Mitel 6800/6900 Series SIP Phones

58016679 REV00

RELEASE 6.3.0 ADMINISTRATOR GUIDE

SEPTEMBER, 2022

NOTICE

Trademarks

CHAPTER 2: CONFIGURATION INTERFACE METHODS

CHAPTER 3: ADMINISTRATOR OPTIONS

CHAPTER 6:

CONFIGURING ADVANCED OPERATIONAL FEATURES

CHAPTER 9: TROUBLESHOOTING

APPENDIX A:

CONFIGURATION PARAMETERS

APPENDIX B:

CONFIGURING THE IP PHONE AT THE ASTERISK IP PBX

APPENDIX C:

SAMPLE CONFIGURATION FILES

APPENDIX H:

LICENSE AGREEMENT

PREFACE

This ***SIP IP Phone Administrator Guide*** provides information on the basic network setup, operation, and maintenance of the Mitel 6800 (6863i, 6865i, 6867i, 6869i, and 6873i) and 6900 (6905, 6910, 6920, 6930, 6940, and 6970) Series SIP IP Phones. It also includes details on the functionality and configuration of the IP phones.

Notes:

1. Features, characteristics, requirements, and configuration that are specific to a particular IP phone model are indicated where required in this guide.
2. This guide will be updated periodically with new and/or updated information. For details on what features have been added or updated, please refer to the ***Mitel 6800/6900 Series SIP IP Phones 6.3.0 Release Notes***.
3. Received Callers List and Outgoing Redial List information in this Administrator Guide describes the phone's native Callers and Redial lists. In some environments, the Received Callers List key and the Outgoing Redial List key may bring up a Callers List and Redial List provided by the call manager; therefore, depending on your call manager, the lists on your phone may function and behave differently then what is documented in this Administrator Guide. If this is the case, refer to the documentation provided with your respective call manager.

WHAT'S NEW

This section describes the new features or enhancements in SIP Phone Release 6.3.0.

The following table summarizes each new feature or enhancement and provides a link to more information about the feature.

FEATURE/ENHANCEMENT	DESCRIPTION	LOCATION
Bug fixes.	NA	NA

AUDIENCE

This guide is for network administrators, system administrators, developers and partners who need to understand how to operate and maintain the IP phone on a SIP network. It also provides some user-specific information.

This guide contains information that is at a technical level, more suitable for system or network administrators. Prior knowledge of IP Telephony concepts is recommended.

DOCUMENTATION

The IP phone documentation suite consists of the following:

- ***Mitel 6800/6900 SIP IP Phone Installation Guides*** – contains installation and set-up instructions, information on general features and functions, and basic options list customization. Included with the phone.
- ***Mitel 6800/6900 SIP IP Phone User Guides*** – explains the most commonly used features and functions for an end user.

- ***Mitel 6800/6900 SIP IP Phone Release Notes*** – provides new features and documents issues resolved for the SIP IP phones.

This Administrator Guide complements the ***Mitel 6800/6900 Installation Guides***, the ***Mitel 6800/6900 SIP IP Phone User Guides***, and the ***Mitel 6800/6900 SIP IP Phone Release Notes***.

CHAPTERS AND APPENDICES IN THIS GUIDE

This guide contains the following chapters and appendices:

FOR	GO TO
An overview of the IP Phones and the IP Phone firmware installation information	Chapter 1
IP Phone interface methods	Chapter 2
Administrator options information	Chapter 3
Configuring the Network and Global SIP Features on the IP Phone	Chapter 4
Configuring operational information on the IP Phones	Chapter 5
Configuring advanced operational information on the IP Phones	Chapter 6
Encryption information	Chapter 7
Firmware upgrade information	Chapter 8
Troubleshooting solutions	Chapter 9
Configuration parameters	Appendix A
Configuring the IP Phones at the Asterisk PBX	Appendix B
Sample configuration files	Appendix C
Sample BLF softkey settings	Appendix D
Sample multiple proxy server configuration	Appendix E

Chapter 1

OVERVIEW

ABOUT THIS CHAPTER

This chapter briefly describes the IP Phone Models, and provides information about installing the IP phone firmware. It also describes the firmware and configuration files that the IP phone models use for operation.

TOPICS

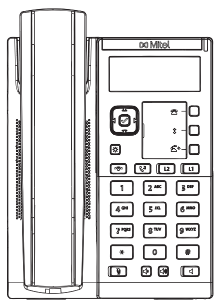
This chapter covers the following topics:

IP PHONE MODELS

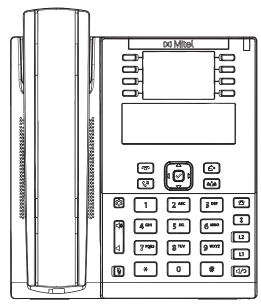
DESCRIPTION

All Mitel SIP IP Phone Models communicate over an IP network allowing you to receive and place calls in the same manner as a regular business telephone. All phone models support the Session Initiation Protocol (SIP).

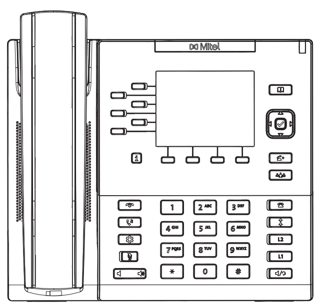
The following illustration show the IP phone models in the 6800 series.



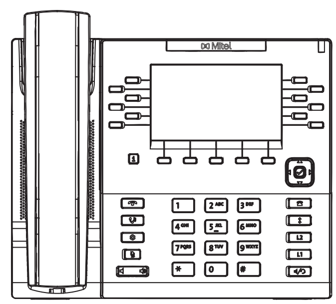
6863i



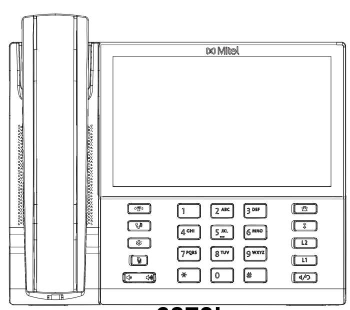
6865i



6867i



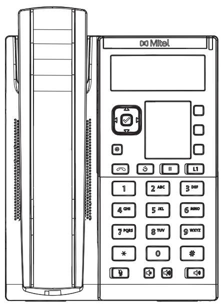
6869i



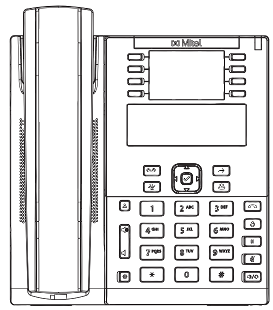
6873i

The following illustration show the IP phone models in the 6900 series.

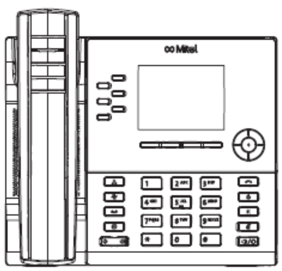
6905



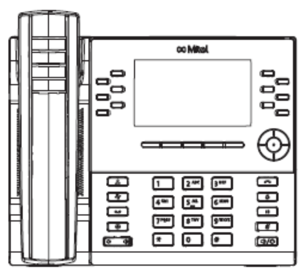
6910



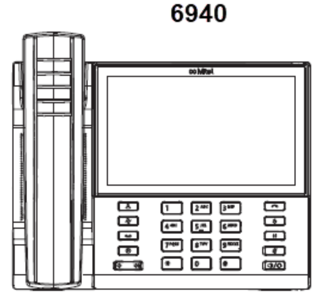
6920



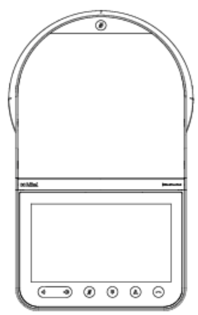
6930



6940

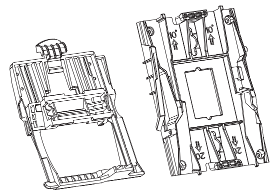


6970

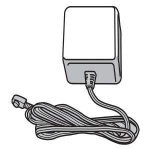


OPTIONAL ACCESSORIES

The 6800/6900 wall mount kit is an optional accessory designed to be used with the 6863i, 6865i, 6867i, 6869i, 6930, and 6940 IP Phones. The power adapter is an optional accessory designed to be used with all the 6800 and 6900 Series IP Phones.

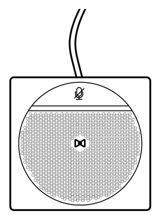


6800/6900 Wall Mount Kit



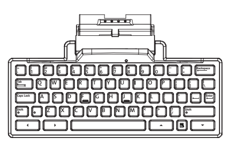
Power Adapter

The corded extension microphones are optional accessories designed to be used with the 6970 IP Conference Phone. The extension microphone will extend the pick up range of the phone to allow it to be used in large rooms.



Corded Extension Microphone

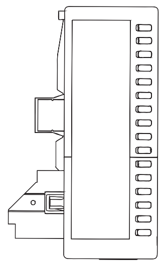
The K680i magnetically connected keyboards (available in QWERTY, QWERTZ, and AZERTY keyboard layouts) are optional accessories designed to be used with the 6867i and 6869i IP Phones. The full keyboard provides a more natural typing interface and helps to easily facilitate dial by name, directory search, XML applications, etc....



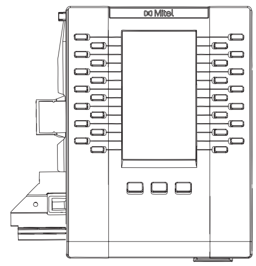
K680i Detachable Magnetic Keyboard

Note: The 6900 series IP phones does not support the K680i detachable magnetic keyboard.

The following expansion modules are optional accessories designed to be used with the 6865i, 6867i, 6869i, and 6873i IP Phones.



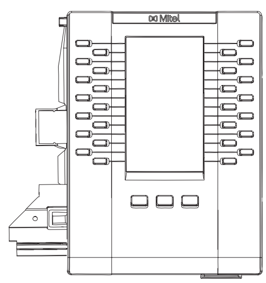
M680i Expansion Module



M685i Expansion Module

The M680i module adds 16 additional softkeys to the 6865i, 6867i, 6869i, and 6873i IP phones and provides paper labels for each softkey. The M685i adds 3 pages of 28 (i.e. 84 total) additional softkeys to the 6865i, 6867i, 6869i, zand 6873i IP phones.

The following expansion modules are optional accessories designed to be used with the 6920, 6930, and 6940 IP Phones.



M695 Expansion Module

The M695 adds 3 pages of 28 (i.e. 84 total) additional programmable softkeys with LEDs to the 6920, 6930, and 6940 IP Phones.

Labels can be configured and displayed on the backlit color LCD display.

No separate power adapter is required for the expansion modules as they are powered by the respective IP phone.

Up to 3 modules (mixed in any combination) can be daisy-chained together to provide a large number of additional softkeys.

Note: 6900 models only support M695 and do not support M680i or M685i expansion modules.

M680i and M685i Expansion Modules Daisy-Chaining Support

IP PHONE MODEL	MAXIMUM # OF DAISY-CHAINED MODULES WHEN POWERED VIA 48V AC ADAPTER	MAXIMUM # OF DAISY-CHAINED MODULES WHEN POWERED VIA POE	POE CLASS
6865i	3	3	Class 2 (< 6.49W)
6867i	3	3	Class 2 (< 6.49W) without modules. Dynamically switches to Class 3 (< 12.95W) when modules are attached.
6869i	3	3	Class 3 (< 12.95W)
6873i	3	3	Class 3 (< 12.95W) without modules. Dynamically switches to Class 4 (< 25.50W) when modules are attached (see notes below).

Notes:

1. Some 802.3at switches require connected devices to send power allocation requests in excess of 12.95 W using LLDP. Therefore, Mitel recommends that Administrators ensure LLDP is enabled when powering a 6873i SIP phone with one or more expansion modules connected using Power over Ethernet plus (PoE plus). For more information on LLDP, see “Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) and Emergency Location Identification Number (ELIN)” on page 5-113.
2. For the 6873i, the USB port on the phone will be disabled if the phone is being powered using 802.3af PoE and one or more expansion modules are connected. Use the recommended AC adapter (optional accessory) or power the 6873i using 802.3at PoE plus to ensure the USB port will be functional when expansion modules are connected to the phone.

M680i and M685i Software Upgrades

The M680i and M685i do not require separate firmware packages. M680i/M685i software is embedded within the respective phone’s firmware package.

When the M680i or M685i is connected and is powered up (for the M680i the LED corresponding to the second button will turn solid red indicating it is powered up; for the M685i the LCD screen will turn on) the module will check to see if an upgrade is required. If it does not have the latest software, the module will upgrade itself using the phone’s embedded firmware.

For the M680i, this process will take approximately 10 seconds, in which case the LED corresponding to the second button will stay solid red for the duration. If the upgrade is successful, the LED will turn green. If the LED stays solid and red for longer than 10 seconds, the upgrade may have failed. In such scenarios, unplug and reattach the power source from the phone to attempt the upgrade again.

As software upgrades on the M680i are performed one at a time, each additional module connected increases the approximate upgrade time (e.g. three connected M680i expansion modules will take approximately 30 seconds to upgrade).

For the M685i, the upgrade process will take approximately 7 to 10 minutes, in which case an upgrading icon will be displayed on the module's LCD screen and an upgrading message will be displayed on the phone's LCD screen. If the upgrade is successful, the module's LCD screen will refresh with the softkey images. If the screen is not refreshed after ~15 minutes, the upgrade may have failed. In such scenarios, unplug and reattach the power source from the phone to attempt the upgrade again.

Unlike the M680i, software upgrades for the M685i are performed simultaneously and therefore do not increase the upgrade time (e.g. three connected M685i expansion modules will still take approximately 7 to 10 minutes to upgrade).

Note: When using a combination of M680i and M685i expansion modules in tandem, the M685i modules must be connected to the phone first, followed by the M680i modules. Additionally, if a software update is available for both expansion modules, the M685i modules will upgrade first and a reboot will be required after the M685i module upgrade is complete before the M680i can be upgraded.

M695 Software Upgrades

The M695 do not require separate firmware packages. M695 software is embedded within the respective phone's firmware package.

When the M695 is connected and is powered up (the LCD screen will turn on) the module will check to see if an upgrade is required. If it does not have the latest software, the module will upgrade itself using the phone's embedded firmware.

For the M695, the upgrade process will take approximately 7 to 10 minutes, in which case an upgrading icon will be displayed on the module's LCD screen and an upgrading message will be displayed on the phone's LCD screen. If the upgrade is successful, the module's LCD screen will refresh with the softkey images. If the screen is not refreshed after ~15 minutes, the upgrade may have failed. In such scenarios, unplug and reattach the power source from the phone to attempt the upgrade again.

Software upgrades for the M695 are performed simultaneously and therefore do not increase the upgrade time (for example, the three connected M695 expansion modules will still take approximately 7 to 10 minutes to upgrade).

Do not plug an M695 into a 6800i model. Ensure that an M695 is plugged into a 6920, 6930 or 6940 Phone. The 5.1.0 SP2 firmware pushes a new hardware ID into the M695 Expansion Module which requires PKMs to be plugged to the correct phone models.

Reference

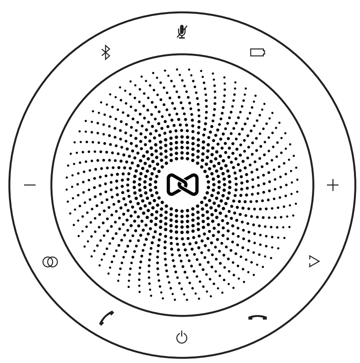
For more information about installing the 6800 Wall Mount Kit and setting up and using the K680i keyboard and M680i/M685i expansion modules, see the following respective documents:

- 6800/6900 Wall Mount Kit Installation Guide
- K680i Detachable Magnetic Keyboard Installation Guide

- M680i Expansion Module Installation Guide
- M685i Expansion Module Installation Guide
- M680i Expansion Module Quick Start Guide
- M685i Expansion Module Quick Start Guide
- M695 Expansion Module Installation Guide
- <Model-Specific> Installation Guide
- <Model-Specific> SIP Phone User Guide

The Mitel S720 Bluetooth Speakerphone is supported with Mitel 6930 and 6940 IP phones that allows you to instantly transform any room into a conference room. You can easily connect and enjoy the crystal clear HD audio, while maximizing productivity during conference calls through this premium portable and easy-to-use Bluetooth speakerphone.

Note: The 6873i IP phone supports S720 as a Bluetooth headset device.

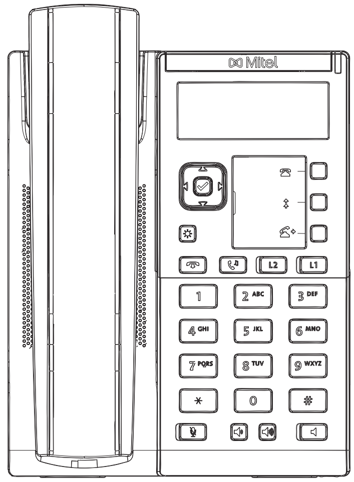


S720 Bluetooth Speakerphone

For more information, see the Mitel S720 Bluetooth Speakerphone Quick Start Guide.

MODEL 6863I IP PHONE

This section provides brief information about the Model 6863i IP Phone. It includes a list of features and describes the hard keys on the 6863i.

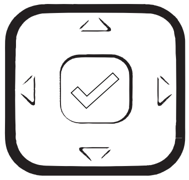
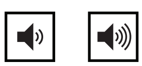
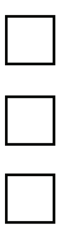


6863I PHONE FEATURES

- LCD screen
- Built-in-two-port, 10/100 Fast Ethernet switch - lets you share a connection with your computer
- 3 programmable keys
- Press-and-hold speeddial key configuration feature
- Supports up to 2 call lines with LEDs
- Wideband handset
- Wideband, full-duplex speakerphone for handsfree calls
- AC power adapter (sold separately)
- Set paging*

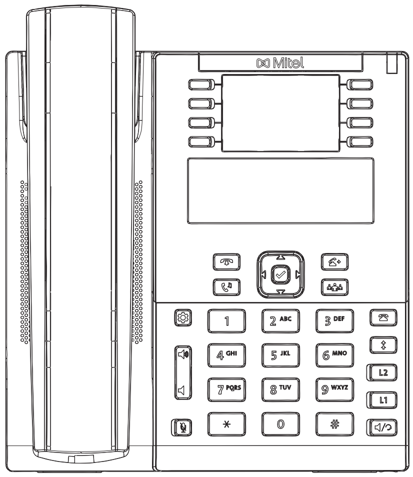
*Availability of feature dependent on your phone system or service provider.

6863I KEY DESCRIPTION

KEY	DESCRIPTION
	**Navigation/Select Keys** - Pressing the UP and DOWN keys lets you view different status and text messages on the LCD display (if there is more than 1 line of status/text messages). These buttons also let you scroll through menu selections, such as the Options List. Pressing the LEFT and RIGHT keys lets you view the different line/call appearances. While in the Options List, these keys allow you to exit or enter the current option. When you are editing entries on the display, pressing the LEFT key erases the character on the left; pressing the RIGHT key sets the option. Alternatively, pressing the center Select key sets the option as well on specific screens.
	**Options Key** - Accesses services and options to customize your phone. Your System Administrator may have already customized some of your settings. Check with your System Administrator before changing the administrator-only options.
	**Goodbye Key** - Ends an active call. The Goodbye key also exits an open list, such as the Options List, without saving changes.
	**Hold Key** - Places an active call on hold. To retrieve a held call, press the call appearance button beside the light that is flashing.
L2 L1	**Line/Call Appearance Keys** - Connects you to a line or call. The Mitel 6863i supports two line keys, each with LED indicator lights.
	**Mute Key** - Mutes the microphone so that your caller cannot hear you (the light indicator flashes when the microphone is on mute).
	**Volume Controls** - Adjusts the volume for the handset, ringer, and handsfree speaker.
	**Speaker Key** - Transfers the active call to the speaker, allowing handsfree use of the phone.
	**Programmable Keys** - When programmed, allows you to easily perform up to 3 specific functions (e.g. Services, Directory, Intercom, etc...) and access enhanced services provided by third parties (e.g. XML applications). The programmable keys are pre-configured as (from top to bottom) Received Callers, Outgoing Redial, and Transfer keys.

MODEL 6865I IP PHONE

This section provides brief information about the Model 6865i IP Phone. It includes a list of features and describes the hard keys on the 6865i.

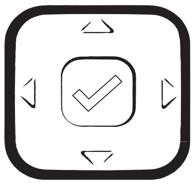
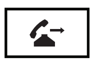
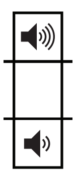
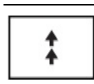


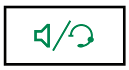
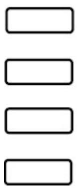
6865I PHONE FEATURES

- LCD screen with backlight
- Built-in-two-port, 10/100/1000 Gigabit Ethernet switch - lets you share a connection with your computer
- 8 programmable top keys
- Press-and-hold speeddial key configuration feature
- Supports up to 24 call lines with LEDs
- Wideband handset
- Wideband, full-duplex speakerphone for handsfree calls
- Headset mode support
- AC power adapter (sold separately)
- Enhanced busy lamp fields*
- Set paging*

*Availability of feature dependent on your phone system or service provider.

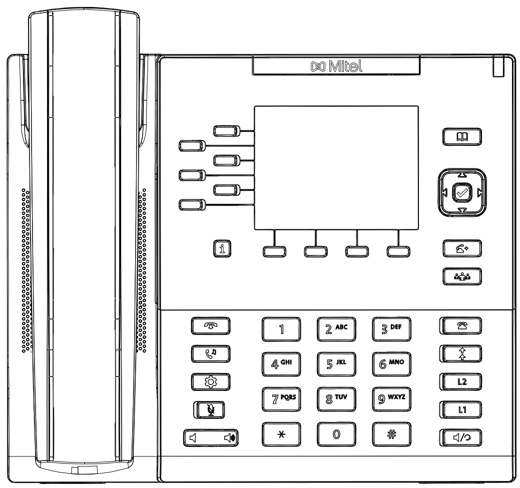
6865I KEY DESCRIPTION

KEY	DESCRIPTION
	**Goodbye Key** - Ends an active call. The Goodbye key also exits an open list, such as the Options List, without saving changes.
	**Hold Key** - Places an active call on hold. To retrieve a held call, press the call appearance button beside the light that is flashing.
	**Navigation/Select Keys** - Pressing the UP and DOWN keys lets you view different status and text messages on the LCD display (if there is more than 1 line of status/text messages). These buttons also let you scroll through menu selections, such as the Options List. Pressing the LEFT and RIGHT keys lets you view the different line/call appearances. While in the Options List, these keys allow you to exit or enter the current option. When you are editing entries on the display, pressing the LEFT key erases the character on the left; pressing the RIGHT key sets the option. Alternatively, pressing the center Select key sets the option as well on specific screens.
	**Transfer Key** - Transfers the active call to another number.
	**Conference Key** - Begins a conference call with the active call.
	**Options Key** - Accesses services and options to customize your phone. Your System Administrator may have already customized some of your settings. Check with your System Administrator before changing the administrator-only options.
	**Volume Controls** - Adjusts the volume for the handset, ringer, and handsfree speaker.
	**Mute Key** - Mutes the microphone so that your caller cannot hear you (the light indicator flashes when the microphone is on mute).
	**Callers List Key** - Displays All folder list which includes the list of your missed, outgoing, and received calls.
	**Redial Key** - Accesses a list of the last 100 previously dialed numbers. Pressing the Redial key twice redials the last dialed number.

KEY	DESCRIPTION
L2 L1	**Line/Call Appearance Keys** - Connects you to a line or call. The Mitel 6865i IP Phone supports two line keys, each with LED indicator lights.
	**Speaker/Headset Key** - Transfers the active call to the speaker or headset, allowing handsfree use of the phone.
	**Programmable Keys** - When programmed, allows you to easily perform up to 8 specific functions (e.g. Services, Directory, Received Callers List, Intercom, etc...) and access enhanced services provided by third parties (e.g. XML applications).

MODEL 6867I IP PHONE

This section provides brief information about the Model 6867i IP Phone. It includes a list of features and describes the hard keys on the 6867i.

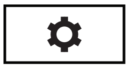
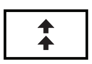
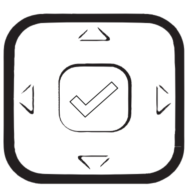
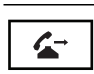


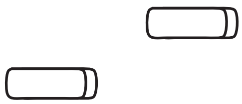
6867I PHONE FEATURES

- 3.5” QVGA color TFT LCD with backlight
- Built-in-two-port, 10/100/1000 Gigabit Ethernet switch - lets you share a connection with your computer
- USB 2.0 port (100mA maximum)
- 6 programmable and 4 context-sensitive softkeys
- Press-and-hold speeddial key configuration feature
- Supports up to 24 call lines with LEDs
- Wideband handset
- Wideband, full-duplex speakerphone for handsfree calls
- Headset mode support
- AC power adapter (sold separately)
- Enhanced busy lamp fields*
- Set paging*

*Availability of feature dependent on your phone system or service provider.

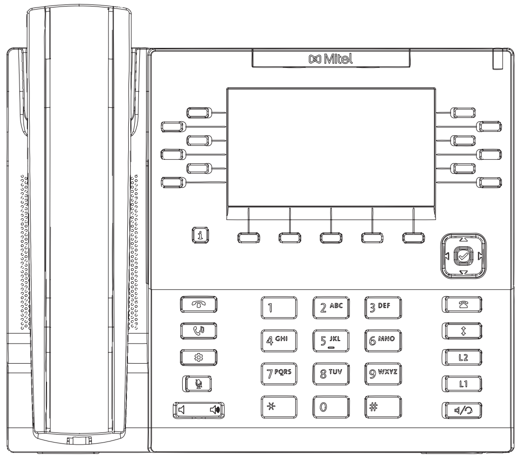
6867I KEY DESCRIPTION

KEY	DESCRIPTION
	**Goodbye Key** - Ends an active call. The Goodbye key also exits an open list, such as the Options List, without saving changes.
	**Hold Key** - Places an active call on hold. To retrieve a held call, press the call appearance button beside the light that is flashing.
	**Options Key** - Accesses services and options to customize your phone. Your System Administrator may have already customized some of your settings. Check with your System Administrator before changing the administrator-only options.
	**Mute Key** - Mutes the microphone so that your caller cannot hear you (the light indicator flashes when the microphone is on mute).
	**Volume Controls** - Adjusts the volume for the handset, ringer, and handsfree speaker.
	**Callers List Key** - Displays All folder list which includes the list of your missed, outgoing, and received calls.
	**Outgoing Redial Key** - Accesses a list of the last 100 previously dialed numbers. Pressing the Outgoing Redial key twice redials the last dialed number.
L2 L1	**Line/Call Appearance Keys** - Connects you to a line or call. The Mitel 6867i IP Phone supports two line keys, each with LED indicator lights.
	**Speaker/Headset Key** - Transfers the active call to the speaker or headset, allowing handsfree use of the phone.
	**Directory Key** - Accesses a directory of names and phone numbers.
	**Navigation/Select Keys** - Multi-directional navigation keys allow you to navigate through the phone’s user interface. Pressing the center Select key selects/sets options and performs various actions (such as dialing out when in the Directory, Received Callers, and Outgoing Redial Lists).
	**Transfer Key** - Transfers the active call to another number.

KEY	DESCRIPTION
	**Conference Key** - Begins a conference call with the active call.
	**Presence Key** - Accesses the partial and full contact presence information screens, which provide more detailed information about the selected contact.
	**Left Softkeys** - 6 programmable keys that allow you to easily perform up to 20 specific functions and access enhanced services provided by third parties (e.g. XML applications).
	**Bottom Softkeys** - 4 programmable keys that support up to 18 functions. These keys also act as state-based keys allowing you to easily perform context-sensitive functions during specific states (i.e. when the phone is an idle, connected, incoming, outgoing, or busy state).

MODEL 6869I IP PHONE

This section provides brief information about the Model 6869i IP Phone. It includes a list of features and describes the hard keys on the 6869i.

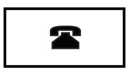
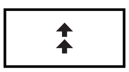
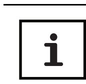


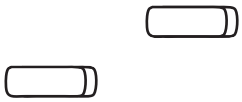
6869I PHONE FEATURES

- 4.3” QVGA color TFT LCD with backlight
- Built-in-two-port, 10/100/1000 Gigabit Ethernet switch - lets you share a connection with your computer
- USB 2.0 port (100mA maximum)
- 12 programmable and 5 context-sensitive softkeys
- Press-and-hold speeddial key configuration feature
- Supports up to 24 call lines with LEDs
- Wideband handset
- Wideband, full-duplex speakerphone for handsfree calls
- Headset mode support
- AC power adapter (sold separately)
- Enhanced busy lamp fields*
- Set paging*

*Availability of feature dependent on your phone system or service provider.

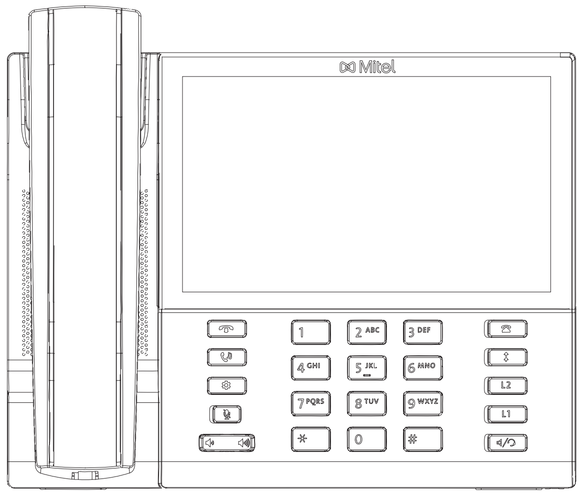
6869I KEY DESCRIPTION

KEY	DESCRIPTION
	**Goodbye Key** - Ends an active call. The Goodbye key also exits an open list, such as the Options List, without saving changes.
	**Hold Key** - Places an active call on hold. To retrieve a held call, press the call appearance button beside the light that is flashing.
	**Options Key** - Accesses services and options to customize your phone. Your System Administrator may have already customized some of your settings. Check with your System Administrator before changing the administrator-only options.
	**Mute Key** - Mutes the microphone so that your caller cannot hear you (the light indicator flashes when the microphone is on mute).
	**Volume Controls** - Adjusts the volume for the handset, ringer, and handsfree speaker.
	**Callers List Key** - Displays All folder list which includes the list of your missed, outgoing, and received calls.
	**Outgoing Redial Key** - Accesses a list of the last 100 previously dialed numbers. Pressing the Outgoing Redial key twice redials the last dialed number.
L2 L1	**Line/Call Appearance Keys** - Connects you to a line or call. The Mitel 6869i IP Phone supports two line keys, each with LED indicator lights.
	**Speaker/Headset Key** - Transfers the active call to the speaker or headset, allowing handsfree use of the phone.
	**Navigation/Select Keys** - Multi-directional navigation keys allow you to navigate through the phone's user interface. Pressing the center Select key selects/sets options and performs various actions (such as dialing out when in the Directory, Received Callers, and Outgoing Redial Lists).
	**Presence Key** - Accesses the partial and full contact presence information screens, which provide more detailed information about the selected contact.

KEY	DESCRIPTION
	**Top Softkeys** - 12 programmable keys that allow you to easily perform up to 44 specific functions and access enhanced services provided by third parties (e.g. XML applications).
	**Bottom Softkeys** - 5 programmable keys that support up to 24 functions. These keys also act as state-based keys allowing you to easily perform context-sensitive functions during specific states (i.e. when the phone is an idle, connected, incoming, outgoing, or busy state).

MODEL 6873I IP PHONE

This section provides brief information about the Model 6873i IP Phone. It includes a list of features and describes the hard keys on the 6873i.

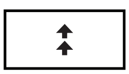
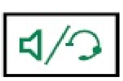


6873I PHONE FEATURES

- 7" WVGA (800x480) color TFT capacitive touch LCD
- Built-in-two-port, 10/100/1000 Gigabit Ethernet switch - lets you share a connection with your computer
- USB 2.0 port (500mA maximum)
- Up to 48 top and 30 bottom softkeys
- Press-and-hold speeddial key configuration feature
- Supports 2 hard line keys with LEDs (additional line keys programmable via softkeys)
- Wideband handset
- Wideband, full-duplex speakerphone for handsfree calls
- USB and Bluetooth headset support
- AC power adapter (sold separately)
- Enhanced busy lamp fields*
- Set paging*

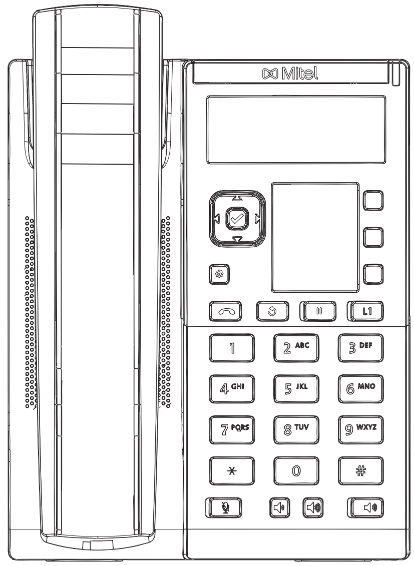
*Availability of feature Dependant on your phone system or service provider.

6873I KEY DESCRIPTION

KEY	DESCRIPTION
	**Goodbye Key** - Ends an active call. The Goodbye key also exits an open list, such as the Options List, without saving changes.
	**Hold Key** - Places an active call on hold. To retrieve a held call, press the call appearance button beside the light that is flashing.
	**Options Key** - Accesses services and options to customize your phone. Your System Administrator may have already customized some of your settings. Check with your System Administrator before changing the administrator-only options.
	**Mute Key** - Mutes the microphone so that your caller cannot hear you (the light indicator flashes when the microphone is on mute).
	**Volume Controls** - Adjusts the volume for the handset, ringer, and handsfree speaker.
	**Callers List Key** - Displays All folder list which includes the list of your missed, outgoing, and received calls.
	**Outgoing Redial Key** - Accesses a list of the last 100 previously dialed numbers. Pressing the Outgoing Redial key twice redials the last dialed number.
L2 L1	**Line/Call Appearance Keys** - Connects you to a line or call. The Mitel 6869i IP Phone supports two line keys, each with LED indicator lights.
	**Speaker/Headset Key** - Transfers the active call to the speaker or headset, allowing handsfree use of the phone.

MODEL 6905 IP PHONE

This section provides brief information about the Model 6905 IP Phone. It includes a list of features and describes the hard keys on 6905.



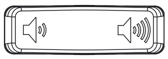
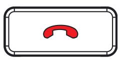
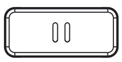
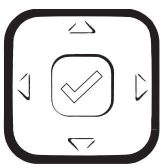
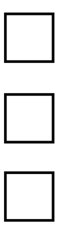
6905 PHONE FEATURES

- Built-in two-port, 10/100 Megabit Ethernet switch that enables you to share a connection with your computer
- Class 1 Power-Over-Ethernet (PoE)
- 2.75" 128x48 Pixel back-lit display
- Wide-band speaker phone
- Wide-band 6900 handset
- 3 programmable paper labeled personal keys with LEDs
- Support for wall mounting using the 6800/6900 wall-mount kit
- Single line support
- Mitel Wireless LAN Adapter

*Availability of feature dependent on your phone system or service provider.

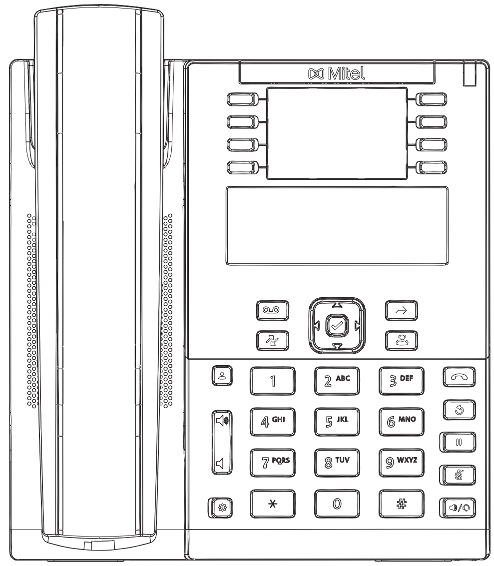
6905 KEY DESCRIPTION

The following table describes the keys on the Mitel 6905 IP phone:

Key	Description
	**Options key** - Provides services and static settings that allow you to customize your phone.
	**Volume controls** - Adjusts the volume for the ringer, handset, and speakerphone. Pressing these keys during an active call adjusts the volume of the audio device being used (handset or speaker).
	**Goodbye key** - Ends an active call. The **Goodbye** key also exits an open list (such as **Call History**) and menus (such as the **Static Settings** menu) without saving changes.
	**Redial key** - Redials the last manually dialed number displayed on the LCD screen.
	**Hold key** - Places an active call on hold. To retrieve a held call, press the applicable **Line** key.
	**Mute key** - Mutes the microphone so that your caller cannot hear you (the LED beside the key turns on when the microphone is on mute).
	**Speaker** - Transfers the active call to the speaker.
	**Navigation keys and select button** - Multi-directional navigation keys that allow you to navigate through the phone's User Interface (UI). The right, left, and center navigation keys are used as softkeys.
	**Prime Line key** - Line or Call Appearance Keys connect you to a line or call. The Mitel 6905 IP phone supports one line key with an LED indicator light.
	**Programmable Keys** - When programmed, allows you to easily perform up to 3 specific functions (e.g. Do not disturb, Call History, Intercom, etc).

MODEL 6910 IP PHONE

This section provides brief information about the Model 6910 IP Phone. It includes a list of features and describes the hard keys on 6910.



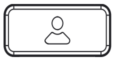
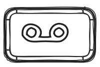
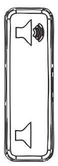
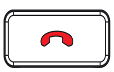
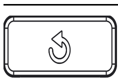
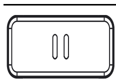
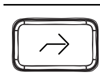
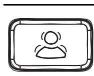
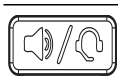
6910 PHONE FEATURES

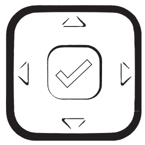
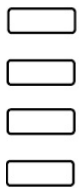
- LCD screen with backlight
- Built-in two-port, 10/100/1000 Megabyte Ethernet switch that enables you to share a connection with your computer
- Class 2 Power-Over-Ethernet (PoE)
- 3.4" 128x48 Pixel back-lit display
- Wide-band speaker phone
- Wide-band 6900 handset
- "8 programmable paper labeled personal keys with LEDs
- Analog handset port with DHSG support
- Support for wall mounting using the 6800/6900 wall-mount kit
- Mitel Wireless LAN Adapter

*Availability of feature dependent on your phone system or service provider.

6910 KEY DESCRIPTION

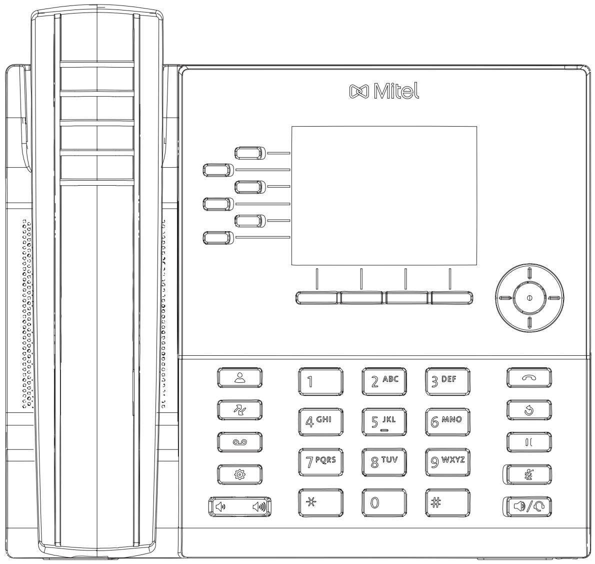
The following table describes the keys on the Mitel 6910 IP phone:

Key	Description
	**Directory key**—Displays the corporate contacts from phonebook.
	**Call History key**—Displays All folder list which includes the list of your missed, outgoing, and received calls.
	**Voicemail key**—Provides access to your voicemail service (if configured).
	**Options key**—Provides services and static settings that allow you to customize your phone.
	**Volume controls**—Adjusts the volume for the ringer, handset, headset, and speaker phone. Pressing these keys during an active call adjusts the volume of the audio device being used (handset, headset, or speaker).
	**Goodbye key**—Ends an active call. The **Goodbye** key also exits an open list (such as **Call History**) and menus (such as the **Static Settings** menu) without saving changes.
	**Redial key**—Redials the last manually dialed number displayed on the LCD screen.
	**Hold key**—Places an active call on hold. To retrieve a held call, press the applicable **Line** key.
	**Mute key**—Mutes the microphone so that the caller cannot hear you. The LED beside the key turns on when the microphone is on mute.
	**Transfer Key**—Transfers the active call to another number.
	**Conference Key**—Begins a conference call with the active call.
	**Speaker/Headset key**—Transfers the active call to the speaker or headset, allowing hands-free use of the phone.

Key	Description
	**Navigation keys and select button** —Multi-directional navigation keys that allow you to navigate through the phone’s UI. The right, left, and center navigation keys are used as softkeys.
	**Programmable Keys** - When programmed, allows you to easily perform up to 8 specific functions (e.g. Do not disturb, Phone lock, Intercom, etc).

MODEL 6920 IP PHONE

This section provides brief information about the Model 6920 IP Phone. It includes a list of features and describes the hard keys on 6920.



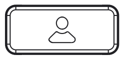
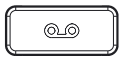
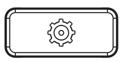
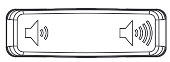
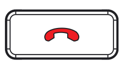
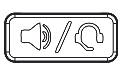
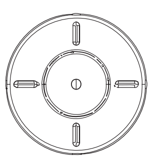
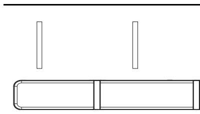
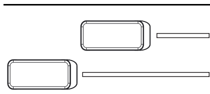
6920 PHONE FEATURES

- 3.5” QVGA (320x240) color TFT LCD display with brightness controls
- Built-in-two-port, 10/100/1000 Gigabit Ethernet switch - lets you share a connection with your computer
- USB 2.0 port (100mA maximum)
- 6 top softkeys supporting up to 20 functions and four context-sensitive bottom softkeys supporting up to 18 functions
- Press-and-hold speed dial key configuration feature
- Wideband handset
- Enhanced wideband, full-duplex speakerphone for handsfree calls
- Extensive support for peripherals and modules: USB, DHSG/EHS, and wired analog head-sets, Mitel M695 Programmable Key Module, and Mitel Wireless LAN Adapter
- AC power adapter (sold separately)

*Availability of feature dependent on your phone system or service provider.

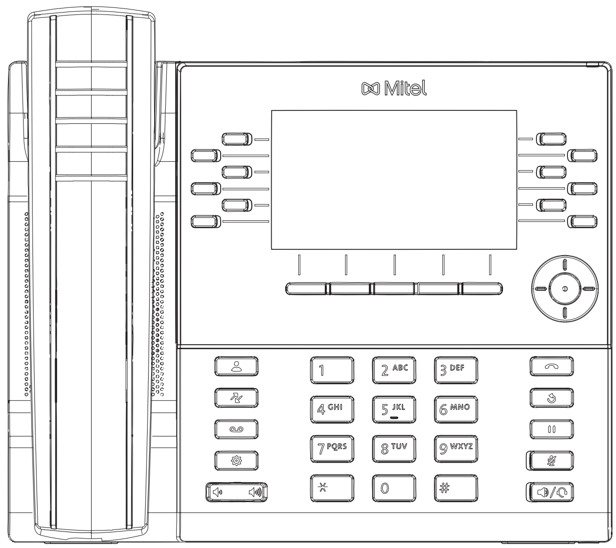
6920 KEY DESCRIPTION

The following table describes the keys on the Mitel 6920 IP phone:

Key	Description
	**Directory key** - Displays a list of your contacts.
	**Call History key** - Displays All folder list which includes the list of your missed, outgoing, and received calls.
	**Voicemail key** - Provides access to your voicemail service (if configured).
	**Options key** - Provides services and static settings that allow you to customize your phone.
	**Volume controls** - Adjusts the volume for the ringer, handset, headset, and speakerphone. Press the volume control keys while the phone is ringing to adjust the ringer volume. Pressing these keys during an active call adjusts the volume of the audio device being used (handset, headset, or speaker).
	**Goodbye key** - Ends an active call. The **Goodbye** key also exits an open list (such as **Call History**) and menus (such as the **Static Settings** menu) without saving changes.
	**Redial key** - Displays a list of your previously dialed calls. Pressing the **Redial** key twice redials the last dialed number displayed on the **Home** screen.
	**Hold key** - Places an active call on hold. To retrieve a held call, press the applicable **Line** key.
	**Mute key** - Mutes the microphone so that your caller cannot hear you (the LED beside the key turns on when the microphone is on mute).
	**Speaker/Headset key** - Transfers the active call to the speaker or headset, allowing handsfree use of the phone.
	**Navigation keys and select button** - Multi-directional navigation keys that allow you to navigate through the phone's User Interface (UI). Pressing the center **Select** button sets options as well as performs actions such as dialing out from the **Contacts** or **Call History**. On the Home screen, the left and right navigation keys can be used to switch between the home screen, the line manager, and active calls.
	**Bottom softkeys** - Four context-sensitive bottom softkeys that allow you to use up to 18 functions.
	**Top softkeys** - Six multi-function top softkeys that allow you to use up to 20 specific functions.

MODEL 6930 IP PHONE

This section provides brief information about the Model 6930 IP Phone. It includes a list of features and describes the hard keys on the 6930.



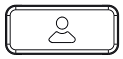
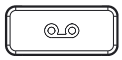
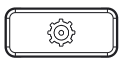
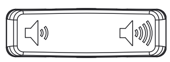
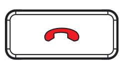
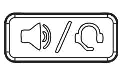
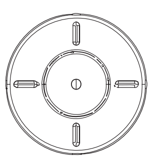
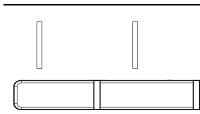
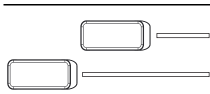
6930 PHONE FEATURES

- 4.3” WQVGA (480x272) color TFT LCD display with brightness controls
- Built-in-two-port, 10/100/1000 Gigabit Ethernet switch - lets you share a connection with your computer
- Embedded Bluetooth 4.0
- USB 2.0 port (500mA maximum)
- 12 top softkeys supporting up to 44 functions and 5 context-sensitive bottom softkeys supporting up to 24 functions
- Press-and-hold speeddial key configuration feature
- Wideband handset
- Enhanced wideband, full-duplex speakerphone for handsfree calls
- Extensive support for peripherals and modules: Mitel cordless Bluetooth handset, Bluetooth, USB, DHSG/EHS, and wired analog headsets, M695 Color Programmable Key Module (PKM), and Mitel Wireless LAN Adapter
- AC power adapter (sold separately)
- Mobile integration using Bluetooth wireless technology

*Availability of feature dependent on your phone system or service provider.

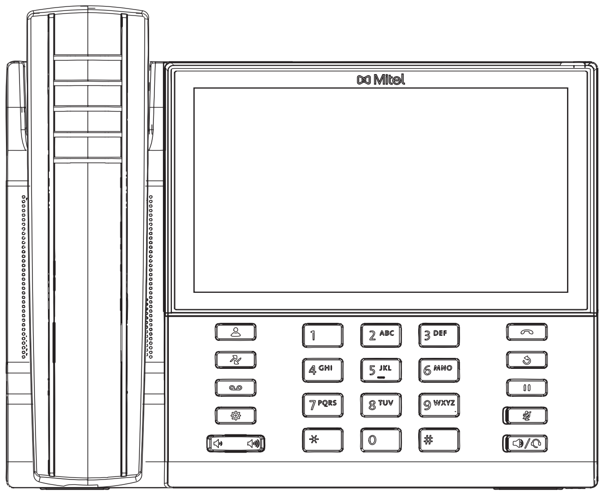
6930 KEY DESCRIPTION

The following table describes the keys on the Mitel 6930 IP phone:

Key	Description
	**Directory key** - Displays a list of your contacts.
	**Call History key** - Displays All folder list which includes the list of your missed, outgoing, and received calls.
	**Voicemail key** - Provides access to your voicemail service (if configured).
	**Options key** - Provides services and static settings that allow you to customize your phone.
	**Volume controls** - Adjusts the volume for the ringer, handset, headset, and speakerphone. Press the volume control keys while the phone is ringing to adjust the ringer volume. Pressing these keys during an active call adjusts the volume of the audio device being used (handset, headset, or speaker).
	**Goodbye key** - Ends an active call. The **Goodbye** key also exits an open list (such as **Call History**) and menus (such as the **Static Settings** menu) without saving changes.
	**Redial key** - Displays a list of your previously dialed calls. Pressing the **Redial** key twice redials the last dialed number displayed on the **Home** screen.
	**Hold key** - Places an active call on hold. To retrieve a held call, press the applicable **Line** key.
	**Mute key** - Mutes the microphone so that your caller cannot hear you (the LED beside the key turns on when the microphone is on mute).
	**Speaker/Headset key** - Transfers the active call to the speaker or headset, allowing handsfree use of the phone.
	**Navigation keys and select button** - Multi-directional navigation keys that allow you to navigate through the phone's User Interface (UI). Pressing the center **Select** button sets options as well as performs actions such as dialing out from the **Contacts** or **Call History**. On the Home screen, the left and right navigation keys can be used to switch between the home screen, the line manager, and active calls.
	**Bottom softkeys** - Five context-sensitive bottom softkeys that allow you to perform 24 different functions during specific states (i.e. when the phone is in idle, connected, incoming, outgoing, or busy state).
	**Top softkeys** - 12 programmable, multi-function top softkeys that allow you to use up to 44 specific functions.

MODEL 6940 IP PHONE

This section provides brief information about the Model 6940 IP Phone. It includes a list of features and describes the hard keys on the 6940.



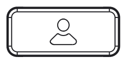
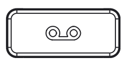
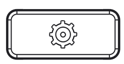
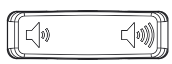
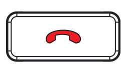
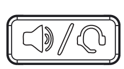
6940 PHONE FEATURES

- 7" WVGA (800x480) color TFT capacitive touch-screen LCD display with brightness controls
- Built-in-two-port, 10/100/1000 Gigabit Ethernet switch - lets you share a connection with your computer
- Embedded Bluetooth 4.0
- USB 2.0 port (500mA maximum)
- 12 touchscreen top softkeys supporting up to 48 functions and 6 context-sensitive touch-screen bottom softkeys supporting up to 30 functions.
- Cordless Bluetooth Handset
- Press-and-hold speed dial key configuration feature
- Enhanced wideband, full-duplex speakerphone for handsfree calls
- Extensive support for peripherals and modules: USB and Bluetooth headsets, M695 Color Programmable Key (PKM) modules, and Mitel Wireless LAN Adapter
- AC power adapter (sold separately)
- Mobile integration using Bluetooth wireless technology

*Availability of feature Dependant on your phone system or service provider.

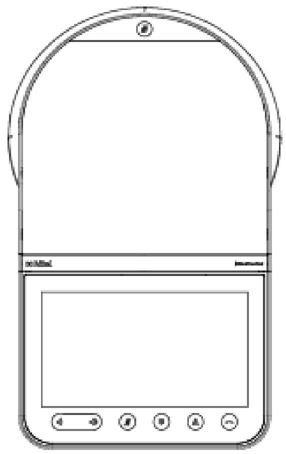
6940 KEY DESCRIPTION

The following table describes the keys on the Mitel 6940 IP phone:

Key	Description
	**Directory key** - Displays a list of your contacts.
	**Call History key** - Displays All folder list which includes the list of your missed, outgoing, and received calls.
	**Voicemail key** - Provides access to your voicemail service (if configured).
	**Options key** - Provides services and static settings that allow you to customize your phone.
	**Volume controls** - Adjusts the volume for the ringer, handset, headset, and speakerphone. Press the volume control keys while the phone is ringing to adjust the ringer volume. Pressing these keys during an active call adjusts the volume of the audio device being used (handset, headset, or speaker).
	**Goodbye key** - Ends an active call. The **Goodbye** key also exits an open list (such as **Call History**) and menus (such as the **Static Settings** menu) without saving changes.
	**Redial key** - Displays a list of your previously dialed calls. Pressing the **Redial** key twice redials the last dialed number displayed on the **Home** screen.
	**Hold key** - Places an active call on hold. To retrieve a held call, tap the applicable **Line** key.
	**Mute key** - Mutes the microphone so that your caller cannot hear you (the LED beside the key turns on when the microphone is on mute).
	**Speaker/Headset key** - Transfers the active call to the speaker or headset, allowing handsfree use of the phone.

MODEL 6970 IP CONFERENCE PHONE

This section provides brief information about the Model 6970 IP Conference Phone. It includes a list of features and describes the hard keys on the 6970.



6970 IP CONFERENCE PHONE FEATURES

Feature highlights include:

- 7" WVGA (800x480) color TFT capacitive touch-screen LCD with brightness controls
- Power Over Ethernet (PoE) LAN port supporting 10/100/1000 Base T
- Embedded Bluetooth 4.1
- 1 USB 2.0 Host port one on the side of the unit
- 1 peripheral mini USB port underneath the unit
- 2 ports for optional external microphones underneath the unit
- Enhanced conference audio with high output speaker and 8 microphone beam-forming array
- Support for wireless network connection via optional Mitel Wireless LAN adapter
- Support for two optional corded extension microphones
- Twelve touchscreen top softkeys supporting up to 48 functions and six state-based touchscreen bottom softkeys supporting up to 30 functions
- MobileLink support - seamless mobile integration using Bluetooth wireless technology

Administrators should evaluate if certain features should be enabled or disabled depending on their intended usage of the 6970 IP Conference Phone. For example, if the 6970 is used as a public device, it may be appropriate to turn off Call History, Redial, and Missed Calls indicator. If the 6970 is used as a personal device, disabling the Hotdesk auto logout feature and configuring the Mobile key may be desirable.

6970 KEY DESCRIPTION

The following table describes the keys of the Mitel 6970 IP Conference Phone:

Key	Description
	**Goodbye key:** ends an active call.
	**Directory key**: displays a list of company contacts.
	**Dialpad key:** opens and closes the dialpad to dial an extension manually.
	**Mute key:** mutes the microphones so that you are not heard during a call.
	**Volume Up, Volume Down** - Adjusts the volume for the ringer and the speakerphone. Press the volume control keys while the phone is ringing to adjust the ringer volume. Pressing these keys during an active call adjusts the volume of the speaker.

FIRMWARE INSTALLATION INFORMATION

DESCRIPTION

The firmware setup and installation for the IP phone can be done using any of the following:

- Phone User Interface via the keypad (Phone UI)
- Mitel Web-based user interface (Mitel Web UI)

When the IP phone is initialized for the first time, DHCP is enabled by default. Depending on the type of configuration server setup you may have, the IP phone may download a firmware version automatically, or you may need to download it manually.

IMPORTANT M685I EXPANSION MODULE FIRMWARE DOWNGRADE INFORMATION

If you upgrade your phone to Release 5.1.0 SP2 and an M685i Expansion Module is attached, the M685i Expansion Module will also upgrade to align itself with the new UI changes.

If you are downgrading your phone from Release 5.1.0 SP2 to a firmware version of Release 4.3.0 or earlier and your phone has an M685i Expansion Module attached, you must first downgrade to Release 4.1.0 Hot Fix or 4.1.0 Service Pack and then to the Release 4.3.0 or earlier firmware version.

This will ensure the UI of the M685i Expansion Module is aligned with the UI at all times.

IMPORTANT M695 EXPANSION MODULE FIRMWARE INFORMATION

Do not plug an M695 into a 6800i model. Ensure that an M695 is plugged into a 6920, 6930 or 6940 Phone. The 5.1.0 SP2 firmware pushes a new hardware ID into the M695, M685i, and M680i Expansion Modules which requires PKMs to be plugged to the correct phone models.

The PKMs upgrade to version 3.1.0.2. This version supports a new UI as per 5.1.0 SP2 release.

INSTALLATION CONSIDERATIONS

The following considerations must be made before connecting the IP phone to the network:

- If you are planning on using dynamic IP addresses, make sure a DHCP server is enabled and running on your network.
- If you are not planning on using dynamic IP addresses, see Chapter 4, the section, "Configuring Network Settings Manually" on page 4-24 for manually setting up an IP address.

To install the IP phone hardware and cabling, refer to the <Model-Specific> ***SIP IP Phone Installation Guide***.

INSTALLATION REQUIREMENTS

The following are general requirements for setting up and using your SIP IP phone:

- SIP-based IP PBX system or network installed and running with a SIP account created for the IP phone
- Access to a Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP) server, or Hyper Text Transfer Protocol over Secure Sockets Layer (SSL) (HTTPS)
- Ethernet/Fast Ethernet LAN (10/100 Mb) (Gigabit Ethernet LAN [1000 Mbps] recommended for Gigabit Ethernet compliant phones)
- Category 5/5e straight through cabling (Category 6 straight-through cabling recommended for Gigabit Ethernet compliant phones)
- Power source (6863i, 6865i, 6867i, 6869i, 6905, 6910, 6920, 6930)
  - For Ethernet networks that supply inline power to the phone (IEEE 802.3af) use an Ethernet cable to connect from the phone directly to the network for power (no 48V AC power adapter required if using Power-over-Ethernet [PoE])
  - For Ethernet networks that DO NOT supply power to the phone:
    - Use the respective power adapter to connect from the DC power port on the phone to a power source
      or
    - Use a PoE power injector or a PoE switch
- Power source (6873i, 6940, 6970)
  - For Ethernet networks that supply inline power to the phone (IEEE 802.3af or IEEE 802.3at [IEEE 802.3at recommended]) use an Ethernet cable to connect from the phone directly to the network for power (no 48V AC power adapter required if using Power-over-Ethernet [PoE] or PoE plus)
  - For Ethernet networks that DO NOT supply power to the phone:
    - Use only the GlobTek Inc. Limited Power Source [LPS] adapter model no. GT-41080-1848 (sold separately) to connect from the DC power port on the phone to a power source
      or
    - Use a PoE power injector or a PoE switch (PoE plus recommended)

CONFIGURATION SERVER REQUIREMENT

A basic requirement for setting up the IP phone is to have a configuration server. The configuration server allows you to:

- Store the firmware images that you need to download to your IP phone
- Stores configuration files for the IP phone

REFERENCE

To set the protocol for your configuration server, see Chapter 4, “Configuring Network and Session Initiation Protocol (SIP) Features”, the section, “Configuring the Configuration Server Protocol” on page 4-104.

To update the firmware on your phone, see Chapter 8, “Upgrading the Firmware”.

FIRMWARE AND CONFIGURATION FILES

DESCRIPTION

By default on startup, the phone downloads its firmware and configuration files from the configuration server you have set; or you can manually download the firmware from the configuration server. The phone supports TFTP, FTP, HTTP and HTTPS configuration servers.

Note:

1. Automatic download is dependent on your configuration server setup. For more information about manual and automatic download of firmware, see Chapter 8, "Upgrading the Firmware." For more information on changing the download protocol on your phone, see Chapter 4, the section, "Configuring the Configuration Server Protocol" on page 4-104.
2. By factory default, the 6900 series IP phones have the Minet firmware installed. You have to manually download the SIP firmware. For more information on MiNet to SIP and SIP to MiNet conversion, see Chapter 8, "Upgrading the Firmware."

The IP Phone firmware file (*.st*) include all the necessary files you need for your phone.

The firmware consists of the following file:

- **<phone model>.st** - This file contains information about the specific IP Phone model and contains the language packs to load to the phone.

The configuration files consist of three files called:

- ***startup.cfg*** - This file contains configuration information about the IP Phone.

  Note:

  1. In releases previous to 4.0.0 SP1, the "startup.cfg" file was named "aastra.cfg". Apart from the file names, the "startup.cfg" file acts as an identical replacement for the "aastra.cfg" file. Releases including and above 4.0.0 SP1 support both the "startup.cfg" and "aastra.cfg" files, but if the "startup.cfg" file is available, the phone will disregard the "aastra.cfg" file (if available). The "aastra.cfg" file will be used if the "startup.cfg" file is unavailable and will continue to be supported going forward to ensure backwards compatibility with existing customer deployments.
  2. Ensure a startup.cfg or aastra.cfg file is available during the bootup. Only after the retrieval of a startup.cfg or aastra.cfg file, the phone requests for the <model>.cfg and <mac>.cfg files.

- ***<model>.cfg*** - This file contains model specific information, where "model" should be the same string that is used for the model name (e.g. 6863i.cfg, 6865i.cfg, 6867i.cfg, 6869i.cfg, 6873i.cfg, 6905.cfg, 6910.cfg, 6920.cfg, 6930.cfg, 6940.cfg, 6970.cfg).
- ***<MAC>*.cfg** - This file contains configuration information about the IP Phone (for example, 00085D1610DE.cfg).

- ***G722 overload point setting in aastra.cf*g**

Note: When the default overload point of G722 is set at -3dbm0. You need to set the overload point at the level as specified by the following standard:

- Need to add the command line to aastra.cfg file mentioned as **g7229dbm0:1**.
- Reset the phone to update the configuration ensuring the location of configuration server is set through the phone web interface to the same location where the *startup.cfg* is.
- Ensure that the formal load with all audio improvements measure the same levels as 4.1.0.2038.
- Check the configuration is set to the correct overload point as default value in the load and overload becomes 0 on each upgrade that you make.

The following table provides the files that the phone requests from the configuration server during bootup of the phone:

IP PHONE MODEL	ASSOCIATED FIRMWARE	CONFIGURATION FILES	LANGUAGE FILES
6863i	6863i.st	startup.cfg	lang_ar.txt (Arabic - 6867i, 6869i, 6873i,6920,6920,6930,6940 and 6970 only)
6865i	6865i.st		lang_ca.txt (Catalan)
6867i	6867i.st	<model>.cfg (for example, 6867i.cfg)	lang_ca_va.txt (Valencian)
6869i	6869i.st		lang_cs.txt (Czech - UTF-8)
6873i	6873i.st		lang_cs_op.txt (Czech - ASCII)
6905	6905.st	<MAC>.cfg (for example, 00085D1610DE.cfg)	lang_cy.txt (Welsh)
6910	6910.st		lang_de.txt (German)
6920	6920.st		lang_da.txt (Danish)
6930	6930.st		lang_el.txt (Greek - 6867i, 6869i, and 6873i only)
6940	6940.st		lang_es.txt (Spanish)
6970	6970.st		lang_es_mx.txt (Mexican Spanish)
			lang_eu.txt (Euskera)
			lang_fi.txt (Finnish)
			lang_fr.txt (French)
			lang_fr_ca.txt (Canadian French)
			lang_gl.txt (Galego)
			lang_hu.txt (Hungarian)
			lang_it.txt (Italian)
			lang_ko.txt(Korean- 6867i, 6869i, 6920, 6930 only)
			lang_nl.txt (Dutch)
			lang_nl_nl.txt (Dutch - Netherlands)
			lang_no.txt (Norwegian)
			lang_pl.txt (Polish - ASCII)
			lang_pl_pl.txt (Polish - UTF-8)
			lang_pt.txt (Portuguese)
			lang_pt_br.txt (Brazilian Portuguese)
			lang_ro.txt (Romanian)
			lang_ru.txt (Russian)
			lang_sk.txt (Slovak - UTF-8)
			lang_sk_op.txt (Slovak - ASCII)
			lang_sv.txt(Swedish)
			lang_tr.txt (Turkish)
			lang_zh_cn.txt (Simplified Chinese - 6867i, 6869i, 6920, 6930 only)
			lang_zh-tw.txt (Traditional Chinese - 6867i, 6869i, 6920, 6930 only)

ENHANCED CONFIGURATION FILE DOWNLOAD MECHANISM

For 6800 series phones, you may now specify the mandatory configuration files for the phone to download. Also, you may specify the number of reattempts to download the file in case of an unsuccessful attempt.

Administrators can set the following parameters in the configuration file -

- **config files mandatory download**
- **config files number of reattempt**
- **config files max delay**
- **config files skip key enabled**

Note:

1. If the phone fails to download any of the mandatory files within the specified times of reattempt, it does not overwrite the existing configuration, and the old configuration is retained. Only when all the mandatory files are downloaded, the old configuration is replaced with new one.
2. If the *config files number of reattempt* is set to -1, the phone attempts to download the mandatory file in a loop, unless and until the skip softkey is pressed or the file is downloaded.
3. An Error Message will be logged at **Status->Error Message** specifying the file that failed to download.
4. Do not configure both 'startup' and 'aastra' config files as mandatory download, since the phone only looks for 'startup' config in this case.
5. If 'aastra' config file is specified as mandatory download, ensure there is no 'startup' config file present at the download server, failing which download of 'aastra' config file is skipped.

Enable or disable mandatory configuration file download and number of reattempts

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A section, Enhanced Configuration File Download on page A-11.

REFERENCE

For more information about loading language files and using the various languages on the IP phone, see Chapter 5, the section, “Language” on page 5-60.

CONFIGURATION FILE PRECEDENCE

Mitel IP phones can accept three sources of configuration data:

- The server configuration most recently downloaded/cached from the configuration server files, *startup.cfg/<model>.cfg/<mac>.cfg* (or the *startup.tuz/<model>.tuz/<mac>.tuz* encrypted equivalents)
- Local configuration changes stored on the phone that were entered using either the IP phone UI or the Mitel Web UI

If the same parameter appears more than once in the above configuration files, the last parameter/value read will be used (i.e. the following precedence rules will apply):

- Settings in the <model>.cfg file can overwrite startup.cfg settings
- Settings in the <mac>.cfg file can overwrite <model>.cfg settings

In the event of conflicting values set by the different methods, values are applied in the following sequence:

1. Default values hard-coded in the phone software
2. Values downloaded from the configuration server
3. Values stored locally on the phone

The last values to be applied to the phone configuration are the values that take effect.

For example, if a parameter's value is set in the local configuration (via Mitel Web UI or IP phone UI) and the same value was also set differently in one of the *startup.cfg/<model>.cfg/<mac>.cfg* files on the configuration server, the local configuration value is the value that takes effect because that is the last value applied to the configuration.

INSTALLING THE FIRMWARE/CONFIGURATION FILES

The following procedure describes how to install the firmware and configuration files.

1. If DHCP is disabled, manually enter the configuration server's IP address. For details on manually setting DHCP, see Chapter 4, the section "DHCP" on page 4-4.
2. Copy the firmware file *<phone model>.st* to the root directory of the configuration server. The IP phone accepts the new firmware file only if it is different from the firmware currently loaded on the IP phone.

   Note: The *<phone model>* attribute is the IP phone model (i.e. 6863i.st, 6865i.st, 6867i.st, 6869i.st, 6873i.st,6905.st, 6910.st, 6920.st, 6930.st, 6940.st, 6970.st).

3. Copy the Mitel configuration files (*startup.cfg*, *<model>.cfg*, and *<mac>.cfg*) to the root directory of the configuration server.

Notes:

1. The *<mac>* attribute represents the actual MAC address of your phone (i.e. *00085D030996.cfg*).
2. The <model> represents a specific model of phone. (i.e. 6869i.cfg).
3. Restart the IP phone as described in Chapter 3, "Restarting Your Phone" on page 3-15.

MULTIPLE CONFIGURATION SERVER SUPPORT

An Administrator has the option of specifying whether the phones get their firmware file, CSV directory files, language packs, TLS certificate files, 802.1x certificate files, and HTTPS files from the original configuration server or from another server in the network. This feature allows you to specify the URL of other servers from which the phone can get this information.

FIRMWARE FILES AND MULTIPLE CONFIGURATION SERVERS

The firmware file for the phones can be downloaded from the original configuration server or from another server specified by a URL. You can specify a valid full or partial URL (server IP address) from which the phones get the firmware using a new parameter called, "**firmware server**" in the configuration files. If a *full URL* is specified for this parameter, the phones in the network get the *security.tuz*, *startup.cfg, <model>.cfg,* and *<mac>.cfg* files from the original configuration server, and the firmware files from the server specified in the URL.

When the "**firmware server**" parameter specifies a *partial URL* path, the configuration server that is linked to the partial path is used to load the firmware.
For example,

```
firmware server: /path
```

When there is *no* "**firmware server**" parameter (or if it is empty), the original configuration server is used to load the firmware.

Note: The default method for the download of all files and firmware to the phones is from the original configuration server. The Administrator must **specify a correct full or partial server URL** for the phones to get their firmware information from that server. If the URL is incorrect, no firmware download occurs to the phones from the specified server.

Examples

To download all configuration and firmware files from the original configuration server:

```
firmware server:
```

Leaving this parameter blank downloads all configuration and firmware files from the original configuration server.

To download all firmware files from another specified server:

```
firmware server: tftp://10.30.102.158/test1
```

The above example uses TFTP to download all firmware files that exist in the “test1” directory on the specified server, to the phone.

Note: Specifying the download of a “**.st**” file is not supported. For example, the following filename should NEVER be entered as a value string for the “**firmware server**” parameter:

```
firmware server: tftp://10.30.102.158/test1/67i.st
```

To download a partial from another specified server:

```
firmware server: /path
```

The above example uses the configuration server that is linked to the partial path to load the firmware.

SPECIFYING A SERVER TO DOWNLOAD FIRMWARE FILES

You can use the following parameter to specify a server other than the original configuration server from which the phones get their firmware:

- **firmware server**

CONFIGURATION FILES

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, “Multiple Configuration Server Settings” on page A-44.

CSV DIRECTORY FILES, LANGUAGE PACKS, TLS CERTIFICATES, 802.1X CERTIFICATES, HTTPS FILES AND MULTIPLE CONFIGURATION SERVERS

The CSV directory files, language packs, TLS certificate files, 802.1x certificate files, and HTTPS files can also be downloaded to the phone from a server other than the configuration server. For each of these types of files, you can specify a URL (server IP address) from which the phone gets these files. You can use existing parameters on the phone to specify the URL. For applicable parameters, see “Specifying a Server Using Existing Parameters on the IP Phones” on page 1-47.

The following table specifies the files that the original configuration server downloads, and the files that another server can download to the phone.

FILES ALWAYS DOWNLOADED FROM ORIGINAL CONFIGURATION SERVER ARE, BY ORDER:	ALL FILES THAT CAN BE DOWNLOADED FROM ORIGINAL CONFIGURATION SERVER OR ANOTHER SPECIFIED SERVER ARE, BY ORDER:
security.tuz startup.cfg/startup.tuz <model>.cfg/<model>.tuz <mac>.cfg/<mac>.tuz	CSV Directory Files • directory 1 • directory 2 Language Pack Files • language 1 • language 2 • language 3 • language 4 Transport Layer Security (TLS) Certificate Files • sips root and intermediate certificates • sips local certificate • sips private key • sips trusted certificates 802.1x Security Authentication Certificate Files • 802.1x root and intermediate certificates: • 802.1x local certificate: • 802.1x trusted certificates HTTPS Files • https user certificates

Specifying a Server Using Existing Parameters on the IP Phones

The following table provides the parameters on the phone that you can use to download CSV directory files, language packs, TLS certificates, 802.1x certificates, and HTTPS files from the original configuration server OR from another server in the network.

TYPE OF FILE	PARAMETERS THAT SUPPORT THE MULTIPLE CONFIGURATION SERVER FEATURE ARE:
CSV Directory Files	directory 1: directory 2:

TYPE OF FILE	PARAMETERS THAT SUPPORT THE MULTIPLE CONFIGURATION SERVER FEATURE ARE:
Language Pack Files	language 1: language 2: language 3: language 4: Valid files names you can specify for languages are: lang_ar.txt (Arabic) lang_ca.txt (Catalan) lang_ca_va.txt (Valencian) lang_cs.txt (Czech - UTF-8) lang_cs_op.txt (Czech - ASCII) lang_cy.txt (Welsh) lang_de.txt (German) lang_da.txt (Danish) lang_el.txt (Greek - 6867i, 6869i, and 6873i only) lang_es.txt (Spanish) lang_es_mx.txt (Mexican Spanish) lang_eu (Euskera) lang_fi.txt (Finnish) lang_fr.txt (French) lang_fr_ca.txt (Canadian French) lang_gl.txt (Galego) lang_hu.txt (Hungarian) lang_it.txt (Italian) lang_ko.txt (Korean) lang_nl.txt (Dutch) lang_nl_nl.txt (Dutch - Netherlands) lang_no.txt (Norwegian) lang_pl.txt (Polish - ASCII) lang_pl_pl.txt (Polish - UTF-8) lang_pt.txt (Portuguese) lang_pt_br.txt (Brazilian Portuguese) lang_ro.txt (Romanian) lang_ru.txt (Russian) lang_sk.txt (Slovak - UTF-8) lang_sk_op.txt (Slovak - ASCII) lang_sv.txt(Swedish) lang_tr.txt (Turkish) lang_zh_cn.txt (Simplified Chinese) lang_zh_tw.txt (Traditional Chinese)

TYPE OF FILE	PARAMETERS THAT SUPPORT THE MULTIPLE CONFIGURATION SERVER FEATURE ARE:
Transport Layer Security (TLS) Certificate Files	sips root and intermediate certificates: sips local certificate: sips private key: sips trusted certificates:
802.1x Security Authentication Certificate Files	802.1x root and intermediate certificates: 802.1x local certificate: 802.1x trusted certificates:
HTTPS Files	https user certificates

Reference

For more information on each of these parameters, refer to Appendix A, “About this Appendix.”

Examples

CSV Directory Files

The following example downloads no directory:

```
directory 1:
```

The following example downloads a company directory from the original configuration server:

```
directory 1: companylist.csv
```

The following example downloads a company directory file from the specified server in the “path” directory:

```
directory 1: tftp://10.30.102.158/path/companylist.csv
```

Note: To download a specific file, the string value MUST HAVE A FILENAME at the end of the string. For example:

```
directory 1: tftp://10.30.102.158/path/companylist.csv
```

where “**path**” is the directory and “**companylist.csv**” is the filename. If you do not specify a filename, the download fails.

Language Pack Files

The following example downloads no language pack file:

```
language 1:
```

The following example downloads the German language pack to the phones from the original configuration server:

```
language 1: lang_de.txt
```

The following example uses FTP to download the firmware file “lang_de.txt” (German language pack) from the “path” directory on server 1.2.3.4 using port 50:

```
language 1:ftp://admin:admin!@1.2.3.4:50/path/lang_de.txt
```

Transport Layer Security (TLS) Certificate Files

The following example downloads no local certificate file:

```
sips local certificate:
```

The following example downloads the local certificate file from the original configuration server.

```
sips local certificate: phonesLocalCert.pem
```

The following example uses FTP to download the firmware file “phonesLocalCert.pem” (local certificate file) from the “path” directory on server 1.2.3.4 using port 50.

```
sips local certificate:ftp://admin:admin!@1.2.3.4:50/path/
phonesLocalCert.pem
```

802.1x Security Authentication Certificate Files

The following example downloads no 802.1x local certificate file:

```
802.1x local certificate:
```

The following example downloads the 802.1x local certificate for the phone from the original configuration server.

```
802.1x local certificate: 8021xlocalCert.pem
```

The following example uses FTP to download the firmware file “8021xlocalCert.pem” (802.1x local certificate file) from the “path” directory on server 1.2.3.4 using port 50.

```
802.1x local certificate:ftp://admin:admin!@1.2.3.4:50/path/
8021xlocalCert.pem
```

The phone checks the issue of the server certificate to verify whether the certificate is issued by a trusted Certificate Authority.

For example, the following parameter adds the issue of the certificate to the default Certificate Authority list:

```
802.1x trusted certificates: comodocacert.pem
```

HTTPS User Certificate Files

The following example downloads no HTTPS user certificate files:

```
https user certificates:
```

The following example downloads the HTTPS user certificates for the phone from the original configuration server.

```
https user certificates: trustedCerts.pem
```

The following example uses FTP to download the firmware file “user.crt.pem” (https user certificate file) from the “test1” directory on server 12.43.33.234 using port 50.

```
https user certificates:
ftp://test:password@12.43.33.234:50/test1/user.crt.pem
```

ENHANCED E911 LOCATION REPORTING FOR IP ENDPOINTS (RAY BAUM)

This feature mainly focuses on the Section 506 which refers to the rules adopted by the FCC requiring enterprises utilizing multi-line telephone systems (MLTS) to provide automated dispatchable location for all 911 calls. The feature establishes the concept of dispatchable location for Interconnected VoIP services and other 911 capable services. It is critical to achieve successful emergency outcomes for calls that originate from multi-line telephone systems (MLTS).

The MLTS (Multi-line Telephone Systems) provides a dispatchable location for 911 calls that includes street address, apartment, suite to adequately identify the location of the calling party.

Note: If LLDP Chassis-ID is selected for location query, the network switch used must be IEEE802.1d compliant. If non-compliant L2 switches or hubs are used, Chassis-ID might not be correctly populated in the LLDP messages received from phones and other devices, in the neighborhood leading to incorrect location identification.

See Enhanced E911 Location Reporting for IP Endpoints (Ray baum) on page A-21 for the parameters added to enable this feature.

Note: Location Reporting for IP Endpoints is applicable for US customers only.

Chapter 2

CONFIGURATION INTERFACE METHODS

ABOUT THIS CHAPTER

This chapter describes the methods you, as an Administrator, can use to configure the IP phones.

Note: Features, characteristics, requirements, and configuration that are specific to a particular phone model are indicated where required in this guide.

TOPICS

This chapter covers the following topics:

CONFIGURATION METHODS

DESCRIPTION

You can use the following to setup and configure the IP phone:

- IP phone UI
- Mitel Web UI
- Configuration files

Note: Not all parameters are available from all three methods. For more information about configuring the phone, see Chapter 4, Chapter 5, and Chapter 6.

The following paragraphs describe each method of configuring the IP Phone.

IP PHONE UI

The IP Phone User Interface (UI) provides an easy way to access features and functions for using and configuring the IP phone. Access to specific features and functions are restricted to the Administrator. A User can configure a subset of these features and functions. Users of the IP phones should see their <Model-Specific> ***SIP Phone User Guide*** for available features and functions.

REFERENCE

Refer to Chapter 1, “IP Phone Models” on page 1-3 for keys specific to your phone model.

For more information about using the hard keys on each phone, see Chapter 1, “IP Phone Models” on page 1-3.

For more information about the softkeys/programmable keys, see Chapter 5, “Softkeys/Programmable Keys/Expansion Module Keys” on page 5-157.

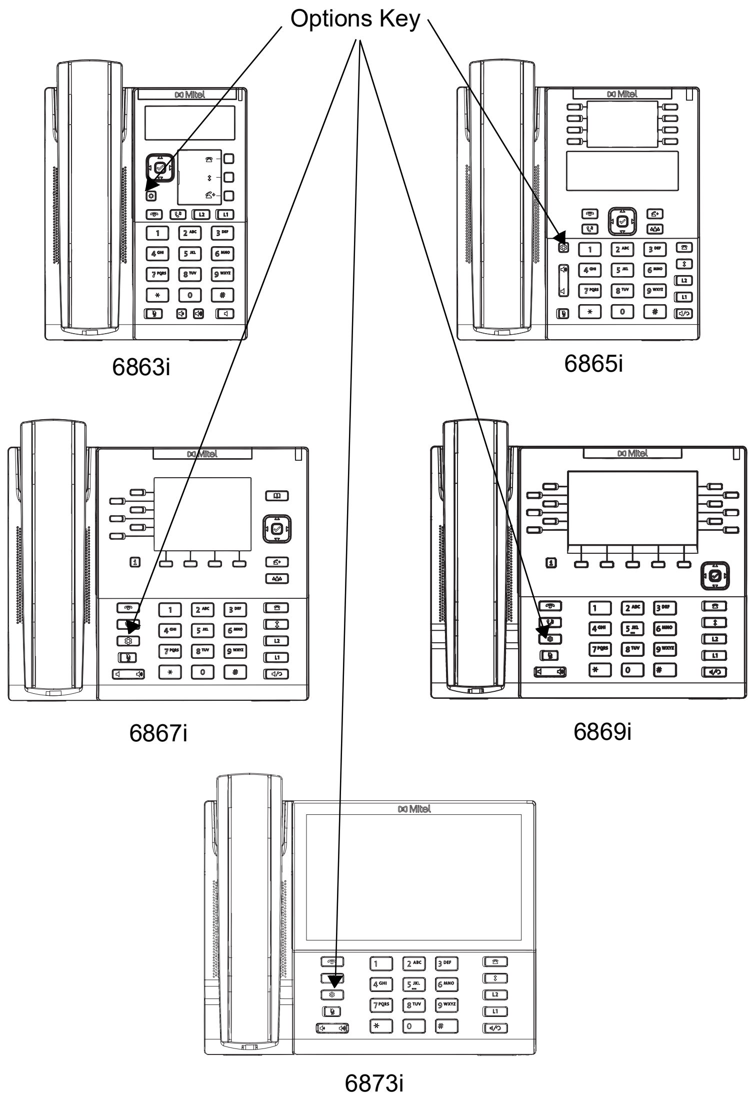
OPTIONS KEY

The Options key allows you to access the “Options List” on the IP phone. Accessible options in this list are for both User and Administrator use. The Administrator must enter a password for administrator options.

Note: An Administrator can apply a simplified options menu to the IP phones. An Administrator can also enable and disable the use of an Administrator password protection in the IP phone UI. These features are configurable using the configuration files only. For more information about these features, see Chapter 3, the section, “Simplified IP Phone UI Options Menu” on page 3-7, and Chapter 5, the section, “Administrator Passwords” on page 5-9.

This document describes the administrator options only. For a description of the user options in the “Options List”, see your <Model-Specific> ***SIP Phone User Guide***.

The following illustrations indicate the location of the Options Key on each phone model.



USING THE OPTIONS KEY ON THE 6863I/6865I

1. Press the **Options** key on the phone to enter the Options List.
2. Use the ▲ and ▼ to scroll through the list of options.
3. To select an option, press the **Enter** softkey, the button (if applicable), or select the number on the keypad that corresponds to the option in the Option List.
4. Use the **Set** softkey after making a change to an option, to save the change.
5. Press the **Done** softkey at any time to save the changes and exit the current option.
6. Press the **Cancel** softkey, or press at any time to exit without saving changes.

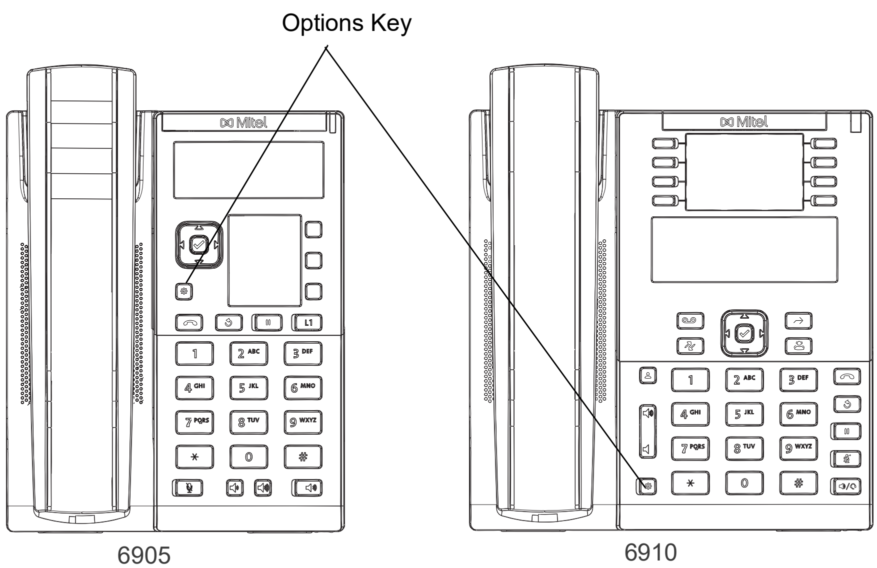
USING THE OPTIONS KEY ON THE 6867I/6869I

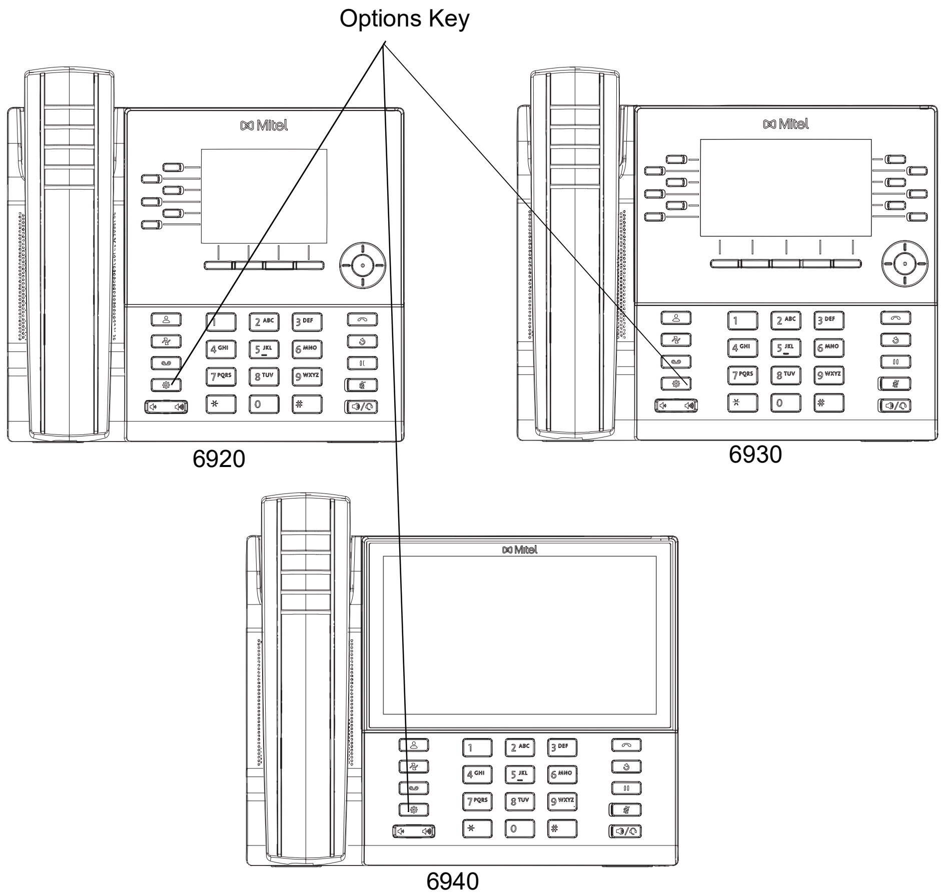
1. Press the key on the phone to enter the Options List.
2. Use the ◀ and ▶ to scroll through the list of options.
3. To select an option, press the button or **Select** softkey.
4. Change your desired settings and use the button or **Save** softkey to apply and save your changes.
5. Press the key or the key at any time to return to the idle screen.

