?”



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 204](#) – adds to existing entries
- [“file.contact.blacklist.overwrite” on page 204](#) – replaces existing entries

Blocked List files in XML format have the following tags:

Blocked List WebUI field	Blocked List 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>

Please note that although the above parameters and XML tags contain the word “blacklist”, they are for the Blocked List.

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 179.

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.

Setting	Description
Directory Name	Enter the LDAP directory name.
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.

Setting	Description
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.
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

The M500 supports the display of Broadsoft directories.

Setting	Description
XSI Directory Account	Select the desired account number to be used for cordless handset/deskset to access XSI directory.

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.

Remote XML

The M500 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 M500 will sync with the directory server. The M55 / M56 / M58 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>
```

ID	Name	Remote XML URI	Enable Incoming/Outgoing Call Lookup
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Resync Interval:

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	<p>Sets the name of the directory as it will appear on the M500 Directory list.</p> <p>The following order applies to the Directory list when multiple server-based directories are enabled:</p> <ol style="list-style-type: none">1. Local2. Blocked list3. LDAP4. Remote XML directory 15. Remote XML directory 26. Remote XML directory 3 <p>Any Remote XML directories will move up the list if LDAP directory is not enabled.</p>
Remote XML URI	<p>Enter the location of the XML directory file, from which the phone will sync and retrieve directory entries.</p>
Enable Incoming/ Outgoing Call Lookup	<p>Enables/disables the call lookup feature for incoming and outgoing calls.</p>
Resync Interval	<p>Sets the interval (in minutes) for the base station to automatically update the XML directory. To disable automatic updates, set the value to 0.</p>

Servicing Pages

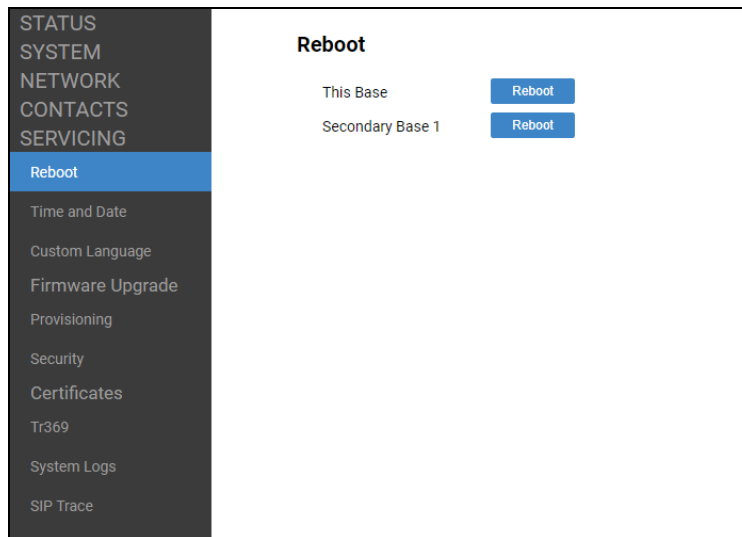
Reboot

To manually reboot the M500 base station and apply settings that you have updated, click



In a dual cell configuration:

- if you are signed on the WebUI of the primary base station, you can reboot the primary base station (indicated by **This Base**) or the secondary base station (indicated by **Secondary Base**).
- If you are signed on the WebUI of the secondary base station, you can reboot the secondary base station (indicated by **This Base**).



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 173.



In a dual cell configuration, the Time and Date page is only displayed in the WebUI of the **Primary** base station.

STATUS
SYSTEM
NETWORK
CONTACTS
SERVICING
Reboot
Time and Date
Custom Language
Firmware Upgrade
Provisioning
Security
Certificates
Tr369
System Logs
Site-Wide Settings

Time and Date Format

Date Format:

Time Format:

Network Time Settings:

Enable Network Time

NTP Server:

Use DHCP (Option 42)

Time Zone and Daylight Savings Settings

Time Zone:

Automatically adjust clock for Daylight Savings

User-defined Daylight Savings Time

Daylight Savings Start:

Daylight Savings End:

Daylight Savings Offset (minutes):

Use DHCP (Option 2/100/101)

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 DHCP (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: <ol style="list-style-type: none"> 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.

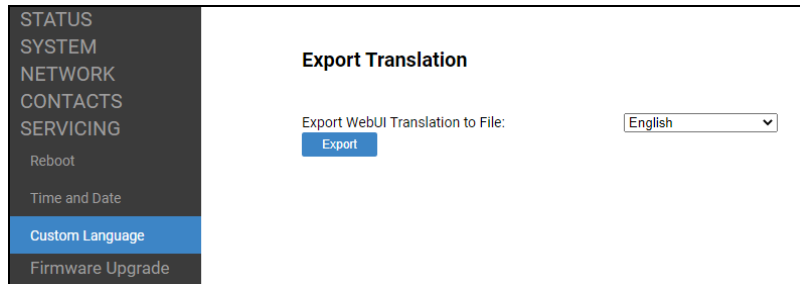
Setting	Description
Daylight Savings Start: <ul style="list-style-type: none">■ Month■ Week■ Day■ Hour	If User-defined DST is enabled, set the start date and time for daylight savings: Month, week, day, and hour.
Daylight Savings End: <ul style="list-style-type: none">■ Month■ Week■ Day■ Hour	If User-defined 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.

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.language.webui.url” on page 204](#).



The available languages for export are identical to the WebUI Language list described in [“User Preferences” on page 66](#).

The filename of the exported language file will be:

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

Firmware Upgrade

You can update the M500 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. Click **Firmware Upgrade** and enter the URL under **Firmware Server Settings**.
- **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 **Firmware Upgrade** and then click **Manual Upgrade** to view the page where you can manually upgrade the M500 firmware.

The firmware upgrade settings are also available as parameters in the configuration file. See [“provisioning” Module: Provisioning Settings](#) on page 168.

Auto Upgrade

Firmware Server Settings

In the table 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.



In a dual cell configuration, the Firmware Server Settings page is only displayed in the WebUI of the **Primary** base station.

Setting	Description
Base Firmware URL	The URL where the M500 Base Station firmware update file resides. This should be a full path, including the filename of the firmware file.

Setting	Description
Handset Firmware URL	The URL where the M55 Cordless Handset firmware update file resides. This should be a full path, including the filename of the firmware file.
Installed Handset Firmware	The version number of handset firmware currently installed.
Cordless Deskset Firmware URL	The URL where the M58 Deskset Accessory firmware update file resides. This should be a full path, including the filename of the firmware file.
Installed Cordless Deskset Firmware	The version number of deskset firmware currently installed.
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 Handset Firmware Now](#) , or [Install Cordless Deskset Firmware Now](#) .



NOTE

You can also configure the M500 to check for firmware updates at regular intervals. See [“Provisioning” on page 110](#).

Manual Firmware Update and Upload

On the Manual Firmware Update Settings page, you can upgrade the M500, handset, and cordless deskset firmware using a file located on your computer or local network.

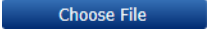

Updating the base station



NOTE

In a dual cell environment, you must perform the following steps on the **Primary** base station. The system will perform a site-wide auto firmware upgrade on all secondary base station(s) on the same site.

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

1. Under **Base File Name**, click  to locate and open the firmware update file.
2. Click .

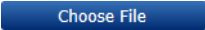

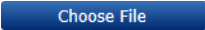

The confirmation dialog box shown below appears.

3. To begin installing the M500 firmware, click **OK**.

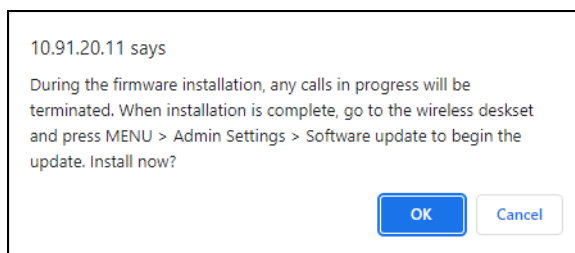
The message “Firmware installation in progress, the device will reboot after completion” appears.

4. Wait a few minutes for the base station to install the upgrade and reboot. You can keep refreshing the Web browser until you can sign in in the WebUI again.
5. To make sure the firmware on the base station(s) has been installed successfully, click **Status** and **Base Status**, and then check the **Version** column.

Updating handsets/desksets

1. **To update M55 / M56 handset firmware:** Under **Handset File name**, click  to locate and open the firmware update file, and then click .
2. **To update M58 deskset firmware:** Under **Cordless deskset File name**, click  to locate and open the firmware update file, and then click .

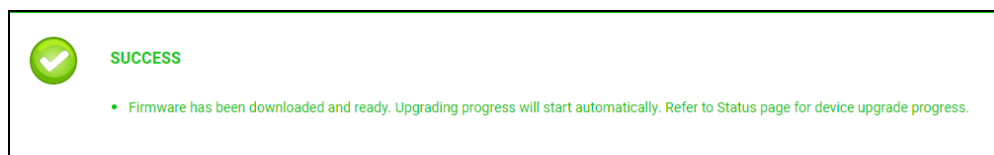
The confirmation dialog box shown below appears.



3. Click **OK**.

The message “Installing handset firmware. Please wait...” appears.

The message “Success” appears.



The base station(s) begin downloading the firmware file.


4. Open the **Status** > **Cordless Upgrade Status** page to check the progress of the firmware update.

Cordless Upgrade Status

Restart upgrades: [Restart](#)

Base	M58 Version	Handset Version	Shared Directory	Handset Wallpaper	Deskset Wallpaper	Upgrading
1	1.14.3	1.14.3 (16%)	27	255	255	Idle
2	1.14.3	1.14.3 (6%)	27	255	255	Idle

Cordless ID	Localized at Base	Type	Software Version	Shared Directory	Wallpaper Version	Upgrade Status
1	2	Handset	1.12.2	27	-1	Pending
2	2	Deskset	1.12.2	27	255	Idle
3	1	Handset	1.12.2	27	-1	Pending
4	1	Handset	1.12.2	27	-1	Pending

- The **Handset Version** and **M58 Version** columns show what percentage of the firmware file has been downloaded to the base station(s). Keep refreshing this page to update the percentage.
- After the firmware download is complete, the base station sends the firmware over the air to each of the registered handsets/desksets one at a time.
- The **Upgrade Status** column shows the progress of the firmware update for each registered handset/deskset – Pending, Updating, or Idle (update completed). Keep refreshing the web page to update the **Upgrade Status**.
- On the handset/deskset, a flashing icon  indicates the handset/deskset is receiving the firmware update from the base station in the background. When the update is completed, the icon disappears from the handset/deskset.

Provisioning

Provisioning refers to the process of acquiring and applying new settings for the M500 using configuration files retrieved from a remote computer. After a M500 is deployed, subsequent provisioning can update the M500 with new settings; for example, if your service provider releases new features. See also [“Provisioning Using Configuration Files” on page 129](#).

With automatic provisioning, the M500 checks periodically and/or during bootup for a settings update hosted by a provisioning server via the sever URL. The provisioning schedule and server URL can be configured via **Resynchronization** settings and **Provisioning Server** settings respectively (see [“Resynchronization” on page 112](#) and [“Provisioning Server” on page 111](#)).

Note: Auto firmware upgrade uses the same scheduler and can be enabled via provisioning.resync_mode as part of the process (see [“provisioning.resync_mode” on page 168](#)).

With manual provisioning on the WebUI, you update the M500 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 M500 at a time.

On the Provisioning page, you can enter settings that will enable the M500 to receive automatic configuration and firmware updates. The Provisioning page also allows you to manually update M500 configuration from a locally stored configuration file using an Import function. You can also export the M500 configuration—either to back it up or apply the configuration to another M500 in the future—to a file on your computer.

The M500 supports multiple ways to retrieve the provisioning server URL for zero-touch phone deployment. The following lists out the possible sources in the priority below:

1. PnP—Plug and Play Subscribe and Notify protocol
2. DHCP Options
3. Preconfigured URL—The URL will point to the Snom redirection server by default (see [“provisioning.server_address” on page 172](#)). This makes zero-touch phone deployment possible by enabling users to set up redirection rules and create provisioning templates through an account set up on the Snom Redirection and Provisioning Service (SRAPS) at <https://sraps.snom.com>.



Using SRAPS requires contacting the Snom support team for an account.

NOTE

If one of these sources is disabled, not available, or has not been configured, the M500 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 168](#).

STATUS SYSTEM NETWORK CONTACTS SERVICING Reboot Time and Date Custom Language Firmware Upgrade Provisioning Security Certificates Tr369 System Logs SIP Trace	<h3>Provisioning Server</h3> <p>Server URL: <input type="text" value="https://secure-provisioning.si"/></p> <p>Server Authentication Name: <input type="text"/></p> <p>Server Authentication Password: <input type="password"/></p> <h3>Plug-and-Play Settings</h3> <p><input checked="" type="checkbox"/> Enable PnP Subscribe</p> <h3>DHCP Settings</h3> <p><input checked="" type="checkbox"/> Use DHCP Options</p> <p>DHCP Option Priority 1: <input type="text" value="66"/></p> <p>DHCP Option Priority 2: <input type="text" value="159"/></p> <p>DHCP Option Priority 3: <input type="text" value="160"/></p> <p>Vendor Class ID (DHCP 60): <input type="text" value="snomM500"/></p> <p>User Class Info (DHCP 77): <input type="text" value="snomM500"/></p>
--	---

Provisioning Server



In a dual cell configuration, the settings listed below must be configured for each specific base station. These are NOT site-wide settings.

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	Sets the provisioning server address. The format of the URL must be RFC 1738 compliant, as follows: "<schema>://<user>:<password>@<host>:<port>/<url-path>" <ul style="list-style-type: none"> ■ "<user>:<password>@" may be empty. ■ "<port>" can be omitted if you do not need to specify the port number.
Server Authentication Name	Sets the authentication name for accessing the provisioning server.
Server Authentication Password	Sets the authentication password for accessing the provisioning server.

Plug-and-Play Settings



In a dual cell configuration, the setting listed below must be configured for each specific base station. This is NOT a site-wide setting.

Setting	Description
Enable PnP Subscribe	Enables or disables checking for the provisioning URL using Plug-and-Play Subscribe and Notify protocol. Select the checkbox to enable the M500 to search for the provisioning URL via a SUBSCRIBE message to a multicast address (224.0.1.75). The M500 expects the server to reply with a NOTIFY that includes the provisioning URL. The process times out after five attempts.

DHCP Settings



NOTE

In a dual cell configuration, the settings listed below must be configured for each specific base station. These are NOT site-wide settings.

Setting	Description
Use DHCP Options	Enables or disables checking for the provisioning URL using DHCP options. When selected, the M500 automatically attempts to get a provisioning URL through one of the enabled DHCP Option Priorities listed below. 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 81).
DHCP Option Priority 1	If DHCP is enabled, sets the first priority DHCP option for obtaining the provisioning URL.
DHCP Option Priority 2	If DHCP is enabled, sets the second priority DHCP option for obtaining the provisioning URL.
DHCP Option Priority 3	If DHCP is enabled, sets the DHCP Option priority. third priority DHCP option for obtaining the provisioning URL.
Vendor Class ID (DHCP 60)	Sets the vendor ID for DHCP option 60.
User Class Info (DHCP 77)	Sets the user class for DHCP option 77.

Resynchronization

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

Resynchronization

Mode:

Bootup Check:

Schedule Check:

Disable

Interval(minutes)

Days of the Week

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

Start Hour:

End Hour:

Use encryption for configuration file

Passphrase:



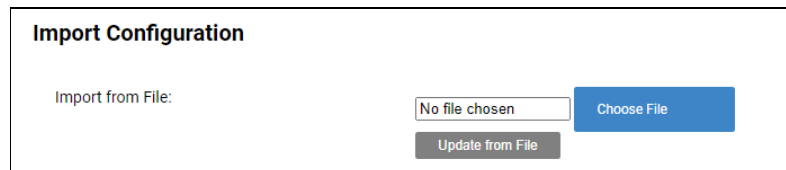
In a dual cell configuration, the settings listed below must be configured for each specific base station. These are NOT site-wide settings.

Setting	Description
Mode	<p>Sets the mode of the M500's provisioning/firmware file check. This determines which files the M500 retrieves when the resync process begins.</p> <p>The M500 can check for configuration files, firmware update files (from the URL entered on the Firmware Server Settings page), or both.</p> <p>Note: When checking for both configuration and firmware files, users have the option to specify the firmware URL within the configuration file. This firmware URL takes precedence over the existing URL on the Firmware Server Settings page. This enables you to change the firmware URL automatically.</p>
Bootup Check	<p>Sets the M500 to check the provisioning URL for new configuration and/or firmware files upon bootup. The update is applied as part of the reboot process.</p>
Schedule Check: Disable	<p>When selected, disables regularly scheduled file checking.</p>
Schedule Check: Interval(minutes)	<p>Sets an interval for checking for updates. After selecting Interval(minutes), enter the interval in minutes between update checks.</p>
Schedule Check: Days of the Week	<p>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 M500 checks for updates.</p>

Setting	Description
Start Hour	Select the hour of the day when the M500 checks for new firmware and/or configuration files.
End Hour	Select the hour of the day on which the M500 stops checking for new firmware and/or configuration files.
Use encryption for configuration file	Enables the use of encryption for the configuration file(s). Select this checkbox if you have encrypted the configuration file(s) using AES encryption. See “Securing configuration files with AES encryption” on page 135 .
Passphrase	Sets the AES encryption passphrase for decrypting the configuration file(s). Enter the key that was generated when you encrypted the file.

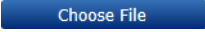
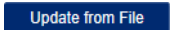
Import Configuration

You can configure the M500 by importing a configuration file from your computer or your local network. For information about the import behavior of settings, see [“Provisioning” on page 26](#). For information about configuration file types and configuration file formatting, see [“Provisioning Using Configuration Files” on page 129](#).



The screenshot shows a web interface titled "Import Configuration". It features a label "Import from File:" followed by a text input field containing "No file chosen". To the right of the input field is a blue button labeled "Choose File". Below the input field is a grey button labeled "Update from File".

To import a configuration file:

1. Click  to locate and open the configuration file.
2. Click .

The M500 will update its configuration.

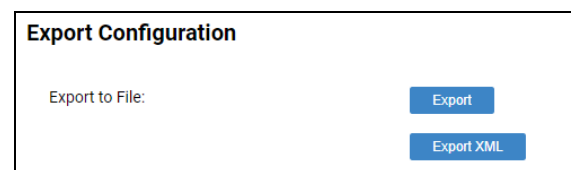
Manually importing a configuration file differs from the auto-provisioning process in that:

- The M500 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 M500 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.



The screenshot shows a web interface titled "Export Configuration". It features a label "Export to File:" followed by two blue buttons: "Export" and "Export XML".

For information about the export behavior of settings, see [“Exporting settings” on page 27](#).

To export the configuration file:

- Click .

The format of the exported file is **<model name>–<mac address>.htm**. For example, **M500–0011A0OCF489.htm**.

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:

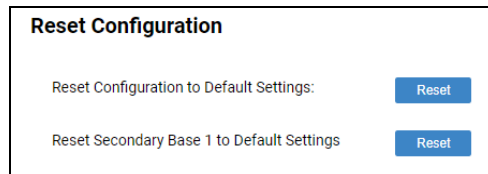
```
#Model Number = xxxxxxxx
```

```
#SW Version = xxxxxxxx
```

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 a single cell base station to its default configuration:

1. Under **Reset Configuration**, click  next to **Reset Configuration to Default Settings**.
2. When the confirmation box appears, click **OK**.


To reset a primary base station to its default configuration:

1. On the WebUI of the primary base station, under **Reset Configuration**, click  next to **Reset Configuration to Default Settings**.
2. When the confirmation box appears, click **OK**.

To reset a secondary base station to its default configuration:

1. On the WebUI of the secondary base station, under **Reset Configuration**, click  next to **Reset Configuration to Default Settings**.

–OR–

On the WebUI of the primary base station, under **Reset Configuration**, click  next to **Reset Secondary Base 1 to Default Settings**.

2. When the confirmation box appears, click **OK**.

Security

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

- Reset the admin password, support 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.

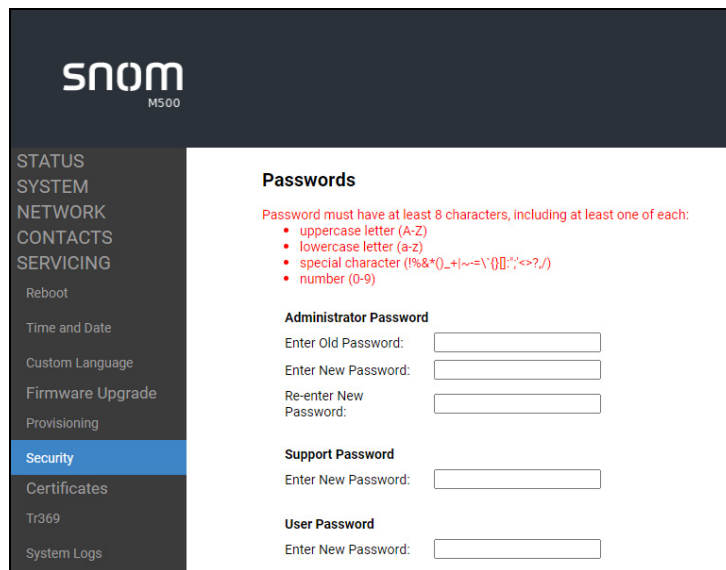
These security settings are also available as parameters in the configuration file. See [“web” Module: Web Settings](#) on page 184.

Passwords

You can set the administrator password, support 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 211.

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)



To change the admin password:

1. Enter the old password (for a new M500, the default password is **admin**).
2. Enter and re-enter a new password.
3. Click .

To change the support password:

1. Enter the new password.
The default password is **support**.

2. Click  .

To change the user password:

1. Enter the new password.
The default password is **user**.

2. Click  .

Web Server

Web Server

HTTP Server Port:

Enable Secure Browsing

HTTPS Server Port:

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 M500.

Cordless Pin Code

Cordless Pin Code

Cordless Pin Code:

Setting	Description
Cordless Pin Code	Sets the PIN for DECT registration with cordless device.

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.



In a dual cell configuration, the Trusted Servers section is only displayed in the WebUI of the **Primary** base station.

Trusted Servers

Accept SIP account servers only

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.



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

Trusted IP

Accept only allowed IP for incoming requests

Allowed IP 1:

Allowed IP 2:

Allowed IP 3:

Allowed IP 4:

Allowed IP 5:

Allowed IP 6:

Allowed IP 7:

Allowed IP 8:

Allowed IP 9:

Allowed IP 10:

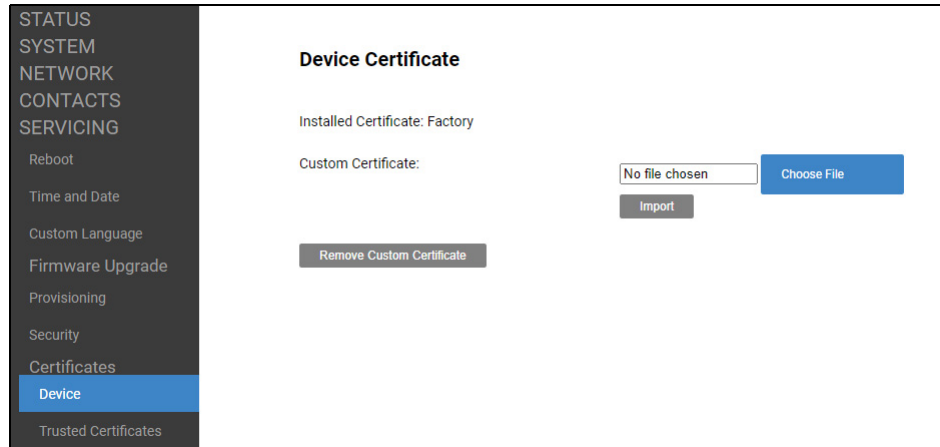
Setting	Description
Accept only allowed IP for incoming requests	Enable or disable using the “Allowed IP” list to filter all IP traffic.
Allowed IP 1–10	Enter IP addresses or address ranges to be used as sources of authorized IP traffic.

Certificates

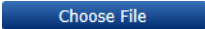

You can add two types of certificates using the WebUI or the provisioning file (see [“file” Module: Imported File Settings](#) on page 201). The two types of certificates are:

- 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.

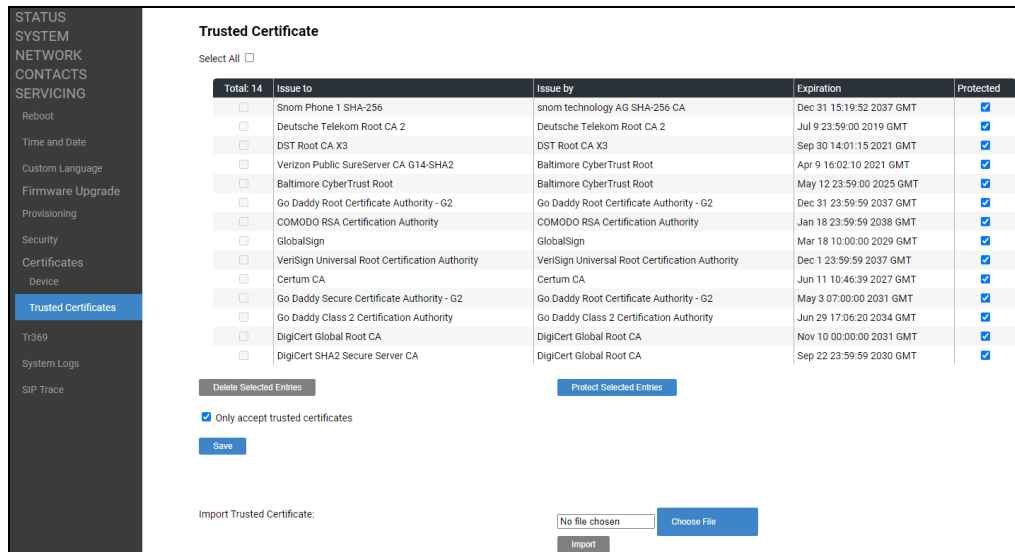
Device Certificate



To import a device certificate:

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

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-369 Settings

STATUS SYSTEM NETWORK CONTACTS SERVICING Reboot	TR369 <input type="checkbox"/> Enable TR369 Controller URL <input type="text" value="iot.snom.com"/> <input type="button" value="Save"/>
--	--

The provisioning settings are also available as parameters in the configuration file. See [“tr369” Module: TR-369 Settings](#) on page 205.



In a dual cell configuration, the TR-369 Settings page is only displayed in the WebUI of the **Primary** base station.

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 TR369	Enable or disable the TR369 module on device to support remote device management.
Controller URL	URL of the TR369 controller that our device is connecting to.

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 178](#).

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	<p>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.</p> <ul style="list-style-type: none">■ DEBUG■ INFO■ NOTICE■ WARN■ ERROR■ CRIT■ ALERT■ EMERG

The logging levels are:

- **DEBUG:** Developer messages for troubleshooting/debugging purposes.
- **INFO:** Normal operational messages.
- **NOTICE:** Events that are unusual but not error conditions. No immediate action is required.
- **WARN:** 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).
- **ALERT:** Conditions that should be corrected immediately (for example, a loss of backup ISP connection).
- **EMERG:** Emergency conditions that affect multiple apps/servers/sites.


Network Trace

To perform a network trace:

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

Download Log

To download the system log:

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

SIP Trace

The SIP Trace page displays a log of sent and received SIP packets. You can use this page to analyze and troubleshoot SIP issues.

STATUS

SYSTEM

NETWORK

CONTACTS

SERVICING

Reboot

Time and Date

Custom Language

Firmware Upgrade

Provisioning

Security

Certificates

Tr69

System Logs

SIP Trace

SIP Trace

Clear
Reload