USING THE OPTIONS KEY ON THE 6873I

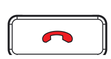
1. Press the key on the phone to enter the Options List.
2. Press an icon to enter the respective menu. Touch the screen to navigate through the sub-menus and scroll ◀ and ▶ to switch pages (if applicable).
3. Press the **Save** softkey to save your changes.

Press the key or the key at any time to return to the idle screen.

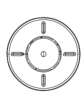




USING THE OPTIONS KEY ON THE 6905 AND 6910

1. Press the **Options** key on the phone to enter the Options List.
2. Use the ▲ and ▼ to scroll through the list of options.
3. To select an option, press the **Enter** softkey, the  button (if applicable), or select the number on the keypad that corresponds to the option in the Option List.
4. Use the **Set** softkey after making a change to an option, to save the change.
5. Press the **Done** softkey at any time to save the changes and exit the current option.
6. Press the **Cancel** softkey or press  at any time to exit without saving changes.

USING THE OPTIONS KEY ON THE 6920 AND 6930

1. Press the  key on the phone to enter the Options List.
2. Use the  to scroll through the list of options.
3. To select an option, press the center button or **Select** softkey.

4. Change your desired settings and use the center button or **Save** softkey to apply and save your changes.
5. Press the key or the key at any time to return to the idle screen.

USING THE OPTIONS KEY ON THE 6940

1. Press the key on the phone to enter the Options List.
2. Press an icon to enter the respective menu. Touch or swipe the screen to navigate through the sub-menus.
3. Press the **Save** softkey to save your changes.
4. Press the key or the key at any time to return to the idle screen.

USING THE SETTINGS SOFTKEY ON THE 6970

There is no **Options** key on the 6970. The Administrator must use the **Settings** softkey to reach the Settings menu.

1. Tap the **Settings** softkey to enter the Settings menu.
2. Tap an icon to enter the respective menu. Touch or swipe the screen to navigate through the sub-menus.
3. Tap the **Save** softkey to save your changes.

Tap the **Quit** softkey at any time to return to the idle screen.

MITEL WEB UI

An administrator can setup and configure the IP phone using the **Mitel Web UI**. The **Mitel Web UI** supports Internet Explorer and Gecko engine-based browsers like Firefox, Mozilla or Netscape.

Note: An Administrator can enable or disable the Mitel Web UI for a single phone or all phones in a network. For more information about enabling/disabling the Mitel Web UI, see “Enabling/Disabling the Mitel Web UI” on page 2-18.

HTTP/HTTPS SUPPORT

The Mitel Web UI supports both Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) client and server protocols.

HTTP is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) over the Internet. When you open your Web browser, you are indirectly making use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols (the foundation protocols for the Internet).

HTTPS is a Web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS uses Secure Socket Layer (SSL) or Transport Layer Security (TLS) as a sublayer under its regular HTTP application layering. SSL is a commonly-used protocol for managing the security of a message transmission on the Internet. It uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange. TLS is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to SSL.

Note: HTTPS uses port 443 instead of HTTP port 80 in its interactions with the TCP/IP lower layer. Both the HTTP and HTTPS port numbers are configurable using the configuration files, the IP Phone UI, the Mitel Web UI and DHCP Option 66. For more information about configuring these ports, see Chapter 4, the section, "Configuring the Configuration Server Protocol" on page 4-104.

CONFIGURABLE HTTP/HTTPS PORTS FOR WEB UI SERVER

Users may now specify the HTTP/HTTPS ports for the Web UI server by adding the configuration parameters "**web interface http port**" and "**web interface https port**" in any of the configuration files startup.cfg/mac.cfg/model.cfg.

The range of the ports vary from 10000 to 11000. For example,

web interface http port: 10001

web interface https port: 10101

The Web UI may then be accessed through *http://webui_ip:10001* or *https://webui_ip:10101*.

Note:

1. If the port values used are out of the specified range, it will be forced to default values. (default_http_port:80, default_https_port:443).
2. If same port values are configured for HTTP and HTTPS, it will be forced to default values.

HTTP/HTTPS CLIENT AND SERVER SUPPORT

The Mitel IP phones allow for HTTP request processing and associated data transfers to perform over a secure connection (HTTPS). The IP phones support the following:

- Transfer of firmware images, configuration files, script files, and web page content over a secure connection.
- Web browser phone configuration over a secure connection
- TLS 1.0, 1.1, and 1.2 methods for both client and server

The following ciphers and cipher suites are supported by https client on the phone:

CIPHER	CIPHER SUITES
AES128	ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA256, ECDHE-RSA-AES128-SHA256 ECDHE-ECDSA-AES128-SHA, ECDHE-RSA-AES128-SHA AES128-GCM-SHA256, AES128-SHA256, AES128-SHA

CIPHER	CIPHER SUITES
AES256	ECDHE-ECDSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-SHA384, ECDHE-RSA-AES256-SHA384 ECDHE-ECDSA-AES256-SHA, ECDHE-RSA-AES256-SHA AES256-GCM-SHA384, AES256-SHA256,AES256-SHA
DES	DES-CBC3-SHA

The following ciphers and cipher suites are supported by https server on the phone:

CIPHER	CIPHER SUITES
AES128	ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA AES128-GCM-SHA256, AES128-SHA256, AES128-SHA
AES256	ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA AES256-GCM-SHA384, AES256-SHA256,AES256-SHA
DES	DES-CBC3-SHA

HTTPS Client

When an HTTPS client opens and closes its TCP socket, the SSL software respectively handshakes upon opening and disconnects upon closing from the HTTPS server. The main HTTPS client functions are:

- Downloading of configuration files and firmware images
- Downloading of script files based on an “HTTPS://” URL supplied by a softkey definition

HTTPS Server

The HTTPS server provides HTTP functionality over secure connections. It coexists with the HTTP server but has its own set of tasks. The main HTTPS server functions are:

- Delivery of web page content to a browser client over a secure connection
- Execution of HTTP GET and POST requests received over a secure connection

NON-BLOCKING HTTP CONNECTIONS

The IP Phones support a non-blocking HTTP connection feature. This feature allows the user to continue using the phone when there is a delay during an HTTP connection while the phone is waiting for the HTTP server to respond. This feature also allows a user to abort the connection and perform other operations on the phone (which will abort the HTTP connection automatically). A user can also abort the HTTP loading by pressing the GOODBYE key while the phone is displaying “Loading Page.......”.

> **Note:** This feature impacts only the HTTP calls triggered by a phone key (softkey or programmable key); the HTTP calls performed by action URIs are still blocking.

Authentication Support for HTTP/HTTPS Download Methods for BroadSoft Client Management System (CMS)

The IP Phones have authentication support as referenced in RFC 2617 when using HTTP or HTTPS as download protocols. If a 5i Series phone is challenged by an HTTP or HTTPS server when the server attempts to download the *startup.cfg* file, the phone automatically sends "**aastra**" as the default Username and Password back to the server. For more information about this feature, see Chapter 5, the section, “Authentication Support for HTTP/HTTPS Download Methods, used with BroadSoft Client Management System (CMS)” on page 5-355.

USING HTTPS VIA THE MITEL WEB UI

HTTPS is enabled by default on the IP phones. When you open a browser window and enter an IP address or host name for a phone using HTTP, a server redirection occurs which automatically converts an HTTP connection to an HTTPS connection. After the redirection, a “Security Alert” certificate window displays alerting the user that information exchanged with the phone cannot be viewed or changed by others. Accepting the certificate then forwards you to the phone’s Web UI.

> **Notes:**
>
> **1.** The private key and certificate generate outside the phone and embed in the phone firmware for use by the HTTPS server during the SSL handshake.
>
> **2.** Using the configuration files, the IP phone UI, or the Mitel Web UI, you can configure the following regarding HTTPS:
>
> - Specify HTTPS security client method to use (TLS 1.0, 1.1, and 1.2)
> - Enable or disable HTTP to HTTPS server redirect function
> - HTTPS server blocking of XML HTTP POSTS to the phone

REFERENCE

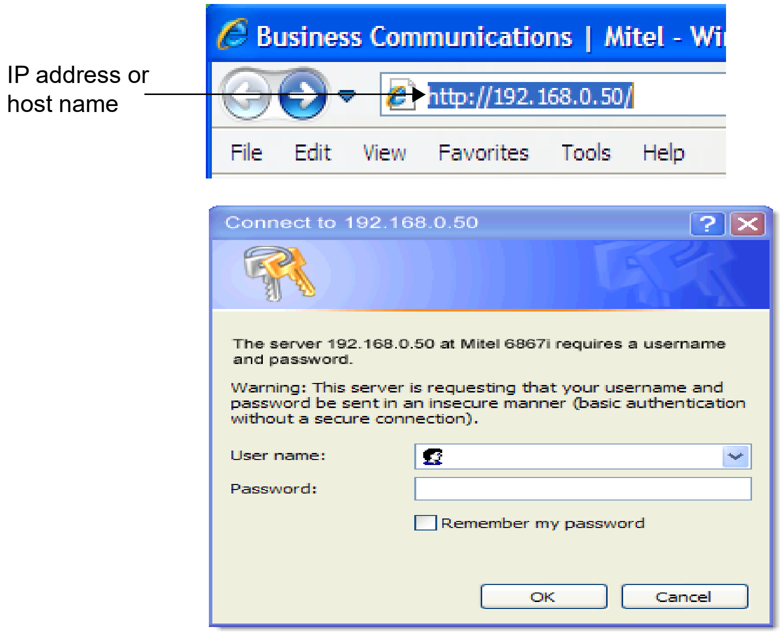
For more information on configuring the HTTPS protocol, see Chapter 4, the sections:

- “Configuring the Configuration Server Protocol” on page 4-104
- “HTTPS Client/Server Configuration” on page 4-36

ACCESSING THE MITEL WEB UI

Use the following procedure to access the Mitel Web UI.

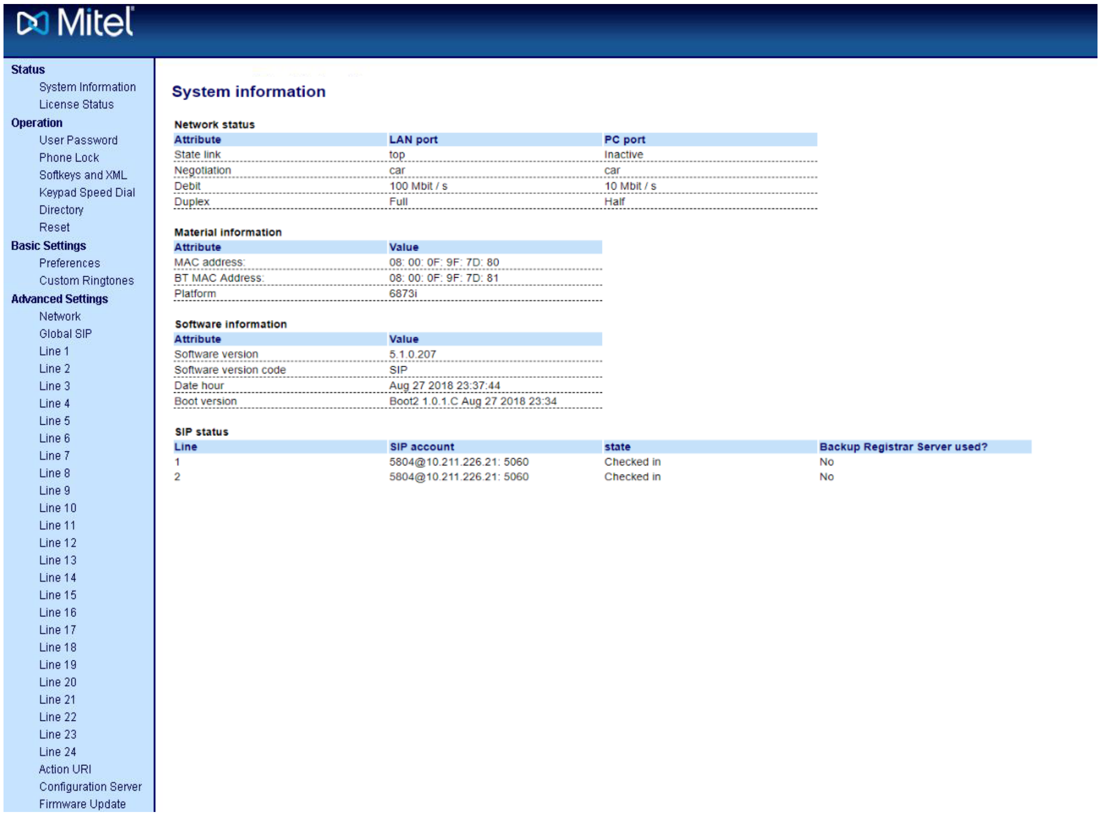
1. Open your web browser and enter the phone's IP address or host name into the address field.
   The following is an example of the Login screen that displays.



2. Enter your username and password and click **OK**.

Note: For an administrator, the default username is "**admin**" and the password is "**22222**". For a user, the default username is "**user**" and the password field is left blank. The IP phones accept numeric passwords only.

The Status window displays for the IP phone you are accessing. The following illustration is an example of a Status screen for the 6873i IP phone.



You can logout of the Mitel Web UI at any time by clicking **Log Off**.

Depending on the model phone you are accessing, the following categories display in the side menu of the Mitel Web UI: **Status, Operation, Basic Settings, Advanced Settings**.

Note: Programmable Keys apply to the 6863i, 6865i, 6905 and 6910. Softkeys apply to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970. Expansion Modules apply to the 6865i, 6867i, 6869i, 6873i, 6920, 6930,and 6940 only.

Status

The **Status** section displays the following information for the IP phone:

- Network status
- MAC address
- Hardware and firmware information
- SIP Account information
- License status

The information in the Status window is read-only.

Operation

The **Operation** section provides the following options:

HEADING	DESCRIPTION
User Password	Allows you to change user password. (Applicable to User and Administrator)
Phone Lock	Allows you to assign an emergency dial plan to the phone, lock the phone to prevent any changes to the phone and to prevent use of the phone, and reset the user password. **Note:** You can also configure a softkey for locking/unlocking the phone. (Applicable to User and Administrator)
Softkeys and XML	6867i - 6 top, multi-functional, static softkeys (maximum of 20 functions) / 4 bottom, state-based, multi-functional softkeys (maximum of 18 functions). 6869i - 12 top, multi-functional, static softkeys (maximum of 44 functions) / 5 bottom, state-based, multi-functional softkeys (maximum of 24 functions). 6873i - 12 top, multi-functional, touch softkeys (maximum of 48 functions) / 6 bottom, state-based, multi-functional touch softkeys (maximum of 30 functions). 6920 - 6 top, multi-functional, softkeys (20 functions) / 4 bottom, context-sensitive, softkeys (18 functions). 6930 - 12 top, multi-functional, softkeys (44 functions) / 5 bottom, context-sensitive softkeys (24 functions). 6940 - 12 top, multi-functional, touch softkeys (48 functions) / 6 bottom, state-based, touch softkeys (30 functions). 6970 - 12 top, multi-functional, touch softkeys (48 functions) / 6 bottom, state-based, touch softkeys (30 functions) (Applicable to User and Administrator)
Programmable Keys	6863i - 3 multi-functional, programmable keys 6865i - 8 multi-functional, programmable keys (Applicable to User and Administrator)
Expansion Module <N>	The M680i has up to 16 configurable keys. The M685i and M695 have up to 84 configurable keys. You can have up to 3 expansion modules attached to a single phone allowing you to configure keys for Expansion Module 1, Expansion Module 2, and Expansion Module 3. See your <Model-Specific> ***SIP Phone User Guide*** for applicable expansion modules for your model phone. **Note:** M680i and M685i Expansion Modules apply to the 6865i, 6867i, 6869i, 6873i only. M695 Expansion Module applies to the 6930, 6930 and 6940 phones only. (Applicable to User and Administrator)
Keypad Speed Dial	Allows you to configure up to 9 speeddial keys. These fields map to the keypad digits 1 through 9 on the phone. You can also configure additional speeddials on the programmable keys, softkeys and expansion modules. See your <Model-Specific> ***SIP Phone User Guide*** for more information about this feature. (Applicable to User and Administrator)

HEADING	DESCRIPTION
Directory	Allows you to copy the Received Callers List and Local Directory List from your IP phone to your PC. (Applicable to User and Administrator)
Reset	Allows you to restart the IP phone when required. (Applicable to User and Administrator). This setting also allows you to set the IP phone back to its factory default settings or remove the local configuration. (Applicable Administrator only)

Basic Settings

The **Basic Settings** section provides the following options:

HEADING	DESCRIPTION
Preferences	Allows you to set the following General specifications on the IP phone. • Local Dial Plan (Admin Only) • Send Dial Plan Terminator (Admin Only) • Digit Timeout (Admin Only) • Park Call • Pick Up Parked Call • Display DTMF Digits • Play Call Waiting Tone • Stuttered Dial Tone • XML Beep Support • Status Scroll Delay (seconds) • Switch UI Focus to Ringing Line • Call Hold Reminder During Active Calls • Call Hold Reminder • Call Waiting Tone Period • Preferred Line • Preferred Line Timeout (seconds) • Goodbye Key Cancels Incoming Call • Message Waiting Indicator Line • DND Key Mode • Call Forward Key Mode This section also allows you to set: • Outgoing Intercom Settings (Admin Only; Administrator can enable these for a User if required) • Incoming Intercom Settings • Group Paging RTP Settings • Key Mapping (Admin Only) • Http Digest Settings • Ring Tones • Priority Alert Settings (Admin Only) • Directed Call Pickup Settings (Admin Only) • Auto Call Distribution Settings (Admin Only) • Time and Date Settings • Language Settings (Only the Admin can specify the language pack names to load to the phone). Both the Admin and User can select the language type to display for the Web UI.
Account Configuration	Allows you to configure DND (Do Not Disturb) and/or Call Forwarding by specific account or by all accounts. Also allows you to enable/disable specific states for each account, specify different phone numbers for call forwarding, and specify number of rings for a “No Answer” state.

HEADING	DESCRIPTION
Custom Ringtones	Allows you to upload up to 8 custom WAV file ringtones on the phone that can be used as your incoming ringtone.

Advanced Settings (Applicable to Administrator Only)

The **Advanced Settings** section provides the following options:

HEADING	DESCRIPTION
Network	Allows you to set Basic Network Settings, Advanced Network Settings, HTTPS Settings, Type of Service DSCP, and VLAN settings.
Global SIP	Allows you to set global Basic SIP Authentication Settings, Basic SIP Network Settings, Advanced SIP Settings, Real-time Transport Protocol (RTP) settings, Codec Preference List Settings, and Autodial Settings that apply to all lines on the IP phone.
Line N (where N = line number)	Allows you to set per-line Basic SIP Authentication Settings, Basic SIP Network Settings, Advanced SIP Settings, Real-time Transport Protocol (RTP) settings, and Autodial Settings that apply to specific lines on the IP phone.
Action URI	Allows an administrator to specify a uniform resource identifier (URI) that triggers a GET when certain events occur. An Administrator can also specify a URI to be called, enable polling for the URI, and specify the interval between polls. (Applicable to Administrator Only)
Configuration Server	Allows you to set the protocol to use on the configuration server (TFTP (default), FTP, HTTP, or HTTPS), configure automatic firmware and configuration file updates, enable/disable auto-resync, and assign an XML push server list. (Applicable to Administrator Only)
Firmware Update	Allows you to manually perform a firmware update on the IP phone from the configuration server using any of the IP Phones supported protocols. (Applicable to Administrator Only)
TLS Support	Allows you to specify SIP Root and Intermediate Certificate files, local certificate files, private key filename, and/or trusted certificate filename to use when the phone uses the TLS transport protocol to setup a call. (Applicable to Administrator Only)
802.1x Support	Allows you to enable/disable the 802.1x Protocol (Extensible Authentication Protocol (EAP)) to use on the IP phones for authentication purposes. Applicable choices are EAP-MD5 or EAP-TLS. (Applicable to Administrator Only)
Troubleshooting	Allows you to perform troubleshooting tasks whereby the results can be forwarded to Mitel Technical Support for analyzing and troubleshooting. Also displays system messages and error messages if applicable. **Note:** You can also specify whether a user can upload system information automatically or manually by configuring a parameter in the configuration files. For more information on this feature, see **Chapter 9**, the section“Configuration and Crash File Retrieval” on page 9-17. (Applicable to Administrator Only)

HEADING	DESCRIPTION
Capture	Tcpdump network packet capture functionality is natively available on the phones. Administrators can start/stop packet capturing, configure capture ports, set how long the capture should last, and retrieve the capture file through the Capture page. For more information on this feature, see **Chapter 9**, the section "Tcpdump Network Packet Capture Support" on page 9-20. (Applicable to Administrator Only)
Diagnostics	The Diagnostics option allows you to capture TCP network packets for up to 5 minutes as well as various logs that can in turn be used to help debug and troubleshoot various issues. For more information on this feature, see **Chapter 3**, the section "Diagnostics" on page 3-90. (Applicable to Administrator Only)
Screenshot	The Screenshot option allows you to capture a screenshot image of what is currently displayed on the respective IP phone's LCD screen in PNG format. This can be used to help document the procedures leading up to an issue or help in identifying issues with the UI. For more information on this feature, see **Chapter 3**, the section "Screenshot" on page 3-96. (Applicable to Administrator Only)

ENABLING/DISABLING THE MITEL WEB UI

The Mitel Web UI is enabled by default on the IP phones. A System Administrator can disable the Mitel Web UI on a single phone or on all phones if required using the configuration files.

System Administrators can also disable Users ability to login to the Mitel Web UI. With the Mitel Web UI disabled, users will still be able to lock/unlock the phone with a PIN from the IP Phone. Administrators can disable the user Web UI using the configuration file. System Administrators have the option to either disable the Web UI for both the Administrator and User, enable for both the Administrator and User, or enable the Web UI only for the Administrator.Use the following procedure to enable and disable the Mitel Web UI.

To Disable the Mitel Web UI:

CONFIGURATION FILES

1. Using a text-based editing application, open the *<mac>.cfg* file if you want to disable the Web UI on a single phone. Open the *startup.cfg* file to disable the Web UI on all phones
2. Enter the following parameter:

```
web interface enabled: 0
```

> **Note:** A value of zero (**0**) disables the Web UI on the phone for Administrators and Users. A value of **(1)** enables the Web UI for Administrators and Users. A value of (**2**) enables the Web UI for administrators only.

3. Save the changes and close the *<model>.cfg*, *<mac>.cfg* or the *startup.cfg* file.
4. Restart the phone to apply the changes. The Mitel Web UI is disabled for a single IP phone or for all phones.

WEB UI SECURITY FEATURES

WEB UI Lock

A security enhancement has been implemented whereby after multiple failed attempts to access the phone's Web UI, the Web UI access page will be locked for a specified period of time. The period of time is exponential (i.e. the period of time increase relative to the number of failed attempts). The table below details the period of time the Web UI is locked vs. the number of failed attempts made.

# OF FAILED ATTEMPTS	LOCKOUT TIME
1-5	N/A
6	1 minute
7	5 minutes
8	15 minutes
9-10	1 hour
11+	12 hours

Blacklist for Web Interface Attacks

An additional security feature is available for the Web UI whereby when the phone detects an attack on its Web UI, it will automatically blacklist the IP of the attacker. By default, when the initial attack is detected by the phone, access will be denied for 10 minutes. After the blacklist period expires, if another attack is detected from the same IP, access will be denied for 20 minutes and every attack thereafter will trigger the blacklist again for incrementally larger durations (i.e. 30 minutes, 1 hour, and 10 hours).

Administrators have the option of defining the maximum blacklist duration using the “**web interface blacklist duration**” parameter. By configuring this parameter, administrators can set the maximum amount of time the IP of the offending attacker will remain on the blacklist.

Use the following procedures to configure the maximum Web UI blacklist duration.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Mitel Web UI Settings” on page A-32.

SECURE WEB SERVICE FEATURE

The parameter "**secure web service**" is available allowing Administrators the ability to manually open or close HTTP/HTTPs ports 80 and 443 as well as port 49249. Closing these ports not only disables users from accessing the Web UI and other services such as XML, BroadWorks Xsi, and custom ring tones, but will also help nullify web server attacks as the ports will not be visible using port scanning software.

By defining the "**secure web service**" parameter as "1" in the configuration files, Administrators can close TCP ports 80, 443, and 49249 on the phone.

Notes:

1. Ports 80, 443, and 49249 are open by default.
2. Closing ports 80, 443, and 49249 does not have an effect on the HTTP/HTTPs client service on the phone.
3. This parameter takes precedence over the "**web interface enabled**" parameter. For example, if the "**web interface enabled**" parameter is defined as "1" (the Web UI is enabled) and the "**secure web service**" parameter is defined as "1" (ports 80, 443, and 49249 are closed), users will not be able to access the Web UI. Alternatively, if the "**web interface enabled**" parameter is defined as "0" (the Web UI is disabled) and the "**secure web service**" parameter is defined as "0" (ports80, 443, and 49249 are open), users will not be able to access the Web UI but the ports will still be open and visible.

Use the following procedures to manually open/close ports 80, 443, and 49249.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Secure Web Service Settings” on page A-33.

CONFIGURATION FILES (ADMINISTRATOR ONLY)

A system administrator can enter specific parameters in the configuration files to configure the IP phones. All parameters in configuration files can only be set by an administrator.

You can enter specific configuration parameters in either of the following configuration files:

- startup.cfg
- <model>.cfg
- <mac>.cfg

REFERENCES

For information about configuration file precedence, see Configuration File Precedence on page 1-43. For a description of each configuration file parameter, see Appendix A, "About this Appendix."

USING THE CONFIGURATION FILES

When you use the configuration files to configure the IP phones, you must use a text-based editing application to open the configuration file (startup.cfg, <model>.cfg, or <mac>.cfg).

Use the following procedure to add, delete, or change parameters and their settings in the configuration files.

Note: Apply this procedure wherever this Administrator Guide refers to configuring parameters using the configuration files.

CONFIGURATION FILES

1. Using a text-based editing application, open the configuration file for the phone, for which you want to configure the CSV directory list (either startup.cfg, <model>.cfg, <mac>.cfg or all three).
2. Enter the required configuration parameters followed by the applicable value. For example,

```
directory 1: company_directory
directory 2: my_personal_directory
```

3. Save the changes and close the configuration file.
4. If the parameter requires the phone to be restarted in order for it to take affect, use the IP Phone UI or the Mitel Web UI to restart the phone.

LOCKING PARAMETERS IN THE CONFIGURATION FILE

The IP Phones allow you to lock individual configuration parameters to prevent an end user from changing the configuration on the phone. This feature allows service providers to prevent the end-user from changing the values of specific parameters that would affect the service they provide.

An Administrator can lock parameters on the phone by placing an **exclamation mark** (**!**) before the parameter in the configuration file. For example,

```
!admin password: 22222
!emergency dial plan: 911|999
```

You can lock parameters on the phone using the configuration files. Once the parameters are locked, they cannot be changed at all during the phones run-time. The parameters appear as read-only when accessing the Mitel Web UI and the IP Phone UI. In the Mitel Web UI, they appear grayed out. In the IP Phone UI the ability to change the parameters is removed. In addition, when parameters are locked, they cannot be changed via XML.

Notes:

1. The “parameter locking” feature applies to Release 2.4 and up. Any phones that have a previous release loaded on the phone will not be able to use the locking functionality in the configuration file.
2. Any parameter duplicated in the ***<model>.cfg*** from the ***startup.cfg*** is overwritten by the locking status and the value of the parameter found in the ***<model>.cfg*** file. Parameters in the ***<mac>.cfg*** file overwrite parameters in the ***<model>.cfg*** and ***startup.cfg*** files.

Limitations

- A User possessing the Administrator password can bypass the locking of configuration server details by defaulting the phone.
- Softkeys can be locked and unlocked via XML using the **AastraIPPhoneConfiguration** object and **softkeyN locked** parameter (for more information about using the **AastraIP-PhoneConfiguration** object, contact Mitel Customer Support regarding the ***Mitel XML Development Guide***). All other parameters cannot be locked or unlocked using XML.
- Configuration files that include locked parameters are not backwards compatible.

OVERWRITING PARAMETERS WITH DEFAULTS IN THE CONFIGURATION FILES

An Administrator can specify a “ **^** “ (caret character) before a configuration parameter in the *startup.cfg, <model>.cfg,* and *<mac>.cfg* configuration files, which allows the parameter to be overwritten and reset back to a specified value. This can be convenient when changes are made by a user to specific parameters on the phone locally (via Mitel Web UI or IP Phone UI), and the Administrator wants to set the parameters back to the default values using the configuration files.

As an example, the following table describes how the parameter “**sip proxy ip**” is handled by the phone during phone bootup when either the “ ^ “ (default parameter) is used or the “ ! “ (locked parameter) is used.

IF	THEN
new *<mac>.cfg* file is loaded to the phone with “**^sip proxy ip**” and any other parameter(s) from the file specifying a “ **^** “	the “**^sip proxy ip**” and any other “ **^** “ parameters are overwritten if previously changed by the user.

IF	THEN
new *<model>.cfg* file is loaded to the phone with "**^sip proxy ip**" and any other parameter(s) from the file specifying a " **^** "	the "**^sip proxy ip**" and any other " **^** " parameters are overwritten if previously changed by the user.
new *startup.cfg* file is loaded to the phone with "**^sip proxy ip**" and any other parameter(s) from the file specifying a " **^** "	the "**^sip proxy ip**" and any other " **^** " parameters are overwritten if previously changed by the user.
the first instance is "**^sip proxy ip**" and second instance is "**!sip proxy ip**" in the *startup.cfg, <model>.cfg,* and/or *<mac>.cfg* file,	the value for the second instance of the parameter ("**!sip proxy ip**") overwrites to the *startup.cfg, <model>.cfg,* and/or *<mac>.cfg files* previously on the phone.

Notes:

1. XML reboots take precedence over *server.cfg* values. Therefore, " ^ " parameters are ignored in the *startup.cfg* file during XML reboots.
2. If a parameter has both a " ^ " and a " ! " preceding the same parameter (i.e. ^!sip proxy ip: pbx.company.com), then the parameter is ignored and NOT overwritten.

Example 1

The following example illustrates the use of the " ^ " in the configuration files.

startup.cfg

```
^sip proxy ip: pbx.company.com
^sip proxy port: 5060
^sip registrar ip: pbx.company.com
^sip registrar port: 5060
```

In the above example, if an Administrator indicates the " ^ " before the parameters in the *startup.cfg* file, and then loads the *startup.cfg* file to the phone, these four parameters are reset to their default values, even if the parameters were previously changed on the phone.

Example 2

The following example illustrates the use of the " ^ " and "!" in the configuration files.

startup.cfg

```
^sip proxy ip: pbx.company.com
^sip proxy port: 5060
^sip registrar ip: pbx.company.com
^sip registrar port: 5060
```

<model>.cfg

```
!sip proxy ip: pbx.mitel.com //this parameter is locked
!sip proxy port: 5062 //this parameter is locked
!sip registrar ip: pbx.mitel.com//this parameter is locked
!sip registrar port: 5062//this parameter is locked
```

<mac>.cfg

```
sip proxy port: 5064 //this parameter is unlocked
sip registrar port: 5064//this parameter is unlocked
```

With this configuration, on the Web UI, the "**sip proxy ip**" and "**sip registrar ip**" parameters cannot be modified (they are grayed out), and the value is "pbx.mitel.com" since ***<model>.cfg*** has overwritten ***startup.cfg***.

The "**sip proxy port**" and "**sip registrar port**" parameters can be modified through Web UI because ***<mac>.cfg*** has overwritten ***<model>.cfg*** and ***startup.cfg***. On the Web UI, the value for these parameters is 5064.

CONFIGURATION SERVER REDUNDANCY VIA DNS A RECORDS

The phone sends a DNS query and in the DNS response, it accepts the first server IP address and contacts that server, ignoring any additional IP addresses in the response. This allows service providers to manage load balancing (via the DNS server putting different records first on each request), but does not provide redundancy.

The phones also provide support of multiple IP addresses being returned for the DNS lookup for server redundancy via multiple DNS A record entries. The phone tries to contact the first server address it receives, but if this fails, it now tries to contact the second server address, etc.

This feature supports all the download protocols (TFTP, FTP, HTTP, and HTTPS).

Notes:

1. Once the phone has failed over to a redundant server, it continues to use that server for all other server-related processes on the phone (i.e. firmware upgrades from the Web UI, boot-up process, etc.).
2. If a server fails while downloading a file(s) to the phone, the phone performs the discovery process of finding a redundant server that is available. When the boot is complete on the redundant server, the phone tries to download the file(s) again from the previous server. The check-sync process also performs the same way when a server fails.
3. The “**Skip**” softkey displays in the event of a network outage, the user can skip the configuration download and continue the boot.
4. All server failovers and failed server IP addresses are logged in the “Error Messages” page on the IP Phone UI at *Options->Phone Status->Error Messages*.

Limitation

In certain cases, the TFTP Protocol cannot distinguish between “server down” and “no file on server” error messages; therefore, the failover in these instances may fail.

Chapter 3

ADMINISTRATOR OPTIONS

ABOUT THIS CHAPTER

The IP phones provide specific options on the IP Phone that only an Administrator can access. These options are password protected and allow an Administrator to change or set features and configuration information as required. For all models, an Administrator can use the IP Phone UI, the Mitel Web UI, or the configuration files to enter and change values.

Note: Specific options are configurable only via the IP Phone UI, and/or Mitel Web UI, and/or configuration files.

This chapter provides information about the available Administrator options.

TOPICS

This chapter covers the following topics:

ADMINISTRATOR LEVEL OPTIONS

DESCRIPTION

There are options on the IP phone that both a User and Administrator can access. However, there are specific options that an Administrator can access only. These options allow the Administrator to configure and manage local and/or remote IP phones in a network.

An Administrator can access and manage these options using the IP Phone UI, the Mitel Web UI, or the configuration files.

IP PHONE UI OPTIONS

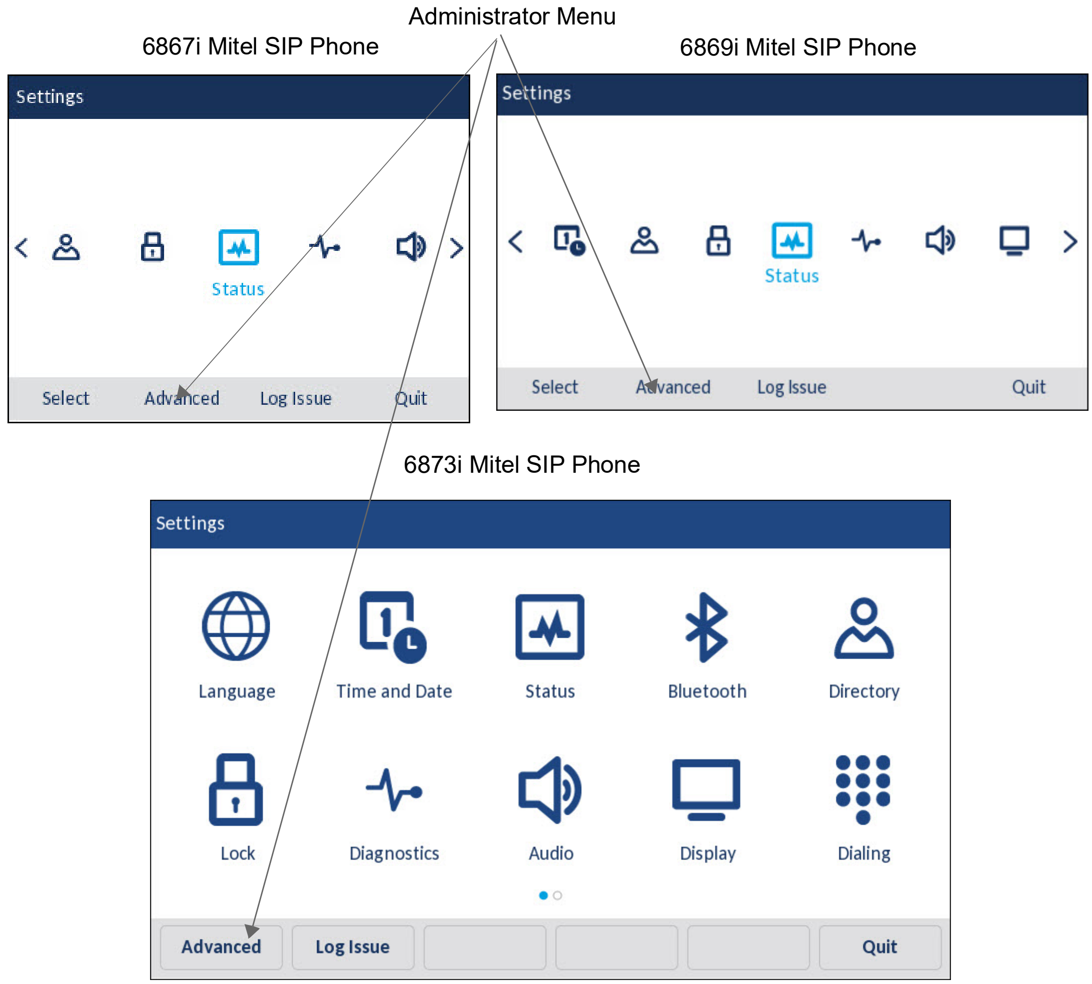
ADMIN MENU/ ADVANCED KEY

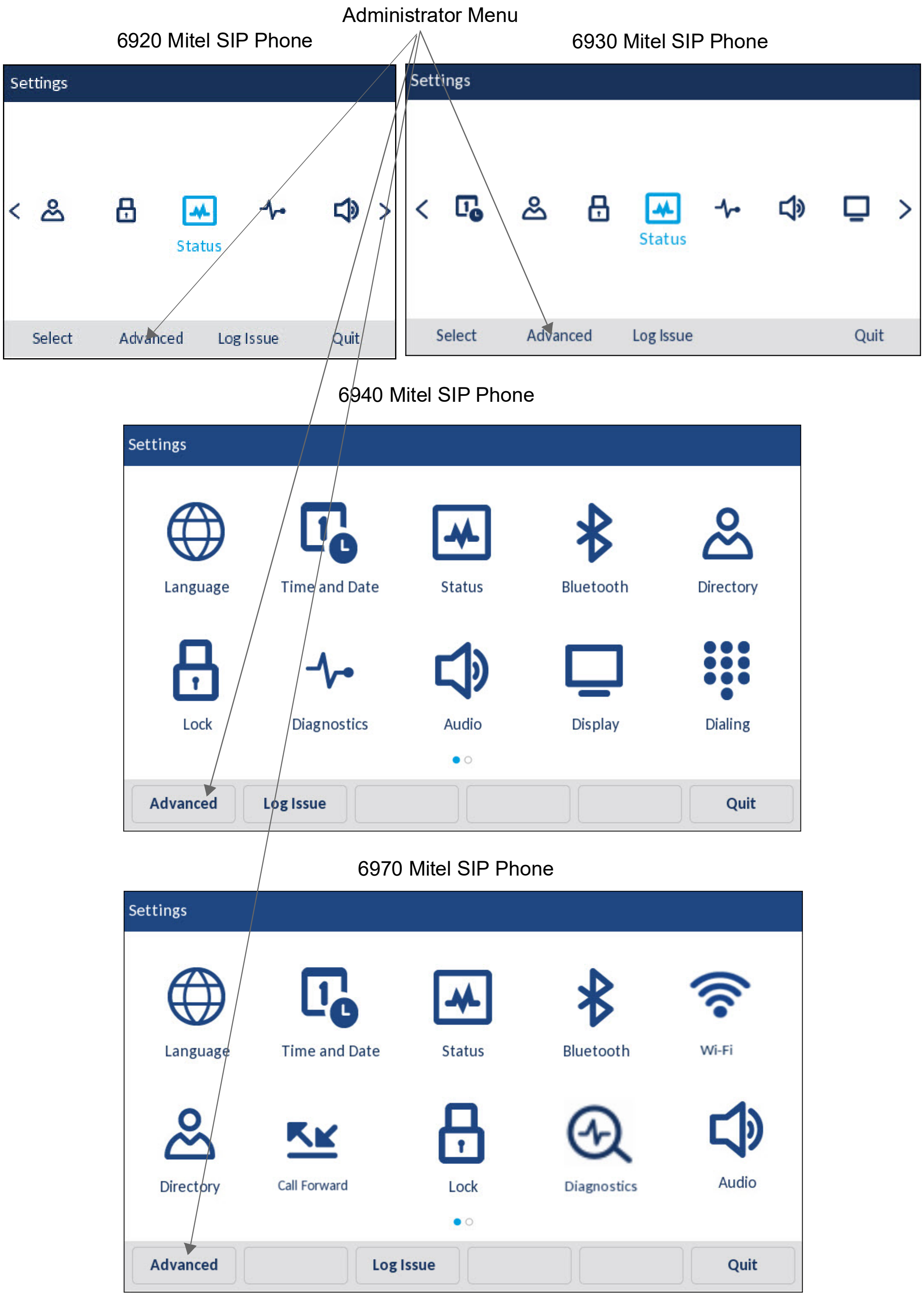
Using the 6863i/6865i/6905/6910 IP Phone UI, you can access the Administrator options at **Options > Admin Menu** using the default password of "**22222**"

The following are administrator options in the "**Options List**" on the 6863i, 6865i, 6905, and 6910:

- Administrator Menu
  - Configuration Server
  - SIP Settings
  - Network Settings
  - Factory Default
  - Erase Local Config

The 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 have an "Advanced" softkey, which when pressed and the password entered gives access to the Administrator options.




Administrator Menu
6920 Mitel SIP Phone
6930 Mitel SIP Phone
Settings
Status
Select
Advanced
Log Issue
Quit
Settings
Status
Select
Advanced
Log Issue
Quit
6940 Mitel SIP Phone
Settings
Language
Time and Date
Status
Bluetooth
Directory
Lock
Diagnostics
Audio
Display
Dialing
Advanced
Log Issue
Quit
6970 Mitel SIP Phone
Settings
Language
Time and Date
Status
Bluetooth
Wi-Fi
Directory
Call Forward
Lock
Diagnostics
Audio
Advanced
Log Issue
Quit

The following are administrator options in the "**Options List**" on the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 Advanced menu:

- Configuration Server
- SIP Settings
- Network Settings
- Bluetooth Auto Connect

Note: On the 6970 IP Phone user can control the Bluetooth auto-connect behavior, by using the options available in Advanced Settings. For more information refer to the Bluetooth section of the **Mitel 6970 SIP Phone User Guide**.

- Reset (includes options for “Erase Local Config” and “Factory Default”)

Note: An administrator has the option of enabling and disabling the use of password protection on the IP phone UI for all model phones. This is configurable using the configuration files only. For more information about this feature, see Appendix A, the section “Password Settings” on page A-20.

References

For information about all other user options in the "**Options Menu**", see your <Model-Specific> ***SIP Phone User Guide***.

For procedures on configuring Administrator Options on the IP phone via the IP phone UI, see:

- Chapter 4, "Configuring Network and Session Initiation Protocol (SIP) Features"
- Chapter 5, "Configuring Operational Features"
- Chapter 6, "Configuring Advanced Operational Features"

SIMPLIFIED IP PHONE UI OPTIONS MENU

An Administrator can replace the existing options menu on the Phone UI with a more simplified options menu. In the configuration files, the "**options simple menu**" parameter allows you to display either the full menu (if set to 0), or the simplified menu (if set to 1). The following table illustrates the differences between the full menu and the simplified menu.

Note: When setting the "**options simple menu"** parameter, the menu changes in the Phone UI only. The Mitel Web UI is not affected.

6863i, 6865i, 6905, and 6910

FULL OPTIONS MENU	SIMPLIFIED OPTIONS MENU
Preferences	Preferences
Phone Status	Phone Status
Password	Removed
Administrator Menu	Removed
Restart Phone	Accessible through Phone Status
Phone Lock	Phone Lock

6867i, 6869i, 6920, and 6930

FULL OPTIONS MENU	SIMPLIFIED OPTIONS MENU
Language	Removed
Time and Date	Removed
Directory	Removed
Credentials	Removed
Lock	Lock (Password Sub-Option Removed)
Status	Status
Diagnostics	Removed
Audio	Audio
Display	Display
Dialing	Removed
Restart	Restart
Advanced	Only Factory Default option available.

6873, 6940, and 6970

FULL OPTIONS MENU	SIMPLIFIED OPTIONS MENU
Language	Removed
Time and Date	Removed
Status	Status
Bluetooth	Bluetooth
Directory	Removed
Lock	Lock (Password Sub-Option Removed)
Diagnostics	Removed
Audio	Audio
Display	Display
Dialing	Removed
Restart	Restart
Advanced	Only Factory Default option available.

Note: When using the simplified menu, you cannot change the Network settings from the IP Phone UI. If the network settings become misconfigured, you must use the Mitel Web UI to configure the network settings or factory default the phone through the Web UI and then use the Phone UI's full options menu to recover the networks setting.

CONFIGURING THE SIMPLIFIED IP PHONE UI OPTIONS MENU

You can enable the simplified IP Phone UI Options menu using the configurations files only.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, “Simplified IP Phone UI Options Menu” on page 12.

LOG ISSUE KEY

You can collect and upload logs to the diagnostic server from your 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 SIP phones.

By default, Log Issue is not displayed on the phone's UI. The system administrator needs to set the configuration parameters to enable or disable the Log Issue option.

Enabling/Disabling Log Issue Using the Configuration Files

Use the following procedure to enable/disable Log Issue on the phone using the configuration files.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section,"Diagnostics," on page 355.

Collecting and Uploading Logs

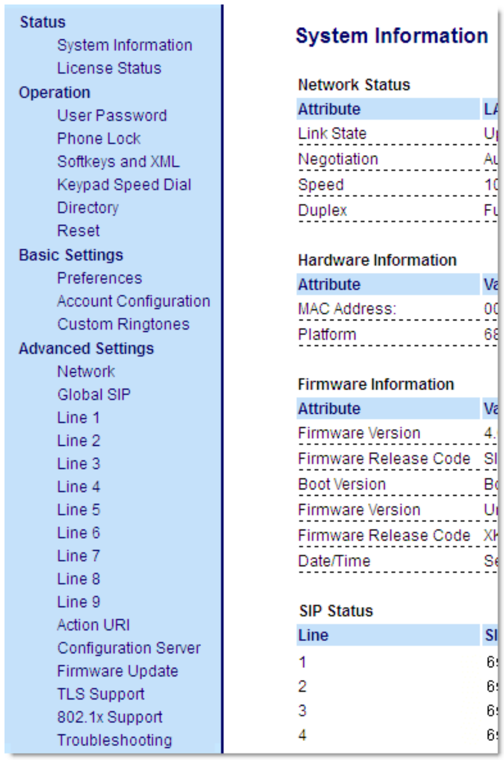
1. Press the **Settings** key / the **Settings** softkey on your SIP phone.
2. Press the **Log Issue** softkey, and wait for at least five minutes for the log processing to occur. The phone UI displays 'Logging the issue - Please wait...'.

For information on downloading logs from the Web UI using Get Log Files command, see "Performing Troubleshooting Tasks," on page 8.

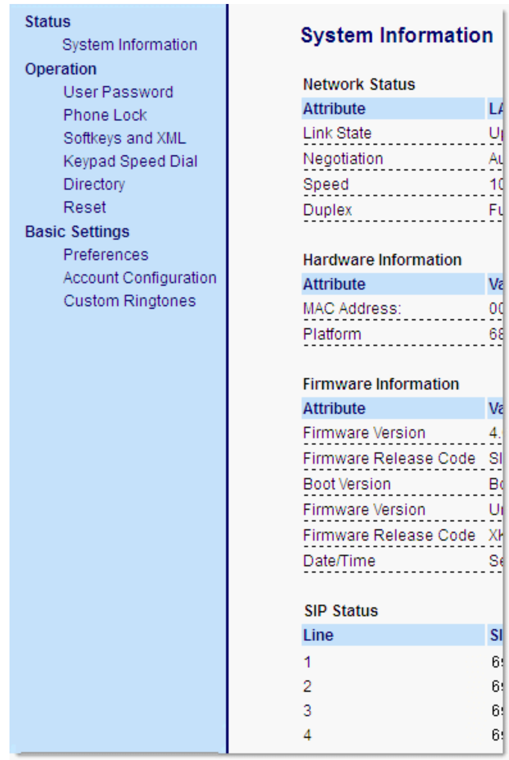
MITEL WEB UI OPTIONS

An Administrator can configure specific options using the Mitel Web UI. These options display after an Administrator logs into the Web UI using a Web browser and entering the Admin username and password at the login prompt (The default username is "**admin**" and the default password is "**22222**". The IP phones accept numeric passwords only.) The column on the left side of the screen indicates the configurable options. A User has limited configuration options as shown in the following illustrations.

Administrator Web UI Menu



User Web UI Menu



The following are options that an Administrator can configure in the Mitel Web UI (and are not available for the User to configure):

- Operation->Reset
  - Restore to Factory Defaults
  - Remove Local Configuration Settings
- Basic Settings->Preferences->General
  - Local Dial Plan
  - Send Dial Plan Terminator
  - Digit Timeout (seconds)
- **Basic Settings->Preferences->Outgoing Intercom Settings** (User can configure this via the Mitel Web UI if enabled by an Administrator)
- Basic Settings->Preferences->Key Mapping
- Basic Settings->Preferences->HTTP Digest Settings
- Basic Settings->Preferences->Priority Alerting Settings
- Basic Settings->Preferences->Directed Call Pickup Settings
- Basic Settings->Preferences->Auto Call Distribution Settings
- Basic Settings->Preferences->Language Settings

  - Language 1 (entering language pack filename)
  - Language 2 (entering language pack filename)
  - Language 3 (entering language pack filename)
  - Language 4 (entering language pack filename)
- Basic Settings->Custom Ringtones (User can configure this via the Mitel Web UI if enabled by an Administrator)
- Advanced Settings
  - Network
  - Global SIP
  - Line 1 through N Settings
  - Action URI
  - Configuration Server
  - Firmware Update
  - TLS Support
  - 802.1x Support
  - Troubleshooting
  - Capture
  - Diagnostic
  - Screenshot

REFERENCES

For information about options available to a User AND Administrator in the Mitel Web UI, see your <Model-Specific> ***SIP Phone User Guide***.

For procedures to Restart your phone or restore factory defaults, see "Restarting Your Phone" on page 3-15, and "Set Phone to Factory Defaults/Erase Local Configuration" on page 3-16.

For more information about Advanced Settings for the IP Phone, see Chapter 4, "Configuring Network and Session Initiation Protocol (SIP) Features."

For procedures on configuring the Basic Settings for the IP Phone, see Chapter 5, "Configuring Operational Features."

CONFIGURATION FILE OPTIONS

An Administrator can enter specific parameters in the configuration files to configure the IP phones. All parameters in configuration files can only be set by an administrator.

REFERENCES

For a procedure on using the configuration files, see Chapter 2, the section, "Configuration Files (Administrator Only)" on page 2-1.

For a description of each parameter you can enter in the configuration files, see Appendix A, "Configuration Parameters."

PHONE STATUS

The **Phone Status** on the IP Phone displays the network status and firmware version of the IP phone.

You can display phone status using the IP phone UI or the Mitel Web UI.

PHONE STATUS VIA IP PHONE UI

In the IP phone UI, the Phone Status options are available to the user and the administrator and do not require a password entry.

Phone Status for 6863i, 6865i, 6905, and 6910 IP Phones

- **IP&MAC Addresses**
  - Displays the IP address and MAC address of the phone.
- **LAN Port**
  - Displays the Link State, Negotiation Method, Speed, and Duplex Method that the phone uses on its LAN port.
- **PC Port**
  - Displays the Link State, Negotiation Method, Speed, and Duplex Method that the phone uses on its PC Port.
- **Firmware Info**
  - Displays information about the firmware and boot version that is currently installed on the IP phone.
- **Error Messages**
  - Displays any error messages that occurred during the phone's last reboot.

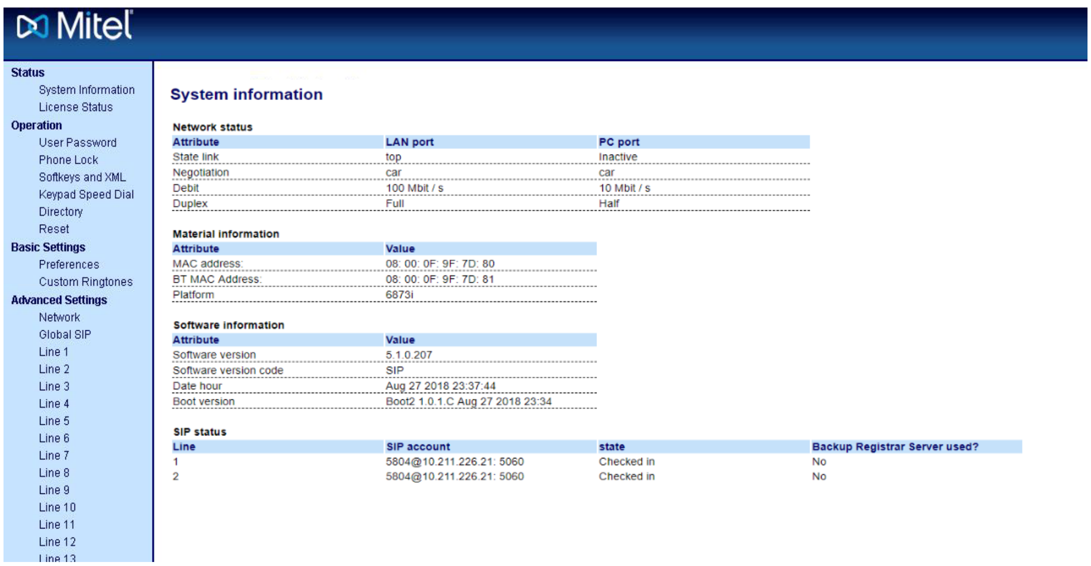
Phone Status for 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones

- **Firmware Info**
  - Displays information about the platform, phone info, and boot version that is currently installed on the IP phone.

- **Accessory Info**
  - Displays firmware information about any accessories currently attached to the phone.
- **Network**
  - **IP Address** - Displays the IP address of the phone.
  - **MAC Address** - Displays the MAC address of the phone.
  - **LAN Port** - Displays the Link State, Negotiation Method, Speed, and Duplex Method that the phone uses on its LAN port.
  - **PC Port** - Displays the Link State, Negotiation Method, Speed, and Duplex Method that the phone uses on its PC Port.
- **Storage**
  - Displays the number of Local Directory, Received Callers, and Outgoing Redial List entries saved on the phone.
- **Error Messages**
  - Displays any error messages that occurred during the phone's last reboot.

PHONE STATUS VIA MITEL WEB UI

The first screen that displays after logging into the Mitel Web UI for a phone is the Status screen. This screen also displays when selecting **Status->System Information**. The information on this screen is available to the user and the administrator as read-only.



The following is a description of the information on the Status screen:

- **Network Status**
  - Displays the network status of the Ethernet ports at the back of the phone. You can also view the phone's IP and MAC addresses. Information in this field includes Link State, Negotiation, Speed, and Duplex for Port 0 and Port 1.
- **Hardware Information**
  - Displays the current IP phone platform and the MAC address.
- **Firmware Information**
  - Displays information about the firmware that is currently installed on the IP phone (and K680i Keyboard if applicable). Information in this field includes Firmware Version, Firmware Release Code, Boot Version, Release Date/Time.
- **SIP Status**
  - Displays information about the SIP registration status of the phone and provides option to upload the system information. If there are accounts configured on the IP Phone, their SIP status displays in this field. Excluding the 6863i (2 lines), all model phones display the status of up to 24 lines.

The following table describes the status conditions that can display for an account(s).

STATUS CONDITION	DESCRIPTION
Registered	Displays this status on accounts that HAVE been registered with the SIP proxy server. **Example**: **Line** | **SIP Account** | **Status** | **Backup Registrar Used?** 1 | 650@proxy.com:5060 | Registered | Yes **where** Account Number is "1" SIP Account is "650@proxy.com" on port "5060" Status is "Registered" Backup registrar is used ("Yes")
SIP Error Number	Displays on accounts when registration fails with the SIP proxy server. **Example**: **Line** | **SIP Account** | **Status** | **Backup Registrar Used?** 4 | 653@proxy.com:5060 | 401 | No **where** Account Number is "4" SIP Account is "653@proxy.com" on port "5060" Status is "401" - Unregistered if SIP registration fails. Backup registrar is used ("No")

Note: The IP Phones can register with multiple server using the same user name. So the SIP Status information on the Status screen may display the same account with different registrar and proxy IP addresses.

RESTARTING YOUR PHONE

As System Administrator, there may be times when you need to restart a phone. The Restart option allows you reboot the phone when required. A reset may be necessary when:

- There is a change in your network, **OR**
- To re-load modified configuration files, **OR**
- If the settings for the IP phone on the IP PBX system have been modified.

Note: The SIP phones unregister all accounts before executing a reboot.

You can restart the phone using the IP Phone UI or the Mitel Web UI.

RESTARTING THE PHONE USING THE IP PHONE UI

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Restart Phone**.
3. Press **#** to confirm.

Note: To cancel the Restart, press the 3key.

For the 6867i/6869i/6920/6930:

1. Press or on the phone to enter the Options List.
2. Navigate to the **Restart** option and press the or **Select** button or **Select** softkey. A "Restart Phone?" prompt displays.
3. Select **Yes** using the or **Select** button to restart the phone. Press **No** using the or **Select** button to cancel the restart function.

For the 6873i/6940:

1. Press or on the phone to enter the Options List.
2. Tap the **Restart** icon. A "Restart Phone?" prompt displays.

Note: If required, swipe left on the screen to navigate to the second page of options.

3. Tap **Yes** to restart the phone. Tap **No** to cancel the restart function.

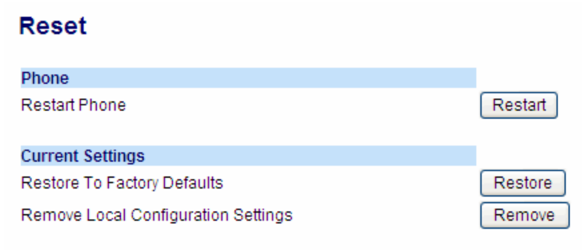
For the 6970:

1. Tap the **Settings** softkey.
2. Select **Restart**.
3. Tap **Yes**.

RESTARTING THE PHONE USING THE MITEL WEB UI

MITEL WEB UI

1. Click on **Operation->Reset->Phone.**



2. Click **Restart** to restart the phone.

SET PHONE TO FACTORY DEFAULTS/ERASE LOCAL CONFIGURATION

You can set phones to their factory default settings or remove a local phone's configuration using the IP Phone UI or the Mitel Web UI.

SETTING FACTORY DEFAULTS ON THE PHONE

Factory default settings are the settings that reside on the phone after it has left the factory. Performing a factory default on the phone will revert all the settings in the *startup.cfg*, *<model>.cfg*, *<mac>.cfg,* and local configuration back to the original factory values. You can reset a phone to factory defaults using the IP Phone UI or the Mitel Web UI.

Note: Performing a factory default is only applicable to the phone settings and does not affect the firmware version loaded on the phone.

Setting Factory Defaults Using the IP Phone UI

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Administrator Menu** and enter your Administrator Password (default is **22222**).
3. Select **Factory Default.**
   The "*Restore Defaults?*" prompt displays.

4. Press **#** to confirm.
5. After **#** is selected the phone reboots and a Voice Services screen auto-prompts the user to select an appropriate service.

For the 6867i/6869i/6920/6930:

1. Press or on the phone to enter the Options List.
2. Press the **Advanced** softkey.
3. Enter the Administrator password and press **Enter**. Default is “**22222**”.
4. Navigate to the **Reset** option and press the or **Select** button or **Select** softkey.
5. Select **Factory Default** using the or **Select** button or press the **Select** softkey. A “*Factory Default?*” prompt displays.
6. Select **Yes** using the or **Select** button to factory default the phone. Press **No** using the button to cancel the factory default function.
7. If **Yes** is selected the phone reboots and a Voice Services screen auto-prompts the user to select an appropriate service.

For the 6873i/6940:

1. Press or on the phone to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password and press the blue Enter key. Default is “**22222**”.
4. Tap the **Reset** icon.

   Note: If required, swipe left on the screen to navigate to the second page of options.

5. With the **Factory Default** option highlighted press the **Select** softkey. A “*Factory Default?*” prompt displays.
6. Tap **Yes** to restart the phone. Tap **No** to cancel the restart function.
7. If **Yes** is selected the phone reboots and a Voice Services screen auto-prompts the user to select an appropriate service.

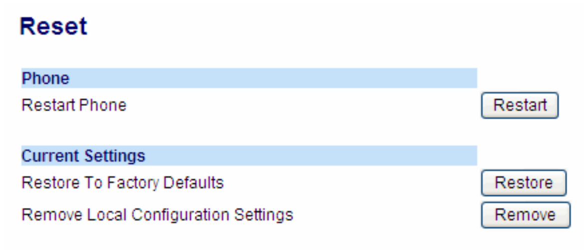
For the 6970:

1. Tap the **Settings** softkey.
2. Select **Reset** > **Factory Default**.
3. Tap **Yes** to execute factory default of the phone. Press **No** to cancel the factory default function.
4. If **Yes** is selected the phone reboots and a Voice Services screen auto-prompts the user to select an appropriate service.

Settings Factory Defaults Using the Mitel Web UI

MITEL WEB UI

1. Click on **Operation->Reset->Current Settings.**



2. In the "**Restore to Factory Defaults**" field, click **Restore**.
   This restores all factory defaults, and removes any saved configuration and directory list files.

3. After factory default of the 6900 series SIP phone, a Voice Services screen auto-prompts the user to select an appropriate service.

ERASING THE PHONE'S LOCAL CONFIGURATION

You can reset the IP Phone's local configuration if required. The local configuration is the last updated configuration you performed using the IP Phone UI or the Mitel Web UI. Performing this action results in losing all recently user-modified settings. For more information about local configuration, see Chapter 1, the section, "Configuration File Precedence" on page 1-43.

Erasing the Phone's Local Configuration Using the IP Phone UI

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Administrator Menu** and enter your Administrator Password (default is **22222**).
3. Select **Erase Local Config.**
   The "*Erase local config?*" prompt displays.
4. Press **#** to confirm.

For the 6867i/6869i/6920/6930:

1. Press or on the phone to enter the Options List.
2. Press the **Advanced** softkey.
3. Enter the Administrator password and press **Enter**. Default is "**22222**".
4. Navigate to the **Reset** option and press the or **Select** button or **Select** softkey.
5. Select **Erase Local Cfg.** using the or **Select** button or press the **Select** softkey.
   An "*Erase Local Configuration?*" prompt displays.
6. Select **Yes** using the or **Select** button to erase the local configuration. Press **No** using the button to cancel the erase function.

For the 6873i/6940:

1. Press or on the phone to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password and press the blue Enter key. Default is "**22222**".
4. Tap the **Reset** icon.

   Note: If required, swipe left on the screen to navigate to the second page of options.

5. Tap **Erase Local Cfg.**
6. With the **Erase Local Cfg**. option highlighted press the **Select** softkey.
   An "*Erase Local Configuration?*" prompt displays.
7. Tap **Yes** to erase the local configuration. Tap **No** to cancel the erase function.

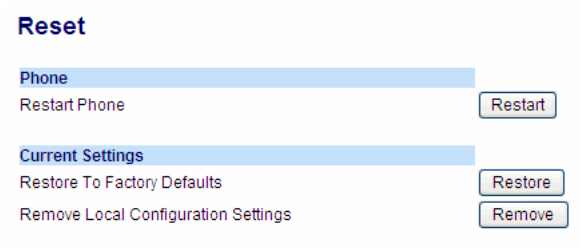
For the 6970:

1. Tap the **Settings** softkey.
2. Tap **Advanced**.
3. Enter the Administrator password and tap **Enter**. The default password is “**22222**”.
4. Select **Reset** > **Erase Local Cfg.**
5. Tap **Yes** to erase the local configuration. Tap **No** to cancel the erase function.

Erasing the Phone’s Local Configuration Using the Mitel Web UI

MITEL WEB UI

1. Click on **Operation->Reset->Current Settings.**



2. In the "**Remove Local Configuration Settings**" field, click **Remove**.
   This removes the last customized configuration settings made on the phone.

BASIC SETTINGS

An Administrator has access to specific Basic Setting options to configure and manage the IP Phone in the network. The following sections identify the options available to an Administrator only, or where indicated, to a User and Administrator. These tables also identify whether you can configure them using the Mitel Web UI, IP Phone UI, or the configuration files.

GENERAL SETTINGS

PARAMETER IN MITEL WEB UI	PARAMETER IN CONFIGURATION FILES	DESCRIPTION
Local Dial Plan	sip dial plan	A dial plan that describes the number and pattern of digits that a user dials to reach a particular telephone number. Dial Plan field accepts up to 512 characters. For more information on this feature, see "Local Dial Plan" on page 5-80.
Send Dial Plan Terminator	sip dial plan terminator	Specifies whether or not pressing the hash/pound (i.e. "#") key, while performing an outgoing call on an open line, should be sent as %23 to the proxy in the dial string or if the key should be used as a dial plan terminator (i.e. dials out the call immediately). For more information on this feature, see "SIP Dial Plan Terminator" on page 5-82.
Digit Timeout	sip digit timeout	Represents the time, in seconds, to configure the timeout between consecutive key presses. For more information on this feature, see. "Digit Timeout" on page 5-82.
Park Call **Note:** This option can be set by both Users and Administrators.	sip lineN park pickup config	The parking of a live call to a specific extension. **Note:** This feature on the Basic Preferences screen is not available on the 6863i and 6865i. To configure the Park feature on a key, see Chapter 5, the section, "Park/Pick Up Static and Programmable Configuration" on page 5-241.
Pick Up Parked Call **Note:** This option can be set by both Users and Administrators.	sip lineN park pickup config	Picking up a parked call at the specified extension. **Note:** This feature on the Basic Preferences screen is not available on the 6863i and 6865i. To configure the Pickup feature on a key, see Chapter 5, the section, "Park/Pick Up Static and Programmable Configuration" on page 5-241.
N/A	suppress dtmf playback	Enables and disables suppression of DTMF playback when a number is dialed from the softkeys or programmable keys. For more information on this feature, see. "Suppressing DTMF Playback" on page 5-85.

PARAMETER IN MITEL WEB UI	PARAMETER IN CONFIGURATION FILES	DESCRIPTION
Display DTMF Digits **Note:** This option can be set by both Users and Administrators.	display dtmf digits	Enables and disables the display of DTMF digits on the IP phone display during a connected state. For more information on this feature, see. "Display DTMF Digits" on page 5-85.
Play Call Waiting Tone **Note:** This option can be set by both Users and Administrators.	call waiting tone	Enable or disables the playing of a call waiting tone when a caller is on an active call and a new call comes into the phone. For more information on this feature, see. "Call Waiting Tone" on page 5-89.
Stuttered Dial Tone **Note:** This option can be set by both Users and Administrators.	stutter disabled	Enable or disables the playing of a stuttered dial tone when there is a message waiting on the IP phone. For more information on this feature, see. "Stuttered Dial Tone" on page 5-94.
XML Beep Support **Note:** This option can be set by both Users and Administrators.	xml beep notification	Enables or disables the playing of a beep to indicate a status on the phone. When the phone receives a status message, the BEEP notifies the user that the message is displaying. For more information on this feature, see "XML Beep Support" on page 5-95.
Status Scroll Delay (seconds) **Note:** This option can be set by both Users and Administrators.	xml status scroll delay	Allows you to set the time delay, in seconds, between the scrolling of each status message on the phone. For more information on this feature, see "Status Scroll Delay" on page 5-97.
Switch UI Focus to Ringing Line **Note:** This option can be set by both Users and Administrators.	switch focus to ringing line	Enables or disables whether or not the UI focus is switched to a ringing line while the phone is in the connected state. For more information on this feature, see "Switch Focus to Ringing Line" on page 5-98.

PARAMETER IN MITEL WEB UI	PARAMETER IN CONFIGURATION FILES	DESCRIPTION
Call Hold Reminder During Active Calls **Note:** This option can be set by both Users and Administrators.	call hold reminder during active calls	Enables or disables the ability for the phone to initiate a continuous reminder tone on the active call when another call is on hold. When this feature is disabled, a ring splash is heard when the active call hangs up and there is still a call on hold. For more information on this feature, see “Call Hold Reminder During Active Calls” on page 5-99.

PARAMETER IN MITEL WEB UI	PARAMETER IN CONFIGURATION FILES	DESCRIPTION
Call Hold Reminder **Note:** This option can be set by both Users and Administrators.	call hold reminder	Enables or disables the reminder ring splash timer to start as soon as you put a call on hold (even when no other calls are active on the phone). When enabled, the phone initiates a reminder ring splash periodically for the single call on hold. When disabled, no reminder ring splash is audible. For more information on this feature, see "Call Hold Reminder (on Single Hold)" on page 5-101.
	call hold reminder timer **Note:** This option can be set by an Administrator only.	Specifies the time delay, in seconds, that a ring splash is heard on an active call when another call was placed on hold. For example, if a call comes into Line 1, and then a call comes into Line 2 and you answer Line 2, Line 1 is automatically placed on hold. While on the active Line 2, after 7 seconds, a ring splash audio sounds on the line reminding you that the call on Line 1 is still on hold. This timer begins to increment after Line 2 is answered. **Notes:** **1.** This parameter is used with the "call hold reminder frequency" parameter. **2.** You must enable this "call hold reminder timer" parameter for it to work. **3.** A value of "0" disables the call hold reminder feature. For more information on this feature, see "Call Hold Reminder Timer & Frequency" on page 5-102.
	call hold reminder frequency **Note:** This option can be set by an Administrator only.	Specifies the time interval, in seconds, between each ring splash sound on the active line. For example, if a call comes into Line 1, and then a call comes into Line 2 and you answer Line 2, Line 1 is automatically placed on hold. While on the active Line 2, after 7 seconds, a ring splash audio sounds on the line reminding you that the call on Line 1 is still on hold (determined by the "call hold reminder timer" parameter), and then the ring splash is heard again after 60 seconds (determined by this parameter). **Notes:** **1.** You must enable the "call hold reminder" and/or "call hold reminder during active calls" parameter(s), and the "call hold reminder timer" parameter, for this parameter to work. **2.** A value of "0" prevents additional rings. For more information on this feature, see "Call Hold Reminder Timer & Frequency" on page 5-102.

PARAMETER IN MITEL WEB UI	PARAMETER IN CONFIGURATION FILES	DESCRIPTION
Call Waiting Tone Period **Note:** This option can be set by an Administrator only.	call waiting tone period	Specifies the time period, in seconds, that the call waiting tone is audible on an active call when another call comes in. When enabled, the call waiting tone plays at regular intervals for the amount of time set for this parameter. For example, if set to “30” the call waiting tone plays every 30 seconds. When set to “0”, the call waiting tone is audible only once on the active call. For more information on this feature, see “Call Waiting Tone Period” on page 5-90.
Preferred Line **Note:** This option can be set by both Users and Administrators.	preferred line	Specifies the preferred line to switch focus back to when incoming or outgoing calls end on the phone. For more information on this feature, see “Preferred Line and Preferred Line Timeout” on page 5-103.
Preferred Line Timeout (seconds) **Note:** This option can be set by both Users and Administrators.	preferred line timeout	Specifies the time, in seconds, that the phone switches back to the preferred line after a call (incoming or outgoing) ends on the phone, or after a duration of inactivity on an active line. For more information on this feature, see “Preferred Line and Preferred Line Timeout” on page 5-103.
Goodbye Key Cancels Incoming Call **Note:** This option can be set by both Users and Administrators.	goodbye key cancels incoming call	Enable or disables the behavior of the Goodbye Key on the IP phone. For more information on this feature, see “Goodbye Key Cancels Incoming Call” on page 5-105.
Message Waiting Indicator Line **Note:** This option can be set by both Users and Administrators.	mwi led line	Allows you to enable the Message Waiting Indicator (MWI) on a single line or on all lines on the phone. For example, if you set this parameter to 3, the LED illuminates if a voicemail is pending on line 3. If you set this parameter to 0, the LED illuminates if a voicemail is pending on any line on the phone. For more information on this feature, see “Message Waiting Indicator Line” on page 5-107.
DND Key Mode **Note:** This option can be set by both Users and Administrators.	dnd key mode	Allows you to configure the DND mode to use on the phone (Account, Phone, Custom) when the DND key is pressed. You can configure DND for all accounts or a specific account. For more information on this feature, see “DND Key Mode” on page 5-109. Also see Chapter 5, the section, “Do Not Disturb (DND)” on page 5-218.

PARAMETER IN MITEL WEB UI	PARAMETER IN CONFIGURATION FILES	DESCRIPTION
Call Forward Key Mode **Note:** This option can be set by both Users and Administrators.	call forward key mode	Allows you to configure the Call Forward mode to use on the phone (Account, Phone, or Custom). You can configure Call Forward for all accounts or a specific account. For more information on this feature, see "Call Forward Mode" on page 5-111. Also see Chapter 5, the section, "Call Forwarding" on page 5-252.
N/A	use lldp elin	Enables or disables the use of an Emergency Location Identification Number (ELIN) received from LLDP as a caller ID for emergency numbers. For more information on this feature, see "Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) and Emergency Location Identification Number (ELIN)" on page 5-113.

INCOMING/OUTGOING INTERCOM CALLS

The Incoming/Outgoing Intercom Call settings on the IP Phone specify whether the IP phone or the server is responsible for notifying the recipient that an Intercom call is being placed. These settings also specify the prefix code for server-side Intercom calls, and specifies the configuration to use when making the Intercom call.

PARAMETER IN MITEL WEB UI	PARAMETER IN CONFIGURATION FILES	DESCRIPTION
INCOMING INTERCOM SETTINGS		
Auto-Answer **Note:** This option can be set by both Users and Administrators.	sip allow auto answer	Enables or disables the IP phone to allow automatic answering for an Intercom call. If auto-answer is enabled on the IP phone, the phone plays a tone to alert the user before answering the intercom call. If auto-answer is disabled, the phone treats the incoming intercom call as a normal call. For more information on this feature, see "Incoming/Outgoing Intercom with Auto-Answer and Barge In" on page 5-117.
Microphone Mute **Note:** This option can be set by both Users and Administrators.	sip intercom mute mic	Enables or disables the microphone on the IP phone for Intercom calls made by the originating caller. For more information on this feature, see "Incoming/Outgoing Intercom with Auto-Answer and Barge In" on page 5-117.

PARAMETER IN MITEL WEB UI	PARAMETER IN CONFIGURATION FILES	DESCRIPTION
Play Warning Tone **Note:** This option can be set by both Users and Administrators.	sip intercom warning tone	Enables or disables a warning tone to play when the phone receives an incoming intercom call on an active line. For more information on this feature, see "Incoming/Outgoing Intercom with Auto-Answer and Barge In" on page 5-117.
Allow Barge In **Note:** This option can be set by both Users and Administrators.	sip intercom allow barge in	Enable or disables how the phone handles incoming intercom calls while the phone is on an active call as well as how the phone handles multicast paging calls while the phone is in a dialing state. For more information on this feature, see "Incoming/Outgoing Intercom with Auto-Answer and Barge In" on page 5-117.
OUTGOING INTERCOM SETTINGS		
Type	sip intercom type	Determines whether the IP phone or the server is responsible for notifying the recipient that an Intercom call is being placed. Applicable settings are Phone-Side, Server-Side, OFF. For more information on this feature, see "Incoming/Outgoing Intercom with Auto-Answer and Barge In" on page 5-117.
Prefix Code	sip intercom prefix code	The prefix to add to the phone number for server-side outgoing Intercom calls. This parameter is required for all server-side Intercom calls. For more information on this feature, see "Incoming/Outgoing Intercom with Auto-Answer and Barge In" on page 5-117.
Line	sip intercom line	Specifies the line for which the IP phone uses the configuration from, when making the Intercom call. The IP phone uses the first available line for physically making the call but uses the configuration from the line you set for this parameter. **Note:** The "*sip intercom type*" parameter must be set with the **Server-Side** option to enable the "*sip intercom line*" parameter. For more information on this feature, see "Incoming/Outgoing Intercom with Auto-Answer and Barge In" on page 5-117.

GROUP PAGING RTP SETTINGS

PARAMETER IN MITEL WEB UI	PARAMETER IN CONFIGURATION FILES	DESCRIPTION
Paging Listen Addresses **Note:** This option can be set by both Users and Administrators.	paging group listening	Allows you to specify up to 5 listening multicast addresses to send/receive a Real Time Transport Protocol (RTP) stream to/from these pre-configured multicast addresses without involving SIP signaling. For more information on this feature, see "Group Paging RTP Settings" on page 5-121.

KEY MAPPING

PARAMETER IN MITEL WEB UI	PARAMETER IN CONFIGURATION FILES	DESCRIPTION
Map Redial Key To	map redial key to	Sets the **Redial** key as a Speeddial key if a value is entered for this parameter. If you leave this parameter blank, the **Redial** key returns to its original functionality. For more information on this feature, see "Speeddial Key Mapping" on page 5-125.
Map Conf Key To	map conf key to	Sets the **Conf** key as a Speeddial key if a value is entered for this parameter. If you leave this parameter blank, the **Conf** key returns to its original functionality. For more information on this feature, see "Speeddial Key Mapping" on page 5-125.
NA	map redial as dtmf	The "Redial" key remappings has the same behavior as the "Speeddial" key when the phone is idle. During an active call the phone will send the custom number as DTMF using the phone configured DTMF method (inbound vs out-of-band RFC2833 vs SIP INFO). When a user presses the **Redial** key, the mapped number will be sent out as DTMF during an active call if the current "**map redial key to**" parameter is configured to a number and the "**map redial as dtmf**" parameter is set to "1". For more information on this feature, see "Speeddial Key Mapping" on page 5-125.

PARAMETER IN MITEL WEB UI	PARAMETER IN CONFIGURATION FILES	DESCRIPTION
NA	Map redial as conf	The “Redial” key remappings has the same behavior as the “Speeddial” key when the phone is idle. During an active call the phone will send the custom number as DTMF using the phone configured DTMF method (inbound vs out-of-band RFC2833 vs SIP INFO). When a user presses the **Conf** key, the mapped number will be sent out as DTMF during an active call if the current “**map conf key to**” parameter is configured to a number and “**map conf as dtmf**” parameter is set to “1”. For more information on this feature, see “Speeddial Key Mapping” on page 5-125.

HTTP DIGEST SETTINGS

PARAMETER IN MITEL WEB UI	PARAMETER IN CONFIGURATION FILES	DESCRIPTION
Set Domain	http digest domain enable	Specifies whether the HTTP Digest Domain is enabled or disabled. For more information on this feature, see “Authentication Support for HTTP/HTTPS Download Methods, used with BroadSoft Client Management System (CMS)” on page 5-355.
Domain ID	http digest domain	Specifies the domain for HTTP/HTTPS digest authentication. For more information on this feature, see “Authentication Support for HTTP/HTTPS Download Methods, used with BroadSoft Client Management System (CMS)” on page 5-355.

RING TONES

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETER IN CONFIGURATION FILES	DESCRIPTION
Tone Set **Note:** This option can be set by both Users and Administrators.	Tone Set	tone set	Globally sets a tone set for a specific country For more information on this feature, see "Ring Tones and Tone Sets" on page 5-127.
Ring Tone **Note:** This option can be set by both Users and Administrators.	Global Ring Tone	ring tone	Globally sets the type of ring tone on the IP phone. Ring tone can be set to one of 15 distinct rings (excluding silence) or a custom ring tone. For more information on this feature, see "Ring Tones and Tone Sets" on page 5-127.
N/A	LineN **Note:** This option can be set by both Users and Administrators.	lineN ring tone	Sets the type of ring tone on the IP phone on a per-line basis. Ring tone can be set to one of 15 distinct rings (excluding silence) or a custom ring tone. For more information on this feature, see "Ring Tones and Tone Sets" on page 5-127.

PRIORITY ALERTING SETTINGS

PARAMETER IN MITEL WEB UI	PARAMETER IN CONFIGURATION FILES	DESCRIPTION
Enable Priority Alerting	priority alerting enabled	Enables and disables distinctive ringing on the IP phone for incoming calls and call-waiting calls. For more information on this feature, see "Priority Alerting" on page 5-145.
Group	alert group	When an "alert-group" keyword appears in the header of the INVITE request, the configured Bellcore ring tone is applied to the IP phone. For more information on this feature, see "Priority Alerting" on page 5-145.

PARAMETER IN MITEL WEB UI	PARAMETER IN CONFIGURATION FILES	DESCRIPTION
External	alert external	When an "alert-external" keyword appears in the header of the INVITE request, the configured Bellcore ring tone is applied to the IP phone. For more information on this feature, see "Priority Alerting" on page 5-145.
Internal	alert internal	When an "alert-internal" keyword appears in the header of the INVITE request, the configured Bellcore ring tone is applied to the IP phone. For more information on this feature, see "Priority Alerting" on page 5-145.
Emergency	alert emergency	When an "alert-emergency" keyword appears in the header of the INVITE request, the configured Bellcore ring tone is applied to the IP phone. For more information on this feature, see "Priority Alerting" on page 5-145.
Priority	alert priority	When an "alert-priority" keyword appears in the header of the INVITE request, the configured Bellcore ring tone is applied to the IP phone. For more information on this feature, see "Priority Alerting" on page 5-145.
Auto Call Distribution	alert auto call distribution	When an "alert-acd" keyword appears in the header of the INVITE request, the configured Bellcore ring tone is applied to the IP phone. For more information on this feature, see "Priority Alerting" on page 5-145.
Community 1 through Community 4	alert community 1 alert community 2 alert community 3 alert community 4	When an "alert-community-#" keyword appears in the header of the INVITE request, the configured Bellcore ring tone is applied to the IP phone. Available Bellcore tones are: • 0 - Normal ringing (default) • 1 - Bellcore-dr2 • 2 - Bellcore-dr3 • 3 - Bellcore-dr4 • 4 - Bellcore-dr5 • 5 - Silent For more information on this feature, see "Priority Alerting" on page 5-145.

DIRECTED CALL PICKUP

PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Directed Call Pickup	directed call pickup	Enables or disables the use of "directed call pickup" feature. For more information on this feature, see “Directed Call Pickup (BLF or XML Call Interception)” on page 5-150.
N/A	enhanced directed call pickup	Enables or disabled the use of the “enhanced directed call pickup” feature. For more information on this feature, see “Two-Stage BLF Key Directed Call Pickup Support” on page 5-156.
Directed Call Pickup Prefix	directed call pickup prefix	Allows you to specify a prefix to use for "directed call pickup" that you can use with a BLF or BLF List softkey. For more information on this feature, see “Directed Call Pickup (BLF or XML Call Interception)” on page 5-150.
Play a Ring Splash	play a ring splash	Enables or disables the playing of a short "ring splash tone" when there is an incoming call on the BLF or BLF/List monitored extension. For more information on this feature, see “Ring Signal Type for BLF and BLF/List” on page 5-197.
N/A	prgkeyN ring splash	Controls the ring splash alert pattern per programmable key. For more information on this feature, see “Ring Signal Type for BLF and BLF/List” on page 5-197.
N/A	softkeyN ring splash	Controls the ring splash alert pattern per softkey. For more information on this feature, see “Ring Signal Type for BLF and BLF/List” on page 5-197.
N/A	topsoftkeyN ring splash	Controls the ring splash alert pattern per top softkey. For more information on this feature, see “Ring Signal Type for BLF and BLF/List” on page 5-197
N/A	expmodX keyN ring splash	Controls the ring splash alert pattern per expansion module key. For more information on this feature, see “Ring Signal Type for BLF and BLF/List” on page 5-197.
N/A	ring splash delay	Indicates the delay (seconds) between rings. For more information on this feature, see “Ring Signal Type for BLF and BLF/List” on page 5-197.

PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
N/A	ring splash volume	Indicates the volume of the ring splash. For more information on this feature, see "Ring Signal Type for BLF and BLF/List" on page 5-197.

AUTO CALL DISTRIBUTION (ACD) SETTINGS

PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Auto Available	acd auto available	Enables or disables the use of the ACD Auto-Available Timer. For more information on this feature, see "Automatic Call Distribution (ACD) (for Sylantro/BroadWorks Servers)" on page 5-213.
Auto Available Timer	acd auto available timer	Specifies the length of time, in seconds, before the IP phone status switches back to "available." For more information on this feature, see "Automatic Call Distribution (ACD) (for Sylantro/BroadWorks Servers)" on page 5-213.

TIME AND DATE

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Time Format **Note:** This option can be set by both Users and Administrators.	Time Format	time format	This parameter changes the time to 12 hour or 24 hour format. Use “0” for the 12 hour format and “1” for the 24 hour format. For more information on this feature, see “Time and Date” on page 5-19.
Date Format **Note:** This option can be set by both Users and Administrators.	Date Format	date format	This parameter allows the user to change the date to various formats. For more information on this feature, see “Time and Date” on page 5-19.
Time Zone **Note:** This option can be set by both Users and Administrators.	N/A	time zone name **Custom Parameters**: • time zone minutes • dst minutes • dst start relative date • dst end relative date • dst start month • dst end month • dst start week • dst end week • dst start day • dst end day • dst start hour • dst end hour	This parameter allows you to set the time zone code or customize the time zone for their area as required. For more information on this feature, see “Time Zone & DST” on page 5-20.
Time Servers **Note:** This option can be set by both Users and Administrators.	NTP Time Servers	time server disabled	This parameter allows you to enable or disable the Network Time Server (NTP) to set the time on the phone. For more information on this feature, see “Time Servers” on page 5-31.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Time Server 1 **Note:** This option can be set by both Users and Administrators.	Time Server 1	time server1	This parameter allows you to set the IP address of Time Server 1 in dotted decimal format. For more information on this feature, see "Time Servers" on page 5-31.
Time Server 2 **Note:** This option can be set by both Users and Administrators.	Time Server 2	time server2	This parameter allows you to set the IP address of Time Server 2 in dotted decimal format. For more information on this feature, see "Time Servers" on page 5-31.
Time Server 3 **Note:** This option can be set by both Users and Administrators.	Time Server 3	time server3	This parameter allows you to set the IP address of Time Server 3 in dotted decimal format. For more information on this feature, see "Time Servers" on page 5-31.

LIVE DIALPAD

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Live Dialpad **Note:** This option can be set by a User via the IP Phone UI and by an Administrator via the IP Phone UI and the configuration files.	N/A	live dialpad	This parameter turns the "Live Dialpad" feature ON or OFF. For more information on this feature, see "Live Dialpad" on page 5-58.

LIVE KEYBOARD

Note: The Live Keyboard setting is only available in the IP Phone UI if a K680i keyboard is attached to the phone.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Live Keyboard **Note:** This option can be set by a User via the IP Phone UI and by an Administrator via the IP Phone UI and the configuration files.	N/A	live keyboard	This parameter turns the "Live Keyboard" feature ON or OFF. For more information on this feature, see "Live Dialpad" on page 5-58.
N/A	N/A	keyboard script	Specifies the URI to be called when an alphabetic key on a K680i keyboard attached to a 6867i or 6869i SIP phone is pressed. If this parameter is not defined or left blank, the phone's native Directory search function will be launched. **Note:** The Live Keyboard feature must be enabled to use this feature. For more information on this feature, see "Live Dialpad" on page 5-58.

LANGUAGE

PARAMETER IN MITEL WEB UI	PARAMETER IN CONFIGURATION FILES	DESCRIPTION
N/A	language	The language you want to display for the IP Phone UI. Valid values are: • 0 (English) is default • 1-4 The values 1-4 are dependent on the "language N" parameter. For example, if "language 1: lang_fr.txt", then "language: 1" would set the IP Phone UI language to French. **Note:** All languages may not be available for selection. The available languages are dependent on the language packs currently loaded to the IP phone. For more information about loading language packs, see "Loading Language Packs" on page 5-62. For more information on specifying a language to use on the IP Phone, see "Specifying the Screen Language to Use" on page 5-64.
Webpage Language **Note:** This option can be set by both Users and Administrators.	web language	The language you want to display for the Mitel Web UI. Valid values are: • 0 (English) is default • 1-4 The values 1-4 are dependent on the "language N" parameter. For example, if "language 1: lang_fr.txt", then "language: 1" would set the webpage language to French. **Note:** All languages may not be available for selection. The available languages are dependent on the language packs currently loaded to the IP phone. For more information about loading language packs, see "Loading Language Packs" on page 5-62.

PARAMETER IN MITEL WEB UI	PARAMETER IN CONFIGURATION FILES	DESCRIPTION
Input Language **Note:** This option can be set by both Users and Administrators.	input language	Allows you to specify the language to use for inputs on the IP Phone. Entering a language value for this parameter allows users to enter text and characters in the IP Phone UI and in XML applications via the keypad on the phone (or for the 6873i, the on-screen keyboard), in the language(s) specified. Valid values are: • English • French • Français • German • Deutsch • Italian • Italiano • Spanish • Español • Portuguese • Português • Russian • Русский • Nordic • Greek (6867i, 6869i, and 6873i only) • ελληνικά (6867i, 6869i, and 6873i only) For more information on this feature, see “Specifying the Input Language to Use” on page 5-67.

PARAMETER IN MITEL WEB UI	PARAMETER IN CONFIGURATION FILES	DESCRIPTION
Language 1 thru 4	language N	The language pack you want to load to the IP phone. Valid values are: • lang_ar.txt (Arabic) • lang_ca.txt (Catalan) • lang_ca_va.txt (Valencian) • lang_cs.txt (Czech - UTF8) • lang_cs_op.txt (Czech - ASCII) • lang_cy.txt (Welsh) • lang_de.txt (German) • lang_da.txt (Danish) • lang_el.txt (Greek - 6867i, 6869i, and 6873i only) • lang_es.txt (Spanish) • lang_es_mx.txt (Mexican Spanish) • lang_eu.txt (Euskera) • lang_fi.txt (Finnish) • lang_fr.txt (French) • lang_fr_ca.txt (Canadian French) • lang_gl.txt (Galego) • lang_hu.txt (Hungarian) • lang_it.txt (Italian) • lang_ko.txt (Korean) • lang_nl.txt (Dutch) • lang_nl_nl.txt (Dutch - Netherlands) • lang_no.txt (Norwegian) • lang_pl.txt (Polish - ASCII) • lang_pl_pl.txt (Polish - UTF8) • lang_pt.txt (Portuguese) • lang_pt_br.txt (Brazilian Portuguese) • lang_ro.txt (Romanian) • lang_ru.txt (Russian) • lang_sk.txt (Slovak - UTF8) • lang_sk_op.txt (Slovak - ASCII) • lang_sv.txt(Swedish) • lang_tr.txt (Turkish) • lang_zh_cn.txt (Simplified Chinese) • lang_zh_tw.txt (Traditional Chinese) **Notes:** **1.** The languages packs you load are dependent on available language packs from the configuration server. **2.** You must reboot the phone to load a language pack. For more information on this feature, see "Loading Language Packs" on page 5-62.

ACCOUNT CONFIGURATION

The IP phones have a DND and CFWD feature that allows an Administrator and User to configure “do not disturb” and “call forwarding” by account. You can set specific modes for the way you want the phone to handle DND and CFWD. The three modes you can set on the phone for these features are:

- Account
- Phone
- Custom

You can set the modes for DND and CFWD in the Mitel Web UI at the path *Basic Settings->Preferences->General*, or using the following parameters in the configurations files:

- dnd key mode
- call forward key mode

The following table describes the behavior of the mode settings for DND and CFWD.

MODES	DND	CFWD
Account	Sets DND for a specific account. A pre-configured DND key toggles the account in focus on the IP Phone UI, to ON or OFF.	Sets CFWD on a per account basis. Pressing a pre-configured CFWD key applies to the account in focus
Phone	Sets DND ON for all accounts on the phone. A pre-configured DND key toggles all accounts on the phone to ON or OFF.	Sets the same CFWD configuration for all accounts (**All**, **Busy**, and/or **No Answer**). When you configure the initial account, the phone applies the configuration to all other accounts. (In the Mitel Web UI, only the account you configured is enabled. All other accounts are grayed out but set to the same configuration.) Using the Mitel Web UI, if you make changes to that initial account, the changes apply to all accounts on the phone.
Custom	Sets the phone to display custom screens after pressing a pre-configured DND key, that list the account(s) on the phone. The user can select a specific account for DND, turn DND ON for all accounts, or turn DND OFF for all accounts	Sets CFWD for a specific account or all accounts. You can configure a specific mode (**All**, **Busy**, and/or **No Answer**) for each account independently or all accounts. On the 6863i and 6865i, you can set all accounts to **ALL On** or **ALL Off**. On the 6867i, 6869i, and 6873i, you can set all accounts to **All On**, **All Off**, or copy the configuration for the account in focus to all other accounts using a **CopytoAll** softkey.

REFERENCES

For more information about account configuration of DND and CFWD on the IP Phones, see Chapter 5, the sections:

For DND:

- "DND Key Mode" on page 5-109.
- "Do Not Disturb (DND)" on page 5-218.

For CFWD:

- "Call Forward Mode" on page 5-111.
- "Call Forwarding" on page 5-252.

CUSTOM RINGTONES

The IP phones support up to eight custom ringtones. Administrators can install ringtones on the phone using the configuration files or the Web UI and users can then simply select a ringtone on the phone to use as their incoming call ringtone.

REFERENCE

For more information about custom ring tones, see "Custom Ring Tones," on page 140.

NETWORK SETTINGS

The following paragraphs describe the network parameters you can configure on the IP phone. Network settings are in two categories:

- Basic network settings
- Advanced network settings

Note: Specific parameters are configurable using the Mitel Web UI only and are indicated where applicable.

NOTIFICATION WHEN INCORRECT NETWORK SETTINGS ENTERED

If an Administrator enters incorrect network settings over the IP Phone UI or the Mitel Web UI, such as:

- A 0.0.0.0 entered as values for the **IP Address**, **Subnet Mask**, and **Gateway** parameters,
- **IP Address** and **Gateway** IP address parameter values entered exactly the same,
- **Gateway** IP address and the **IP address** parameter values configured not on the same subnet,

the UI will immediately notify the Administrator with a specific message that an incorrect value was entered.

BASIC NETWORK SETTINGS

If Dynamic Host Configuration Protocol (DHCP) is enabled, the IP phone automatically configures all of the Network settings. If the phone cannot populate the Network settings, or if DHCP is disabled, you can set the Network options manually.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
DHCP	DHCP	dhcp	Enables or disables DHCP. Enabling DHCP populates the required network information. The DHCP server serves the network information that the IP phone requires. If the IP phone is unable to get any required information, then you must enter it manually. DHCP populates the following network information: IP Address, Subnet Mask, Gateway, Domain Name System (DNS) servers, TFTP, HTTP HTTPS, and FTP servers, and Timer servers. **Note:** For DHCP to automatically populate the IP address or qualified domain name for the TFTP server, your DHCP server must support Option 66. The IP phones also support Option 60 and 43. For more information, see "DHCP" on page 4-4.
IP Address	IP Address	ip	IP address of the IP phone. To assign a static IP address, disable DHCP. For more information, see "Configuring Network Settings Manually" on page 4-24.
IPv6 Address	IPv6	ip6	IPv6 address of the IP phone. For more information, see "IPv6 Support on 6800 and 6900 Series SIP Phones" on page 4-114.
Subnet Mask	Subnet Mask	subnet mask	Subnet mask defines the IP address range local to the IP phone. To assign a static subnet mask, disable DHCP. For more information, see "Configuring Network Settings Manually" on page 4-24.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Gateway	Gateway	default gateway	The IP address of the network's gateway or default router IP address. To assign a static Gateway IP address, disable DHCP. For more information, see "Configuring Network Settings Manually" on page 4-24.
Primary DNS	Primary DNS	dns1	Primary DNS server IP address. For any of the IP address settings on the IP phone a domain name value can be entered instead of an IP address. With the help of the DNS servers the domain names for such parameters can then be resolved to their corresponding IP addresses. To assign static DNS addresses, disable DHCP. **Note:** If a host name is configured on the IP phone, you must also set a DNS. For more information, see "Configuring Network Settings Manually" on page 4-24.
Secondary DNS	Secondary DNS	dns2	A service that translates domain names into IP addresses. To assign static DNS addresses, disable DHCP. For more information, see "Configuring Network Settings Manually" on page 4-24.
Hostname	Hostname	hostname	Specifies the hostname DHCP Option 12 that the phone sends with the DHCP Request packet. For more information, see "Using Option 12 Hostname on the IP Phone" on page 4-13.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Ethernet	N/A		The send (TX) and receive (RX) negotiation to use on the Ethernet LAN Port and Ethernet PC Port for transmitting and receiving data over the LAN or to/from your PC, respectively as well as to enable or disable port mirroring.
LAN Port Link	LAN Port	ethernet port 0	
PC Port Link	PC Port	ethernet port 1	
PC Port Enabled (6863i and 6865i)	PC Port PassThru Enable/Disable (6863i and 6865i)	pc port passthrough enabled	For more information on Ethernet ports, see “Ethernet” on page 4-27.
Port Mirroring	N/A	ethernet port mirroring	
Enable PassThru Port (6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970)	PC Port PassThru Enable/Disable (6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970)		

ADVANCED NETWORK SETTINGS

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
DHCP User Class	N/A	dhcp userclass	Specifies the User Class DHCP Option 77 that the phone sends to the configuration server with the DHCP Request packet. **Note:** If you specify a value for this parameter, you must restart your phone for the change to take affect. Any change in its value during start-up results in an automatic reboot. For more information, see "Using Option 77 User Class on the IP Phone" on page 4-16.
Download Options	DHCP Download Options	dhcp config option override	The value specified for this parameter overrides the precedence order for determining a configuration server. Valid values are: • -1 (Disabled - ignores all DHCP configuration options). • 0 (Any) • 43 • 66 • 159 • 160 **Notes:** **1.** If the DHCP server supplies Options 159 and 160, the phones will attempt to contact the configuration server given in these options. **2.** You must restart the IP Phone for this parameter to take affect. For more information, see "Using Options 159 and 160 on the IP Phone" on page 4-17. For more information about setting DHCP download preference, see "Configuration Server Download Precedence" on page 4-20.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
LLDP Support	LLDP	lldp	Enables or disables Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) on the IP Phone. For more information on this feature, see "Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) and Emergency Location Identification Number (ELIN)" on page 5-113.
N/A	LLDP Packet Interval	lldp interval	The amount of time, in seconds, between the transmission of LLDP Data Unit (LLDPDU) packets. The value of zero (0) disables this parameter. For more information on this feature, see "Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) and Emergency Location Identification Number (ELIN)" on page 5-113.
N/A	Rport (RFC 3581)	sip rport	Allows you to enable (1) or disable (0) the use of Rport on the IP phone. "Rport" in RFC 3581, allows a client to request that the server send the response back to the source IP address **and** the port from which the request came. For more information, see Chapter 4, "RPORT" on page 4-58.

HTTPS SETTINGS

Advanced Network Settings includes HTTPS settings for the IP Phones.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
HTTPS	HTTPS Server - Redirect HTTP to HTTPS	https redirect http get	Allows or disallows redirection from the HTTP server to the HTTPS server. For more information, see Chapter 4, "HTTPS Client/Server Configuration" on page 4-36.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
XML HTTP POSTs	HTTPS Server - Block XML HTTP POSTs	https block http post xml	Enables or disables the blocking of XML scripts from HTTP POSTs. Some client applications use HTTP POSTs to transfer XML scripts. The phones's HTTP server accepts these POSTs even if server redirection is enabled, effectively bypassing the secure connection. When this parameter is enabled (blocking is enabled), receipt of an HTTP POST containing an XML parameter header results in the following response: "403 Forbidden". This forces the client to direct the POSTs to the HTTPS server through use of the "https://" URL. For more information, see Chapter 4, "HTTPS Client/Server Configuration" on page 4-36.
Client Method	HTTPS Client Method	https client method	Defines the security method that the client advertises to the server during the Secure Socket Layer (SSL) handshake. Available options are: • **TLS 1.0** - The phone will attempt to communicate using TLS 1.0 only. • **TLS 1.1** - The phone will attempt to communicate using TLS 1.1 only. • **TLS 1.2** - The phone will attempt to communicate using TLS 1.2 only. • **TLS Preferred** - The phone will negotiate with the highest possible TLS version during the handshake. **Note:** This implementation has changed, see Chapter 4, "HTTPS Client/Server Configuration" on page 4-36.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Cert Validation	Validate Certificates	https validate certificates	Enables or disables the HTTPS validation of certificates on the phone. When this parameter is set to 1, the HTTPS client performs validation on SSL certificates before accepting them. **Notes:** **1.** If you are using HTTPS and the certificates are not valid or are not signed by the certificate vendors listed in Appendix F, "Certificates Supported in This Software Release" the phones fail to download configuration files. **2.** Defining this parameter as "0" (disabled) significantly reduces security for the provisioning process to encryption only. Validation of the chain-of-trust (i.e. the originator of the files) will not be performed if this feature is disabled. Therefore, disabling HTTPS validation of certificates is only recommended for troubleshooting purposes or when self-signed certificates are in use. For more information, see Chapter 4, "HTTPS Server Certificate Validation" on page 4-41.
Check Hostnames	Check Certificate Hostnames	https validate hostname	Enables or disables the HTTPS validation of hostnames on the phone. For more information, see Chapter 4, "HTTPS Server Certificate Validation" on page 4-41.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
N/A	Trusted Certificates Filename	https user certificates	Specifies a file name for a .PEM file located on the configuration server. This file contains the User-provided certificates in PEM format. These certificates are used to validate peer certificates. **Note:** To install a user-provided certificate through a configuration server using the HTTPS protocol, you must temporarily disable the "**https validate certificates**". After the certificate is installed and you can re-enable the "**https validate certificates**" parameter. For more information, see Chapter 4, "HTTPS Server Certificate Validation" on page 4-41.

TYPE OF SERVICE (TOS), DSCP

Advanced Network Settings include Type of Service (ToS) and Differentiated Services Code Point (DSCP) for the IP phones.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Type of Service SIP	SIP	tos sip	The Differentiated Services Code Point (DSCP) for SIP packets. For more information, see Chapter 4, "Type of Service (ToS), Quality of Service (QoS), and DiffServ QoS" on page 4-47.
Type of Service RTP	RTP	tos rtp	The Differentiated Services Code Point (DSCP) for RTP packets. For more information, see Chapter 4, "Type of Service (ToS), Quality of Service (QoS), and DiffServ QoS" on page 4-47.
Type of Service RTCP	RTCP	tos rtcp	The Differentiated Services Code Point (DSCP) for RTCP packets. For more information, see Chapter 4, "Type of Service (ToS), Quality of Service (QoS), and DiffServ QoS" on page 4-47.

VLAN

You can enable or disable VLAN and set specific VLAN IDs and priorities under Network Settings.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
GLOBAL SETTINGS			
VLAN Enable	VLAN Enable	tagging enabled	Enables or disables VLAN on the IP phones. For more information, see Chapter 4, "Virtual LAN (optional)" on page 4-46.
Other Priority	Priority, Non-IP Packet	priority non-ip	Specifies the priority value for non-IP packets. For more information, see Chapter 4, "Virtual LAN (optional)" on page 4-46.
LAN PORT SETTINGS (PORT 0)			
Phone VLAN ID	VLAN ID	vlan id	Allows you to configure a VLAN ID that associates with the physical Ethernet Port 0 (LAN port). For more information, see Chapter 4, "Virtual LAN (optional)" on page 4-46.
SIP Priority RTP Priority RTCP Priority	SIP Priority RTP Priority RTCP Priority	tos priority map	This parameter is based on the Type of Service (ToS), Differentiated Services Code Point (DSCP) setting for SIP (tos sip parameter), RTP (tos rtp parameter) and RTCP (tos rtcp parameter). It is the mapping between the DSCP value and the VLAN priority value for SIP, RTP, and RTCP packets. You enter the tos priority map value as follows: (DSCP_1,Priority_1)(DSCP_2,Priority_2).. ...(DSCP_64,Priority_64) where the DSCP value range is 0-63 and the priority range is 0-7. Mappings not enclosed in parentheses and separated with a comma, or with values outside the ranges, are ignored. For more information, see Chapter 4, "Virtual LAN (optional)" on page 4-46.
PC PORT SETTINGS (PORT 1)			

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
PC Port VLAN ID	VLAN ID	vlan id port 1	Allows you to configure a VLAN ID that associates with the physical Ethernet Port 1 (PC port). For more information, see Chapter 4, "Virtual LAN (optional)" on page 4-46.
PC Port Priority	Priority	qos eth port 1 priority	Specifies the priority value used for passing VLAN packets through to a PC via Port 1. For more information, see Chapter 4, "Virtual LAN (optional)" on page 4-46.

SIP SETTINGS

The following paragraphs describe the SIP parameters you can configure on the IP phone. SIP configuration consists of configuring:

- Basic SIP Authentication Settings
- Basic SIP Network Settings
- Advanced SIP settings
- RTP Settings
- Autodial Settings

Notes:

1. Specific parameters are configurable on a global and per-line basis. You can also configure specific parameters using the IP Phone UI, the Mitel Web UI, or the configuration files. If you have a proxy server or have a SIP registrar present at a different location than the PBX server, the SIP parameters may need to be changed.
2. Global SIP settings are applicable only to Lines 1 and 2 for the 6800/6900 series SIP phones. 6900 series phone have pre-configured Line 1 and Line 2 softkeys. To configure lines that do not have an associated Line hard key, Administrators must configure each individual line manually.
3. The IP phones allow you to define different SIP lines with the same account information (i.e. same user name) but with different registrar and proxy IP addresses. This feature works with Registration, Subscription, and Notify processing. This feature also works with the following types of calls: incoming, outgoing, BroadSoft Shared Call Appearance (SCA), Bridged Line Appearance (BLA), conference, transfer, blind transfer.

Basic SIP Authentication Settings

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Screen Name	Screen Name (Global and Per-Line)	sip screen name (global) sip lineN screen name (per-line)	Name that displays on the idle screen. Valid values are up to 20 alphanumeric characters. For more information, see Chapter 4, "Basic SIP Settings" on page 4-62.
N/A	Screen Name 2 (Global and Per-Line)	sip screen name 2 (global) sip lineN screen name 2 (per-line)	Custom text message that displays on the idle screen. Valid values are up to 20 alphanumeric characters. For more information, see Chapter 4, "Basic SIP Settings" on page 4-62.
User Name	Phone Number (Global and Per-Line)	sip user name (global) sip lineN user name (per-line)	User name used in the name field of the SIP URI for the IP phone and for registering the phone at the registrar. Valid values are up to 20 alphanumeric characters. For more information, see Chapter 4, "Basic SIP Settings" on page 4-62.
Display Name	Caller ID (Global and Per-Line)	sip display name (global) sip lineN display name (per-line)	Name used in the display name field of the "From SIP" header field. Some IP PBX systems use this as the caller's ID, and some may overwrite this with the string that is set at the PBX system. Valid values are up to 20 alphanumeric characters. For more information, see Chapter 4, "Basic SIP Settings" on page 4-62.
Auth Name	Authentication Name (Global and Per-Line)	sip auth name (global) sip lineN auth name (per-line)	Authorization name used in the username field of the Authorization header field of the SIP REGISTER request. Valid values are up to 20 alphanumeric characters. For more information, see Chapter 4, "Basic SIP Settings" on page 4-62.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Password	Password (Global and Per-Line)	sip password (global) sip lineN password (per-line)	Password used to register the IP phone with the SIP proxy**.** Valid values are up to 20 alphanumeric characters. Passwords are encrypted and display as asterisks when entering. **Note:** The "mask sip password" parameter can be used to mask a user's SIP account password in the server.cfg and local.cfg files (downloaded from the IP phone's Web UI troubleshooting page for debug purposes). For more information, see Chapter 4, "Basic SIP Settings" on page 4-62.
N/A	BLA Number (Global and Per-Line)	sip bla number (global) sip lineN bla number (per-line)	Phone number that you assign to BLA lines that is shared across all phones (global configuration) or shared on a per-line basis (per-line configuration). For more information, see Chapter 4, "Basic SIP Settings" on page 4-62. For more information about BLA, see Chapter 5, the section, "Bridged Line Appearance (BLA)" on page 5-228.
N/A	Line Mode (Global and Per-Line)	sip mode (global) sip lineN mode (per-line)	The mode-type that you assign to the IP phone. Valid values are Generic (0), BroadSoft SCA (1), Reserved for (2), or BLA (3). Default is Generic (0). For more information, see Chapter 4, "Basic SIP Settings" on page 4-62.
N/A	Call Waiting	call waiting	Enable or disables Call Waiting on the IP Phone. For more information on this feature, see. "Call Waiting" on page 5-87.

Basic SIP Network Settings

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Proxy Server	Proxy Server (Global and Per-Line)	sip proxy ip (global) sip lineN proxy ip (per-line)	IP address of the SIP proxy server. Up to 64 alphanumeric characters. For more information, see Chapter 4, "Basic SIP Settings" on page 4-62.
Proxy Port	Proxy Port (Global and Per-Line)	sip proxy port (global) sip lineN proxy port (per-line)	SIP proxy server's port number. Default is 0. For more information, see Chapter 4, "Basic SIP Settings" on page 4-62.
N/A	Backup Proxy Server (Global and Per-Line)	sip backup proxy ip (global) sip lineN backup proxy ip (per-line)	The IP address of the backup SIP proxy server for which the IP phone uses when the primary SIP proxy is unavailable. For more information, see Chapter 4, "Basic SIP Settings" on page 4-62.
N/A	Backup Proxy Port (Global and Per-Line)	sip backup proxy port (global) sip lineN backup proxy port (per-line)	The port number of the backup SIP proxy server for which the IP phone uses when the primary SIP proxy port is unavailable. For more information, see Chapter 4, "Basic SIP Settings" on page 4-62.
N/A	Outbound Proxy Server (Global and Per-Line)	sip outbound proxy (global) sip lineN outbound proxy (per-line)	Address of the outbound proxy server. All SIP messages originating from the phone are sent to this server. For example, if you have a Session Border Controller in your network, then you would normally set its address here. Default is 0.0.0.0. For more information, see Chapter 4, "Basic SIP Settings" on page 4-62.
N/A	Outbound Proxy Port (Global and Per-Line)	sip outbound proxy port (global) sip lineN outbound proxy port (per-line)	The proxy port on the proxy server to which the IP phone sends all SIP messages. Default is 0. For more information, see Chapter 4, "Basic SIP Settings" on page 4-62.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
N/A	Backup Outbound Proxy Server (Global and Per-Line)	sip backup outbound proxy (global) sip lineN backup outbound proxy (per-line)	The IP address or domain name of the backup outbound SIP proxy server for which the IP phone uses when the primary SIP proxy is unavailable. For more information, see Chapter 4, "Backup Outbound Proxy and Failover Support" on page 4-67.
N/A	Backup Outbound Proxy Port (Global and Per-Line)	sip backup outbound proxy port (global) sip lineN backup outbound proxy port (per-line)	The backup outbound proxy port on the backup outbound proxy server to which the IP phone sends all SIP messages. For more information, see Chapter 4, "Backup Outbound Proxy and Failover Support" on page 4-67.
Registrar Server	Registrar Server (Global and Per-Line)	sip registrar ip (global) sip lineN registrar ip (per-line)	IP address of the SIP registrar. Up to 64 alphanumeric characters. Enables or disables the phone to be registered with the Registrar. When Register is disabled globally, the phone is still active and you can dial using username and IP address of the phone. A message "No Service" displays on the idle screen and the LED is steady ON. If Register is disabled for a single line, no messages display and LEDs are OFF. For more information, see Chapter 4, "Basic SIP Settings" on page 4-62.
Registrar Port	Registrar Port (Global and Per-Line)	sip registrar port (global) sip lineN registrar port (per-line)	SIP registrar's port number. Default is 0. For more information, see Chapter 4, "Basic SIP Settings" on page 4-62.
N/A	Backup Registrar Server (Global and Per-Line)	sip backup registrar ip (global) sip lineN backup registrar ip (per-line)	The address of the backup registrar (typically, the backup SIP proxy) for which the IP phone uses to send *REGISTER* requests if the primary registrar is unavailable. For more information, see Chapter 4, "Basic SIP Settings" on page 4-62.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
N/A	Backup Registrar Port (Global and Per-Line)	sip backup registrar port (global) sip lineN backup registrar port	The backup registrar's (typically the backup SIP proxy) port number. For more information, see Chapter 4, "Basic SIP Settings" on page 4-62.
N/A	Registration Period (Global and Per-Line)	sip registration period (global) sip lineN registration period (per-line)	The requested registration period, in seconds, from the registrar. For more information, see Chapter 4, "Basic SIP Settings" on page 4-62.
N/A	Conference Server URI (Global and Per-Line)	sip centralized conf (global) sip lineN centralized conf (per-line)	Globally enables or disables SIP centralized conferencing for an IP phone. For more information, see Chapter 4, "Centralized Conferencing (for Sylantro and BroadSoft Servers)" on page 5-349.

Advanced SIP Settings

In addition to the basic SIP settings, you can also configure the following advanced SIP parameters. These parameters may be configurable via the Mitel Web UI and/or the configuration files.

PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Explicit MWI Subscription	sip explicit mwi subscription	If the IP phone has a message waiting subscription with the Service Provider, a Message Waiting Indicator (MWI) (LED or display icon) tells the user there is a message on the IP Phone. You can enable and disable MWI by setting this parameter to 0 (disable) or 1 (enable) in the configuration files or by checking the box for this field in the Mitel Web UI. Default is disabled. For more information, see Chapter 4, "Advanced SIP Settings (optional)" on page 4-80.

PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Explicit MWI Subscription Period	sip explicit mwi subscription period	The requested duration, in seconds, before the MWI subscription times out. The phone re-subscribes to MWI before the subscription period ends. For more information, see Chapter 4, "Advanced SIP Settings (optional)" on page 4-80.
AS-Feature-Event Subscription (Global and Per-Line)	sip as-feature-event subscription (global) sip lineN as-feature-event subscription (per-line)	Enables or disables the specified line with the BroadSoft's server-side DND, CFWD, or ACD features. For more information about this parameter, see Chapter 6, the section, "As-Feature-Event Subscription" on page 6-15.
AS-Feature-Event Subscription Period	sip as-feature-event subscription period	Specifies the amount of time, in seconds, between re-subscribing. If the phone does not re-subscribe in the time specified for this parameter, it loses subscription. For more information about this parameter, see Chapter 6, the section, "As-Feature-Event Subscription" on page 6-15.
Send MAC Address in REGISTER Message	sip send mac	Adds an "Aastra-Mac:" header to the SIP REGISTER messages sent from the phone to the call server, where the value is the MAC address of the phone. For more information about this parameter, see Chapter 6, the section, "TR-069 Support" on page 6-8.
Send Line Number in REGISTER Message	sip send line	Adds an "Aastra-Line:" header to the SIP REGISTER messages sent from the phone to the call server, where the value is the line number that is being registered. For more information about this parameter, see Chapter 6, the section, "TR-069 Support" on page 6-8.
Session Timer	sip session timer	The time, in seconds, that the IP phone uses to send periodic re-*INVITE* requests to keep a session alive. The proxy uses these re-*INVITE* requests to maintain the status' of the connected sessions. See RFC4028 for details. Default is 0. For more information, see Chapter 4, "Advanced SIP Settings (optional)" on page 4-80.

PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Timer 1 and Timer 2	sip T1 timer sip T2 timer	These timers are SIP transaction layer timers defined in RFC 3261. Timer 1 is an estimate, in milliseconds, of the round-trip time (RTT). Timer 2 represents the amount of time, in milliseconds, a non-INVITE server transaction takes to respond to a request. For more information, see Chapter 4, "Advanced SIP Settings (optional)" on page 4-80.
Transaction Timer	sip transaction timer	The amount of time, in milliseconds that the phone allows the call server (registrar/proxy) to respond to SIP messages that it sends. If the phone does not receive a response in the amount of time designated for this parameter, the phone assumes the message has timed out. For more information, see Chapter 4, "Advanced SIP Settings (optional)" on page 4-80.
Transport Protocol	sip transport protocol	The protocol that the IP phone uses to send out SIP messages. **Notes:** **1.** If you set the value of this parameter to 4 (TLS), the phone checks to see if the "sips persistent tls" is enabled. If it is enabled, the phone uses Persistent TLS on the connection. If "sips persistent tls" is disabled, then the phone uses TLS on the connection. If TLS is used, you must specify the Root and Intermediate Certificates, the Local Certificate, the Private Key, and the Trusted Certificates. **2.** If the phone uses Persistent TLS, you MUST specify the Trusted Certificates; the Root and Intermediate Certificates, the Local Certificate, and the Private Key are optional. For more information, see Chapter 4, "Advanced SIP Settings (optional)" on page 4-80.

PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Local SIP UDP/TCP Port	sip local port	Specifies the local source port (UDP/TCP) from which the phone sends SIP messages. **Notes:** **1.** It is recommended that you avoid the conflict RTP port range in case of a UDP transport. **2.** By default, the IP phones use symmetric UDP signaling for outgoing UDP SIP messages. When symmetric UDP is enabled, the IP phone generates and listens for UDP messages using port 5060.If symmetric UDP signaling is disabled, the phone sends from random ports but it listens on the configured SIP local port. For more information, see Chapter 4, "SIP and TLS Source Ports" on page 4-34.
Local SIP TLS Port	sip local tls port	Specifies the local source port (SIPS/TLS) from which the phone sends SIP messages. **Notes:** **1.** It is recommended that you avoid the conflict with any TCP ports being used. For example: WebUI HTTP server on 80/tcp and HTTPS on 443/tcp. **2.** By default, the IP phones use symmetric TLS signaling for outgoing TLS SIP messages. When symmetric TLS is enabled, the IP phone uses port 5061 as the persistent TLS connection source port. When symmetric TLS signaling is disabled, the IP phone chooses a random persistent TLS connection source port for TLS messages from the TCP range (i.e. 49152...65535) after each reboot regardless of whether the parameter "sip outbound support" is enabled or disabled. For more information, see Chapter 4, "SIP and TLS Source Ports" on page 4-34.
Registration Failed Retry Timer	sip registration retry timer	Specifies the time, in seconds, that the phone waits between registration attempts when a registration is rejected by the registrar. For more information, see Chapter 4, "Advanced SIP Settings (optional)" on page 4-80.

PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Registration Timeout Retry Timer	sip registration timeout retry timer	Specifies the length of time, in seconds, that the phone waits until it re-attempts to register after a REGISTER message times out. If this parameter is set lower than 30 seconds, the phone uses a minimum timer of 30 seconds. For more information, see Chapter 4, "Advanced SIP Settings (optional)" on page 4-80.
Registration Renewal Timer	sip registration renewal timer	The threshold value, in seconds, prior to expiration, that the phone renews registrations. The phone will automatically send registration renewals half-way through the registration period, unless half-way is more than the threshold value. For example, if the threshold value is set to 60 seconds and if the registration period is 600 seconds, the renewal REGISTER message will be sent 60 seconds prior to the expiration, as half-way (600/2) > 60. If the registration period was 100 seconds, then the renewal would be sent at the half-way point as (100/2) < 60. For more information, see Chapter 4, "Advanced SIP Settings (optional)" on page 4-80.
N/A	sip subscription timeout retry timer	Applicable for all event packages, this parameter controls how long the phone delays then retries a subscription when a SUBSCRIBE request is responded with a 408 (timeout) or 503 (service unavailable) error code. For more information, see Chapter 4, "Advanced SIP Settings (optional)" on page 4-80.
N/A	sip subscription failed retry timer	Applicable for all event packages, this parameter controls how long the phone delays then retries a subscription when a SUBSCRIBE request is responded with error codes other than 408 (timeout) or 503 (service unavailable). For more information, see Chapter 4, "Advanced SIP Settings (optional)" on page 4-80.

PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
BLF Subscription Period	sip blf subscription period	The requested duration, in seconds, before the BLF subscription times out. The phone re-subscribes to the BLF subscription service before the defined subscription period ends. **Note:** This parameter is N/A to BLF/List subscriptions. For more information, see Chapter 4, "Advanced SIP Settings (optional)" on page 4-80.
ACD Subscription Period	sip acd subscription period	Specifies the time period, in seconds, that the IP phone re-subscribes the Automatic Call Distribution (ACD) subscription service after a software/firmware upgrade or after a reboot of the IP phone. For more information, see Chapter 4, "Advanced SIP Settings (optional)" on page 4-80.
BLA Subscription Period	sip bla subscription period	Specifies the amount of time, in seconds, that the phone waits to receive a BLA subscribe message from the server. If you specify zero (0), the phone uses the value specified for the BLA expiration in the subscribe message received from the server. If no value is specified, the phone uses the default value of 300 seconds. For more information, see Chapter 4, "Advanced SIP Settings (optional)" on page 4-80.
Blacklist Duration	sip blacklist duration	Specifies the length of time, in seconds, that a failed server remains on the server blacklist. The IP phone avoids sending a SIP message to a failed server (if another server is available) for this amount of time. For more information about Blacklist Duration, see Chapter 6, the section, "Blacklist Duration" on page 6-17.

PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Whitelist Proxy	sip whitelist	This parameter enables/disables the whitelist proxy feature, as follows: • Set to 0 to disable the feature. • Set to 1 to enable the feature. When this feature is enabled, an IP phone accepts call requests from a trusted proxy server *only*. The IP phone rejects any call requests from an untrusted proxy server. For more information about Whitelist Proxy see Chapter 6, the section, "Whitelist Proxy" on page 6-19.
XML SIP Notify	sip xml notify event	Enables or disables the phone to accept or reject an aastra-xml SIP NOTIFY message. **Note:** To ensure the SIP NOTIFY is coming from a trusted source, it is recommended that you enable the Whitelist feature (**Whitelist Proxy** parameter) on the IP phone. If enabled, and the phone receives a SIP NOTIFY from a server that is NOT on the whitelist (i.e. untrusted server), the phone rejects the message. For more information about XML SIP Notify see Chapter 6, the section, "XML SIP Notify Events" on page 5-338.

RTP Settings

You can configure the following RTP settings.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
RTP Port Base	RTP Port	sip rtp port	The RTP port is used for sending DTMF tones and for the audio stream. Your network administrator may close some ports for security reasons. You may want to use this parameter to send RTP data using a different port. Default is 3000. The SIP RTP port is used to send audio streams; port 5012 is used to record the streams. For more information, see Chapter 4, "Real-time Transport Protocol (RTP) Settings" on page 4-87.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
N/A	Force RFC2833 Out of Band DTMF	sip out-of-band dtmf	Enables or disables out-of-band DTMF. Enabling this parameter forces the IP phone to use out-of-band DTMF according to RFC2833. Valid values are 0 (disabled) and 1 (enabled). Default is 1 (enabled). For more information, see Chapter 4, "Real-time Transport Protocol (RTP) Settings" on page 4-87.
N/A	DTMF Method (Global and Per-Line)	sip dtmf method (global) sip lineN dtmf method (per-line)	Sets the dual-tone multi-frequency (DTMF) method to use on the IP phone on a global or per-line basis. Valid values are 0 (RTP), 1 (SIP INFO), or 2 (BOTH). Default is 0 (RTP). For more information, see Chapter 4, "Real-time Transport Protocol (RTP) Settings" on page 4-87.
N/A	RTP Encryption (Global and Per-Line)	sip srtp mode (global) sip lineN srtp mode (per-line)	This parameter determines if SRTP is enabled on this IP phone, as follows: **3.** If set to 0, then disable SRTP. **4.** If set to 1 then SRTP calls are preferred. **5.** If set to 2, then SRTP calls only are generated/accepted. For more information, see Chapter 4, "Real-time Transport Protocol (RTP) Settings" on page 4-87.

Codec Preference List

You can configure the following codec preference list settings.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
N/A	Basic Codecs (G.711 u-Law, G.711 a-Law, G.729)	sip use basic codecs	Enables or disables basic codecs. Enabling this parameter allows the IP phone to use the basic Codecs when sending/receiving RTP packets. Valid values are 0 (disabled) and 1 (enabled). Default is 0 (disabled). For more information, see Chapter 4, "Real-time Transport Protocol (RTP) Settings" on page 4-87.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
N/A	Customized Codec Preference List	sip customized codec	Specifies a customized Codec preference list which allows you to use the preferred Codecs for this IP phone. For more information, see Chapter 4, "Real-time Transport Protocol (RTP) Settings" on page 4-87.
N/A	Packetization Interval	"sip customized codec" attribute	Packetization interval (ptime) is a measurement of the duration of PCM data within each RTP packet sent to the destination, and hence defines how much network bandwidth is used for transfer of the RTP stream. Enter the ptime values for the customized Codec list in milliseconds. For more information, see Chapter 4, "Real-time Transport Protocol (RTP) Settings" on page 4-87.
N/A	Silence Suppression	sip silence suppression	Silence suppression is enabled by default on the IP phones. The phone negotiates whether or not to use silence suppression. Disabling this feature forces the phone to ignore any negotiated value. For more information, see Chapter 4, "Real-time Transport Protocol (RTP) Settings" on page 4-87.

Autodial Settings

You can configure the following Autodial settings.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
N/A	Autodial Number (Global and Per-Line)	sip autodial number sip lineN autodial number	Globally or on a per-line basis, specifies the SIP phone number that the IP phone autodials when the handset is lifted from the phone cradle. An empty (blank) value disables autodial on the phone. For more information, see Chapter 4, "Autodial Settings" on page 4-101.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
N/A	Autodial Timeout (Global and Per-Line)	sip autodial timeout sip lineN autodial timeout	Globally or on a per-line basis, specifies the time, in seconds, that the phone waits to dial a pre-configured number after the handset is lifted from the IP phone cradle. If this parameter is set to 0 (hotline), the phone immediately dials a pre-configured number when you lift the handset. If this parameter is set to a value greater than 0, the phone waits the specified number of seconds before dialing the pre-configured number (warmline) when you lift the handset. Default is 0 (hotline). For more information, see Chapter 4, "Autodial Settings" on page 4-101.
N/A	Use Global Settings (Per-line configurations only)	N/A	For each line, this parameter specifies to use the global autodial settings of "Autodial Number" and "Autodial Timeout". For more information, see Chapter 4, "Autodial Settings" on page 4-101.

LINE SETTINGS

An administrator can configure multiple lines on the IP phone with the same SIP network configuration (global) or a different SIP network configuration (per-line). The following table provides the number of lines available for each IP phone model.

IP PHONE MODEL	AVAILABLE LINES
6863i	2
6865i	24
6867i	24
6869i	24
6873i	24
6905	2
6910	24
6920	24
6930	24
6940	24
6970	24

On the IP Phones, you can configure the following on a per-line basis using the configuration files or the Mitel Web UI:

- **Basic SIP Authentication Settings**
- **Basic SIP Network Settings**
- **RTP Settings** (DTMF Method and RTP Encryption only)
- **Autodial Settings** (On a per-line basis, you can also enable/disable the "**Use Global Settings**" parameter).
- **Additional Settings** (Missed Calls only [i.e. configure missed calls indicator applicability for specific lines]).

REFERENCES

For more information about configuring the features listed above on a per-line basis, see the sections:

- "Basic SIP Settings" on page 4-62
- "Advanced SIP Settings (optional)" on page 4-80
- "Real-time Transport Protocol (RTP) Settings" on page 4-87
- "Autodial Settings" on page 4-101
- "Missed Calls Indicator" on page 284

SOFTKEYS, PROGRAMMABLE KEYS, EXPANSION MODULE KEYS

A user or administrator can assign specific functions to softkeys, programmable keys, or expansion module keys. The available keys for configuration depend on the IP phone model as shown in the following table.

IP PHONE MODEL	SOFTKEYS	EXPANSION MODULE KEYS	PROGRAMMABLE KEYS
6863i	-	N/A	3
6865i	-	16 to 48* (Model M680i) 84 to 252** (Model (M685i)	8
6867i	6 top (maximum of 20 functions) 4 bottom (maximum of 18 functions)	16 to 48* (Model M680i) 84 to 252** (Model (M685i)	-
6869i	12 top (maximum of 44 functions) 5 bottom (maximum of 24 functions)	16 to 48* (Model M680i) 84 to 252** (Model (M685i)	-
6873i	12 top (maximum of 48 functions) 6 bottom (maximum of 30 functions)	16 to 48* (Model M680i) 84 to 252** (Model (M685i)	-
6905	-	N/A	3
6910	-	N/A	8
6920	6 top (maximum of 20 functions) 4 bottom (maximum of 18 functions)	84 to 252*** (Model M695)	-
6930	12 top (maximum of 44 functions) 5 bottom (maximum of 24 functions)	84 to 252*** (Model M695)	-
6940	12 top (maximum of 48 functions) 6 bottom (maximum of 30 functions)	84 to 252*** (Model M695)	-
6970	12 top (maximum of 48 functions) 6 bottom (maximum of 30 functions)	N/A****	

Notes:

1. *The M680i expansion module consists of 16 softkeys. You can have up to 3 expansion modules on an IP phone totaling 48 softkeys. Valid for 6865i, 6867i, 6869i, and 6873i phones.
2. **The M685i expansion module consists of 3 pages of 28 softkeys (for a total of 84). You can have up to 3 expansion modules on an IP phone totaling 252 softkeys. Valid for 6865i, 6867i, 6869i, and 6873i phones.
3. ***The M695 expansion module consists of 3 pages of 28 softkeys (for a total of 84). You can have up to 3 expansion modules on an IP phone totaling 252 softkeys. Valid for 6920, 6930, and 6940 phones.
4. ****The 6970 IP Phone does not support an expansion module.

The softkey, programmable key, or expansion module key can be set to use a specific function. Available functions depend on the IP phone model.

REFERENCE

For more information about key functions see Appendix A, the section, "Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters" on page 248.

For information about configuring softkeys, programmable keys, and expansion module keys, see Chapter 5, the section, "Softkeys/Programmable Keys/Expansion Module Keys" on page 5-157.

ACTION URI

The IP phones have a feature that allows an administrator to specify a uniform resource identifier (URI) that triggers a GET when certain XML events occur. The Action URI feature prevents the phones from hanging if the Action URIs should fail. The phones also support transparent, non-blocking, XML post execute item URIs.

The IP phone XML events that support this feature are defined in the following table.

ACTION URI	DESCRIPTION
Startup	Specifies the URI for which the phone executes a GET on when a startup event occurs.
Successful Registration	Specifies the URI for which the phone executes a GET on when a successful registration event occurs.
Registration Event	Specifies the URI for when registration events occur or when there are registration state changes. **Note:** If defined, this action URI is also called upon at startup if the SIP registrar IP has not been configured (i.e. the IP is 0.0.0.0). **Note:** This action URI is not called when the same event is repeated (for example, a timeout occurs again when registration is already in a timeout state.)
Incoming Call	Specifies the URI for which the phone executes a GET on when an incoming call event occurs.
Outgoing Call	Specifies the URI for which the phone executes a GET on when an outgoing call event occurs.
Offhook	Specifies the URI for which the phone executes a GET on when an offhook event occurs.
Onhook	Specifies the URI for which the phone executes a GET on when an onhook event occurs.
Connected	Specifies the URI for which the phone executes an HTTP GET when it goes into the “connected” state. This includes regular phone calls, intercom calls, paging calls, RTP streaming, and the playing of a WAV file. It is also triggered when the phone establishes the second leg of a 3-way call.
Disconnected	Specifies the URI that the phone executes a GET on, when it transitions from the incoming, outgoing, calling, or connected state into the idle state.
XML SIP Notify	Specifies the URI to be called when an empty XML SIP NOTIFY is received by the phone.
Poll	Specifies the URI to be called every "action uri poll interval" seconds.
Poll Interval	Specifies the interval, in seconds, between calls from the phone to the "action uri poll".

You can set these parameters using the configuration files or the Mitel Web UI.

REFERENCE

For more information about setting the Action URIs for XML applications, see “Action URIs” on page 5-324.

XML SIP NOTIFY EVENTS AND ACTION URIS

In order for an XML push to bypass the firewall, the phone supports a proprietary SIP NOTIFY event (aastra-xml) with or without XML content.

If XML content is provided in the SIP NOTIFY, it is processed directly by the phone as it is done for an XML PUSH.

Reference

For more information about enabling the XML SIP Notify on the IP Phones, see Chapter 5, the section, "XML SIP Notify Events" on page 5-338.

POLLING ACTION URIS

Another way to reach a phone behind a firewall is to have the phone make an XML call at periodic intervals. An Administrator can use the **action uri poll** to command the phone to perform an XML call at configurable intervals.

An Administrator can specify the URI to be called and specify the interval between polls. Configuration of this feature is dynamic (no reboot required).

Reference

For more information about configuring the polling and polling interval of Action URIs, see "Polling Action URIs" on page 5-331.

CONFIGURATION SERVER SETTINGS

The configuration server stores the firmware images, configuration files, and software when performing software upgrades to the IP phone. An administrator can configure the following parameters for the configuration server:

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
DOWNLOAD PROTOCOL SETTINGS			
Download Protocol	Download Protocol	download protocol	Protocol to use for downloading new versions of software to the IP phone. Valid values are: TFTP FTP HTTP HTTPS **Note:** For DHCP to automatically populate the IP address or domain name for the download servers, your DHCP server must support Option 66. The IP phones also support Option 60 and 43. For more information, see Chapter 4, the section, "DHCP" on page 4-4. For more information about download protocols on the IP Phone, see Chapter 4, "Configuration Server Protocol" on page 4-104.
Primary TFTP	TFTP Server	tftp server	The TFTP server's IP address or qualified domain name. If DHCP is enabled and the DHCP server provides the information, this field is automatically populated. Use this parameter to change the IP address or domain name of the TFTP server. This will become effective after this configuration file has been downloaded into the phone. For more information, see Chapter 4, "Configuration Server Protocol" on page 4-104.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Primary TFTP Path	TFTP Path	tftp path	Specifies the path name for which the configuration files reside on the TFTP server for downloading to the IP Phone. If the IP phone's configuration and firmware files are located in a sub-directory beneath the server's root directory, the relative path to that sub-directory should be entered in this field. **Note:** Enter the path name in the form *folderX\folderX\folderX*. For example, ***ipphone\6867i\configfiles***. For more information, see Chapter 4, "Configuration Server Protocol" on page 4-104.
Alternate TFTP	Alternate TFTP	alternate tftp server	The alternate TFTP server's IP address or qualified domain name. This will become effective after this configuration file has been downloaded into the phone. For more information, see Chapter 4, "Configuration Server Protocol" on page 4-104.
Alternate TFTP Path	Alternate TFTP Path	alternate tftp path	Specifies the path name for which the configuration files reside on the Alternate TFTP server for downloading to the IP Phone. If the IP phone's configuration and firmware files are located in a sub-directory beneath the server's root directory, the relative path to that sub-directory should be entered in this field. For more information, see Chapter 4, "Configuration Server Protocol" on page 4-104.
Select TFTP	Use Alternate TFTP	use alternate tftp	Enables or disables the alternate TFTP server. Valid values are "0" disabled and "1" enabled. For more information, see Chapter 4, "Configuration Server Protocol" on page 4-104.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
FTP Server	FTP Server	ftp server	The FTP server's IP address or network host name. This will become effective after this configuration file has been downloaded into the phone. **Optional**: You can also assign a username and password for access to the FTP server. See the following parameters for setting username and password. For more information, see Chapter 4, "Configuration Server Protocol" on page 4-104.
FTP Path	FTP Path	ftp path	Specifies the path name for which the configuration files reside on the FTP server for downloading to the IP Phone. If the IP phone's configuration and firmware files are located in a sub-directory beneath the server's root directory, the relative path to that sub-directory should be entered in this field. For more information, see Chapter 4, "Configuration Server Protocol" on page 4-104.
FTP Username	FTP Username	ftp username	The username to enter for accessing the FTP server. This will become effective after this configuration file has been downloaded into the phone. **Note:** The IP Phones support usernames containing dots ("."). For more information, see Chapter 4, "Configuration Server Protocol" on page 4-104.
FTP Password	FTP Password	ftp password	The password to enter for accessing the FTP server. This will become effective after this configuration file has been downloaded into the phone. For more information, see Chapter 4, "Configuration Server Protocol" on page 4-104.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
HTTP Server	HTTP Server	http server	The HTTP server's IP address. This will become effective after this configuration file has been downloaded into the phone. **Note:** You can also assign an HTTP relative path to the HTTP server. See the next parameter (http path). For more information, see Chapter 4, "Configuration Server Protocol" on page 4-104.
HTTP Path	HTTP Path	http path	Specifies the path name for which the configuration files reside on the HTTP server for downloading to the IP Phone. If the IP phone's configuration and firmware files are located in a sub-directory beneath the server's root directory, the relative path to that sub-directory should be entered in this field. For more information, see Chapter 4, "Configuration Server Protocol" on page 4-104.
HTTP Port	HTTP Port	http port	Specifies the HTTP port that the server uses to load the configuration to the phone over HTTP. For more information, see Chapter 4, "Configuration Server Protocol" on page 4-104.
Download Server	HTTPS Server	https server	The HTTPS server's IP address. This will become effective after this configuration file has been downloaded into the phone. **Note:** You can also assign an HTTPS relative path to the HTTPS server. See the next parameter (https path). For more information, see Chapter 4, "Configuration Server Protocol" on page 4-104.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
Download Path	HTTPS Path	https path	Specifies the path name for which the configuration files reside on the HTTPS server for downloading to the IP Phone. If the IP phone's configuration and firmware files are located in a sub-directory beneath the server's root directory, the relative path to that sub-directory should be entered in this field. For more information, see Chapter 4, "Configuration Server Protocol" on page 4-104.
Download Port	HTTPS Port	https port	Specifies the HTTP port that the server uses to load the configuration to the phone over HTTP. For more information, see Chapter 4, "Configuration Server Protocol" on page 4-104.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
AUTO-RESYNC SETTINGS			
N/A	Mode	auto resync mode	Enables and disables the phone to be updated automatically once a day at a specific time in a 24-hour period. This parameter works with TFTP, FTP, and HTTP servers. **Notes:** **1.** If a user is accessing the Mitel Web UI, they are not informed of an auto-reboot. **2.** Any changes made using the Mitel Web UI or the IP phone UI are not overwritten by an auto-resync update. Auto-resync affects the configuration files only. However, the settings in the Mitel Web UI take precedence over the IP phone UI and the configuration files. **3.** The resync time is based on the local time of the IP phone. **4.** If the IP phone is in use (not idle) at the time of the resync check, the reboot occurs when the phone becomes idle. **5.** The automatic update feature works with both encrypted and plain text configuration files. For more information, see Chapter 8, the section, "Using the Auto-Resync Feature" on page 8-8.

<table>
<tr><th>PARAMETER IN
IP PHONE UI</th><th>PARAMETER IN MITEL WEB UI</th><th>PARAMETERS IN CONFIGURATION FILES</th><th>DESCRIPTION</th></tr>
<tr><td>N/A</td><td>Time (24-hour)</td><td>auto resync time</td><td>Sets the time of day in a 24-hour period for the IP phone to be automatically updated. This parameter works with TFTP, FTP, and HTTP servers.

Notes:
1. The resync time is based on the local time of the IP phone.
2. The value of 00:00 is 12:00 A.M.
3. When selecting a value for this parameter in the Mitel Web UI, the values are in 30-minute increments only.
4. When entering a value for this parameter using the configuration files, the value can be entered using minute values from 00 to 59 (for example, the auto resync time can be entered as 02:56).

For more information, see Chapter 8, the section, “Using the Auto-Resync Feature” on page 8-8.</td></tr>
<tr><td>N/A</td><td>Maximum Delay</td><td>auto resync max delay</td><td>Specifies the maximum time, in minutes, the phone waits past the scheduled time before starting a checksync.

For more information, see Chapter 8, the section, “Using the Auto-Resync Feature” on page 8-8.</td></tr>
<tr><td>N/A</td><td>Days</td><td>auto resync days</td><td>Specifies the amount of days that the phone waits between checksync operations.

Note: A value of 0 causes the phone to checksync every time the clock reads the proper time. A value of 1 forces the phone to wait 24 hours prior to doing the first checksync.

For more information, see Chapter 8, the section, “Using the Auto-Resync Feature” on page 8-8.</td></tr>
</table>

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
XML PUSH SERVER LIST (APPROVED IP ADDRESSES)			
N/A	XML Push Server List (Approved IP Addresses)	xml application post list	The HTTP server that is pushing XML applications to the IP phone. For more information, see Chapter 5, the section, "XML Push Requests" on page 5-320.

FIRMWARE UPDATE FEATURES

The IP phones support the protocols, TFTP, FTP, HTTP or HTTPS to download configuration files and upgrade firmware to the phones from a configuration server.

You can download the firmware stored on the configuration server in one of three ways:

- Using the "**Firmware Update**" page in the Mitel Web UI at the location ***Advanced Settings->Firmware Update***.
- Using the IP Phone UI or the Mitel Web UI to **restart** the phone. The phone automatically looks for firmware updates and configuration files during the boot process.
- Setting an **Auto-Resync** feature to automatically update the firmware, configuration files, or both at a specific time in a 24-hour period). (Feature can be enabled using the configuration files or the Mitel Web UI).

REFERENCE

For more information about firmware update, see Chapter 8, "Upgrading the Firmware."

MACRO SUPPORT TO PROVISION PHONES

Administrators can provision the phones using macros such as $DM (device model) and $MAC (mac address). The $DM and $MAC parameters are searched in the specified path and are replaced with a corresponding value.

Note: Only uppercase characters of $DM and $MAC are supported while using macros.

Note: As on 6.2.0 Macros have been implemented for these 2 feature only firmware server and configuration server.

For example:

http server: RC.lab.mitel.com

http path: Provisioning /mitel/$DM

firmware server: https://RC.lab.mitel.com:443/Provisioning/mitel/$DM/$MAC

In above example, phone (example: 6920) sends following requests

Provisioning /mitel/6920/startup.cfg

Provisioning/mitel/6920/1400E905117A/6920.st

TLS SUPPORT

The IP Phones support a transport protocol called **Transport Layer Security (TLS)** and **Persistent TLS**. TLS is a protocol that ensures communication privacy between the SIP phones and the Internet. TLS ensures that no third party may eavesdrop or tamper with any message. An Administrator can configure the following parameters for TLS Support.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
N/A	Transport Protocol	sip transport protocol	Specifies the protocol that the IP phone uses to send out SIP messages. Default is UDP. **Notes:** **1.** If you set the value of this parameter to 4 (TLS), the phone checks to see if the "**sips persistent tls**" is enabled. If it is enabled, the phone uses Persistent TLS on the connection. If "**sips persistent tls**" is disabled, then the phone uses TLS on the connection. If TLS is used, you must specify the Root and Intermediate Certificates, the Local Certificate, the Private Key, and the Trusted Certificates. **2.** If the phone uses Persistent TLS, you MUST specify the Trusted Certificates; the Root and Intermediate Certificates, the Local Certificate, and the Private Key are optional. For more information, see Chapter 6, the section, "Transport Layer Security (TLS)" on page 6-22.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
N/A	N/A	sips persistent tls	Enables or disables the use of Persistent Transport Layer Security (TLS). Persistent TLS sets up the connection to the server once and re-uses that connection for all calls from the phone. The setup connection for Persistent TLS is established during the registration of the phone. If the phones are set to use Persistent TLS, and a call is made from the phone, this call and all subsequent calls use the same authenticated connection. This significantly reduces the delay time when placing a call. **Notes:** **1.** There can be only one persistent TLS connection created per phone. **2.** If you configure the phone to use Persistent TLS, you must also specify the **Trusted Certificate** file to use. The Root and Intermediate Certificates, Local Certificate, and Private Key files are optional. For more information, see Chapter 6, the section, "Transport Layer Security (TLS)" on page 6-22.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
NA	NA	sip persistent tls keep alive	Allows you to configure the keep-alive feature for persistent TLS connections only. When this feature is configured, the phone will send keep-alive pings to the proxy server at configured intervals. **Note**: The real time interval will vary between 80% and 100% of the configured value. The keep-alive feature for persistent TLS connections performs the following functionalities: • After a persistent TLS connection is established or re-established, activate the keep-alive, which will send CRLF to peer periodically. • The phone will retry the connection automatically when a persistent TLS connection is down. • When a persistent TLS connection is re-established (primary is up or primary is down and backup is up), refresh registration of the accounts associated with the connection. • When a persistent TLS connection to primary is down, switch to backup if connection to backup is working.
NA	NA	sip send sips over tls	Allows administrators the ability to manually configure the IP phones to use either the SIP or SIPS URI scheme when TLS or persistent TLS is enabled. For more information, see Chapter 6, the section, "Transport Layer Security (TLS)" on page 6-22.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
N/A	Root and Intermediate Certificates Filename	sips root and intermediate certificates	Allows you to specify the SIP Root and Intermediate Certificate files to use when the phone uses the TLS transport protocol to setup a call. The Root and Intermediate Certificate files contain one root certificate and zero or more intermediate certificates which must be placed in order of certificate signing with root certificate being the first in the file. If the local certificate is signed by some well known certificate authority, then that authority provides the user with the Root and Intermediate Certificate files (most likely just CA root certificate). This parameter is required when configuring TLS (optional for Persistent TLS.) **Note:** The certificate files must use the format ".pem". To create custom certificate files to use on your IP phone, contact Mitel Technical Support. For more information, see Chapter 6, the section, "Transport Layer Security (TLS)" on page 6-22.
N/A	Local Certificate Filename	sips local certificate	Allows you to specify the Local Certificate file to use when the phone uses the TLS transport protocol to setup a call. This parameter is required when configuring TLS (optional for Persistent TLS.) **Note:** The certificate file must use the format ".pem". To create specific certificate files to use on your IP phone, contact Mitel Technical Support. For more information, see Chapter 6, the section, "Transport Layer Security (TLS)" on page 6-22.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
N/A	Private Key Filename	sips private key	Allows you to specify a Private Key file to use when the phone uses the TLS transport protocol to setup a call. This parameter is required when configuring TLS (optional for Persistent TLS.) **Note:** The key file must use the format ".pem". To create specific private key files to use on your IP phone, contact Mitel Technical Support. For more information, see Chapter 6, the section, "Transport Layer Security (TLS)" on page 6-22.
N/A	Trusted Certificates Filename	sips trusted certificates	Allows you to specify the Trusted Certificate files to use when the phone uses the TLS transport protocol to setup a call. The Trusted Certificate files define a list of trusted certificates. The phone's trusted list must contain the CA root certificates for all the servers it is connecting to. For example, if the phone is connecting to server A which has a certificate signed by CA1, and server B that has a certificate signed by CA2, the phone must have CA1 root certificate and CA2 root certificate in its Trusted Certificate file. This parameter is required when configuring TLS or Persistent TLS. **Note:** The certificate files must use the format ".pem". To create custom certificate files to use on your IP phone, contact Mitel Technical Support. For more information, see Chapter 6, the section, "Transport Layer Security (TLS)" on page 6-22.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
N/A	SAN Support for IP Address	N/A	Enables phones to parse the IP address in the server certificate Subject Alternative Name (SAN) entries. By default, SAN certificate support is enabled on phones. If the SIP server certificate includes a SAN extension, the phone compares the IP addresses in the SAN entries with the SIP peer name. For more information about TLS, see Chapter 6, the section, "Transport Layer Security (TLS)" on page 6-22.
N/A	Wildcard Support for Common Names (CNs)	sips strict cert cn validation	Enables phones to validate the CNs from the server certificates by comparing the names with the configured SIP peer name. The configuration parameter "*sips strict cert cn validation*" is used to enable this parameter. If disabled, the phones will validate the SIP server certificates with a CN specified as a wildcard. The first name of the CN can be in the following format: <LH>*<RH>.<Any Other Labels>.com Where, LH and RH can be any valid string or empty and Asterisk (*) is the wildcard character. For example, The CN can be: • *.example.com • *xyz.example.com • xyz*.example.com • abc*xyz.example.com The first label of the CN is wildcard matched with the first label of the configured SIP peer name. For more details about this configuration parameter, see "*sips strict cert cn validation*" in Appendix A, "Transport Layer Security (TLS) Settings." For more information about TLS, see Chapter 6, the section, "Transport Layer Security (TLS)" on page 6-22.

802.1X SUPPORT

The IP phones support the IEEE 802.1x Protocol. The 802.1x Protocol is a standard for passing Extensible Authentication Protocol (EAP) over a wired or wireless Local Area Network (LAN).

The 802.1x Protocol on the IP phone facilitates media-level access control, and offers the capability to permit or deny network connectivity, control LAN access, and apply traffic policy, based on user or endpoint identity. This feature supports both the EAP-MD5 and EAP-TLS Protocols.

Note: If configuring 802.1x using the IP Phone UI, the certificates and private keys must already be configured and stored on the phone. Use the configuration files or the Mitel Web UI to load certificates and private keys

An Administrator can configure the following parameters for the 802.1x Protocol.

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
GENERAL			
802.1x Mode	EAP Type	eap-type	Specifies the type of authentication to use on the IP Phone. For more information, see Chapter 6, the section, “802.1x Configuration” on page 6-27.
Identity	Identity	identity	Specifies the identity or username used for authenticating the phone. **Note:** The value you enter for this parameter also displays in the Mitel Web UI at the path Advanced Settings->802.1x Support->General->Identity For more information, see Chapter 6, the section, “802.1x Configuration” on page 6-27.
EAP-MD5 SETTINGS			

PARAMETER IN IP PHONE UI	PARAMETER IN MITEL WEB UI	PARAMETERS IN CONFIGURATION FILES	DESCRIPTION
MD5 Password	MD5 Password	md5 password	Specifies the password used for the MD5 authentication of the phone. **Note:** The value you enter for this parameter also displays in the Mitel Web UI at the path Advanced Settings->802.1x Support->EAP-MD5 Settings->MD5 Password. The password displays as "*******". For more information, see Chapter 6, the section, "802.1x Configuration" on page 6-27.
EAP-TLS SETTINGS			
N/A	Root and Intermediate Certificates Filename	802.1x root and intermediate certificates	Specifies the file name that contains the root and intermediate certificates related to the local certificate. For more information, see Chapter 6, the section, "802.1x Configuration" on page 6-27.
N/A	Local Certificate Filename	802.1x local certificate	Specifies the file name that contains the local certificate. For more information, see Chapter 6, the section, "802.1x Configuration" on page 6-27.
N/A	Private Key Filename	802.1x private key	Specifies the file name that contains the private key. For more information, see Chapter 6, the section, "802.1x Configuration" on page 6-27.
N/A	Trusted Certificates Filename	802.1x trusted certificates	Specifies the file name that contains the trusted certificates. For more information, see Chapter 6, the section, "802.1x Configuration" on page 6-27.

TROUBLESHOOTING

The Troubleshooting feature in the Mitel Web UI provides tasks that a system administrator can perform on the IP phones for troubleshooting purposes. Using this feature, a system administrator can:

- Assign an IP address and IP port to which log information will be transmitted
- Filter the logs according to severity
- Save the current local configuration file to a specified location
- Save the current server configuration file to a specified location
- Save the phone logs (sys logs) to a specified location
- Save the current user configuration file to a specified location (if logged on using the Visitor Desk Phone feature).
- Save the current user_local configuration file to a specified location (if logged on using the Visitor Desk Phone feature).
- Show task and stack status (including “Free Memory” and “Maximum Memory Block Size”)
- Enable/disable a WatchDog task
- View System and Error Messages
- Enable/disable the uploading of configuration and crash file information to a pre-defined server

Note:

1. If the diagnostic server is programmed, and the user attempts to download log files from the Troubleshooting page, the file size of the download will be zero. The files are sent only to the diagnostic server.

2. If the diagnostic Server is not programmed, and the user attempts to download log files from the Troubleshooting page after performing a Log Issue or Log Upload operation, the latest log files will be downloaded successfully. To download the latest log files from the Troubleshooting page, it is recommended that the user perform a fresh Log Issue or Log Upload operation before proceeding to download, failing which previously generated log files will be downloaded.

Mitel Technical Support can then use the information gathered to perform troubleshooting tasks.

REFERENCE

For more information about troubleshooting on the IP Phones, see Chapter 9, “Troubleshooting.”

For more information about the Visitor Desk Phone feature see "Visitor Desk Phone Support, " on page 102.

DIAGNOSTICS

The Diagnostics option allows you to capture TCP network packets for up to 5 minutes as well as collect the captured logs that can in turn be used to help debug and troubleshoot various issues.

By default, Diagnostics is not displayed in the phone's UI. The system administrator needs to set the configuration parameters to enable or disable the Diagnostics option.

ENHANCED LOGGING AND DIAGNOSTICS

When the Enhanced logging and Diagnostic feature is enabled, the following will be displayed in the phone's UI in the Diagnostic menu.

- Troubleshooting (Admin only)
- Ping
- TraceRoute
- Capture
- Log Upload
- Diagnostic server (Admin only)
- Audio Diagnostic

This feature is enabled by default. However, users may opt to disable it using the configuration parameter "diagnostics".

Enabling/Disabling Diagnostics Using the Configuration Files.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section,"Diagnostics," on page 355.

AUDIO DIAGNOSTICS

The **Audio Diagnostics** sub-menu allows you to collect up to 5 minutes of audio log files that can help to debug audio issues on the Mitel 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 SIP phones.

Capturing Audio Log Files Using the IP Phone UI

IP PHONE UI

To capture audio diagnostic logs on the Mitel MiVoice 6867i, 6869i, 6873i, 6920, and 6930 SIP phones:

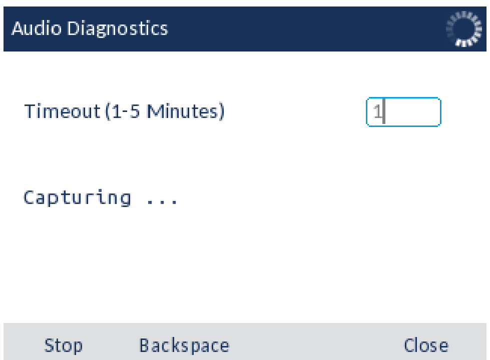
1. Press the (**Settings**) key on the phone to enter the **Settings** menu.
2. Navigate to **Diagnostics** > **Audio Diagnostics** using the navigation keys and press the **Select** softkey.

3. In the **Timeout** input field, enter the amount of time (in minutes from 1 to 5) you would like to run the audio diagnostic tool for, using the dialpad keys.
4. Press the **Start** softkey.
   The IP phone displays "**Capturing**" and when the timeout elapses, "**Collecting Logs**" is displayed. When all the logs have been collected, a "**Complete**" message is displayed.

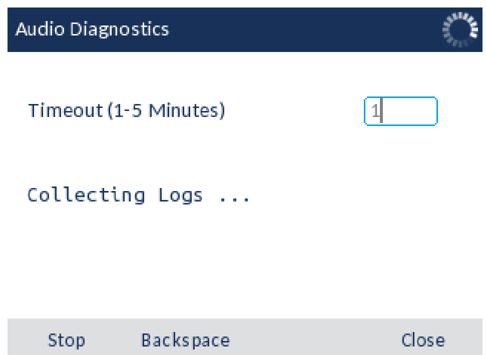
> **Note:**
> 1. Press the **Stop** softkey at any time to stop capturing the audio diagnostic logs.
> 2. A "log issue" is issued only after the completion of an audio diagnostics run.

CAUTION: Do not change the audio device when you run the audio diagnostics tool.

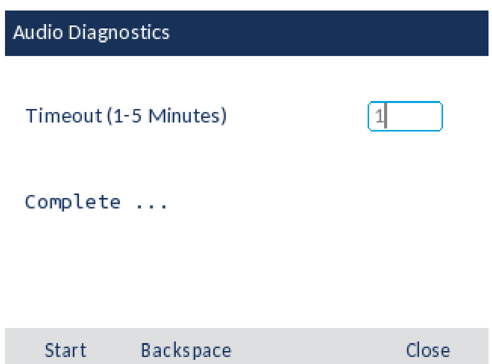
Capture



Collect



Complete



To capture audio diagnostic logs on the Mitel MiVoice 6873i/ 6940/6970 SIP phones:

1. Press the (**Settings**) key / the **Settings** softkey on the phone to enter the **Settings** menu.
2. Tap the **Diagnostics** icon.
3. In the **Audio Diagnostics** menu, enter the amount of time (in minutes from 1 to 5) you would like to run the audio diagnostic tool for in the **Timeout** input field using the dialpad keys.
   The IP phone displays "**Capturing**..." and when the timeout elapses, "**Collecting**

Logs..."isdisplayed. When all the logs have been collected, a "**Complete**..." message displayed.

Note:

1. Tap the **Stop** softkey at any time to stop capturing the audio diagnostic logs.
2. A "log issue" is issued only after the completion of an audio diagnostics run.

CAUTION: Do not change the audio device when you run the audio diagnostics tool.

Note: The 5.1 configuration parameters "log issue" and "audio diagnostics" are deprecated in 6.0. They are effectively replaced with "diagnostics: 0/1".

LOGGING LEVELS

When the phone registers with the generic SIP platform, the log level for Sip Module is set to 1 by default.

When the phone registers with MiVoice Connect or MiCloud Connect, the default logging level for SIP is set to max.

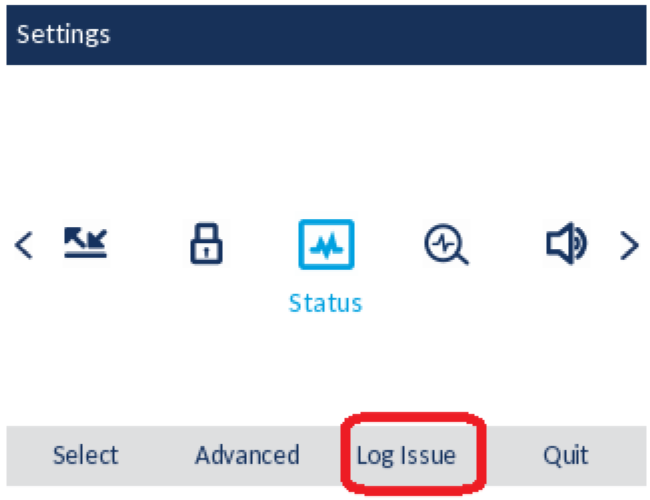
Note: The default logging level for SIP is raised to 8191.

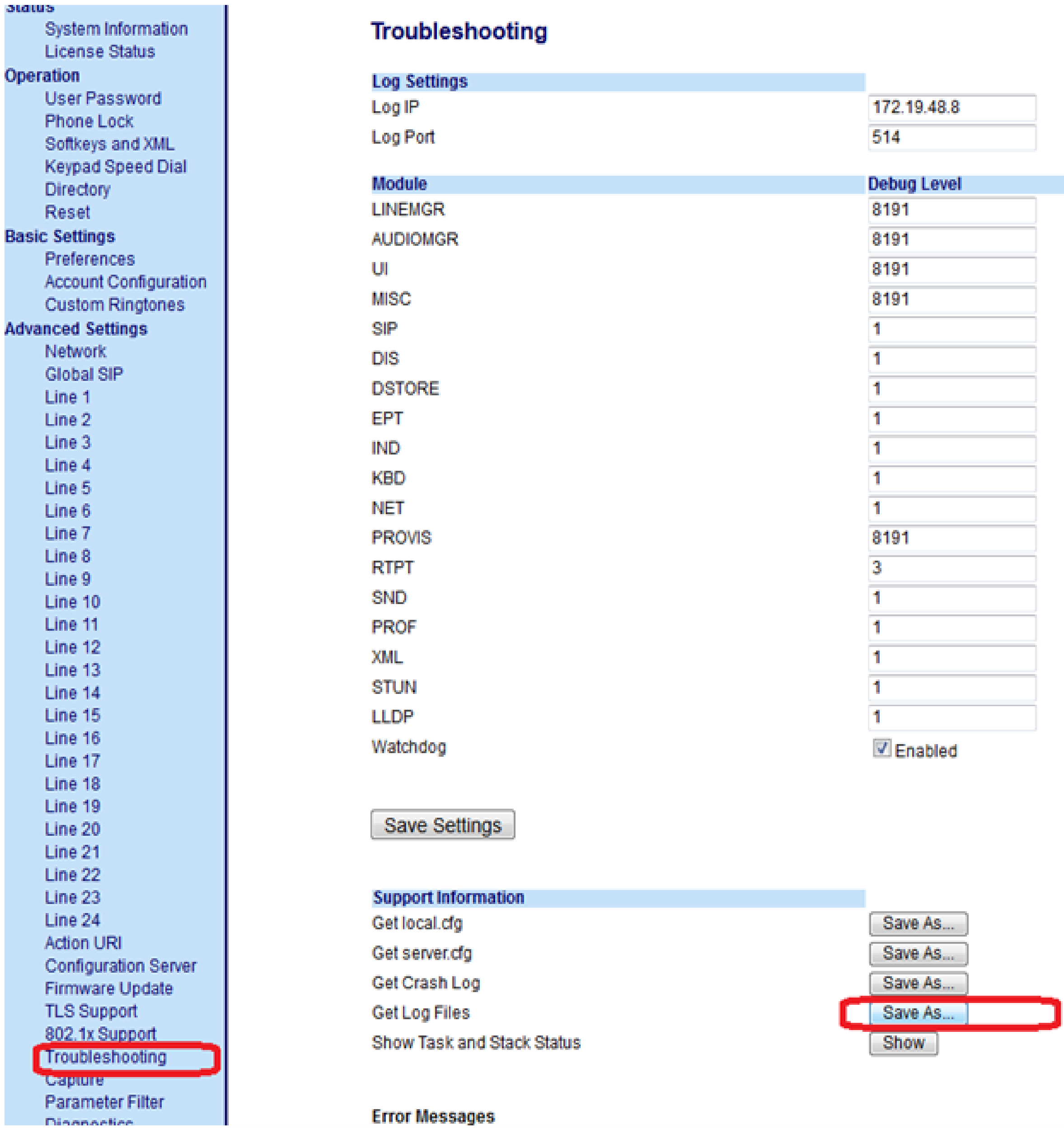
LOG GATHERING

There are three ways to gather logs:

1. **Logs through Web UI** -
   Press or tap the “Log Issue” key on the phone UI. After waiting for 3-4 minutes, on the Web UI of phone, go to **Advanced Settings >Troubleshooting > Get Log Files > Save As** as shown in the following image.

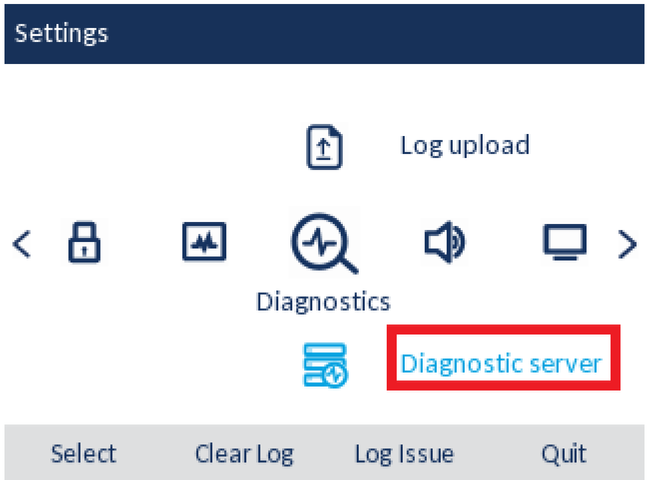
Note: Do not configure Diagnostic Server if you want logs through Web UI.


Settings
Status
Select
Advanced
Log Issue
Quit



2. **Logs through Diagnostic Server** -
   Users can now configure Diagnostic Server from the phone UI or from configuration files. If cloud diagnostic server is configured, the phone will upload logs only to the configured server. In this scenario, logs cannot be downloaded from the Web UI. The default protocol used is FTP (if no protocol is specified).

   On the phone UI, go to **Settings > Advanced > <password> > Diagnostics > Diagnostic server.**



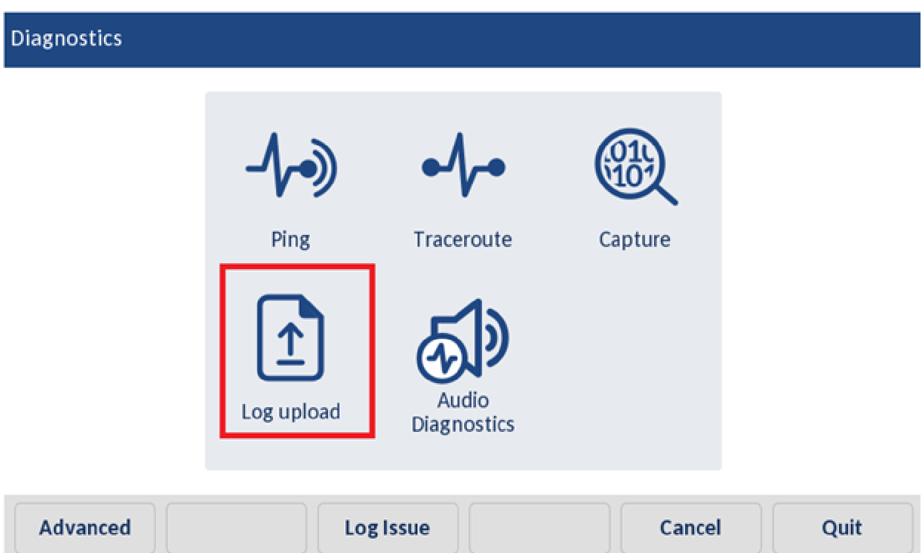
To configure the cloud diagnostic server through configuration files, see Appendix A, the section,"Diagnostics," on page 355.

3. **Log Upload** -
"Log Issue" and "Log Upload" perform the same functionality except that "Log upload" also uploads logs to the Diagnostic Server whereas the "Log Issue" requires WebUI to upload logs.

.

Note: If you try to download logs from the WebUI without hitting "Log Issue" or "Log Upload", you will receive an empty log file.

.



SCREENSHOT

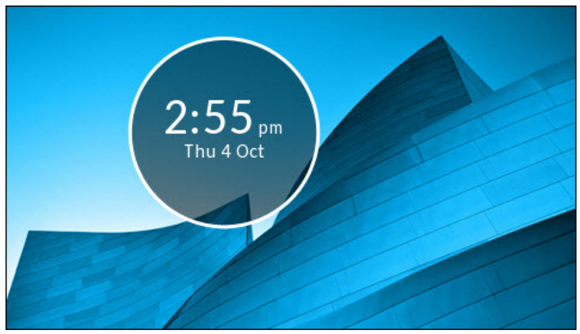
The **Screenshot** option allows you to capture a screenshot image of what is currently displayed on the respective IP phone's LCD screen in PNG format. This can be used to help document the procedures leading up to an issue or help in identifying issues with the UI.

Taking a Screenshot Using the Mitel Web UI

MITEL WEB UI

To take a screenshot:

1. Click on **Screenshot**.



2. Right click on the image to save the image to a desired location on your PC.

Chapter 4

CONFIGURING NETWORK AND SESSION INITIATION PROTOCOL (SIP) FEATURES

ABOUT THIS CHAPTER

This chapter provides the information required to configure the Network and Global SIP features on the IP Phone. These features are password protected on the IP Phone UI and the Mitel Web UI. This chapter also includes procedures for configuring the Network and Global SIP features via the configuration files, the IP Phone UI, and the Mitel Web UI where applicable.

TOPICS

This chapter covers the following topics:

OVERVIEW

An administrator can configure the IP Phone Network and SIP options from the phone UI, from the **Mitel Web UI, or the configuration files**. Administrator level options are password protected in both the IP phone UI and the Mitel Web UI.

Note: An administrator has the option of enabling and disabling the use of password protection in the IP phone UI. This is configurable using the configuration files only. For more information about this feature, see Appendix A, the section "Password Settings" on page 20.

The procedures in this section include configuring from the IP phone UI and the Mitel Web UI. To configure the IP phones using the configuration files, see Appendix A, "About this Appendix."

To configure the phone using the IP phone UI, you must enter an administrator password. To configure the phone using the Mitel Web UI, you must enter an administrator username and password.7

Note: In the IP phone UI, the default password is "22222". In the Mitel Web UI, the default admin username is "Admin" and the default password is "22222".

REFERENCES

For configuring the IP phone at the Asterisk IP PBX, see Appendix B, "Configuring the IP Phone at the Asterisk IP PBX."

For sample configuration files, see Appendix C, "Sample Configuration Files." These sample files include basic parameters required to register the IP phone at the PBX.

NETWORK SETTINGS

This section describes the network settings on the IP phone which include configuring for:

- DHCP
- IP Address (of phone)
- Subnet Mask (of phone)
- Gateway
- Primary DNS
- Secondary DNS
- Hostname
- LAN Port
- PC Port
- Port Mirroring
- PC Port Pass Thru Enable/Disable

BASIC NETWORK SETTINGS

DHCP

The IP phone is capable of querying a DHCP server, allowing a network administrator a centralized and automated method of configuring various network parameters for the phone. If DHCP is enabled, the IP phone requests the following network information:

- Subnet Mask
- Gateway (i.e. router)
- Domain Name System (DNS) Server
- Network Time Protocol Server
- IP Address
- TFTP Server or Alternate TFTP Server if enabled on the phone
- TFTP Path or Alternate TFTP Path if enabled on the phone
- FTP Server
- FTP Path
- HTTP Server
- HTTP Path
- HTTP Port
- HTTPS Server
- HTTPS Path

- HTTPS Port

The network administrator chooses which of these parameters (if any) are supplied to the IP phone by the DHCP server. The administrator must configure the phone manually to provide any required network parameters not supplied by the DHCP server.

Enabling/Disabling DHCP Using the Configuration Files

Use the following procedure to enable/disable DHCP on the phone using the configuration files.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Network Settings" on page A-13.

Enabling/Disabling DHCP Using the IP Phone UI

Use the following procedure to enable/disable DHCP on the phone using the IP Phone UI.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Administrator Menu.**
3. Enter your Administrator password.

   Note: The IP Phones accept numeric passwords only.

4. Select **Network Settings**.
5. Select option **DHCP**.
6. Press **Change** to set "*Use DHCP?*" to "Yes" (enable) or "No" (disable).
7. Press **Done** to save the changes.

For the 6867i/6869i/6920/6930:

1. Press or on the phone to enter the Options List.
2. Press the **Advanced** softkey.
3. Enter the Administrator password using the keypad. Default is "**22222**".
4. Select **Network > Settings**.
5. In the "**Use DHCP?**" checkbox, press the button to enable or disable DHCP.
6. Press the **Save** softkey.
7. Press the or button, the or button, or the **Quit** softkey to return to the idle screen.

For the 6873i/6940/6970:

1. Press , , or the **Settings** softkey on the phone to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password and press the blue Enter key. Default is “**22222**”.
4. Tap the **Network** icon.

> **Note:** If required, swipe left on the screen to navigate to the second page of options.