```

Thu May 2 11:17:22 2024
Received on 10.91.20.124:5059 to 192.65.79.250:5060
SIP/2.0 403 Forbidden
Via: SIP/2.0/UDP 10.91.20.124:5059;received=206.108.192.2;branch=29HG4bK4137b1fBeeaa461;rport=64760
From: "0365" <sip:9725980365@iopas.tekvision.com>;tag=db826570a0
To: "0365" <sip:9725980365@iopas.tekvision.com>;tag=424949231-1714673842359
Call-ID: e18cce7d2bc0e53
CSeq: 1912911434 REGISTER
Content-Length: 0

-----
Thu May 2 11:17:32 2024
Sent on 10.91.20.124:5059 to 192.65.79.250:5060
REGISTER sip:iopas.tekvision.com SIP/2.0
Accept: application/reginfo+xml, application/rml+xml, application/sdp, application/simple-message-summary, application/watcherinfo+xml, message/sipfrag, multipart/mixed
Via: SIP/2.0/UDP 10.91.20.124:5059;branch=29HG4bK418947d9009127f96;rport
Route: <sip:sbc2.tekvision.com;r>
Max-Forwards: 70
From: "0365" <sip:9725980365@iopas.tekvision.com>;tag=064bd3e3de
To: "0365" <sip:9725980365@iopas.tekvision.com>
Call-ID: 64234c3840bf84ff0
CSeq: 1931891168 REGISTER
Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, SUBSCRIBE, UPDATE
Allow-Events: refer
Contact: <sip:9725980365@10.91.20.124:5059;transport=udp;expires=3600;reg-id=1;sip.instance="urn:uuid:52212ed6-6caa-4c26-82b2-0004138802E0">
Supported: eventlist, join, replaces, sdp-anat
User-Agent: snomM500/1.14.2
Content-Length: 0

-----
Thu May 2 11:17:32 2024
Received on 10.91.20.124:5059 to 192.65.79.250:5060
SIP/2.0 403 Forbidden
Via: SIP/2.0/UDP 10.91.20.124:5059;received=206.108.192.2;branch=29HG4bK418947d9009127f96;rport=64760
From: "0365" <sip:9725980365@iopas.tekvision.com>;tag=064bd3e3de
To: "0365" <sip:9725980365@iopas.tekvision.com>;tag=1631206439-1714673852557
                    