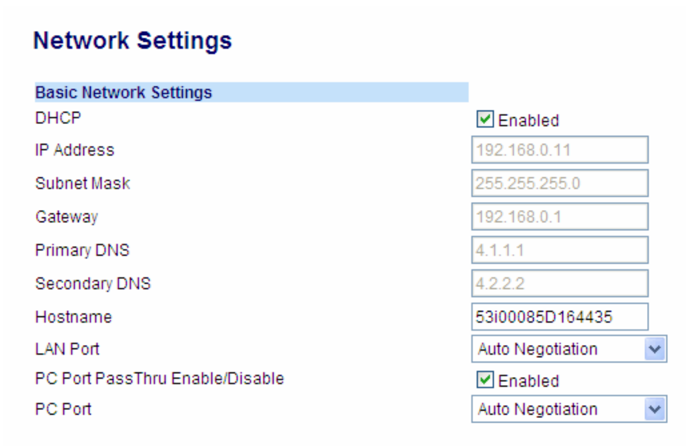
5. Tap the **Settings** icon.
6. Tap the “**Use DHCP?**” checkbox to enable or disable DHCP.
7. Tap the **Save** softkey.
8. Press the or button, the or button, or the **Quit** softkey to return to the idle screen.

Enabling/Disabling DHCP Using the Mitel Web UI

Use the following procedure to enable/disable DHCP using the Mitel Web UI.

MITEL WEB UI

1. Click on **Advanced Settings->Network->Basic Network Settings.**



2. Enable the "**DHCP**" field by checking the check box. (Disable this field by unchecking the box).
3. Click **Save Settings** to save your settings.

DHCP REQUEST AND RELEASE SCENARIO

During normal reboot, a SIP phone sends a DHCP Request and the DHCP server responds with a DHCP ACK mentioning the lease time for the existing IP address for that SIP phone.

Note: If a SIP phone sends a DHCP Release on reboot, the DHCP server changes the IP address of the SIP phone on each reboot. Hence, the SIP phone sends a DHCP Request for retaining the same IP assigned to it before the reboot.

On reboot, the SIP phones trigger the DHCP Release in the following conditions:

- Factory reset
- DHCP enabled or disabled
- VLAN tagging change
- VLAN-ID change when VLAN tagging is enabled
- LLDP enabled or disabled
- 802.1x enabled or disabled

DNS PARAMETER UPDATE IN DHCP LEASE RENEWAL-DHCP ACK

The SIP phone updates the DNS parameters in DHCP ACK through DHCP release renewal when the user changes DNS settings on the DHCP server.

This feature is supported on the 6863i 6865i, 6867i, 6869i, 6873i, and 6900 Series SIP phones.

DHCP OPTIONS 66, 60, AND 43 SERVER CONFIGURATIONS

Option 66

The IP Phones support download protocols as referenced in RFC2131 and RFC1541 (TFTP, FTP, HTTP,. HTTPS) to support DHCP option 66. Option 66 is part of the DHCP Offer message that the DHCP server generates to tell the phone which configuration server it should use to download new firmware and configuration files.

For DHCP to automatically populate the IP address or domain name for the servers, your DHCP server must support Option 66. Option 66 is responsible for forwarding the server's IP address or domain name to the phone automatically. If your DHCP server does not support Option 66, you must manually enter the IP address or domain name for your applicable configuration server into your IP phone configuration.

Options 60

The Mitel phones support Option 60 as referenced in RFC 2132.

Option 60 (Vendor Class Identifier) provides the DHCP server with a unique identifier for each phone model. This enables a system administrator to send the phone a customized Server Configuration in option 43.

The table below lists the identifier values for each phone model.

MODEL	IDENTIFIER VALUE
6863i	AastraIPPhone6863i
6865i	AastraIPPhone6865i
6867i	AastraIPPhone6867i
6869i	AastraIPPhone6869i
6873i	AastraIPPhone6873i
6905	AastraIPPhone6905
6910	AastraIPPhone6910
6920	AastraIPPhone6920
6930	AastraIPPhone6930
6940	AastraIPPhone6940

A configuration parameter ("**dhcp opt60 extended vendor class**") is available allowing the phones to provide the DHCP server with enhanced DHCP Option 60 (Vendor Class Identifier) information that includes firmware and bootrom information in addition to the identifier value.

If the parameter is configured as "**0**" (disabled - default), the phone will send simply a DHCP Option 60 value consisting of the identifier value. If the parameter is configured as "**1**" (enabled), the phone will send a DHCP Option 60 value consisting of the identifier value, firmware version, and bootrom version.

Configuring DHCP Option 60 Settings Using the Configuration Files

Use the following procedure to configure DHCP Option 60 settings using the configuration files.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "DHCP Option Settings" on page A-17.

Option 43

The Mitel phones also support Option 43 as referenced in RFC 2132. Option 43 consists of the following sub-options:

SUB-OPTION/CODE	DESCRIPTION
02	Configuration server (protocol, server, and path).
03	Redirection and Configuration Server (RCS) enable/disable.
08	ID string to enable the use of the VLAN identity in sub-option/code 09. Must be specified to avoid conflict with other vendors.
09	VLAN ID value.

The System administrator can use the Vendor Class Identifier to send the phone a customized Server Configuration in option 43 (Vendor-Specific information).

Note: If Mitel IP Phones receive the server configuration from both DHCP Option 66 and DHCP Option 43, then Option 43 takes precedence over Option 66.

Using Option 43 to Customize the IP Phone

A System Administrator can customize the IP Phone(s) in the network by entering a text string in the phone's configuration files. The following is an Option 43 example using Linux.

On the startup of the phones, when the DHCP server receives the request with the information in this example, it allows the 6867i phones to use FTP and the 6869i phones to use TFTP from the same server.

Linux Example

A System Administrator can enter the following in the DHCP server:

```
option space AastraIPPhone6867i;
option AastraIPPhone6867i.cfg-server-name code 02 = text;

option space AastraIPPhone6869i;
option AastraIPPhone6869i.cfg-server-name code 02 = text;

Subnet 192.168.1.0 netmask 255.255.255.0 {

  class "vendor-class-6867i" {
    match if option vendor-class-identifier="AastraIPPhone6867i";
    vendor-option-space AastraIPPhone6867i;
    option AastraIPPhone6867i.cfg-server-name
"ftp://username:password@10.10.10.1";
  }
  class "vendor-class-6869i" {
    match if option vendor-class-identifier="AastraIPPhone6869i";
    vendor-option-space AastraIPPhone6869i;
    option AastraIPPhone6869i.cfg-server-name "tftp://10.10.10.1";
  }
}
```

Your DHCP server configuration file, such as the *dhcpd.conf* file, may include one of these lines to configure the configuration server protocol and the server details.

PROTOCOL	FORMAT	EXAMPLES
HTTP	http://<server>/<path>	option AastraIPPhone6869i.cfg-server-name "http://192.168.1.45";
		option AastraIPPhone6869i.cfg-server-name "http://192.168.1.45/path";
		option AastraIPPhone6869i.cfg-server-name "http://httpsvr.example.com/path";

PROTOCOL	FORMAT	EXAMPLES
HTTPS	https://<server>/<path>	option AastraIPPhone6869i.cfg-server-name "https://192.168.1.45"; option AastraIPPhone6869i.cfg-server-name "https://192.168.1.45/path"; option AastraIPPhone6869i.cfg-server-name "https://httpssvr.example.com/path";
FTP	ftp://user:password@ftpserver	option AastraIPPhone6869i.cfg-server-name "ftp://192.168.1.45"; option AastraIPPhone6869i.cfg-server-name "ftp://ftpsvr.example.com"; (for anonymous user) option AastraIPPhone6869i.cfg-server-name "ftp://userID:password@ ftpsvr.example.com";
TFTP	tftp://tftpserver	option AastraIPPhone6869i.cfg-server-name "192.168.1.45"; option AastraIPPhone6869i.cfg-server-name "tftpsvr.example.com"; option AastraIPPhone6869i.cfg-server-name "tftp://tftpsvr.example.com";

Option 43 Redirection and Configuration Server (RCS) Bypass

DHCP Option 43 includes the ability to bypass contacting Mitel's Redirection and Configuration Server (RCS), in addition to the previous support of setting the configuration server to contact.

A sub-option code 3 uses a boolean value (true or false) that controls whether or not the phone should contact the RCS after a factory default. If this value is set to false, the RCS is not contacted. If it is set to true or is missing, then the RCS is contacted as per previous releases. This can be used in conjunction with the existing code 2 sub-option to set the configuration server.

Configuring RCS Bypass via Option 43 on a Linux DHCP Server

The following example illustrates how to configure RCS bypass via Option 43 on a Linux DHCP server.

```
option space AastraIPPhone;
option AastraIPPhone.cfg-server-name code 02 = text;
option AastraIPPhone.contact-rcs code 03 = boolean;

Subnet 192.168.1.0 netmask 255.255.255.0 {
```

```
#The 6867i phones do not contact the RCS but use the defined FTP
server for configuration #files.
  class "vendor-class-67i" {
    match if option vendor-class-identifier="AastraIPPhone6867i";
    vendor-option-space AastraIPPhone;
    option AastraIPPhone.cfg-server-name
"ftp://username:password@10.10.10.1";
    option AastraIPPhone.contact-rcs false;
  }

#The 6869i phones do not contact the RCS.
class "vendor-class-69i" {
    match if option vendor-class-identifier="AastraIPPhone6869i";
    vendor-option-space AastraIPPhone;
    option AastraIPPhone.contact-rcs false;
```

USING OPTION 120 ON THE IP PHONE

DHCP Option 120 (as referenced in RFC 3361) allows SIP clients to locate a local SIP server (i.e. outbound proxy server) that can be used for all outbound SIP requests. Using the "**use dhcp option 120**" configuration parameter, administrators can enable support for DHCP Option 120 on the IP phones. This is particularly useful when service providers require the IP phones to use certain outbound proxy servers or Session Border Controllers (SBCs) based on geographical location and have provisioned the outbound proxy by using DHCP Option 120. The parameter is disabled by default.

Considerations

The following considerations must be taken into account when enabling support for DHCP Option 120 on the IP phones:

- If the parameter is enabled and DHCP Option 120 contains a valid value, the IP phones will use the server IP/name obtained via DHCP Option 120 as the outbound proxy for both the Global SIP and Line 1 profiles.
- If Line 2 is configured and the outbound proxy is not defined, the phone will use the outbound proxy located in the Global SIP profile.
- If Line 2 is configured with a valid outbound proxy, the phone will retain the configured Line 2 outbound proxy and ignore the Global SIP profile. This allows for Line 2 to be registered to another service with another outbound proxy if required.
- If Line 2 is configured for another service but no outbound proxy is wanted/required, administrators should not leave the outbound proxy as undefined (i.e. 0.0.0.0) as the phone will use the outbound proxy located in the Global SIP profile. Instead, administrators should specify the proxy/registrar's address as the outbound proxy.
- If the parameter is enabled, but the server does not have an outbound proxy configured, DHCP Option 120 is ignored and the phone will behave as if the parameter is disabled.
- As Option 120 does not support port numbers directly, if a non-standard port (i.e. other than 5060) is required, this must be set using the configuration parameter "**sip outbound proxy port**" or by the use of DNS SRV in which case "**sip outbound proxy port**" must be set to 0.

Enabling/Disabling DHCP Option 120 Using the Configuration Files

Use the following procedure to enable/disable DHCP Option 120 using the configuration files.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "DHCP Option Settings" on page A-17.

USING OPTION 132 (802.1P VLAN ID) AND OPTION 43 TO TRANSFER VLAN ID ASSIGNMENT USING DHCP

There are now two ways of transporting the VLAN ID parameter in the Dynamic Host Configuration Protocol (DHCP):

- By DHCP Option 43 (vendor specific information)
- By DHCP Option 132 (802.1P VLAN ID)

When the phone receives the VLAN ID from the DHCP and the value is different from the one used by the phone to trigger the DHCP request, the phone reboots and then sends a new DHCP request in the new VLAN. The phone will remember the VLAN ID obtained by DHCP options so that on a reboot, the phone will send a DHCP request using the correct VLAN.

If using DHCP Option 43 to transfer VLAN ID assignment the following sub-options are utilized. Additionally, the corresponding rules must be followed:

SUB-OPTION/ CODE	DESCRIPTION	RULE
08	ID string to enable the use of the VLAN identity in sub-option/code 09. Must be specified to avoid conflict with other vendors.	Must be the 16-byte character string "Aastra{space}Telecom{space}{space}" (i.e. Aastra Telecom followed by two space characters). 16-byte hex equivalent: 41617374726120546656c65636f6d2020
09	VLAN ID value	Must be 4 bytes, whereas the first and second byte must be 0x00, and the third and fourth bytes encompass the VLAN ID. The valid range of the VLAN ID is 1 - 4095. For example, a VLAN ID of 100 (in dec) is 00 00 00 64 in hex.

Alternatively, administrators can use the "**dhcp option 132 vlan id enabled**" parameter to enable the VLAN ID assignment transfer using DHCP feature. Option 132 provides the same functionality as Option 43 but the data format of the VLAN ID value must be 2 bytes, whereas the first and second bytes encompass the VLAN ID (the valid range of the VLAN ID being 1 - 4095).

Precedence

- LLDP values should have precedence over the DHCP
- DHCP values should have precedence over the configuration files
- DHCP should have precedence over the local values (configured via the Web UI or native phone UI)
- DHCP Option 43 should have precedence over DHCP Option 132

Configuring Option 43 to Transfer VLAN ID Assignment on a Linux DHCP Server

The following example (covering all the phones) illustrates how to configure Option 43 to transfer VLAN ID assignment on a Linux DHCP server.

```
option space AastraIPPhone;
option AastraIPPhone.cfg-server-name        code 02 = text;
option AastraIPPhone.contact-rcs            code 03 = boolean;
option AastraIPPhone.ActivateVLANHeader     code 08 = text;
option AastraIPPhone.VLAN-ID          code 09 = unsigned integer 32;

class "AastraSIP" {
match if ( (option vendor-class-identifier="AastraIPPhone6863i")
or (option vendor-class-identifier="AastraIPPhone6865i")
or (option vendor-class-identifier="AastraIPPhone6867i")
or (option vendor-class-identifier="AastraIPPhone6869i")
or (option vendor-class-identifier="AastraIPPhone6873i") );
vendor-option-space AastraIPPhone;
option AastraIPPhone.cfg-server-name
"http://192.168.174.200/aastra"; # option 43
option AastraIPPhone.contact-rcs false; # option 43
option AastraIPPhone.ActivateVLANHeader "Aastra Telecom "; # option
43
option AastraIPPhone.VLAN-ID 100;  # option 43
} # endClass
```

Enabling/Disabling DHCP Option 132 VLAN ID Using the Configuration Files

Use the following procedure to enable/disable DHCP Option 132 VLAN ID using the configuration files.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "DHCP Option Settings" on page A-17.

USING OPTION 12 HOSTNAME ON THE IP PHONE

If you set the phone to use DHCP Option 12, the phone automatically sends this option to the configuration server. This option specifies the hostname (name of the client). The name may or may not be qualified with the local domain name (based on RFC 2132). See RFC 1035 for character set restrictions.

Notes:

1. The hostname of [<model><MAC address>] automatically populates the field on initial startup of the phone. For example, for a 6867i, the “Hostname” field is automatically populated as “67i00085D164435”, where the model number is “6867i” and the MAC address is “00085D164435”.
2. If the configuration server sends the hostname back to the phone in a DHCP Reply Packet, the hostname is ignored.

An Administrator can change the “Hostname” for the DHCP Option 12 via the configuration files, the IP Phone UI, and the Mitel Web UI.

Configuring DHCP Option 12 Hostname on the IP Phone

Use the following procedures to configure DHCP Option 12 Hostname on the IP Phone.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “DHCP Option Settings” on page A-17.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Administrator Menu.**
3. Select **Network Settings**.
4. Select **Hostname**.
5. By default, the “**Hostname**” field is automatically populated with [<Model><MAC address>] of your phone (for example, 53i00085D164435).
   If you want to change the hostname, enter a hostname for your phone in the “**Hostname**” field, then press **DONE**.
   Valid values are up to 64 alpha-numeric characters. You can use a fully qualified domain name if required.
6. Restart the phone for the change to take affect.

For the 6867i/6869i/6920/6930:

1. Press or on the phone to enter the Options List.
2. Press the **Advanced** softkey.
3. Enter the Administrator password using the keypad. Default is “**22222**”.
4. Select **Network > Settings**.
5. Press ▼ or down navigation key to enter the **Hostname** field.

6. By default, the "**Hostname**" field is automatically populated with [<Model><MAC address>] of your phone (for example, 53i00085D164435).
   If you want to change the hostname, enter a hostname for your phone in the "**Hostname**" field, then press the **Save** softkey.
   Valid values are up to 64 alpha-numeric characters. You can use a fully qualified domain name if required.
7. Restart the phone for the change to take affect.

For the 6873i/6940:

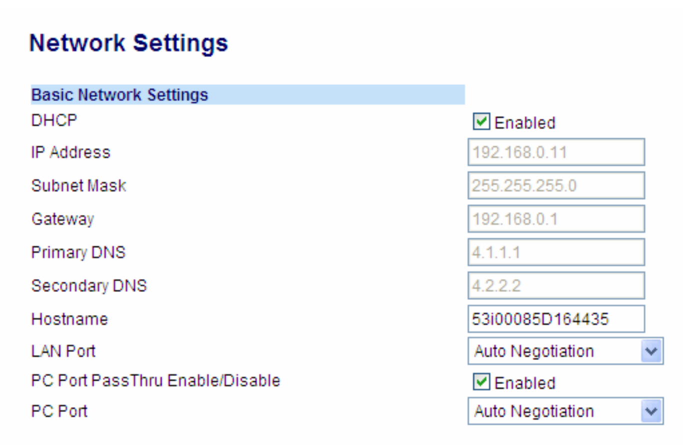
1. Press [⚙] or [⚙] on the phone to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password and press the blue Enter key. Default is "**22222**".
4. Tap the **Network** icon.

   Note: If required, swipe left on the screen to navigate to the second page of options.

5. Tap the **Settings** icon.
6. Tap the **Hostname** field.
7. By default, the "**Hostname**" field is automatically populated with [<Model><MAC address>] of your phone (for example, 53i00085D164435).
   If you want to change the hostname, enter a hostname for your phone in the "**Hostname**" field, then tap the **Save** softkey.
   Valid values are up to 64 alpha-numeric characters. You can use a fully qualified domain name if required.
8. Restart the phone for the change to take effect.

MITEL WEB UI

1. Click on **Advanced Settings->Network->Basic Network Settings.**



2. By default, the "**Hostname**" field is automatically populated with [<Model><MAC address>] of your phone (for example, 53i00085D164435).
3. If you want to change the hostname, enter a hostname for your phone in the "**Hostname**" field.
   Valid values are up to 64 alpha-numeric characters. You can use a fully qualified domain name if required.
4. Click **Save Settings** to save your changes.

   Note: Changing the "**Hostname**" field requires a reboot of your phone.

5. Click on **Operation->Reset**, and click **Restart**.

USING OPTION 77 USER CLASS ON THE IP PHONE

DHCP Option 77 User Class is sent in DHCP request packets from the phone to the configuration server. This Option 77 defines specific User Class identifiers to convey information about a phone's software configuration or about its user's preferences. For example, you can use the User Class option to configure all phones in the Accounting Department with different user preferences than the phones in the Marketing Department. A DHCP server uses the User Class option to choose the address pool for which it allocates an address from, and/or to select any other configuration option.

Notes:
1. If the User Class is not specified (left blank) in the DHCP request packet, the phone does not send the User Class DHCP Option 77.
2. Multiple User Classes inside a DHCP Option 77 are not supported.
3. DHCP Option 77 may affect the precedence of DHCP Options, dependent on the DHCP Server.

An Administrator can configure the DHCP Option 77 User Class via the configuration files and the IP Phone UI.

Configuring DHCP Option 77 User Class on the IP Phone

Use the following procedures to configure DHCP Option 77 User Class on the IP Phone.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "DHCP Option Settings" on page A-17.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Administrator Menu.**

3. Select **Network Settings**.
4. Select **DHCP Settings**.
5. Select **DHCP User Class**.
6. In the "**DHCP User Class**" field, enter a DHCP User Class to apply to your phones, then press **DONE**.
   Valid values are up to 64 alpha-numeric characters. For example, "**admin**".
7. Restart the phone for the change to take affect.

For the 6867i/6869i/6920/6930:

1. Press or on the phone to enter the Options List.
2. Press the **Advanced** softkey.
3. Enter the Administrator password using the keypad. Default is "**22222**".
4. Select **Network > Settings**.
5. Press the or down navigation key to move to the **DHCP User Class** field.
6. In the "**DHCP User Class**" field, enter a DHCP User Class to apply to your phones, then press the **Save** softkey.
   Valid values are up to 64 alpha-numeric characters. For example, "**admin**".
7. Restart the phone for the change to take affect.

For the 6873i/6940:

1. Press or on the phone to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password and press the blue Enter key. Default is "**22222**".
4. Tap the **Network** icon.

   Note: If required, swipe left on the screen to navigate to the second page of options.

5. Tap the **Settings** icon.
6. Tap the **DHCP User Class** field.
7. In the "**DHCP User Class**" field, enter a DHCP User Class to apply to your phones, then tap the **Save** softkey.
   Valid values are up to 64 alpha-numeric characters. For example, "**admin**".
8. Restart the phone for the change to take affect.

USING OPTIONS 159 AND 160 ON THE IP PHONE

In addition to DHCP options 43 and 66 already supported on the IP Phones, the phones also support DHCP Options 159 and 160. The IP Phones use the following order of precedence when deriving the configuration server parameters: 43, 160, 159, 66.

In addition, an administrator can override this order of precedence by setting a configuration parameter called, **dhcp config option override** (configuration files), **DHCP Download Options** (Mitel Web UI), or **Download Options** (IP Phone UI). Setting this parameter results in the phone only using the chosen DHCP option and ignoring the other options.

For more information about setting DHCP download preference, see "Configuration Server Download Precedence" on page 4-20.

Note: Administrators should review the updated IP phone DHCP option precedence order and configuration options to avoid potential impact to existing Mitel IP phone deployments.

Configuring DHCP Download Options on the IP Phones

Use the following procedures to configure DHCP Option Override on the IP Phone.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "DHCP Option Settings" on page A-17.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Administrator Menu.**
3. Select **Network Settings**.
4. Select **DHCP Settings**.
5. Select **Download Options**. The following list displays:
   - Any (default) - no override - uses normal precedence order of 43, 160, 159, 66.
   - Option 43
   - Option 66
   - Option 159
   - Option 160
   - Disabled (Ignores all DHCP configuration options (43, 66, 159, 160))
6. Choose an option that you want to use to override the DHCP normal precedence order, and press **Done**.
7. Restart the phone for the selection to take affect.

For the 6867i/6869i/6920/6930:

1. Press or on the phone to enter the Options List.
2. Press the **Advanced** softkey.
3. Enter the Administrator password using the keypad. Default is "**22222**".

4. Select **Network > Settings**.
5. Press the ▼ or down navigation key to move to the **DHCP Download Options** field.
6. Select one of the following DHCP download options using the ◄ and ► or left and right navigation keys.
   - Any (default) - no override - uses normal precedence order of 43, 160, 159, 66.
   - Option 43
   - Option 66
   - Option 159
   - Option 160
   - Disabled (Ignores all DHCP configuration options (43, 66, 159, 160))
7. Press the **Save** softkey.
8. Restart the phone for the selection to take affect.

For the 6873i/6940:

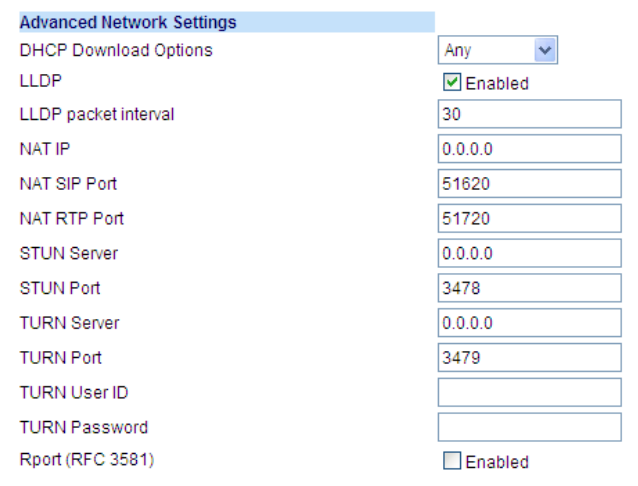
1. Press ⚙ or ⚙ on the phone to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password and press the blue Enter key. Default is "**22222**".
4. Tap the **Network** icon.

Note: If required, swipe left on the screen to navigate to the second page of options.

5. Tap the **Settings** icon.
6. Tap **DHCP Download Options** field.
7. Select one of the following DHCP download options:
   - Any (default) - no override - uses normal precedence order of 43, 160, 159, 66.
   - Option 43
   - Option 66
   - Option 159
   - Option 160
   - Disabled (Ignores all DHCP configuration options (43, 66, 159, 160))
8. Tap the **Save** softkey.
9. Restart the phone for the selection to take affect.

MITEL WEB UI

1. Click on **Advanced Settings->Network->Advanced Network Settings.**



2. In the “**DHCP Download Options**” field, select an option to use to override the normal precedence order. Valid values are:
   - Any (default) - no override - uses normal precedence order of 43, 160, 159, 66.
   - Option 43
   - Option 66
   - Option 159
   - Option 160
   - Disabled (Ignores all DHCP configuration options (43, 66, 159, 160))
3. Click **Save Settings** to save your changes.
4. Click on **Operation->Reset**, and restart the phone for the changes to take affect.

CONFIGURATION SERVER DOWNLOAD PRECEDENCE

An Administrator can set the phone’s download precedence to ignore DHCP, **(only during the boot when the remote configuration server is contacted)** and use the following precedence instead:

1. Configuration URI,
2. DHCP, and then
3. Direct configuration.

To configure the download precedence, you use the option value (-1) as the value for the “**dhcp config option override**” parameter in the configuration files. Setting this parameter to “-1” causes all DHCP configuration options to be ignored.

Configuring a Download Precedence Using the Configuration Files

Use the following procedure to configure the DHCP download precedence using the configuration files.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "DHCP Option Settings" on page A-17.

Configuring a Download Precedence Using the IP Phone UI

Use the following procedure to configure a download precedence using the IP Phone UI.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Administrator Menu.**
3. Select **Network Settings**.
4. Select **DHCP Settings**.
5. Select **Download Options**.

   Note: Disabled (Ignores all DHCP configuration options (43, 66, 159, 160))

6. Select the **Disabled** option and press **Enter**.

   Note: The "**Disabled**" download option performs the same function as the "-1" in the configuration files (ignores DHCP options)

7. Restart the phone for the selection to take affect.

For the 6867i/6869i/6920/6930:

1. Press or on the phone to enter the Options List.
2. Press the **Advanced** softkey.
3. Enter the Administrator password using the keypad. Default is "**22222**".
4. Select **Network > Settings**.
5. Press the or down navigation key to move to the **DHCP Download Options** field.
6. Select the "**Disabled**" value.

   Note: Disabled (Ignores all DHCP configuration options (43, 66, 159, 160). This option also performs the same function as the "-1" in the configuration files (ignores DHCP options)

7. Press the **Save** softkey.
8. Restart the phone for the selection to take affect.

For the 6873i/6940:

1. Press or on the phone to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password and press the blue Enter key. Default is "**22222**".
4. Tap the **Network** icon.

Note: If required, swipe left on the screen to navigate to the second page of options.

5. Tap the **Settings** icon.
6. Tap the **DHCP Download Options** field.
7. Select the "**Disabled**" value.

Note: Disabled (Ignores all DHCP configuration options (43, 66, 159, 160). This option also performs the same function as the "-1" in the configuration files (ignores DHCP options)

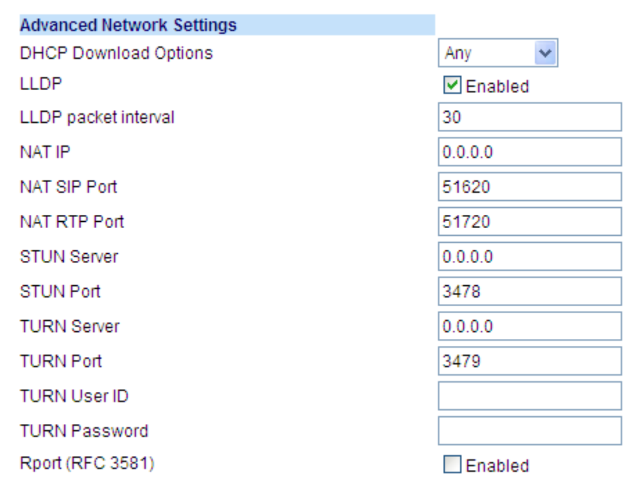
8. Tap the **Save** softkey.
9. Restart the phone for the selection to take affect.

Configuring a Download Precedence Using the Mitel Web UI

Use the following procedure to configure a download precedence using the Mitel Web UI.

MITEL WEB UI

1. Click on **Advanced Settings->Network->Advanced Network Settings.**



2. In the "**DHCP Download Options**" field, select "**Disabled**" from the list of options.

> **Note:** In the Mitel Web UI, the "**Disabled**" download option performs the same function as the "-1" in the configuration files (ignores DHCP options).

3. Click **Save Settings** to save your setting.

4. Select **Operation->Reset**, and click **Restart** to reboot the phone.

MULTIPLE DHCP SERVERS

The IP phones can receive messages from multiple DHCP servers (up to a maximum of five DHCP servers).

The phone sends DHCP discoveries every six seconds to the DHCP servers until it receives a valid DHCP offer. Within the six second time interval, before the next discovery request, any DCHP offers received by the phone from the DHCP servers are serviced in the order that they are received. If the first DHCP offer contains configuration server information (Options 43, 66, 159 or 160), the offer is accepted and the phone stops listening for additional offers. If the offer does not contain configuration server information, the phone continues to listen for DHCP messages and reviews the next received offers until an offer containing configuration server information is found. If no DHCP offers containing configuration server information are received within the six second time interval, the DHCP offer that was received first is used.

Notes:

1. If the DHCP Download Options parameter is enabled with a value (Option 43, Option 66, Option 159, or Option 160), the phone checks the override option setting before timing out.
2. If the DHCP servers do not have any of the Options (43, 66, 159, and 160) configured, the phone's boot up process of will take approximately six more seconds.
3. In certain multiple DHCP server scenarios, due to the configuration of the servers as well as the response time and speed of the servers, a DHCP offer with no configuration server information may be accepted instead of an offer with configuration server information.
   For example, when three DHCP servers are available (the fastest with no configuration server information defined, the second fastest with no configuration server information defined but with an IP reserved for the phone, and the slowest with configuration server information defined) the phone will initially select the offer from the slowest server as it contains configuration server information. However, the phone will then send a broadcast request, whereby the second fastest server will reply with a NACK before the slowest server's ACK reply, causing the phone to send another broadcast request and triggering the phone to change to a selecting state. The fastest server will then reply with an ACK and, due to the state change, the phone will accept the fastest server's offer.

WARNING: USERS CURRENTLY USING MULTIPLE DHCP SERVERS ON A SINGLE NETWORK COULD BE AFFECTED BY THIS FEATURE.

DNS CACHING

The IP phones have the ability to cache DNS requests as referenced in RFC1035 and RFC2181. The phone caches DNS lookups according to the TTL field, so that the phone only performs another lookup for an address when the TTL expires.

CONFIGURING NETWORK SETTINGS MANUALLY

If you disable DHCP on your phone, you need to configure the following network settings manually:

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

Note: If you disable DHCP on the phone, the phone uses the TFTP protocol as the default server protocol. If you want to specify a different protocol to use, see "Configuration Server Protocol" on page 4-104.

You can configure the network settings using the configuration files, the IP phone UI, or the Mitel Web UI.

Errors Messages Display when Incorrect Network Settings Entered

The IP Phone UI AND the Mitel Web UI immediately notify the Administrator if an incorrect value is being entered for the following network parameters in the IP Phone UI and the Mitel Web UI:

- A 0.0.0.0 entered as values for the **IP Address**, **Subnet Mask** and **Gateway** parameters
- **IP Address** and **Gateway** IP address parameter values entered exactly the same
- **Gateway** IP address and the **IP address** parameter values configured on the same subnet

If you configure the Gateway parameter and the IP Address parameter on the same subnet, the following error message displays:

```
"Gateway IP address and the IP address parameter values configured
are not on the same subnet".
```

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Network Settings" on page A-13.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Administrator Menu.**
3. Select **Network Settings**.
4. Select **IP Address** and enter the IP address of the phone.
5. Select **Subnet Mask** and enter the subnet mask.
6. Select **Gateway** and enter the gateway address.
7. Select **DNS** and enter a Primary and/or Secondary DNS server.
8. Press **Done** to save the changes.
   The IP phone is manually configured.

For the 6867i/6869i/6920/6930:

Note: To manually configure DHCP parameters, DHCP must be disabled on the phone.

1. Press or on the phone to enter the Options List.
2. Press the **Advanced** softkey.
3. Enter the Administrator password using the keypad. Default is "**22222**".
4. Select **Network > Settings**.

5. In the **IP Address** field, enter the IP address of your phone. The IP Address must be entered in the format 0.0.0.0; for example, 192.168.0.7.
6. In the **Subnet Mask** field, enter the subnet mask address. For example, 255.255.0.0.
7. In the **Gateway** field, enter the IP address of your gateway. The Gateway must be entered in the format 0.0.0.0; for example, 192.168.0.1.
8. If required, enter the Primary DNS and/or Secondary DNS in the respective fields. The IP addresses must be entered in the format 0.0.0.0.
9. Press the **Save** softkey.
   The IP Phone is manually configured.

For the 6873i/6940:

Note: To manually configure DHCP parameters, DHCP must be disabled on the phone.

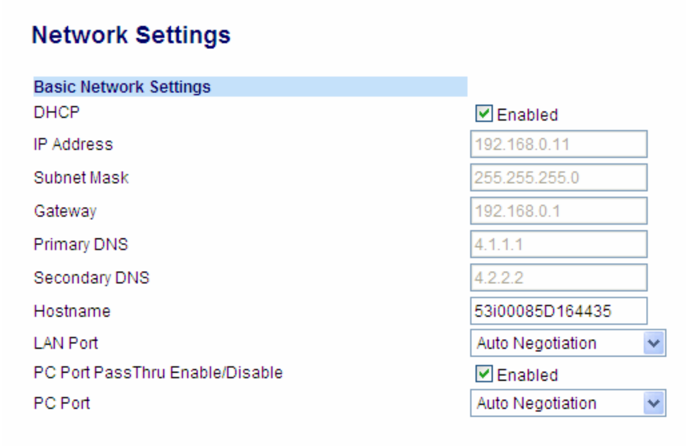
1. Press or on the phone to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password and press the blue Enter key. Default is “**22222**”.
4. Press the **Network** icon.

   Note: If required, swipe left on the screen to navigate to the second page of options.

5. Tap the **Settings** icon.
6. In the **IP Address** field, enter the IP address of your phone. The IP Address must be entered in the format 0.0.0.0; for example, 192.168.0.7.
7. In the **Subnet Mask** field, enter the subnet mask address. For example, 255.255.0.0.
8. In the **Gateway** field, enter the IP address of your gateway. The Gateway must be entered in the format 0.0.0.0; for example, 192.168.0.1.
9. If required, enter the Primary DNS and/or Secondary DNS in the respective fields. The IP addresses must be entered in the format 0.0.0.0.
10. Tap the **Save** softkey.
    The IP Phone is manually configured.

MITEL WEB UI

1. Click on **Advanced Settings->Network->Basic Network Settings.**



2. Enter an IP address of the phone in the **IP Address** field.
3. Enter a subnet mask in the **Subnet Mask** field.
4. Enter a gateway address in the **Gateway** field.
5. Enter a Primary DNS in the **Primary DNS** field, and/or a secondary DNS in the **Secondary DNS** field.
6. Click **Save Settings** to save your settings.
   The IP phone is manually configured.

ETHERNET

Ethernet is the computer networking technology for local area networks (LANs). You use the LAN Port to connect to a LAN using a twisted pair 10BASE-T cable to transmit 10BASE-T Ethernet. You use the PC Port to connect to the configuration server (your PC).

The Ethernet sub-menu allows you to change the speed and duplex method of the IP phone’s LAN and PC ports as well as enable or disable port mirroring.

There are two Ethernet ports on the rear of the IP phones: LAN Port and PC Port. Using the Mitel Web UI, you can select the type of transmission you want these ports to use to communicate over the LAN. The IP phones support each of the following methods of transmission:

- Auto-negotiation
- Half-duplex (10Mbps, 100 Mbps, or 1000Mbps [if applicable])
- Full-duplex (10Mbps, 100 Mbps, or 1000Mbps [if applicable])

Auto-negotiation

Auto-negotiation is when two connected devices choose common transmission parameters. In the auto-negotiation process, the connected devices share their speed and duplex capabilities and connect at the highest common denominator (HCD). Auto-negotiation can be used by devices that are capable of different transmission rates (such as 10Mbit/sec and 100Mbit/sec for the 6863i and 6905 and 1000Mbit/sec for the 6865i, 6867i, 6869i, 6873i, 6910, 6920, 6930, and 6940), different duplex modes (half duplex and full duplex) and/or different standards at the same speed. You can set the LAN and PC Ports on the IP phones to auto-negotiate during transmission.

Note: After connecting a device to the PC port, a reboot may be required before the connected device can acquire network connectivity.

Half-Duplex (10Mbps, 100Mbps, or 1000Mbps)

Half-duplex data transmission means that data can be transmitted in both directions on a signal carrier, but not at the same time. For example, on a LAN using a technology that has half-duplex transmission, one device can send data on the line and then immediately receive data on the line from the same direction in which data was just transmitted. Half-duplex transmission implies a bidirectional line (one that can carry data in both directions). On the 6863i and 6905 IP phones, you can set the half-duplex transmission to transmit in 10Mbps or in 100Mbps. For the 6865i, 6867i, 6869i, 6873i, 6910, 6920, 6930, and 6940 IP phones, you can set the half-duplex transmission to transmit in 1000Mbps.

Full-Duplex (10Mbps, 100Mbps or 1000Mbps)

Full-duplex data transmission means that data can be transmitted in both directions on a signal carrier at the same time. For example, on a LAN with a technology that has full-duplex transmission, one device can be sending data on the line while another device is receiving data. Full-duplex transmission implies a bidirectional line (one that can move data in both directions). On the 6863i and 6905 IP phones, you can set the full-duplex transmission to transmit in 10Mbps or in 100Mbps. For the 6865i, 6867i, 6869i, 6873i, 6910, 6920, 6930, and 6940 IP phones, you can set the full-duplex transmission to transmit in 1000Mbps.

Configuring the LAN Port and PC Port

You can configure the Ethernet port transmission method to use on the IP phones using the configuration files, the IP Phone UI, or the Mitel Web UI.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Network Settings” on page A-13.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Administrator Menu.**

3. Select **Network Settings**.
4. Select **Ethernet**.
5. Select **LAN Port Link.**
6. Select a negotiation method to use on port 0 and press **Done**. Valid values are:
   - AutoNegotiation
   - Full 10Mbps
   - Full 100Mbps
   - Full 1000Mbps (applicable for the 6865i)
   - Half 10Mbps
   - Half 100Mbps
   - Half 1000Mbps (applicable for the 6865i)
7. Default is **AutoNegotiation.**
8. Select **PC Port Link**.
9. Select a negotiation method to use on port 1and press **Done**. Valid values are:
   - AutoNegotiation
   - Full 10Mbps
   - Full 100Mbps
   - Full 1000Mbps (applicable for the 6865i)
   - Half 10Mbps
   - Half 100Mbps
   - Half 1000Mbps (applicable for the 6865i)
10. Default is **AutoNegotiation**.
11. Press **Done** (3 times) to finish configuring the configuration server protocol for the IP phone.

    Note: The session prompts you to restart the IP phone to apply the configuration settings.

12. Select **Restart**.

For the 6867i/6869i/6920/6930:

1. Press or on the phone to enter the Options List.
2. Press the **Advanced** softkey.
3. Enter the Administrator password using the keypad. Default is “**22222**”.
4. Select **Network > Ethernet Ports**.
5. With **LAN Port** highlighted, press the or the right navigation key and select a negotiation method to use on port 0. Valid values are:
   - AutoNegotiation
   - Full 10Mbps

- Full 100Mbps
- Full 1000Mbps
- Half 10Mbps
- Half 100Mbps
- Half 1000Mbps

6. Default is **AutoNegotiation.**
7. Press the ◀ or left navigation key and press down to highlight **PC Port**.
8. Select a negotiation method to use on port 1. Valid values are:
   - AutoNegotiation
   - Full 10Mbps
   - Full 100Mbps
   - Full 1000Mbps
   - Half 10Mbps
   - Half 100Mbps
   - Half 1000Mbps
9. Default is **AutoNegotiation**.
10. Press the **Save** softkey.
11. Restart the phone for the selection to take affect.

For the 6873i/6940:

1. Press ⚙ or ⚙ on the phone to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password and press the blue Enter key. Default is “**22222**”.
4. Tap the **Network** icon.

   Note: If required, swipe left on the screen to navigate to the second page of options.

5. Tap the **Ethernet Ports** icon.
6. With **LAN Port** highlighted, select a negotiation method to use on port 0. Valid values are:
   - AutoNegotiation
   - Full 10Mbps
   - Full 100Mbps
   - Full 1000Mbps
   - Half 10Mbps
   - Half 100Mbps
   - Half 1000Mbps

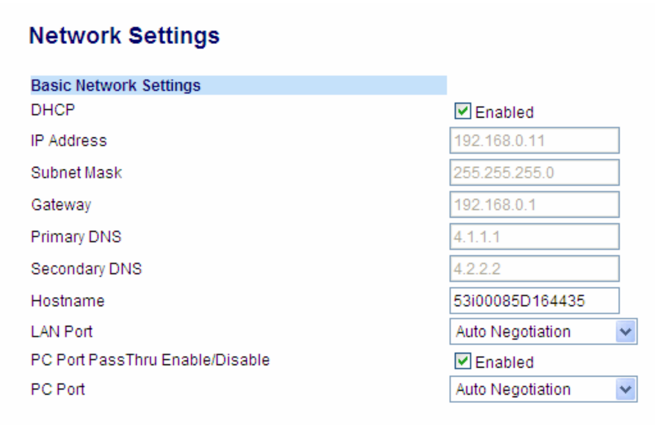
   Default is **AutoNegotiation.**

7. Tap **PC Port**.
8. Select a negotiation method to use on port 1. Valid values are:
   - AutoNegotiation
   - Full 10Mbps
   - Full 100Mbps
   - Full 1000Mbps
   - Half 10Mbps
   - Half 100Mbps
   - Half 1000Mbps

   Default is **AutoNegotiation**.
9. Tap the **Save** softkey.
10. Restart the phone for the selection to take affect.

MITEL WEB UI

1. Click on **Advanced Settings->Network->Basic Network Settings.**



2. In the “**LAN Port**” field, select a negotiation method to use on port 0. Valid values are:
   - Auto Negotiation
   - Full Duplex, 10Mbps
   - Full Duplex, 100Mbps
   - Full Duplex, 1000Mbps (applicable for the 6865i, 6867i, 6869i, and 6873i IP phones only)
   - Half Duplex, 10Mbps
   - Half Duplex, 100Mbps
   - Half Duplex, 1000Mbps (applicable for the 6865i, 6867i, 6869i, and 6873i IP phones only)

   Default is Auto Negotiation.
3. In the “**PC Port**” field, select a negotiation method to use on port 1. Valid values are:

- Auto Negotiation
- Full Duplex, 10Mbps
- Full Duplex, 100Mbps
- Full Duplex, 1000Mbps (applicable for the 6865i, 6867i, 6869i, and 6873i IP phones only)
- Half Duplex, 10Mbps
- Half Duplex, 100Mbps
- Half Duplex, 1000Mbps (applicable for the 6865i, 6867i, 6869i, and 6873i IP phones only)

Default is **Auto Negotiation**.

4. Click **Save Settings** to save your settings.

Port Mirroring

Port mirroring allows you to mirror the LAN and PC ports to and from the phone for debugging purposes.

You can enable or disable Port Mirroring option on the IP phone using the configuration files or the IP Phone UI.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Network Settings" on page A-13.

IP PHONE UI

For 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Administrator Menu.**
3. Select **Network Settings**.
4. Select **Ethernet**.
5. Select **Port Mirroring.**
6. Select **Enable** or **Disable** (default) and press **Done**.

For 6867i/6869i/6920/6930:

1. Press or on the phone to enter the Options List.
2. Press the **Advanced** softkey.
3. Enter the Administrator password using the keypad and press **Enter** softkey. Default is "**22222**".
4. Navigate to **Network > Ethernet** using the navigation keys and press the **Select** softkey.

5. With **Port Mirroring** highlighted, press ▶ or the right navigation key and use the up and down navigation keys to enable or disable (default) port mirroring.
6. Press the **Save** softkey to save your changes.

For 6873i/6940:

1. Press ⚙ or ⚙ on the phone to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password and tap the **Enter** softkey. Default is “**22222**”.
4. Tap the **Network** icon.

Note: If required, swipe left on the screen to navigate to the second page of options.

5. Tap the **Ethernet** icon and tap **Port Mirroring.**
6. With Port Mirroring highlighted, tap **Enable** or **Disable** (default) to enable or disable port mirroring.
7. Tap the **Save** softkey to save your changes.

ADVANCED NETWORK SETTINGS

You can set advanced network settings on the IP phone such as Network Time Protocol (NTP) Time Servers, Virtual LAN (VLAN), and Quality of Service (QoS) using the Mitel Web UI or the configuration files.

Note: The available advanced network parameters via the IP phone UI are VLAN and QoS only.

SIP AND TLS SOURCE PORTS

A System Administrator can configure the SIP and TLS source ports on the IP Phone. Previously, the IP phone used default values (**5060** for UDP/TCP and **5061** for TLS). The two new parameters for configuring the SIP and TLS source ports are:

- sip local port
- sip local tls port

You can configure the SIP and TLS source ports using the configuration files or the Mitel Web UI. **After configuring these parameters, you must reboot the phone.**

Notes:

1. By default, the IP phones use symmetric UDP signaling for outgoing UDP SIP messages. When symmetric UDP is enabled, the IP phone generates and listens for UDP messages using port 5060.If symmetric UDP signaling is disabled, the phone sends from random ports but it listens on the configured SIP local port. Refer to "Symmetric UDP Signaling," on page 33 for more information.
2. The IP phones also use symmetric TLS signaling for outgoing TLS SIP messages by default. When symmetric TLS is enabled, the IP phone uses port 5061 as the persistent TLS connection source port. When symmetric TLS signaling is disabled, the IP phone chooses a random persistent TLS connection source port for TLS messages from the TCP range (i.e. 49152...65535) after each reboot regardless of whether the parameter “sip outbound support” is enabled or disabled. Refer to "Symmetric TLS Signaling," on page 34 for more information.

Configuring SIP and TLS Source Ports Using the Configuration Files

You use the following parameters to configure SIP and TLS ports:

- sip local port
- sip local tls port

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the sections:

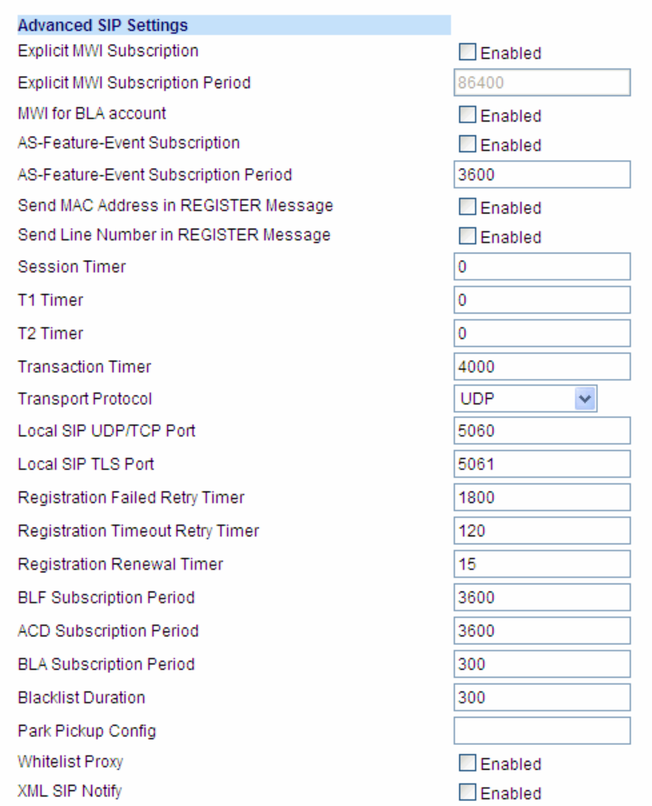
- “Local SIP UDP/TCP Port Setting” on page A-45.
- “Local SIP TLS Port” on page A-46.

Configuring SIP and TLS Source Ports Using the Mitel Web UI

Use the following procedure to configure SIP and TLS source ports using the Mitel Web UI.

MITEL WEB UI

1. Click on **Advanced Settings->Global SIP->Advanced SIP Settings.**



2. The “**Local SIP UDP/TCP Port**” field has a default value of **5060**. Change this value if required to a value greater than 1024 and less than 65535.

   Note: It is recommended that you avoid the conflict RTP port range in case of a UDP transport.

3. The “**Local SIP TLS Port**” field has a default value of **5061**. Change this value if required to a value greater than 1024 and less than 65535.

   Note: It is recommended that you avoid the conflict with any TCP ports being used. For example: WebUI HTTP server on 80/tcp and HTTPS on 443/tcp.

4. Click **Save Settings** to save your changes.

HTTPS CLIENT/SERVER CONFIGURATION

HTTPS is a Web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS uses Secure Socket Layer (SSL) or Transport Layer Security (TLS) as a sublayer under its regular HTTP application layering. SSL is a commonly-used protocol for managing the security of a message transmission on the Internet. It uses a 40-bit key size f

or the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange. TLS is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to SSL.

Note: HTTPS uses port 443 instead of HTTP port 80 in its interactions with the TCP/IP lower layer.

When an HTTPS client opens and closes its TCP socket, the SSL software respectively handshakes upon opening and disconnects upon closing from the HTTPS server. The main HTTPS client functions are:

- Downloading of configuration files and firmware images.
- Downloading of script files based on an “HTTPS://” URL supplied by a softkey definition.

The HTTPS server provides HTTP functionality over secure connections. It coexists with the HTTP server but has its own set of tasks. The main HTTPS server functions are:

- Delivery of web page content to a browser client over a secure connection.
- Execution of HTTP GET and POST requests received over a secure connection.

Using the configuration files, the IP phone UI, or the Mitel Web UI, you can configure the following regarding HTTPS:

- Specify HTTPS security client method to use (TLS Preferred, TLS 1.0, TLS 1.1, TLS 1.2)
- Enable or disable HTTP to HTTPS server redirect function
- HTTPS server blocking of XML HTTP POSTS to the phone

Prior to Release 5.0.0 SP2, the phone initiated a TLS connection using the following available options

- TLS 1.0 - The phone will attempt to communicate using TLS 1.0 only.
- TLS 1.1 - The phone will attempt to communicate using TLS 1.1 only.
- TLS 1.2 - The phone will attempt to communicate using TLS 1.2 only.

With Release 5.0.0 SP2, the phone initiates a TLS connection with the highest supported TLS version and falls back to the selected protocol version.

If the TLS version is set to TLSv1.0, the phone starts the negotiation with TLSv1.2.

- If the server supports TLSv1.2, the phone communicates on TLSv1.2

- If the server supports TLSv1.1, the phone communicates on TLSv1.1
- If the server supports TLSv1.0, the phone communicates on TLSv1.0

If TLS version is set to TLSv1.1, the phone starts the negotiation with TLSv1.2.

- If the server supports TLSv1.2, the phone communicates on TLSv1.2
- If the server supports TLSv1.1, the phone communicates on TLSv1.1
- If the server supports TLSv1.0, the phone terminates the TLS connection as the minimum TLS version is set to TLSv1.1

If the TLS version is set to TLSv1.2, the phone starts the negotiation with TLSv1.2.

- If the server supports TLSv1.2, the phone communicates on TLSv1.2.
- If the server supports TLSv1.1, the phone terminates the TLS connection as the minimum TLS version is set to TLSv1.2.
- If the server supports TLSv1.0, the phone terminates the TLS connection as the minimum TLS version is set to TLSv1.2.

Configuring HTTPS Client and Server Settings

Use the following procedures to configure the HTTPS client and server for the IP phones.

Note: To enable or disable the IP phones to use the HTTPS protocol as the configuration server, see the section, "Configuring the Configuration Server Protocol" on page 4-104.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "HTTPS Client and Server Settings" on page A-47.

For the 6863i/6865i/6905/6910:

IP PHONE UI

1. Press ⚙ or ⚙ on the phone to enter the Options List.
2. Select **Administrator Menu.**
3. Select **Configuration Server.**
4. Select **HTTPS Settngs.**

Configure HTTPS Client:

5. Select **HTTPS Client.**
6. Select **Client Method.**
7. Press **Change** to select a client method to use for HTTPS. Valid values are:
   - **TLS 1.0** - The phone will attempt to communicate using TLS 1.0 only.

- **TLS 1.1** - The phone will attempt to communicate using TLS 1.1 only.
- **TLS 1.2** - The phone will attempt to communicate using TLS 1.2 only.
- **TLS Preferred** - The phone will negotiate with the highest possible TLS version during the handshake.

Note: This implementation has changed, see Chapter 4, "HTTPS Client/Server Configuration" on page 4-36.

8. Press **Done** to save the changes.

Configure HTTPS Server:

9. Select **HTTPS Server.**
10. Select **HTTP->HTTPS.**
11. Press **Change** to select "**Yes**" or "**No**". Default is "**No**".
Enabling this feature redirects the HTTP protocol to HTTPS.
12. Press **Done** to save the changes.
13. Select **XML HTTP POSTs.**
14. Press **Change** to select "**Yes**" or "**No**". Default is "**No**".
Enabling this feature blocks XML HTTP POSTs from the IP Phone.
15. Press **Done** (4 times) to finish.

Note: The session prompts you to restart the IP phone to apply the configuration settings.

16. Select **Restart**.

For the 6867i/6869i/6920/6930:

IP PHONE UI

1. Press or on the phone to enter the Options List.
2. Press the **Advanced** softkey.
3. Enter the Administrator password using the keypad. Default is "**22222**".
4. Select **Configuration Server**.
5. In the **Download Protocol** field, select **HTTPS**.

Configure HTTPS Client:

6. In the **HTTPS Client Method** field, press a client method value to use for HTTPS. Valid values are:
   - **TLS 1.0** - The phone will attempt to communicate using TLS 1.0 only.
   - **TLS 1.1** - The phone will attempt to communicate using TLS 1.1 only.
   - **TLS 1.2** - The phone will attempt to communicate using TLS 1.2 only.
   - **TLS Preferred** - The phone will negotiate with the highest possible TLS version during the handshake.

   Note: This implementation has changed, see Chapter 4, "HTTPS Client/Server Configuration" on page 4-36.

Configure HTTPS Server:

7. In the **HTTPS Server** field, enter the IP address of the HTTPS server in the text box. Enabling this feature redirects the HTTP protocol to HTTPS.
8. Press the **Save** softkey.
9. Restart the phone for the selection to take affect.

For the 6873i/6940:

IP PHONE UI

1. Press or on the phone to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password and press the blue Enter key. Default is "**22222**".
4. Tap the **Configuration Server** icon.

   Note: If required, swipe left on the screen to navigate to the second page of options.

5. In the **Download Protocol** field, select **HTTPS**.

Configure HTTPS Client:

6. In the **HTTPS Client Method** field, press a client method value to use for HTTPS. Valid values are:
   - **TLS 1.0** - The phone will attempt to communicate using TLS 1.0 only.
   - **TLS 1.1** - The phone will attempt to communicate using TLS 1.1 only.
   - **TLS 1.2** - The phone will attempt to communicate using TLS 1.2 only.
   - **TLS Preferred** - The phone will negotiate with the highest possible TLS version during the handshake.

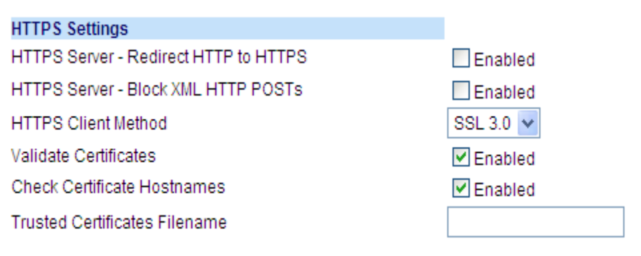
   Note: This implementation has changed, see Chapter 4, “HTTPS Client/Server Configuration” on page 4-36.

Configure HTTPS Server:

7. In the **HTTPS Server** field, enter the IP address of the HTTPS server. Enabling this feature redirects the HTTP protocol to HTTPS.
8. Tap the **Save** softkey.
9. Restart the phone for the selection to take affect.

MITEL WEB UI

1. Click on **Advanced Settings->Network->HTTPS Settings**.



2. Select an HTTPS client method to use from the **HTTPS Client Method** field. Valid values are:
   - **TLS 1.0** - The phone will attempt to communicate using TLS 1.0 only.
   - **TLS 1.1** - The phone will attempt to communicate using TLS 1.1 only.
   - **TLS 1.2** - The phone will attempt to communicate using TLS 1.2 only.
   - **TLS Preferred** - The phone will negotiate with the highest possible TLS version during the handshake.

   Note: This implementation has changed, see Chapter 4, “HTTPS Client/Server Configuration” on page 4-36.

3. Enable HTTP to HTTPS redirect by checking the **HTTPS Server - Redirect HTTP to HTTPS** field check box. (Disable this field by unchecking the check box). Default is disabled.
4. Enable the blocking of XML HTTP POSTs by the HTTPS server by checking the **HTTPS Server - Block XML HTTP POSTs** field check box. (Disable this field by unchecking the check box). Default is disabled.

5. Click **Save Settings** to save your settings.

HTTPS 302-REDIRECTION SUPPORT

The 6800 and 6900 series IP Phones now support the 302-redirection response if the configuration protocol is set to HTTPS only.

> **Note:** Double or multiple redirection is not supported. For example, if the phone sends a HTTPs request to server1 and server1 sends 302 redirections to server2, then the phone contacts server2 and server2 sends the redirection to server 1. The phone does not try to contact server1.

HTTPS LOCAL CERTIFICATE SUPPORT/MUTUAL AUTHENTICATION

The 6800 and 6900 series IP phones provide a built-in common 2048-bit HTTPs certificate allowing for mutual authentication between the HTTPs server and the phones during an HTTPs session. The certificate can be used for file download processes (e.g. configuration file download for secure provisioning) and for HTTPs/XML requests. You may download the client certificate from the Software Download Center accessible through Mitel MiAccess Portal.

HTTPS SERVER CERTIFICATE VALIDATION

The HTTPS client on the IP Phones support validation of HTTPS certificates. This feature supports the following:

- SHA-1 and SHA-2 signed certificates from various certificate vendors as detailed in Appendix F, "Certificates Supported in This Software Release"
- User-provided certificates
- Checking of hostnames
- SSL Wildcard certificate (i.e. SSL certificate specifying the Common Name as a wildcard [e.g. CN=*.company.com]) support.
- Checking of certificate expiration
- Ability to disable any or all of the validation steps
- Phone displays a message when a certificate is rejected (except on check-sync operations)

All validation options are enabled by default.

Certificate Management

Mitel Provided Certificates

The phones come pre-loaded with root and intermediate SHA-1 and SHA-2 certificates various certificate vendors.For detailed information regarding the certificates supported on the IP phones, see Appendix F, "Certificates Supported in This Software Release".

User Provided Certificates

The administrator has the option to upload their own certificates onto the phone. The phone downloads these certificates in a file of .PEM format during boot time after configuration downloads. The download of the user-provided certificates are based on a filename specified in the configuration parameter, **https user certificates** (**Trusted Certificates Filename** in the Mitel Web UI; user-provided certificates are not configurable via the IP Phone UI). The user-provided certificates are saved on the phone between firmware upgrades but are deleted during a factory default (or if the configured value in the **https user certificates/Trusted Certificates Filename** parameter/setting is changed or omitted).

Note: Certificates that are signed by providers other than those listed in Appendix F, “Certificates Supported in This Software Release” do not verify on the phone by default. The user can overcome this by adding the root certificate of their certificate provider to the user-provided certificate .PEM file.

Certificate Validation

Certificate validation is enabled by default. Validation occurs by checking that the certificates are well formed and signed by one of the certificates in the trusted certificate set. It then checks the expiration date on the certificate, and finally, compares the name in the certificate with the address for which it was connected.

If any of these validation steps fail, the connection is rejected. Certificate validation is controlled by three parameters which you can configure via the configuration files, the IP Phone UI, or the Mitel Web UI:

- **https validate certificates** - Enables/disables validation.
- **https validate hostname** - Enables/disables the checking of the certificate commonName against the server name.

SSL Certificate Subject Alternative Name (SAN) Support

The 6800 and 6900 Series SIP phones support Subject Alternative Names (SANs) when validating SSL certificates. SANs allow Administrators to specify a list of hostnames that can be protected by a single SSL certificate.

When the "**https validate hostname**" ("**Check Hostnames**" option on the Web UI) is enabled, the names defined as SANs in a certificate are used for matching against the phone's configured server name. If no matches are found, the common name in the certificate is used.

The following considerations should be noted:

- When matching the configured server name against names from the certificate SAN, both DNS names and IP address names from the SAN are selected. Other names such as the Service (SRV) record names are ignored.
- Multiple DNS names and IP address names from the certificate SAN are supported.
- If the phone's configured HTTPS server name is a DNS name, wildcard matching is supported. However, only the first label of the DNS name will be wildcard matched. The remaining labels of the DNS name are matched identically.
- The first label of a DNS name from a certificate SAN can be in the following format:

  <LH>*<RH>.<Any Other Labels>.com

where LH and RH can be any valid string or empty and the asterisk (i.e "*") is the wildcard character. For example, service providers can add DNS names like the following in the SAN of their certificates:

- *.example.com
- *xyz.example.com
- xyz*.example.com
- abc*xyz.example.com

- If the phone's configured HTTPS server name is an IP address, it will be matched identically with the DNS names and IP address names from the certificate SAN.

User Interface

Certificate Rejection

When the phone rejects a certificate, it displays, ***"Bad Certificate"*** on the LCD.

For Verisign Certificate Rejection

The phones support 2048-bit Verisign certificates. In case of a certificate error, detailed descriptions can be found from the error message list in the phone status menu.

The following error descriptions are now available:

- No Certificate
- Bad Certificate
- Unsupported Certificate
- Certificate Revoked
- Certificate Expired
- Certificate Unknown

Configuring HTTPS Server Certificate Validation

An Administrator can configure HTTPS Server Certificate Validation using the configuration files, the IP Phone UI, or the Mitel Web UI. Use the following procedures to configure the HTTPS server certificate validation on the IP phones.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "HTTPS Server Certificate Validation Settings" on page A-48.

For the 6863i/6865i/6905/6910:

IP PHONE UI

1. Press or on the phone to enter the Options List.
2. Select **Administrator Menu.**
3. Select **Configuration Server**.
4. Select **HTTPS Settings->Cert. Validation**.
   The following list displays:
   - Enable
   - Check Hostnames

Enable/Disable HTTPS Server Certificate Validation:

5. Select **Enable**.
6. Press **Change** to toggle the **"Enable"** field to **"Yes" or "No".**

Note: If you are using HTTPS as a configuration method, and use a self signed certificate, you must set this field to "**No**" before upgrading to Release 2.3 of the IP Phones.

7. Press **DONE** to save the change and return to the Certificates screen.

Note: This change is immediately applied after pressing **DONE**.

Enable/Disable HTTPS Validate Hostname:

8. Select **Check Hostnames**.
9. Press **Change** to toggle the **"Check Hostnames"** field to **"Yes" or "No".**
10. Press **DONE** to save the change and return to the Certificates screen.

Note: This change is immediately applied after pressing **DONE**.

For the 6867i/6869i/6920/6930:

IP PHONE UI

1. Press or on the phone to enter the Options List.
2. Press the **Advanced** softkey.
3. Enter the Administrator password using the keypad. Default is "**22222**".
4. Select **Configuration Server**.
5. In the **Download Protocol** field, select **HTTPS**.

Enable/Disable HTTPS Server Certificate Validation:

6. In the **Cert. Validation** checkbox, press the or **Select** button to enable the feature.

Enable/Disable HTTPS Validate Hostname:

7. In the **Check Hostnames** checkbox, press the or **Select** button to enable the feature.
8. Press the **Save** softkey.
9. Restart the phone for the selection to take affect.

For the 6873i/6940:

IP PHONE UI

1. Press or on the phone to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password using the keypad. Default is “**22222**”.
4. Tap the **Configuration Server** icon.

Note: If required, swipe left on the screen to navigate to the second page of options.

5. In the **Download Protocol** field, select **HTTPS**.

Enable/Disable HTTPS Server Certificate Validation:

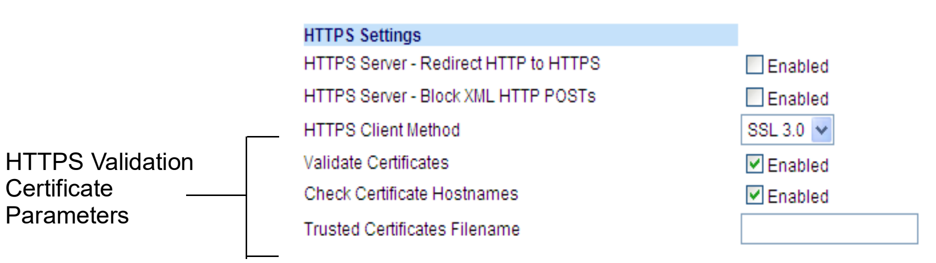
6. In the **Cert. Validation** checkbox, tap the checkbox to enable the feature.

Enable/Disable HTTPS Validate Hostname:

7. In the **Check Hostnames** checkbox, tap the checkbox to enable the feature.
8. Tap the **Save** softkey.
9. Restart the phone for the selection to take affect.

MITEL WEB UI

1. Click on **Advanced Settings->Network->HTTPS Settings.**



2. The **“Validate Certificates”** field is enabled by default. To disable validation of certificates, click the check mark in the box to clear the check mark.

When this parameter is enabled, the HTTPS client performs validation on SSL certificates before accepting them.

Notes:

1. This parameter is immediately applied after clicking the **SAVE SETTINGS** button.
2. If you are using HTTPS as a configuration method, and use a self signed certificate, you must disable (uncheck) this field before upgrading to Release 2.3 of the IP Phones.

3. The **"Check Certificate Hostnames**" field is enabled by default. To disable validation of hostnames, click the check mark in the box to clear the check mark.

   Note: This parameter is immediately applied after clicking the **SAVE SETTINGS** button.

4. If you require the download of User-provided certificates in a PEM formatted file, enter the file name in the format <filename.pem> in the "**Trusted Certificates Filename**" field. For example:
   trustedCerts.pem
   This parameter specifies a file name for a .PEM file located on the configuration server. This file contains the User-provided certificates in PEM format. These certificates are used to validate peer certificates.

   Notes:

   1. You must disable the "**Validate Certificates**" field in order for the phone to accept the User-provided certificates.
   2. This parameter requires you restart the phone in order for it to take affect.

5. Click **Save Settings** to save your changes.
6. If you entered a filename in the "**Trusted Certificates Filename**" field, click on **Operation->Reset**, and restart the phone for the changes to take affect.

VIRTUAL LAN (OPTIONAL)

Virtual Local Area Network (VLAN) is a feature on the IP phone that allows for multiple logical Ethernet interfaces to send outgoing RTP packets over a single physical Ethernet as described in IEEE Std 802.3. On the IP phone, you configure a VLAN ID that associates with the physical Ethernet port.

By configuring specific VLAN parameters, the IP phones have the capability of adding and removing tags, and processing the ID and priority information contained within the tag.

Note: All latest VLAN functionality is backwards compatible with IP Phone Releases 1.3 and 1.3.1.

VLAN on the IP phones is disabled by default. When you enable VLAN, the IP phone provides defaults for all VLAN parameters. If you choose to change these parameters, you can configure them using the configuration files, the IP Phone UI, or the Mitel Web UI.

The following sections describe the VLAN features you can configure on the IP phones.

TYPE OF SERVICE (TOS), QUALITY OF SERVICE (QOS), AND DIFFSERV QOS

ToS is an octet as a field in the standard IP header. It is used to classify the traffic of the different QoSs.

QoS provides service differentiation between IP packets in the network. This service differentiation is noticeable during periods of network congestion (for example, in case of contention for resources) and results in different levels of network performance.

Port 0 is the Ethernet LAN Port connected to the network. Port 1 is the Ethernet PC Port used for passthrough to a PC.

Differentiated Service (DiffServ) QoS is class-based where some classes of traffic receive preferential handling over other traffic classes.

The Differentiated Services Code Point (DSCP) value is stored in the first six bits of the ToS field. Each DSCP specifies a particular per-hop behavior that is applied to a packet.

The following parameters allow an administrator to configure ToS, QoS, and DiffServ QoS for VLAN:

PARAMETERS IN CONFIGURATION FILES	PARAMETERS IN MITEL WEB UI
GLOBAL	
tagging enabled	VLAN Enable
priority non-ip	Priority, Non-IP Packet
LAN PORT	
vlan id	VLAN ID
tos priority map	SIP Priority
tos priority map	RTP Priority
tos priority map	RTCP Priority
PC PORT	
vlan id port 1	VLAN ID
QoS eth port 1 priority	Priority

Notes:

1. In order for the software to successfully maintain connectivity with a network using VLAN functionality, the IP phone reboots if you modify the "**tagging enabled**" (**VLAN Enable** in the Web UI), "**vlan id**", or "**vlan id port 1**" parameters.
2. Setting the LAN Port VLAN ID (**vlan id**) to 4095 and PC Port VLAN ID (**vlan id port 1**) to any ID from 1 to 4094 will allow frames from the PC Port (containing a VLAN ID) to be untagged before being forwarded to the LAN Port and frames from the LAN Port (without a VLAN ID) to be tagged with the configured VLAN ID before being forwarded to the PC Port. For configuring this feature via the Phone UI and the Mitel Web UI, see “Configuring VLAN (optional)” on page 4-51. For configuring this feature using the configuration files, see Appendix A, the section, “Virtual Local Area Network (VLAN) Settings” on page 51.
3. Alternatively setting the LAN Port VLAN ID (**vlan id**) to any ID from 1 to 4094 and PC Port VLAN ID (**vlan id port 1**) to 4095 will allow frames from the LAN Port (containing a VLAN ID) to be untagged before being forwarded to the PC Port and frames from the PC Port (without a VLAN ID) to be tagged with the configured VLAN ID before being forwarded to the LAN Port. For configuring this feature via the Phone UI and the Mitel Web UI, see “Configuring VLAN (optional)” on page 4-51. For configuring this feature using the configuration files, see Appendix A, the section, “Virtual Local Area Network (VLAN) Settings” on page 51.

DSCP Range/VLAN Priority Mapping

DSCP bits in the ToS field of the IP header are set for RTP, RTCP, and SIP packets using either the default values or the values configured via the "**tos sip**", "**tos rtp**", and "**tos rtcp**" parameters.

When the VLAN global configuration parameter, "**tagging enabled**" is set to **1**, VLAN priority for IP packets is mapped to the DSCP value instead of a single priority for all packets. An administrator can also configure VLAN priority for non-IP packets using the "**priority non-ip**" parameter.

Since the default DSCP settings for SIP, RTP, and RTCP are 26, 46, and 46 respectively, this results in corresponding default VLAN priorities of 3 for SIP, 5 for RTP, and 5 for RTCP (based on the settings in the table “DSCP Range/VLAN Priority Mapping” on page 4-48).

You can change the default parameters by modifying just the DSCP values, just the VLAN priority values, or by modifying all values.

The following table shows the DSCP range/VLAN priority mapping:

DSCP RANGE	VLAN PRIORITY
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6

56-63	7

The following table identifies the default DSCP values for the protocols:

PROTOCOL NAME	DEFAULT DSCP VALUES IN THE TOS FIELD
sip	26
rtp	46
rtcp	46

Configuring Type of Service (ToS)/DSCP (optional)

Use the following procedures to configure ToS/DSCP on the IP phone.

Note: ToS/DSCP is enabled by default. The SIP, RTP, and RTCP parameters show defaults of 26, 46, and 46, respectively. Use the following procedures to change these settings if required.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Type of Service (ToS)/DSCP Settings" on page A-57.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Administrator Menu.**
3. Select **Network Settings.**
4. Select **Type of Service DSCP.**
5. Select **Type of Service SIP.**
   or
   Select **Type of Service RTP.**
   or
   Select **Type of Service RTCP**.
6. Enter a value for "**Type of Service SIP**". Default is **26**.
   or
   Enter a value for "**Type of Service RTP**". Default is **46**.
   or
   Enter a value for "**Type of Service RTCP**". Default is **46**.
   Valid values are **0** to **63**.

   Note: If you change the ToS/DSCP setting for a Protocol, and VLAN is enabled, you will need to map the applicable priority to the Protocol setting as shown in the first table in "DSCP Range/VLAN Priority Mapping" on page 4-48 For more information, see the section "Configuring VLAN (optional)" on page 4-51.

7. Press **Done** (3 times) to save the changes.

Note: The session prompts you to restart the IP phone to apply the configuration settings

8. Select **Restart.**

For the 6867i/6869i/6920/6930:

1. Press or on the phone to enter the Options List.
2. Press the **Advanced** softkey.
3. Enter the Administrator password using the keypad. Default is “**22222**”.
4. Select **Network > DSCP**.
5. Enter a value for “**Type of Service SIP**”. Default is **26**.
   or
   Enter a value for “**Type of Service RTP**”. Default is **46**.
   or
   Enter a value for “**Type of Service RTCP**”. Default is **46**.
   Valid values are **0** to **63**.

   Note: If you change the ToS/DSCP setting for a Protocol, and VLAN is enabled, you will need to map the applicable priority to the Protocol setting as shown in the first table in “DSCP Range/VLAN Priority Mapping” on page 4-48 For more information, see the section “Configuring VLAN (optional)” on page 4-51.

6. Press the **Save** softkey.
7. Restart the phone for the selection to take affect.

For the 6873i/6940:

1. Press or on the phone to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password and press the blue Enter key. Default is “**22222**”.
4. Tap the **Network** icon.

   Note: If required, swipe left on the screen to navigate to the second page of options.

5. Tap the **DSCP** icon.
6. Enter a value for “**Type of Service SIP**”. Default is **26**.
   or
   Enter a value for “**Type of Service RTP**”. Default is **46**.
   or

Enter a value for “**Type of Service RTCP**”. Default is **46**.
Valid values are **0** to **63**.

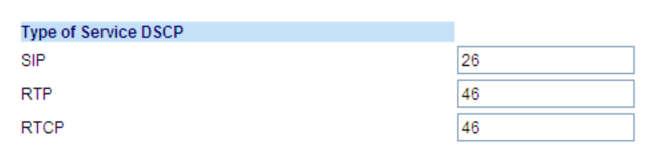
> **Note:** If you change the ToS/DSCP setting for a Protocol, and VLAN is enabled, you will need to map the applicable priority to the Protocol setting as shown in the first table in “DSCP Range/VLAN Priority Mapping” on page 4-48 For more information, see the section “Configuring VLAN (optional)” on page 4-51.

7. Tap the **Save** softkey.

8. Restart the phone for the selection to take affect.

MITEL WEB UI

1. Click on **Advanced Settings->Network->Type of Service DSCP**.



2. Select a Protocol field:
“SIP”
or
“RTP”
or
“RTCP”

3. Enter a value from **0** to **63**. Default values are as follows:

- SIP = 26
- RTP = 46
- RTCP = 46

> **Note:** If you change the ToS/DSCP setting for a Protocol, and VLAN is enabled, you will need to map the applicable priority to the Protocol setting as shown in the first table in “DSCP Range/VLAN Priority Mapping” on page 4-48. For more information, see the section “Configuring VLAN (optional)” on page 4-51.

4. Click **Save Settings** to save your settings.

Configuring VLAN (optional)

Use the following procedures to configure VLAN on the IP phone.

> **Note:** VLAN is disabled by default. When you enable VLAN, the IP phones use the default settings for each VLAN parameter. You can change the default settings if required using the following procedure.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Virtual Local Area Network (VLAN) Settings" on page A-51.

For the 6863i/6865i/6905/6910:

IP PHONE UI

1. Press or on the phone to enter the Options List.
2. Select **Administrator Menu.**
3. Select **Network Settings.**
4. Select **Ethernet and VLAN**.

To globally enable/disable VLAN and set priority for non-IP packet:

5. Select **VLAN Settings**.
6. Select **VLAN**.
7. Select **Enable**.
8. Press **Done** or **Set** to save the changes.
9. Select **LAN Port VLAN**.
10. Select **Other Priority** and enter a non-IP priority value from **0** to **7** for non-IP packets. Default for this field is **5**.
11. Press **Done** (2 times) to return to the VLAN Settings menu.

To set VLAN ID and priority for LAN Port (Port 0):

12. Select **LAN Port VLAN.**
13. Select **LAN Port VLAN ID** and enter a value from **1** to **4095** to specify the VLAN ID for the LAN Port.
    Default is **1**.

    Note: Setting the LAN Port VLAN ID to 4095 and PC Port VLAN ID to any ID from 1 to 4094 will allow frames from the PC port (containing a VLAN ID) to be untagged before being forwarded to the LAN port and frames from the LAN port (without a VLAN ID) to be tagged with the configured VLAN ID before being forwarded to the PC port.

    Example:
    You enable tagging on the phone port as normal but set the LAN Port VLAN ID to 4095 and the PC Port VLAN ID to any ID from 1 to 4094. The following example sets the PC port to be on VLAN 3 but the LAN port is configured as untagged.

    - VLAN Settings->VLAN: Enable
    - VLAN Settings->LAN Port VLAN->LAN Port VLAN ID: 4095
    - VLAN Settings->PC Port VLAN->PC Port VLAN ID: 3
14. Press **Enter** or **Set** to save the change.
15. Select **VLAN Priority**.

16. Select one of the following VLAN Protocols:
    - SIP Priority
    - RTP Priority
    - RTCP Priority
17. Enter a VLAN priority value from **0** to **7** for the associated Protocol. Default values for each Protocol are:
    - SIP Priority = 3
    - RTP Priority = 5
    - RTCP Priority = 5
18. Press **Done** (2 times) to return to the VLAN Settings menu.

To set VLAN ID and priority for PC Port (Port 1):

19. Select **PC Port VLAN**.
20. Select PC Port VLAN ID and enter a value from 1 to 4095 to specify the VLAN ID for the PC Port.
    Default is 4095.

    Note: Setting the PC Port VLAN ID to 4095 and LAN Port VLAN ID to any ID from 1 to 4094 will allow frames from the LAN port (containing a VLAN ID) to be untagged before being forwarded to the PC port and frames from the PC port (without a VLAN ID) to be tagged with the configured VLAN ID before being forwarded to the LAN port.

    Example:
    You enable tagging on the phone port as normal but set the PC Port VLAN ID to 4095 and the LAN Port VLAN ID to any ID from 1 to 4094. The following example sets the LAN port to be on VLAN 3 but the PC port is configured as untagged.
    - VLAN Settings->VLAN: Enable
    - VLAN Settings->LAN Port VLAN->LAN Port VLAN ID: 3
    - VLAN Settings->PC Port VLAN->PC Port VLAN ID: 4095
21. Press **Enter** or **Set** to save the change.
22. Select **PC Port Priority**.
23. Select a PC Port VLAN priority value from **0** to **7** for the PC Port.
    Default is **0**.
24. Press **Done** to save the changes.
25. Navigate back to the **Options List** menu.
26. Select **Restart Phone** and follow the prompts to restart the phone and apply the configuration changes.

For the 6867i/6869i/6920/6930:

IP PHONE UI

1. Press [gear key] or [options key] on the phone to enter the Options List.

2. Press the **Advanced** softkey.
3. Enter the Administrator password using the keypad. Default is “**22222**”.
4. Select **Network > VLAN**.

To globally enable/disable VLAN and set priority for non-IP packets:

5. In the **Basic Settings > VLAN** field enable VLAN by pressing the navigation key.
6. In the **LAN Port VLAN > Other Priority** field, change the non-IP priority value from **0** to **7** for non-IP packets.
   Default for this field is **5**.

To set VLAN ID and priority for LAN Port (Port 0):

7. In the **LAN Port VLAN > LAN Port VLAN ID** field, enter a value from 1 to 4095 to specify the VLAN ID for the LAN Port. Default is **1**.

   Note: Setting the LAN Port VLAN ID to 4095 and PC Port VLAN ID to any ID from 1 to 4094 will allow frames from the PC port (containing a VLAN ID) to be untagged before being forwarded to the LAN port and frames from the LAN port (without a VLAN ID) to be tagged with the configured VLAN ID before being forwarded to the PC port.

   Example:
   You enable tagging on the phone port as normal but set the LAN Port VLAN ID to 4095 and the PC Port VLAN ID to any ID from 1 to 4094. The following example sets the PC port to be on VLAN 3 but the LAN port is configured as untagged.

   - VLAN Settings->VLAN: Enable
   - VLAN Settings->LAN Port VLAN->LAN Port VLAN ID: 4095
   - VLAN Settings->PC Port VLAN->PC Port VLAN ID: 3

8. In the **LAN Port VLAN > SIP Priority** field, enter a value from **0** to **7** to specify the SIP priority for the LAN Port. Default is **3**.
9. In the **LAN Port VLAN > RTP Priority** field, enter a value from **0** to **7** to specify the RTP priority for the LAN Port. Default is **5**.
10. In the **LAN Port VLAN > RTCP Priority** field, enter a value from **0** to **7** to specify the RTCP priority for the LAN Port. Default is **5**.

To set VLAN ID and priority for PC Port (Port 1):

11. In the **PC Port VLAN > PC Port VLAN ID** field, enter a value from 1 to 4095 to specify the VLAN ID for the LAN Port. Default is **4095**.

    Note: Setting the PC Port VLAN ID to 4095 and LAN Port VLAN ID to any ID from 1 to 4094 will allow frames from the LAN port (containing a VLAN ID) to be untagged before being forwarded to the PC port and frames from the PC port (without a VLAN ID) to be tagged with the configured VLAN ID before being forwarded to the LAN port.

    Example:
    You enable tagging on the phone port as normal but set the PC Port VLAN ID to 4095 and the LAN Port VLAN ID to any ID from 1 to 4094. The following example sets the LAN port to be on VLAN 3 but the PC port is configured as untagged.

- VLAN Settings->VLAN: Enable
- VLAN Settings->LAN Port VLAN->LAN Port VLAN ID: 3
- VLAN Settings->PC Port VLAN->PC Port VLAN ID: 4095

12. In the **PC Port VLAN > Priority** field, enter a value from **0** to **7** to specify the PC Port VLAN priority. Default is **0**.
13. Press the **Save** softkey.
14. Restart the phone for the selection to take affect.

For the 6873i/6940:

IP PHONE UI

1. Press [⚙] or [⚙] on the phone to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password and press the blue Enter key. Default is “**22222**”.
4. Tap the **Reset** icon.

   Note: If required, swipe left on the screen to navigate to the second page of options.

5. Tap the **VLAN** icon.

To globally enable/disable VLAN and set priority for non-IP packets:

6. In the **Basic Settings > VLAN** field enable VLAN by pressing the right arrow key.
7. In the **LAN Port VLAN > Other Priority** field, change the non-IP priority value from **0** to **7** for non-IP packets.
   Default for this field is **5**.

To set VLAN ID and priority for LAN Port (Port 0):

8. In the **LAN Port VLAN > LAN Port VLAN ID** field, enter a value from 1 to 4095 to specify the VLAN ID for the LAN Port. Default is **1**.

   Note: Setting the LAN Port VLAN ID to 4095 and PC Port VLAN ID to any ID from 1 to 4094 will allow frames from the PC port (containing a VLAN ID) to be untagged before being forwarded to the LAN port and frames from the LAN port (without a VLAN ID) to be tagged with the configured VLAN ID before being forwarded to the PC port.

   Example:
   You enable tagging on the phone port as normal but set the LAN Port VLAN ID to 4095 and the PC Port VLAN ID to any ID from 1 to 4094. The following example sets the PC port to be on VLAN 3 but the LAN port is configured as untagged.

   - VLAN Settings > VLAN: Enable
   - VLAN Settings > LAN Port VLAN > LAN Port VLAN ID: 4095
   - VLAN Settings > PC Port VLAN > PC Port VLAN ID: 3

9. In the **LAN Port VLAN > SIP Priority** field, enter a value from **0** to **7** to specify the SIP priority for the LAN Port. Default is **3**.

10. In the **LAN Port VLAN > RTP Priority** field, enter a value from **0** to **7** to specify the RTP priority for the LAN Port. Default is **5**.

11. In the **LAN Port VLAN > RTCP Priority** field, enter a value from **0** to **7** to specify the RTCP priority for the LAN Port. Default is **5**.

To set VLAN ID and priority for PC Port (Port 1):

12. In the **PC Port VLAN > PC Port VLAN ID** field, enter a value from 1 to 4095 to specify the VLAN ID for the LAN Port. Default is **4095**.

    Note: Setting the PC Port VLAN ID to 4095 and LAN Port VLAN ID to any ID from 1 to 4094 will allow frames from the LAN port (containing a VLAN ID) to be untagged before being forwarded to the PC port and frames from the PC port (without a VLAN ID) to be tagged with the configured VLAN ID before being forwarded to the LAN port.

    Example:
    You enable tagging on the phone port as normal but set the PC Port VLAN ID to 4095 and the LAN Port VLAN ID to any ID from 1 to 4094. The following example sets the LAN port to be on VLAN 3 but the PC port is configured as untagged.

    - VLAN Settings > VLAN: Enable
    - VLAN Settings > LAN Port VLAN > LAN Port VLAN ID: 3
    - VLAN Settings > PC Port VLAN > PC Port VLAN ID: 4095

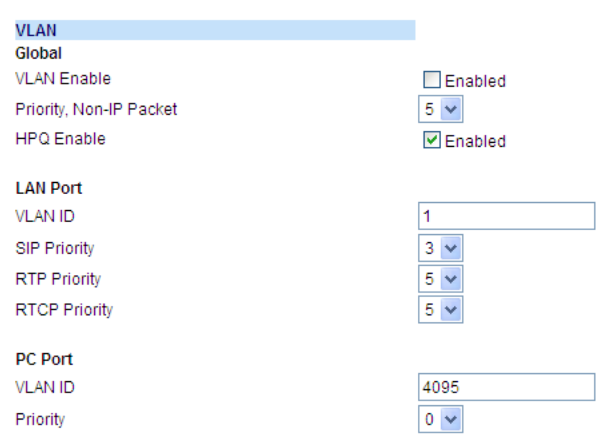
13. In the **PC Port VLAN > Priority** field, enter a value from **0** to **7** to specify the PC Port VLAN priority. Default is **0**.