```

Click **Clear** to remove all the SIP packet contents and clear the on screen display.

Click **Reload** to reload the latest SIP packet contents. Newer SIP packets are added at the bottom of the page.

CHAPTER 4

PROVISIONING USING CONFIGURATION FILES

Provisioning using configuration files is the quickest way to configure multiple M500 Dual-cell SIP DECT Base Stations. You can place configuration files on a provisioning server, where the M500 Dual-cell SIP DECT Base Stations retrieve the files and update their configuration automatically.

Configuration files have the extension **.htm** and contain settings that will apply to M500 Dual-cell SIP DECT Base Stations. 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 M500 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 M500 configuration file modules and their associated parameters, see ["Configuration File Parameter Guide" on page 137](#).

Using the WebUI, you can also import a configuration file and apply the configuration file settings to the M500. For more information, see ["Import Configuration" on page 115](#).

This chapter covers:

- ["The Provisioning Process" on page 130](#)
- ["Configuration File" on page 132](#)
- ["Data Files" on page 133](#)
- ["Configuration File Tips and Security" on page 134](#).

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 110](#) and [“Resynchronization: configuration file checking” on page 131](#). The M500 maintains a list of the last loaded provisioning files. The M500 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 M500 checks for updated files after one minute of inactivity.

2. Download the configuration files.

If any file on the provisioning server has changed, the M500 treats it as a new file and downloads it.

If the provisioning URL specifies a path only with no filename, then by default the M500 looks for and retrieves the following file:

- MAC-specific file: **<model>–<MAC Address>.htm**.

The <model> variable is the Snom product model: M500, for example.

If the provisioning URL specifies both a path and filename, then the M500 retrieves only the configuration file specified.

3. The M500 restarts after one minute of inactivity.

During provisioning, the M500 reads the configuration file and validates each module and setting. The M500 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 137](#) 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 M500 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 M500 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 M500 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).

M500 restart

If the M500 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 M500 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 M500 will download the file(s) when there is no call activity.

When you update the M500 by importing a configuration file using the WebUI, the device restarts immediately after applying the new settings, regardless of whether the M500 is idle.

Configuration File

The MAC-specific configuration file has the filename format:

<model>--<MAC Address>.htm

The <model> variable is the Snom product model; for example, **M500**. For more information about the MAC-specific configuration file, see [“Guidelines for the MAC-specific configuration file” on page 134](#).

Data Files

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

- Directory (contacts, blocked list) 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 M500 Dual-cell SIP DECT Base Station may require.

None of the data files are exported when you export a configuration file from the M500. However, you can export a Directory or Blocked List .xml file using the WebUI. After modifying the .xml file, you can use the configuration file "file" module to have the M500 import the new file. For a complete list of data file parameters, see ["file" Module: Imported File Settings](#) on page 201.

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 the MAC-specific configuration file(s) you will need. You can store the MAC-specific file(s) on your provisioning server.

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

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

Create a MAC-specific configuration file for each M500 in your organization's telephone system. The file name must contain the M500 MAC address, which is printed on a label on the back of the device. For example, a Snom M500 Dual-cell SIP DECT Base Station with the MAC address of 00:11:A0:10:6F:2D would download the **M500-0011A0106F2D.htm** file.



NOTE

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

See also [“Suggested practice for importing configuration files in a dual cell operation:” on page 27.](#)

Securing configuration files with AES encryption

You can encrypt your configuration files to prevent unauthorized users modifying the configuration files. The M500 firmware decrypts files using the AES 256 algorithm. After encrypting a file and placing it on your provisioning server, you can enable the M500 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 M500. 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.

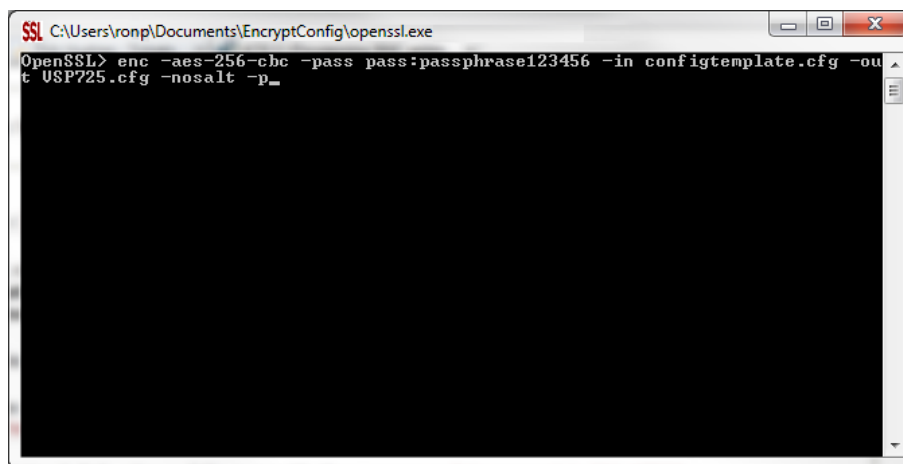


Figure 2. OpenSSL command line

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**.

Resynchronization

Mode:

Bootup Check:

Schedule Check:

Disable

Interval(minutes)

Days of the Week

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

Start Hour:

End Hour:

Use encryption for configuration file

Passphrase:

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

**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 M500 configuration file. Most settings in the configuration file have an equivalent in the WebUI (see the settings tables in [“Using the WebUI” on page 37](#)). However, the options you must enter when editing the configuration file have a different syntax and format.

There are two types of settings – site-wide and local. **Site-wide settings** are applicable to all base stations in a dual cell configuration. When you update a site-wide setting via provisioning, the setting will be automatically updated for all base stations in the system.

Local settings are applicable to a specific base station in a dual cell configuration. When you update a local setting via provisioning, the setting will only be updated for the specified base station.

The settings are divided into modules. Most modules correspond to a page on the M500 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 139](#)
- [“cordless” Module: Cordless Settings” on page 154](#)
- [“multicell” Module: Multicell Settings” on page 158](#)
- [“network” Module: Network Settings” on page 163](#)
- [“system” Module: System settings” on page 161](#)
- [“provisioning” Module: Provisioning Settings” on page 168](#)
- [“time_date” Module: Time and Date Settings” on page 173](#)

- [“log” Module: Log Settings” on page 178](#)
- [“remoteDir” Module: Remote Directory Settings” on page 179](#)
- [“web” Module: Web Settings” on page 184](#)
- [“trusted_ip” Module: Trusted IP Settings” on page 185](#)
- [“trusted_servers” Module: Trusted Server Settings” on page 186](#)
- [“user_pref” Module: User Preference Settings” on page 187](#)
- [“call_settings” Module: Call Settings” on page 189](#)
- [“speeddial” Module : Speed Dial Settings” on page 213](#)
- [“audio” Module: Audio Settings” on page 192](#)
- [“page_zone” Module: Page Zone Settings” on page 194](#)
- [“ppversion” Module: PP Version Settings” on page 196](#)
- [“alarm” Module: Alarm settings” on page 197](#)
- [“file” Module: Imported File Settings” on page 201](#)
- [“tr369” Module: TR-369 Settings” on page 205](#)
- [“tone” Module: Tone Definition Settings” on page 206](#)

"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 48 for the M500.

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 48 for the M500.

Site-wide settings

Setting: sip_account.x.dial_plan

Description: Sets the dial plan for account x. See ["Dial Plan" on page 54](#).

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:	<code>sip_account.x.inter_digit_timeout</code>		
Description:	Sets the inter-digit timeout (in seconds) for account x. The inter-digit timeout sets how long the M500 waits after the last digit is entered before dialing the number.		
Values:	1–10	Default:	3

Setting:	<code>sip_account.x.maximum_call_number</code>		
Description:	Sets the maximum number of concurrent active calls allowed for that account.		
Values:	1–8	Default:	8

Setting:	<code>sip_account.x.dtmf_transport_method</code>		
Description:	Sets the transport method for DTMF signaling for account x.		
Values:	auto, rfc2833, inband, info	Default:	auto

Setting:	<code>sip_account.x.unregister_after_reboot_enable</code>		
Description:	Enables or disables the M500 to unregister account x after rebooting.		
Values:	0 (disabled), 1 (enabled)	Default:	0

Setting:	<code>sip_account.x.primary_sip_server_address</code>		
Description:	Sets the SIP server IP address for account x.		
Values:	IPv4, IPv6 or FQDN	Default:	Blank

Setting:	<code>sip_account.x.primary_sip_server_port</code>		
Description:	Sets the SIP server port for account x.		
Values:	1–65535	Default:	5060

Setting:	<code>sip_account.x.primary_registration_server_address</code>		
Description:	Sets the registration server IP address for account x.		
Values:	IPv4, IPv6 or FQDN	Default:	Blank

Setting:	<code>sip_account.x.primary_registration_server_port</code>		
Description:	Sets the registration server port for account x.		
Values:	1–65535	Default:	5060
Setting:	<code>sip_account.x.primary_registration_expires</code>		
Description:	Sets the expiration time (in seconds) of the current registration for account x.		
Values:	30–7200	Default:	3600
Setting:	<code>sip_account.x.registration_retry_time</code>		
Description:	Sets the retry frequency of the current registration for account x.		
Values:	1–1800	Default:	10
Setting:	<code>sip_account.x.reliable_provisional_response_option</code>		
Description:	Sets the 100rel/PRACK option. Indicates if the reliable provisional responses are disabled, supported, or required.		
	1 (supported):		
	<ul style="list-style-type: none"> ■ 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):		
	<ul style="list-style-type: none"> ■ 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:	<code>sip_account.x.primary_outbound_proxy_server_address</code>		
Description:	Sets the outbound proxy server IP address for account x.		
Values:	IPv4, IPv6 or FQDN	Default:	Blank

Setting:	<code>sip_account.x.primary_outbound_proxy_server_port</code>		
Description:	Sets the outbound proxy server port for account x.		
Values:	1–65535	Default:	5060

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

Setting:	<code>sip_account.x.backup_outbound_proxy_server_port</code>		
Description:	Sets the backup outbound proxy server port for account x.		
Values:	1–65535	Default:	5060

Setting:	<code>sip_account.x.codec_priority.1</code>		
Description:	Sets the highest-priority codec for account x.		
Values:	g711u, g711a, g729, g726, g722, ilbc	Default:	g711u

Setting:	<code>sip_account.x.codec_priority.2</code>		
Description:	Sets the second highest-priority codec for account x.		
Values:	none, g711u, g711a, g729, g726, g722, ilbc	Default:	g711a

Setting:	<code>sip_account.x.codec_priority.3</code>		
Description:	Sets the third highest-priority codec for account x.		
Values:	none, g711u, g711a, g729, g726, g722, ilbc	Default:	g729

Setting:	<code>sip_account.x.codec_priority.4</code>		
Description:	Sets the fourth highest-priority codec for account x.		
Values:	none, g711u, g711a, g729, g726, g722, ilbc	Default:	g726

Setting:	<code>sip_account.x.codec_priority.5</code>		
Description:	Sets the fifth highest-priority codec for account x.		
Values:	none, g711u, g711a, g729, g726, g722, ilbc	Default:	g722
Setting:	<code>sip_account.x.codec_priority.6</code>		
Description:	Sets the highest-priority codec for account x.		
Values:	none, g711u, g711a, g729, g726, g722, ilbc	Default:	ilbc
Setting:	<code>sip_account.x.codec_priority.7</code>		
Description:	Sets the highest-priority codec for account x.		
Values:	none, g711u, g711a, g729, g726, g722, ilbc	Default:	none
Setting:	<code>sip_account.x.voice_encryption_enable</code>		
Description:	Enables or disables SRTP voice encryption for account x.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>sip_account.x.g729_annexb_enable</code>		
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 <code>sip_account.x.codec_priority</code> parameter.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>sip_account.x.ilbc_payload_type</code>		
Description:	Set the default payload type for the ilbc codec.		
Values:	96-127	Default:	98
Setting:	<code>sip_account.x.dscp</code>		