14. Press the **Save** softkey.

15. Restart the phone for the selection to take affect.

MITEL WEB UI

1. Click on **Advanced Settings->Network->VLAN.**



To globally enable/disable VLAN and set priority for non-IP packets:

2. Enable VLAN by checking the **VLAN Enable** field check box. (Disable this field by un-checking the check box).

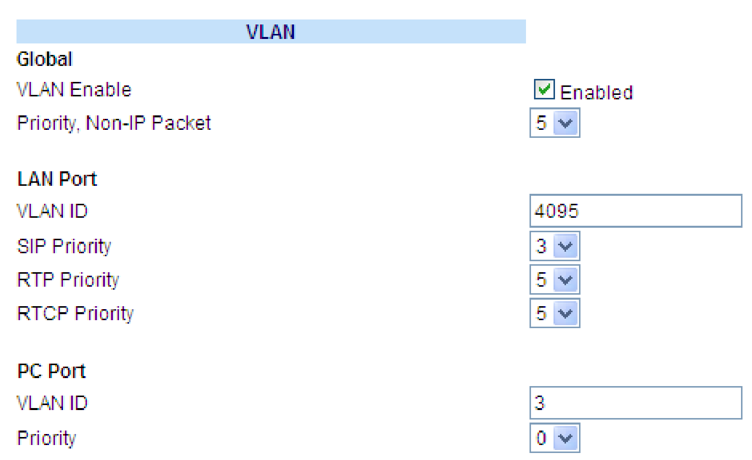
3. With VLAN enabled, select the priority (**0** to **7**) for non-IP packets in the **Priority, Non-IP Packet** field.

To set VLAN ID and priority for the LAN Port (Port 0):

4. Enter a VLAN ID value from **1** to **4095** in the **VLAN ID** field. Default is **1**.

> **Note:** Setting the LAN Port VLAN ID to 4095 and PC Port VLAN ID to any ID from 1 to 4094 will allow frames from the PC port (containing a VLAN ID) to be untagged before being forwarded to the LAN port and frames from the LAN port (without a VLAN ID) to be tagged with the configured VLAN ID before being forwarded to the PC port.

Example:
You enable tagging on the phone port as normal but set the LAN Port VLAN ID to 4095 and the PC Port VLAN ID to any ID from 1 to 4094. The following example sets the PC port to be on VLAN 3 but the LAN port is configured as untagged.



5. Choose a VLAN Protocol (**SIP Priority**, **RTP Priority**, and/or **RTCP Priority**), and select a priority for the associated Protocol. Valid values are **0** to **7**, Defaults are as follows:
   - SIP Priority = 3
   - RTP Priority = 5
   - RTCP Priority = 5

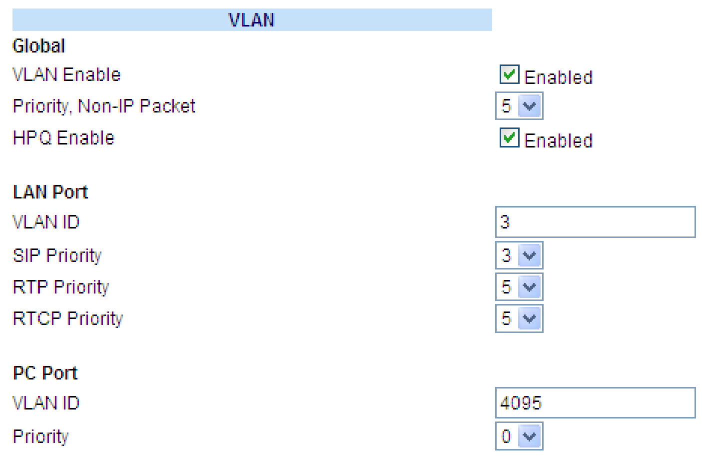
To set VLAN ID and priority for the PC Port (Port 1):

6. Enter a VLAN ID value from **1** to **4095** in the **VLAN ID** field. Default is **4095**.

> **Note:** Setting the PC Port VLAN ID to 4095 and LAN Port VLAN ID to any ID from 1 to 4094 will allow frames from the LAN port (containing a VLAN ID) to be untagged before being forwarded to the PC port and frames from the PC port (without a VLAN ID) to be tagged with the configured VLAN ID before being forwarded to the LAN port.

Example:

You enable tagging on the phone port as normal but set the PC Port VLAN ID to 4095 and the LAN Port VLAN ID to any ID from 1 to 4094. The following example sets the LAN port to be on VLAN 3 but the PC port is configured as untagged.



7. Select a VLAN priority value from **0** to **7** for the PC Port in the **Priority** field. Default is **0**.

8. Click **Save Settings** to save your settings.

RPORT

The Session Initiation Protocol (SIP) operates over UDP and TCP. When used with UDP, responses to requests are returned to the source address from which the request came, and returned to the port written into the topmost "Via" header of the request. However, this behavior is not desirable when the client is behind a firewall.

A parameter created for the "Via" header called "**Rport**" in RFC 3581, allows a client to request that the server send the response back to the source IP address **and** the port from which the request came.

When you enable "Rport, the phone always uses symmetric signaling (listens on the port used for sending requests).

Note: Configuring the Rport parameter is recommended for clients behind a firewall since this parameter allows a client to request that the server send the response back to the source IP address and the port from which the request came.

An Administrator can configure "**Rport**" using the configuration files or the Mitel Web UI.

Configuring Rport Using the Configuration Files

Use the following procedures to configure Rport on your phone.

CONFIGURATION FILES

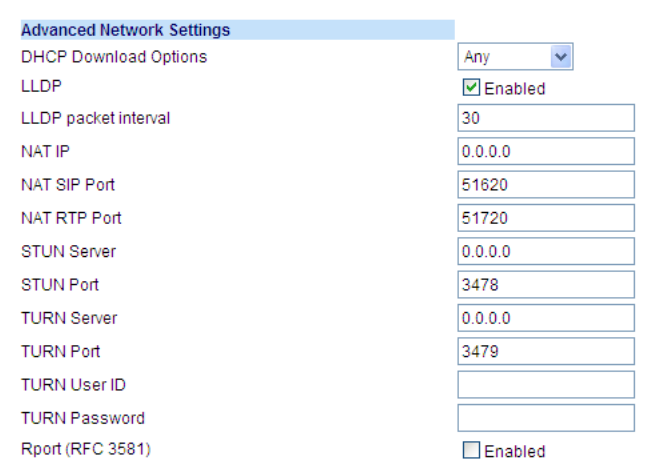
For specific parameters you can set in the configuration files, see Appendix A, the section, "Rport Setting" on page A-45.

Configuring Rport Using the Mitel Web UI

Use the following procedure to configure Rport on your phone using the Mitel Web UI.

MITEL WEB UI

1. Click on **Advanced Settings->Network->Advanced Network Settings**.



2. In the "Advanced Network Settings" section, enable the "**Rport (RFC3581**" field by checking the check box. (Disable Rport by unchecking the box).
   "Rport" in RFC 3581, allows a client to request that the server send the response back to the source IP address **and** the port from which the request came.
3. Click **Save Settings** to save your changes.

NETWORK TIME SERVERS

Network Time Protocol (NTP) is a protocol that the IP phone uses to synchronize the phone clock time with a computer (configuration server) in the network.

To use NTP, you must enable it using the configuration files or the Mitel Web UI. You can specify up to three time servers in your network.

Notes:

1. The IP phones support NTP version 3.
2. NTP time syncs are performed every 4 hours.

Configuring NTP Servers (optional)

Use the following procedure to enable/disable and configure the NTP servers using the configuration files.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Time Server Settings" on page A-66.

Use the following procedure to enable/disable the NTP server using the IP Phone UI.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Preferences.**
3. Select **Time and Date.**
4. Select **Timer Server 1**, **Timer Server 2**, or **Time Server 3**.
5. Enter the IP Address (in dotted decimal) or qualified domain name for the Time Server.
6. Press **Done** to save the change.

For the 6867i/6869i/6920/6930:

1. Press or on the phone to enter the Options List.
2. Select **Time and Date > Set Date and Time**.
3. In the **Timer Server 1, Time Server 2,** and/or **Time Server 3** fields, enter the respective IP address (in dotted decimal) or qualified domain name.
4. Press the **Save** softkey.

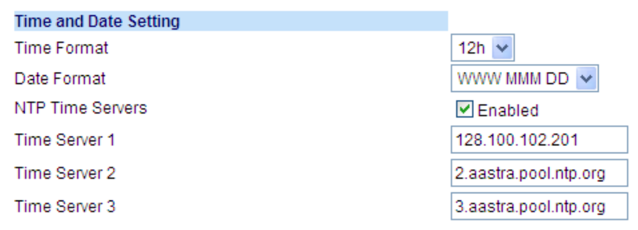
For the 6873i/6940:

1. Press or on the phone to enter the Options List.
2. Tap the **Time and Date** icon.
3. Tap the **Set Date and Time** icon.
4. In the **Timer Server 1, Time Server 2,** and/or **Time Server 3** fields, enter the respective IP address (in dotted decimal) or qualified domain name.
5. Tap the **Save** softkey.

Use the following procedure to enable/disable and configure the NTP Servers using the Mitel Web UI.

MITEL WEB UI

1. Click on **Basic Settings->Preferences->Time and Date Setting.**



2. Enable the "**NTP Time Servers**" field by checking the check box.
   (Disable this field by unchecking the box). Default is disabled.
3. Enter an IP address or qualified domain name in the "**Time Server 1"**, "**Time Server 2**", and/or "**Time Server 3**" field(s) to specify the location of the NTP time server.
4. Click **Save Settings** to save your changes.

GLOBAL SIP SETTINGS

DESCRIPTION

The IP phone uses the information in the Global Session Initiation Protocol (SIP) settings to register at the IP PBX.

The IP phone configuration defines network and user account parameters that apply **globally** to all applicable SIP lines. Since not all SIP lines are necessarily hosted using the same IP-PBX/server or user account, additional sets of **per-line** parameters can also be defined for network and user accounts.

You configure and modify these parameters and associated values using the configuration files, the IP phone UI, or the Mitel Web UI. The Mitel Web UI and configuration file methods configure global and per-line SIP settings on the IP phone. The IP phone UI configures global SIP settings only.

On the IP Phones, you can configure Basic and Advanced SIP Settings. The Basic SIP Settings include authentication and network settings. The Advanced SIP Settings include other features you can configure on the IP Phone.

Note: Global SIP settings are applicable only to Lines 1 and 2 for the 6800 series SIP phones. To configure lines that do not have an associated Line hard key, Administrators must configure each individual line manually.

REFERENCE

For more information about Basic SIP Settings (for authentication and network), see "Basic SIP Settings" on page 4-62.

For more information about Advanced SIP Settings, see "Advanced SIP Settings (optional)" on page 4-80.

BASIC SIP SETTINGS

Specific parameters are configurable on a global and per-line basis. You can also configure specific parameters using the IP Phone UI, the Mitel Web UI, or the configuration files. If you have a proxy server or have a SIP registrar present at a different location than the PBX server, the SIP parameters may need to be changed.

The IP phones allow you to define different SIP lines with the same account information (i.e. same user name) but with different registrar and proxy IP addresses. This feature works with Registration, Subscription, and Notify processing. This feature also works with the following types of calls: incoming, outgoing, BroadSoft Shared Call Appearance (SCA), Bridged Line Appearance (BLA), conference, transfer, blind transfer.
The following tables identify the SIP global and per-line, authentication and network parameters on the IP phones.

SIP GLOBAL PARAMETERS

IP PHONE UI PARAMETERS	MITEL WEB UI PARAMETERS	CONFIGURATION FILE PARAMETERS
SIP GLOBAL AUTHENTICATION PARAMETERS		
• Screen Name	• Screen Name	• sip screen name
	• Screen Name 2	• sip screen name 2
• User Name	• Phone Number	• sip user name
• Display Name	• Caller ID	• sip display name
• Authentication Name	• Authentication Name	• sip auth name
• Password	• Password	• sip password
	• BLA Number	• sip bla number
	• Line Mode	• sip mode
	• Call Waiting (see Chapter 5, “Configuring Operational Features”)	• call waiting (see Chapter 5, “Configuring Operational Features”
		• sip vmail
SIP GLOBAL NETWORK PARAMETERS		
• Proxy Server	• Proxy Server	• sip proxy ip
• Proxy Port	• Proxy Port	• sip proxy port
	• Backup Proxy Server	• sip backup proxy ip
	• Backup Proxy Port	• sip backup proxy port
	• Outbound Proxy Server	• sip outbound proxy
	• Outbound Proxy Port	• sip outbound proxy port
• Registrar Server	• Backup Outbound Proxy	• sip backup outbound proxy
• Registrar Port	• Backup Outbound Proxy Port	• sip backup outbound proxy port
	• Registrar Server	• sip registrar ip
	• Registrar Port	• sip registrar port
	• Backup Registrar Server	• sip backup registrar ip
	• Backup Registrar Port	• sip backup registrar port
	• Registration Period	• sip registration period
	• Conference Server URI (see Chapter 5, “Configuring Operational Features”)	• sip centralized conf (see Chapter 5, “Configuring Operational Features”)

Reference

For more information about centralized conferencing, see Chapter 5, the section, “Centralized Conferencing (for Sylantro and BroadSoft Servers)” on page 5-349.

SIP PER-LINE PARAMETERS

IP PHONE UI PARAMETERS	MITEL WEB UI PARAMETERS	CONFIGURATION FILE PARAMETERS
SIP PER-LINE AUTHENTICATION PARAMETERS		
• Screen Name	• Screen Name	• sip lineN screen name
	• Screen Name 2	• sip lineN screen name 2
• User Name	• Phone Number	• sip lineN user name
• Display Name	• Caller ID	• sip lineN display name
• Auth Name	• Authentication Name	• sip lineN auth name
• Password	• Password	• sip lineN password
	• BLA Number	• sip lineN bla number
	• Line Mode	• sip lineN mode
	• Call Waiting (see Chapter 5, "Configuring Operational Features"	• sip lineN call waiting (see Chapter 5, "Configuring Operational Features"
		• sip lineN vmail
SIP PER-LINE NETWORK PARAMETERS		
• Proxy Server	• Proxy Server	• sip lineN proxy ip
• Proxy Port	• Proxy Port	• sip lineN proxy port
	• Backup Proxy Server	• sip lineN backup proxy ip
	• Backup Proxy Port	• sip lineN backup proxy port
	• Outbound Proxy Server	• sip lineN outbound proxy
	• Outbound Proxy Port	• sip lineN outbound proxy port
• Registrar Server • Registrar Port	• Backup Outbound Proxy Server	• sip lineN backup outbound proxy
	• Backup Outbound Proxy Port	• sip lineN backup outbound proxy port
	• Registrar Server	• sip lineN registrar ip
	• Registrar Port	• sip lineN registrar port
	• Backup Registrar Server	• sip lineN backup registrar ip
	• Backup Registrar Port	• sip lineN backup registrar port
	• Registration Period	• sip lineN registration period
	• Conference Server URI (see Chapter 5, "Configuring Operational Features")	• sip lineN centralized conf (see Chapter 5, "Configuring Operational Features")

Reference

For more information about centralized conferencing, see Chapter 5, the section, "Centralized Conferencing (for Sylantro and BroadSoft Servers)" on page 5-349.

Note: The "sip vmail" and "sip lineN vmail" parameters are configurable using the configuration files only. To configure voicemail see Chapter 5, the section, "Voicemail" on page 5-312.

Specific sets of SIP parameters are inter-dependent with each other. To prevent conflicting parameter values from being applied, per-line values always take precedence over the corresponding set of global values.

For example, if a parameter value is configured for one of the per-line sets, all parameters from that set are applied and all parameters from the corresponding global section are ignored, even if some of the parameters within the global set are not defined in the per-line set.

SIP PASSWORD MASKING

The "**mask sip password**" configuration parameter can be used to mask a user's SIP account password in the server.cfg and local.cfg files (downloaded from the IP phone's Web UI troubleshooting page for debug purposes). The parameter is disabled by default.

Note: By enabling the '**mask sip password**' parameter, the SIP, Administrator, and user password can be masked.

Configuring SIP Password Masking

Use the following procedure to configure SIP password masking using the configuration files.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "SIP Basic, Global Settings" on page A-89.

SIP PRECEDENCE EXAMPLE

The following example shows the SIP proxy feature and example schema for storage and parsing of the SIP configuration parameters.

The following SIP configuration is assumed:

```
# SIP network block
sip proxy ip:  10.30.11.154
sip proxy port: 5060
sip registrar ip:  10.44.122.37
sip registrar port: 4020
sip line3 proxy ip: siparator.vonage.com
sip line3 proxy port: 0
```

Line3 specifies per-line values for proxy IP address and proxy port, so the phone uses those parameter values for SIP calls made on that line. However, because those parameters are part of the SIP network block, the phone does not apply any of the global SIP network block parameters. So even though the global parameters configure a SIP registrar, Line3 on the phone ignores all global network block parameters. Since line3 does not contain a per-line SIP registrar entry, the phone does not use a registrar for that line.

Note: Global SIP parameters apply to all lines unless overridden by a per-line configuration. Per-line settings are configurable for lines 1 through 7.

BACKUP PROXY/REGISTRAR SUPPORT

The IP phones support a backup SIP proxy and backup SIP registrar feature. If the primary server is unavailable, the phone automatically switches to the backup server allowing the user's phone to remain in service.

How it Works

All SIP registration messages are sent to the primary registrar first. If the server is unavailable, then a new registration request is sent to the backup registrar. This also applies to registration renewal messages, which try the primary server before the backup.

Similarly, any outgoing calls attempt to use the primary proxy first, then the backup if necessary. In addition, subscriptions for BLF, BLA, and explicit MWI can also use the backup proxy when the primary fails. Outgoing calls and the previously mentioned subscriptions behave the same as registrations, where the primary proxy is tried before the backup.

You can configure the backup SIP proxy on a global or per-line basis via the configuration files or the Mitel Web UI.

SIP OUTBOUND SUPPORT

The IP Phones support draft-ietf-sip-outbound-15. That specification describes how a SIP User Agent (UA) behind a firewall, reuses an existing connection (usually the REGISTER outbound connection) for the inbound request if the proxy supports it. The UA uses keep-alive packets to monitor the connection status.

An Administrator can enable or disable this feature using the following parameter in the configuration files:

- sip outbound support

Note: If the Global SIP parameter “Persistent TLS” is set on the phone, then only one TLS persistent connection can be established since the phone uses the local port 5061 for connection. If the Global SIP parameter “TLS” is set on the phone, more than one connection can be setup since the phone uses a random local port for connection.

DNS A Record Flow Behavior for SIP Outbound Proxies Using Persistent TLS

When the "sip outbound support" parameter is enabled and the phone is configured to use the DNS A query method to resolve FQDNs for outbound proxies, if multiple IP addresses are provided, the phone establishes a persistent TLS connection with the first flow target IP provided in the list; all SIP message will then be sent through this TLS connection. Time-To-Live (TTL) from the A record response is used for caching and future queries.

If a DNS re-query is initiated and the IP address of the current flow target is on the DNS A response list in any position, the phone will renew using the current flow target’s IP address. If the IP address of the current flow target has been removed from the DNS A response, or if the IP address of the current flow target is not reachable, the phone will then proceed to disconnect from the current flow target and establish a connection with the first IP address provided on the list.

In software releases previous to Release 4.3.0 SP1, if TTL expired and a SIP request was required, the phone would initiate a DNS A re-query and would attempt to establish a connection with the first IP provided on the list. Therefore, if the IP address of the current connected flow target was on the DNS A response list but was listed as the second or third IP address, the phone would disconnect from the current flow target and establish a connection with the first IP address provided on the list.

Enabling/Disabling SIP Outbound Draft 15 Support

Use the following procedure to enable/disable SIP outbound Draft 15 support.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "SIP Outbound Support" on page A-88.

BACKUP OUTBOUND PROXY AND FAILOVER SUPPORT

The IP phones support a backup outbound proxy and failover. This feature provides the following:

- The ability to specify a backup outbound proxy.
- The ability to support SIP outbound on all connection types.
- The ability to configure the SIP outbound keep alive timer.
- The ability to reestablish failed outbound connections in the background.
- The ability to support the DNS Cache Time-to-Live (TTL) requirements

Using this feature depends on the SIP network settings on your phone. The following table identifies network configuration scenarios, and the method by which this specific feature works in each scenario.

IF	THEN
SIP OUTBOUND DISABLED AND	
backup proxy and backup registrar configured,	• All invite, register, and subscribe requests attempt to use the primary proxy/registrar first • If the primary registrar fails, the phone registers to the backup proxy. • If the backup proxy fails, the phone registers using the Address of Record (AOR) of the backup proxy, and moves all subscriptions to the backup proxy. • When the primary registrar comes back online, the phone registers to it using the currently active AOR. • When the primary proxy comes back online the phone registers with the primary AOR to the currently active registrar and moves all subscriptions to the primary proxy.

backup proxy, backup registrar, and backup outbound proxy configured,	• All invite, register, and subscribe requests attempt to use the primary proxy/registrar first. • If any connection fails, the phone registers the backup AOR on the backup registrar. It moves all subscriptions to the backup proxy. • When the primary is functional again, registration and subscriptions are moved back to the primary proxy/registrar.
backup outbound proxy configured only,	• All invite, register and subscribe requests are sent through the primary outbound proxy first. • If the primary proxy fails, the phone performs registration and subscriptions through the backup outbound proxy. • When the primary proxy comes back online, the registrations and subscriptions are performed again through the primary outbound proxy.
SIP OUTBOUND ENABLED AND	

backup proxy and backup registrar configured,	• Establishes flow to the primary proxy and registrar.
	• If the flow to the primary registrar fails, the phone:
	  • establishes flow to the backup registrar.
	  • registers to the backup registrar.
	  • attempts to reestablish flow to the primary registrar in the background.
	  • When the primary registrar comes back up, the phone unregisters from the backup and registers with the primary.
	•If the flow to the primary proxy fails, the phone:
	  • establishes flow to the backup proxy.
	  • registers the new AOR with the active registrar.
	  • moves subscriptions to the backup proxy.
	  • attempts to reestablish the flow to the primary proxy in the background.
	• When the flow to the primary proxy is reestablished, the phone:
	  • registers the primary AOR to the active registrar.
	  • moves subscriptions to the primary proxy.
	  • unregisters/unsubscribes from the backup proxy/registrar.

backup proxy, backup registrar, and backup outbound proxy configured,
 	
Note: This configuration assumes that the outbound proxy is maintaining its own outbound connections to the proxy/registrar.
	• Establishes a flow to the primary outbound proxy.
	• If the flow fails, the phone:
	  • establishes the flow to the backup proxy.
	  • registers the backup AOR to the backup registrar.
	  • moves subscriptions to the backup proxy.
	  • attempts to reestablish connection to the primary outbound proxy in the background.
	• When the flow to the primary proxy is reestablished, the phone:
	  • registers the primary AOR to the primary registrar.
	  • moves the subscriptions to the primary proxy.
	  • unregisters/unsubscribes from the backup proxy/registrar.

backup outbound proxy configured only,	• Establishes a flow to the primary outbound proxy.
	• If the flow fails, the phone:
	  • establishes the flow to the backup proxy.
	  • registers the backup AOR to the backup registrar.
	  • moves subscriptions to the backup proxy.

Configuring a Backup Outbound Proxy

To configure this feature an Administrator can set the following parameters in the configuration files or the Mitel Web UI:

PARAMETER	MITEL WEB UI CONFIGURATION	CONFIGURATION FILE CONFIGURATION
sip outbound support	-	4
sip symmetric udp signaling	-	4
sip transport protocol	4	4
GLOBAL PARAMETERS		
sip backup outbound proxy	4	4
sip backup outbound proxy port	4	4
PER-LINE PARAMETERS		
sip lineN backup outbound proxy	4	4
sip lineN backup outbound proxy port	4	4

Note: The “sip outbound support”, “sip symmetric udp signaling”, and “sip transport protocol” parameters are existing parameters on the phone. For more information about these parameters, see Appendix A “SIP Outbound Support”, “Symmetric UDP Signaling Setting”, and “Advanced SIP Settings”.

Use the following procedure to configure backup outbound proxies.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "Backup Outbound Proxy (Global Settings)" on page A-97 and "Backup Outbound Proxy (Per-line Settings)" on page A-108.

Limitations

The following are limitations with this feature:

- Keep-alive mechanisms shall be limited to IPv4 only.
- Per M5T, RFC5686 is not fully supported although the draft upon which it was based (draft-ietf-sip-outbound-15) is supported.

SIP SERVER (SRV) LOOKUP

The SIP SRV Lookup feature allows you to configure the IP phone to issue a DNS query to retrieve records pertaining to a SIP proxy, a SIP registrar, or a SIP outbound proxy.

The IP phone issues a DNS query for an SRV record when the IP address of the server is FQDN and the corresponding port is 0.

Note: The phones only generate a 'request' and do *not* facilitate the 'DNS or SRV service or provide a response to the requests.

For example, if the phone is configured with **sip proxy ip of "ana.mitel.com"**, and **sip proxy port of "0"**, the SRV lookup may return multiple servers, based on the priorities if one is selected as primary and others are selected as secondary. However, if the IP address is an FQDN and the corresponding server port is non-zero, then the phone issues a DNS "A" Name Query to resolve the FQDN into dot notation form.

If the IP address is a valid dot notation and the port is zero, then a default port 5060 is used.

You can configure SRV lookup using the configuration files (**startup.cfg** and *<mac>.cfg*) only. The parameters to use are:

- sip proxy ip
- sip proxy port

CONTACT HEADER MATCHING

When sending SIP packets, the IP Phones observe the Contact header by matching the username, domain name, port, and transport as referenced in SIP RFC 3261.This is called "strict SIP Contact header matching." However, in specific networks (such as behind some SOHO routers), the phone registers with its private address in the Contact, but when the response is sent back, the router maintains the public side IP address in the Contact header. This causes a non-matching Contact header and the phone does not accept the new registration expiry timer.

You can set the parameter, "**sip contact matching**", which allows the Administrator to specify the method used by the phone to match the Contact Header. Previously by default, when sending SIP packets, the IP phones observed the contact header by doing a full URI matching of username, domain, phone IP and port name, and transport (value='0'). Now the default value for the “**sip contact matching**” parameter is to match the username only (value=’2’). This parameter is available via the configuration files only.

Enabling/Disabling the “Contact Header Matching” Feature

Use the following procedure to enable/disable the “Contact Header Matching” feature.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, “Contact Header Matching” on page A-88.

CONFIGURING BASIC SIP AUTHENTICATION SETTINGS

You can configure SIP authentication settings using the configuration files, the IP Phone UI, or the Mitel Web UI.

Note: To configure the SIP settings per-line, use the configuration files or the Mitel Web UI.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “SIP Basic, Global Settings” on page A-89 or “SIP Basic, Per-Line Settings” on page A-98. For specific parameters you can set in the configuration files for call waiting, see the section, “Call Waiting Settings” on page A-92 or “SIP Per-Line Call Waiting Setting” on page A-103.

Reference

For more information about setting the call waiting parameters, see Chapter 5, the section, “Call Waiting” on page 5-87. Call Waiting cannot be set via the IP Phone UI.

You can set global configuration only using the IP Phone UI.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press ⚙ or ⚙ on the phone to enter the Options List.
2. Select **Administrator Menu.**
3. Select **SIP Settings.**

4. Select **User Name** to enter the username that appears in the name field of the SIP URI. This user name is also used for registering the phone at the registrar.

   Note: The IP phones allow usernames containing dots ("."). You can also enter the same user name for different registrar and proxy IP addresses.

5. Press **Done** to save the changes.
6. Select **Display Name** to enter the name used in the display name field of the "From SIP" header field.
7. Press **Done** to save the changes.
8. Select **Screen Name** and enter the name to display on the idle screen.
9. Press **Done** to save the changes.
10. Select **Authentication Name** to enter the authorization name used in the username field of the Authorization header field of the SIP REGISTER request.
11. Press **Done** to save the changes.
12. Select **Password** to enter the password used to register the IP phone with the SIP proxy**.**

    Note: The IP phones accept numeric passwords only.

13. Press **Done** (3 times) to save the changes.

    Note: The session prompts you to restart the IP phone to apply the configuration settings.

14. Select **Restart.**

For the 6867i/6869i/6920/6930:

1. Press or on the phone to enter the Options List.
2. Press the **Advanced** softkey.
3. Enter the Administrator password using the keypad. Default is "**22222**".
4. Select **SIP > User**.
5. In the **User Name** field, enter the username that appears in the name field of the SIP URI. This user name is also used for registering the phone at the registrar.

   Note: The IP phones allow usernames containing dots ("."). You can also enter the same user name for different registrar and proxy IP addresses

6. In the **Display Name** field, enter the name used in the display name field of the "From SIP" header.
7. In the **Screen Name** field, enter the name to display on the idle screen.
8. In the **Auth. Name** field, enter the authorization name used in the username field of the Authorization header field of the SIP REGISTER request.

9. In the **Password** field, enter the password used to register the IP phone with the SIP proxy.

   Note: The IP phones accept numeric passwords only.

10. Press the **Save** softkey.
11. Restart the phone for the changes to take affect.

For the 6873i/6940:

1. Press or on the phone to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password and press the blue Enter key. Default is "**22222**".
4. Tap the **SIP** icon.

   Note: If required, swipe left on the screen to navigate to the second page of options.

5. Tap the **User** icon
6. In the **User Name** field, enter the username that appears in the name field of the SIP URI. This user name is also used for registering the phone at the registrar.

   Note: The IP phones allow usernames containing dots ("."). You can also enter the same user name for different registrar and proxy IP addresses

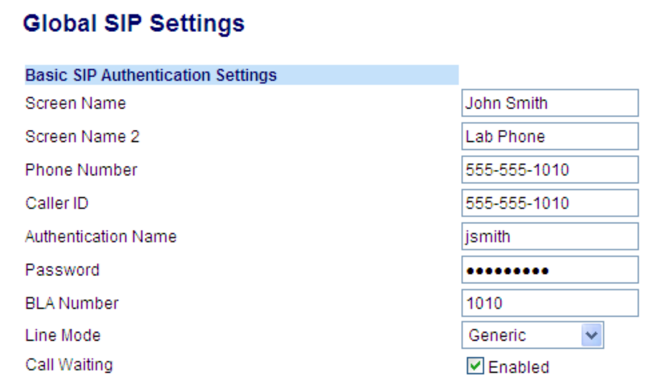
7. In the **Display Name** field, enter the name used in the display name field of the "From SIP" header.
8. In the **Screen Name** field, enter the name to display on the idle screen.
9. In the **Auth. Name** field, enter the authorization name used in the username field of the Authorization header field of the SIP REGISTER request.
10. In the **Password** field, enter the password used to register the IP phone with the SIP proxy.

    Note: The IP phones accept numeric passwords only.

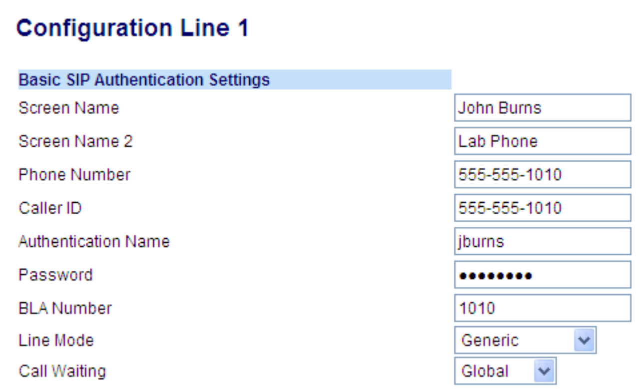
11. Tap the **Save** softkey.
12. Restart the phone for the changes to take affect.

MITEL WEB UI

1. For global configuration, click on **Advanced Settings->Global SIP->Basic SIP Authentication Settings.**



2. Or, for per-line configuration, click on **Advanced Settings->Line *N* ->Basic SIP Authentication Settings**.



Configure SIP Authentication Settings:

3. In the "**Screen Name**" field, enter the screen name that displays on the idle screen.
4. In the "**Screen Name 2**" field, enter the text you want to display on the phone under the “Screen Name” on the idle screen.

Notes:

1. If other status messages display on the phone, such as “Network Disconnected”, the Screen Name 2 value does not display.
2. Symbol characters are allowed (such as “#”).
3. If the text is longer than the display width, than the display truncates the text to fit the display.

5. In the "**Phone Number**" field, enter the phone number of the IP phone.
6. In the "**Caller ID**" field, enter the phone number of the IP phone.
7. In the "**Authentication Name**" field, enter the name used in the username field of the Authorization header of the SIP REGISTER request.

8. In the "**Password**" field, enter the password used to register the IP phone with the SIP proxy.

Note: The IP phones accept numeric passwords only.

9. In the "**BLA Number**" field, enter the Bridge Line Appearance (BLA) number to be shared across all IP phones.
   For more information about setting the BLA on the phone, see Chapter 5, the section, "Bridged Line Appearance (BLA)" on page 5-228.

10. In the "**Line Mode**" field, select "Generic" for normal mode, "BroadSoft SCA" for a BroadWorks network.

Configure Global Call Waiting:

11. The "**Call Waiting**" field is enabled by default. To disable call waiting on a global basis, uncheck this box.
    For more information about setting the call waiting parameters, see Chapter 5, the section, "Call Waiting" on page 5-87.

Configure Per-Line Call Waiting:

12. The "**Call Waiting**" field is set to "**Global**" by default. To enable call waiting for a specific line, select "**enabled**" from the list in this field. To disable call waiting for a specific line, select "**disabled**" from the list in this field.
    For more information about setting the call waiting parameters, see Chapter 5, the section, "Call Waiting" on page 5-87.

13. Click **Save Settings** to save your changes.

CONFIGURING BASIC SIP NETWORK SETTINGS (OPTIONAL)

You can configure SIP network settings using the configuration files, the IP Phone UI, or the Mitel Web UI.

Note: To configure the SIP settings per-line, use the configuration files or the Mitel Web UI.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "SIP Basic, Global Settings" on page A-89 or "SIP Basic, Per-Line Settings" on page A-98.

Note: You can set global configuration only using the IP Phone UI.

For the 6863i/6865i/6905/6910:

IP PHONE UI

1. Press ⚙ or ⚙ on the phone to enter the Options List.
2. Select **Administrator Menu.**
3. Select **SIP Settings.**

Configuring Proxy IP and Proxy Port:

4. Select **Proxy IP/Port.**
5. Enter an IP address or fully qualified host name in the **Proxy Server** field. Default is **0.0.0.0**.
6. Enter a Proxy Port number in the **Proxy Port** field for accessing the SIP proxy server. Default is **0**.
7. Press **Done** to save the changes.

Configuring Registrar IP and Registrar Port:

8. Select **Registrar IP/Port.**
9. Enter an IP address or fully qualified host name in the **Registrar Server** field. Default is **0.0.0.0**.
   A global value of 0.0.0.0 disables registration. However, the phone is still active and you can dial using username@ip address of the phone.
   If the Registrar IP address is set to 0.0.0.0 for a per-line basis (i.e. line 1, line 2, etc.), then the register request is not sent, the "No Service" message does not display, and the message waiting indicator (MWI) does not come on.
10. Enter a Registrar Port number in the **Registrar Port** field for accessing the SIP registrar server.
    Default is **0**.
11. Press **Done** to save the changes.

Enabling/Disabling the Use of the Registrar Server:

12. Select **SIP Register**.
13. Press **Change** to set Register to "**Yes**" (enable) or "**No**" (disable). Default is “**Yes**”.
    This parameter enables/disables the IP phone to register on the network.
14. Press **Done** to save the changes.

    Note: The session prompts you to restart the IP phone to apply the configuration settings.

15. Select **Restart.**

For the 6867i/6869i/6920/6930:

Note: You can set global configuration only using the IP Phone UI.

IP PHONE UI

1. Press or on the phone to enter the Options List.
2. Press the **Advanced** softkey.
3. Enter the Administrator password using the keypad. Default is “**22222**”.
4. Select **SIP > Call Server**.

Configuring Proxy IP and Proxy Port:

5. In the **Proxy Server** field, enter an IP address or fully qualified host name in the **Proxy Server** field. Default is **0.0.0.0**.
6. In the **Proxy Port** field, enter a Proxy Port number in the **Proxy Port** field for accessing the SIP proxy server. For example, **5060**. Default is **0**.

Configuring Registrar IP and Registrar Port:

7. In the **Registrar Server,** enter an IP address or fully qualified host name in the **Registrar Server** field. Default is **0.0.0.0**.
   A global value of 0.0.0.0 disables registration. However, the phone is still active and you can dial using username@ip address of the phone.
   If the Registrar IP address is set to 0.0.0.0 for a per-line basis (i.e, line 1, line 2, etc.), then the register request is not sent, the "No Service" message does not display, and the message waiting indicator (MWI) does not come on.
8. In the **Registrar Port** field, enter a Registrar Port number in the **Registrar Port** field for accessing the SIP registrar server. For example, **5060**. Default is **0**.
9. Press the **Save** softkey.

For the 6873i/6940:

Note: You can set global configuration only using the IP Phone UI.

IP PHONE UI

1. Press or on the phone to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password and press the blue Enter key. Default is “**22222**”.

4. Tap the **SIP** icon.

> **Note:** If required, swipe left on the screen to navigate to the second page of options.

5. Tap the **Call Server** icon.

Configuring Proxy IP and Proxy Port:

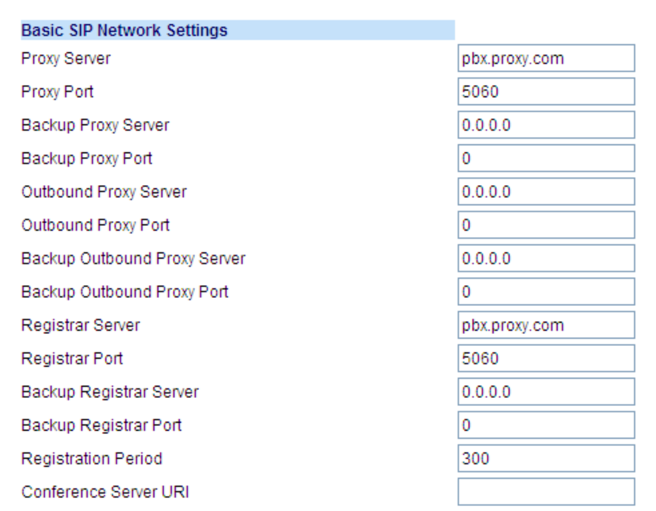
6. In the **Proxy Server** field, enter an IP address or fully qualified host name in the **Proxy Server** field. Default is **0.0.0.0**.
7. In the **Proxy Port** field, enter a Proxy Port number in the **Proxy Port** field for accessing the SIP proxy server. For example, **5060**. Default is **0**.

Configuring Registrar IP and Registrar Port:

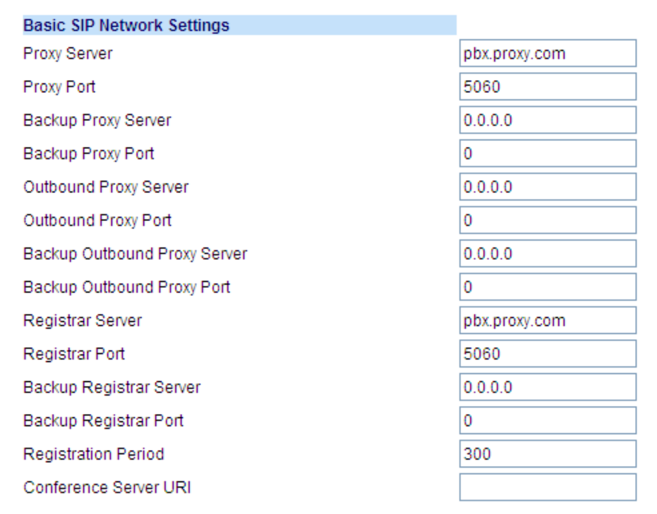
8. In the **Registrar Server,** enter an IP address or fully qualified host name in the **Registrar Server** field. Default is **0.0.0.0**.
   A global value of 0.0.0.0 disables registration. However, the phone is still active and you can dial using username@ip address of the phone.
   If the Registrar IP address is set to 0.0.0.0 for a per-line basis (i.e, line 1, line 2, etc.), then the register request is not sent, the "No Service" message does not display, and the message waiting indicator (MWI) does not come on.
9. In the **Registrar Port** field, enter a Registrar Port number in the **Registrar Port** field for accessing the SIP registrar server. For example, **5060**. Default is **0**.
10. Tap the **Save** softkey.
11. Restart the phone for the changes to take affect.

MITEL WEB UI

1. For global configuration, click on **Advanced Settings->Global SIP->Basic SIP Network Settings.**



2. Or, for per-line configuration, click on **Advanced Settings->Line *N* ->Basic SIP Network Settings**.



3. In the "**Proxy Server**" field, enter an IP address or fully qualified host name of the SIP proxy server.
4. In the "**Proxy Port**" field, enter a port number for accessing the SIP proxy server.
5. In the "**Backup Proxy Server**" field, enter an IP address or fully qualified host name for the backup proxy server.
6. In the "**Backup Proxy Port**" field, enter a port number for accessing the backup proxy server.
7. In the "**Outbound Proxy Server**" field, enter the SIP outbound proxy server IP address or fully qualified domain name. This parameter allows all SIP messages originating from a line on the IP phone, to be sent to an outbound proxy server.

   Note: If you configure an outbound proxy and registrar for a specific line, and you also configure a global outbound proxy and registrar, the IP phone uses the global configuration for all lines except line 1. Line 1 uses the outbound proxy and registrar that you configured for that line.

8. In the "**Outbound Proxy Port**" field, enter the port on the IP phone that allows SIP messages to be sent to the outbound proxy server.
9. In the "**Backup Outbound Proxy Server**" field, enter the backup SIP outbound proxy server IP address or fully qualified domain name.
10. In the "**Backup Outbound Proxy Port**" field, enter the port on the IP phone that allows SIP messages to be sent to the backup outbound proxy server.
11. In the "**Registrar Server**" field, enter an IP address or fully qualified host name for the SIP registrar server. A global value of 0.0.0.0 disables registration. However, the phone is still active and you can dial using username@ip address of the phone.
    If the Registrar IP address is set to 0.0.0.0 for a per-line basis (i.e. line 1, line 2, etc.), then the register request is not sent, the "No Service" message does not display, and the message waiting indicator (MWI) does not come on.

12. In the "**Registrar Port**" field, enter the port number associated with the Registrar.
13. In the "**Backup Registrar Server**" field, enter an IP address or fully qualified host name for the backup registrar server. A global value of 0.0.0.0 disables registration. However, the phone is still active and you can dial using username@ip address of the phone.
    If the Backup Registrar IP address is set to 0.0.0.0 for a per-line basis (i.e. line 1, line 2, etc.), then the register request is not sent, the "No Service" message does not display, and the message waiting indicator (MWI) does not come on.
14. In the "**Backup Registrar Port**" field, enter the port number associated with the backup registrar.
15. In the "**Registration Period**" field, enter the requested registration period, in seconds, from the registrar.
16. To enter a value in the "**Conference Server URI**" field, see Chapter 5, the section, "Centralized Conferencing (for Sylantro and BroadSoft Servers)" on page 5-349.
17. Click **Save Settings** to save your changes.

HASH PASSWORD SUPPORT FOR SIP AUTHENTICATION

SIP phones support configuration of digest authentication (a1 hash) as opposed to the clear text password.

A new configuration parameter "**sip lineN hash**" is introduced in this release to support provisioning of digest authentication (a1 hash). When this parameter is configured, sip lineN hash will override the existing parameter "sip lineN password".

Configure Digest Authentication (a1 Hash) For SIP Authentication

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, section, Hash Password Setting For SIP Authentication on page A-102.

The following lists the limitations to the new parameter:

- Applies to lineN and global line
- Works with the 401 response and 407 response
- If the configuration parameter "mask sip password" is enabled, when local.cfg and server.cfg are downloaded from the troubleshooting page in Web UI, the hash value is masked.

ADVANCED SIP SETTINGS (OPTIONAL)

Advanced SIP Settings on the IP Phone allow you to configure specific features on the phone. The following table provides a list of Advanced SIP Settings that you can configure using the Mitel Web UI or the configuration files.

MITEL WEB UI PARAMETERS	CONFIGURATION FILE PARAMETERS
Explicit MWI Subscription	sip explicit mwi subscription
Explicit MWI Subscription Period	sip explicit mwi subscription period

MITEL WEB UI PARAMETERS	CONFIGURATION FILE PARAMETERS
MWI for BLA Account	sip mwi for bla account (see Chapter 5, "Configuring Operational Features")
AS-Feature-Event Subscription (global) AS-Feature-Event Subscription (per-line) (see Chapter 6, "Configuring Advanced Operational Features") AS-Feature Event Subscription Period (see Chapter 6, "Configuring Advanced Operational Features")	sip as-feature-event subscription (global) sip lineN as-feature-event subscription (per-line) (see Chapter 6, "Configuring Advanced Operational Features") sip as-feature-event subscription period (see Chapter 6, "Configuring Advanced Operational Features")
Send MAC Address in REGISTER Message (see Chapter 6, "Configuring Advanced Operational Features") Send Line Number in REGISTER Message (see Chapter 6, "Configuring Advanced Operational Features")	sip send mac (see Chapter 6, "Configuring Advanced Operational Features") sip send line (see Chapter 6, "Configuring Advanced Operational Features")
Session Timer	sip session timer
T1 Timer T2 Timer	sip T1 timer sip T2 timer
Transaction Timer	sip transaction timer
Transport Protocol	sip transport protocol
Local SIP UDP/TCP Port (see page 4-34)	sip local port (see page 4-34)
Local SIP TLS Port (see page 4-34)	sip local tls port (see page 4-34)
Registration Failed Retry Timer Registration Timeout Retry Timer Registration Renewal Timer	sip registration retry timer sip registration timeout retry timer sip registration renewal timer
N/A N/A	sip subscription timeout retry timer sip subscription failed retry timer
BLF Subscription Period (see Chapter 5, "Configuring Operational Features")	sip blf subscription period (see Chapter 5, "Configuring Operational Features")
ACD Subscription Period (see Chapter 5, "Configuring Operational Features")	sip acd subscription period (see Chapter 5, "Configuring Operational Features")
BLA Subscription Period (see Chapter 5, "Configuring Operational Features")	sip acd subscription period (see Chapter 5, "Configuring Operational Features")
Blacklist Duration (see Chapter 6, "Configuring Advanced Operational Features")	sip blacklist duration (see Chapter 6, "Configuring Advanced Operational Features")
Whitelist Proxy (see Chapter 6, "Configuring Advanced Operational Features")	sip whitelist (see Chapter 6, "Configuring Advanced Operational Features")

MITEL WEB UI PARAMETERS	CONFIGURATION FILE PARAMETERS
XML SIP Notify (see Chapter 6, "Configuring Advanced Operational Features")	XML SIP Notify (see Chapter 6, "Configuring Advanced Operational Features")

The "**sip subscription timeout retry timer**" and "**sip subscription failed retry timer**" are only configurable through the configuration files. The "**sip subscription timeout retry timer**" parameter can be used to control how long the phone delays then retries a subscription when a SUBSCRIBE request is responded with a 408 (timeout) or 503 (service unavailable) error code. The "**sip subscription failed retry timer**" parameter can be used to control how long the phone delays then retries a subscription when a SUBSCRIBE request is responded with error codes other than 408 or 503.

If any one of the above parameters are configured with a valid setting, the default retry times for all event packages will be overwritten with the new setting. If the parameters are not configured or contains a invalid setting, the default retry timers for all event packages will be retained. Both parameters are disabled by default.

Reference

Refer to Appendix A,"Advanced SIP Settings" on page 116 for a description of each of the above parameters.

For more information about Blacklist Duration and Whitelist Proxy, see Chapter 6, "Configuring Advanced Operational Features."

CONFIGURING ADVANCED SIP SETTINGS

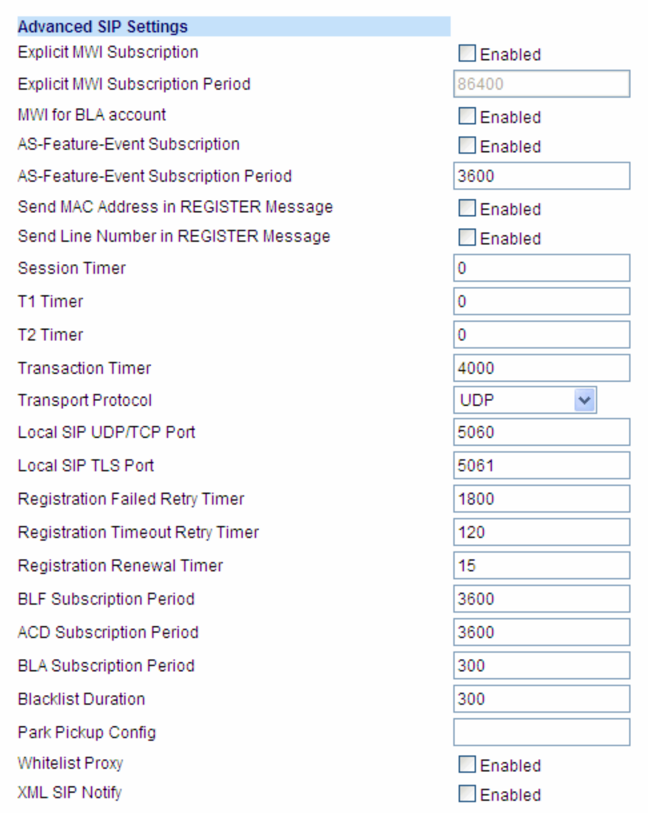
Use the following procedures to configure the advanced SIP settings on the IP phone.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Advanced SIP Settings" on page A-116.

MITEL WEB UI

1. For Global configuration, click on **Advanced Settings->Global SIP->Advanced SIP Settings.**



Or for per-line configuration, click on **Advanced Settings->Line *N*.**

2. Enable the "**Explicit MWI Subscription**" field by checking the check box.
(Disable this field by unchecking the check box. Default is disabled).
If the IP phone has a message waiting subscription with the Service Provider, a Message Waiting Indicator (MWI) (LED or display icon) tells the user there is a message on the IP Phone.

3. If you enable the “**Explicit MWI Subscription**” field, then in the “**Explicit MWI Subscription Period**” field, enter the requested duration, in seconds, before the MWI subscription times out. The phone re-subscribes to MWI before the subscription period ends. Default is 86400.

4. Enable the “**MWI for BLA Account**” to enable or disable a BLA configured line to send an MWI SUBSCRIBE message for the BLA account.

Notes:

1. If you change the setting on this parameter, you must reboot the phone for it to take affect.
2. Both the “sip explicit mwi subscription” and “sip mwi for bla account” parameters must be enabled in order for the MWI subscription for BLA to occur.
3. The MWI re-subscription for the BLA account uses the value set for the "sip explicit mwi subscription period" parameter to re-subscribe.
4. Whether or not the "sip mwi for bla account" parameter is enabled, the priority for displaying MWI does not change.

5. Enable the “**AS-Feature-Event Subscription**” field by checking the check box.
(Disable this field by unchecking the check box. Default is disabled).
This feature enables or disables the specified line with the BroadSoft’s server-side DND, CFWD, or ACD features.
For more information about this feature, see Chapter 6, the section, “As-Feature-Event Subscription” on page 6-15.

Note: The “AS-Feature-Event Subscription” feature is configurable on a global or per-line basis.

6. If you enable the “**AS-Feature-Event Subscription**” field, then in the “**AS-Feature-Event Subscription Period**” field, enter the amount of time, in seconds, between re-subscribing. If the phone does not re-subscribe in the time specified for this parameter, it loses subscription. Default is 3600.
For more information about this feature, see Chapter 6, the section, “As-Feature-Event Subscription” on page 6-15.

7. Enable the “**Send MAC Address in REGISTER Message**” and the “**Send Line Number in REGISTER Message**” fields by checking the check boxes.
(Disable these fields by unchecking the check boxes. Default is disabled for both fields).
For more information about these message features, see Chapter 6, the section, “TR-069 Support” on page 6-8.

Note: The “AS-Feature-Event Subscription Period” feature is configurable on a global basis only.

8. In the "**Session Timer**" field, enter the time, in seconds, that the IP phone uses to send periodic re-*INVITE* requests to keep a session alive. The proxy uses these re-*INVITE* requests to maintain the status' of the connected sessions. See RFC4028 for details.

9. In the "**Timer 1** and **Timer 2**" fields, enter a time, in milliseconds, that will apply to an IP phone session. These timers are SIP transaction layer timers defined in RFC 3261.
Timer 1 is an estimate of the round-trip time (RTT). Default is 500 msec.
Timer 2 represents the amount of time a non-INVITE server transaction takes to respond to a request. Default is 4 seconds.

10. In the "**Transaction Timer**" field, enter the amount of time, in milliseconds, that the phone allows the call server (registrar/proxy) to respond to SIP messages that it sends.
    Valid values are 4000 to 64000. Default is 4000.

    Note: If the phone does not receive a response in the amount of time designated for this parameter, the phone assumes the message has timed out

11. In the "**Transport Protocol"** field, select a transport protocol to use when sending SIP Real-time Transport Protocol (RTP) packets. Valid values are User Datagram Protocol (UDP) and Transmission Control Protocol (TCP), UDP, TCP, Transport Layer Security (TLS) or Persistent TLS. The value "**UDP**" is the default. For more information about TLS, see "RTP Encryption" on page 4-95 and Chapter 6, the section, "Transport Layer Security (TLS)" on page 6-22.

12. In the "**Local SIP UDP/TCP Port"** field, specify the local source port (UDP/TCP) from which the phone receives SIP messages. Default is 5060.
    For more information about this feature, see the section, "SIP and TLS Source Ports" on page 4-34.

13. In the "**Local SIP TLS Port"** field, specify the local source port (SIPS/TLS) from which the phone sends SIP messages. Default is 5061.
    For more information about this feature, see the section, "SIP and TLS Source Ports" on page 4-34.

14. In the "**Registration Failed Retry Timer"** field, enter the amount of time, in seconds, that the phone waits between registration attempts when a registration is rejected by the registrar.
    Valid values are 30 to 1800. Default is 1800.

15. In the "**Registration Timeout Retry Timer**" field, enter the amount of time, in seconds, that the phone waits until it re-attempts to register after a REGISTER message times out.
    Valid values are 30 to 2147483647. Default is 120.

16. In the "**Registration Renewal Timer**" field, enter the threshold value, in seconds, prior to expiration, that the phone renews registrations. The phone will automatically send registration renewals half-way through the registration period, unless half-way is more than the threshold value.
    For example, if the threshold value is set to 60 seconds and if the registration period is 600 seconds, the renewal REGISTER message will be sent 60 seconds prior to the expiration, as half-way (600/2) > 60. If the registration period was 100 seconds, then the renewal would be sent at the half-way point as (100/2) < 60.
    Valid values are 0 to 2147483647. Default is 15.

17. The "**BLF Subscription Period**" field is enabled by default with a value of 3600 seconds. This feature sets the duration, in seconds, before the BLF subscription times out. The phone re-subscribes to the BLF subscription service before the defined subscription period ends.

    Note: This parameter is not applicable to BLF/List subscriptions.

    For information about setting the "BLF Subscription Period", see Chapter 5, the section, "BLF Subscription Period" on page 5-200.

18. (For Sylantro/BroadWorks servers) The “**ACD Subscription Period**” field is enabled by default with a value of 3600 seconds.
This feature sets the time period, in seconds, that the IP phone re-subscribes the BLF subscription service after a software/firmware upgrade or after a reboot of the IP phone.
For information about setting the “ACD Subscription Period”, see Chapter 5, the section, “ACD Subscription Period” on page 5-217.

19. The “**BLA Subscription Period**” field is enabled by default with a value of 300 seconds.
This feature sets the amount of time, in seconds, that the phone waits to receive a BLA subscribe message from the server. If you specify zero (0), the phone uses the value specified for the BLA expiration in the subscribe message received from the server. If no value is specified, the phone uses the default value of 300 seconds.
For information about setting the “BLA Subscription Period”, see Chapter 5, the section, “BLA Subscription Period” on page 5-232.

20. (For BroadSoft Servers) The “**Blacklist Duration**” field is enabled by default with a value of 300 seconds (5 minutes). Valid values are 0 to 9999999.
This feature specifies the length of time, in seconds, that a failed server remains on the server blacklist. The IP phone avoids sending a SIP message to a failed server (if another server is available) for this amount of time.

Note: The value of “**0**” disables the blacklist feature.

21. For information about setting the “Blacklist Duration”, see Chapter 6, the section, “Blacklist Duration” on page 6-17.

22. In the “**Park Pickup Config**” field, enter the appropriate value based on the server in your network.

Notes:

1. For values to enter in this field, see the table “Park/Pickup Call Server Configuration Values” on page 5-247.
2. Leave the park/pickup configuration field blank to disable the park and pickup feature.

23. Enable the "**Whitelist Proxy**" field by checking the check box.
(Disable this field by unchecking the check box. Default is disabled).
When this feature is enabled, an IP phone accepts call requests from a trusted proxy server *only*. The IP phone rejects any call requests from an untrusted proxy server.
For information about setting the “Whitelist Proxy”, see Chapter 6, the section, “Whitelist Proxy” on page 6-19.

24. Enable the "**XML SIP Notify**" field by checking the check box.
(Disable this field by unchecking the check box. Default is disabled).
Enabling this parameter allows the phone to accept or reject an aastra-xml SIP NOTIFY message.

Note: To ensure the SIP NOTIFY is coming from a trusted source, it is recommended that you enable the Whitelist feature (**Whitelist Proxy** parameter) on the IP phone. If enabled, and the phone receives a SIP NOTIFY from a server that is NOT on the whitelist (i.e. untrusted server), the phone rejects the message.

For information about setting this feature, see Chapter 5, the section, "XML SIP Notify Events" on page 5-338.

25. Click **Save Settings** to save your changes.

REAL-TIME TRANSPORT PROTOCOL (RTP) SETTINGS

Real-time Transport Protocol (RTP) is used as the bearer path for voice packets sent over the IP network. Information in the RTP header tells the receiver how to reconstruct the data and describes how the bit streams are packetized (i.e. which codec is in use). Real-time Transport Control Protocol (RTCP) allows endpoints to monitor packet delivery, detect and compensate for any packet loss in the network. Session Initiation Protocol (SIP) and H.323 both use RTP and RTCP for the media stream, with User Datagram Protocol (UDP) as the transport layer encapsulation protocol.

Note: If RFC2833 relay of DTMF tones is configured, it is sent on the same port as the RTP voice packets. The phones support decoding and playing out DTMF tones sent in SIP INFO requests. The following DTMF tones are supported:

- Support signals 0-9, #, *
- Support durations up to 5 seconds

You can set the following parameters for RTP on the IP Phones:

MITEL WEB UI PARAMETERS	CONFIGURATION FILE PARAMETERS
RTP Port	sip rtp port
Basic Codecs (G.711 u-Law, G.711 a-Law, G.729)	sip use basic codecs
AMR and AMR-WB (G.722.2) Codecs (Licensed feature)	sip amr codec payload format sip amr codec mode set sip amr wb codec mode set
Force RFC2833 Out-of-Band DTMF	sip out-of-band dtmf
Customized Codec Preference List	sip customized codec
DTMF Method (global and per-line settings)	sip dtmf method (global and per-line settings)
RTP Encryption (global and per-line settings)	sip srtp mode (global and per-line settings)
Silence Suppression	sip silence suppression

RTP PORT

RTP is described in RFC1889. The UDP port used for RTP streams is traditionally an even-numbered port, and the RTCP control is on the next port up. A phone call therefore uses one pair of ports for each media stream.

The RTP port is assigned to the first line on the phone, and is then incremented for each subsequent line available within the phone to provided each line a unique RTP port for its own use.

On the IP phone, the initial port used as the starting point for RTP/RTCP port allocation can be configured using "**RTP Port Base**". The default RTP base port on the IP phones is 3000.

For example, if the RTP base port value is 5000, the first voice patch sends RTP on port 5000 and RTCP on port 5001. Additional calls would then use ports 5002, 5003, etc.

You can configure the RTP port on a global-basis only, using the configuration files, the IP Phone UI, or the Mitel Web UI.

SYMMETRICAL/ASYMMETRICAL RTP PORT HANDLING

By default, the phone supports symmetrical RTP port handling (i.e. the phone will only play an RTP stream if it comes from a "source" port that is the same as the "listening" port negotiated by the call manager.

Administrators can configure the phones to support asymmetrical RTP port handling by defining the "**rtp symmetric port**" parameter as "**0**". By defining the parameter as "0" (i.e. disabling symmetrical RTP port handling), the phone will accept the RTP stream coming from the different "source" port and send RTP traffic to the caller at the "listening" port.

You can configure symmetrical/asymmetrical RTP port handling behavior using the configuration files only.

BASIC CODECS (G.711 U-LAW, G.711 A-LAW, G.729)

CODEC is an acronym for **CO**mpress-**DEC**ompress. It consists of a set of instructions that together implement one or more algorithms. In the case of IP telephony, these algorithms are used to compress the sampled speech data, to decrease the content's file size and bit-rate (the amount of network bandwidth in kilobits per second) required to transfer the audio. With smaller file sizes and lower bit rates, the network equipment can store and stream digital media content over a network more easily.

Mitel IP phones support the International Telecommunications Union (ITU) transmission standards for the following CODECs:

- **Waveform CODECs**: G.711 pulse code modulation (PCM) with a-Law or u-Law companding
- **Parametric CODEC**: G.729a conjugate structure - algebraic code excited linear prediction (CS_ACELP)

All codecs have a sampling rate of 8,000 samples per second, and operate in the 300 Hz to 3,700 Hz audio range. The following table lists the default settings for bit rate, algorithm, packetization time, and silence suppression for each codec, based on a minimum packet size.

Default Codec Settings

CODEC	BIT RATE	ALGORITHM	PACKETIZATION TIME	SILENCE SUPPRESSION
G.711 a-law	64 Kb/s	PCM	30 ms	enabled
G.711 u-law	64 Kb/s	PCM	30 ms	enabled
G.729a	8 Kb/s	CS-ACELP	30 ms	enabled

You can enable the IP phones to use a default "basic" codec set, which consists of the set of codecs and packet sizes shown above;

or
you can configure a custom set of codecs and attributes instead of using the defaults (see "Customized Codec Preference List" below).

Note: The basic and custom codec parameters apply to all calls, and are configured on a global-basis only using the configuration files or the Mitel Web UI.

AMR AND AMR-WB (G722.2) CODECS (LICENSED FEATURE)

Administrators can configure Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR -WB) codecs on the 6863i, 6865i, 6867i, 6869i, and 6873i IP phones. AMR/AMR-WB codecs provide improved speech quality during calls due to wider speech bandwidth, and cover both real-time transfers through Real-time Transport Protocol (RTP) and non-real-time transfers through stored files. AMR supports eight narrowband speech encoding modes (0-7) with bit-rates ranging from 4.75 to 12.2 kilobits per second (kbps). AMR-WB supports nine wideband speech encoding modes (0-8), with bit-rates ranging from 6.60 to 23.85 kbps.

Note: AMR/AMR-WB codecs is a licensed feature on the SIP IP phones. To confirm that the license is active, Administrators can view the license through the phone's Web UI on the Licensing Status page. AMR/AMR-WB should be listed if the feature is available to be used. If Administrators configure AMR/AMR-WB when there is no license, the codec will be ignored and not negotiated.

Administrators can configure AMR/AMR-WB on the IP phones in the **Customized Codec Preference List** on the Web UI or in the configuration files using the existing "**sip customized codec**" parameter.

Optional parameters have also been created to configure this feature. Administrators can enable the feature by using the "**sip amr codec payload format**", which specifies the payload format for AMR/AMR-WB. AMR/AMR-WB can operate in either bandwidth-efficient mode (0) or in octet-aligned mode (1), depending on the value configured. Administrators can also disable the octet-align mode and still send the octet-align:0 header in the Session Description Protocol (SDP) by using value (2) for the parameter. By default, the IP phones utilize bandwidth-efficient mode.

Administrators can also specify the list of mode sets that the IP phones support and state the preferred mode to use if multiple modes are supported by both sides, using the "**sip amr codec mode set**" and/or the "**sip amr wb codec mode set**" parameters. If no modes are defined then all codec modes are allowed for the payload type.

The following tables list the AMR/AMR-WB codec modes and corresponding bit-rates.

AMR Codec Modes

AMR MODE	BIT-RATE (KBPS)
0	4.75
1	5.15
2	5.90
3	6.70
4	7.40
5	7.95
6	10.2
7	12.2

AMR-WB (G.722.2) Codec Modes

AMR-WB MODE	BIT-RATE (KBPS)
0	6.60
1	8.85
2	12.65
3	14.25
4	15.85
5	18.25
6	19.85
7	23.05
8	23.85

DTMF SUPPORT FOR TELEPHONE-EVENT

The IP phones support IMS/VoLTE deployments and end-to-end DTMF functioning without any transcoders in the carrier network. To enable this feature, IP phones must be signaled based on RFC4733 (DTMF, that is, Dual Tone-Multi Frequency) in combination with codecs having a clock rate of 8 KHz and 16 KHz. The default clock rate is 8 KHz. The clock rate of 16KHz for telephone-event is backward compatible. This feature does not work for clock rates higher than 16 KHz.

Note: This feature is supported on 6863i, 6865i, 6867i, 6869i, and 6873i IP phones that have the Broadcom PhoneExchange patch installed.

For this feature to work, no changes are required in the In-Band DTMF functionality. The Broadcom patch is adjusted to a clock rate of 16 KHz. The generated DTMF tone frequency cannot be verified.

Note: This feature supports RTP/AVP and RTP/SAVP streams; but, RTP/AVPF and RTP/SAVPF streams are not supported.

Depending on the voice codec used for the audio communication, the DTMF of the RTP telephony-event codec can be 8KHz or 16KHz. For example, if L16 codec which supports 16KHz is chosen for audio (as final offer-answer negotiation), a DTMF of clock rate 16Hz is selected.

According to RFC 4733, IP phones support a telephony-event for each audio codec with a different sample rate included in SDP.

- For a selected audio codec in offer-answer negotiation with a clock rate of 8KHz, a DTMF of clock rate 8KHz is selected.
- For a selected audio codec in offer-answer negotiation with a clock rate of 16KHz, a DTMF of clock rate 16KHz is selected.

Limitations

- When a caller is on a release that does not support this feature and the called party is on a release that supports this feature, and AMR-WB codec is supported on both the phones, the called party phone falls back to 8 KHz support as the caller does not support 16 KHz DTMF.
- When the caller is on a release that supports this feature and the called party is on a release that does not support this feature, and AMR-WB codec is supported on both the phones, the caller phone falls back to 8 KHz support as the called party does not support 16 KHz DTMF.
- While using narrowband and wideband codecs, if *a=rtpmap:99 telephone-event/16000/1* is not used, DTMF is not supported for codecs with a clock rate of 16 KHz.

CUSTOMIZED CODEC PREFERENCE LIST

You can also configure the IP phones to use preferred codecs. To do this, you must enter the payload value (**payload**), the packetization time in milliseconds (**ptime**), and enable or disable silence suppression (**silsupp**).

Payload is the codec type to be used. This represents the data format carried within the RTP packets to the end user at the destination. The default payload setting is to allow all codecs. You can set payload to use only basic codecs (G.711 u-Law, G.711 a-Law, G.729), and/or Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR -WB) (G.722.2) codecs (if a license is available), or select from up to 14 codecs for the phones AND customize a codec preference list of up to 10 codecs. In the Mitel Web UI, codecs 2 through 10 can be set to “None” if required (no codecs).

Note: In the Mitel Web UI:

- Setting Codec 1 to “All” ignores the packetization interval (ptime). The packetization interval setting defaults to 30, which is the default for all codecs.
- Setting Codec 1 to “All” automatically sets all other codec preference fields 2 through 10 to “None”.
- Setting Codec 1 to “Basic” and all other codec preferences in 2 through 10 to “None”, forces the phone to use only the basic codecs as in previous releases (G.711 u-law, G.711 a-law, and G.729). If you select an additional codec to use in the codec preferences 2 through 10 fields, those codecs are added to the list of Basic codecs for the phone to use.

Ptime (packetization time) is a measurement of the duration of PCM data within each RTP packet sent to the destination, and hence defines how much network bandwidth is used for transfer of the RTP stream. You enter the ptime values for the customized codec list in milliseconds. (See table below).

Silsupp is used to enable or disable silence suppression. Voice Activity Detection (VAD) on the IP phones is used to determine whether each individual packet contains useful speech data. Enabling **silsupp** results in decreased network bandwidth, by avoiding the transmission of RTP packets for any frame where no voice energy was detected by the VAD.

You must enter the values for this feature in list form as shown in the following example:

```
payload=8;ptime=10;silsupp=on,payload=0;ptime=10;silsupp=off
```

The valid values for creating a codec preference list are as follows (in numerical order of payload).

Customized Codec Settings

ATTRIBUTE	VALUE	
payload	Configuration Files	Web UI
	0 - G711u/8000	G.711u (8K)
Codec 1	8 - G711a/8000	G.711a (8K)
Codec 2	9 - G722/8000	G.722
.	18 - G729/8000	G.729
.	96 - G726-40/8000	G.726-40
.	97 - G726-24/8000	G.726-24
.	98 - G726-16/8000	G.726-16
.	110 - G711u/16000	G711u (16K)
Codec 10	111 - G711a/16000	G711a (16K)
(in Web UI)	112 - L16/8000	L16 (8K)
	113 - L16/16000	L16 (16K)
	115 - G726-32/8000	G.726-32
	118 - AMR	AMR (Licensed feature)
	119 - AMR-WB G.722.2	AMR-WB (Licensed feature)
	Leave blank for all codecs	All (Codec 1 only)
		Basic (Codec 1 only)
		None (Codecs 2 thru 10 only)
ptime (in milliseconds) Packetization Interval (in Web UI)	5, 10, 15, 20.......90	
silsupp Silence Suppression (in Web UI)	on off	

If the customized codec preference list is configured as “All”, the phone will set the codec order of preference as per the following table:

PREFERENCE	PAYLOAD	CODEC
1	0	G711u/8000
2	18	G729/8000
3	113	L16/16000
4	110	G711u/16000
5	111	G711a/16000
6	112	L16/8000
7	98	G726-16/8000
8	97	G726-24/8000
9	115	G726-32/8000
10	96	G726-40/8000
11	9	G722/8000
12	8	G711a/8000
13	118	AMR (Licensed feature)
14	119	AMR-WB (G.722.2) (Licensed feature)

You can specify a customized codec preference list on a global-basis using the configuration files or the Mitel Web UI.

OUT-OF-BAND DTMF AND DTMF METHOD

The IP phones support out-of-band Dual-Tone Multifrequency (DTMF) mode as referenced in RFC2833. In the Mitel Web UI, you can enable or disable this feature as required. The "out-of-band DTMF" is enabled by default. In out-of-band mode, the DTMF audio is automatically clamped (muted) and DTMF digits are not sent in the RTP packets. You can configure out-of-band DTMF on a global-basis using the configuration files or the Mitel Web UI.

An additional feature on the IP phone allows you to select the DTMF method that the phone uses to send DTMF digits from the IP phone via INFO messages. You can set the DTMF method as Real-Time Transport Protocol (RTP), SIP INFO, or both. You can configure the DTMF method on a global or per-line basis using the configuration files or the Mitel Web UI.

The matrix below details DTMF behavior when the out-of-band DTMF and DTMF method settings are configured in various scenarios:

WEB UI SETTING/CONFIGURATION PARAMETER SETTING		DTMF BEHAVIOR		
DTMF METHOD/ SIP DTMF METHOD	FORCE RFC2833 OUT-OF-BAND DTMF/ SIP OUT-OF-BAND DTMF	SIP INFO	IN-BAND DTMF	OUT-OF-BAND DTMF (RFC2833)
RTP (0)	Disabled (0)	No	Yes	No
RTP (0)	Enabled (1)	No	No	Yes
SIP INFO (1)	Disabled (0)	Yes	No	No
SIP INFO (1)	Enabled (1)	Yes	No	Yes
RTP and SIP INFO (2)	Disabled (0)	Yes	Yes	No
RTP and SIP INFO (2)	Enabled (1)	Yes	No	Yes

RTP ENCRYPTION

The IP Phones include support for Secure Real-time Transfer Protocol (SRTP), using Session Description Protocol Security (SDES) key negotiation, for encryption and authentication of RTP/RTCP messages sent and received by the Mitel IP phones on your network.

As administrator, you specify the global SRTP setting for all lines on the IP phone. You can choose among three levels of SRTP encryption, as follows:

- **SRTP Disabled (default)**: IP phone generates and receives non-secured RTP calls. If the IP phone gets called from SRTP enabled phone, it ignores SRTP tries to answer the call using RTP. If the receiving phone has SRTP only enabled, the call fails; however, if it has SRTP preferred enabled, it will accept RTP call.
- **SRTP Preferred**: IP phone generates RTP secured calls, and accepts both secured and non-secured RTP calls. If the receiving phone is not SRTP enabled, it sends non-secured RTP calls instead.
- **SRTP Only**: IP phone generates and accepts RTP secured calls only; all other calls are rejected (fail).
- **SRTP and RTP**: IP phone generates both secured and non-secured RTP calls, and accepts both secured and non-secured RTP calls.

Note: SRTP and RTP mode is only supported for Mitel MiVoice Connect and Mitel MiCloud Connect platforms. This mode is not supported for any other SIP call manager/servers.

You can override the global setting as necessary, configuring SRTP support on a per-line basis. This allows IP phone users to have both secured and unsecured lines operating on the same phone.

When an active call is using SRTP (i.e. when an SRTP enabled IP phone initiates a call and the receiving phone is also SRTP enabled) and the transport protocol is set to TLS, the IP

Phone UI displays a “lock” icon, indicating that the call is secure. If one of the phones does not support SRTP and/or TLS is not enabled, the IP Phone UIs do not display the lock icon, indicating that the call may not be secure.

Note: If you enable SRTP, then you should also enable Transport Layer Security (TLS). This prevents capture of the key used for SRTP encryption. To enable TLS, set the **Transport Protocol** parameter (located on the Global SIP Settings menu) to **TLS**.

You can configure SRTP on a global or per-line basis using the configuration files or the Mitel Web UI.

SILENCE SUPPRESSION

In IP telephony, silence on a line (lack of voice) uses up bandwidth when sending voice over a packet-switched system. Silence suppression is encoding that starts and stops the times of silence in order to eliminate that wasted bandwidth.

Silence suppression is enabled by default on the IP phones. The phone negotiates whether or not to use silence suppression. Disabling this feature forces the phone to ignore any negotiated value.

You can configure silence suppression on a global-basis using the configuration files or the Mitel Web UI.

Option to Include/Remove Silence Suppression Attribute from SDP Offer

The parameter **sip remove silence suppression offer** is available allowing administrators the ability to control whether or not the silence suppression attribute should be included in the Session Description Protocol (SDP) offer.

If enabled (1), the silence suppression attribute will be removed from the SDP offer. If disabled (0), the attribute will not be removed from the SDP offer. This parameter is disabled by default and requires a reboot if the value of the parameter has changed. You can configure this parameter using the configuration files only.

CONFIGURING RTP FEATURES

Use the following procedures to configure the RTP features on the IP phone.

CONFIGURATION FILES

For specific parameters you can set for RTP features in the configuration files, see Appendix A, the section, “RTP, Codec, DTMF Global Settings” on page A-136.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.

2. Select **Administrator Menu.**
3. Select **SIP Settings.**
4. Select **RTP Port Base** to change the RTP port base setting. Default is **3000**.
5. Press **Done** (2 times) to save the change.

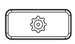
> **Note:** The session prompts you to restart the IP phone to apply the configuration settings

6. Select **Restart.**

For the 6867i/6869i/6920/6930:

1. Press  or  on the phone to enter the Options List.
2. Press the **Advanced** softkey.
3. Enter the Administrator password using the keypad. Default is “**22222**”.
4. Select **SIP > Call Server**.
5. In the **RTP Port Base** field, enter an RTP port base setting. Default is **3000**.
6. Press the **Save** softkey.
7. Restart the phone for the change to take affect.

For the 6873i/6940:

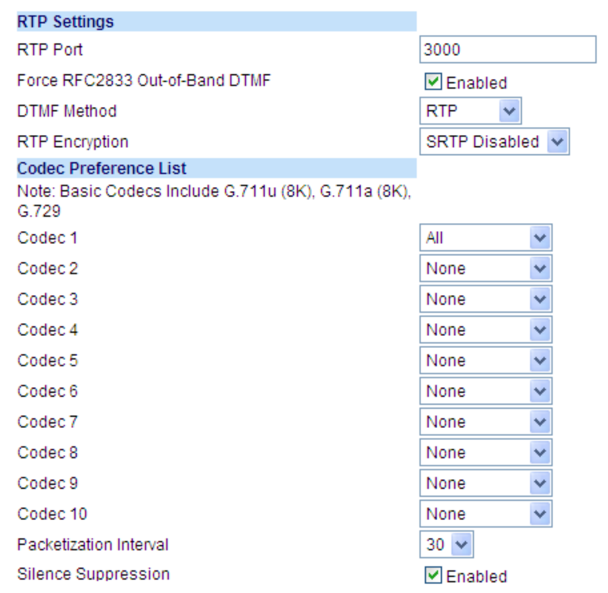
1. Press  or  on the phone to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password and press the blue Enter key. Default is “**22222**”.
4. Tap the **SIP** icon.

> **Note:** If required, swipe left on the screen to navigate to the second page of options.

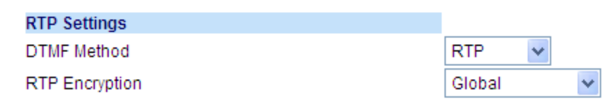
5. Tap the **Call Server** icon.
6. In the **RTP Port Base** field, enter an RTP port base setting. Default is **3000**.
7. Tap the **Save** softkey.
8. Restart the phone for the change to take affect.

MITEL WEB UI

1. Click on **Advanced Settings->Global SIP->RTP Settings.**
   Global Settings:



2. Click on **Advanced Settings->Line <N>->RTP Settings.**
   Per-Line Settings:



3. Enter an RTP Port Base in the **RTP Port** field. Default is **3000**.
   |The RTP Port indicates the port through which the RTP packets are sent. This value must specify the beginning of the RTP port range on the gateway or router. The RTP port is used for sending DTMF tones and for the audio stream. Your network administrator may close some ports for security reasons. You may want to use this parameter to send RTP data using a different port.

   Note: The phones support decoding and playing out DTMF tones sent in SIP INFO requests. The following DTMF tones are supported:

   - Support signals 0-9, #, *
   - Support durations up to 5 seconds

4. The "**Force RFC2833 Out-of-Band DTMF**" field is enabled by default. Disable this field by unchecking the box.
   Enabling this parameter forces the IP phone to use out-of-band DTMF according to RFC2833.

5. Select a method to use from the "**DTMF Method"** list box. Valid values are **RTP**, **SIP Info**, **Both**. Default is **RTP**.

> **Note:** You can configure the DTMF Method on a global or per-line basis.

6. Select the type of RTP encryption to use from the "**RTP Encryption"** list box. Valid values are **SRTP Disabled, SRTP Preferred, SRTP Only**, **or SRTP and RTP**. Default is **SRTP Disabled**.

> **Note:** You can configure RTP Encryption on a global or per-line basis.

7. In the **Codec Preference List**, select the desired codec you want the phones to use. Valid values are:
   - All
   - Basic (G.711 u-law, G.711 a-law, G.729)
   - G.722
   - G.711u (8K)
   - G.711u (16K)
   - G.711a (8K)
   - G.711a (16K)
   - G.729
   - G.726-16
   - G.726-24
   - G.726-32
   - G.726-40
   - L16 (8K)
   - L16 (16K)
   - AMR (Licensed feature)
   - AMR-WB (G.722.2) (Licensed feature)

> **Notes:**
>
> 1. Setting Codec 1 to "All" ignores the packetization interval (ptime). The packetization interval setting defaults to 30, which is the default for all codecs.
> 2. Setting Codec 1 to "All" automatically sets all other codec preference fields 2 through 10 to "None".
> 3. Setting Codec 1 to "Basic" and all other codec preferences in 2 through 10 to "None", forces the phone to use only the basic codecs as in previous releases (G.711 u-law, G.711 a-law, and G.729). If you select an additional codec to use in the codec preferences 2 through 10 fields, those codecs are added to the list of Basic codecs for the phone to use.

8. (Optional) In Codec 2 through Codec 10, select a preference of codecs to use on the phone. Valid values are:

- None
- G.722
- G.711u/8K
- G.711u/16K
- G.711a/8K
- G.711a/16K
- G.729
- G.726-16
- G.726-24
- G.726-32
- G.726-40
- L16 (8K)
- L16 (16K)
- AMR (Licensed feature)
- AMR-WB (G.722.2) (Licensed feature)

Note: You can select up to 9 codecs in addition to the codec you selected in step 7.

9. In the “**Packetization Interval**” field, select the time, in milliseconds. Valid values are 5 to 90, in increments of 5 milliseconds.
10. The “**Silence Suppression**” field is enabled by default. Disable this field by unchecking the check box.
    When enabled, the phone negotiates whether or not to use silence suppression. Disabling this feature forces the phone to ignore any negotiated value.
11. Click **Save Settings** to save your changes.

RTCP SUMMARY REPORTS

The IP phones include the capability of enabling/disabling the generation of RTCP summary reports using the SIP vq-rtcpxr event package. These RTCP summary reports include voice quality statistics according to draft-ietf-sipping-rtcp-summary-05 specifications including packet loss, jitter, and delay statistics, as well as call quality scores. When this feature is enabled, an RTCP summary report is sent at the end of each call via a PUBLISH message to the configured server (known as the collector).

In addition to enabling/disabling the generation of these reports, you must specify the hostname and port of the collector receiving the reports. Similar to the other IP Phone SIP account parameters, the RTCP summary report parameters can be set on a global or a per-line basis using the configuration files only.

The RTCP summary report parameters are:

- sip rtcp summary reports
- sip Line*N* rtcp summary reports

- sip rtcp summary report collector
- sip Line*N* rtcp summary report collector
- sip rtcp summary report collector port
- sip Line*N* rtcp summary report collector port

Note: The transport protocol used for RTCP summary reports is also configurable. Refer to "Configurable Transport Protocol for SIP Services and RTCP Summary Reports," on page 54 for more information.

LIMITATIONS

The following is a limitation when enabling RTCP summary reports on the phone:

- The call must be at least 5 seconds long in order to generate the RTCP extended reports.

CONFIGURING RTCP SUMMARY REPORTS

Use the following procedure to configure RTCP summary reports.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "RTCP Summary Reports" on page A-55.

AUTODIAL SETTINGS

The IP phones include a feature called "Autodial". When you configure Autodial on an IP phone, the phone automatically dials a pre-configured number whenever it is off-hook. Depending on the configuration you specify, the Autodial functions as either a "**hotline**", or as a "**warmline**," as follows:

- **Hotline (default)**: The IP phone immediately dials a preconfigured number when you lift the handset.
- **Warmline**: The IP phone waits for a specified amount of time after you lift the handset before dialing a pre-configured number. If you do not dial a number within the time allotted, then the IP phone begins to dial the number.

By default, the Autodial feature functions as a hotline. If you want Autodial to function as a warmline, you can use the Autodial "time-out" parameter to specify the length of time (in seconds) the IP phone waits before dialing a pre-configured number.

As administrator, you configure Autodial globally, or on a per-line basis, for an IP phone. The line setting overrides the global setting. For example, you can disable Autodial on a specific line simply by setting the line's autodial number parameter to empty (blank).

WARNING:BEFORE CONFIGURING AUTODIAL ON YOUR IP PHONE:

- **ANY SPEEDDIAL NUMBERS THAT YOU CONFIGURE ON AN IP PHONE ARE NOT AFFECTED BY AUTODIAL SETTINGS.**
- **IF YOU CONFIGURE AUTODIAL ON YOUR IP PHONE, ANY LINES THAT FUNCTION AS HOTLINES DO NOT ACCEPT CONFERENCE CALLS, TRANSFERRED CALLS, AND/OR INTERCOM CALLS.**

CONFIGURING AUTODIAL USING THE CONFIGURATION FILES

You use the following parameters to configure Autodial using the configuration files:

Global Configuration:

- sip autodial number
- sip autodial timeout

Per-Line Configuration:

- sip lineN autodial number
- sip lineN autodial timeout

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Autodial Settings" on page A-144.

CONFIGURING AUTODIAL USING THE MITEL WEB UI

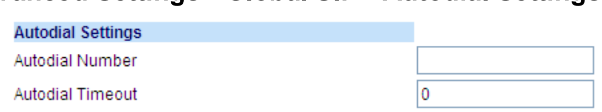
Use the following procedure to configure Autodial using the Mitel Web UI.

By default, your IP phone uses the global settings you specify for Autodial for all lines on your IP phone. However, you can also configure Autodial on a per-line basis.

MITEL WEB UI

Global Configuration:

1. Click on **Advanced Settings->Global SIP->Autodial Settings.**

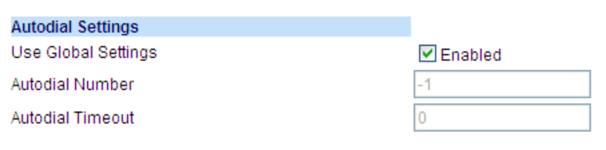


2. In the "**Autodial Number**" field, specify the SIP number that the IP phone dials whenever the IP phone is off-hook. An empty (blank) value disables autodial on the phone.
   For example: **8500**
3. In the **"Autodial Timeout"** field, specify a value, in seconds, for the timer as follows:
   - If you want the IP phone to autodial the number immediately (hotline) whenever the IP phone is off-hook, accept the default value of **0.**
   - If you want to specify a length of time for the IP phone to wait before dialing the number, enter the length of time (in seconds). For example: **30**

   Valid values are 0 to 120.
4. Click **Save Settings** to save your changes.