Description:	Sets the Voice Quality of Service Layer 3 - DSCP for account x.		
Values:	0-63	Default:	46

Setting:	<code>sip_account.x.sip_dscp</code>		
Description:	Sets the Signalling Quality of Service Layer 3 - DSCP for account x.		
Values:	0–63	Default:	26
Setting:	<code>sip_account.x.local_sip_port</code>		
Description:	Sets the Local SIP port for account x.		
Values:	1–65535	Default:	Account 1: 5059 Account 2-48: 5059+x e.g. Account 3: 5062
Setting:	<code>sip_account.x.type</code>		
Description:	Determines the call sharing nature among devices that share the usage of a SIP account. <ul style="list-style-type: none"> ■ standard: Established call with one device remains private and will not be shared with other devices sharing the SIP account ■ kle: Established call with one device will be visible to other devices sharing the SIP account. Shared device can interact with the call via Line keys or Call list. <p>where x = 1–48 (Account number).</p>		
Values:	standard, kle	Default:	kle (for account 1) standard (for account 2-48)
Setting:	<code>sip_account.x.transport_mode</code>		
Description:	Sets the Signalling Transport Mode for account x.		
Values:	udp, tcp, tls	Default:	udp
Setting:	<code>sip_account.x.mwi_enable</code>		
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:	<code>sip_account.x.mwi_subscription_expires</code>		
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:**

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:	<code>sip_account.x.keep_alive_enable</code>		
Description:	Enable SIP keep alive for NAT traversal and monitoring SIP server status.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>sip_account.x.keep_alive_interval</code>		
Description:	Sets the interval (in seconds) for sending keep-alives.		
Values:	1-3600	Default:	15
Setting:	<code>sip_account.x.keep_alive_ignore_failure</code>		
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:	<code>sip_account.x.music_on_hold_enable</code>		
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:	<code>sip_account.x.sip_session_timer_enable</code>		
Description:	Enables or disables the SIP session timer.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>sip_account.x.sip_session_timer_min</code>		
Description:	Sets the session timer minimum value (in seconds) for account x.		
Values:	90–65535	Default:	90
Setting:	<code>sip_account.x.sip_session_timer_max</code>		
Description:	Sets the session timer maximum value (in seconds) for account x.		
Values:	90–65535	Default:	1800

Setting:	<code>sip_account.x.check_trusted_certificate</code>		
Description:	Enables or disables accepting only a trusted TLS certificate for account x.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>sip_account.x.preferred_ptime</code>		
Description:	Enter the packetization interval time in milliseconds.		
Values:	10, 20, 30, 40, 50, 60	Default:	20
Setting:	<code>sip_account.x.cid_src_priority.1</code>		
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:	<code>sip_account.x.cid_src_priority.2</code>		
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:	<code>sip_account.x.cid_src_priority.3</code>		
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:	<code>sip_account.x.call_rejection_response_code</code>		
Description:	Select the response code for call rejection. This code applies to the following call rejection cases: <ul style="list-style-type: none"> ■ 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:	<code>sip_account.x.dtmf_payload_type</code>		
Description:	Set the configurable RTP payload type for in-call DTMF.		
Values:	96-127	Default:	101
Setting:	<code>sip_account.x.use_register_route_header</code>		
Description:	Use Route header for REGISTER		
Values:	0 (disabled), 1 (enabled)	Default:	1
Setting:	<code>sip_account.x.use_register_x_real_ip_header</code>		
Description:	If enabled, a custom X-Real-IP header will be added to SIP REGISTER messages. Otherwise, no custom header should be presented.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>sip_account.dirty_host_ttl</code>		
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:	<code>sip_account.mac_info_in_every_sip_message</code>		
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: <i>model /firmware version (MAC=MAC address)</i> e.g. User-Agent: snomM500/1.14.4 (MAC=000413BB0634)		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>sip_account.pnp_local_sip_port</code>		
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:** 5059

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

Setting:	<code>sip_account.x.sip_account_enable</code>		
Description:	Enables account x to be used by the device.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>sip_account.x.label</code>		
Description:	Sets the text that identifies the account on the device LCD. The account label appears on the Dialing Line list, dialing screen and other call appearance screens.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.display_name</code>		
Description:	Sets the text portion of the caller ID that is displayed for outgoing calls using account x.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.user_id</code>		
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. "@sip-service.com"). The configuration file automatically adds the default host name.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.authentication_name</code>		
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:	<code>sip_account.x.authentication_password</code>		
Description:	Sets the authentication password for account x. This parameter is NON-EXPORTABLE .		
Values:	Text string	Default:	Blank

Setting:	<code>sip_account.x.feature_sync_enable</code>		
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:	<code>sip_account.x.secure_renegotiation</code>		
Description:	Enables or disables SIP TLS secure renegotiation (RFC 5746 compliance). This parameter is only applicable to the TLS connection between the primary base and the server. This parameter is NON-EXPORTABLE .		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>sip_account.x.access_code_retrieve_voicemail</code>		
Description:	Sets the voicemail retrieval feature access code for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.access_code_dnd_on</code>		
Description:	Sets the do not disturb (DND) ON feature access code for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.access_code_dnd_off</code>		
Description:	Sets the do not disturb (DND) OFF feature access code for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.access_code_cfa_on</code>		
Description:	Sets the Call Forward All ON feature access code for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.access_code_cfa_off</code>		
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:	<code>sip_account.x.mwi_uri</code>		
Description:	Sets the MWI URI that will be used for MWI subscription. If this setting is left blank, the M500 uses the account x user ID for MWI subscription.		
Values:	SIP URI text string	Default:	Blank
Setting:	<code>sip_account.x.network_conference_enable</code>		
Description:	Enables or disables network conferencing for account x.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>sip_account.x.network_bridge_uri</code>		
Description:	Sets the URI for the network conferencing bridge on account x.		
Values:	Text string (SIP URI)	Default:	Blank

"cordless" Module: Cordless Settings

The cordless settings allow you to configure settings for the cordless handsets/desksets that are registered to the base station. For more information on registering cordless handsets/desksets, see the M55 / M56 / M58 User Guide.

Site-wide settings

All of the cordless settings are site-wide settings.

Setting:	<code>cordless.autoreg_enable</code>		
Description:	Enable or disable handset/deskset auto registration. <ul style="list-style-type: none"> ■ If enabled, handset/deskset with IPEI matching with cordless.x.ipei will be allowed to register without going through manual DECT registration. ■ Otherwise, handset/deskset have to be registered through manual DECT registration. ■ See also parameters cordless.x.ipei, system.x.registered_ipei 		
Values:	0 (disabled), 1 (enabled)	Default:	0

Setting:	<code>cordless.pin_code</code>		
Description:	PIN for DECT registration with cordless device.		
Values:	4-digit number	Default:	0000

Setting:	<code>cordless.statistics_enable</code>		
Description:	Enable our phone to send DECT statistics to a server via HTTP POST.		
Values:	0 (disabled), 1 (enabled)	Default:	1

Setting:	<code>cordless.statistics_post_authentication_name</code>		
Description:	Authentication user name for the server where our phone will send DECT statistics via HTTP POST.		
Values:	Text string	Default:	Blank

Setting:	<code>cordless.statistics_post_authentication_password</code>		
Description:	Authentication password for the server where our phone will send DECT statistics via HTTP POST.		
Values:	Text string	Default:	Blank

Setting: `cordless.statistics_post_timer`
Description: Frequency (in seconds) for our phone to send DECT statistics via HTTP POST.
Values: 1–32767 (seconds) **Default:** 3600

Setting: `cordless.statistics_post_url`
Description: Server URL where our phone will send DECT statistics via HTTP POST.
Values: URL **Default:** Blank

Setting: `cordless.statistics_timer`
Description: Frequency (in seconds) for base to collect statistics info from its registered cordless devices.
Values: Integer **Default:** 900

Setting: `cordless.theme`
Description: Sets the theme display for all the handsets/desksets.
Values: dark, light **Default:** dark

Setting: `cordless.wallpaper`
Description: Sets the wallpaper for all the handsets/desksets.
 Select Custom If custom wallpaper has been uploaded via parameters:
 file.handset_wallpaper or file.deskset_wallpaper
Values: none, snom, sky, ocean, starry, custom **Default:** dark

Setting: `cordless.wideband_enabled`
Description: Configure the use of wideband or narrowband for DECT audio.
 Changing to wideband mode lowers the system call capacity to four devices per base unit. A reboot is also required with all calls in progress terminated.
Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `cordless.x.allow_barge_in`

Description: Configures the default Call Privacy setting for handset/deskset x. If enabled, barge-in will be allowed for shared calls by default when a call is dialed out, answered or resumed from held on handset/deskset x. During a call, user can override the barge-in default via the PUI.

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

Setting: `cordless.x.default_account`

Description: Sets the default account for cordless handset/deskset x. The cordless handset/deskset attempts to use this account first when going off hook. Where x ranges from 1–48 (device number).
Note: The M500 supports a maximum of 16 devices in dual cell mode.

Values: 1–48 **Default:** 1

Setting: `cordless.x.device_name`

Description: Set the device name for cordless handset/deskset x. Where x ranges from 1–48 (device number).
Note: The M500 supports a maximum of 16 devices in dual cell mode.

Values: Text string **Default:** Blank

Setting: `cordless.x.ipei`

Description: Registration slot reserved for handset/deskset with the same IPEI as the configured one.

- Handset/deskset with the same IPEI as the configured IPEI can register as Handset/Deskset x without going through manual DECT registration.
- See also parameters **cordless.autoreg_enable**, **system.x.registered_ipei**.

Where x ranges from 1–48 (device number).
Note: The M500 supports a maximum of 16 devices in dual cell mode.

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

"multicell" Module: Multicell Settings

The multicell settings enable you to configure settings for the base station(s).

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

Site-wide settings

Setting:	<code>multicell.device.x.ip</code>		
Description:	This setting is READ-ONLY . Provides status information for bases on a dual cell site. Where x ranges from 1–2 (base number). 1 is reserved for primary base.		
Values:	IPv4 or IPv6	Default:	N/A

Setting:	<code>multicell.device.x.mac</code>		
Description:	This setting is READ-ONLY . Provides status information for bases on a dual cell site. Where x ranges from 1–2 (base number). 1 is reserved for primary base.		
Values:	Text string (MAC address)	Default:	N/A

Setting:	<code>multicell.device.x.rfpi</code>		
Description:	This setting is READ-ONLY . Provides status information for bases on a dual cell site. Where x ranges from 1–2 (base number). 1 is reserved for primary base.		
Values:	Text string (RFPI)	Default:	N/A

Setting: multicell.site_id

Description: With matched site identifier, it allows primary base and multiple secondary bases to form a site. **Once a site is joined by one or more secondary base(s), multicell.site_id should not be modified.**

- For "primary" base, multicell.site_id will automatically be filled with its own MAC address, which will be used as the site identifier of the site by default. Configuration of the parameter is not required by the user.
- For "secondary" base, multicell.site_id can be left as unconfigured to allow the base to join any available "primary" base to form a site. Configuration of the parameter is not required by the user.

Values: Text string (<18 characters) **Default:** Blank

“system” Module: System settings

The system settings enables you to configure DECT related settings for the M500 Dual-cell SIP DECT Base Station.

Site-wide settings

Setting:	<code>system.eco</code>		
Description:	Enables or disables ECO mode.		
Values:	0 (disabled), 1 (enabled)	Default:	0

Setting:	<code>system.x.registered_ipei</code>		
Description:	This setting is READ-ONLY , and indicates handset/deskset registration status (for both auto & manual registration), where x ranges from 1-48 (device number). <ul style="list-style-type: none"> ■ [blank] if no handset/deskset is registered to the slot ■ See also parameters <code>cordless.autoreg_enable</code> and <code>cordless.x.ipei</code>. <p style="text-align: center;">This parameter is NON-EXPORTABLE.</p>		
Values:	N/A	Default:	N/A

Local settings



In a dual cell configuration, the settings listed below must be configured for each specific base station. These are NOT site-wide settings.

Setting:	<code>system.command_key_for_reboot</code>		
Description:	This setting is READ-ONLY , and is meant for INTERNAL DIAGNOSTIC purposes.		
Values:	Text string	Default:	N/A

Setting:	<code>system.dcx_reboot_cnt</code>		
Description:	This setting is READ-ONLY , and is meant for INTERNAL DIAGNOSTIC purposes.		
Values:	Integer	Default:	N/A

Setting:	<code>system.last_reboot_reason</code>		
Description:	This setting is READ-ONLY , and is meant for INTERNAL DIAGNOSTIC purposes.		
Values:	Text string	Default:	N/A

"network" Module: Network Settings

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

Local settings



In a dual cell configuration, the settings listed below must be configured for each specific base station. These are NOT site-wide settings.

Setting:	<code>network.vlan.pc.enable</code>		
Description:	Enables or disables the PC Port VLAN (on the M500 port labeled "MULTI-CELL").		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>network.vlan.pc.id</code>		
Description:	Sets the PC Port VLAN ID.		
Values:	0–4095	Default:	0
Setting:	<code>network.vlan.pc.priority</code>		
Description:	Sets the PC port VLAN priority.		
Values:	0–7	Default:	0
Setting:	<code>network.vlan.wan.enable</code>		
Description:	Enables or disables the WAN VLAN (on the M500 port labeled "NET").		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>network.vlan.wan.id</code>		
Description:	Sets the WAN VLAN ID.		
Values:	0–4095	Default:	0
Setting:	<code>network.vlan.wan.priority</code>		
Description:	Sets the WAN port VLAN priority.		
Values:	0–7	Default:	0

Setting:	<code>network.lldp_med.enable</code>
Description:	Enables or disables LLDP-MED.
Values:	0 (disabled), 1 (enabled) Default: 1

Setting:	<code>network.lldp_med.interval</code>
Description:	Sets the LLDP-MED packet interval (in seconds).
Values:	1–30 Default: 30

Setting:	<code>network.dhcpv6_vendor_class_id</code>
Description:	Sets the vendor ID for DHCPv6 option 16.
Values:	Text string Default: M500

Setting:	<code>network.eapol.enable</code>
Description:	Enables or disables 802.1x EAPOL.
Values:	0 (disabled), 1 (enabled) Default: 0

Setting:	<code>network.eapol.identity</code>
Description:	Sets the 802.1x EAPOL identity.
Values:	Text string Default: Blank

Setting:	<code>network.eapol.password</code>
Description:	Sets the 802.1x EAPOL MD5 password. This parameter is NON-EXPORTABLE .
Values:	Text string Default: Blank

Setting:	<code>network.vendor_class_id</code>
Description:	Sets the vendor ID for DHCP option 60.
Values:	Text string Default: snomM500

Setting:	<code>network.user_class</code>
Description:	Sets the user class for DHCP option 77.
Values:	Text string Default: snomM500

Setting:	<code>network.ip.mode</code>		
Description:	Sets the IPv4 network mode.		
Values:	disable, dhcp, static, pppoe	Default:	dhcp
Setting:	<code>network.ip.static_ip_addr</code>		
Description:	Sets a static IP address for the network.		
Values:	Text string (IPv4)	Default:	Blank
Setting:	<code>network.ip.subnet_mask</code>		
Description:	Sets the subnet mask for the network.		
Values:	Text string (IPv4)	Default:	Blank
Setting:	<code>network.ip.gateway_addr</code>		
Description:	Sets the Gateway IP address.		
Values:	Text string (IPv4)	Default:	Blank
Setting:	<code>network.ip.dns1</code>		
Description:	Sets the primary DNS server IP address.		
Values:	Text string (IPv4)	Default:	Blank
Setting:	<code>network.ip.dns2</code>		
Description:	Sets the secondary DNS server IP address.		
Values:	Text string (IPv4)	Default:	Blank
Setting:	<code>network.ip.manually_configure_dns</code>		
Description:	Enable or disable manual DNS configuration.		
Values:	0 (disable), 1 (enable)	Default:	0

Setting:	<code>network.ip.pppoe.service_name</code>		
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:	<code>network.ip.pppoe.username</code>		
Description:	If IPv4 mode is PPPoE, enter your PPPoE account username.		
Values:	Text string	Default:	Blank

Setting:	<code>network.ip.pppoe.password</code>		
Description:	If parameter <code>network.ip.mode</code> is pppoe, enter your PPPoE account password. This parameter is NON-EXPORTABLE .		
Values:	Text string	Default:	Blank

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

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

Setting:	<code>network.ip6.prefix</code>		
Description:	When IPv6 mode is static, enter the IPv6 address prefix length.		
Values:	0–128	Default:	64

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

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

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

Setting:	<code>network.ip6.manually_configure_dns</code>		
Description:	Enable or disable manual DNS configuration for IPv6.		
Values:	0 (disable), 1 (enable)	Default:	0

"provisioning" Module: Provisioning Settings

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

Local settings



In a dual cell configuration, the settings listed below must be configured for each specific base station. These are NOT site-wide settings.

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

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

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

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

Setting:	<code>provisioning.resync_mode</code>		
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,	Default:	config_and_firmware
	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:	<code>provisioning.remote_check_sync_enable</code>
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:	<code>provisioning.crypto_enable</code>
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:	<code>provisioning.crypto_passphrase</code>
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:	<code>provisioning.check_trusted_certificate</code>
Description:	Enables or disables accepting only a trusted TLS certificate for access to the provisioning server.
Values:	0 (disabled), 1 (enabled) Default: 0

Setting:	<code>provisioning.pnp_enable</code>
Description:	Enables or disables the M500 checking for the provisioning URL using the Plug-and-Play Subscribe and Notify protocol.
Values:	0 (disabled), 1 (enabled) Default: 1

Setting:	<code>provisioning.pnp_response_timeout</code>
Description:	Sets how long the M500 repeats the SUBSCRIBE request if there is no reply from the PnP server.
Values:	1–60 Default: 10

Setting:	<code>provisioning.firmware_url</code>		
Description:	Sets the URL for the server hosting the firmware file.		
Values:	URI	Default:	Blank
Setting:	<code>provisioning.cordless_deskset_firmware_url</code>		
Description:	Sets the URL for the server hosting the cordless deskset firmware file.		
Values:	URI	Default:	Blank
Setting:	<code>provisioning.handset_firmware_url</code>		
Description:	Sets the URL for the server hosting the handset firmware file.		
Values:	URI	Default:	Blank
Setting:	<code>provisioning.fw_server_username</code>		
Description:	Sets the authentication name for the server hosting the firmware file.		
Values:	Text string	Default:	Blank
Setting:	<code>provisioning.fw_server_password</code>		
Description:	Sets the authentication password for the server hosting the firmware file. This parameter is NON-EXPORTABLE .		
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>/snomM500.htm
http://<path>/snomM500-{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://secure-provisioning.snom.com/snomM500/{mac}.htm`

Setting: `provisioning.server_username`

Description: Sets the authentication name for the provisioning server.

Values: Text string **Default:** Blank

Setting: `provisioning.server_password`

Description: Sets the authentication password for the provisioning server. This setting is **NON-EXPORTABLE**.

Values: Text string **Default:** Blank

"time_date" Module: Time and Date Settings

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

Site-wide settings

All of the time and date settings are site-wide settings.

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.clock_24hr

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

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:	<code>time_date.ntp_server_update_interval</code>		
Description:	Sets the delay between NTP server updates, in seconds.		
Values:	0-4294967295	Default:	1000

"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].

Site-wide settings

All of the log settings are site-wide settings.

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.

7—debug
 6—informational
 5—notice
 4—warning
 3—error
 2—critical
 1—alert
 0—emergency

Values: 0–7 **Default:** 4

"remoteDir" Module: Remote Directory Settings

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

Site-wide settings

All of the remote directory settings are site-wide settings.

Setting:	<code>remoteDir.ldap_enable</code>		
Description:	Enables or disables the M500 Dual-cell SIP DECT Base Station's access to the LDAP directory.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>remoteDir.ldap_directory_name</code>		
Description:	Sets the LDAP directory name.		
Values:	Text string	Default:	Blank
Setting:	<code>remoteDir.ldap_server_address</code>		
Description:	Sets the LDAP server IP address.		
Values:	Text string	Default:	Blank
Setting:	<code>remoteDir.ldap_port</code>		
Description:	Sets the LDAP server port.		
Values:	1-65535	Default:	389
Setting:	<code>remoteDir.ldap_protocol_version</code>		
Description:	Sets the LDAP protocol version.		
Values:	version_2, version_3	Default:	version_3
Setting:	<code>remoteDir.ldap_authentication_type</code>		
Description:	Sets the LDAP authentication type.		
Values:	simple, ssl	Default:	simple

Setting:	<code>remoteDir.ldap_user_name</code>		
Description:	Sets the LDAP authentication user name.		
Values:	Text string	Default:	Blank
Setting:	<code>remoteDir.ldap_password</code>		
Description:	Sets the LDAP authentication password. This setting is NON-EXPORTABLE .		
Values:	Text string	Default:	Blank
Setting:	<code>remoteDir.ldap_base</code>		
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:	<code>remoteDir.ldap_max_hits</code>		
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:	<code>remoteDir.ldap_search_delay</code>		
Description:	Sets the LDAP maximum search delay in seconds.		
Values:	0-500	Default:	0
Setting:	<code>remoteDir.ldap_firstname_filter</code>		
Description:	Sets the LDAP first name attribute filter.		
Values:	Text string	Default:	Blank
Setting:	<code>remoteDir.ldap_lastname_filter</code>		
Description:	Sets the LDAP last name attribute filter.		
Values:	Text string	Default:	Blank

Setting:	<code>remoteDir.ldap_number_filter</code>		
Description:	Sets the LDAP number filter.		
Values:	Text string	Default:	Blank
Setting:	<code>remoteDir.ldap_firstname_attribute</code>		
Description:	Sets the name attributes. Enter the name attributes that you want the M500 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:	<code>remoteDir.ldap_lastname_attribute</code>		
Description:	Sets the last name attributes.		
Values:	Text string	Default:	Blank
Setting:	<code>remoteDir.ldap_work_number_attributes</code>		
Description:	Sets the number attributes. Enter the number attributes that you want the M500 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:	<code>remoteDir.ldap_mobile_number_attributes</code>		
Description:	Sets the mobile number attributes.		
Values:	Text string	Default:	Blank