Per-Line Configuration:

1. Click on **Advanced Settings->Line N ->Autodial Settings.**



2. Perform one of the following actions:
   - To allow this line to use the global autodial settings, click on the **Use Global Settings** parameter to enable it, then click **Save Settings** to save your changes.
   - To specify a different autodial configuration for this specific line, disable the **Use Global Settings** parameter. Then proceed to step 3.
3. In the "**Autodial Number**" field, specify the SIP number for this line that the IP phone dials whenever the IP phone is off-hook as follows:
   - If set to -1, then the global autodial settings for this IP phone to this line.
   - If set to empty (blank), then disable Autodial on this line.
   - If set to a valid SIP number, dial the SIP number specified for this line. For example: **8500**
4. In the **"Autodial Timeout"** field, specify a value, in seconds, for the timer for this line as follows:
   - If you want the IP phone to autodial the number immediately (hotline) whenever the IP phone is off-hook, accept the default value of **0.**
   - If you want to specify a length of time for the IP phone to wait before dialing the number, enter the length of time (in seconds). For example: **30**
     Valid values are 0 to 120.
5. Click **Save Settings** to save your changes.

CONFIGURATION SERVER PROTOCOL

You can download new versions of firmware and configuration files from the configuration server to the IP phone using any of the following types of protocols: TFTP, FTP, HTTP, and HTTPS. For each Protocol, you can specify the path for which the configuration files are located on the server. For HTTP and HTTPS, you can also specify the port number to use for downloading the phone configuration. For FTP, you can configure a Username and Password that are authenticated by the FTP server.

The TFTP setting is the default download protocol. You can configure the type of protocol that the IP phones use by setting it in the configuration files, the IP phone UI, or the Mitel Web UI.

Note: For DHCP to automatically populate the IP address or domain name for the TFTP, FTP, HTTP, or HTTPS server, your DHCP server must support download protocol as referenced in RFC2131 and RFC1541 for Option 66. For more information, see this chapter, the section, "DHCP" on page 4-4.

CONFIGURING THE CONFIGURATION SERVER PROTOCOL

Use the following procedure to configure the configuration server protocol.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Configuration Server Settings" on page A-33.

For the 6863i/6865i/6905/6910:

IP PHONE UI

1. Press ⚙ or ⚙ on the phone to enter the Options List.
2. Select **Administrator Menu.**
3. Select **Configuration Server**.
4. Select **Download Protocol.**
5. Select from the following:
   - Use TFTP
   - Use FTP
   - Use HTTP
   - Use HTTPS

   Default is "**Use TFTP**".
   The IP phone uses the protocol you select to download new firmware and configuration files from the configuration server.
6. Press **Set** to save the changes.

7. From the Configuration Server menu, select from the following. This selection is dependent on the Download Protocol you selected in step 6.
   - TFTP Settings
   - FTP Settings
   - HTTP Settings
   - HTTPS Settings
8. Enter the IP address of the protocol server (in dotted decimal format).

9. Use the following table to configure the applicable server.

TFTP SETTINGS

- Select **Primary TFTP**
- Enter the IP address or fully qualified domain name of the primary TFTP server.
- Press **Done** or **Set** to save the change.
- Select **Pri TFTP Path**.
- Enter the path name for which the configuration files reside on the TFTP server for downloading to the IP Phone. If the IP phone's files are located in a sub-directory beneath the server's root directory, the relative path to that sub-directory should be entered in this field. Enter the path name in the form *folderX\folderX\folderX*. For example, ***ipphone\6863i\configfiles.***
- **Optional**: You can also configure an Alternate TFTP server and Alternate TFTP Path if required by selecting the "Alternate TFTP" and the "Alt TFTP Path" parameters.
- From the TFTP Settings menu, select **Alternate TFTP** and press Enter.
- Enter the IP address or fully qualified domain name of the alternate TFTP server.
- Press **Done** or **Set** to save the change.
- Select **Alt TFTP Path**.
- Enter the path name for which the configuration files reside on the Alternate TFTP server for downloading to the IP Phone. If the IP phone's files are located in a sub-directory beneath the server's root directory, the relative path to that sub-directory should be entered in this field. Enter the path name in the form *folderX\folderX\folderX*. For example, ***ipphone\6863i\configfiles.***

FTP SETTINGS

- Select **FTP Server**.
- Enter the IP address or fully qualified domain name of the FTP server.
- Press **Done** or **Set** to save the change.
- Select **FTP Path**.
- Enter the path name for which the configuration files reside on the FTP server for downloading to the IP Phone. If the IP phone's files are located in a sub-directory beneath the server's root directory, the relative path to that sub-directory should be entered in this field. Enter the path name in the form *folderX\folderX\folderX*. For example, ***ipphone\6863i\configfiles.***
- **Optional**: You can enter a username and password for accessing the FTP server if required:
- Select **FTP Username**.
- Enter a username for accessing the FTP server.
- Press **Done**.
- Select **FTP Password**.
- Enter a password for accessing the FTP server.
- Press **Done** or **Set**.

HTTP SETTINGS

- Select **HTTP Server**
- Enter the IP address of the HTTP server.
- Press **Done** or **Set**.
- Select **HTTP Path**.
- Enter the path name for which the configuration files reside on the HTTP server for downloading to the IP Phone. If the IP phone's files are located in a sub-directory beneath the server's root directory, the relative path to that sub-directory should be entered in this field. Enter the path name in the form *folderX\folderX\folderX*. For example, ***ipphone\6863i\configfiles.***
- Select **HTTP Port**.
- Enter the HTTP port that the server uses to load the configuration to the phone over HTTP. Default is 80.
- Press **Done** or **Set**.

HTTPS SETTINGS

- Select **HTTP Client.**
- Select **Download Server**.
- Enter the IP address of the HTTPS server.
- Press **Done** or **Set**.
- Select **Download Path**.
- Enter the path name for which the configuration files reside on the HTTPS server for downloading to the IP Phone. If the IP phone's files are located in a sub-directory beneath the server's root directory, the relative path to that sub-directory should be entered in this field. Enter the path name in the form *folderX\folderX\folderX*. For example, ***ipphone\6863i\configfiles.***
- Press **Done** or **Set**.
- Select **Client Method**.
- Select the client method to use for downloading the configuration files (TLS Preferred, TLS 1.0, TLS 1.1, TLS 1.2). For more information about which client method to use, see the section, "HTTPS Client/Server Configuration" on page 4-36.
- Select **Download Port**.
- Enter the HTTPS port that the server uses to load the configuration to the phone over HTTPS. Default is 443.
- Select **HTTPS Server.**
- Select **HTTP->HTTPS**.
- Press **Change** to select "**Do not redirect**" or "**Redirect**". Default is "**Do not redirect**". Enabling this feature redirects the HTTP protocol to HTTPS.
- Press **Set**.
- Select **XML HTTP POSTs**.
- Press **Change** to select "**Do not block**" or "**Block**". Enabling this feature blocks XML HTTP POSTs from the IP Phone.

Note: For more information on configuring the HTTPS security method, HTTP to HTTPS redirect, and HTTPS server blocking for HTTP XML POSTs, see the section, "HTTPS Client/Server Configuration" on page 4-36.

10. Press **Done** or **Set** repeatedly until the session prompts you to restart the IP phone to apply the configuration settings.
11. Select **Restart.**

For the 6867i/6869i/6920/6930:

IP PHONE UI

1. Press or on the phone to enter the Options List.
2. Press the **Advanced** softkey.
3. Enter the Administrator password using the keypad. Default is "**22222**".
4. Select **Configuration Server**.
5. In the **Download Protocol** field, select the protocol you want the phone to use for downloading from the configuration server. Valid values are:
   - TFTP (Default)
   - FTP
   - HTTP
   - HTTPS

   The IP phone uses the protocol you select to download new firmware and configuration files from the configuration server.

For the 6873i/6940:

IP PHONE UI

1. Press or on the phone to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password and press the blue Enter key. Default is “**22222**”.
4. Tap the **Configuration Server** icon.

   Note: If required, swipe left on the screen to navigate to the second page of options.

5. In the **Download Protocol** field, select the protocol you want the phone to use for downloading from the configuration server. Valid values are:
   - TFTP (Default)
   - FTP
   - HTTP
   - HTTPS

   The IP phone uses the protocol you select to download new firmware and configuration files from the configuration server.
6. After selecting the download protocol, you must identify specific parameters for that specific protocol.

Use the following table to configure the applicable server.

TFTP SETTINGS

- In the **Primary Server** field, enter the IP address or fully qualified domain name of the primary TFTP server.
- In the **Pri TFTP Path** field, enter the path name for which the configuration files reside on the TFTP server for downloading to the IP Phone. If the IP phone's files are located in a sub-directory beneath the server's root directory, the relative path to that sub-directory should be entered in this field. Enter the path name in the form *folderX\folderX\folderX*. For example, ***ipphone\6867i\configfiles.***

- **Optional**: You can also configure an Alternate TFTP server and Alternate TFTP Path if required by selecting the **Use Alt TFTP** checkbox and entering the alternate path in the **Alt TFTP Path** field.

FTP SETTINGS

- In the **FTP Server** field, enter the IP address or fully qualified domain name of the FTP server.
- In the **FTP Path** field, enter the path name for which the configuration files reside on the FTP server for downloading to the IP Phone. If the IP phone's files are located in a sub-directory beneath the server's root directory, the relative path to that sub-directory should be entered in this field. Enter the path name in the form *folderX\folderX\folderX*. For example, ***ipphone\6867i\configfiles.***

- **Optional**: You can enter a username and password for accessing the FTP server if required by entering them in the **FTP Username** and **FTP Password** fields.

HTTP SETTINGS

- In the **HTTP Server** field, enter the IP address of the HTTP server.
- In the **HTTP Port** field, enter the HTTP port that the server uses to load the configuration to the phone over HTTP. Default is **80**.
- In the **HTTP Path** field, enter the path name for which the configuration files reside on the HTTP server for downloading to the IP Phone. If the IP phone's files are located in a sub-directory beneath the server's root directory, the relative path to that sub-directory should be entered in this field. Enter the path name in the form *folderX\folderX\folderX*. For example, ***ipphone\6867i\configfiles.***

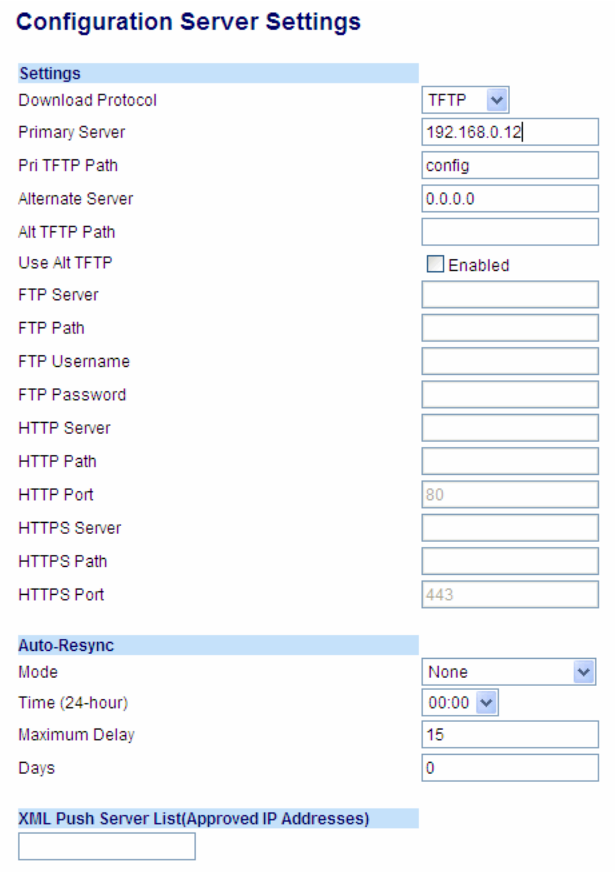
HTTPS SETTINGS

- In the **HTTPS Server** field, enter the IP address of the HTTPS server.
- In the **HTTPS Port** field, enter the HTTPS port that the server uses to load the configuration to the phone over HTTPS. Default is **443**.
- In the **HTTPS Path** field, enter the path name for which the configuration files reside on the HTTPS server for downloading to the IP Phone. If the IP phone's files are located in a sub-directory beneath the server's root directory, the relative path to that sub-directory should be entered in this field. Enter the path name in the form *folderX\folderX\folderX*. For example, ***ipphone\6867i\configfiles.***
- In the **HTTPS Client Method** field, select the client method to use for downloading the configuration files (TLS Preferred, TLS 1.0, TLS 1.1, TLS 1.2). For more information about which client method to use, see the section, "HTTPS Client/Server Configuration" on page 4-36.

7. Tap the **Save** softkey.
8. Restart the phone for the change to take affect.

MITEL WEB UI

1. Click on **Advanced Settings->Configuration Server.**



2. Select the protocol from the "**Download Protocol**" list box. Valid values are **TFTP**, **FTP**, **HTTP**, and **HTTPS**. Default is **TFTP**.

The IP phone uses the protocol you select to download new firmware and configuration files from the configuration server. Use the following table to configure the applicable server.

TFTP

- Enter an IP address or fully qualified domain name in the **"TFTP Server"** field.
- Enter the path name in the "**TFTP Path**" field for which the configuration files reside on the TFTP server for downloading to the IP Phone. If the IP phone's files are located in a sub-directory beneath the server's root directory, the relative path to that sub-directory should be entered in this field. Enter the path name in the form *folderX\folderX\folderX*. For example, ***ipphone\6867i\configfiles.***
- **Optional**: You can also configure an alternate TFTP server if required. If **"Use Alternate TFTP"** is enabled, you must also enter an IP address or qualified domain name for the alternate server in the **"Alternate TFTP"** field. You can also enter a path name for the alternate TFTP server in the "**Alternate TFTP Path**" field.

FTP

- Enter an IP address or fully qualified domain name in the **"FTP Server"** field.
- Enter the path name in the "**FTP Path**" field for which the configuration files reside on the FTP server for downloading to the IP Phone. If the IP phone's files are located in a sub-directory beneath the server's root directory, the relative path to that sub-directory should be entered in this field. Enter the path name in the form *folderX\folderX\folderX*. For example, ***ipphone\6867i\configfiles.***
- **Optional**: You can enter a username and password for accessing the FTP server if required.
- Enter a username for a user that will access the FTP server in the **"FTP User Name"** field.
- Enter a password for a user that allows access to the FTP server in the **"FTP Password"** field.

HTTP

- Enter an IP address or fully qualified domain name in the **"HTTP Server"** field.
- Enter the path name in the "**HTTP Path**" field for which the configuration files reside on the HTTP server for downloading to the IP Phone. If the IP phone's files are located in a sub-directory beneath the server's root directory, the relative path to that sub-directory should be entered in this field. Enter the path name in the form *folderX\folderX\folderX*. For example, ***ipphone\6867i\configfiles.***
- Enter the HTTP port number in the "**HTTP Port"** field that the server uses to load the configuration to the phone over HTTP.
- **Optional**: You can enter a list of users to be authenticated when they access the HTTP server in the **"XML Push Server List (Approved IP Addresses)"** field.

HTTPS

- Enter an IP address or fully qualified domain name in the **"HTTPS Server"** field.
- Enter the path name in the "**HTTPS Path**" field for which the configuration files reside on the HTTP server for downloading to the IP Phone. If the IP phone's files are located in a sub-directory beneath the server's root directory, the relative path to that sub-directory should be entered in this field. Enter the path name in the form *folderX\folderX\folderX*. For example, ***ipphone\6867i\configfiles.***
- Enter the HTTPS port number in the "**HTTPS Port"** field that the server uses to load the configuration to the phone over HTTPS.
- **Optional**: You can enter a list of users to be authenticated when they access the HTTP server in the **"XML Push Server List (Approved IP Addresses)"** field.

Note: For more information on configuring the HTTPS security method, HTTP to HTTPS redirect, and HTTPS server blocking for HTTP XML POSTs, see the section, "HTTPS Client/Server Configuration" on page 4-36.

3. Click **Save Settings** to save your settings.

> **Note:** The session prompts you to restart the IP phone to apply the configuration settings.

4. Select **Operation->Reset** and click **Restart**.

IPV6 SUPPORT ON 6800 AND 6900 SERIES SIP PHONES

Release 5.1 introduces IPV6 support for the Mitel 6800 and 6900 series SIP phones.

The intial IPV6 offering is limited (refer to supported features and known limitations) to a basic IPV6 capability and has been certified with MiVoice MX-ONE.

Mitel SIP phones can now be deployed in the following deployment configurations:

1. IPv4-only network
2. IPv6/IPv4 dual network

Note: By factory-default, the IPv6 mode is disabled in the SIP phone.

SUPPORTED FEATURES AND COMPONENTS

Mitel 6800 and 6900 series SIP phones when configured for IPv6 support the following features and components:

- DHCPv6 - DHCPv6 is the network protocol used to configure IPv6 hosts with IP addresses, IP prefixes and other configuration data that is required to operate an IPv6 network.
- DNSv6 - The system sends a DNS6 name query to the Domain Name System (DNS). If the DNS has an IPv6 address - name mapping for the query, the DNS returns the IPv6 address to the server.
- Network Time Protocol version 6 (NTPv6)
- LDAP
- Images and Avatars hosted on IPv6 configuration server
- XML API
- Syslog
- TCPdump
- VDP and 802.1x support
- SLAAC (StateLess Address Auto Configuration) by Router Advertisement

KNOWN LIMITATIONS AND RESTRICTIONS

The following are the known limitations and restrictions for IPv6 implementation on 6800 and 6900 series SIP phones:

- From Release 5.1.0 DHCPv6 based configuration is supported and static address is not supported.
- All services including XML, LDAP, RTCP-XR will function only in IPv6 after switching to IPv6 mode.

- This release does not support call recording and paging in IPv6 mode.
- M- and O-Flag in the Router's Advertisement are not supported and so any subsequent request to use DHCP is not supported.
- RTCP-XR statistics are sent only to IPv6 enabled collectors.
- SIP calls are supported either in IPv6 mode or IPv4 mode but not in dual mode.
- Media transcoding between IPv4 and IPv6 is carried out through call manager and no direct media exists between the phones in different IP domain.
- This release does not support User Agent Computer Supported Telecommunications Applications (uACSTA), TR-06, Extensible Messaging and Presence Protocol (XMPP), and XSI on IPv6.
- DNS server should be in IPv6.
- All settings or services should be in IPv6 (For example, Proxy Server, Registrar Server, VDP server, XML server, Image Server and so on).
- Does not support connecting multiple phones to a 802.1x enabled port on Cisco SG500 switch.

MIGRATING 6800 AND 6900 SERIES SIP PHONES FROM IPV4 TO IPV6 ADDRESSING

This section describes the pre-requisites and steps that you must follow to migrate the 6800 and 6900 series phones with factory-default settings into IPv6 mode.

PRE-REQUISITES

Ensure following requirements are met before you migrate the 6800 and 6900 series phones from IPv4 to IPv6 mode:

1. A 6800/6900 series phone with factory-default configuration in IPv4-mode on MX-ONE call controller with SIP Version 5.1.0 or later installed.
2. A DHCPv4 server with option 43 configured and available on the same network to provide the IPv4 configuration download server required to enable IPv6 on the phone.
3. An IPv6 configuration server.
4. Access to a Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP) server, or Hyper Text Transfer Protocol over Secure Sockets Layer (SSL) (HTTPS).
5. An Ethernet/Fast Ethernet LAN (10/100 Mbps).
6. A category 5/5e straight-through cabling.
7. Power source:
   a. For Ethernet networks that supply inline power to the phone (IEEE 802.3af) use an Ethernet cable to connect from the phone directly to the network for power (no 48V AC power adapter required if using Power-over-Ethernet [PoE]).
   b. For Ethernet networks that do not supply power to the phone, ensure that you use:

- only the GlobTek Inc. Limited Power Source [LPS] adapter model no. GT-41080-1848 (sold separately) to connect from the DC power port on the phone to a power source.
- a PoE power injector or a PoE switch.

TO MIGRATE 6800 SERIES SIP PHONES FROM IPV4 TO IPV6 MODE

Perform the following steps to migrate the 6800/6900 Series phones with factory default settings in IPv4 mode to IPv6 mode:

1. On the DHCP v6 server, perform the following tasks to point the DHCP v6 server to the IPv6 configuration server. You can do this by inserting a code snippet to the DHCP configuration file located at the DHCP server (for example, ISC-dhcpv6 server). You can use one of the following options to perform this configuration:

a. If you use option 17, insert the following code snippet into the DHCP configuration file:

```
    if substring(option dhcp6.vendor-class, 2, 2)=04:03 and
substring(option dhcp6.vendor-class, 6, 18)="AastraIPPhone6869i" {
    # Mitel Vendor option configuration
    option dhcp6.vendor-opts
    00:00:04:03: // enterprise number - mitel (0x0403/1027)
    00:11: // suboption (17) - don't change it
    00:21: // suboption lenght = 2*(number of counts of subcode) +
code1-len + code2-len + ... - need calculation if code data change
    # // 43 = 2*4 + 26 + 01 + 10 + 02
    # code:data-len:data in hex string:

02:1f:68:74:74:70:3a:2f:2f:5b:32:30:30:31:3a:64:62:38:3a:30:3a:32:3a
:3a:32:30:37:5d:2f:69:70:76:36;
    # // 02:cfg-server-url 26:data-len data:
http://2001:db8:0:2::207/ipv6 - convert ASCII string to hex string
    }
```

where http://2001:db8:0:2::207/ipv6 is the IPv6 address of the IPv6 configuration server.

b. If you use option 159, insert the following code snippet into the DHCP configuration file:

```
    option dhcp6.opt-159 code 159 = text;
    option dhcp6.opt-159 "http://2001:db8:0:2::207/ipv6";
```

where http://2001:db8:0:2::207/ipv6 is the IPv6 address of the IPv6 configuration server.

2. On the IPv4 configuration server, perform the following tasks:

a. Add the 5.1.0 or later firmware that supports IPv6 mode, to the IPv4 configuration server.

   b. b.Insert the following parameter in the configuration file of the phone:

   ipv6: 1

3. On the IPv6 configuration server, perform the following tasks:
   a. Add the IPv6 SIP account and the IPv6 SIP server for the phone in the ipv6 configuration file.
   b. Insert the following parameter in the configuration file of the phone:

   ipv6: 1

4. Reboot the 6800 Series phone.
   The phone obtains the configuration file and reboots in IPv6 mode.

CONFIGURATION FILES

For specific parameters you can set in the configuration files to support IPv6 on 6800/6900 Series SIP phones, see Appendix A, section "IPv6 Support on 6800/6900 Series SIP phones" on page A-42.

Chapter 5

CONFIGURING OPERATIONAL FEATURES

ABOUT THIS CHAPTER

The IP phones have specific operational features you can configure to customize your IP phone. This chapter describes each feature and provides procedures for configuring your phone to use these features.

TOPICS

This chapter covers the following topics:

OPERATIONAL FEATURES

DESCRIPTION

This section describes the operational features managed and configured by a System Administrator.

USER PASSWORDS

A user or an administrator can change the user passwords on the phone using the configuration files, the IP phone UI, or the Mitel Web UI.

Use the following procedures to change the user password.

Note: The IP phones support alphanumeric password with the supported characters.

CONFIGURING A USER PASSWORD

CONFIGURATION FILES

If unsupported characters are present in the user password or if the password length exceeds 15 characters in the configuration file then the phone uses the default password. The default password for user is blank.

The following full character sets are supported:

- 0-9
- A-Z
- a-z
- +.:;=_,-'&()$!*/@

Note: User password does not support space and pound in the configuration file.

For specific parameters you can set in the configuration files, see Appendix A, the section, "Password Settings" on page A-20.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **User Password**.
3. Enter the current user password.
4. Press **Enter**.

5. Enter the new user password.

> **Note:** The IP phones support alphanumeric password with the supported characters.

6. Press **Enter**.
7. Re-enter the new user password.
8. Press **Enter**.
   A message, “Password Changed” displays on the screen.

For the 6867i/6869i/6920/6930:

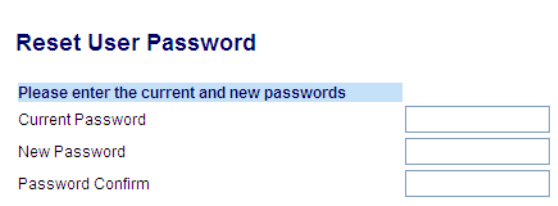
1. Press or to enter the Options List.
2. Select **Lock > Password**.
3. In the “**Current Password**” field enter the current user password.
4. In the “**New Password**” field enter the new user password.
5. In the “**Re-enter Password**” field re-enter the user password.
6. Press **Save**.

For the 6873i/6940/6970:

1. Press , , or the **Settings** softkey to enter the Options List.
2. Press the **Lock** icon.
3. Press the **Password** icon.
4. In the “**Current Password**” field enter the current user password.
5. In the “**New Password**” field enter the new user password.
6. In the “**Re-enter Password**” field re-enter the user password.
7. Press **Save**.

MITEL WEB UI

1. Click on **Operation->User Password**.



2. In the "**Current Password**" field, enter the current user password.

3. In the "**New Password**" field, enter the new user password.

Note: The IP phones support alphanumeric password with the supported characters.

4. In the "**Password Confirm**" field, enter the new user password again.
5. Click **Save Settings** to save your changes.

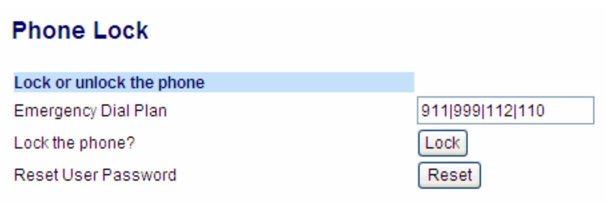
RESETTING A USER PASSWORD

If a user forgets his password, either the user or an administrator can reset it so a new password can be entered. The reset user password feature resets the password to the factory default which is blank (no password).

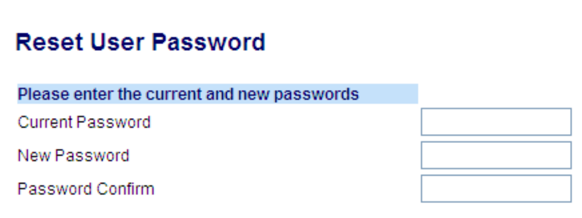
You can reset a user password using the Mitel Web UI only at the path *Operation->Phone Lock*. Use the following procedure to reset a user password.

MITEL WEB UI

1. Click on **Operation->Phone Lock**.



2. In the “**Reset User Password**” field, click **Reset**.
   The following screen displays:



3. In the “**Current Password**” field, leave this blank.
4. In the “**New Password**” field, enter a new password for the user.

Note: The IP phones support alphanumeric password with the supported characters.

5. In the “**Password Confirm**” field, re-enter the new user password.
6. Click **Save Settings** to save the new user password and perform the next procedure.

ADMINISTRATOR PASSWORDS

An administrator can change the administrator passwords on the phone using the configuration files only.

An administrator can also assign a password for using the Options key on the IP phone. You turn this feature on and off by entering the "**options password enabled**" parameter followed by a valid value in the configuration files. Valid values are **0** (false; Options key not password protected), or **1** (true; Options key password protected). If this parameter is set to 1, a user has to enter a password at the IP phone UI. If the password is entered correctly, the user is allowed to gain access to the Options Menu and no more password prompts display for other password protected screens. If the user fails to enter the correct password in three attempts, access to the Options Menu is denied and the IP phone returns to the idle screen.

CHANGING THE ADMINISTRATOR PASSWORD

CONFIGURATION FILES

If unsupported characters are present in the Administrator password or if the password length exceeds 15 characters in the configuration file then the phone uses the default password. The default password for admin is 22222.

The following full character sets are supported:

- 0-9
- A-Z
- a-z
- +.:;=_,-'&()$!*/@

Note: Admin password does not support space and pound in the configuration file.

For specific parameters you can set in the configuration files, see Appendix A, the section, “Password Settings” on page A-20.

LOCKING/UNLOCKING THE PHONE

A user or administrator can lock a phone to prevent it from being used or configured. Once the phone is locked, the user or administrator can enter their password to unlock the phone.

You can lock/unlock a phone using the configuration files, the IP Phone UI, or the Mitel Web UI.

You can use any of the following methods to lock/unlock a phone:

- Using the IP Phone UI at the path *Options->Lock*.
- Using the Mitel Web UI via the path *Operation->Phone Lock*.
- Using the configuration files to configure a softkey as “phonelock”, and then pressing the key to lock/unlock the phone.

- Using the Mitel Web UI to configure a softkey as “Phone Lock”, and then pressing the key to lock/unlock the phone.
- Using the configuration file parameter "phone lock" to lock and unlock the phone.

Note: All of the methods above configure locking/unlocking of the phone dynamically. Once configured, the feature takes affect immediately. To unlock the phone, a user or administrator must enter their password.

CONFIGURING PHONE LOCK/UNLOCK USING CONFIGURATION FILES

Using the **phone lock** parameter, you can enable and disable the phone lock functionality on the IP phones.

When the phone is in the locked state:

- The MWI LED is lit with the status message, 'Phone is locked' on the Idle screen.
- An emergency dial plan allows calls to be placed to numbers specified in an emergency dial plan. For details, see "Configuring an Emergency Dial Plan," on page 17.
- Calls cannot be placed to numbers not specified in the emergency dial plan.
  For example, if you press the line key and dial a number that is not specified in the emergency dial plan, the call does not go through and the phone returns to the Idle screen.
- Incoming calls can be answered using the normal call answering methods such as by lifting the handset or pressing the handsfree key, the line key, or the softkeys without enabling any call answering features.
  Call transfer, conference call, intercom call, and call forward features are disabled.
- On the WebUI, **Operation** > **Phone Lock** offers an input box for emergency dial plan and a **TOGGLE** button for phone locking/unlocking.
- The locked status is retained after the phone reboots.

Use the following procedure to lock and unlock the phone using the configuration files.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Enabling/Disabling phone lock," on page 292.

LOCKING/UNLOCKING THE PHONE USING THE IP PHONE UI

Use the following IP Phone UI procedure to lock/unlock an IP phone and prevent it from being used or configured.

For the 6863i/6865i6905/6910:

IP PHONE UI

Lock the phone:

1. Press or on the phone to enter the Options List.

2. Select **Phone Lock.**
   The prompt, "*Lock the phone*?" displays.
3. Press **Lock** to lock the phone.Unlock the phone:
1. Press on the phone to enter the Options List.
   The prompt, "*To unlock the phone...Password:*"
2. Enter the user or administrator password and press **Enter**. Default is "**22222**".
   The phone unlocks.

For the 6867i/6869i/6920/6930:

IP PHONE UI

Lock the phone:

1. Press or on the phone to enter the Options List.
2. Select **Lock > Phone Lock.**
   The prompt, "*Lock the phone*?" displays.
3. Select **Yes** to lock the phone.

Unlock the phone:

1. Press or on the phone to enter the Options List.
   An "Enter Unlock Password" prompt displays.
2. Enter the user or administrator password and press **Enter**. Default is "**22222**".
   A prompt "Unlock the Phone?" displays.
3. Select **Yes** to unlock the phone.

For the 6873i/6940/6970:

IP PHONE UI

Lock the phone:

1. Press , , or the **Settings** softkey on the phone to enter the Options List.
2. Press the **Lock** icon.
3. Press the **Phone Lock** icon.
   The prompt, "*Lock the phone*?" displays.
4. Press **Yes** to lock the phone.

Unlock the phone:

1. Press or on the phone to enter the Options List.
   An "Enter Unlock Password" prompt displays.
2. Enter the user or administrator password and press the blue **Enter** key. Default is "**22222**".
   A prompt "Unlock the Phone?" displays.
3. Select **Yes** to unlock the phone.

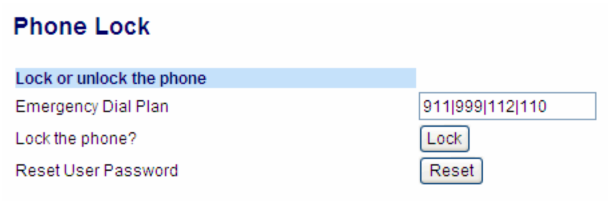
LOCKING/UNLOCKING THE PHONE USING THE MITEL WEB UI

Use the following Mitel Web UI procedure to lock/unlock an IP phone and prevent it from being used or configured.

MITEL WEB UI

Lock the phone:

1. Click on **Operation->Phone Lock**.



2. In the “**Lock the Phone?**” field, click **Lock**.
The phone locks dynamically and displays the following message:
“*Phone is locked*”.

Unlock the phone:

1. Click on **Operation->Phone Lock**.

2. In the “**Unlock the Phone?**” field, click **Unlock**.
The phone unlocks dynamically and displays the following message: “*Phone is unlocked*”.

CONFIGURING A LOCK/UNLOCK KEY USING THE CONFIGURATION FILES

Using the configuration files, you can configure a key on the phone (softkey, programmable key, or expansion module key) to use as a lock/unlock key. In the configuration files, you assign the function of the key as “**phonelock**”.

Use the following procedure to configure a key as a lock/unlock key using the configuration files.

CONFIGURATION FILES

To configure a softkey/programmable key as a lock/unlock key using the configuration files, see Appendix A, the section, "Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters" on page A-248.

Reference

To use the lock/unlock softkey or programmable key, see "Using the Configured Lock/Unlock Softkey on the IP Phone" on page 5-13.

CONFIGURING A LOCK/UNLOCK SOFTKEY USING THE MITEL WEB UI

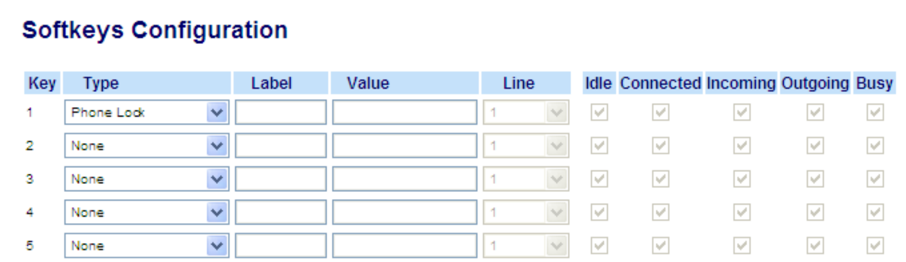
Using the Mitel Web UI, you can configure a softkey on the phone (softkey, programmable key, expansion module key) to use as a lock/unlock key. In the Mitel Web UI, you assign the function of the softkey as "**Phone Lock**".

Use the following procedure to configure a key as a lock/unlock key using the Mitel Web UI.

MITEL WEB UI

1. Click on **Operation->Softkeys and XML**
or
Click on Operation->Programmable Keys
or
Click on Operation->Expansion Module <N>.

Note: Depending on your phone-model, the key configuration screen displays.



2. Select a key you want to configure for locking/unlocking the phone.

3. In the "**Type**" field, select **Phone Lock** from the list of options.

4. Click **Save Settings** to save your changes.

Using the Configured Lock/Unlock Softkey on the IP Phone

After configuring a key as a lock/unlock key, refer to the following procedure to use the key on the IP phone.

For the 6863i/6865i/6905/6910:

IP PHONE UI

Lock the phone:

1. Press the **LOCK** softkey.
   The phone locks.
   The LED for the softkey AND the Message Waiting Lamp illuminate steady ON.
   An “**Unlock**” label appears next to the softkey you just pressed.

Unlock the phone:

2. Press the **UNLOCK** softkey.
   A password prompt displays.
3. Enter the user or administrator password and press ENTER.
   The phone unlocks.
   The LED for the softkey AND the Message Waiting Lamp go OFF.
   The “**Lock**” label appears next to the softkey you just pressed.

For the 6867i/6869i/6920/6930:

IP PHONE UI

Lock the phone:

1. Press the **Lock** softkey. The phone locks.
   The message “*Phone is Locked*” displays on the screen.

Unlock the phone:

1. Press the **Unlock** softkey.
   A password prompt displays.
2. Enter the user or administrator password and press the button or **Enter** softkey. Default is “**22222**”.
   A prompt “*Unlock the Phone?*” displays.
3. Press **Yes** to unlock the phone.
   The phone unlocks.

For the 6873i/6940/6970:

IP PHONE UI

Lock the phone:

1. Press the **Lock** softkey. The phone locks.
   The message “*Phone is Locked*” displays on the screen.

Unlock the phone:

1. Press the **Unlock** softkey.
   A password prompt displays.
2. Enter the user or administrator password and press the blue **Enter** key. Default is “**22222**”.
   A prompt “Unlock the Phone?” displays.
3. Select **Yes** to unlock the phone.

EMERGENCY DIAL PLAN

Public telephone networks in countries around the world have an emergency services number that allows a caller to contact local emergency services for assistance when required. The emergency services number may differ from country to country. It is typically a three-digit number so that it can be easily remembered and dialed quickly. Some countries have a different emergency number for each of the different emergency services.

You can include your country's emergency services numbers in the phone's emergency dial plan. The numbers defined in the emergency dial plan are those that the phone considers emergency services, and thus can be dialed out even when the phone is locked.

Note: The default local dial plan is configured to allow for all emergency numbers to be dialed out when the phone is unlocked. If you change the local dial plan, ensure it is configured to take into consideration any emergency services numbers for your country. Otherwise, calls to emergency services while the phone is unlocked may be blocked. See “Local Dial Plan” on page 5-80 for more information.

Additionally, if additional emergency call features are enabled, the enabled emergency call behaviors will be applied.

Note: See “Configurable Emergency Call Behavior” on page 5-17 for more information on additional emergency call features.

The following table describes the default emergency numbers on the IP phones.

EMERGENCY NUMBER	DESCRIPTION
911	A United States emergency number
999	A United Kingdom emergency number
112	An international emergency telephone number for **GSM mobile phone** networks. In all European Union countries it is also the emergency telephone number for both mobile and fixed-line telephones.
110	A police and/or fire emergency number in Asia, Europe, Middle East, and South America.

Note: Contact your local phone service provider for the emergency services numbers that are applicable to your region.

Available symbols that can be used in the emergency dial plan are as follows:

SYMBOL	DESCRIPTION
0, 1, 2, 3, 4, 5, 6, 7, 8, 9	Digit symbol
X	Match any digit symbol (wildcard)
*, #, .	Other keypad symbol
|	Expression inclusive OR
+	0 or more of the preceding digit symbol or [] expression The dial plan must not end with +. The dial plan must be suffixed with "#", if the sip dial plan terminator is disabled or it must be suffixed with "^", if the sip dial plan terminator is enabled.
[]	Symbol inclusive OR
-	Used only with [], represent a range of acceptable symbols; For example, [2-8]

Note: A secondary dial tone is not supported when defining an emergency dial plan.

EMERGENCY DIAL PLAN AND PATTERN MATCHING

The IP Phones support emergency dialing using pattern matching (i.e. once a user enters a set of numbers that matches a pattern defined in the emergency dial plan, the phone will automatically dial out the number without the user having to press the Dial softkey).

Note: Emergency dial plan pattern matching is only functional when the live dialpad feature is enabled. For more information on the live dialpad feature, see "Live Dialpad" on page 5-58.

With Live Dialpad enabled, if a Speeddial key is used to dial out, the number dials automatically but the whole defined number string is examined against the emergency dial plan.

If the whole string does not match a pattern defined in the emergency dial plan at all, the number will not be dialed out. If the whole string matches partially with a pattern defined in the emergency dial plan but has less numbers, the number will not be dialed out. If the whole string matches partially with a pattern defined in the emergency dial plan, but has more numbers, the full string is dialed out.

For example, if the emergency dial plan is defined as 9xx and speeddial key number is 5000, the call will not dial out. If a pre-dial or speeddial key number is 91, the call will not dial out. If a pre-dial or speeddial key number is 911, the call will be dialed out as 911. If a pre-dial or speeddial key number is 9112, the call will be dialed out as 9112.

Note: If the phone is unlocked, dialed numbers are matched against the local dial plan. For more information on configuring a local dial plan, see "Local Dial Plan" on page 5-80.

EMERGENCY DIAL PLAN AND PREFIX DIALING

The IP phones also support a prefix dialing feature for outgoing emergency calls. If the dialed number matches against the emergency dial plan, the phone automatically maps the pre-configured prepended digit in the configuration to the beginning of the dialed number.

You can enable this feature by adding prepend digits to the end of the emergency dial plan parameter string separated by a comma in the configuration files or the Mitel Web UI at Operation > Phone Lock. For example, if you specify the emergency dial plan with a prepend map of “911,9”, if the user dials the number "911", the SIP phone will automatically add the digit “9” before the "911".

Note: Patterns/numbers in the dial plan with prepend digits defined take priority over those that do not have prepend digits defined.

CONFIGURING AN EMERGENCY DIAL PLAN

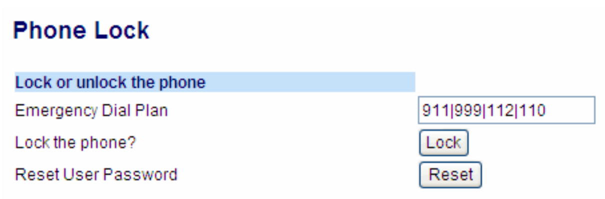
Use the following procedures to specify the numbers to use on your phone for dialing emergency services in your area.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Emergency Dial Plan Settings” on page A-30.

MITEL WEB UI

1. Click on **Operation->Phone Lock**.



2. In the “**Emergency Dial Plan**” field, enter the number used in your local area to contact emergency services. For multiple numbers, enter a “**|**” between each emergency number. For example:
   911|110.
   Default for this field is "911|999|112|110". You can enter up to 512 characters in this field.
3. Click **Save Settings** to save the emergency dial plan to your phone.

CONFIGURABLE EMERGENCY CALL BEHAVIOR

Administrators have the option of changing the default behavior of the IP phones when an emergency call (i.e. a call made to an emergency number matching one of the values defined in the "**emergency dial plan**" parameter) is placed. If the "**emergency call connection hold enabled**" configuration parameter is enabled, the IP phones employ the following behaviors:

- **Connection Hold**: If an emergency call is placed, the IP phones ensure the voice/audio path and other resources associated with the emergency call are continually active, even if the caller hangs up the phone (i.e. the handset is placed on-hook).
  - If the handset is placed on-hook, the phone automatically switches to speakerphone mode ensuring that the call is still active. Alternatively, if the handset is taken off-hook, the phone automatically switches to handset mode.
  - All softkey and hardkey events (e.g. hold, conference, transfer, end call, park, mute, etc...) are disabled as they may impede or be disruptive to the active call.
  - The phone does not allow for the origination or termination of any call while the phone is connected to the emergency services agent. All incoming calls and pages are ignored and a busy tone is presented to the remote caller.
- **Enhanced Called Party Hold**: As a complement to the Connection Hold feature, Enhanced Called Party Hold allows the voice/audio path to be established the moment the emergency call is placed.
  - When a caller places a call to an emergency services number, all Connection Hold features are activated, even if the SIP session has not been established completely.
  - Even if the caller abandons the call before the emergency services agent answers, the voice/audio path and Connection Hold features will still be active.
- **Forced Disconnect**: As the Connection Hold feature ensures that the caller cannot terminate the call, the only way the call can be terminated is if the emergency services agent forces the disconnection by ending the call himself/herself.

The “**emergency call connection hold enabled**" parameter is disabled by default.

CONFIGURING EMERGENCY CALL BEHAVIOR

Use the following procedures to configure the IP phone’s behavior when emergency calls are placed.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Emergency Call Behavior Settings” on page A-31.

USER DIAL PLAN SETTING

The IP Phones have a parameter for configuring a dial plan that distinguishes between calling a real PSTN number and a number that looks like a PSTN number but is actually on an IP network.

This parameter is “sip user parameter dial plan”. Using the configuration files, an Administrator can configure a dial plan corresponding to a IP network number (e.g. 6xx|8xxxx|9xxxxxxx) that the phone checks before sending the SIP packet.

If for example, the number that was dialed was 645, the phone checks the dial plan and matches the number to the dial plan (6xx in the example above), before sending out the SIP packet. The SIP packet header omits the user parameter user=ip (e.g. “To: <sip:645@10.30.102.24:10060>“) identifying the number as one from an IP network.

If the number that was dialed was 456-2345, the phone tries to match the number to the dial plan before sending out the SIP packet but as it is not part of the dial plan the phone identifies the number as a PSTN number. The SIP packet header in this case indicates user=phone (i.e. “To: <sip:4562345:10060;user=phone>“).

Notes:

1. Entering a dial plan value for this parameter enables this feature. Entering no value for this parameter in the configuration files, disables this feature.
2. You can configure the “**sip user parameter dial plan**” parameter on a global basis only. If it is mis-configured, then the parameter is ignored.

USER DIAL PLAN AND PREFIX DIALING

The IP phones also support a prefix dialing feature for outgoing user dial plan numbers. If the dialed number matches against the user dial plan, the phone automatically maps the pre-configured prepended digit in the configuration to the beginning of the dialed number.

You can enable this feature by adding prepend digits to the end of the user dial plan parameter string separated by a comma in the configuration files. For example, if you specify the user dial plan with a prepend map of “6xx,9”, if the user dials the number "645", the SIP phone will automatically add the digit “9” before the "645".

Note: Patterns/numbers in the dial plan with prepend digits defined take priority over those that do not have prepend digits defined.

Configuring the SIP User Parameter Dial Plan

Use the following procedure to configure the SIP user parameter dial plan.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, “User Dial Plan Setting” on page A-31.

TIME AND DATE

In addition to enabling/disabling the time server, you can also set the time and date format, set the time zone, and set daylight savings time on the IP phones. You configure these features using the configuration files, the IP Phone UI, or the Mitel Web UI. The following table identifies which method of configuration applies to each feature.

FEATURE	METHOD OF CONFIGURATION
Set Time Format	Configuration Files IP Phone UI Mitel Web UI
Set Date Format	Configuration Files IP Phone UI Mitel Web UI
Set Time Zone	IP Phone UI Configuration Files
Set Daylight Savings Time	IP Phone UI Configuration Files

DAYLIGHT SAVINGS TIME (DST) INFORMATION

The Mitel IP Phones incorporate the federally mandated DST observance change. This change became affective starting in 2007.

The US has made a change to its daylight savings time observance starting in 2007. The Energy Policy Act of 2005 mandates that DST will now begin at 2:00 A.M. on the second Sunday in March and revert to Standard time on the first Sunday in November.

Note: In previous years, the DST began on the first Sunday of April and ended on the first Sunday of October.

The changes to daylight savings time applies to the U.S. and Canada, but may impact other countries outside North America.

Note: DST can be set on the phones using the IP Phone UI and configuration files only. For more information, see "Time Zone & DST" on page 5-20.

TIME ZONE & DST

There are two ways you can set the time zone on the IP Phones.

Method 1

You can set a time zone using the **Time Zone** option in the IP Phone UI or you can use the "**time zone name"** parameter in the configuration files. Both methods allow you to enter a value from the Time Zone table. The list of time zone names is provided in the table in Appendix A, the section, "Time Zone Name/Time Zone Code Table" on page A-61. The following is an example:

```
time zone name: US-Eastern
```

Method 2

You can use the **Time Zone** option in the IP Phone UI or your can use the "**time zone name"** parameter in the configuration files, and specify a value of "**Custom**" for this parameter (must use initial caps). The "Custom" option allows you to customize the time zone for your area using additional configuration parameters. The following is an example using relative time for EST:

```
time zone name: Custom
```

The following table identifies the additional time zone and DST parameters you can enter in the configuration files.

CUSTOM CONFIGURATION FILE PARAMETER	DESCRIPTION	EXAMPLE
time zone minutes	The number of minutes the time zone is offset from UTC (Coordinated Universal Time). This can be positive (West of the Prime Meridian) or negative (East of the Prime Meridian). The default is Eastern Standard Time (EST) with a value of 300 (GMT minus 5 hours).	time zone minutes: 300 **Note:** For additional values for this parameter, see "Custom Time Zone and DST Settings" on page A-67.
dst minutes	The number of minutes to add during Daylight Saving Time. Valid values are a positive integer between 0 to 60.	dst minutes: 60
dst start relative date dst end relative date	Specifies how to interpret the start and end day, month, and week parameters - absolute (0) or relative (1).	dst start relative date: 1 dst end relative date: 1
ABSOLUTE TIME (NOT APPLICABLE TO EASTERN STANDARD TIME (EST))		
dst start month	The month that DST starts. Valid values are 1 to 12 (January to December).	dst start month: 3
dst end month	The month that DST ends. Valid values are 1 to 12 (January to December).	dst end month: 4
dst [start |end] week	Not applicable to absolute time.	N/A
dst start day	The day of the month that DST starts. Valid values are 1 to 31.	dst start day: 15
dst end day	The day of the month that DST ends. Valid values are 1 to 31.	dst end day: 31
dst start hour	The hour that DST starts. Valid values are an integer from 0 (midnight) to 23.	dst start hour: 5
dst end hour	The hour that DST ends. Valid values are an integer from 0 (midnight) to 23.	dst end hour: 23
RELATIVE TIME		
dst start month	The month that DST starts. Valid values are 1 to 12 (January to December).	dst start month: 4
dst end month	The month that DST ends. Valid values are 1 to 12 (January to December).	dst end month: 5

CUSTOM CONFIGURATION FILE PARAMETER	DESCRIPTION	EXAMPLE
dst start week	The week in the specified month in which DST starts. Valid value is a positive or negative integer from 1 to 5. 1 = first full week of month -1 = last occurrence "dst start day" in the month 2 = second full week of month -2 =second last occurrence "dst start day" in the month . . . 5 = fifth full week of month -5 = fifth last occurrence "dst start day" in the month	dst start week: 2
dst end week	The week in the specified month in which DST ends. Valid value is a positive or negative integer from 1 to 5. 1 = first full week of month -1 = last occurrence "dst end day" in the month 2 = second full week of month -2 =second last occurrence "dst end day" in the month . . . 5 = fifth full week of month -5 = fifth last occurrence "dst end day" in the month	dst end week: -1
dst start day	The day of the specified week in the specified month that DST starts on. Valid values are an integer from 1 to 7. 1 = Sunday 2 = Monday . . . 7 = Saturday	dst start day: 2

CUSTOM CONFIGURATION FILE PARAMETER	DESCRIPTION	EXAMPLE
dst end day	The day of the specified week in the specified month that DST ends on. Valid values are an integer from 1 to 7. 1 = Sunday 2 = Monday . . . 7 = Saturday	dst end day: 7
dst start hour	The hour that DST starts. Valid values are an integer from 0 (midnight) to 23.	dst start hour: 10
dst end hour	The hour that DST ends. Valid values are an integer from 0 (midnight) to 23.	dst end hour: 23

Example 1

The following is an example of a custom time zone configuration in the configuration files using relative time (for EST):

```
time zone name: Custom
dst start relative date: 1 #relative
dst end relative date: 1 #relative

time zone minutes: 300
dst minutes: 60
```

Example 2

The following is an example of a custom time zone configuration in the configuration files using absolute time:

```
time zone name: Custom
dst start relative date: 0 #absolute
dst end relative date: 0 #absolute


#start of DST
dst start month: 3 #March
dst start week: 2 #second full week
dst start day: 1 #Sunday

#End of DST
dst end month: 11 #November
dst end week: 1 #first full week
dst end day: 1 #Sunday
```

DHCP TIME OFFSET (OPTION 2) SUPPORT

DHCP Option 42 enables the phone to be configured with the Network Time Protocol (NTP) server addresses. However, NTP provides the Coordinated Universal Time (UTC) time so the phone requires the offset from UTC in order to deliver the correct local time.

A User or Administrator can set the offset of UTC using DHCP Option 2.

An Administrator can enable Option 2 in the configuration files by setting the parameter "**time zone name**". If this parameter contains the **DP-Dhcp** value, the phone derives the time and date from UTC and the time offset offered by the DHCP server.

Using the IP Phone UI, a User or Administrator can enable the phone to use DHCP Option 2 by setting the following values from the Country Code list on the phone:

COUNTRY NAME	COUNTRY CODE
Dhcp	DP

Note: The country name, country code, and time zone name are case sensitive.

On the IP Phone UI for 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP phones, a User or Administrator can select ***Time and Date->Time Zone->Others*** and choose "**DP-Dhcp**" from the displayed time zone list.

On the IP Phone UI for 6863i, 6865i, 6905, and 6910 IP phones, you select ***Preferences->Time and Date->Time Zone->Others*** and enter "**DP**" for the country code, or press "*****" and select "**Dhcp**" from the displayed time zone list.

If you enable DHCP Option 2 via the IP Phone UI, the change takes place dynamically.

Notes:

1. When DHCP Option 2 is enabled on the phone, the phone still uses the values configured for ***Daylight Savings*** to control daylight savings time.
2. The default behavior for the phone is to use the NTP server from Option 42 (or current configuration setting) and the current time zone settings.
3. If the time zone name parameter is set to a value other than Dhcp, then DHCP Option 2 is disabled.

References

For more information about setting DP-DHCP for the timezone, see Appendix A, "Time Zone Name" on page A-60.

For more information about setting the country code, see Appendix A, "Country Codes (from Standard ISO 3166)" on page A-221.

CUSTOM TIME ZONE SUPPORT

A User or Administrator can also set a custom time zone on the phone to be configured with the Network Time Protocol (NTP) server addresses. However, NTP provides the Coordinated Universal Time (UTC) time so the phone requires the offset from UTC in order to deliver the correct local time.

On the IP Phone UI for 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP phones, a User or Administrator can select ***Time and Date->Time Zone->Others*** and choose "**Custom**" from the displayed time zone list.

On the IP Phone UI for 6863i, 6865i, 6905, and 6910 IP phones, you select ***Preferences->Time and Date->Time Zone->Others*** and enter "**Custom**" for the country code.

References

For more information about setting a custom timezone, see Appendix A, "Time Zone Name" on page A-60.

CONFIGURING TIME AND DATE USING THE CONFIGURATION FILES

Use the following information to set a time and date format, time zone, and daylight savings time using the configuration files.

CONFIGURATION FILES

For specific date and time parameters you can set in the configuration files, see Appendix A, the section, "Time and Date Settings" on page A-58.

For specific parameters you can set for custom time zone settings, see Appendix A, the section, "Custom Time Zone and DST Settings" on page A-67.

CONFIGURING TIME AND DATE USING THE IP PHONE UI

Use the following procedure to set a time and date, time and date format, time zone, and daylight savings time using the IP Phone UI.

For the 6863i/6865i/6905/6910:

IP PHONE UI

1. Press ⚙ or ⚙ on the phone to enter the Options List.

Set Time Format:

2. Select **Time and Date.**

3. Select **Time Format.**
   Valid values are **12 Hour** and **24 Hour**.

   Note: The default Time Format is **12 Hour**.

4. Use the navigation keys to select the preferred time format.
5. Press **Done** to save the Time Format you selected.

Set Date Format:

6. Select **Date Format.**
7. Select a date format from the list of options.
   Valid values are:
   - WWW MMM DD (default)
   - DD-MMM-YY
   - YYYY-MM-DD
   - DD/MM/YYYY
   - DD/MM/YY
   - DD-MM-YY
   - MM/DD/YY
   - MMM DD
   - DD MMM YYYY
   - WWW DD MMM
   - DD MMM
   - DD.MM.YYYY

   Note: The default Date Format is **WWW MMM DD** (Day of Week, Month, Day).

8. Press **Done** to save the Date Format.

Set Time Zone:

9. Select **Time Zone**.
10. Press * to display a list of time zones.

    Note: For more information about setting the time zone to "DP-Dhcp" or "Custom", see "DHCP Time Offset (Option 2) Support" on page 5-24, "Custom Time Zone Support" on page 5-25, or Appendix A, "Time Zone Name" on page A-60.

11. Select a Time Zone from the list of values.
    For valid values, see Appendix A, the section, "Time and Date Settings" on page A-58.

    Note: The default Time Zone is **US-Eastern**.

12. Press **Done** to save the Time Zone you selected.

Set Daylight Savings Time:

13. Select **Daylight Savings**.

14. Select a Daylight Savings time from the list of options.
Valid values are:
    - OFF
    - 30 min summertime
    - 1 hr summertime
    - automatic

Note: The default for Daylight Savings is **Automatic**.

15. Press **Done** to save the Daylight Savings value you selected.

For the 6867i/6869i/6920/6930:

IP PHONE UI

1. Press ⚙ or ⚙ to enter the Options List.

Set Time Format:

2. Navigate to the **Time and Date -> Settings** option and press the ☑ button or **Select** softkey.
3. With Time Format highlighted press the ▶ key to move to selection column.
4. Use the ▲ and ▼ keys to scroll through and choose the desired time format. Valid values are 12 Hour and 24 Hour (the default is 12 Hour).

Set Daylight Savings:

5. Press the ◀ key to move to back to the options column and press the ▶ key to highlight **Daylight Savings**.
6. With **Daylight Savings** highlighted press the ▶ key to move to selection column.
7. Use the ▲ and ▼ keys to scroll through and choose the desired daylight savings setting. Valid values are:
    - Off
    - 30 min summertime
    - 1h summertime
    - Automatic (default)

Set Date Format:

8. Press the ◀ key to move to back to the options column and press the ▶ key to highlight **Date Format**.
9. With **Date Format** highlighted press the ▶ key to move to selection column.

10. Use the ▲ and ▼ keys to scroll through and choose the desired date format. Valid values are:
    - WWW MMM DD (default)
    - DD-MMM-YY
    - YYYY-MM-DD
    - DD/MM/YYYY
    - DD/MM/YY
    - DD-MM-YY
    - MM/DD/YY
    - MMM DD
    - DD MMM YYYY
    - WWW DD MMM
    - DD MMM
    - DD.MM.YYYY
11. Press the **Save** softkey to save your changes.

Set Time Zone:

12. Navigate to the **Time and Date -> Time Zone** option and press the ☑ button or **Select** softkey.
    A list of time zones displays for different areas of the world.
13. Use the ▲ and ▼ keys to scroll through and highlight the desired region. Valid values are:
    - America
    - Asia
    - Atlantic
    - Australia
    - Europe
    - Pacific
    - Others
14. With the desired region highlighted press the ▶ key to move to selection column.
15. Use the ▲ and ▼ keys to scroll through and choose the time zone that applies to your area. The default time zone is **US-Eastern**.
16. Press the **Save** softkey to save your changes.

For the 6873i/6940/6970:

IP PHONE UI

1. Press ⚙, ⚙, or the **Settings** softkey to enter the Options List.

Set Time Format:

2. Press the **Time and Date** icon.
3. Press the **Settings** icon.
4. Choose the desired time format. Valid values are 12 Hour and 24 Hour (the default is 12 Hour).

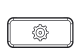
Set Daylight Savings:

5. Press **Daylight Savings**.
6. Choose the desired daylight savings setting. Valid values are:
   - Off
   - 30 min summertime
   - 1h summertime
   - Automatic (default)

Set Date Format:

7. Press **Date Format**.
8. Choose the desired date format. Valid values are:
   - WWW MMM DD (default)
   - DD-MMM-YY
   - YYYY-MM-DD
   - DD/MM/YYYY
   - DD/MM/YY
   - DD-MM-YY
   - MM/DD/YY
   - MMM DD
   - DD MMM YYYY
   - WWW DD MMM
   - DD MMM
   - DD.MM.YYYY
9. Press the **Save** softkey to save your changes.

Set Time Zone:

10. Press ,  , or the **Settings** softkey to enter the Options List.
11. Press the **Time and Date** icon.
12. Press the **Time Zone** icon.
    A list of time zones displays for different areas of the world.
13. Select the desired region. Valid values are:
    - America
    - Asia

- Atlantic
- Australia
- Europe
- Pacific
- Others

14. Choose the time zone that applies to your area. The default time zone is **US-Eastern**.

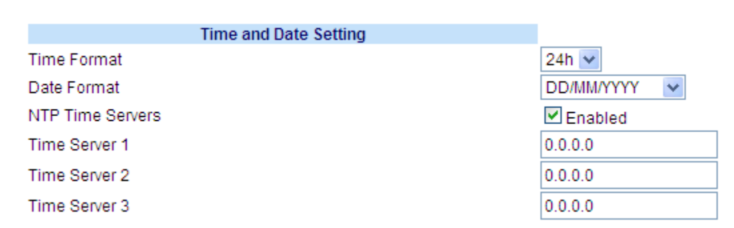
15. Press the **Save** softkey to save your changes.

CONFIGURING TIME AND DATE USING THE MITEL WEB UI

Use the following procedure to set a time and date, time and date format, time zone, and daylight savings time using the Mitel Web UI.

MITEL WEB UI

1. Click on **Basic Settings->Preferences->Time and Date Setting**.



2. In the **"Time Format"** field, select the time format you want to use on your phone. Valid values are:

- **12h** (12 hour format) (default)
- **24h** (24 hour format).

Note: The time displays on the phone's idle screen in the format you select for this field.

3. In the **"Date Format"** field, select the date format you want to use on your phone. Valid values are:

- WWW MMM DD (default)
- DD-MMM-YY
- YYYY-MM-DD
- DD/MM/YYYY
- DD/MM/YY
- DD-MM-YY
- MM/DD/YY
- MMM DD
- DD MMM YYYY

- WWW DD MMM
- DD MMM
- DD.MM.YYYY

Note: The date displays on the phone's idle screen in the format you select for this field.

4. Click **Save Settings** to save your changes.

TIME SERVERS

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

On the IP phones, you can enable or disable a Time Server to be used to synchronize time on the phones with the Timer Server you specify. An Administrator can use the IP Phone UI, Mitel Web UI, or configuration files to enable/disable the Time Server and specify a Time Server 1, Timer Server 2, and/or Time Server 3. A User can enable/disable the Time Server using the IP Phone UI or Mitel Web UI only. The Time Server is enabled by default.

Notes:

1. Time syncs are performed every 4 hours.
2. Depending on the status of the Time Server, the phone may not immediately display the correct time and date after it has been rebooted. The time and date may take several minutes to resynchronize.

Setting Time Server Using the Configuration Files

Use the following procedure to enable/disable the Time Server and optionally set the IP Address of Time Servers 1, 2, and/or 3.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Time Server Settings" on page A-66.

Setting Time Server Using the IP Phone UI

Use the following procedure to set the Time Server and optionally set the IP Address of Time Servers 1, 2, and/or 3.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.

2. Select **Preferences->Time and Date.**
3. Select **Timer Server 1**, **Time Server 2**, and/or **Time Server 3**.
4. Enter the IP address of the Time Server, in dotted decimal format. Use the available softkeys to help you enter the information.
5. Click **Done** to save your changes.

For the 6867i/6869i/6920/6930:

1. Press or to enter the Options List.
2. Select **Time and Date -> Set Date and Time.**
3. Ensure there is a checkmark in the box corresponding to the **Use Network Time** setting. If there is no checkmark, press the button to enable the **Use Network Time** setting.
4. Press the key to highlight **Time Server 1**, **Time Server 2**, or **Time Server 3**.
5. Using the keys on the dialpad, enter an IP address or domain name for the time server.
6. Press the **Save** softkey to save your changes.

For the 6873i/6940/6970:

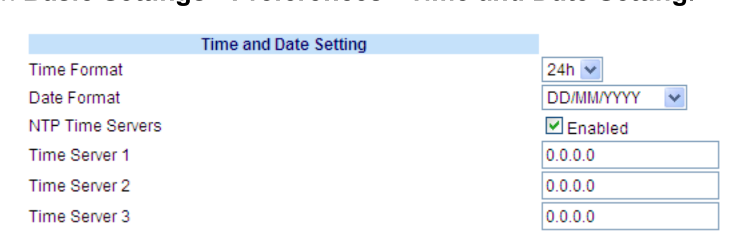
1. Press , , or the **Settings** softkey to enter the Options List.
2. Press the **Time and Date** icon.
3. Press the **Set Date and Time** icon.
4. Ensure there is a checkmark in the box corresponding to the **Use Network Time** setting. If there is no checkmark, press the checkbox to enable the **Use Network Time** setting.
5. Enter an IP address or domain name for the time server in the **Time Server 1**, **Time Server 2**, or **Time Server 3** fields.
6. Press the **Save** softkey to save your changes.

Setting Time Server Using the Mitel Web UI

Use the following procedure to set the Time Server and optionally set the IP Address of Time Servers 1, 2, and/or 3.

MITEL WEB UI

1. Click on **Basic Settings->Preferences->Time and Date Setting**.



To enable/disable Time Server:

2. The “**NTP Time Server**” field is enabled by default. If you need to disable the Time Server, uncheck the box. The Time Server 1, 2, and 3 fields are grayed out when disabled.

To set Time Server 1, 2, and/or 3:

Note: The “**Time Server**” field must be enabled to enter values in the “**Time Server 1, 2, and 3**” fields.

3. In the “**Time Server 1**”, “**Time Server 2**”, and/or “**Time Server 3**” field(s), enter the IP address of the Time Server 1, 2, and/or 3 in your network, in dotted decimal format. For example, 132.234.5.4
4. Click **Save Settings** to save your changes.

BACKLIGHT MODE

Note: Backlight mode is applicable on all phone types. **Off** is only applicable on 6865i and 6910.

6865i and 6910 have a backlight that can be turned on and off using configuration parameters:

- **Off** - Backlight is always OFF.

Note: Off is only applicable for 6865i and 6910i Phones. For rest of the phones, it will be treated as **Auto**.

- **Auto** (Default)- Automatically turns ON the backlight when the phone is in use, and then automatically turns brightness level to configured value of "inactivity brightness level" when the phone is idle after a specified duration of seconds in **bl on time**.

“The Auto” setting sets the phone to turn off the backlighting after a period of inactivity. The period of time that the phone waits before turning the backlight off is also configurable.

You can set this backlight feature using the configuration files and the IP Phone UI.

CONFIGURING THE BACKLIGHT MODE USING THE CONFIGURATION FILES

Use the following information to set the backlight mode and backlight timer on the IP Phones.

Note: The Backlight mode can be configured using the configuration files and the IP Phone User Interface (UI) for the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 phones.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Backlight Mode Settings” on page A-75.

Note: Using the configuration files, you can set the backlight to Off (always off) or Auto (On and then off after a period of inactivity).

CONFIGURING THE BACKLIGHT MODE USING THE IP PHONE UI

Use the following procedure to set the backlight mode and backlight timer on the IP Phone using the IP Phone UI.

IP PHONE UI

1. Press on the phone to enter the Options List.
2. Select Preferences.
3. Select **Display**.
4. Select **Backlight**.
5. Use the ▲ and ▼ arrow keys to select the Backlight status for your phone. Default is "**Auto**". Valid options are:
   - Off
   - Auto (Default)

   Note: Setting the Backlight to "**Auto**" displays an **ADVANCED** button for you to set the Auto timer.

6. If you select "**Off**", press **Done** to save your setting.
7. If you select "**Auto**", press the **Advanced** softkey to set the automatic timer.
8. Using the keypad, enter the amount of seconds you want the phone to stay backlit when the phone is idle. Valid values are **1** to **36000** seconds. Default is **600 seconds** (equals 10 minutes). When this period of time is reached, the phone turns OFF the backlight. Use the "**Backspace**" and/or "**Clear**" softkeys to delete entries if required.
9. Press **Done** to save your setting. The setting applies immediately to the phone.

Note: The Backlight mode can be configured for the IP phones using the IP Phone User Interface (UI) and through configuration file.

DISPLAY

Note: Applicable to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones only.

The **Display** option on the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP phones allows you to set the following on your phone:

- Brightness Level

- Brightness Timer

BRIGHTNESS LEVEL

The "**Brightness Level**" option allows you to set the amount of light that illuminates the LCD display. Use this option to set your preference of brightness.

SETTING BRIGHTNESS

For the 6867i/6869i/6920/6930:

IP PHONE UI

1. Press or to enter the Options List.
2. Navigate to the **Display** option and press the button or Select softkey.
3. Press the key to navigate to the **Brightness Level** setting.
4. Use the and navigation buttons to increase or decrease the intensity of brightness on the LCD.
5. Press the **Save** softkey to save your changes.

For the 6873i/6940/6970:

IP PHONE UI

1. Press , , or the **Settings** softkey to enter the Options List.
2. Press the **Display** icon.
3. Press the **Brightness Level** field.
4. Use the and arrow buttons to increase or decrease the intensity of brightness on the LCD.
5. Press the **Save** softkey to save your changes.

BRIGHTNESS TIMER

The "**Brightness Timer**" option allows you to set the amount of time you want the LCD display to stay illuminated before turning the backlight off during a period of inactivity. For example, if you set the brightness timer to 60, when the phone reaches 60 seconds of inactivity, the LCD backlight goes off.

SETTING BRIGHTNESS TIMER

For the 6867i/6869i/6920/6930:

IP PHONE UI

1. Press or to enter the Options List.

2. Navigate to the **Display** option and press the button or Select softkey.
3. Press the ▲ key to navigate to the **Brightness Timer** setting.
4. Enter a value, in seconds, using the dialpad keys. You can set the timer from 1 to 36000 seconds. Default is 600 (10 minutes).
5. Press the **Save** softkey to save your changes.

For the 6873i/6940/6970:

IP PHONE UI

1. Press , , or the **Settings** softkey to enter the Options List.
2. Press the **Display** icon.
3. Press the **Brightness Timer** field.
4. Enter a value, in seconds, using the dialpad keys. You can set the timer from 1 to 36000 seconds. Default is 600 (10 minutes).
5. Press the **Save** softkey to save your changes.

CONFIGURING THE BRIGHTNESS LEVEL SETTINGS USING THE CONFIGURATION FILES

Use the following information to configure the brightness level settings on the 6867i, 6869i, and 6873i.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the sections, "Backlight Mode Settings" on page A-75 and "Brightness Level Settings" on page A-76.

BACKGROUND IMAGE ON IDLE SCREEN

Note: Applicable to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones only.

Administrators can brand the idle screen of the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP phones with their own company logo or image. The background image is displayed on the bottom layer of the idle screen. This image can be set by the "**background image**" parameter. Current text (i.e. screen name, extension, and date/time) and softkeys on the idle screen are displayed on top of the background image. The background image can be downloaded from your configuration server using either FTP, HTTP, and HTTPs protocols.

Note: The TFTP protocol is supported but not recommended to be used if the image file is large and in the PNG file format. If the TFTP protocol must be used, it is recommended the image be in the JPG file format.

IDLE SCREEN IMAGE REQUIREMENTS:

- 320x240 pixels (6867i / 6920)
- 480x272 pixels (6869i / 6930)
- 800x480 pixels (6873i / 6940 / 6970)
- 24 or 32-bit color depth
- 1MB maximum file size
- Both JPG and PNG files are supported (JPG strongly recommended due to smaller file size and faster loading time)
- There should be no frame around the image

CONFIGURING A BACKGROUND IMAGE ON THE IDLE SCREEN

Use the following procedures to configure a background image on the idle screen

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Background Image on Idle Screen" on page A-77.

CONFIGURABLE HOME/IDLE SCREEN MODES

Note: Applicable to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones only.

The 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP phones contain two Home/Idle screen layout options. The default primary screen mode provides users with a larger date and time and displays the Screen Name ("**sip screen name**") parameter beside the line number in the top status bar.

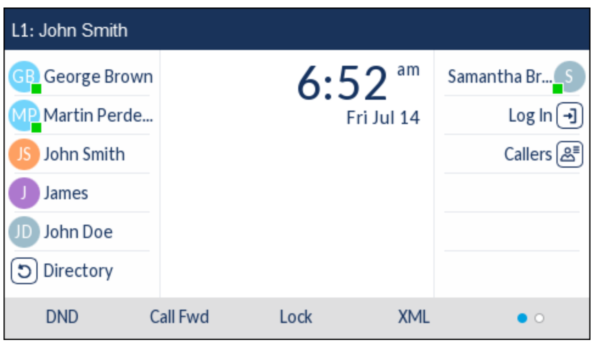
Note: Screen Name 2 ("**sip screen name 2**") is not displayed on the 6867i/6869i/6873i/6920/6930/6940 IP phone's screen when the primary screen mode is configured for use.

The secondary screen mode displays both the Screen Name and Screen Name 2 parameters. They are displayed above the smaller, repositioned date and time.

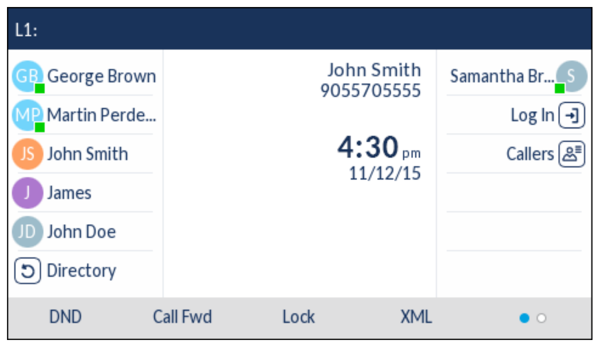
6867i/6920 Primary Home/Idle Screen Mode

6867i/6920 Secondary Home/Idle Screen Mode

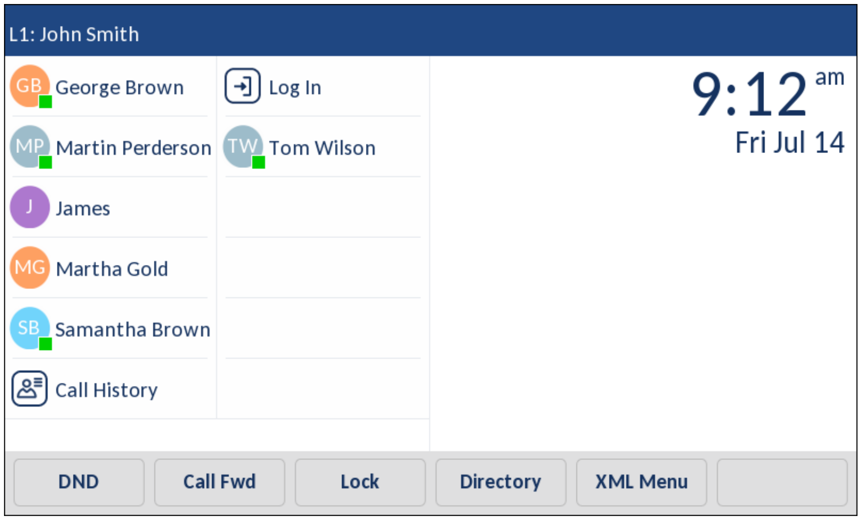
6869i/6930 Primary Home/Idle Screen Mode



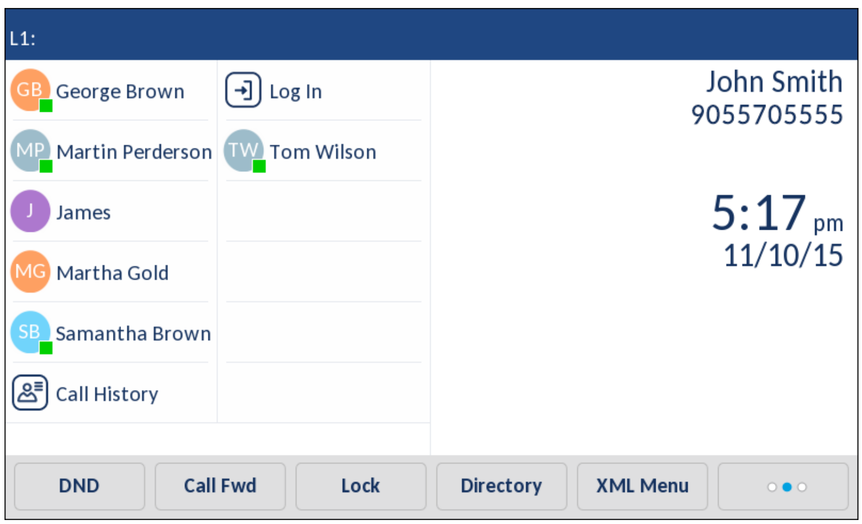
6869i/6930 Secondary Home/Idle Screen Mode



6873i/6940 Primary Home/Idle Screen Mode



6873i/6940 Secondary Home/Idle Screen Mode



Administrators can switch the home/idle screen to the preferred layout by defining the "**idle screen mode**" parameter in the configuration files or by navigating to the Display options menu on the phone.

Note: On 6867i, 6869i, and 6873i IP Phones, if you are upgrading your phone from Release 5.1.0 or earlier to a firmware version of Release 6.0.0 or later, idlescreen UI font size is smaller.

SWITCHING THE 6867I/6869I/6873I/6920/6930/6940/6970 IP PHONE'S HOME/IDLE SCREEN MODE USING THE CONFIGURATION FILES

Use the following parameter to switch the 6867i/6869i/6873i/6920/6930/6940/6970 IP phones home/idle screen mode.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Home/Idle Screen Settings" on page A-77.

SWITCHING THE 6867I/6869I/6873I/6920/6930/6940/6970 IP PHONE'S HOME/IDLE SCREEN MODE USING THE IP PHONE UI

Use the following procedure to switch the 6867i/6869i/6873i/6920/6930/6940/6970 IP phones home/idle screen mode using the IP Phone UI.

For the 6867i/6869i/6920/6930:

IP PHONE UI

1. Press ⚙ or ⚙ to enter the Options List.
2. Navigate to the **Display** option and press the ✓ button or Select softkey.
3. With **Home Screen Mode** highlighted press the 3 or ► key to change to the desired mode.
4. Press the **Save** softkey to save your changes.

For the 6873i/6940/6970:

IP PHONE UI

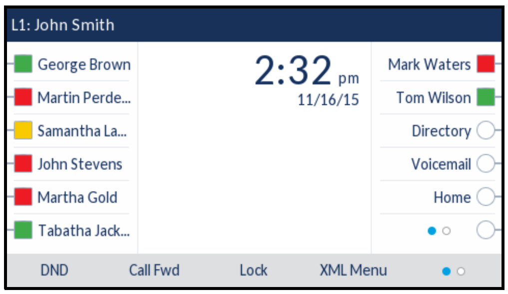
1. Press ⚙, ⚙, or the **Settings** softkey to enter the Options List.
2. Press the **Display** icon.
3. Press the **Home Screen Mode** field.
4. Press the left or right arrow keys to change to the desired mode.
5. Press the **Save** softkey to save your changes.

CONFIGURABLE HOME/IDLE SCREEN FONT COLOR

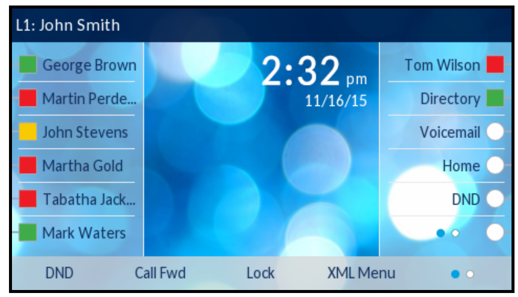
Note: Applicable to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones only.

Administrators have the option of changing the font color of the date, time, and status message text on the home/idle screen of the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 from Mitel blue to white or black using the "**idle screen font color**" configuration parameter.

6869i Example: Default Font Color



6869i Example: White Font Color



White is recommended when using a dark-colored background image while black or Mitel blue provides the contrast required when using a light-colored background image.

CONFIGURING THE HOME/IDLE SCREEN FONT COLOR USING THE CONFIGURATION FILES

Use the following parameter to configure the home/idle screen font color.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Home/Idle Screen Settings" on page A-77.

SCREEN SAVER

Note: Applicable to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones only.

A screen saver displaying the date and time and the number of missed calls (if applicable) is displayed for the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP phones after a specified amount of inactivity.

The amount of time the phone must be idle before the screen saver initiates is configurable through the phone's UI or by defining the "**screen save time**" parameter in the configuration files.

Note: If there are no missed calls, only the date and time are displayed.

CONFIGURING THE SCREEN SAVER TIMER USING THE CONFIGURATION FILES

Use the following parameter to configure the screen saver timer.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Screen Saver Settings" on page A-78.

CONFIGURING THE SCREEN SAVER TIMER USING THE PHONE UI

Use the following procedure to configure the screen saver timer using the IP Phone UI.

For the 6867i/6869i/6920/6930:

IP PHONE UI

1. Press or to enter the Options List.
2. Navigate to the **Display** option and press the button or Select softkey.
3. Press the navigation button to highlight the **Screen Saver Timer** setting.
4. Using the keypad, enter in the desired amount of time (in seconds) the phone must be idle before the screen saver is initiated. The range is 1 to 14400 seconds (with a default of 1800 seconds).

Note: From Release 6.1.0, IP phones will not support the complete disabling of the screen saver.

5. Press the **Save** softkey to save your changes.

For the 6873i/6940/6970:

IP PHONE UI

1. Press , , or the **Settings** softkey to enter the Options List.
2. Press the **Display** icon.
3. Press the **Screen Saver Timer** field.
4. Enter in the desired amount of time (in seconds) the phone must be idle before the screen saver is initiated. The range is 1 (Screensaver disabled) to 14400 seconds (with a default of 1800 seconds).

Note: From Release 6.1.0, IP phones will not support the complete disabling of the screen saver.

5. Press the **Save** softkey to save your changes.

SCREEN SAVER BACKGROUND IMAGE SUPPORT

Administrators have the ability to display a screen saver background image on the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 SIP phones. The screen saver background image is displayed on the bottom layer of the screen saver, beneath the date, time, and missed calls indicator. The image can be set by defining the location and filename of the image using the "**screen saver background image**" parameter. For screen saver background image file transfers, the FTP, HTTP, and HTTPS protocols are supported.

Note: The TFTP protocol is supported but not recommended to be used if the image file is large and in the PNG file format. If the TFTP protocol must be used, it is recommended the image be in the JPG file format.

The screen saver background images can also be dynamically updated at a set interval, by configuring the "**screen saver refresh timer**" parameter. For example, if the "**screen saver refresh timer**" parameter is defined as "5" the screen saver background image will be refreshed every five minutes.

Screen saver background images share the same requirements as the idle screen background images. These requirements are as follows:

- 320x240 pixels (6867i / 6920)
- 480x272 pixels (6869i / 6930)
- 800x480 pixels (6873i / 6940 / 6970)
- 24 or 32-bit color depth
- 1MB maximum file size
- Both JPG and PNG files are supported (JPG strongly recommended due to smaller file size and faster loading time)
- There should be no frame around the image

CONFIGURING A BACKGROUND IMAGE ON THE SCREEN SAVER

Use the following procedures to configure a background image on the screen saver.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Background Image on Screen Saver” on page A-79.

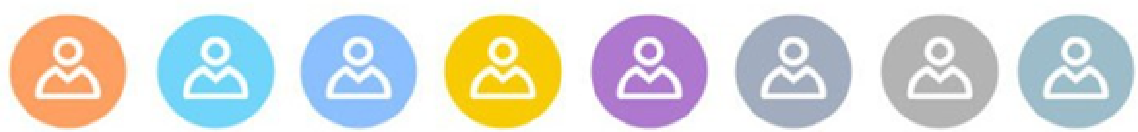
COLOR AVATARS

Note: Applicable to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones only.

Color Avatars on the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones shows color avtar of the caller in the following events:

- Incoming Calls
- Outgoing Calls
- Received Callers List entries
- Outgoing Redial List entries
- Directory entries
- Chat
- Contact softkeys
- Speed dial

Color Avatar feature is enabled using configuration files only. Once this feature is enabled phone will display the avatar image/initials in white and a random color among a choice of eight.



Color Avatar Image

When Use Color Avatar feature disabled a generic avatar image is displayed as below.

Generic Avatar Image

Enabling/Disabling the Color Avatars Using the Configuration Files

Use the following parameter to enable/disable use color avatar on the phone.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Use Color Avatar," on page 79.

PICTURE ID FEATURE

Note: Applicable to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones only.

The Picture ID feature on the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 shows a picture ID of a caller on the LCD for all of the following events on the phone:

- Incoming Calls (matched to Caller ID numbers)
- Outgoing Calls (matched to dialed numbers)
- Directory entries
- Received Callers List entries
- Outgoing Redial List entries
- Speed dial
- BLF/BLF List

Note: The M685i and M695i expansion module BLF keys do not display picture ID.

Your Administrator stores the pictures in a centralized picture repository. The pictures are dynamically retrieved from the centralized server for each call and then locally cached in the phone to reduce network traffic.

If there is no picture on the central server for the dialed number and/or Caller Id number, and Directory, Received Callers List, and/or Outgoing Redial List entry, the generic avatar image is shown.

Generic Avatar Image

For 6800 series phones, pictures must be in ".png" format, 150 pixels wide x 150 pixels tall, and in 24-bit or 32-bit color. The filenames for pictures must be stored using the phone number as the filename (for example, 9995551234.png). Enabling and disabling Picture ID on the phone can be done by an Administrator using the configuration files only

Notes:

1. The Picture ID feature supports the use of TFTP, FTP, HTTP, and HTTPS protocols when downloading pictures.
2. The resolution specification for Picture IDs in releases previous to Release 4.3.0 SP1 was 150x200 pixels. Picture IDs that are 150x200 pixels can still be used, but will not be optimally displayed on-screen due to the UI redesign implemented in Release 4.3.0 SP1. To align with the new UI implemented in Release 4.3.0 SP1, ensure the resolution of your Picture IDs are 150x150 pixels.

Enabling/Disabling the Picture ID on the Phone Using the Configuration Files

Use the following parameter to enable/disable Picture ID on the phone.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Picture ID Feature" on page A-81.

SELF-AVATAR DISPLAY ON IDLE SCREEN

The 6873i, 6940, and 6970 phone models allow users to display a self-picture ID on the idle screen attached to the focused line.

When this feature is enabled, the phone requests image from the server if the picture was not previously downloaded and displays the image corresponding to the focused line.

For example, if Line1 of the SIP phone is configured with extension 1234, the phone requests an image from the server corresponding to the SIP account extension and 1234.png is displayed when the phone is focused on Line1.

Note: The display of the line picture is supported only if the **image server uri** is configured.