Setting:	<code>remoteDir.ldap_other_number_attributes</code>		
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 M500 searches the LDAP directory for the incoming call number. If the number is found, the M500 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.resync_interval`

Description: Sets the interval (in minutes) for the base station to automatically update the XML directory. To disable automatic updates, set the value to 0.

Values: 0–65535 **Default:** 0

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].

Site-wide settings

All of the web settings are site-wide settings.

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 M500. 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].

Site-wide settings

All of the trusted_IP settings are site-wide settings.

Setting:	<code>trusted_ip.only_accept_allowed_ip</code>
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:	<code>trusted_ip.x.allow_ip</code>
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 120 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 M500. 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].

Site-wide settings

All of the trusted_server settings are site-wide settings.

Setting:	<code>trusted_servers.only_accept_sip_account_servers</code>
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 M500 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]`.

Site-wide settings

All of the user preference settings are site-wide settings.

Setting:	<code>user_pref.call_terminated.busy_tone_enable</code>		
Description:	Enables the M500 to play a busy tone when the far-end party ends the call, or when a network error condition (keep-alive failure) occurs.		
Values:	0 (disabled), 1 (enabled)	Default:	0

Setting:	<code>user_pref.account.x.diversion_display</code>		
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:	<code>user_pref.feature_access_code_on_sip_registered_enable</code>		
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

Setting:	<code>user_pref.web_language</code>	Default:	en
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).		

"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 48.

Site-wide settings

All of the call settings are site-wide settings.

Setting:	<code>call_settings.early_media_preferred</code>		
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). <ul style="list-style-type: none"> ■ 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

Setting:	<code>call_settings.ext_conf_limit</code>		
Description:	In a dual-cell system, sets the maximum number of external conference calls per base. If set to 0, conference calls are disabled. For single base system, there is no restriction.		
Values:	0-8	Default:	2

Setting:	<code>call_settings.account.x.block_anonymous_enable</code>		
Description:	Enables or disables anonymous call blocking.		
Values:	0 (disabled), 1 (enabled)	Default:	0

Setting:	<code>call_settings.account.x.outgoing_anonymous_enable</code>		
Description:	Enables or disables outgoing anonymous calls.		
Values:	0 (disabled), 1 (enabled)	Default:	0

Setting:	<code>call_settings.account.x.dnd_enable</code>		
Description:	Enables or disables Do Not Disturb for account x.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>call_settings.account.x.call_fwd_always_enable</code>		
Description:	Enables or disables Call Forward Always for account x.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>call_settings.account.x.call_fwd_always_target</code>		
Description:	Sets the Call Forward Always target number for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>call_settings.account.x.call_fwd_busy_enable</code>		
Description:	Enables or disables Call Forward Busy for account x.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>call_settings.account.x.call_fwd_busy_target</code>		
Description:	Sets the Call Forward Busy target number for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>call_settings.account.x.call_waiting_enable</code>		
Description:	Enables or disables Call Waiting for account x.		
Values:	0 (disabled), 1 (enabled)	Default:	1
Setting:	<code>call_settings.account.x.cfna_enable</code>		
Description:	Enables or disables Call Forward No Answer for account x.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>call_settings.account.x.cfna_target</code>		
Description:	Sets the Call Forward No Answer target number for account x.		
Values:	Text string	Default:	Blank

Setting:	<code>call_settings.account.x.cfna_delay</code>		
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.

Site-wide settings

All of the audio settings are site-wide settings.

Setting:	<code>audio.x.jitter_mode</code>		
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:	<code>audio.x.fixed_jitter.delay</code>		
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:	<code>audio.x.adaptive_jitter.min_delay</code>		
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:	<code>audio.x.adaptive_jitter.target_delay</code>		
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:	<code>audio.x.adaptive_jitter.max_delay</code>		
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:	<code>audio.x.rtp.port_start</code>		
Description:	Sets the Local RTP port range start.		
Values:	1–65535	Default:	18000

Setting:	<code>audio.x.rtp.port_end</code>		
Description:	Sets the Local RTP port range end.		
Values:	1-65535	Default:	19000

Setting:	<code>audio.rtcp_xr.enable</code>		
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:	1

“page_zone” Module: Page Zone Settings

The page zone settings enable you to define groups of cordless devices for paging.

Site-wide settings

All of the page zone settings are site-wide settings.

Setting:	<code>page_zone.group.x.members</code>		
Description:	Comma-delimited list of registered cordless devices to be included as members of the paging group. Each member is identified by its registered cordless index. e.g. <code>page_zone.group.1.members = 1,2,3,4,46,48</code> Where x ranges from 1–6 (Paging group number).		
Values:	Comma-delimited list of registered cordless devices index where each index ranges from 1–48	Default:	Blank

Setting:	<code>page_zone.group.x.name</code>		
Description:	Name of the paging group. Where x ranges from 1–6 (Paging group number).		
Values:	Text string (maximum 15 characters)	Default:	Group <x>

Setting:	<code>page_zone.pager_tone_delay</code>		
Description:	Number of seconds to delay a person from speaking when sending a page. During this time, the handset/deskset displays the message “Setting up. Please wait for the tone.” After this time has elapsed, the sender’s handset/deskset makes a page tone, and displays “Broadcasting” with a timer. The person making the page can then begin speaking.		
Values:	1–5	Default:	3

Setting:	<code>page_zone.group.x.enable_external_page</code>		
Description:	Configure the paging group for either internal or external paging operations.		
	If enabled:		
	<ul style="list-style-type: none"> ■ The paging group is set for external paging operation. ■ <code>page_zone.group.x.multicast_address</code> and <code>page_zone.group.x.multicast_port</code> must match the settings on external parties for paging to / receive from external parties. ■ Multicast paging from an external party to the configured IP address and port will reach all members of the paging group. ■ Paging initiated by any handset/deskset will reach both the configured members of the paging group and the external parties listening to the configured multicast IP address and port. 		
	If disabled:		
	<ul style="list-style-type: none"> ■ The paging group is set for internal paging operations. ■ <code>page_zone.group.x.multicast_address</code> and <code>page_zone.group.x.multicast_port</code> can be left blank to use default setting or can be configured with custom settings. ■ Multicast paging from the external party to the configured IP address and port will not be accepted by the M500. ■ By nature of multicast, external parties listening to the configured IP address and port can still hear paging initiated by a handset/deskset. To prevent this, configure the IP address and port to a different combination. 		
	Where x ranges from 1–6 (Paging group number).		
Values:	0 (disabled), 1 (enabled)	Default:	0

Setting:	<code>page_zone.group.x.multicast_address</code>		
Description:	Multicast IP address for multicast paging with external parties. Can be left blank if <code>page_zone.group.x.enable_external_page</code> is disabled. Where x ranges from 1–6 (Paging group number).		
Values:	IP address	Default:	Blank

Setting:	<code>page_zone.group.x.multicast_port</code>		
Description:	Multicast port for multicast paging with external parties. Can be left blank if <code>page_zone.group.x.enable_external_page</code> is disabled. Where x ranges from 1–6 (Paging group number).		
Values:	Integer	Default:	Blank

“ppversion” Module: PP Version Settings

The PP version settings provide read-only diagnostic information.

Site-wide settings

All of the PP version settings are site-wide settings.

Setting:	<code>ppversion.version_vec</code>		
Description:	This setting is READ-ONLY . Provides site-wide handset synchronization version info for diagnostic purposes.		
Values:	Text string	Default:	N/A

“alarm” Module: Alarm settings

The alarm settings enable you to configure the emergency alarm for M56 handsets.

Site-wide settings

All of the page zone settings are site-wide settings.

Setting: `alarm.cordless.x.intercom`

Description: Sets the device number the M56 handset will intercom call when the alarm is signaled. Used when `alarm.x.signal` is set to "intercom". Where x ranges from 1–48 (device number).
 Note: The M500 supports a maximum of 16 devices in dual cell mode.

Values: 1-16 **Default:**

Setting: `alarm.cordless.x.line`

Description: Specifies which line to use on the M56 handset when the alarm is signaled. Where x ranges from 1–48 (device number).
 Note: The M500 supports a maximum of 16 devices in dual cell mode.

Values: 1–48 **Default:** 1

Setting: `alarm.cordless.x.number`

Description: Sets the telephone number the M56 handset will call when the alarm is signaled. Used when `alarm.x.signal` is set to "call". Where x ranges from 1–48 (device number).
 Note: The M500 supports a maximum of 16 devices in dual cell mode.

Values: Text string **Default:** Blank

Setting: `alarm.cordless.x.paging`

Description: Sets the paging group the M56 handset will page when the alarm is signaled. Used when `alarm.x.signal` is set to "paging". Where x ranges from 1–48 (device number).
 Note: The M500 supports a maximum of 16 devices in dual cell mode.

Values: 1-6 **Default:** 1

Setting: `alarm.cordless.x.profile`

Description: Sets which alarm profiles are active. Space-delimited list of alarm profile numbers. For example, 1 2 4 indicates alarm profile numbers 1, 2 and 4 are active.
Where x ranges from 1–48 (device number).
Note: The M500 supports a maximum of 16 devices in dual cell mode.

Values: Space-delimited list of alarm profile numbers where each number ranges from 1–8

Default: Blank

Setting: `alarm.x.howling_enable`

Description: If this setting is enabled, the M56 handset will emit an alarm sound until it has established a call/intercom call/page with the alarm recipient.
Where x ranges from 1–8 (alarm profile number).

Values: 0 (disabled), 1 (enabled)

Default: 0

Setting: `alarm.x.label`

Description: Optional: Assigns a name to each configured alarm profile. The name is added in parentheses to the available profiles on the **M56 Handset** section of the WebUI **Alarm** page.
Where x ranges from 1–8 (alarm profile number).

Values: Text string (maximum 15 characters)

Default: Blank

Setting: `alarm.x.pre_alarm_delay`

Description: Enter the number of seconds from the moment the M56 handset's alarm is activated that the handset will wait before calling the alarm number. The display will show the "Pre-alarm triggered" message.
If `alarm.x.howling_enable` is enabled, the M56 handset plays a continuous loud alarm sound.
Where x ranges from 1–8 (alarm profile number).

Values: 0 -254

Default: 0

Setting:	alarm.x.signal		
Description:	<p>Defines the way an alarm is signaled.</p> <ul style="list-style-type: none"> ■ call : the M56 handset calls the telephone number defined in alarm.cordless.x.number ■ intercom : the M56 handset makes an intercom call to the device defined in alarm.cordless.x.intercom ■ paging : the M56 handset pages the paging group defined in alarm.cordless.x.paging <p>Where x ranges from 1–8 (alarm profile number).</p>		
Values:	call, intercom, paging	Default:	call

Setting:	alarm.x.stop_alarm_enable		
Description:	<p>If this setting is enabled, the call/intercom call/page to the alarm recipient can be canceled from the M56 handset. Where x ranges from 1–8 (alarm profile number).</p>		