If a user has multiple SIP accounts configured on the phone, the avatar on the idle screen changes when the user switches to a different account and the username.png of the focused line is displayed.

You can enable or disable this feature using the "**idle screen avatar**" parameter in the configuration file or at the location ***Options->Display->Show Picture*** in the IP Phone UI.

Enabling or Disabling Self-Avatar Display on Idle Screen Using Configuration Files

Use the following parameter to enable or disable self-picture ID display on idle screen in 6873i, 6940, and 6970 SIP Phones.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, section Self-Avatar Display on Idle Screen on page A-245.

PICTURE REFRESH

In release 5.0.0.SP1, a time to live mechanism is implemented for the avatars to refresh the image cache periodically and keep the phone updated with the most recent images.

A new configuration parameter "**picture refresh timeout**" is introduced which when expires, sends request for Avatar pictures and updates the image cache with the most recent pictures.

Administrators can enable this feature using the configuration files.

Enabling or Disabling Picture Refresh on Idle Screen Using Configuration Files

Use the following parameter to enable or disable the timeout period for picture refresh feature.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, section Picture Refresh Timeout on page A-245.

LINE LABELING WITH CALLER ID

During an incoming call, the caller ID displays on the line and mobile top softkeys and expansion modules (M685i and M695). For 6873i and 6940 phone models, the caller ID is displayed in two lines; one displaying the name and other, the number.

Administrators can enable this functionality by defining the “line show caller id” parameter as “1” in the configuration files.

Enabling or Disabling Line Labeling with Caller ID Using the Configuration Files

Use the following parameter to enable or disable the caller ID display on the 6800 and 6900 series phones.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, section Line Labeling with Caller ID on page A-245.

IDLE SCREEN ERROR MESSAGES SUPPRESSION

A feature on the IP phones allows administrators to enable or disable idle screen error messages suppression.

When idle screen error messages suppression is enabled the IP phone will suppress the error message on the idle screen. This parameter is bitwise, it means only the 3 least significant bit are used, but any value can be configured.

1: suppress 802.1x error

2: suppress TR-069 error

4: suppress https cert error

As a result "idle screen error messages suppression: 3" will suppress 802.1x and TR-069 error message on idle screen.

Note: The idle screen error messages suppression parameter can be configured using the configuration file only.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, Appendix A, "idle screen error messages suppression." on page page A-82.

AUDIO DHSG HEADSET

Notes:

1. Applicable to the 6865i, 6867i, 6869i, 6920, and 6930 IP Phones only.
2. One headset should be plugged in at a time, hence before connecting the DHSG headset to the IP phones, ensure to disconnect (unpair) other headsets.

DHSG is a standard for telecommunication headsets. The 6865i, 6867i, 6869i, 6920, and 6930 IP Phones support the use of a DHSG headset.

Use of a non-verified DHSG headset solution is at the customer's own discretion and the customer should be aware that some DHSG headsets require an optional cable in order to be electrically DHSG compliant. Mitel is not responsible for any damage to the IP phone or headset that may result from the use of non-verified headsets, or from incorrectly connecting headsets or cables.

WARNING:

1. **THE HEADSET PORT IS FOR HEADSET USE ONLY. PLUGGING ANY OTHER DEVICES INTO THIS PORT MAY CAUSE DAMAGE TO THE PHONE AND WILL VOID YOUR WARRANTY.**
2. **CUSTOMERS SHOULD READ AND OBSERVE ALL SAFETY RECOMMENDATIONS CONTAINED IN HEADSET OPERATING GUIDES WHEN USING ANY HEADSET.**

REFERENCE

For more information about installing a DHSG headset on your phone, see the ***IP Phone-Specific Installation Guide***.

CONFIGURING DHSG ON THE PHONE

You can enable or disable the use of a DHSG headset using the parameter "**dhsg**" in the configuration files, or at the location ***Options->Preferences->Set Audio->DHSG*** in the IP Phone UI. Default for DHSG is disabled (OFF).

Configuring DHSG Using the Configuration Files

Use the following information to configure the use of a DHSG headset on the IP Phones.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "idle screen error messages suppression" on page A-82.

Configuring DHSG using the IP Phone UI

Use the following procedure to configure DHSG using the IP Phone UI.

IP PHONE UI

For the 6865i:

1. Press on the phone to enter the Options List.
2. Select Preferences.
3. Select **Set Audio**.
4. Select **DHSG** and toggle the DHSG support ON or OFF
5. If you select "**Off**", press **Done** to save your setting.
6. Press **Set** or **Done** to save your setting. The setting applies immediately to the phone.

For the 6867i/6869i/6920/6930:

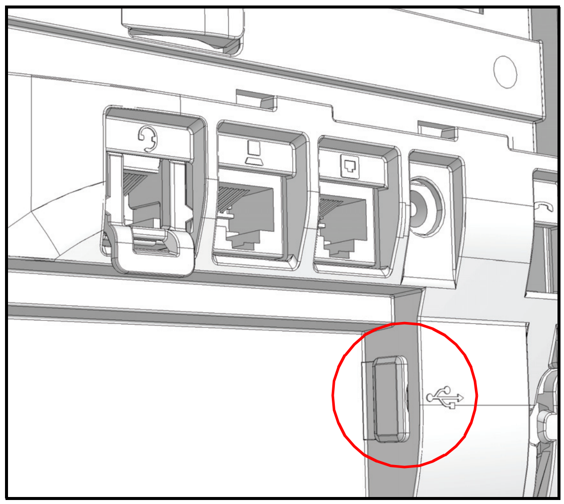
1. Press or to enter the Options List.
2. Navigate to the **Audio > Headset** option and press the button or Select softkey.
3. Press the ▲ key to highlight **DHSG**.
4. With **DHSG** highlighted press the ▶ key to move to selection column.
5. Use the ▲ and ▼ keys to scroll through and choose whether or not to enable DHSG. Valid values are:
   - DHSG is OFF (default)
   - DHSG is ON
6. Press the **Save** softkey to save your changes.

USB HEADSET SUPPORT

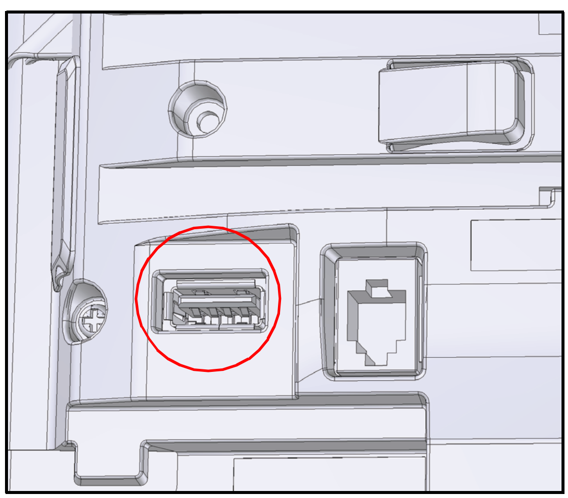
Note: Applicable to the 6867i, 6869i, 6873i, 6920, 6930, and 6940 IP Phones only.

Various USB headsets are supported for the Mitel 6867i, 6869i, 6873i, 6920, 6930, and 6940 SIP phones. Users can simply plug in the supported USB headset into the USB input port located on the back of their phones and configure the phone's audio mode accordingly (e.g. Headset, Speaker/Headset, or Headset/Speaker) to start using their USB headset.

6867i/6869i/6920/6930 USB Input Port Location



6873i/6940 USB Input Port Location



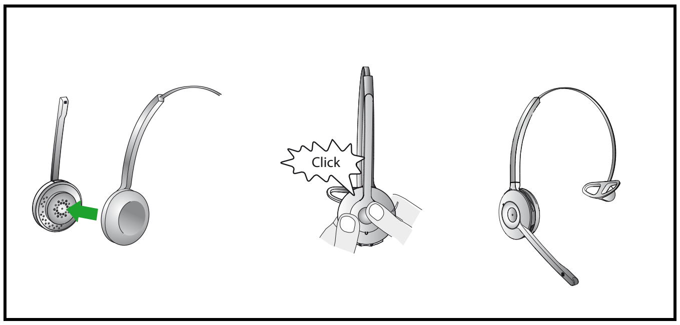
Notes:

1. For the 6867i, 6869i, 6920, and 6930, if both an analog (non-DHSG) headset and a USB headset are connected to the phone, the USB headset will take precedence over the analog headset (i.e. the USB headset will be functional while the analog headset will not be functional).
2. For the 6867i, 6869i, 6920, and 6930, if both a DHSG headset and a USB headset are connected to the phone and DHSG is enabled, the DHSG headset will take precedence over the USB headset.

Mitel Integrated DECT Headset

Applicable to 6930 and 6940 IP Phones only.

The Mitel Integrated DECT Headset is a professional wireless headset designed for maximum performance.



The Mitel Integrated DECT Headset is compatible with Mitel MiVoice 6930 and 6940 phone. The Mitel Integrated DECT Headset is also compatible with the Mitel M695 Programmable Key Module, supporting up to three modules connected to your 6930 and 6940 IP phone.

To enable audio on the Mitel Integrated DECT Headset, set the audio mode on the 6930 and 6940 IP phone to Headset, Headset/Speaker, or Speaker/Headset.

Notes:

1. One headset should be plugged in at a time, hence before connecting the Mitel Integrated Headset to Mitel MiVoice 6930 IP phone, ensure to disconnect (unpair) other headsets.
2. Use a IEEE 802.3at compliant PoE L2 Switch, IEEE 802.2at Inline Power Injector, or an AC to DC Adapter to power the Mitel MiVoice 6930 IP phone when connecting the Mitel Integrated DECT Headset to a Mitel M695 Programmable Key Module.

Features

- Wideband audio for exceptional sound quality
- Volume and mute controls
- Intuitive headset multi-function button for easy call handling
- LED and audio indicators
- Advanced hearing protection

- Noise-canceling microphone
- Up to 8 hours battery life
- Headset recharge docking cradle
- Visual and audio call status indicators
- Battery indicator

Note: For more information on Mite DECT headset usage, refer to the ***<model specific> SIP Phone User Guide***.

CORDED EXTENSION MICROPHONE SUPPORT

Applicable to 6970 IP Phone only.

To ensure better coverage of the larger premises, the Mitel 6970 IP Conference Phone supports up to 2 extension microphones. The extension microphone will extend the pick up range of the phone to allow it to be used in large rooms.

Note: For more information on extension microphone usage, refer to the ***6970 SIP Phone User Guide***.

BLUETOOTH HEADSET SUPPORT

Applicable to 6873i, 6930 and 6940 IP Phones only.

The 6873i, 6930 and 6940 IP Phones do not support pairing with any Bluetooth device that requires a PIN code.

FAT32 USB file system format

The USB drive file system has to be set as FAT32 to be detected by the phone.

The 6873i, 6930 and 6940 IP Phones support the use of various Bluetooth headsets as an alternate audio device. Using the phone UI, you can enable and disable the Bluetooth functionality on your phone as required. You can also pair, connect, and unpair a Bluetooth headset as applicable.

Note: For more information on Bluetooth headset usage, refer to the ***<model specific> SIP Phone User Guide***.

BLUETOOTH CORDLESS HANDSET SUPPORT

Applicable to 6873i, 6930 and 6940 IP Phones only.

The Bluetooth Cordless Handset is a standard accessory for the 6940 SIP phone and an optional accessory for the 6930 and 6873i SIP phones.

The following are the features of the BT cordless handset:

- Uses BT 4.1 technology to provide HD voice quality
- Enables call answer, hang-up, mute, and volume up/down through buttons on the side of handset
- Plays ringtone on handset and base phone
- Recharges in-built battery through contacts built into base phone
- Indicates charge status through LED display

After an upgrade from MiNet to SIP firmware, the Bluetooth Cordless Handset pairing info may not be retained. Users must again pair the Bluetooth Cordless Handset with the 6940, 6930 or 6873i SIP phones.

You can also pair, connect, and unpair a Bluetooth handset as applicable.

Note: For more information on Bluetooth Handset usage, refer to the ***<model specific> SIP Phone User Guide***.

BLUETOOTH MOBILE INTEGRATION

6930, 6940, and 6970 IP phones support Bluetooth mobile integration between a SIP phone and a mobile phone.

Note: User can control the Bluetooth auto-connect behavior on 6970 SIP Phone without Hot desk logged in. For details, see the *Mitel 6970 IP Conference Phone User Guide.*

MOBILE SOFTKEY CONFIGURATION

The user can configure a new softkey type – "mobile" for BT phones on top softkeys or on LCD expansion modules through configuration files and the Web UI.

Configure Mobile Softkey Using Configuration Files

CONFIGURATION FILES

Use the topsoftkeyN type parameter to configure mobile softkey on 6930, 6940, and 6970 SIP phones using the startup.cfg and [mac.cfg] configuration files.

```
For example, topsoftkey4 type: mobile
```

MOBILE CONTACTS SYNC

With Bluetooth mobile integration, users can access the mobile phone directory and import mobile contacts into the SIP Phone. The mobile contacts are then available for look up and dial and for identification through caller ID.

Users can enable or disable the mobile contacts import and assign a custom name to the mobile contacts folder in the directory using the configuration parameters "mobile contacts enabled" and "mobile contacts name".

Enable or disable the mobile contacts import and assign a customized name to the mobile contacts folder in the directory

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, section "Mobile Contacts Sync" on page A-246.

HOT-DESKING

6930, 6940, and 6970 SIP IP phones support mobile integration for hot-desking accounts.

In hotdesking mode, the Bluetooth parameter is always saved in the local.cfg configuration file instead of the user-local.cfg configuration file.

PHONE AUTO-LOCK AND UNLOCK ON MOBILE PROXIMITY

With mobile integration, the 6930, 6940, and 6970 phones automatically lock or unlock after a preconfigured delay when a paired mobile phone is disconnected or reconnected.

Administrators can configure this feature through the configuration files and users through Mitel Web UI and phone UI.

See the <Model-Specific> ***SIP Phone User Guide*** for information on Mitel Web UI and phone UI configuration options.)

Enabling or Disabling the Phone Automatic Lock and Unlock on Mobile Proximity Using the Configuration Files

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, section "Phone Auto-lock and Unlock on Mobile Proximity" on page A-246.

BLUETOOTH MOBILE INTEGRATION LIMITATION

With mobile integration, when you are on an active mobile call using your desk phone handset (connected through a Bluetooth device) and there an incoming call to the desk phone from another desk phone, the desk phone switches to the call from the other desk phone and the caller on the mobile phone is kept on hold. However, no hold tone is played to the mobile caller during the hold period.

Music on hold failure scenario:

- A mobile phone is connected to a desk phone with a Bluetooth device using the Mobile Integration key.
- A call on a mobile phone is answered using the handset of the connected desk phone.
- While the call is active, the desk phone connected to the mobile phone receives a call from another desk phone.
- The desk phone connected to the mobile switches to the new call from the other desk phone.

While the two desk phones are engaged in the call, the call on the mobile phone is placed on hold, but music on hold is not played for the caller on the mobile phone during the hold period. The first call (between the mobile caller and the desk phone connected to the mobile) is re-established after the second call between the two desk phones end.

AUDIO HI-Q ON G.722 CALLS

The Mitel IP phones support the Hi-Q (high quality) audio technology which delivers enhanced performance and voice clarity for Mitel's 6800 and 6900 series of SIP phones. Incorporating wideband audio technology, Mitel Hi-Q significantly improves the audio quality of calls. This technology provides a more lifelike conversation when the G.722 wideband Codec is used. The 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP phones display a large icon when Hi-Q is being used on the call. On the 6863i, 6865i, 6905, and 6910 screens, the text of "**Hi-Q**" displays on the same line as the call timer.

AUDIO TRANSMIT AND RECEIVE GAIN ADJUSTMENTS

You can adjust the IP phone handset, headset, and speakerphone to best suit your comfort level and deployment environment by using the following parameters in the configuration files:

- headset sidetone gain
- handset sidetone gain
- audio mode

HEADSET SIDETONE

Disables the sidetone on the analog headset of the phone.

HANDSET SIDETONE

Disables the sidetone on the analog handset of the phone.

Configuring Audio Transmit and Receive Gain Adjustments Using the Configuration Files

Use the following procedure to configure the audio transmit and gain adjustments using the configuration files.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section "Audio Transmit and Receive Gain Adjustments" on page A-234.

AUDIO MODE CONFIGURATION

The "audio mode" parameter allows you to configure how the handsfree key works. The following four options are available:

- **0.** Speaker - This is the default setting. Calls can be made or received using the handset or handsfree speakerphone. In handset audio mode, pressing the handsfree button on the phone switches to handsfree speakerphone. In Speaker audio mode, lift the handset to switch to the handset.
- **1**. Headset - Choose this setting if you want to make or receive all calls using a handset or headset. For the 6867i, 6869i, 6873i, 6920, 6930, and 6940, calls can be switched from the handset to headset by pressing the handsfree button on the phone. To switch from the headset to the handset, lift the handset.
- **2**. Speaker/Headset - Incoming calls are sent to the handsfree speakerphone first when the handsfree button is pressed. By pressing the handsfree button again, you can switch back and forth between the handsfree speakerphone and the headset. For the 6867i, 6869i, 6873i, 6920, 6930, and 6940 lifting the handset at any time switches back to the handset from either the handsfree speakerphone or the headset.
- **3**. Headset/Speaker - Incoming calls are sent to the headset first when the handsfree button is pressed. By pressing the handsfree button again, you can switch back and forth between the headset and the handsfree speakerphone.
  For the 6867i, 6869i, 6873i, 6920, 6930, and 6940 lifting the handset at any time switches back to the handset from either the headset or the handsfree speakerphone.

Note: On 6865i, 6867i, 6869i, 6873i, 6910, 6920, 6930, and 6940 IP phones, the audio mode is set to Speaker by default. When the headset is connected to the phone, the user must change the audio mode to headset or speaker/headset or headset/speaker.

CONFIGURING AUDIO MODE USING THE CONFIGURATION FILES

Use the following procedure to configure the audio mode using the configuration files.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Audio Transmit and Receive Gain Adjustments" on page 234.

AUDIO MODE VOLUME

Adjusts the volume for the ringer, handset, headset, and speakerphone. Press the volume control keys while the phone is ringing to adjust the ringer volume. Pressing these keys during an active call adjusts the volume of the audio device being used (handset, headset, or speaker).

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "Audio Mode Volume" on page A-236.

LIVE DIALPAD

The "Live Dialpad" option on the IP phone turns the Live Dial Pad mode ON or OFF. With live dial pad ON, the IP phone automatically dials out and turns ON Handsfree mode as soon as a dial pad key or softkey is pressed. With live dial pad OFF, if you dial a number while the phone is on-hook, lifting the receiver or pressing the Speaker/Headset button initiates a call to that number.

*Availability of feature dependent on your phone system or service provider.

A User can turn the “Live Dialpad” ON and OFF using the IP Phone UI only. A System Administrator can turn it ON and OFF using the IP Phone UI or the configuration files.

ENABLING/DISABLING LIVE DIALPAD USING THE CONFIGURATION FILES

Use the following procedure to enable/disable Live Dialpad on the IP Phones.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Live Dialpad Settings” on page A-82.

ENABLING/DISABLING LIVE DIALPAD USING THE IP PHONE UI

Use the following procedure to enable/disable Live Dialpad on the IP Phones.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Preferences**.
3. Select **Live Dialpad**.
4. Press the ▲ and ▼ arrow keys to toggle the live dialpad setting ON or OFF.
5. Press **Done** to save the setting.

For the 6867i/6869i/6920/6930:

1. Press or to enter the Options List.
2. Navigate to the **Dialpad -> Live Dialpad** option and press the button or Select softkey.
3. Use the ▲ and ▼ keys to scroll through and enable (On) or disable (Off) the live dialpad feature.
4. Press the **Save** softkey to save your changes.

For the 6873i/6940/6970:

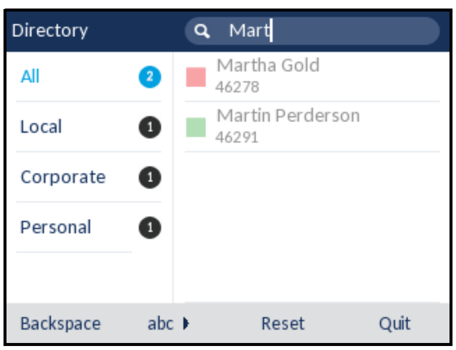
1. Press [settings key], [settings key], or the **Settings** softkey to enter the Options List.
2. Press the **Dialpad** icon.
3. Press the **Live Dialpad** icon.
4. Choose **On** to enable or **Off** to disable the live dialpad feature.
5. Press the **Save** softkey to save your changes.

LIVE KEYBOARD

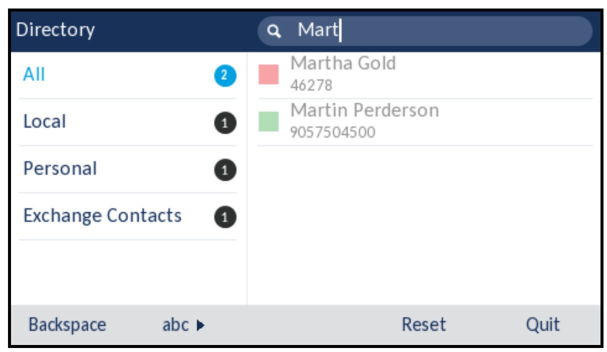
When the 6867i/6869i SIP phone is in an idle state and a alphabetic character key on an attached K680i keyboard is pressed, the default behavior of the phone is to simply wake up (if the phone is dimmed or displaying the Screensaver).

Users can enable the Live Keyboard feature, which, in addition to waking up the phone (if applicable), will launch the Directory search function in such scenarios. For example, pressing the "M" character key on the K680i keyboard when on the idle/home screen will cause the phone to navigate immediately to the Directory with "M" in the search field.

6867i Directory Search



6869i Directory Search



Note: Irrespective of whether the Live Keyboard feature is enabled or disabled, pressing a numerical key on the K680i keyboard when on the idle/home screen will result in the phone initiating the dialing function.

Users can enable/disable the Live Keyboard feature using the phone's native UI setting located in the Options List under *Directory* > *Settings* > *Live Keyboard*. Administrators have the added option of enabling/disabling the Live Keyboard feature by defining the "**live keyboard**" parameter as "1" (enabled) or "0" (disabled) in the respective configuration file.

Note: The Live Keyboard feature is disabled by default.

LIVE KEYBOARD SUPPORT FOR XML APPLICATIONS

The Live Keyboard feature can also be used in conjunction with XML applications (e.g. XML-based directories). By enabling the Live Keyboard feature and by defining the "**keyboard script**" parameter with the respective URI in the configuration files, pressing an alphabetic character key on an attached K680i keyboard on the home/idle screen will launch the XML application and pass the character to the XML application first input field (if available).

Notes:

1. The "**keyboard script**" setting can only be defined using the configuration files.
2. If the "**keyboard script**" parameter is not defined, the phone will attempt to pass the pressed key to the XML application defined in the "**directory script**" parameter. If the "**directory script**" parameter is not defined as well, the phone's native Directory search function will be launched. For more information on the "**directory script**" parameter, see "Customizable Directory List Key" on page 312.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Live Keyboard Settings" on page A-84.

ENABLING/DISABLING THE LIVE KEYBOARD USING THE IP PHONE UI

Use the following procedure to enable/disable the Live Keyboard feature on the IP Phones.

IP PHONE UI

1. Press ⚙ to enter the Options List.
2. Navigate to the **Directory > Settings** option and press the ✓ button or **Select** softkey.
3. Use the ▲ key to scroll down and highlight the Live Keyboard setting.

   Note: The Live Keyboard setting is only available in this menu if a K680i keyboard is attached to the phone.

4. Press 4 to move to the selection column.
5. Use ▲ and ▼ keys to enable (On) or disable (Off) the feature.
6. Press the **Save** softkey to save your changes.

LANGUAGE

The IP phones support several different languages. You can have the IP phone UI and the Mitel Web UI display in a specific language as required. When you set the language to use, all of the display screens (menus, services, options, configuration parameters, etc.) display in that language. The IP phones support the following languages:

AVAILABLE LANGUAGE	ASSOCIATED LANGUAGE FILE (INCLUDED IN THE FIRMWARE FILE WHEN DOWNLOADED FROM CONFIGURATION SERVER)
English	Default (resides on the phone)
Arabic (6867i, 6869i, 6873i, 6920, 6920, 6930, 6940 and 6970 only)	lang_ar.txt

AVAILABLE LANGUAGE	ASSOCIATED LANGUAGE FILE (INCLUDED IN THE FIRMWARE FILE WHEN DOWNLOADED FROM CONFIGURATION SERVER)
Catalan	lang_ca.txt
Valencian	lang_ca_va.txt
Czech (UTF-8)	lang_cs.txt
Czech (ASCII)	lang_cs_op.txt
Welsh	lang_cy.txt
German	lang_de.txt
Greek (6867i, 6869i, 6873i, 6920, 6930, 6940 only)	lang_el.txt
Danish	lang_da.txt
Spanish	lang_es.txt
Mexican Spanish	lang_es_mx.txt
Euskera	lang_eu.txt
Finnish	lang_fi.txt
French	lang_fr.txt
Canadian French	lang_fr_ca.txt
Galego	lang_gl.txt
Hungarian	lang_hu.txt
Italian	lang_it.txt
Korean (6867i, 6869i, 6920, 6930 only)	lang_ko.txt
Dutch	lang_nl.txt
Dutch (Netherlands)	lang_nl_nl.txt
Norwegian	lang_no.txt
Polish (ASCII)	lang_pl.txt
Polish (UTF-8)	lang_pl_pl.txt
Portuguese	lang_pt.txt
Portuguese Brazilian	lang_pt_br.txt
Romanian	lang_ro.txt
Russian	lang_ru.txt
Slovak (UTF-8)	lang_sk.txt
Slovak (ASCII)	lang_sk_op.txt
Swedish	lang_sv.txt
Turkish	lang_tr.txt
Simplified Chinese (6867i, 6869i, 6920, 6930 only)	lang_zh_cn.txt

AVAILABLE LANGUAGE	ASSOCIATED LANGUAGE FILE (INCLUDED IN THE FIRMWARE FILE WHEN DOWNLOADED FROM CONFIGURATION SERVER)
Traditional Chinese (6867i, 6869i, 6920, 6930 only)	lang_zh_tw.txt

LOADING LANGUAGE PACKS

You make languages available to use on the phone by loading language packs from the configuration server to the local *<MAC>.cfg* configuration file. You can use the configuration files or the Mitel Web UI to perform the download. Each language pack consists of the IP Phone UI and Mitel Web UI translated in a specific language.

Loading Language Packs via the Configuration File (<mac>.cfg)

Using the configuration files, you specify a language pack to load in the following format:

```
lang_<ISO 639>_<ISO 3166>.txt
or

lang_<ISO 639>.txt
```

where <ISO 639> is the language code specified in Standard ISO 639 (see Appendix A, the section, Language Codes (from Standard ISO 639) on page 220) and <ISO 3166> is the country code specified in Standard ISO 3166 (see Country Codes (from Standard ISO 3166) on page 221). The <ISO 3166> attribute is optional.

Note: Adding/changing language packs can only be done at bootup of the IP phone. The default language (English) cannot be changed or removed.

Example

The following is an example of the parameters you would enter in the *<MAC>.cfg* file to load a French, Italian, German, and Spanish language pack to the IP phone.

```
language 1: lang_fr_ca.txt
language 2: lang_it.txt
language 3: lang_de.txt
language 4: lang_es.txt
```

The above entries in the *<MAC>.cfg* file tells the phone which language packs to load. When the language pack(s) have loaded, you must then use the configuration files IP Phone UI to specify which language to display on the IP phone. You must use the Mitel Web UI to specify the language to use in the Web UI.

References

For more information about specifying the language to use, see the section, "Specifying the Screen Language to Use" on page 5-64.

For more information about language codes and country codes, see Appendix A, the section, "Language Pack Settings" on page 218.

Loading Language Packs via the Mitel Web UI

Using the Mitel Web UI, you can specify a language pack to load using the parameters at *Basic Settings->Preferences->Language Settings*.

You use the following fields in the Mitel Web UI to specify which language packs to load:

Once the language pack is loaded to the phone, it is available for selection from either the configuration files, the IP Phone UI or the Mitel Web UI.

Procedure to enable Traditional/Simplified Chinese character support on SIP phones

1. Place the <font>.tar.gz file and the Chinese language files (lang_zh_xx.txt files) at the same location on your configuration server folder as is your SIP firmware.

   Ensure that the font_zh_Hans.tar.gz file is not renamed. If this file is renamed, the phone will not read and install the file.

2. Add the parameter "language 1: lang_zh_tw.txt" (traditional) and/or "lang_zh_cn.txt" (simplified) in the configuration file (for example, startup.cfg).

3. Reboot the phone (ensure that the phone points to the configuration folder).

   The phone will reboot twice. During the first reboot cycle, the phone downloads the font and language files and during the second reboot cycle, it applies these files.

Procedure to enable Korean character support on SIP phones

1. Place the <font>.tar.gz file and the Korean language file (lang_ko.txt file) at the same location on your configuration server folder as is your SIP firmware.

   Ensure that the font_zh_Hans.tar.gz file is not renamed. If this file is renamed, the phone will not read and install the file.

2. Add the parameter "language 2: lang_ko.txt" (korean) in the configuration file (for example, startup.cfg).

3. Reboot the phone (ensure that the phone points to the configuration folder).

   The phone will reboot twice. During the first reboot cycle, the phone downloads the font and language files and during the second reboot cycle, it applies these files.

Notes:

1. Korean language support is currently provided for 6867i, 6869i, 6920 and 6930 phones against MX-ONE deployments only.
2. MX-ONE requires a configuration settings for Korean language support.

SPECIFYING THE SCREEN LANGUAGE TO USE

Once the language pack(s) have loaded, you must then specify which language to use on the phone. After the phone has booted up, you can specify which language(s) to use. You can use the configuration files (via the "**language**" parameter) and the IP Phone UI to specify the language for the IP Phone UI. You can use the configuration files (via the "**web language**" parameter) and Mitel Web UI to specify the files for the Mitel Web UI.

Use the following procedures to specify the language to use on the IP phone.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Language Settings" on page A-216 and "Language Pack Settings" on page A-218.

Notes:

1. If you specify the language to use on the phone via the configuration files, you must reboot the phone for the changes to take affect.
2. All languages may not be available for selection. The available languages are dependent on the language packs currently loaded to the IP phone.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Preferences.**
3. Select **Language**.
4. Select **Screen Language**. The language setting displays a check mark indicating this is the current language on the IP phone.
5. Using the ▲ and ▼ keys, scroll through the languages.

   Note: All languages may not be available for selection. The available languages are dependent on the language packs currently loaded to the IP phone. English is the default language and cannot be changed or removed. For more information about loading language packs, see your System Administrator.

6. Press the key or select **Set** to set the language on the phone.
   The change is dynamic. When you exit the Options List, the phone displays all menu items in the language you selected.

For the 6867i/6869i/6920/6930:

1. Press or to enter the Options List.
2. Navigate to the **Language** option and press the button or Select softkey.
3. With **Screen Language** highlighted press the ▶ key to move to selection column.
4. Use the ▲ and ▼ keys to scroll through and choose the desired screen language.
5. Press the **Save** softkey to save your changes.

For the 6873i/6940/6970:

1. Press , , or the **Settings** softkey to enter the Options List.
2. Press the **Language** icon.
3. Choose the desired screen language.
4. Press the **Save** softkey to save your changes.

MITEL WEB UI

1. Click on **Basic Settings->Preferences->Language Settings.**

Loading the Language Pack

2. In the "**Language N**" fields, enter the file name of the language pack you want to use to display a specific language in the Mitel Web UI. For example, you could enter any of the following in the "Language 1", "Language 2", "Language 3", and "Language 4" fields to display the Mitel Web UI in the respective language:

- lang_ar.txt (Arabic)
- lang_ca.txt (Catalan)
- lang_ca_va.txt (Valencian)
- lang_cs.txt (Czech - UTF-8)
- lang_cs_op.txt (Czech - ASCII)
- lang_cy.txt (Welsh)
- lang_de.txt (German)
- lang_el.txt (Greek - 6867i, 6869i, and 6873i only)
- lang_da.txt (Danish)
- lang_es.txt (Spanish)
- lang_es_mx.txt (Mexican Spanish)
- lang_eu.txt (Euskera)
- lang_fi.txt (Finnish)
- lang_fr.txt (French)
- lang_fr_ca.txt (Canadian French)
- lang_gl.txt (Galego)
- lang_hu.txt (Hungarian)
- lang_it.txt (Italian)
- lang_ko.txt (Korean)
- lang_nl.txt (Dutch)
- lang_nl_nl.txt (Dutch - Netherlands)
- lang_no.txt (Norwegian)
- lang_pl.txt (Polish - ASCII)

- lang_pl_pl.txt (Polish - UTF-8)
- lang_pt.txt (Portuguese)
- lang_pt_br.txt (Brazilian Portuguese)
- lang_ro.txt (Romanian)
- lang_ru.txt (Russian)
- lang_sk.txt (Slovak - UTF-8)
- lang_sk_op.txt (Slovak - ASCII)
- lang_sv.txt (Swedish)
- lang_tr.txt (Turkish)
- lang_zh_cn.txt (Simplified Chinese)
- lang_zh_tw.txt (Traditional Chinese)

3. Click **Save Settings** to save your changes.

Specifying the Language to Use in the Mitel Web UI

4. After restarting your phone, log back in using the Mitel Web UI.

5. Click on **Basic Settings->Preferences->Language Settings.**

6. In the "**Webpage Language**" field, select a language to apply to the Mitel Web UI.

> **Note:** All languages may not be available for selection. The available languages are dependent on the language packs currently loaded to the IP phone. English is the default language and cannot be changed or removed. For more information about loading language packs, see "Loading Language Packs" on page 5-62.

7. Click **Save Settings** to save your changes.
The Mitel Web UI displays all screens in the language you chose.

SPECIFYING THE INPUT LANGUAGE TO USE

The phones support text and character inputs in various languages (English, German, French, Spanish, Italian, Portuguese, Russian, Nordic, and Greek [6867i, 6869i, and 6873i only]).

Inputting textual or character information into the IP Phone UI and XML scripts can now be done in various languages using the keypad on the phone (or for the 6873i, the on-screen keyboard). The System Administrator and User can enable this feature using the Mitel Web UI or the IP Phone UI. An Administrator can also use the configuration files to enable this feature. Users can then use text and characters in a specific language when performing inputs on the phone.

The following tables identify the language characters that a User can enter on the phones that support the Input Language feature.

> **Note:** For information regarding the 6873i on-screen keyboard, refer to the *6873i SIP Phone User Guide*.

Keypad Text/Character Input Tables

English (default)

KEY	UPPERCASE CHARACTERS	LOWERCASE CHARACTERS
0	0	0
1	1;=_,-'&()	1.:;=_,-'&()
2	ABC2	abc2
3	DEF3	def3
4	GHI4	ghi4
5	JKL5	jkl5
6	MNO6	mno6
7	PQRS7	pqrs7
8	TUV8	tuv8
9	WXYZ9	wxyz9
*	* <SPACE>	* <SPACE>
#	#/\@	#/\@

French

KEY	UPPERCASE CHARACTERS	LOWERCASE CHARACTERS
0	0	0
1	1.:;=_,-'&()	1.:;=_,-'&()
2	ABC2ÀÂÇÁÅÆ	abc2àâçáåæ
3	DEF3ÉÈÊË	def3éèêë
4	GHI4ÎÏ	ghi4îï
5	JKL5	jkl5
6	MNO6ÑÓÒÔÖ	mno6ñóòôö
7	PQRS7	pqrs7
8	TUV8ÚÙÛÜ	tuv8úùûü
9	WXYZ9	wxyz9
*	* <SPACE>	* <SPACE>
#	#/\@	#/\@

Spanish

KEY	UPPERCASE CHARACTERS	LOWERCASE CHARACTERS
0	0	0
1	1.:;=_,-'&()	1.:;=_,-'&()
2	ABC2ÁÀÇ	abc2áàç
3	DEF3ÉÈ	def3éè
4	GHI4ÏÍ	ghi4ïí
5	JKL5	jkl5
6	MNO6ÑÓÒ	mno6ñóò
7	PQRS7	pqrs7
8	TUV8ÚÜ	tuv8úü
9	WXYZ9	wxyz9
*	* <SPACE>	* <SPACE>
#	#/\@	#/\@

German

KEY	UPPERCASE CHARACTERS	LOWERCASE CHARACTERS
0	0	0
1	1.:;=_,-'&()	1.:;=_,-'&()
2	ABC2ÄÀ	abc2äà
3	DEF3É	def3é
4	GHI4	ghi4
5	JKL5	jkl5
6	MNO6Ö	mno6ö
7	PQRS7ß	pqrs7ß
8	TUV8Ü	tuv8ü
9	WXYZ9	wxyz9
*	* <SPACE>	* <SPACE>
#	#/\@	#/\@

Italian

KEY	UPPERCASE CHARACTERS	LOWERCASE CHARACTERS
0	0	0
1	1.:;=_,-'&()	1.:;=_,-'&()
2	ABC2ÀCÇ	abc2àcç
3	DEF3ÉÈË	def3éèë
4	GHI4	ghi4
5	JKL5	jkl5
6	MNO6ÓÒ	mno6óò
7	PQRS7	pqrs7
8	TUV8Ù	tuv8ù
9	WXYZ9	wxyz9
*	* <SPACE>	* <SPACE>
#	#/\@	#/\@

Portuguese

KEY	UPPERCASE CHARACTERS	LOWERCASE CHARACTERS
0	0	0
1	1.:;=_,-'&()	1.:;=_,-'&()
2	ABC2ÁÀÂÃÇ	abc2áàâãç
3	DEF3ÉÊ	def3éê
4	GHI4Í	ghi4í
5	JKL5	jkl5
6	MNO6ÓÔÕ	mno6óôõ
7	PQRS7	pqrs7
8	TUV8ÚÜ	tuv8úü
9	WXYZ9	wxyz9
*	* <SPACE>	* <SPACE>
#	# / \ @	# / \ @

Russian

KEY	UPPERCASE CHARACTERS	LOWERCASE CHARACTERS
0	0	0
1	1.:;=_,-'&()	1.:;=_,-'&()
2	АБВГ2ABC	абвг2abc
3	ДЕЁЖЗ3DEF	Деёжз3def
4	ИЙКЛ4GHI	ийкл4ghi
5	МНОП5JKL	мноп5jkl
6	РСТУ6MNO	рсту6mno
7	ФХЦЧ7PQRS	фхЧч7pqrs
8	ШЩЪЫ8TUV	шщъы8tuv
9	ЬЗЮЯ9WXYZ	ьзюя9wxyz
*	* <SPACE>	* <SPACE>
#	#/\@	#/ \@

Nordic

KEY	UPPERCASE CHARACTERS	LOWERCASE CHARACTERS
0	0	0
1	1.:;=_,-'&()	1.:;=_,-'&()
2	ABC2ÅÄÆÀ	abc2åäæà
3	DEF3É	def3é
4	GHI4	ghi4
5	JKL5	jkl5
6	MNO6ÖØ	mno6öø
7	PQRS7ß	pqrs7ß
8	TUV8Ü	tuv8ü
9	WXYZ9	wxyz9
*	* <SPACE>	* <SPACE>
#	#/\@	#/\@

Greek (6867i, 6869i, 6873i, 6920, 6930, 6940 only)

KEY	UPPERCASE CHARACTERS	LOWERCASE CHARACTERS
0	0+	0+
1	1.:;=_,-'&()$!	1.:;=_,-'&()$!
2	ABC2ΑΒΓ	abc2αβγ
3	DEF3ΔΕΖ	def3δεζ
4	GHI4ΗΘΙ	ghi4ηθι
5	JKL5ΚΛΜ	jkl5κλμ
6	MNO6ΝΞΟ	mno6νξο
7	PQRS7ΠΡΣ	pqrs7πρςσ
8	TUV8ΤΥΦ	tuv8τυφ
9	WXYZ9ΧΨΩ	wxyz9χψω
*	* <SPACE>	* <SPACE>
#	#/\@	#/\@

Configuring Language Input Using the Configuration Files

An Administrator can specify the input language to use by entering a specific parameter in the configuration files. An Administrator must enter the following parameter to enable this feature:

- input language

Use the following procedures to specify the input language to use on the IP phone.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Language Settings" on page A-216.

Configuring Language Input Using the IP Phone UI

Once "Language Input" is enabled, an Administrator or User can change the input language on the phone using the IP Phone UI. The "**Input Language**" option appears under the Language option in the IP Phone UI.

Use the following procedure to change the input language using the IP Phone UI.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Language** from the Options List.
3. Select **Input Language** from the Language List.

4. Select the language you want to use on the IP phone for inputting text and characters. Valid values are:
   - English (default)
   - Français (French)
   - Español (Spanish)
   - Deutsch (German
   - Italiano (Italian)
   - Português (Portuguese)
   - Русский (Russian)
   - Nordic
5. Press **Done** when you have selected a language.

For the 6867i/6869i/6920/6930:

1. Press ⚙ or ⚙ to enter the Options List.
2. Navigate to the **Language** option and press the ☑ button or Select softkey.
3. Press the ▲ key to highlight the Input Language option.
4. With **Input Language** highlighted press the ▶ key to move to selection column.
5. Use the ▲ and ▼ keys to scroll through and choose the desired input language. Valid values are:
   - English (default)
   - Français (French)
   - Español (Spanish)
   - Deutsch (German)
   - Italiano (Italian)
   - Português (Portuguese)
   - Русский (Russian)
   - Nordic
   - ελληνικά (Greek)
6. Press the **Save** softkey to save your changes.

For the 6873i/6940:

1. Press ⚙ or ⚙ to enter the Options List.
2. Press the **Language** icon.
3. Press **Input Language**.
4. Choose the desired input language. Valid values are:
   - English (default)
   - Français (French)
   - Español (Spanish)

- Deutsch (German)
- Italiano (Italian)
- Português (Portuguese)
- Русский (Russian)
- Nordic
- ελληνικά (Greek)

5. Press the **Save** softkey to save your changes.

For the 6970:

1. Tap the **Settings** softkey on the phone screen to open the **Settings** menu.

2. Tap the **Language** icon.

3. Swipe up and down to view the language available for selection. Valid values are:

- English
- French
- German
- Spanish
- Spanish (Latin America)
- Portuguese
- Portuguese (Brazil)
- Dutch
- Italian
- Romanian
- Russian
- Swedish
- Polish

4. Tap the applicable language.

5. Tap the **Save** softkey to save your changes.

Configuring Language Input Using the Mitel Web UI

Once "Language Input" is enabled, an Administrator or User can also change the input language on the phone using the Mitel Web UI. The "**Input Language**" option appears at the path *Basic Settings->Preferences->Language Settings.*

Use the following procedure to set the input language using the Mitel Web UI.

MITEL WEB UI

1. Click on **Basic Settings-> Preferences->Language Settings.**

2. Select a language from the "**Input Language**" field. Setting this field allows you to specify the language to use when entering text in the Mitel Web UI, IP Phone UI, or in XML applications on the phone. Valid values are:
   - English (default)
   - Français (French)
   - Español (Spanish)
   - Deutsch (German)
   - Italiano (Italian)
   - Português (Portuguese)
   - Русский (Russian)
   - Nordic
   - ελληνικά (Greek - 6867i, 6869i, and 6873i only)

   Note: Available input languages are dependent on the configuration enabled by your System Administrator.

3. Click **Save Settings** to save your changes.

Configuring Language Input for an XML Application

A System Administrator can enable input languages in XML applications using the **<AastraIPPhoneInputScreen>** object and the “**inputLanguage**” attribute.

Reference

For more information about using XML objects for defining input language, contact Mitel Customer Support regarding the ***Mitel XML Development Guide***.

UTF- 8 CODEC FOR MULTI-NATIONAL LANGUAGE SUPPORT

The IP Phones and expansion modules include support for ISO 8859-2 (Latin2) of multi-national languages when displaying and inputting in the IP Phone UI and the Mitel Web UI. UTF-8 is also compatible with XML encoding on the IP Phones.

The following table illustrates the Latin 2 character set now used on the IP Phones.

	–0	–1	–2	–3	–4	–5	–6	–7	–8	–9	–A	–B	–C	–D	–E	–F
A–	NBSP 00A0 160	Ą 0104 161	˘ 02D8 162	Ł 0141 163	¤ 00A4 164	Ľ 013D 165	Ś 015A 166	§ 00A7 167	¨ 00A8 168	Š 0160 169	Ş 015E 170	Ť 0164 171	Ź 0179 172	SHY 00AD 173	Ž 017D 174	Ż 017B 175
B–	° 00B0 176	ą 0105 177	˛ 02DB 178	ł 0142 179	´ 00B4 180	ľ 013E 181	ś 015B 182	ˇ 02C7 183	¸ 00B8 184	š 0161 185	ş 015F 186	ť 0165 187	ź 017A 188	˝ 02DD 189	ž 017E 190	ż 017C 191
C–	Ŕ 0154 192	Á 00C1 193	Â 00C2 194	Ă 0102 195	Ä 00C4 196	Ĺ 0139 197	Ć 0106 198	Ç 00C7 199	Č 010C 200	É 00C9 201	Ę 0118 202	Ë 00CB 203	Ě 011A 204	Í 00CD 205	Î 00CE 206	Ď 010E 207
D–	Đ 0110 208	Ń 0143 209	Ň 0147 210	Ó 00D3 211	Ô 00D4 212	Ő 0150 213	Ö 00D6 214	× 00D7 215	Ř 0158 216	Ů 016E 217	Ú 00DA 218	Ű 0170 219	Ü 00DC 220	Ý 00DD 221	Ţ 0162 222	ß 00DF 223
E–	ŕ 0155 224	á 00E1 225	â 00E2 226	ă 0103 227	ä 00E4 228	ĺ 013A 229	ć 0107 230	ç 00E7 231	č 010D 232	é 00E9 233	ę 0119 234	ë 00EB 235	ě 011B 236	í 00ED 237	î 00EE 238	ď 010F 239
F–	đ 0111 240	ń 0144 241	ň 0148 242	ó 00F3 243	ô 00F4 244	ő 0151 245	ö 00F6 246	÷ 00F7 247	ř 0159 248	ů 016F 249	ú 00FA 250	ű 0171 251	ü 00FC 252	ý 00FD 253	ţ 0163 254	˙ 02D9 255

MINIMUM RINGER VOLUME

To prevent the user from turning off the ringer, an Administrator can configure a parameter called “**ringer volume minimum**” to set the minimum ringer volume level. When the minimum ringer level is reached while the user keeps pressing the button, the level of sound does not change.

Note: This minimum ringer volume does not affect the “silent” ring tone. When the silent ring tone is selected, no ringing will be played by the phone

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "Minimum Ringer Volume" on page A-237.

LOCKING IP PHONE KEYS

The IP phones allow you to lock or unlock programmable keys, softkeys, keypad keys, hard keys, and expansion keys (for expansion modules). When key locking is enabled, the phone locks the key with the provisioned local settings and prevents users from changing or configuring the key. In this case, the local settings (i.e. those configured through the Web UI) take precedence over any key parameters defined in the configuration files.

Notes:

1. If no settings are configured locally but the key type is defined in a configuration file, the phone will lock the respective key with the type defined in the configuration file along with any values associated with the additional key parameters (e.g. for softkeys, "softkeyN label", "softkeyN value", "softkeyN line", "softkeyN states").
2. Administrators also have the option of simply adding an exclamation mark (i.e. "!") in front of the respective key parameters to lock the keys to the values defined in the configuration files, overriding any locally configured settings (see "Locking Parameters in the Configuration File," on page 20 for further details)

You can lock and unlock keys using the configuration files only. When viewing the locked key via the Mitel Web UI, the key is grayed out (disabled) and cannot be changed. Locking is dynamic for XML pushes.

You use the following "locking" parameters in the configuration files to lock the softkeys and/or programmable keys on all the phones. If no key settings are configured locally, the locking parameters impact existing softkey and programmable key parameters defined in the configuration files as detailed in the table below.

LOCKING PARAMETER	IMPACTED PARAMETERS	APPLICABLE PHONE MODELS
softkeyN locked	softkeyN type softkeyN label softkeyN value softkeyN line softkeyN states	6867i 6869i 6873i 6920 6930 6940 6970
topsoftkeyN locked	topsoftkeyN type topsoftkeyN label topsoftkeyN value topsoftkeyN line	6867i 6869i 6873i 6920 6930 6940 6970

LOCKING PARAMETER	IMPACTED PARAMETERS	APPLICABLE PHONE MODELS
prgkeyN locked	prgkeyN type prgkeyN value prgkeyN line	6863i 6865i 6905 6910
pnhkeypadN locked	pnhkeypadN value pnhkeypadN line	All IP phone models
expmodX keyN locked	expmodX keyN type expmodX keyN label (M685i and M695 only) expmodX keyN value expmodX keyN line	6865i 6867i 6869i 6873i 6910 6920 6930 6940
hardkeyN locked	hardkeyN type hardkeyN value hardkeyN line	6863i 6865i 6867i 6869i 6873i 6905 6910 6920 6930 6940

Note: The 6863i and 6865i IP phones prevent users from setting a Speeddial key via the Phone UI on a key that has been locked.

LOCKING THE IP PHONE KEYS USING THE CONFIGURATION FILES

Use the following procedures to lock the softkeys and programmable keys on the IP phone.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section,"Locking Keys" on page A-288.

LOCKING/UNLOCKING THE SAVE AND DELETE KEYS

Note: Applicable to the 6865i IP Phone only.

By default, the 6865i has two keys dedicated to the **Save** and **Delete** functions. These two keys can be made programmable by the Administrator, freeing up the total number of programmable keys if required.

If a System Administrator unlocks the **Save** and **Delete** keys, these keys can be configured with the same functions that are available for the other programmable keys. Only the System Administrator can unlock these keys.

The **Save** key allows you to save entries to the Local Directory and perform a Save-To from the Received Callers List. It also allows you to save speeddial information to a programmable key. You can also use the **Save** key while using specific XML applications.

The **Delete** key allows you to remove entries from the Local Directory List and Received Callers List. (Must enter the Directory or Received Callers List and select an entry, then press twice to delete entry).

By default, the **Save** and **Delete** keys are locked so that a user can use them for saving and deleting only. An Administrator can unlock these keys using the configuration files, allowing the keys to be programmed with other functions if required. An Administrator can use the following parameters in the configuration file to lock and unlock the **Save** and **Delete** keys for the 6865i:

- prgkey5 locked
- prgkey6 locked

The value of "**0**" unlocks the keys, and the value of "**1**" locks the keys. The default is "1" (lock).

The following is an example of unlocking the **Save** and **Delete** keys on the 6865i using the configuration files:

Example:

```
prgkey5 locked: 0
prgkey6 locked: 0
```

Once the **Save** and **Delete** keys are unlocked, a User can change the function of the keys using the Mitel Web UI. An Administrator can change the function of the keys using the Mitel Web UI or the configuration files.

LOCKING AND UNLOCKING THE SAVE AND DELETE KEYS USING THE CONFIGURATION FILES

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "Locking the SAVE and DELETE Keys" on page A-291.

LOCAL DIAL PLAN

A dial plan describes the number and pattern of digits that a user dials to reach a particular telephone number. Access codes, area codes, specialized codes, and combinations of the number of digits dialed are all part of a dial plan. For instance, the North American Public Switched Telephone Network (PSTN) uses a 10-digit dial plan that includes a 3-digit area code and a 7-digit telephone number. Most PBXs support variable length dial plans that use 3 to 11 digits. Dial plans must comply with the telephone networks to which they connect. Only totally private voice networks that are not linked to the PSTN or to other PBXs can use any dial plan.

The Dial Plan field accepts up to 512 characters. If a user enters a dial plan longer than 512 characters, or a parsing error occurs, the phone uses the default dial plan of "**x+#|xx+*".** You configure the SIP Local Dial Plan using the Mitel Web UI or the configuration files.

Available symbols that can be used in the local dial plan are as follows:

SYMBOL	DESCRIPTION
0, 1, 2, 3, 4, 5, 6, 7, 8, 9	Digit symbol
X	Match any digit symbol (wildcard)
*, #, .	Other keypad symbol
|	Expression inclusive OR
+	0 or more of the preceding digit symbol or [] expression The dial plan must not end with +. The dial plan must be suffixed with "#", if the sip dial plan terminator is disabled or it must be suffixed with "^", if the sip dial plan terminator is enabled.
[]	Symbol inclusive OR
-	Used only with [], represent a range of acceptable symbols; For example, [2-8]
;	Used when a secondary dial tone is required on the phone. (For example, "9;xxxxxx", when a user has to dial "9" to get and outside line and needs a secondary dial tone presented

Dial Plan Example

An example of a SIP Local Dial Plan is:

```
[01]XXX|[2-8]XXXX|91XXXXXX
XXXX|X+.|*XX
```

The dial plan in the above example can accept any 4-digit dial strings that begin with a '0' or '1', any 5-digit dial strings that begin with a '2' up to '8', any 12-digit dial strings that begin with '91', any non-empty digit string that ends with a '.' or any 2-digit code that begins with a '*'.

LOCAL DIAL PLAN AND PATTERN MATCHING

The IP Phones support local dial plan dialing using pattern matching (i.e. once a user enters a set of numbers that matches a pattern defined in the local dial plan, the phone will automatically dial out the number without the user having to press the Dial softkey).

Note: Local dial plan pattern matching is only functional when the live dialpad feature is enabled. For more information on the live dialpad feature, see "Live Dialpad" on page 5-58.

With Live Dialpad enabled, if a Speeddial key is used to dial out, the number dials automatically but the whole defined number string is examined against the local dial plan.

If the whole string does not match a pattern defined in the local dial plan at all, the number will not be dialed out. If the whole string matches partially with a pattern defined in the local dial plan but has less numbers the number will not be dialed out. If the whole string matches partially with a pattern defined in the local dial plan, but has more numbers, the full string is dialed out.

For example, if the local dial plan is defined as 4xxx and a pre-dial or speeddial key number is 5000, the call will not dial out. If a pre-dial or speeddial key number is 412, the call will not dial out. If a pre-dial or speeddial key number is 4123, the call will be dialed out as 4123. If a pre-dial or speeddial key number is 41234, the call will be dialed out as 41234.

Notes:

1. If the phone is locked, dialed numbers are matched against the emergency dial plan.
2. The default local dial plan is configured to allow for all emergency numbers to be dialed out when the phone is unlocked. If you change the local dial plan, ensure it is configured to take into consideration any emergency services numbers for your country. Otherwise, calls to emergency services while the phone is unlocked may be blocked. For more information on configuring an emergency dial plan, see "Emergency Dial Plan" on page 5-15.

LOCAL DIAL PLAN AND PREFIX DIALING

The IP phones also support a prefix dialing feature for outgoing calls. If the dialed number matches against the local dial plan, the phone automatically maps the pre-configured prepended digit in the configuration to the beginning of the dialed number. You can enable this feature by adding prepend digits to the end of the local dial plan parameter string separated by a comma in the configuration files or the Mitel Web UI at Basic Settings > Preferences > General > Local Dial Plan.

Notes:

1. The prepend digits are also added if the dialing times-out on a partial match.
2. Patterns/numbers in the dial plan with prepend digits defined take priority over those that do not have prepend digits defined.

For example, if you add a prepend map of "[2-9]XXXXXXXXX,91", the IP phone adds the digits "91" to any 10-digit number beginning with any digit from 2 to 9 that is dialed out. Other examples of prepend mappings are:

- **1X+#,9** (Prepends "9" to any digit string beginning with "1" and terminated with "#".)
- **6XXX,579** (Prepends "579" to any 4-digit string starting with "6".)

- **[4-6]XXXXXX,78** (Prepends "78" to any 7-digit string starting with "4", "5", or "6".)

Example:

If you enter the following dial string for a local dial plan:

```
sip dial plan: 1+#,9
```

where "9" is the prepended digit, and you dial the following number:

```
15551212
```

the IP phone automatically adds the "**9**" digit to the beginning of the dialed number before the number is forwarded as **915551212**.

Note: You can configure a local dial plan via the configuration files or the Mitel Web UI.

SIP DIAL PLAN TERMINATOR

The IP phone provides a feature that allows an administrator to configure whether or not pressing the hash/pound (i.e. "#") key, while performing an outgoing call on an open line, should be sent as %23 to the proxy in the dial string or if the key should be used as a dial plan terminator (i.e. dials out the call immediately). By default, the hash/pound key is configured as a dial plan terminator; however, an administrator can change the behavior using the Mitel Web UI or the configuration files.

Behavior of phones to handle # character in SIP messages:

- If # is included at the beginning or in-between a dialed number, the invite is sent to the number with %23 replacing # in the dialed number.
  For example, if you dial 50#13 or #5013, the SIP message invite is sent to 50%2313 or %235013 respectively.
- If # is included as the last digit of a dialed number, the invite is sent without %23. In this case, # is considered as the terminator of the dialed number.
  For example, if you dial 5013#, the SIP message invite is sent to 5013.

DIGIT TIMEOUT

The IP phone allows you to configure a "**Digit Timeout**" feature on the IP phone. The Digit Timeout is the time, in seconds, between consecutive key presses on the IP phone's keypad. The default for this parameter is 4 seconds. If you press a key on the phone and wait 4 seconds before pressing the next key, the key times out and cancels the digit selection. You must press consecutive keys before the timeout occurs.

SECONDARY DIAL TONE

The IP phones support a feature that allows the user to dial a predefined dial string, obtain a dial tone, and continue dialing. A User or Administrator can configure this using the existing Dial Plan feature on the phone.

You can enter a new character string in the dial plan that allows you to configure the secondary dial tone. The character string is of the form "**.;.**" , where the period indicates an arbitrary number of digits and the semicolon indicates that the phone is to present a dial tone after the previous dialed digit. For example, in the string:

```
"9;xxxxx"
```

the user dials "**9**" to get the outside line, listens for the dial tone, and continues to dial the applicable number. The "**;**" tells the phone to present a second dial tone after the previously dialed digit. "The "xxxxx" in the example tells the phone that a phone number is dialed after the secondary dial tone is audible.

You can enter the Secondary Dial Tone string in the Dial Plan using the configuration files or the Mitel Web UI.

You use the following parameter in the configuration files to configure a secondary dial tone:

- sip dial plan

Example:

```
sip dial plan: "9;5551313"
```

CONFIGURING THE SIP LOCAL DIAL PLAN, DIAL PLAN TERMINATOR, AND DIGIT TIMEOUT

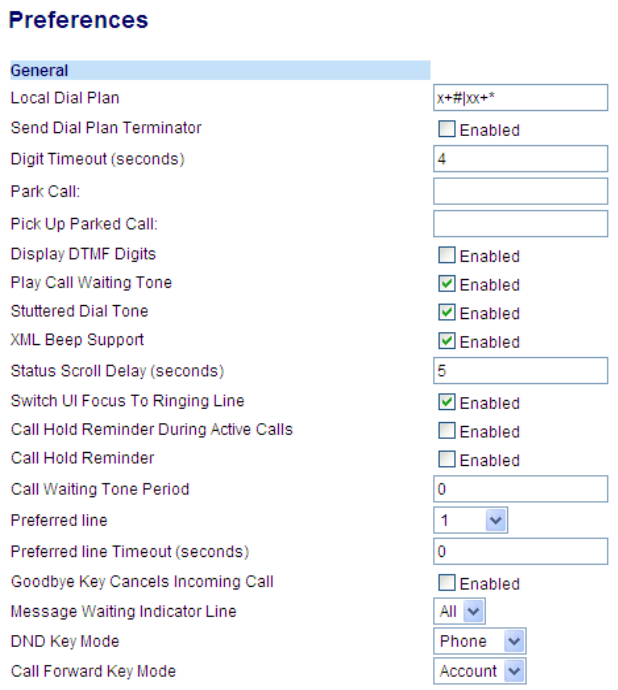
Use the following procedures to configure the SIP Local Dial Plan using the configuration files or the Mitel Web UI.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "SIP Local Dial Plan Settings" on page A-85.

MITEL WEB UI

1. Click on **Basic Settings-> Preferences->General.**



2. In the "**Local Dial Plan**" field, enter a valid local dial plan (up to 512 alphanumeric characters) for the IP phone. Default is X+#|XX+*. Enter prepended digits or a “;”to present a secondary dial tone if required.

Note: If a User enters a dial plan longer than 512 characters, or a parsing error occurs, the phone uses the default dial plan of “x+#|xx+*”.

3. Enable the "**Send Dial Plan Terminator**" field by checking the check box. (Disable this field by unchecking the box). Default is disabled.

4. In the "**Digit Timeout (in seconds)**" field, enter a timeout value. This is the length of time, in seconds, he phone waits before dialing. Default is 4 seconds.

5. Click **Save Settings** to save your changes.

E.164 SUPPORT

E.164 is the international telephone numbering plan that ensures each device on the PSTN has a globally unique number. E.164 numbers are formatted as [+] [country code] [subscriber number including area code], and can have a maximum of 15 digits.

The support from the phone side is that users should be able to dial numbers with the leading '+' symbol.

Users can dial E.164 numbers from 6800 and 6900 series IP phones. The support for inserting the '+' symbol is provided to users in the following ways:

- When dialing from the phone, users can insert the '+' symbol by a long-press of the '0' key.

- When entering an E.164 number as a number entry in the directory from the phone UI, users can insert the '+' symbol by a long-press of the '0' key.
- When entering an E.164 number as a number entry in the keypad Speed dial from the phone UI, users can insert the '+' symbol by a long-press of the '0' key .
- On 6940 and 6873i IP phones:
  - Users can insert the '+' symbol by a long-press of the '0' key.
  - While using the virtual keyboard, users can long-press the '=' symbol for the '+' symbol to pop up, which they can select.

SUPPRESSING DTMF PLAYBACK

A feature on the IP phones allows administrators to enable or disable the suppression of DTMF playback when a number is dialed from the softkeys and programmable keys.

When suppression of DTMF playback is disabled, and you press a softkey or programmable key, the IP phone dials the stored number and displays each digit as dialed in the LCD window.

When the suppression of DTMF playback is enabled, the IP phone dials the stored number and displays the entire number immediately in the LCD window, allowing the call to be dialed much faster.

DTMF playback suppression is enabled by default. The “**suppress dtmf playback**” parameter can be configured using the configuration files.

CONFIGURING SUPPRESSION OF DTMF PLAYBACK

Use the following procedures to configure the suppression of DTMF playback on the IP phone.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Suppress DTMF Playback Setting” on page A-228.

DISPLAY DTMF DIGITS

A feature on the IP phones allows administrators to enable or disable DTMF (dual-tone multi-frequency) digits to display to the IP phone when using the keypad to dial, or when dialing from a softkey or programmable key.

DTMF is the signal sent from the phone to the network that you generate when you press the phone’s touch keys. This is also known as “touchtone” dialing. Each key you press on your phone generates two tones of specific frequencies. One tone is generated from a high-frequency group of tones and the other from a low frequency group.

If you enable the Display DTMF Digits parameter, the digits you are dialing from the keypad or from a softkey or programmable key display to the IP phone’s LCD display. This parameter is disabled by default (no digits display when dialing).

You can enable the “**display dtmf digits**” parameter using the configuration files or the Mitel Web UI.

CONFIGURING DISPLAY DTMF DIGITS

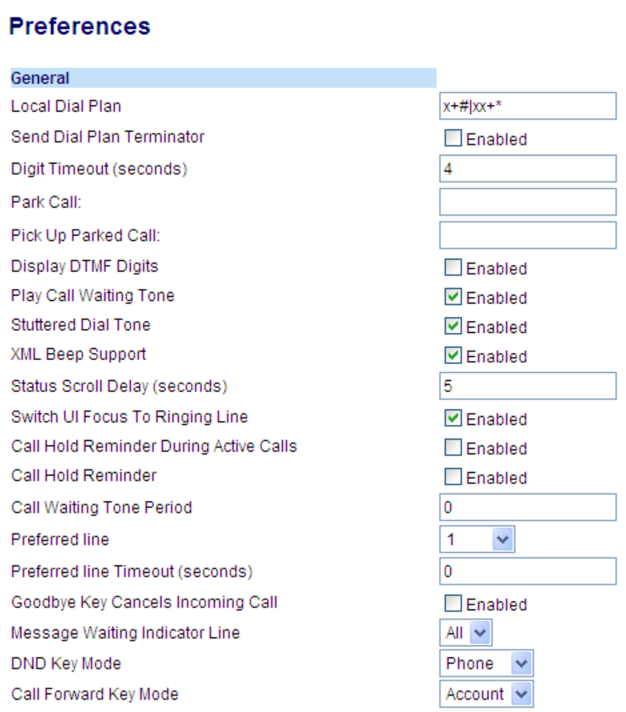
Use the following procedures to configure the display DTMF digits option on the IP phone.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Display DTMF Digits Setting” on page A-228.

MITEL WEB UI

1. Click on **Basic Settings-> Preferences->General.**



2. Enable the "**Display DTMF Digits**" field by checking the check box. (Disable this field by unchecking the box). Default is disabled.
3. Click **Save Settings** to save your changes.
4. You must restart your IP phone for the changes to take effect.
5. Click on **Operation->Reset**.
6. In the “**Restart Phone**” field click **Restart** to restart the IP phone and apply the changes.

FILTER OUT INCOMING DTMF EVENTS

An Administrator can enter a parameter in the configuration files to suppress incoming DTMF playback. This new parameter called "**suppress incoming dtmf playback**" will suppress the playback of both SIP INFO and RFC2833 incoming DTMF tones. The locally generated DTMF tones will still be played.

CONFIGURING SUPPRESS INCOMING DTMF PLAYBACK

Use the following procedures to suppress incoming DTMF playback on the IP phone.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Filter Out Incoming DTMF Events" on page A-229.

CALL WAITING

The call waiting feature notifies a user on an active call on the phone, of a new incoming call. You can disable this call waiting feature, so that the new incoming call is automatically rejected by the phone with a busy message. A User or Administrator can configure this feature.

If you disable call waiting on the phone, and the user is on a call, any further incoming calls will receive busy unless "Call Forward Busy" or "Call Forward No Answer and Busy" is configured on the phone. It will then forward the call according to the rule configured. The phone can only:

- transfer the currently active call

  or

- accept transferred calls if there is no active calls.

If call waiting is disabled:

- intercom calls are treated as regular incoming calls and are rejected.
- pre-dialing with live dialpad disabled still accepts incoming calls.
- the Missed Calls List does not get updated with details of calls.
- the Blind Transfer feature on the phone may not work if two calls are made to the phone at one time.

You can enable/disable call waiting on a global or per-line basis using the configuration files or the Mitel Web UI.

CONFIGURING CALL WAITING

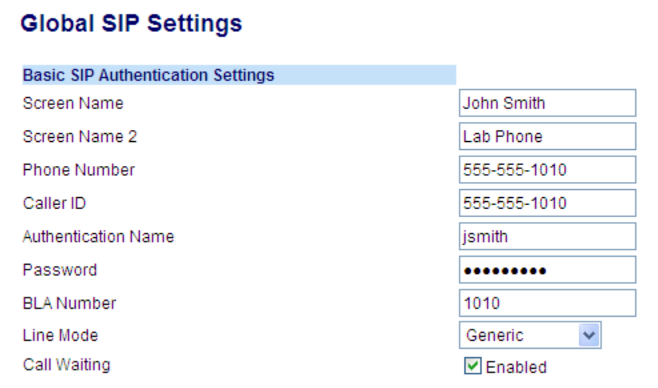
Use the following procedures to configure the Call Waiting feature on the IP phone.

CONFIGURATION FILES

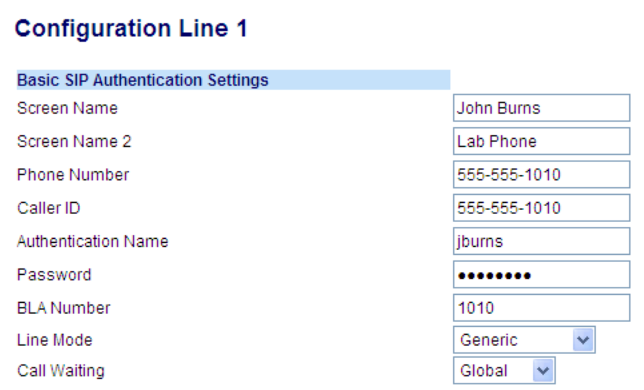
For specific parameters you can set in the configuration files, see Appendix A, the section, "Call Waiting Settings" on page A-92 or "SIP Per-Line Call Waiting Setting" on page A-103.

MITEL WEB UI

1. For global configuration, click on **Advanced Settings->Global SIP->Basic SIP Authentication Settings.**



2. Or, for per-line configuration, click on **Advanced Settings->Line *N* ->Basic SIP Authentication Settings**.



Configure Global Call Waiting

3. The "**Call Waiting**" field is enabled by default. To disable call waiting on a global basis, uncheck this box.

Configure Per-Line Call Waiting

4. The "**Call Waiting**" field is set to "**Global**" by default. To enable call waiting for a specific line, select "**enabled**" from the list in this field. To disable call waiting for a specific line, select "**disabled**" from the list in this field.

5. Click **Save Settings** to save your changes.

CALL WAITING TONE

You can also enable or disable the playing of a short "call waiting tone" when there is an incoming call on your phone using the "**play call waiting tone**" parameter. This feature is enabled by default. If you have Call Waiting enabled, and a call comes into the line for which you are on an active call, a tone is audible to notify you of that incoming call.

Note: The Call Waiting Tone feature works only if Call Waiting is enabled.

A User or Administrator can configure this feature using the Mitel Web UI. An Administrator can also configure this feature using the configuration files.

Configuring Call Waiting Tone

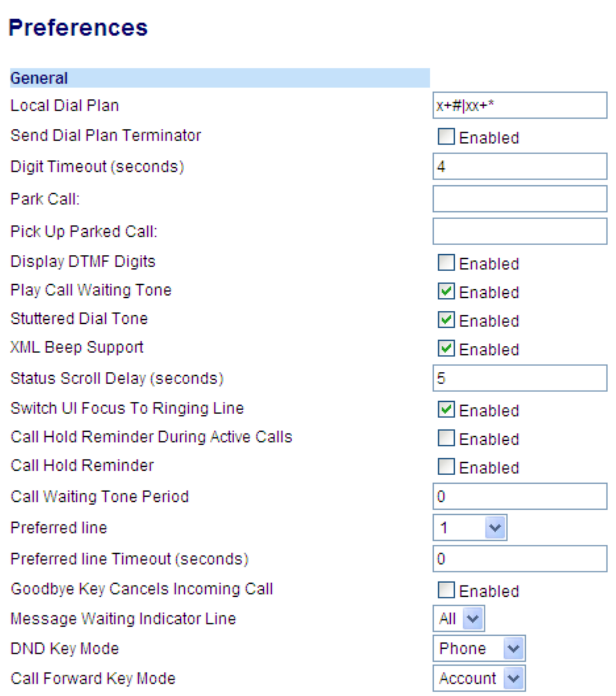
Use the following procedures to configure the Call Waiting Tone feature on the IP phone.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Call Waiting Settings" on page A-92.

MITEL WEB UI

1. Click on **Basic Settings-> Preferences->General.**



2. The "**Play Call Waiting Tone**" field is enabled by default. To disable this field, uncheck the box. This feature allows you to enable or disable the call waiting tone on the IP phone.

> **Note:** The Call Waiting Tone feature works only if the "**Call Waiting**" tone field is enabled at the location *Advanced Settings->Global SIP (or Line X)->Basic SIP Authentication Settings*.

3. Click **Save Settings** to save your changes.

CALL WAITING TONE PERIOD

A User or Administrator can specify a specific time period (in seconds) for the call waiting tone to play at regular intervals on an active call using the parameter "**call waiting tone period**". A value of "0" is the default and plays the call waiting tone only once on the active call. When the incoming caller hangs up, the call waiting tone stops on the existing active call.

You can enable or disable this feature in the configuration files or in the Mitel Web UI.

Configuring "Call Waiting Tone Period"

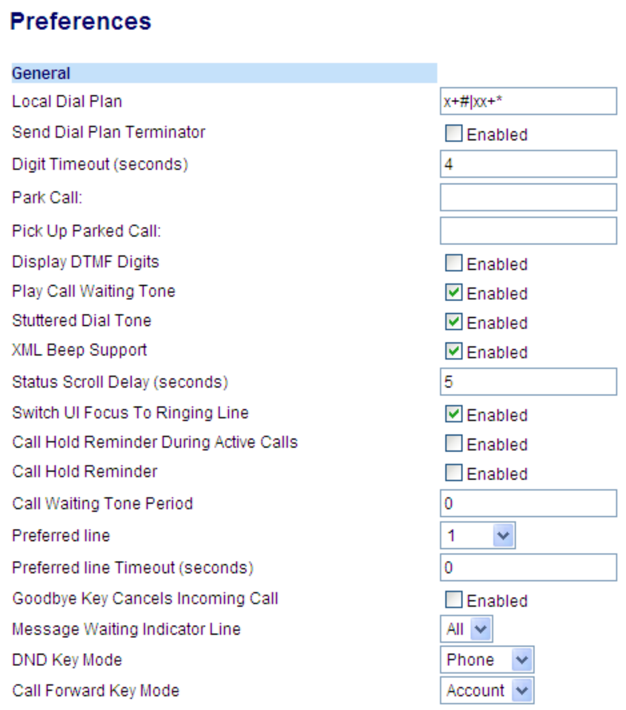
You use the following procedures to enable or disable "Call Waiting Tone Period".

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Call Waiting Settings" on page A-92.

MITEL WEB UI

1. Click on **Basic Settings->Preferences->General**.



2. In the "**Call Waiting Tone Period**" field, enter a time period, in seconds, that the call waiting tone will be audible on an active call when another call comes in. Default is 0 seconds. When enabled, the call waiting tone plays at regular intervals for the amount of time set for this parameter. For example, if set to “30” the call waiting tone plays every 30 seconds. When set to “0”, the call waiting tone is audible only once on the active call

3. Click **Save Settings** to save your changes.

MUTE DTMF PLAYBACK

A feature on the IP phones allows administrators to enable or disable the mute of local DTMF playback tone when the phone is in **Dialing** or **Offhook** state.

- If the administrator has disabled mute DTMF playback: When the phone is **Offhook**, the IP phone plays the DTMF playback tone when any number key is pressed.
- If the administrator has enabled mute DTMF playback: When the phone is **Offhook**, the IP phone does not play the DTMF playback tone when any number key is pressed.

DTMF playback mute is enabled by configuring the “**mute dtmf playback: 1**” parameter in configuration files.

Configuring “Mute DTMF playback”

You use the following procedures to enable or disable “Mute DTMF Playback”.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Mute DTMF Playback Settings" on page A-92.

MEETINGS

The IP phones support the MiCollab Meetings Center application which is accessed via the **Meetings** softkey.

Note: When a **Meetings** softkey is provisioned, the user has access to the MiCollab Meetings Center application, which typically provides easy access to the user's scheduled conferences.

CONFIGURING MEETINGS

Use the following procedures to configure the **Meetings** softkey through the Mitel Web UI or by using the configuration file on the IP phones.

CONFIGURATION FILES

1. Open the configuration file applicable to the conference phone.
2. Using the Softkey parameter in the configuration file, put in the data on the **Meetings** softkey created. For example:

   ```
   softkey5 type: xml
   softkey5 label: Meeting
   softkey5 value:
   http://192.168.151.42/MiCollabMeeting/meetings/1414/$$LOCALIP$$
   ```

   Here you create bottom softkey No.5 of XML type. The softkey is labelled Meetings and links to the predefined meeting room 1414.
3. Save the changes in the file.
4. Download the configuration file into the phone for the change to become effective.

MITEL WEB UI

1. In your web browser, login to the Mitel Web UI by entering your username and password and click **OK**.
2. Select **Operation** > **Softkeys and XML** > **Softkey configuration.**
3. Depending on your intention for the Meeting softkey, select the **Bottom Keys** tab or the **Top Keys** tab.

4. Select from **Key 1** through **Key 48** on the Top keys.
   or
   Select from **Key 1** through **Key 30** on the Bottom keys.
5. In the **Type** column, select **XML** from the drop-down list.
6. In the **Label** column, type **Meetings**.
7. In the Value column, specify the link to the meeting room, where the conference phone is located. For example, http://192.168.151.42/MiCollabMeeting/meetings/1414/$$LOCALIP$$, where
   - 1414 is the user extension number for which the meetings are created
   - $$LOCALIP$$ is the reference to the locally installed conference phone.
8. (For the Bottom softkeys only) In the state fields, check (enable) or uncheck (disable) the states you want to apply to this softkey.
9. Click **Save Settings**.

STUTTERED DIAL TONE

You can enable or disable the playing of a stuttered dial tone when there is a message waiting on the IP phone.

You can configure this feature using the configuration files and the Mitel Web UI.

CONFIGURING STUTTERED DIAL TONE

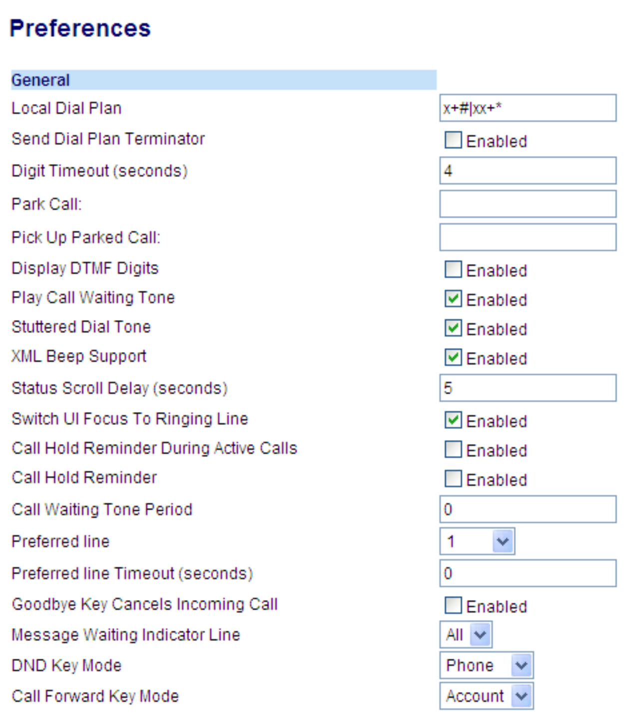
Use the following procedures to configure stuttered dial tone on the IP phones.

CONFIGURATION FILES

For specific parameters you can set in the configuration files for enabling/disabling stuttered dial tone, see Appendix A, the section, "Stuttered Dial Tone Setting" on page A-205.

MITEL WEB UI

1. Click on **Basic Settings->Preferences->General.**



2. The "**Stuttered Dial Tone**" field is enabled by default. To disable this field, uncheck the box.
3. Click **Save Settings** to save your changes.

XML BEEP SUPPORT

The IP phones have a feature that allows you to enable or disable a beep on the phone when it receives a status message from an XML application. This beep can be turned ON or OFF using the Mitel Web UI, the configuration files, or in an XML script. If you disable this feature, then no beep is heard when the XML application arrives to the phone.

If your System Administrator has set a value for this feature in a custom XML application or in the configuration files, the value you set in the Mitel Web UI overrides the Administrator's setting. Setting and saving the value in the Mitel Web UI applies to the phone immediately.

REFERENCE

For more information about enabling/disabling the XML Beep Support in an XML script, see "XML Customized Services" on page 5-316.

CONFIGURING XML BEEP SUPPORT

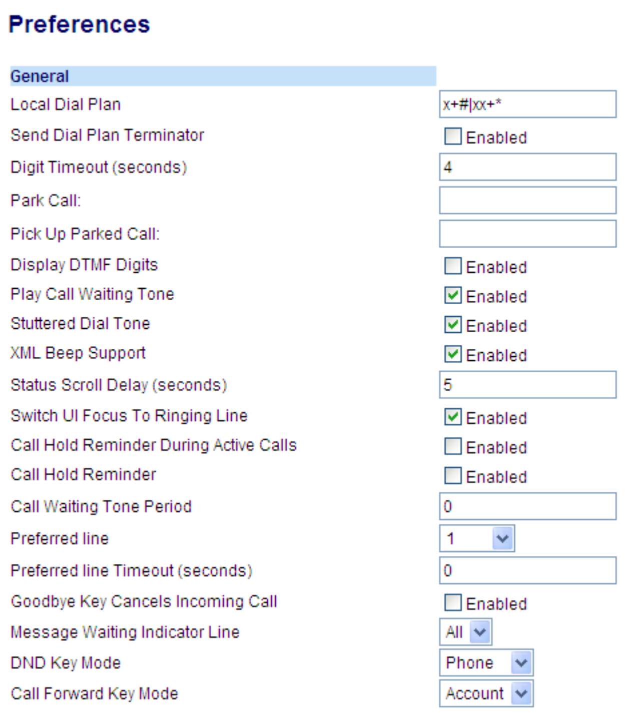
Use the following procedures to enable/disable XML Beep Support.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "XML Settings" on page A-186.

MITEL WEB UI

1. Click on **Basic Settings->Preferences->General.**



2. The “**XML Beep Support**” field is enabled by default. To disable this field, uncheck the box.
3. Click **Save Settings** to save your changes.

STATUS SCROLL DELAY

The IP phones have a feature that allows you to specify the time delay, in seconds, between the scrolling of each status message (including XML status messages) on the phone. The default time is 5 seconds for each message to display before scrolling to the next message. You can configure this option via the configuration files or the Mitel Web UI.

REFERENCE

For more information about configuring the status scroll delay for XML status messages, see "XML Customized Services" on page 5-316.

CONFIGURING STATUS SCROLL DELAY

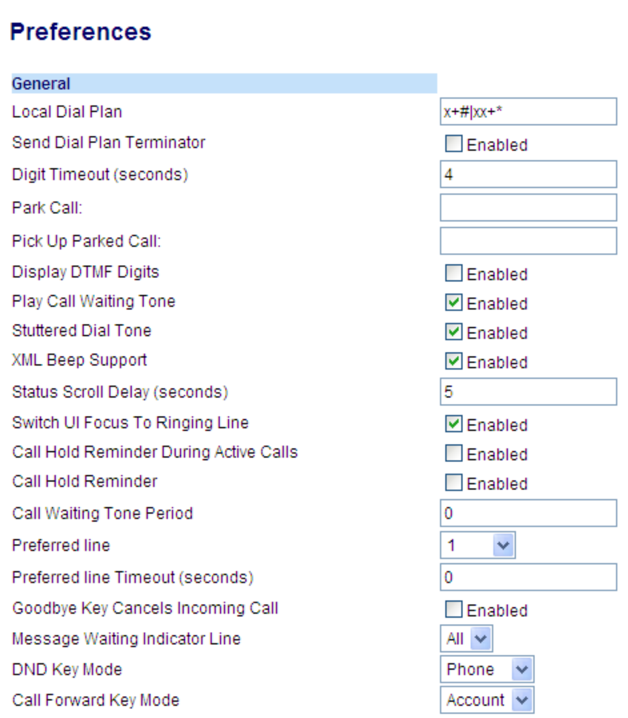
Use the following procedures to configure Status Scroll Delay.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "XML Settings" on page A-186.

MITEL WEB UI

1. Click on **Basic Settings->Preferences->General.**



2. In the "**Status Scroll Delay (seconds)**" field, enter a value, in seconds, that each XML status message displays on the phone. Default is 5 seconds. Valid values are 1 to 25.
3. Click **Save Settings** to save your changes.

SWITCH FOCUS TO RINGING LINE

An Administrator or User can control the behavior of the phone when it receives an incoming call when it is already in a connected call. By default, the phone switches focus to the ringing line to enable the user to see who is calling them.

You can turn off this functionality so that the phone now stays focused on the connected call. You can do this using the "**switch focus to ringing line**" parameter in the configuration files or the Mitel Web UI.

Note: If you configure the BLF/Xfer key(s) and/or Speeddial/Xfer key(s) on the phone, you can enable or disable the switching of the user interface focus to ringing line while the phone is in the connected state.

CONFIGURING "SWITCH FOCUS TO RINGING LINE"

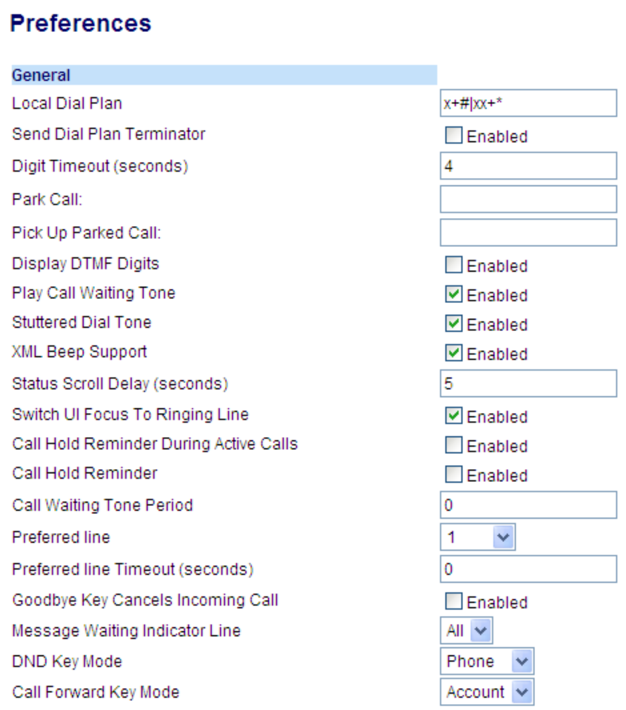
You use the following procedures to enable or disable "Switch Focus to Ringing Line".

CONFIGURATION FILES

For specific parameters you can set in the configuration files for enabling disabling "Switch Focus to Ringing Line", see Appendix A, the section, "Switch Focus to Ringing Line" on page A-200.

MITEL WEB UI

1. Click on **Basic Settings->Preferences->General.**



2. The "**Switch Focus to Ringing Line**" field is enabled by default. To disable this field, uncheck the box.

3. Click **Save Settings** to save your changes.

CALL HOLD REMINDER DURING ACTIVE CALLS

The IP phones allow a User or Administrator to enable or disable the ability for the phone to initiate a continuous reminder tone on the active call when another call is on hold. For example, when this feature is enabled, and the call on Line 1 is on hold, and then the User answers a call on Line 2 and stays on that line, a reminder tone is played in the active audio path on Line 2 to remind the User that there is still a call on hold on Line 1.