Values:	0 (disabled), 1 (enabled)	Default:	0

Setting:	alarm.x.stop_pre_alarm_enable		
Description:	<p>If this setting is enabled, the pre-alarm can be canceled from the M56 handset.</p> <p>Where x ranges from 1–8 (alarm profile number).</p>		
Values:	0 (disabled), 1 (enabled)	Default:	0

Setting:	alarm.x.trigger_delay		
Description:	<p>Enter the time delay (in seconds) that the M56 handset will wait before making a call/intercom call/page to the alarm recipient or, if alarm.x.pre_alarm_delay has also been configured, before the pre-alarm delay is triggered.</p> <p>Where x ranges from 1–8 (alarm profile number).</p>		
Values:	0–254	Default:	0

Setting:	<code>alarm.x.type</code>
Description:	Defines the method that is used to trigger the M56 alarm for the specified alarm profile.
	<p>alarm button:</p> <ul style="list-style-type: none"> ■ Press and hold the alarm key on the top of the M56 handset for 1.5 seconds + <code>alarm.x.trigger_delay</code> time <p>running:</p> <ul style="list-style-type: none"> ■ Swing or shake the M56 handset with frequency > 1.5 Hz in any direction ■ Continuous action > <code>alarm.x.trigger_delay</code> + 3 seconds <p>no movement:</p> <ul style="list-style-type: none"> ■ M56 handset in a steady position (any angle) ■ Continuous no movement time > <code>alarm.x.trigger_delay</code> time (e.g. if the user is sleeping or forgot to bring the handset) <p>man down:</p> <ul style="list-style-type: none"> ■ M56 handset lay down in horizontal position: 0-15 degrees ■ Continuous no movement time > <code>alarm.x.trigger_delay</code> + 5 seconds (Note: If M56 handset is in horizontal position and steady, it will trigger No movement alarm first. If pre-alarm is disregarded then it will trigger Man down alarm.) <p style="text-align: center;">OR</p> <ul style="list-style-type: none"> ■ Continuous movement (in horizontal direction) time > <code>alarm.x.trigger_delay</code> + 5 seconds (This case is assumed an injured person laying down but can move slowly.)
	Where x ranges from 1–8 (alarm profile number).
Values:	alarm button, running, no movement, man down, disabled
	Default: disabled

"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 M500 has a default self-signed web server certificate)
- Provisioning
- Languages

File parameter values are URLs that direct the M500 to the location of the file to be imported.

None of these settings are exported when you manually export the configuration from the M500.

Site-wide settings

All of the imported file settings are site-wide settings.

Setting:	<code>file.certificate.x.url</code>		
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:	<code>file.protected_certificate.x.url</code>		
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:	<code>file.certificate.trusted.url</code>		
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, <code><protocol>://<user>:<password>@<host>:<port>/<url-path></code> This parameter is NON-EXPORTABLE .		
Values:	URI	Default:	Blank
Setting:	<code>file.protected_certificate.trusted.url</code>		
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, <code><protocol>://<user>:<password>@<host>:<port>/<url-path></code> This parameter is NON-EXPORTABLE .		
Values:	URI	Default:	Blank
Setting:	<code>file.protected_certificate.custom_device.url</code>		
Description:	URL to upload a custom device certificate to override the factory installed device certificate. For example, <code><protocol>://<user>:<password>@<host>:<port>/<url-path></code> 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.

Enables you to delete custom wallpaper files.

- `removewallpaper_handset`: remove the handset wallpaper file.
- `removewallpaper_deskset`: remove the deskset wallpaper file.

This parameter is **NON-EXPORTABLE**.

Values: `removecertificate_customdevice`, `removecertificate_allnonprotected`, `removecertificate_all`, `removecustomlanguage_all`, `removecustomlanguage_webui`, `removewallpaper_handset`, `removewallpaper_deskset` **Default:** Blank

Setting: `file.deskset_wallpaper`

Description: URL for uploading custom wallpaper file (BMP format) for M58. This parameter is **NON-EXPORTABLE**.

Values: URI **Default:** Blank

Setting: `file.handset_wallpaper`

Description: URL for uploading custom wallpaper file (BMP format) for M55/M56. This parameter is **NON-EXPORTABLE**.

Values: URI **Default:** Blank

Setting:	<code>file.language.webui.url</code>		
Description:	Sets the custom WUI language for cordless product. This parameter is NON-EXPORTABLE .		
Values:	URI	Default:	no custom language

Setting:	<code>file.contact.directory.append</code>		
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:	<code>file.contact.directory.override</code>		
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:	<code>file.contact.blacklist.append</code>		
Description:	URL of contact blocked list to be imported. Entries in the imported file will be added to existing blocked list entries. This parameter is NON-EXPORTABLE .		
Values:	URI	Default:	Blank

Setting:	<code>file.contact.blacklist.override</code>		
Description:	URL of contact blocked list to be imported. Entries in the imported file will replace all existing blocked list directory entries. This parameter is NON-EXPORTABLE .		
Values:	URI	Default:	Blank

“tr369” Module: TR-369 Settings

The Broadband Forum’s Technical Report 369 (TR-369) defines a protocol for remote management and secure auto-configuration of compatible devices. The TR-369 settings allow you to enable TR-369 and configure access to an auto-configuration server (ACS).

Site-wide settings

All of the TR-369 settings are site-wide settings.

Setting: `tr369.controller.url`

Description: URL of the TR369 controller that our device is connecting to.

Values: URI **Default:** `iot.snom.com`

Setting: `tr369.enable`

Description: Enable or disable the TR369 module on device to support remote device management.

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

"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>: 0-2³²

<off duration>: 0-2³²

<repeat count>: 0-65535

Site-wide settings

All of the tone definition settings are site-wide settings.

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:	<code>tone.inside_dial_tone.element.x</code>		
Description:	Defines the inside dial tone element x (x = 2–5).		
Values:	Tone element string	Default:	Blank
Setting:	<code>tone.inside_dial_tone.num_of_repeat_all</code>		
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:	<code>tone.stutter_dial_tone.num_of_elements</code>		
Description:	Sets the number of tone elements for the stutter dial tone.		
Values:	1–5	Default:	2
Setting:	<code>tone.stutter_dial_dial_tone.element.1</code>		
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:	<code>tone.stutter_dial_dial_tone.element.2</code>		
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:	<code>tone.stutter_dial_tone.element.x</code>		
Description:	Defines the stutter dial tone element x (x = 3–5).		
Values:	Tone element string	Default:	Blank
Setting:	<code>tone.stutter_dial_tone.num_of_repeat_all</code>		
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:	<code>tone.busy_tone.num_of_elements</code>		
Description:	Sets the number of tone elements for the busy tone.		
Values:	1–5	Default:	1
Setting:	<code>tone.busy_tone.element.1</code>		
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:	<code>tone.busy_tone.element.x</code>		
Description:	Defines the busy tone element x (x = 2–5).		
Values:	Tone element string	Default:	Blank
Setting:	<code>tone.busy_tone.num_of_repeat_all</code>		
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:	<code>tone.ring_back_tone.num_of_elements</code>		
Description:	Sets the number of tone elements for the ringback tone.		
Values:	1–5	Default:	2
Setting:	<code>tone.ring_back_tone.element.1</code>		
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:	<code>tone.ring_back_tone.element.2</code>		
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:	<code>tone.ring_back_tone.element.x</code>		
Description:	Defines the ringback tone element x (x = 3–5).		
Values:	Tone element string	Default:	Blank
Setting:	<code>tone.ring_back_tone.num_of_repeat_all</code>		
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:	<code>tone.congestion_tone.num_of_elements</code>		
Description:	Sets the number of tone elements for the congestion tone.		
Values:	1–5	Default:	3
Setting:	<code>tone.congestion_tone.element.1</code>		
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:	<code>tone.congestion_tone.element.2</code>		
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:	<code>tone.congestion_tone.element.3</code>		
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:	<code>tone.congestion_tone.element.x</code>		
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 passwords can also be set using the WebUI. Be aware that scheduled provisioning configuration file updates may reset these passwords.

Site-wide settings

All of the password settings are site-wide settings.

Setting:	<code>profile.admin.password</code>		
Description:	Sets the administrator password for accessing the admin menus on the WebUI. This parameter is NON-EXPORTABLE .		
Values:	Text string (15 characters maximum)	Default:	admin

Setting:	<code>profile.support.password</code>		
Description:	Sets the support password for accessing the DECT Statistics page on the WUI: <code>http(s)://<host:port>/dect_statistics.kl1</code> . This password can only be set via provisioning.		
Values:	Text string	Default:	support

Setting:	<code>profile.user.password</code>		
Description:	Sets the user password for logging on to the WebUI and editing user-accessible settings. This parameter is NON-EXPORTABLE .		
Values:	Text string (15 characters maximum)	Default:	user

Setting: `profile.enable_password_strength_check`

Description: If enabled, the M500 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:** 1

“speeddial” 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 `speeddial.x.y.[element]` , where x is the device number (1-16) and y is the speed dial entry number that matches the dial pad key (0-9).

Setting:	<code>speeddial.x.y.account</code>		
Description:	Sets the account that the speed dial key uses to dial the number.		
Values:	1-48	Default:	1
Setting:	<code>speeddial.x.y.name</code>		
Description:	Sets the name of the speed dial entry.		
Values:	text string	Default:	blank
Setting:	<code>speeddial.x.y.number</code>		
Description:	Sets the telephone number to be dialed.		
Values:	text string	Default:	blank

“XSI” Module: XSI Settings

Site-wide settings

All of the XSI settings are site-wide settings.

Setting:	<code>xsi.directory_account</code>		
Description:	Select the account to be used for cordless handset/deskset to access XSI directory.		
Values:	1-48	Default:	1

Setting:	<code>xsi.x.check_certificate</code>		
Description:	Enables server authentication with the installed trusted certificate.		
Values:	0 (disabled), 1 (enabled)	Default:	0

Setting:	<code>xsi.x.directories</code>		
Description:	Comma-delimited Broadsoft XSI phone lists to be displayed on Menu > Directory > Broadsoft directory . Possible phone lists are: group, groupcommon, enterprise, enterprisecommon, personal.		
Values:	Text string	Default:	group, groupcommon, enterprise, enterprisecommon, personal

Setting:	<code>xsi.x.password</code>		
Description:	Sets the Broadsoft XSI authentication password. This parameter is NON-EXPORTABLE .		
Values:	Text string	Default:	blank

Setting:	<code>xsi.x.port</code>		
Description:	Sets the Broadsoft XSI server port.		
Values:	1-65535	Default:	0

Setting:	<code>xsi.x.server</code>		
Description:	Sets the Broadsoft XSI server address.		
Values:	URI	Default:	blank

Setting:	<code>xsi.x.username</code>		
Description:	Sets the Broadsoft XSI authentication user name.		
Values:	Text string	Default:	blank

TROUBLESHOOTING

If you have difficulty with your M500 Dual-cell SIP DECT Base Station, 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 M500 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 M500 Dual-cell SIP DECT Base Station contains sophisticated electronic parts, so you must treat it with care.
- Avoid rough treatment.
- Place the handset down gently.
- Save the original packing materials to protect your M500 Dual-cell SIP DECT Base Station if you ever need to ship it.

Avoid water

- You can damage your M500 Dual-cell SIP DECT Base Station if it gets wet. Do not use the handset in the rain, or handle it with wet hands. Do not install the M500 Dual-cell SIP DECT Base Station 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 M500 Dual-cell SIP DECT Base Station 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 M500 Dual-cell SIP DECT Base Station 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>.