When this feature is disabled, a ring splash is heard when the active call hangs up and there is still a call on hold.

Your can enable or disable this feature using the "**call hold reminder during active calls**" parameter in the configuration files or in the Mitel Web UI.

Note: During an active Bluetooth mobile call, the call hold reminder tone will not be heard even if the Call Hold Reminder option is enabled on the phone.

CONFIGURING “CALL HOLD REMINDER DURING ACTIVE CALLS”

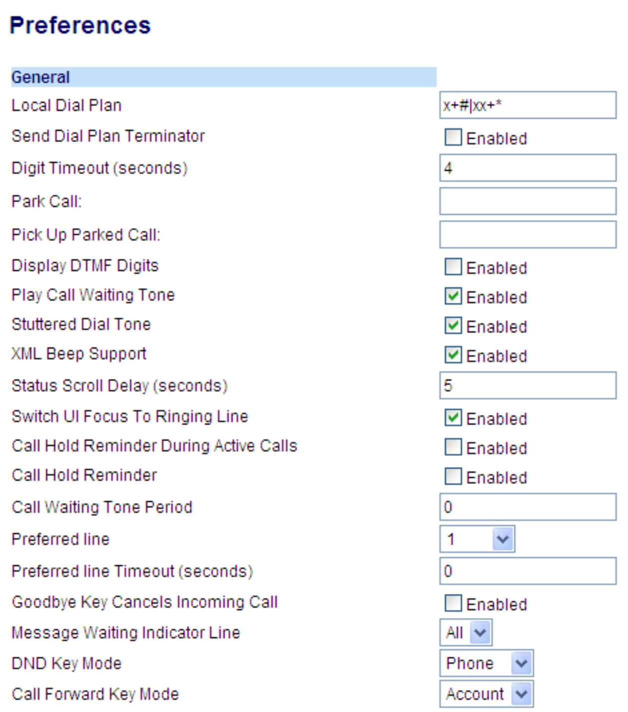
You use the following procedure to enable or disable “Call Hold Reminder During Active Calls”.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files for enabling/disabling “Call Hold Reminder During Active Calls”, see Appendix A, the section, “Call Hold Reminder Settings” on page A-201.

MITEL WEB UI

1. Click on **Basic Settings->Preferences->General.**



2. In the "**Call Hold Reminder During Active Calls**" field, enable this feature by placing a check mark in the box.
   When this feature is enabled, a reminder tone is heard on the active call when another call is on hold. When disabled, a ring splash is heard when the active call hangs up and there is still a call on hold.

3. Click **Save Settings** to save your changes.

CALL HOLD REMINDER (ON SINGLE HOLD)

In previous releases, the call hold reminder ring splash was triggered when you hung up a call and there was at least one other call on hold. The reminder ring splash timer started only when the active call hung up and there was still another call on hold.

On the IP phones, a User or Administrator can enable or disable a feature that would start the reminder ring splash timer as soon as you put a call on hold (even when no other calls are active on the phone). When enabled, the phone initiates a reminder ring splash periodically for the single call on hold. When disabled, no reminder ring splash is audible.

You can enable or disable this feature using the "**call hold reminder**" parameter in the configuration files or in the Mitel Web UI.

CONFIGURING "CALL HOLD REMINDER"

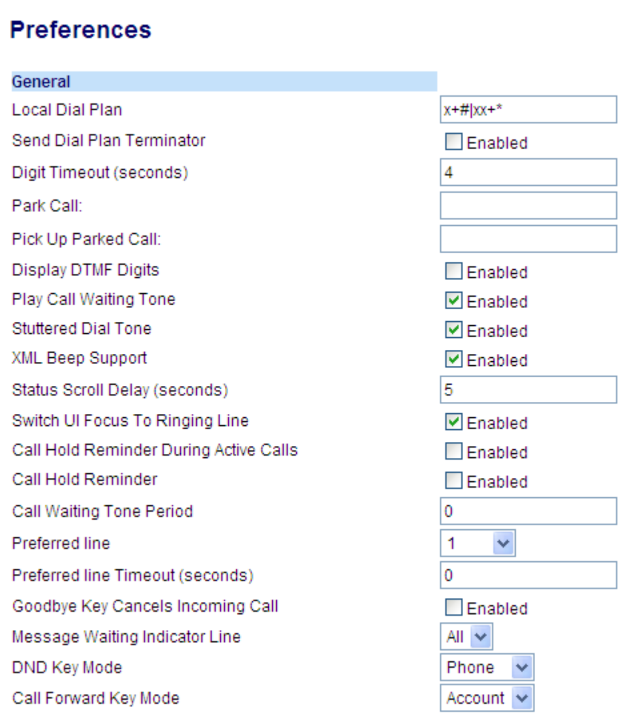
You use the following procedure to enable or disable "Call Hold Reminder".

CONFIGURATION FILES

For the specific parameter you can set in the configuration files for enabling/disabling "Call Hold Reminder", see Appendix A, the section, "Call Hold Reminder Settings" on page A-201.

MITEL WEB UI

1. Click on **Basic Settings->Preferences->General.**



2. The "**Call Hold Reminder**" field is disabled by default. To enable this feature, place a check mark in the box.
   When this feature is enabled, the reminder ring splash timer starts as soon as you put a call on hold (even when no other calls are active on the phone).The phone initiates a reminder ring splash periodically for the single call on hold. When disabled, no reminder ring splash is audible.
3. Click **Save Settings** to save your changes.

CALL HOLD REMINDER TIMER & FREQUENCY

There are two parameters an Administrator can set on the IP Phones along with the "**call hold reminder**" and "**call hold reminder during active calls**" parameters:

- call hold reminder timer
- call hold reminder frequency

These parameters specify the time delay and time frequency of the ring splash that sounds when you are on an active call and have placed another call on hold. You can configure these parameters using the configuration files only.

Notes:

1. You must enable the "**call hold reminder**" and/or "**call hold reminder during active calls**" parameter(s) for the above parameters to work.
2. A value of "**0**" for the "**call hold reminder timer**" parameter disables the call hold reminder feature.
3. A value of "**0**" for the "**call hold reminder frequency**" parameter prevents additional rings.

CONFIGURING "CALL HOLD REMINDER TIMER"

You use the following procedure to configure the "Call Hold Reminder Timer".

CONFIGURATION FILES

For the specific parameter you can set in the configuration files for setting the "Call Hold Reminder Timer", see Appendix A, the section, "Call Hold Reminder Settings" on page A-201.

CONFIGURING "CALL HOLD REMINDER FREQUENCY"

You use the following procedure to configure the "Call Hold Reminder Frequency".

CONFIGURATION FILES

For the specific parameter you can set in the configuration files for setting the "Call Hold Reminder Frequency", see Appendix A, the section, "Call Hold Reminder Settings" on page A-201.

PREFERRED LINE AND PREFERRED LINE TIMEOUT

An Administrator or User can define a **preferred line** as well as a **preferred timeout**. If a preferred line is selected, after a call ends (incoming or outgoing), the display switches back to the preferred line. Next time you go off-hook, you pickup on the preferred line. You can specify the number of seconds it takes for the phone to switch back to the preferred line using the "**preferred timeout**" parameter.

An Administrator can configure the "**preferred line**" and the "**preferred timeout**" parameters using the configuration files or the Mitel Web UI. A User can configure these parameters using the Mitel Web UI only.

The following table provides the behavior of the preferred line focus feature with other features on the phone.

PHONE FEATURE	PREFERRED LINE BEHAVIOR
Call Return	The phone switches back to the focused line immediately after the call ends.
Speeddial	The line is already specified when the speeddial is created. The phone switches back immediately after the call ends.
Conference	For incoming calls, the phone switches back immediately after the call ends.
Transfer	For incoming or outgoing calls, the current behavior is that the same line used to transfer the call does not change. For incoming calls, the phone switches back immediately after the call transfers.
BLF	The phone switches back immediately after the call ends.
Park	The phone switches back immediately after the call ends.
Voicemail	The phone switches back immediately after the call ends.
Redial	The phone switches back immediately after the call ends.
Dialing	For incomplete dialing on a non-preferred line, the focus does not change if some digits are entered. If no digits are entered or digits were cleared, the focus changes to preferred line after the time out has passed without activities.
Caller ID	If the "Switch UI Focus To Ringing Line" parameter is disabled, the User is able to see the Caller ID when the phone switches the focus to the ringing line.
Factory Default	Factory default and recovery mode clears the "preferred line" and "preferred line timeout" parameters, and the phone operates in a non-preferred line mode.

Notes:

1. If you specify a value of "**0**" for the **preferred line** parameter, it disables the preferred line focus feature.
2. If you specify a value of "**0**" for the **preferred line timeout** parameter, the phone returns the line to the preferred line immediately.

CONFIGURING THE PREFERRED LINE AND PREFERRED LINE TIMEOUT

You use the following procedures to configure the Preferred Line and the Preferred Line Timeout on the IP Phones.

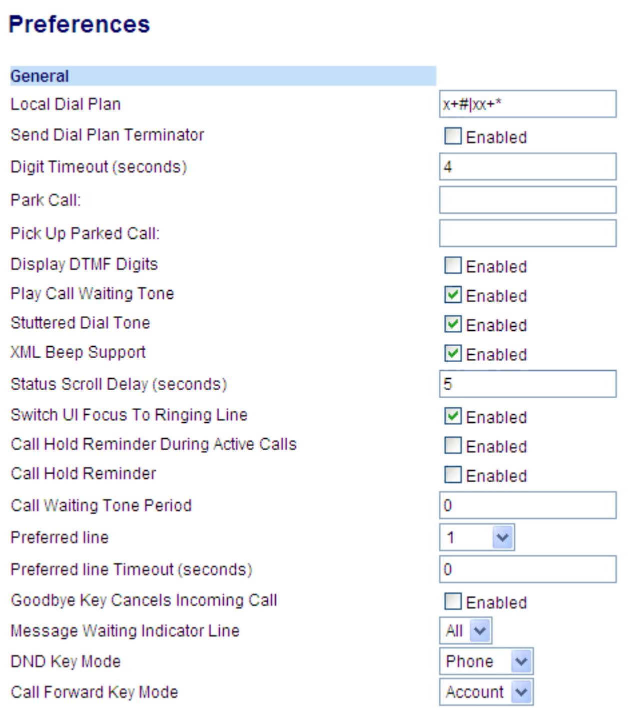
CONFIGURATION FILES

For specific parameters you can set in the configuration files for configuring the Preferred Line and Preferred Line Timeout, see Appendix A, the section, "Preferred Line and Preferred Line Timeout" on page A-203.

Use the following parameters to configure preferred line focus using the Mitel Web UI.

MITEL WEB UI

1. Click on **Basic Settings->Preferences->General.**



2. In the "**Preferred Line**" field, select a preferred line to switch focus to after incoming or outgoing calls end on the phone. Valid values are:
   - None (disables the preferred line focus feature)
   - 1 to N

   Default is **1**.

   For example, if you set the preferred line to "**1**", when a call (incoming or outgoing) ends on the phone (on any line), the phone switches focus back to Line 1.

3. In the "**Preferred Line Timeout**" field, enter the amount of time, in seconds, that the phone switches back to the preferred line after a call (incoming or outgoing) ends on the phone, or after a duration of inactivity on an active line. Default is **0**. Valid values are 0 to 999.

4. Click **Save Settings** to save your changes.

GOODBYE KEY CANCELS INCOMING CALL

You can configure the Goodbye key to drop active calls or ignore incoming calls using the "**goodbye cancels incoming call**" parameter or through the Web UI. This parameter controls the behavior of the goodbye key when the phone is on an active call and a second call is presented to the phone.

HOW IT WORKS

When you enable this parameter (1 = enable in the configuration files), which is the default, the Goodbye key rejects the incoming call. When you disable this parameter (0 = disable in the configuration files), the Goodbye key hangs up the active call.

For the 6863i/6865i/6905/6910

If you disable this parameter, and the phone receives another call when an active call is already present, the "**Ignore**" option displays in the LCD window. The phone will ignore the incoming call if you press the ▼ arrow navigation key. The phone will hang up on the active call if you press the Goodbye key.

You can set this parameter using the configuration files or the Mitel Web UI.

CONFIGURING THE GOODBYE KEY TO CANCEL INCOMING CALLS

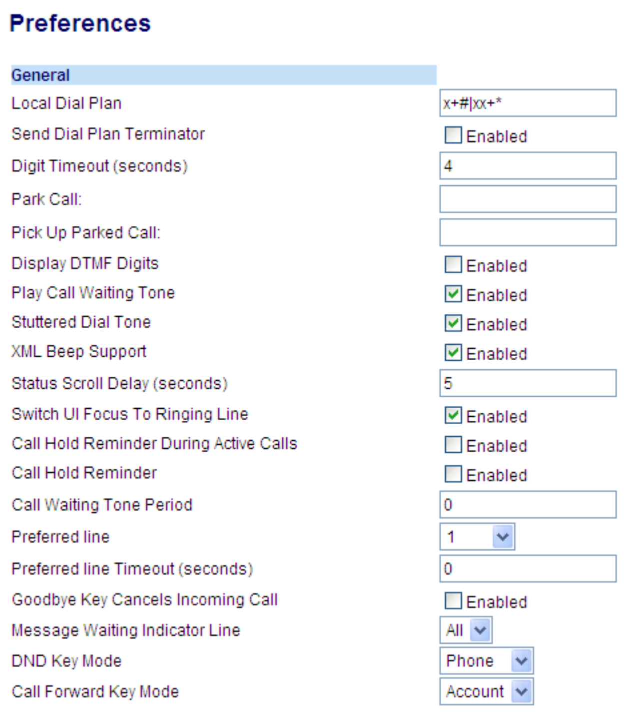
Use the following procedures to configure the behavior of the Goodbye Key on the IP phone.

CONFIGURATION FILES

For specific parameters you can set in the configuration files for enabling/disabling the behavior of the Goodbye Key, see Appendix A, the section, "Goodbye Key Cancels Incoming Call" on page A-204.

MITEL WEB UI

1. Click on **Basic Settings->Preferences->General.**



2. Enable or disable the "**Goodbye Key Cancels Incoming Call**" field by checking or un-checking the check box.

3. Click **Save Settings** to save your changes.

CONFIGURABLE STATUS CODE ON IGNORING INCOMING CALLS

Note: Valid status codes are based on RFC3261.

When a user presses the "**Ignore**" key on the phones during an incoming call, the phone rejects the incoming call with a status code of "486 Busy Here". The IP phones allow an administrator to configure this status code. You can configure the status code using the configuration files only.

Use the following parameter to configure a status code when ignoring incoming calls:

- sip ignore status code

Configuring Status Codes on Ignoring Incoming Calls

You can use the following procedure to set the status code sent in the response when a user presses the "Ignore" key.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "Status Code on Ignoring Incoming Calls" on page A-200.

GOODBYE KEY BEHAVIOR FOR BLUETOOTH MOBILE LINE

When a BT Mobile line is established with the SIP phone, the Goodbye key functions as follows based on the SIP line and Mobile line state –

- If the first SIP line has an active call and the second SIP line is ringing –
  - Pressing Goodbye key cancels the ringing line when "**Goodbye Key Cancels Incoming Call**" is enabled.
  - Pressing Goodbye key cancels the active call line when "**Goodbye Key Cancels Incoming Call**" is disabled.
- If the first line has an active BT Mobile call and the SIP line is ringing –
  - Pressing Goodbye key cancels the ringing line when "**Goodbye Key Cancels Incoming Call**" is enabled.
  - Pressing Goodbye key cancels the BT mobile line if audio is on the desk phone and cancels the ringing line if audio is on the mobile phone call when "**Goodbye Key Cancels Incoming Call**" is disabled.

MESSAGE WAITING INDICATOR LINE

A User or Administrator can configure the Message Waiting Indicator (MWI) to illuminate for a specific line or for all lines. For example, if you configure the MWI LED on line 2 only, the LED illuminates if a voicemail is pending on line 2. If you configure the MWI LED for all lines, the LED illuminates if a voicemail is pending on any line on the phone (lines 1 through N).

A User can configure the MWI using the Mitel Web UI only. An Administrator can configure the MWI on single or all lines using the configuration files or the Mitel Web UI.

LED BEHAVIOR IN FAILOVER SCENARIO

Previously, the red LED in the upper right corner of a 6800/6900 series phone was switched on when the phone was not registered in a failover scenario. The LED is on for approximately 0.5 seconds during a failover from the current to an alternative registrar.

An enhancement is made wherein the LED is switched off unless the registration to an alternative server fails.

If no backup or alternate server (through DNS SRV) is configured, phone will attempt to register to Registrar. If the registrar fails to respond, the phone will display "No Service" and lights up the MWI LED.

If the backup server or alternate server (through DNS SRV) is configured and the registration attempt to primary server fails (due to server maintenance etc), the phone attempts to register with the alternate server. Only if the alternate server registration attempt also fails, the phone displays “No Service” and lights up the MWI LED.

Note: In case of no response from the server, the phone will retry sending registration until the transaction timer expires, after which the phone displays “No Service” and lights up the MWI LED.

CONFIGURING MESSAGE WAITING INDICATOR (MWI)

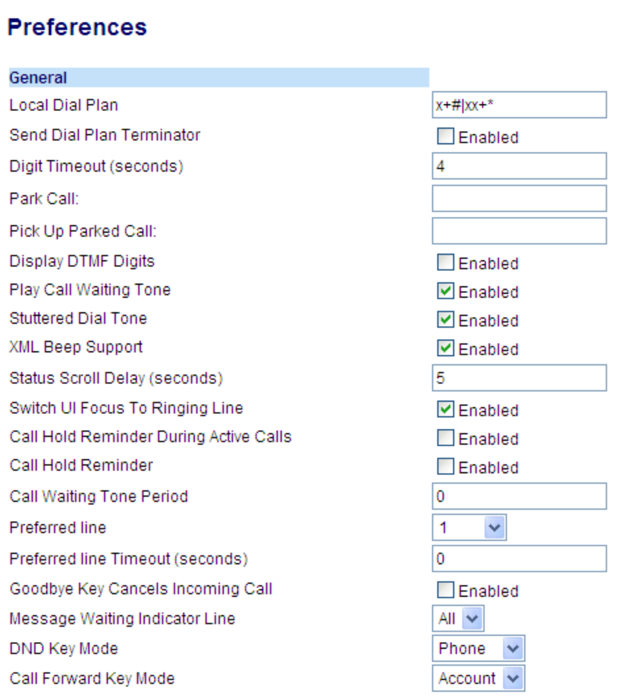
Use the following procedures to configure MWI on the IP phone.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Message Waiting Indicator Settings” on page A-205.

MITEL WEB UI

1. Click on **Basic Settings-> Preferences->General.**



2. In the “**Message Waiting Indicator Line**” field, select a single line from 1 to N, or select “All” for all lines. If you select a single line, the MWI illuminates when a voicemail message is pending on that line. If you select all lines, the MWI illuminates when a voicemail message is pending on any line from 1 to N.

3. Click **Save Settings** to save your changes.

CUSTOMIZABLE MESSAGE WAITING INDICATOR (MWI) REQUEST URI

In Release 3.1 and up, an Administrator can enter a parameter in the configuration files to customize the request-URI for MWI feature subscription. This parameter is called "**sip linex mwi request uri**".

This feature can be set on a per-line basis using the configuration files only.

Note: "**Sip Explicit MWI Subscription**" must be enabled to use this feature. For more information about the Sip Explicit MWI Subscription" parameter, see "Advanced SIP Settings (optional)" on page 4-80.

CONFIGURING MESSAGE WAITING INDICATOR (MWI) REQUEST URI

Use the following procedure to configure an MWI request URI on the IP phone.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "Message Waiting Indicator Settings" on page A-205.

DND KEY MODE

The IP phones have a feature you can enable called "Do not Disturb (DND). An Administrator or User can set "do not disturb" based on the accounts on the phone (all accounts or a specific account). You can set specific modes for the way you want the phone to handle DND. The three modes you can set on the phone for DND are:

- Account
- Phone
- Custom

An Administrator or User can set the DND mode using the Mitel Web UI at the path *Basic Settings->Preferences->General->DND Key Mode*. An Administrator can also set the DND Key Mode using the configuration files.

Note: You must configure a DND key on the phone to use this feature.

REFERENCE

For more information about how DND works and how you can use it on the phones, see the section, "Do Not Disturb (DND)" on page 5-218.

CONFIGURING THE DND KEY MODE

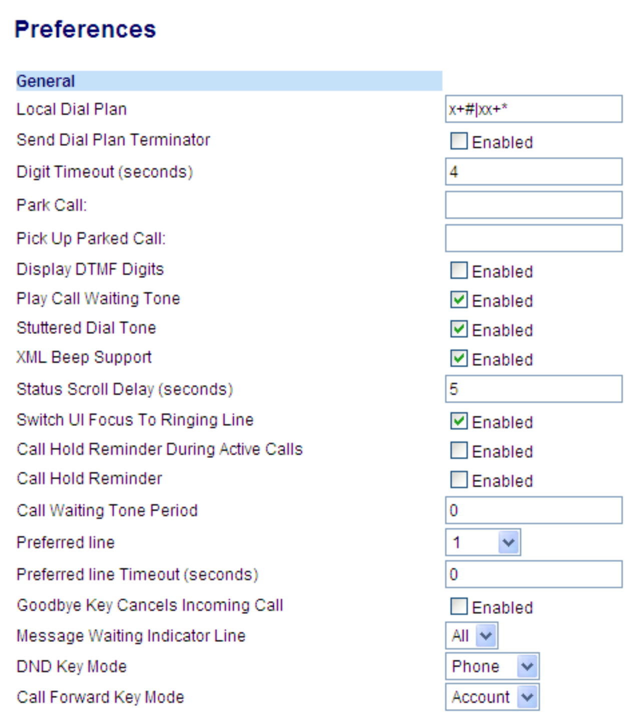
Use the following procedures to set the DND Key Mode on the phone.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "DND Key Mode Settings" on page A-206.

MITEL WEB UI

1. Click on **Basic Settings->Preferences->General.**



2. In the "**DND Key Mode**" field, select a "do not disturb" (DND) mode to use on the phone. Valid values are:
   - **Account**
     Sets DND for a specific account. DND key toggles the account in focus on the IP Phone UI, to ON or OFF.
   - **Phone**
     Sets DND ON for all accounts on the phone. DND key toggles all accounts on the phone to ON or OFF.
   - **Custom**
     Sets the phone to display custom screens after pressing the DND key, that list the account(s) on the phone. The user can select a specific account for DND, turn DND ON for all accounts, or turn DND OFF for all accounts.

The default is **Phone**.

Notes:

1. If there is only one account configured on the phone, then the mode setting is ignored and the phone behaves as if the mode was set to “Phone”.
2. Using the Mitel Web UI, if you change the DND Key Mode to “phone”, all accounts synchronize to the current setting of Account 1.

3. Configure a DND key on the phone using the procedures in the section, “Do Not Disturb (DND)” on page 5-218.
4. Click **Save Settings** to save your changes.
   The change takes effect immediately without a reboot.

REFERENCE

For more information, see the section, “Do Not Disturb (DND)” on page 5-218.

CALL FORWARD MODE

Call Forward (CFWD) on the IP phone allows incoming calls to be forwarded to another destination. The phone sends the SIP message to the SIP proxy, which then forwards the call to the assigned destination.

An Administrator or User can configure CFWD on the phone-side by setting a mode for the phone to use (**Account**, **Phone**, or **Custom**). Once the mode is set, you can use the IP Phone UI to use the CFWD feature at *Options->Call Forward* or by pressing a configured Call Forward softkey/programmable key/extension module key.

The following describes the behavior for each CFWD mode.

- **Account mode** - The account mode allows you to configure CFWD on a per account basis. Pressing a configured CFWD key applies to the account in focus.
- **Phone mode** - The Phone mode allows you to set the same CFWD configuration for all accounts (**All**, **Busy**, and/or **No Answer**). When you configure the initial account, the phone applies the configuration to all other accounts. (In the Mitel Web UI, only the account you configured is enabled. All other accounts are grayed out but set to the same configuration.) Using the Mitel Web UI, if you make changes to that initial account, the changes apply to all accounts on the phone.
- **Custom mode** - The Custom mode allows you to configure CFWD for a specific account or all accounts. You can configure a specific mode (**All**, **Busy**, and/or **No Answer**) for each account independently or all accounts. On the phones and you can set all accounts to **ALL On** or **ALL Off**.

Note: If there is only one account configured on the phone, then the mode setting is ignored and the phone behaves as if the mode was set to “Phone”.

The states you can set for Call Forward are **All**, **Busy**, **No Answer**. You can enable different call forwarding rules/modes independently (for example, you can set different phone numbers for Busy, All, and NoAns modes and then turn them on/off individually. The behavior of these states is dependent on the mode (account, phone, or custom) you configure on the phone.

REFERENCE

For more information about how Call Forwarding works and how you can use it on the IP Phones, see "Call Forwarding" on page 5-252.

CONFIGURING CALL FORWARD KEY MODE

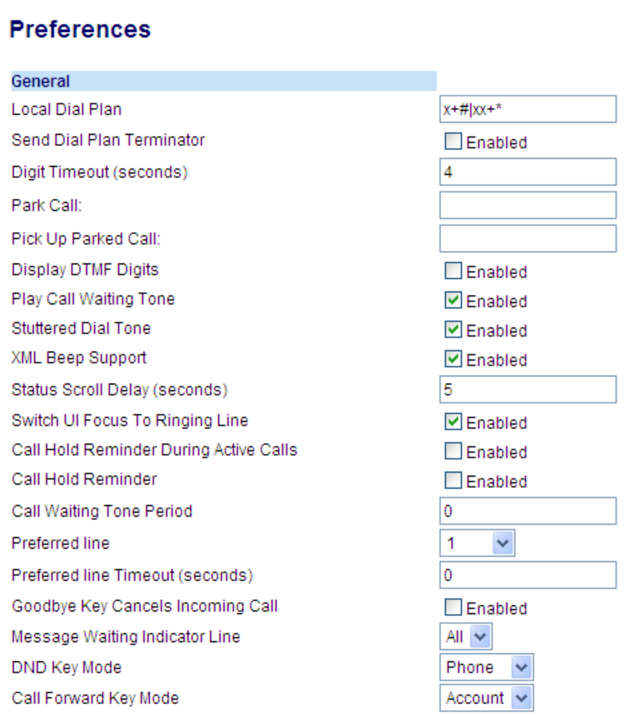
Use the following procedures to set the Call Forward key mode on the IP phones.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Call Forward Key Mode Settings" on page A-181.

MITEL WEB UI

1. Click on **Basic Settings->Preferences->General**.



Note: If there is no CFWD key configured on the phone or it is removed, you can still configure Call Forwarding via the IP Phone UI at the path *Options->Call Forward.*

2. In the "**Call Forward Key Mode**" field, select a call forward mode to use on the phone. Valid values are:

   - **Account**
     The account mode allows you to configure CFWD on a per account basis. Pressing a configured CFWD key applies to the account in focus.

- **Phone**
  The Phone mode allows you to set the same CFWD configuration for all accounts (**All**, **Busy**, and/or **No Answer**). When you configure the initial account, the phone applies the configuration to all other accounts. (In the Mitel Web UI, only the account you configured is enabled. All other accounts are grayed out but set to the same configuration.) Using the Mitel Web UI, if you make changes to that initial account, the changes apply to all accounts on the phone.
- **Custom**
  The Custom mode allows you to configure CFWD for a specific account or all accounts. You can configure a specific state (**All**, **Busy**, and/or **No Answer**) for each account independently or all accounts. You can set all accounts to **ALL On** or **ALL Off**.
  The default is **Account**.

Notes:

1. If there is no CFWD key configured on the phone or it is removed, you can still set the CFWD modes via the IP Phone UI at the path *Options->Call Forward.*
2. If there is only one account configured on the phone, then the mode setting is ignored and the phone behaves as if the mode was set to “Phone”.
3. When configuring a CFWD state (**All**, **Busy**, **No Answer**) for an account, you must configure a CFWD number for that state in order for the state to be enabled.

3. Click **Save Settings** to save your changes.
   The change takes effect immediately without a reboot.

REFERENCE

For more information, see the section, “Call Forwarding” on page 5-252.

LINK LAYER DISCOVERY PROTOCOL FOR MEDIA ENDPOINT DEVICES (LLDP-MED) AND EMERGENCY LOCATION IDENTIFICATION NUMBER (ELIN)

The IP Phones support Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED). LLDP-MED is designed to allow for things such as:

- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and Diffserv settings) leading to "plug and play" networking.
- Extended and automated power management of Power over Ethernet endpoints.
- Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, serial / asset number).

On the IP Phones, LLDP-MED performs the following:

- Supports the MAC/PHY configuration (e.g. speed rate/duplex mode).
- Supports VLAN info from the network policy; this takes precedence over manual settings.
- Allows you to enable/disable LLDP-MED if required.

- Allows you to configure time interval between successive LLDP Data Unit (LLDPDU) frames.
- Allows LLDP packets to be received from the LAN port.
- Allows the phone to use the location information, Explicit Congestion Notification (ECN) Emergency Location Identification Number (ELIN), sent by the switch, as a caller ID for making emergency calls.
  - When LLDP ELIN is enabled (default), if the phone receives location information in ECN ELIN format (10 to 25 numeric string), the phone replaces the caller ID in the From header with the ECN ELIN value and the SIP URI does not change. The phone determines if this is an emergency number by checking the emergency dial plan configured on the phone. For example, the From header of a call from 405 at the IP address 192.168.0.20 on port 5060 with an ELIN of 1234567890 would contain:
    `From: "1234567890" <sip:405@192.168.0.20:5060>;tag=929293baab`
  - You can configure the phones to add an "elin=number" value to the From header indicating the call is an emergency call, by defining the "**use lldp elin**" parameter as "**2**". With the "**use lldp elin**" defined as "**2**", using the example above, the From header would contain:
    `From: "1234567890"`
    `<sip:405@192.168.0.20:5060;elin=1234567890>;tag=929293baab`

Mitel IP Phones have a 32 second time-out for listening to LLDP-MED responses when the phone is booting up. If LLDP-MED responses are received after this initial listening period, the phone will ignore the response. Administrators can configure this time-out interval using the "**lldp startinterval**" parameter. This parameter is only valid during the phone bootup process and it will control the LLDP-MED time-out interval where the phone sends LLDP-MED advertisements and listens for the LLDP-MED responses from the switch before proceeding to the DHCP stage. The default value of this parameter is 32 seconds.

Administrators can also now configure the optional Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) Inventory Management type-length-value (TLV) sets. Using the "**lldp optional inventory management tlv**" parameter, Administrators can configure the phone to either send all Inventory Management TLV (1) sets or to send none (0). The default for this parameter is (1).

The following table identifies the configuration parameters for LLDP and ELIN and which method you can use to configure each parameter. This table also indicates whether the parameters can be configured by an Administrator, a User, or both.

PARAMETER	METHOD OF CONFIGURATION	WHO CAN CONFIGURE
lldp	Configuration Files	Administrator
lldp interval	Configuration Files	Administrator
use lldp elin	Configuration Files	Administrator
lldp startinterval	Configuration Files	Administrator
lldp optional inventory management tlv	Configuration Files	Administrator
LLDP Support	IP Phone UI	Administrator
LLDP	Mitel Web UI	Administrator

PARAMETER	METHOD OF CONFIGURATION	WHO CAN CONFIGURE
LLDP Packet Interval	Mitel Web UI	Administrator

CONFIGURING LLDP-MED AND ELIN

Use the following procedures to configure LLDP-MED and ELIN on the IP phones.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "LLDP-MED and ELIN Settings" on page A-183.

Use the following procedure to enable/disable LLDP-MED using the IP Phone UI.

Note: You cannot configure the "**LLDP Interval**" or the "**Use LLDP ELIN**" parameters via the IP Phone UI.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press ⚙ or ⚙ on the phone to enter the Options List.
2. Select **Administrator Menu.**
3. Select **Network Settings**.
4. Select **Ethernet & VLAN**.
5. Select **LLDP Support**.
6. Press **CHANGE** to toggle the LLDP setting to **Enabled** or **Disabled**.
   This field enables or disables Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) on the IP Phone.
7. Press **DONE** to save the change.

For the 6867i/6869i/6920/6930:

1. Press ⚙ to enter the Options List.
2. Press the **Advanced** softkey.
3. Enter the Administrator password using the keypad. Default is "**22222**".
4. Select **Network > LLDP**.
   This option enables or disables Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) on the IP Phone.
5. Use the ▲ and ▼ keys enable or disable the feature.
6. Press the **Save** softkey.

For the 6873i:

1. Press [ ] to enter the Options List.
2. Press the **Advanced** softkey.
3. Enter the Administrator password and press the blue Enter key. Default is “**22222**”.
4. Press the **Network** icon.

   Note: If required, swipe left on the screen to navigate to the second page of options.

5. Press the **LLDP** icon.
   This option enables or disables Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) on the IP Phone.

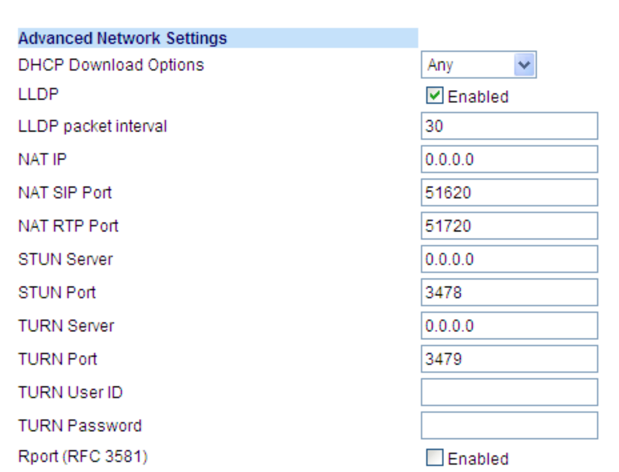
   Note: If required, swipe left on the screen to navigate to the second page of options.

6. Choose **Enabled** or **Disabled**.
7. Press the **Save** softkey.

Use the following procedure to configure LLDP-MED using the Mitel Web UI:

MITEL WEB UI

1. Click on **Advanced Settings->Network->Advanced Network Settings.**



2. The “***LLDP***” field is enabled by default. To disable LLDP, click the check mark in the box to clear the check mark.
3. In the “**LLDP Packet Interval**” field, enter the time, in seconds, between the transmission of LLDP Data Unit (LLDPDU) packets.
   The value of zero (0) disables this parameter. Valid values are 0 to 2147483647. Default is 30.
4. Click **Save Settings** to save your changes.

INCOMING/OUTGOING INTERCOM WITH AUTO-ANSWER AND BARGE IN

The Intercom feature allows you to press the configured Intercom button to initiate an intercom call (either by entering a number manually or automatically initiating the call if a number is predefined). Intercom calls can be controlled either locally (phone-side) or by the SIP server (server-side).

You can configure incoming and outgoing intercom calls on all phone models. A user can configure incoming intercom calls only.

OUTGOING INTERCOM CALLS

On outgoing intercom calls, an available unused line is found when the Icom button is pressed. Since this line has no configuration, the phone applies an existing configuration ("Outgoing Intercom Settings", Line, default is Line 1) to this line in preparation for placing the intercom call. For example, an outgoing intercom call can use the configuration of line 1 but places the actual intercom call using line 9. Only an Administrator can configure outgoing intercom calls.

A **phone-side** Intercom call indicates the phone is responsible for telling the recipient that an intercom call is being placed, while a **server-side** intercom call means the SIP server is responsible for informing the recipient. Server-side calls require additional configuration of a **prefix code**. After pressing the Icom button and, if required, entering the number to call, the phone automatically adds the prefix to the called number and sends the outgoing call via the server.

For outgoing intercom calls, an administrator can configure the following parameters:

CONFIGURATION FILE PARAMETERS	WEB UI PARAMETERS
• sip intercom type	• Type
• sip intercom prefix code	• Prefix Code
• sip intercom line	• Line

Note: To configure outgoing intercom calls using these parameters, see “Configuring Intercom Calls Settings” on page 5-119.

INCOMING INTERCOM CALLS

You can configure how the phone handles incoming intercom calls. You can receive incoming intercom calls whether or not there are active calls on the phone. The way the phone handles the call depends on the incoming intercom call configuration. The following paragraphs describe the configuration parameters for incoming intercom calls.

Microphone Mute

You can mute or unmute the microphone on the IP phone for intercom calls made by the originating caller. If you want to mute the intercom call, you enable this feature. If you want to unmute (or hear the intercom call), you disable this feature.

Auto-Answer/Play Warning Tone

The auto-answer feature on the IP phone allows you to enable or disable automatic answering for an Intercom call. If "Auto-Answer" is enabled, the phone automatically answers an incoming intercom call. If "Play Warning Tone" is also enabled, the phone plays a tone to alert the user before answering the intercom call. If "Auto-Answer" is disabled, the phone treats the incoming intercom call as a normal call.

The IP phone recognizes if an incoming call is an intercom auto-answer call if the SIP INVITE includes one of the following:

- A "Call-Info" header containing "answer-after=0".
- An "Alert-Info" header containing "info=alert-autoanswer".
- An "Alert-Info" header containing "Auto Answer" AND the "To" header containing "intercom=true".

Note: When the IP phones recognize the second and third types of incoming intercom calls (as per the list above), the call will automatically be answered and the call's audio will be played through the IP phone's speaker (i.e. the user's audio preferences will be ignored).

"Delay" before Auto-Answer

The IP Phones include support for the "delay" parameter (in the Alert-Info header, used in conjunction with info=alert-autoanswer) in order to facilitate auto-answer functionality. When present, the value of the "delay" parameter specifies the length of time in seconds an IP phone rings before a call is auto-answered. If this value of the "delay" parameter set to 0 (delay=0), then an incoming call is immediately auto-answered. The absence of the parameter is considered as ring forever.

In order for the delay functionality to operate, you must first enable Auto-Answer on the IP Phone.

Note: Auto answer of BCA call works when **Delay Before Audibly Ringing** parameter is set to a value other than **Don't ring**.

Allow Barge In

You can configure whether or not the IP phone allows an incoming intercom call to interrupt an active call. The "**sip intercom allow barge in"** parameter controls this feature. When you enable the **sip intercom allow barge in** parameter (1 = enable in the configuration files), which is the default value, an incoming intercom call takes precedence over any active call, by placing the active call on hold and automatically answering the intercom call. When you disable this parameter (0 = disable in the configuration files), and there is an active call, the phone treats an incoming intercom call like a normal call and plays the call warning tone. You can set this parameter using the configuration files or the Mitel Web UI.

For incoming intercom calls, an administrator or user can configure the following parameters:

CONFIGURATION FILE PARAMETERS	WEB UI PARAMETERS
sip allow auto answer	Auto-Answer

CONFIGURATION FILE PARAMETERS	WEB UI PARAMETERS
sip intercom mute mic	Microphone Mute
sip intercom warning tone	Play Warning Tone
sip intercom allow barge in	Barge In

Note: To configure incoming intercom calls using these parameters, see "Configuring Intercom Calls Settings" on page 5-119.

CONFIGURING INTERCOM CALLS SETTINGS

You can configure the Intercom feature using the configuration files or the Mitel Web UI.

Note: An administrator can configure the incoming and outgoing Intercom feature. A user can configure the incoming Intercom feature only.

Use the following procedures to configure Intercom calls on the IP phone.

CONFIGURATION FILES

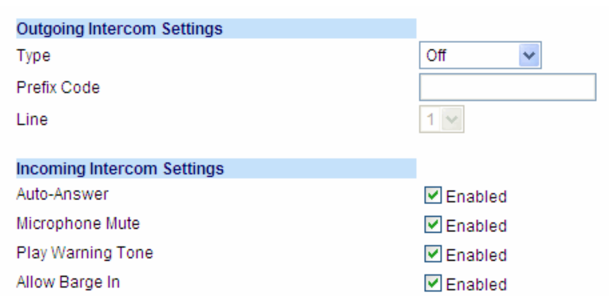
For specific parameters you can set in the configuration files for outgoing Intercom, see Appendix A, the section, "Outgoing Intercom Settings" on page A-230.

For specific parameters you can set in the configuration files for incoming Intercom, see Appendix A, the section, "Incoming Intercom Settings" on page A-231.

MITEL WEB UI

Outgoing intercom Settings

1. Click on **Basic Settings->Preferences->Outgoing Intercom Settings**.



2. Select an Intercom type for outgoing Intercom calls from the **Type** list box. Valid values are **Phone-Side**, **Server-Side**, **Off**. Default is **Off**.

3. If Server-Side is selected, enter a prefix to add to the phone number in the "**Prefix Code"** field.

> **Note:** For Sylantro servers, enter *96.

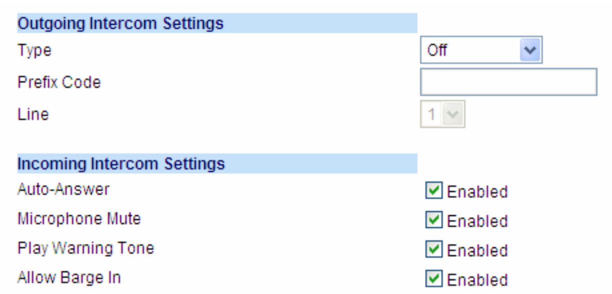
4. If Phone-Side or Server-Side is selected, select a line from the **Line** list box for which you want the IP phone to use as its configuration on the Intercom call.

> **Note:** The IP phone uses the configuration from the line you select from this list box. The call itself is made using the first available line at the time of the call.

5. Click **Save Settings** to save your changes.

Incoming intercom Settings:

6. Click on **Basic Settings->Preferences->Incoming Intercom Settings**.



7. The "**Auto-Answer**" field is enabled by default. The automatic answering feature is turned on for the IP phone for answering Intercom calls. To disable this field, uncheck the box.

> **Note:** If the Auto-Answer field is not checked (disabled), the phone treats the incoming intercom call as a normal call.

8. The "**Microphone Mute**" field is enabled by default. The microphone is muted on the IP phone for Intercom calls made by the originating caller. To disable this field, uncheck the box.

9. The "**Play Warning Tone**" field is enabled by default. If “Auto-Answer” is enabled, the phone plays a warning tone when it receives in incoming intercom call. To disable this field, uncheck the box.

10. The "**Allow Barge In**" field is enabled by default. If an active line on the phone receives an incoming intercom call, the active call is put on hold and the phone automatically answers the incoming intercom call. To disable this field, uncheck the box.

11. Click **Save Settings** to save your changes.

SUPPORT FOR SWITCHING AUDIO FROM ONE-WAY TO TWO-WAY AUDIO FOR INTERCOM CALLS

The SIP phones have a facility to switch from one-way audio to two-way audio calls for Intercom calls.

When an intercom call is initiated with a one-way audio path from the caller to one or more phone(s), one of the called users can activate the full bidirectional audio path by pressing a softkey of the phone. The call manager activates a full two-way audio path between the caller and the answering user.

By default, this feature is disabled. You can enable this feature by configuring the value of the "**action uri answericom**" parameter as "http://<*ipaddress*>/requestType-*XYZ*" (XYZ can be any string here).

- When the parameter is configured with an action uri string on 6867i, 6869i, and 6873i:
  - A softkey labeled *"AnswerIcom"* is displayed in the bottom softkey list of the intercom call screen.
  - You can activate two-way audio intercom by pressing the *"AnswerIcom"* softkey.
  - The Conf and Xfer softkeys are not displayed on the intercom call screen.
- When the parameter is configured with an action uri string on 6863i and 6865i:
  - A label named "*Answer*" is displayed at the right corner of the intercom call screen. This is prefixed with "*arrow down*" icon.
  - You can activate two-way audio intercom by pressing the '*scroll down'* key with the above configuration.
- When the "*AnswerIcom"* softkey or *"scroll down"* key is pressed:
  - The phone sends HTTP GET notification to the configured action uri.
  - The phone keeps the *"AnswerIcom"* softkey or scroll down key on the screen until the two-way intercom is activated by the call manager.
- When the two-way audio intercom is activated by the call manager (through REINVITE)
  - The phone unmutes the microphone if it was muted before.
  - The phone displays the normal connected call screen that has no *"AnswerIcom"* bottom softkey or label prefixed with *"arrow down"* icon.

Note:

1. The server support is required to enable this feature.

2. If the server does not support this feature or this feature is not enabled on server, enabling this feature on the phone may lead to unexpected behavior. Hence this feature is enabled only if it is supported by the server.

Enabling / Disabling Support for Switching Audio from One-way to Two-way audio for Intercom calls Using Configuration Files

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, section "Audio Switching Support for Intercom Calls" on page A-233.

GROUP PAGING RTP SETTINGS

An Administrator or User can configure a specific key (softkey, programmable key, or expansion module key) on the phone that allows you to send/receive a Real Time Transport Protocol

(RTP) stream to/from pre-configured multicast addresses without involving SIP signaling. This is called Group Paging on the IP phones. You can specify up to 5 listening multicast addresses.

An Administrator can use the following parameters in the configuration files to set Group Paging RTP Settings:

- paging group listening
- softkeyN type, topsoftkeyN type, prgkeyN type, or expmodX keyN type
- sofkeyN label
- softkeyN value, topsoftkeyN value, prgkeyN value, or expmodX keyN value

An Administrator or User can use the following parameters in the Mitel Web UI to set Group Paging RTP Settings:

- **Paging Listen Addresses** (Path: ***Basic Settings->Preferences->Group Paging RTP Settings***)
- **<Paging> Key** (***Operation->Softkeys and XML, Programmable Keys, or Expansion Module Keys***)

Note: The Group Paging RTP Settings are dependent upon the setting for the "**Allow Barge In**" parameter.

HOW IT WORKS

After pressing a configured "Paging" key on the phone, the phone sends an RTP stream to a preconfigured multicast address (IP port). Any phone in the local network then listens for the RTP stream on the preconfigured multicast address (IP port). For both sending and receiving of the multicast RTP there is no sip signaling involved. When the phone sends or receives a multicast RTP, it shows its involvement to the user by displaying "Paging".

Note: Multicast RTP is one way only - from sender to the receiver (i.e. from sender to the multicast address (receiver)).

The phone uses a preconfigured G711 uLaw CODEC for multicast RTP.

For Paging Systems, the phone only plays RTP traffic; users have the ability to drop a rogue page. The recipient can drop the incoming page if required. The recipient can also set Do Not Disturb (DND) to ignore any incoming pages.

Note: For outgoing RTP multicasts, all other existing calls on the phone are put on hold.

For incoming RTP multicasts, the ringing display is dependent on the "**Allow Barge-In**" parameter as per the following rules:

- If the "**Allow Barge-In**" parameter is **disabled**, and there is not other call on the phone, then the paging is automatically played via the preferred audio device (see the <Model-Specific> ***SIP Phone User Guide*** for setting Audio Mode on the phone).

- If there is an existing call on the phone, the call initially displays in the ringing state. The user has the option to accept/ignore the call. If the "**Allow Barge-In**" parameter is **enabled**, the RTP multicast call barges in, and any existing calls are put on hold.
- If an RTP multicast session already exists on the phone, and the phone receives another incoming RTP multicast session, the priority is given to the first multicast session and the second multicast session is ignored. The behavior for the incoming calls in this case is also based on the setting for the "**Allow Barge-in**" parameter. The incoming call is handled as if there were an existing call already on the phone.
- If a user is in a dialing state with the "**Allow Barge-In**" parameter enabled and a page is received by the phone, the phone will automatically switch focus to the page screen.
- If a user is in a dialing state with the "**Allow Barge-In**" parameter disabled and a page is received by the phone, the phone will keep its focus on the dialing screen.

CONFIGURING GROUP PAGING RTP SETTINGS

Use the following procedure to configure Group Paging RTP Settings using the configuration files.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Codec Negotiation Behavior" on page A-233.

Use the following procedure to configure RTP streaming for Paging applications using the Mitel Web UI.

MITEL WEB UI

1. Click on **Basic Settings->Preferences->Group Paging RTP Settings**.

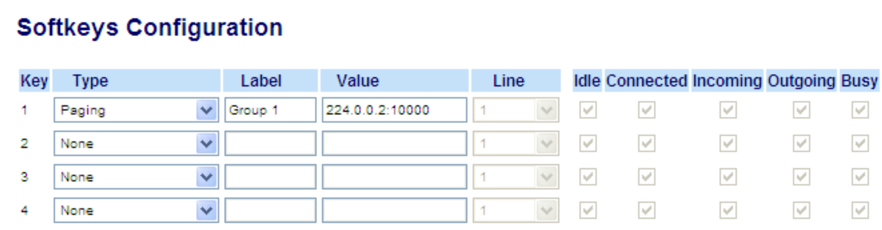
2. In the "**Paging Listen Addresses**" text box, enter the multicast IP address(es) and port number(s) on which the phone listens for incoming multicast RTP packets.

Notes:

1. Enter the IP address in dotted decimal format (for example, **224.0.0.2:10000,239.0.1.20:15000**) If this field is blank, Paging listening capability is disabled on the phone.
2. The valid port range is from 2 to 65534.
3. Use even-number ports only.

3. Click on **Softkeys and XML.**
or
Click on **Programmable Keys**.

or
Click on **Expansion Module Keys**.



4. Choose a key that you want to assign as the Paging Key and select **Paging** from the "**Type**" field.
5. In the "**Label**" field, enter a key label to assign to the Paging key (for example, "**Group 1**").
6. In the "**Value**" field, enter a multicast IP address and a port number for the Paging key. When you press this key, the phone initiates an outgoing multicast RTP session to the specified address using the specified port. (For example, **224.0.0.2:10000).**

   Notes:
   1. When you select **Paging** for the "**Type**" field, the "**Line**" field and state fields are disabled.
   2. The valid port range is from 2 to 65534.

7. Click **Save Settings** to save your changes.

Using the Configured Paging Key on the IP Phone

The following procedure describes the use of the Paging key. The procedures assumes you have already configured the Paging key using the configuration files or the Mitel Web UI.

Notes:
1. The recipient of a Paging call can set a global "Do Not Disturb" (DND) to ignore any incoming pages.
2. For incoming Paging, the phones use the Intercom configuration settings. The incoming Page is dependent on the "**Allow Barge-In**" parameter setting and the "*Idling/On Call*" state.

IP PHONE UI

1. On the IP Phone, press the key you configured for Paging.
   The phone opens a multicast RTP session and an outgoing OR incoming phone screen displays.

   Note: If you enable global DND on the phone, the incoming multicast RTP session is dropped.

2. Press the **Drop** key to end the multicast RTP session and return to the idle screen.

SPEEDDIAL KEY MAPPING

There are hard keys on your phone, such as **Hold, Redial, Xfer,** and **Conf** that are configured by default for specific call-handling features. (See the <Model-Specific> ***SIP Phone User Guide*** for more information about these key functions).

ENABLING/DISABLING REDIAL, XFER, AND CONF KEYS

You can enable or disable the **Redial**, **Xfer**, and **Conf** keys as required using the following parameters in the configuration files:

- redial disabled
- conference disabled
- call transfer disabled

Valid values for this parameter are **0** (enabled) and **1** (disabled).

If this parameter is set to **1**, the key is not active and is ignored if pressed by the user. For "**redial disabled**" the value of 1 does not save the dialed number to the "Outgoing Redial List".

If this parameter is set to **0**, the key is active and can be pressed by the user.

This feature is configurable via the configuration files only.

Use the following procedure to enable/disable the **Redial**, **Xfer**, and **Conf** keys.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Mapping Key Settings" on page A-240.

MAPPING REDIAL AND CONF KEYS AS SPEEDDIALS

You can map the **Redial** and **Conference** keys on the IP phone to use as Speeddial keys. When the **Redial** or **Conference** key is pressed, the number configured for the key automatically speeddials. If no number is configured, the **Redial** and **Conference** keys return to their original functionality.

You can configure this feature using the configuration files or the Mitel Web UI.

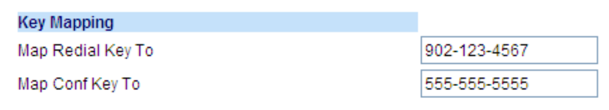
Use the following procedures to set the Redial and Conf keys as Speeddial keys.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Mapping Key Settings" on page A-240.

MITEL WEB UI

1. Click on **Basic Settings->Preferences**.



2. In the **Key Mapping** section, enter a number in the "**Map Redial Key To**" field, that the IP phone will use to speeddial when the Redial key is pressed.
3. Enter a number in the "**Map Conf Key To**" field, that the IP phone will use to speeddial when the Conf Key is pressed.
4. Click **Save Settings** to save your changes.

USING REDIAL KEY FOR "LAST NUMBER REDIAL"

The IP phones have an enhanced redial user interface that allows a user to quickly redial the last number that was dialed out from the phone. You can:

- Press the **Redial** key twice to redial the last number dialed.
- Press the **Redial** key once, scroll the list of numbers, then press the **Redial** button again to dial the number that displays on the screen.

The "last number redial" feature for the Redial key is static and is not configurable.

Note: You can use the Redial key during active calls.

SEND DTMF FOR REMAPPING CONFERENCE OR REDIAL KEY

Previously, the "Conf" and "Redial" keys could be mapped to a speeddial to generate a call to a custom number when the phone was idle. During an active call, pressing the "Redial" or "Conf" keys would put the current call on hold and then dial the custom number. Now the "Conf" and "Redial" key remappings have the same behavior as the "Speeddial" key when the phone is idle. During an active call the phone will send the custom number as DTMF using the phone configured DTMF method (inbound vs out-of-band RFC2833 vs SIP INFO).

This feature can be configured using the new "**map redial as dtmf**" and "**map conf as dtmf**" parameters.

When a user presses the "Redial" key, the mapped number will be sent out as DTMF during an active call if the current "**map redial key to**" parameter is configured to a number and the "**map redial as dtmf**" parameter is set to "1".

When a user presses the "Conf" key, the mapped number will be sent out as DTMF during an active call if the current "**map conf key to**" parameter is configured to a number and "**map conf as dtmf**" parameter is set to "1".

ENABLING OR DISABLING THE SENDING OF DTMF WITH REMAPPED REDIAL AND CONF KEYS

Use the following procedures to configure the remapping of the “Redial” and “Conf” keys on the IP phone.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Send DTMF for Remapping Conference or Redial Key” on page A-242.

RING TONES AND TONE SETS

You can configure ring tones and ring tone sets on the IP phones.

RING TONES

There are several distinct ring tones a user or administrator can select from to set on the IP phones. You can enable/disable these ring tones on a global basis or on a per-line basis.

There are 10 additional ringtones are available (**Velocity, Skyline, Rise, Daybreak, After Hours, Open Road, Pronto, Voyage, Bloom, Move**).

The following table identifies the valid settings and default values for each type of configuration method.

Ring Tone Settings Table

CONFIGURATION METHOD	VALID VALUES	DEFAULT VALUE

Configuration Files	Global: 0 (Tone 1) 1 (Tone 2) 2 (Tone 3) 3 (Tone 4) 4 (Tone 5) 5 (Silent) 6 (Tone 7) 7 (Tone 8) 8 (Tone 9) 9 (Tone 10) 10 (Tone 11) 11 (Tone 12) 12 (Tone 13) 13 (Tone 14) 14 (Tone 15) 15 (Tone 16) 20 Velocity 21 Skyline 22 Rise 23 Daybreak 24 After Hours 25 Open Road 26 Pronto 27 Voyage 28 Bloom 29 Move 100 (Custom Ring Tone 1) 101 (Custom Ring Tone 2) 102 (Custom Ring Tone 3) 103 (Custom Ring Tone 4) 104 (Custom Ring Tone 5) 105 (Custom Ring Tone 6) 106 (Custom Ring Tone 7) 107 (Custom Ring Tone 8)	Global: 0 (tone 1)

Per-Line: -1 (global) 0 (Tone 1) 1 (Tone 2) 2 (Tone 3) 3 (Tone 4) 4 (Tone 5) 5 (Silent) 6 (Tone 7) 7 (Tone 8) 8 (Tone 9) 9 (Tone 10) 10 (Tone 11) 11 (Tone 12) 12 (Tone 13) 13 (Tone 14) 14 (Tone 15) 15 (Tone 16) 20 Velocity 21 Skyline 22 Rise 23 Daybreak 24 After Hours 25 Open Road 26 Pronto 27 Voyage 28 Bloom 29 Move 100 (Custom Ring Tone 1) 101 (Custom Ring Tone 2) 102 (Custom Ring Tone 3) 103 (Custom Ring Tone 4) 104 (Custom Ring Tone 5) 105 (Custom Ring Tone 6) 106 (Custom Ring Tone 7) 107(Custom Ring Tone 8)	Per-Line: -1 (global)

IP Phone UI	Global: Velocity Skyline Rise Daybreak After Hours Open Road Pronto Voyage Bloom Move Tone 1 Tone 2 Tone 3 Tone 4 Tone 5 Tone 6 Tone 7 Tone 8 Tone 9 Tone 10 Tone 11 Tone 12 Tone 13 Tone 14 Tone 15 Silent Custom Ring Tones 1-8 (if available)	Global: Tone 1

Mitel Web UI	Global: Velocity Skyline Rise Daybreak After Hours Open Road Pronto Voyage Bloom Move Tone 1 Tone 2 Tone 3 Tone 4 Tone 5 Tone 6 Tone 7 Tone 8 Tone 9 Tone 10 Tone 11 Tone 12 Tone 13 Tone 14 Tone 15 Silent Custom Ring Tones 1-8 (if available) Per-Line: Global Velocity Skyline Rise Daybreak After Hours Open Road Pronto Voyage Bloom Move Tone 1 Tone 2 Tone 3 Tone 4 Tone 5 Tone 6 Tone 7 Tone 8 Tone 9	Global: Tone 1 Per-Line: Global

RING TONE SETS

In addition to ring tones, you can configure ring tone sets on a global-basis on the IP phones. Ring tone sets consist of tones customized for a specific country. The ring tone sets you can configure on the IP phones are:

- Australia
- Brazil
- Canada
- Europe (generic tones)
- France
- Germany
- Italy
- Italy2
- Malaysia
- Mexico
- Russia
- Slovakia
- UK
- US (Default)

When you configure the country's tone set, the country-specific tone is heard on the phone for the following:

- dial tone
- secondary dial tone
- ring tone
- busy tone
- congestion tones
- call waiting tone
- ring cadence pattern

Note: You configure ring tones and tone sets using the Mitel Web UI, IP Phone UI, or configuration files. However, when using the IP phone UI, you can set global configuration only.

Tone Set Frequencies and Cadences

The following table lists the **Australian** tone set frequencies and cadences.

TONE	FREQUENCY (HZ)	CADENCE (ON/OFF) (MS)
Dial	425 * 25	Continuously On
Secondary Dial	425 * 25	100/40
Ringing	425 * 25	400/200/400/2000
Busy	425	375/375
Congestion	425	2500/500
Call Waiting	425	200/200/200/Continuously Off
Ring Cadence	-	400/200/400/2000

The following table lists the **Brazilian** tone set cadences.

TONE	FREQUENCY (HZ)	CADENCE (ON/OFF) (MS)
Dial	425	Continuously On
Secondary Dial	425	300/100/300/1300
Ringing	425	1000/4000
Busy	425	250/250
Congestion	425	500/500
Call Waiting	425	100/100/100/10000
Ring Cadence	-	1000/4000

The following table lists the **Canadian** tone set frequencies and cadences.

TONE	FREQUENCY (HZ)	CADENCE (ON/OFF) (MS)
Dial	350 * 440	Continuously On
Secondary Dial	350 * 440	100/100/Continuously On
Ringing	440 * 480	2000/4000
Busy	480 * 620	500/500
Congestion	480 * 620	240/260
Call Waiting	440	300/Continuously Off
Ring Cadence	-	2000/4000

The following table lists the generic **European** tone set frequencies and cadences.

TONE	FREQUENCY (HZ)	CADENCE (ON/OFF) (MS)
Dial	425	Continuously On
Secondary Dial	425	500/50
Ringing	425	1000/4000
Busy	425	500/500
Congestion	425	200/200
Call Waiting	425	200/200/200/Continuously Off
Ring Cadence	-	1000/4000

The following table lists the **French** tone set frequencies and cadences.

TONE	FREQUENCY (HZ)	CADENCE (ON/OFF) (MS)
Dial	440	Continuously On
Secondary Dial	340 * 440	Continuously On
Ringing	440	1500/3500
Busy	440	500/500
Congestion	440	500/500
Call Waiting	440	300/Continuously Off
Ring Cadence	-	1500/3500

The following table lists the **German** tone set frequencies and cadences.

TONE	FREQUENCY (HZ)	CADENCE (ON/OFF) (MS)
Dial	425	Continuously On
Secondary Dial	425 * 400	Continuously On
Ringing	425	1000/4000
Busy	425	480/480
Congestion	425	240/240
Call Waiting	425	200/200/200/Continuously Off
Ring Cadence	-	1000/4000

The following table lists the Italian tone set cadences for "**Italy**".

TONE	FREQUENCY (HZ)	CADENCE (ON/OFF) (MS)
Dial	425	200/200/600/1000
Secondary Dial	425	Continuously On
Ringing	425	1000/4000
Busy	425	500/500
Congestion	425	200/200
Call Waiting	425	400/100/250/100/150/14000
Ring Cadence	-	1000/4000

The following table lists the Italian tone set cadences for "**Italy2**".

TONE	FREQUENCY (HZ)	CADENCE (ON/OFF) (MS)
Dial	425	Continuously On
Secondary Dial	425	500/500
Ringing	425	1000/4000
Busy	425	500/500
Congestion	425	200/200
Call Waiting	425	100/Continuously Off
Ring Cadence	-	1000/4000

The following are **Malaysian** tone set cadences.

TONE	FREQUENCY (HZ)	CADENCE (ON/OFF) (MS)
Dial	425	Continuously On
Secondary Dial	425	160/160
Ringing	425 * 50	400/200/400/2000
Busy	425	500/500
Congestion	425	250/250
Call Waiting	425	100/200/100/8600
Ring Cadence	-	400/200/400/2000

Notes:

1. The phone does not apply a different volume level to the first part of the Malaysian call waiting tone.
2. The level of the 50 Hz modulation signal for the Malaysian ringback tone is 90%.

The following are **Mexican** tone set cadences.

TONE	FREQUENCY (HZ)	CADENCE (ON/OFF) (MS)
Dial	425	Continuously On
Secondary Dial	425	300/100/300/1300
Ringing	425	1000/4000
Busy	425	500/500
Congestion	425	250/250
Call Waiting	425	100/100/100/10000
Ring Cadence	-	1000/4000

The following are **Russian** tone set cadences.

TONE	FREQUENCY (HZ)	CADENCE (ON/OFF) (MS)
Dial	425	Continuously On
Secondary Dial	425	500/50
Ringing	425	1000/4000
Busy	425	500/500
Congestion	425	200/200
Call Waiting	425	200/600/200/Continuously Off
Ring Cadence	-	1000/5000

The following are **Slovak** tone set cadences.

TONE	FREQUENCY (HZ)	CADENCE (ON/OFF) (MS)
Dial	425	330/330/660/660
Secondary Dial	425	165/165/165/165/165/165/660/660
Ringing	425	1000/4000
Busy	425	330/330
Congestion	425	165/165
Call Waiting	425	330/9000
Ring Cadence	-	1000/4000

The following table lists the **UK** tone set cadences.

TONE	FREQUENCY (HZ)	CADENCE (ON/OFF) (MS)
Dial	350 * 440	Continuously On
Secondary Dial	350 * 440	750/750
Ringing	400 * 450	400/200/400/2000
Busy	400	375/375
Congestion	400	400/350/225/525
Call Waiting	400	100/Continuously Off
Ring Cadence	-	400/200/400/2000

The following table lists the **US** tone set cadences.

TONE	FREQUENCY (HZ)	CADENCE (ON/OFF) (MS)
Dial	350 * 440	Continuously On
Secondary Dial	350 * 440	100/100/Continuously On
Ringing	440 * 480	2000/4000
Busy	480 * 620	500/500
Congestion	480 * 620	240/260
Call Waiting	440	300/Continuously Off
Ring Cadence	-	2000/4000

CONFIGURING RING TONES AND TONE SETS

Use the following procedures to configure ring tones and tone sets on the IP phones.

CONFIGURATION FILES

For specific parameters you can set in the configuration files for ring tones, see Appendix A, the section, "Ring Tone and Tone Set Global Settings" on page A-195 or "Ring Tone Per-Line Settings" on page A-197.

IP PHONE UI

For global configuration only:

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Preferences**.
3. Select **Tones**.
4. Select **Set Ring Tone**.
5. Select the type of ring tone (**Velocity, Skyline, Rise, Daybreak, After Hours, Open Road, Pronto, Voyage, Bloom, Move, Tone 1** through **Tone 15**, **Silent** or a custom ring tone if available).
6. Press **Done** to save the change.
7. Select **Tone Set**.
8. Select the country for which you want to apply the tone set.
Valid values are **Australia**, **Brazil, Canada, Europe, France**, **Germany**, **Italy**, **Italy2, Malaysia, Mexico, Russia, Slovakia, UK**, and **US**. Default is **US**.
9. Press **Done** to save the change.
The ring tone and tone set you select is immediately applied to the IP phone.

For the 6867i/6869i/6920/6930:

1. Press to enter the Options List.
2. Navigate to the **Audio > Ring Tones** option and press the button or **Select** softkey.
3. Use the ▲ and ▼ keys to scroll through and choose the desired ring tone (**Velocity, Skyline, Rise, Daybreak, After Hours, Open Road, Pronto, Voyage, Bloom, Move, Tone 1** through **Tone 15**, **Silent** or a custom ring tone if available).
4. Press the **Save** softkey to save your changes.
5. Navigate to the **Audio > Tone Sets** option and press the button or **Select** softkey.

6. Use the ▲ and ▼ keys to scroll through and choose the desired tone set.
Valid values are **Australia**, **Brazil, Canada, Europe, France**, **Germany**, **Italy**, **Italy2, Malaysia, Mexico, Russia, Slovakia, UK**, and **US**. Default is **US**.

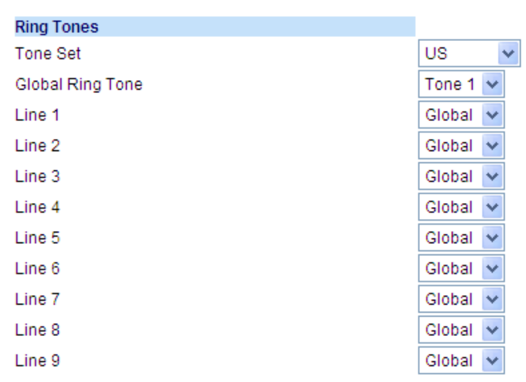
7. Press the **Save** softkey to save your changes.

For the 6873i/6940/6970:

1. Press ⚙ or the **Settings** softkey to enter the Options List.
2. Press the **Audio** icon.
3. Press the **Ring Tones** icon.
4. Choose the desired ring tone (**Velocity, Skyline, Rise, Daybreak, After Hours, Open Road, Pronto, Voyage, Bloom, Move, Tone 1** through **Tone 15**, **Silent** or a custom ring tone if available).
5. Press the **Save** softkey to save your changes.
6. Press the **Tone Sets** icon.
7. Choose the desired tone set.
Valid values are **Australia**, **Brazil, Canada, Europe, France**, **Germany**, **Italy**, **Italy2, Malaysia, Mexico, Russia, Slovakia, UK**, and **US**. Default is **US**.
8. Press the **Save** softkey to save your changes.

MITEL WEB UI

1. Click on **Basic Settings->Preferences**.



For global configuration:

2. In the "**Ring Tones**" section, select a country from the "**Tone Set**" field.
Valid values are **Australia**, **Brazil, Canada, Europe, France**, **Germany**, **Italy**, **Italy2, Malaysia, Mexico, Russia, Slovakia, UK**, and **US**. Default is **US**

3. Select a value from the "**Global Ring Tone**" field.

Note: See the "Ring Tone Settings Table" on page 5-127 for valid values.

For per-line configuration:

4. In the "**Ring Tone**" section, select a line for which you want to set ring tone.
5. Select a value from the "**LineN**" field.

   Note: See the "Ring Tone Settings Table" on page 5-127 for valid values.

6. Click **Save Settings** to save your changes.

CUSTOMIZABLE RINGING/RING BACK TIMEOUT PERIOD

Administrators can define a timeout (applicable to both incoming and outgoing calls) specifying how long the IP phones will play the ringing and ringback tones before it terminates the call. This is controlled by the "**ringback timeout**" configuration parameter.

For outgoing calls, the originating phone will send a SIP CANCEL to stop the ringing at the destination phone after the timeout expires. For incoming calls, the terminating phone will send a SIP 486 Busy Here to stop the ringback at the originating phone after the timeout expires.

Notes:

1. The "**ringback timeout**" parameter is defined as 300 seconds by default.
2. The valid timeout range is from 0 to 86400 seconds.

CONFIGURING THE RINGING/RING BACK TIMEOUT PERIOD

Use the following procedures to configure the ringing/ring back timeout on the IP phones.

CONFIGURATION FILES

For specific parameters you can set in the configuration files for the ringing/ring back timeout period, see Appendix A, the section, "Ringing/Ring Back TimeOut Period Settings" on page A-198.

CUSTOM RING TONES

The 6800 series IP phones support up to eight custom ring tones. Administrators (and if enabled, users) can install ring tones on the phone using the configuration files or the Web UI. Users can then simply select a ring tone on the phone or the Web UI to use as their incoming call ring tone.

Notes:

1. Ring tones must be in .wav format. The IP phones support the following WAV file specifications:
   - Sampling frequency -8 kHz
   - Channel - Mono
   - Bitrate - 64 kbit/s (8 kHz sampling frequency x 8 bits per sample)
   - Codec - G.711 μ-law and a-law
   - Packet size / Voice size - 20 ms packet size / Voice size
2. Individual WAV files cannot exceed 1 MB in size (the total combined size of the eight WAV files cannot exceed 8 MB).
3. Filenames must contain only ASCII characters.
4. For information on how to set a custom ring tone, see "Ring Tone Settings Table" on page 5-127.

Administrators can install local WAV files using the phone's Web UI under the *Basic Settings > Custom Ringtones* menu or install WAV files located on an FTP, TFTP, HTTP, or HTTPS server by defining their location and filename in the respective configuration file using the "**custom ringtone N**" parameter (where N = 1 to 8). For example, if the following parameters are added to the startup.cfg, <model>.cfg, or <mac>.cfg,

```
custom ringtone 1: ftp://192.168.0.50/beep.wav

custom ringtone 2: ftp://192.168.0.50/classic.wav
```

the phone will download both WAV files from the FTP server and store beep.wav in position 1 and classic.wav in position 2 on the phone.

Notes:

1. If the filename of a WAV file defined using the "**custom ringtone N**" parameter matches the filename of an already installed ring tone, the phone will compare hashes and only install if the hashes differ.
2. Ring tones can be deleted from the phone by removing the respective "**custom ringtone N**" parameter from the configuration file or by deleting through the Web UI.
3. All custom ringtones will be deleted from the phone if a factory default is executed.

Additionally, the "**ringtone webui lock**" parameter can be used to restrict Web UI custom ring tone installation functionality in the User Web UI (by defining the parameter as "**1**") or restrict functionality in both the User and Administrator Web UIs (by defining the parameter as "**2**").

Note: The "**ringtone webui lock**" parameter is disabled (i.e. the Custom Ringtone menu is available in both User and Administrator Web UIs) by default.

CONFIGURING THE CUSTOM RING TONE FEATURE

Use the following procedures to configure the custom ring tone feature

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Custom Ring Tone Settings” on page A-198.

INSTALLING A CUSTOM RING TONE USING THE MITEL WEB UI

Use the following procedure to install custom ring tones using the Mitel Web UI

MITEL WEB UI

1. Click on **Basic Settings->Custom Ringtones.**

2. Press the **Browse...** button corresponding to the desired ring tone position (e.g. 1).
3. Navigate to the folder containing the WAV file you want to upload, select the file using your left mouse button, and press the **Open** button.
The filename should now be displayed to the right of the respective **Browse...** button.
4. Press the **Upload** button to upload the file to the phone.
5. Repeat Steps 2 to 4 to upload additional WAV files to the phone.

Note: Press the **Delete** button to delete the desired ring tone from your phone.

RING TONE VIA SPEAKER DURING ACTIVE CALLS

The parameter “**ring audibly enable**” can be used to configure the IP phones to play the ring tone of an incoming call via the phone’s speaker while in an active call.

With the parameter enabled, if a user is in an active call on an extension, and the phone receives a call for the same or different extension, the incoming call will be represented by the call’s ring tone being played through the speaker as well as the respective line’s LED flashing (if available).

If a user is in the process of dialing out to a remote number (either for an initial call or to initiate a conference or transfer) a call for the same or different extension, the call waiting tone will be played. The ring tone will be played when the phone exits the dialing state and transitions to the outgoing state.

When the phone exits the incoming ringing state (e.g. the incoming call is answered), the tone device of the phone will revert back to originally configured audio device.

Notes:

1. The "**ring audibly enable**" parameter is disabled by default.
2. This feature is not supported when utilizing the headset audio mode.
3. With this feature enabled and when the phone's speaker is playing the incoming call's ring tone, call-waiting tones will not be played.

CONFIGURING THE RING TONE VIA SPEAKER DURING ACTIVE CALLS FEATURE

Use the following procedures to configure the ring tone via speaker during active calls feature.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Ring Tone via Speaker During Active Calls Settings" on page A-199.

INDIVIDUAL CONTACT RING TONE SUPPORT

Individual contact ring tones are supported by the 6800 and 6900 series SIP phones. Individual contact ring tones can be used during incoming calls to help users identify the party calling. Users are now able to select contact-specific ring tones (from the phone's 15 preloaded as well as the 8 custom ring tones) for respective contacts in their local directory, which will be played back when a call from the respective contact is incoming.

Individual contact ring tone support is dependent on the phone's directory lookup functionality. During an incoming call, the local directory is examined against the phone number of the incoming call. If a match is found and the contact has an associated contact ring tone, the contact ring tone is played. If a match is not found or if a contact ringtone is not assigned, the standard ring tone for the line being used to field the incoming call is played.

Notes:

1. The individual contact ring tone feature is compatible with the directory loose matching feature described in "Directory Loose Number Matching," on page 311.
2. In instances where a custom ring tone is selected as the individual contact ring tone for a local directory contact and subsequently the custom ring tone is deleted, the standard ring tone will be played.
3. Downgrading to a firmware lower than Release 4.3.0 SP1 and then upgrading back to Release 4.3.0 SP1 or greater will cause the individual contact ring tone settings to be lost.

As individual contact ring tone support is applicable to the local directory, users that would like to apply a ring tone for a contact in an external directory source (e.g. CSV-based directories, Exchange Contacts, LDAP, and Xsi directories) or Received Callers List/Outgoing Redial List must first copy the desired contact to the local directory. Users can also manually create a local directory contact or edit an existing local directory contact to assign an individual contact ring tone. For details on how to create a new local directory contact, edit an existing local directory contact, copy a contact from an external source directory or list, and assign individual contact ring tones, refer to your *Mitel Model-Specific SIP Phone User Guide*.

NO SERVICE CONGESTION TONE

Administrators can configure the IP phones to play a congestion/fast busy tone instead of a dial tone when the phone is in a "No Service" state. This feature allows visually impaired persons the ability to discern whether or not the phone is in service and can be used to send/receive calls.

The configuration parameter "**no service congestion tone**" allows administrators the ability to enable this accessibility feature. When enabled, the congestion tone will replace the conventional dial tone when the handset is off hook, a headset is employed, or the speakerphone is engaged. The congestion tone's frequency/pattern is based on the respective phone's configured tone set. Additionally, the congestion tone is played on a per-line basis whereby only the specific lines that are without service are affected.

Note: If the phone or individual lines are configured to have no registration by intent (e.g. if the Registrar is set to 0.0.0.0) enabling the "**no service congestion tone**" parameter will have no effect and the default dial tone will be played.

With consideration to scenarios where a dial tone should be played even if the phone is in a "No Service" state (e.g. scenarios where the proxy may still accept INVITEs from the phone even if unregistered), the "**no service congestion tone**" parameter has been programmed as disabled by default.

CONFIGURING THE NO SERVICE CONGESTION TONE

Use the following procedures to configure the no service congestion tone feature.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "No Service Congestion Tone Settings" on page A-200.

CUSTOM RING TONE FOR HOTDESK

When a hotdesk user sets a custom ring tone for a phone after login, the configuration is updated to that specific <user>_local.cfg file. But this ring tone is deleted after a reboot of the phone. In such cases, after the hotdesk user re-login, the phone plays the global ring tone instead of the previously configured custom ringtone unless the hotdesk user uploads the custom ringtone file on the phone again. Also, if the hotdesk user sets a custom ring tone for a phone before login, the configuration is updated in the phone's local.cfg. This ring tone is not deleted from the phone during reboot and the user shall hear the same ring tone even after phone reboot.

The global ring tone assigned after the hotdesk user logs in can be either of the following:

- "The phone's default ring tone that was selected as global ring tone by the same hotdesk user before reboot (global ring tone settings will get updated in the <user>_local.cfg file).

- "The global ring tone assigned when no hotdesk user was logged in to the phone.

PRIORITY ALERTING

Priority alerting on the IP phones is a feature that allows incoming calls to trigger pre-defined ringing or call waiting alert tones.

You can enable or disable priority alerting on the IP phone for the Asterisk, BroadWorks, and Sylantro servers using the configuration files and the Mitel Web UI. Configuration of priority alerting is on a global-basis only.

HOW PRIORITY ALERTING WORKS

When the IP phone detects an incoming call, the phone firmware inspects the INVITE request in the IP packet for an "Alert-Info" header.

If it contains an "Alert-Info" header, the firmware strips out the URL and keyword parameter and maps it to the appropriate Bellcore tone.

If there is no keyword parameter in the "Alert-Info" header, or the INVITE message contains no "Alert-Info" header, then the IP phone firmware uses the Bellcore standard ring tone.

Asterisk/BroadWorks Servers

The ring tone keywords that can display in the "Alert-Info" header for an Asterisk and BroadWorks server are:

- Bellcore-dr2
- Bellcore-dr3
- Bellcore-dr4
- Bellcore-dr5

Note: If the Alert-Info header contains <urn:alert:source:external> keyword, it will play Bellcore-dr2 ringtone.
If the Alert-Info header contains <urn:alert:service:recall:callback> keyword, it will play Bellcore-dr3 ringtone.

When the ring tone keywords appear in an "Alert-Info" header from an Asterisk or BroadWorks server, the IP phone maps the keywords to the default ring tone patterns.

Example:

The following are examples of the Asterisk/BroadWorks Server ring tone keywords:

```
Alert-Info: <http://127.0.0.1/Bellcore-dr2>
or
Alert-Info: <Bellcore-dr2>
```

Sylantro Servers

The ring tone keywords that can display in the "Alert-Info" header for a Sylantro server are:

- alert-acd (auto call distribution)
- alert-community-1
- alert-community-2
- alert-community-3
- alert-community-4
- alert-emergency
- alert-external
- alert-group
- alert-internal
- alert-priority

When the ring tone keywords appear in an "Alert-Info" header from a Sylantro server, the keyword is mapped to the ring tone pattern based on the configuration you set in the Mitel Web UI or the configuration files.

RING TONE PATTERNS

In IP Telephony, different ringing patterns have different frequencies and cadences. Ring cadence is the ringing pattern heard by the called party, before they pick up the call.

On the IP phones, if you enable priority alerting when using an Asterisk or BroadWorks server, the IP phone uses the following Bellcore-specified tones by default:

Ring Tone Pattern (Asterisk/BroadWorks Servers)

CALL CRITERIA	BELLCORE TONES
internal calls	Bellcore-dr2
external calls	Bellcore-dr3
calls with contact list	Bellcore-dr4
calls with specific time frames	Bellcore-dr5

If you enable priority alerting when using a Sylantro server, you can specify the Bellcore tone to be used for the following configurable criteria:

Ring Tone Pattern (Sylantro Servers)

CALL CRITERIA	BELLCORE TONES FOR EACH CALL CRITERIA
alert-acd (auto call distribution)	Normal ringing (default)
alert-community-1	Bellcore-dr2
alert-community-2	Bellcore-dr3
alert-community-3	Bellcore-dr4
alert-community-4	Bellcore-dr5
alert-emergency	Silent
alert-external	
alert-group	
alert-internal	
alert-priority	

A System Administrator can configure the ring tone cadences if required, using the configuration files. The following table identifies the different Bellcore ring tone patterns and cadences.

BELLCORE TONE	PATTERN ID	PATTERN	CADENCE	MINIMUM DURATION (MS)	NOMINAL DURATION (MS)	MAXIMUM DURATION (MS)
(Standard)	1	Ringing	2s On	1800	2000	2200
		Silent	4s Off	3600	4000	4400
Bellcore-dr2	2	Ringing	Long	630	800	1025
		Silent		315	400	525
		Ringing	Long	630	800	1025
		Silent	Long	3475	4000	4400
Bellcore-dr3	3	Ringing	Short	315	400	525
		Silent		145	200	525
		Ringing	Short	315	400	525
		Silent		145	200	525
		Ringing	Long	630	800	1025
		Silent		2975	4000	4400
Bellcore-dr4	4	Ringing	Short	200	300	525
		Silent		145	200	525
		Ringing	Long	800	1000	1100
		Silent		145	200	525
		Ringing	Short	200	300	525
		Silent		2975	4000	4400
Bellcore-dr5	5	Ringing		450	500	550

Note: If the "Do Not Disturb" (DND) or the "Call Forward" (CFWD) feature is enabled on the server-side, and the user is still waiting for a call, the "Bellcore-dr5" is a ring splash tone that reminds the user that these are enabled.

CONFIGURING PRIORITY ALERTING AND RING TONE CADENCES USING THE CONFIGURATION FILES

Use the following procedures to configure priority alerting and ring tone cadences on the IP phones.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the sections,

- "Priority Alert Settings" on page A-207.
- "Bellcore Cadence Settings" on page A-212.

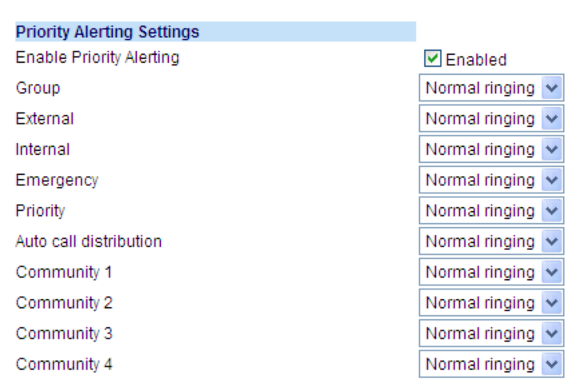
Note: You can configure Bellcore cadences using the configuration files only.

CONFIGURING PRIORITY ALERTING USING THE MITEL WEB UI

Use the following procedure to configure Priority Alerting using the Mitel Web UI.

MITEL WEB UI

1. Click on **Basic Settings->Preferences**.



2. In the "Priority Alerting Settings" section, enable the "**Enable Priority Alerting**" field by checking the check box. (Disable this field by unchecking the box).

For Sylantro Servers:

3. Select a ring tone pattern for each of the following fields:

- Group
- External

- Internal
- Emergency
- Priority
- Auto call distribution
- Community 1
- Community 2
- Community 3
- Community 4

4. Click **Save Settings** to save your changes.

CALL WAITING TONES

Call Waiting is a feature that tells you if a new caller is trying to contact you when you are already on the phone. A discreet tone alerts you to the new caller, so you can answer your second incoming call by putting your first caller on hold.

The IP phones use the following Bellcore-specified call waiting tones.

BELLCORE CALL-WAITING TONE	PATTERN ID	PATTERN	MINIMUM DURATION (MS)	NOMINAL DURATION (MS)	MAXIMUM DURATION (MS)
CallWaitingTone 1	1	Tone On	270	300	330
Bellcore-dr2 CallWaitingTone2	2	Tone On	90	100	110
		Tone Off	90	100	110
Bellcore-dr3 CallWaitingTone3	3	Tone On	90	100	110
		Tone Off	90	100	110
		Tone On	90	100	110
Bellcore-dr4 CallWaitingTone4	4	Tone On	90	100	110
		Tone Off	90	100	110
		Tone On	270	300	330

For Asterisk and BroadWorks servers, call waiting tones are specified by the default Bellcore tones indicated in the table Ring Tone Pattern (Asterisk/BroadWorks Servers) on page 146.

For Sylantro servers, call waiting tones are specified by the Bellcore tones you configure in the Mitel Web UI or the configuration files. See the table Ring Tone Pattern (Sylantro Servers) on page 147.

Reference

For more information about enable/disabling call waiting on the IP Phone, see the section, “Call Waiting” on page 5-87.

DIRECTED CALL PICKUP (BLF OR XML CALL INTERCEPTION)

Note: Feature availability is dependent on your call manager.

Directed call pickup is a feature on the phones that allows a user to intercept a call on a ringing phone which is part of the same interception group. The 6865i, 6867i, 6869i, 6873i IP phones also support the Busy Lamp Field (BLF) hold state that is expressed by a slow flashing LED or a BLF hold icon. When using an Asterisk server, if administrators configure BLF for Directed Call Pickup, users are able to pickup the held call, as the phone sends the directed call pickup prefix to the extension number.

You can use the Directed call pickup feature on the phone in multiple ways:

- With the existing BLF feature on Asterisk or sipXecs, a user can dial "*76" or "*78" respectively, followed by the extension to pick up a ringing call on another phone. (For more information about BLF, see "Busy Lamp Field (BLF)" on page 190.
- Using XML, a user can intercept a call by selecting an extension from a list and then pressing a "Pickup" softkey/programmable key. To use the Directed call pickup feature from an XML application, you must list all ringing extensions using the **AastraIPPhoneTextMenu** XML object in an XML script. This allows the user to select the ringing extension from a text menu without having to dial.

BLF and XML softkeys/programmable keys monitor the states of an extension. The extension states can be one of three states: "busy", "ringing" and "idle". If the monitored extension is in the "ringing" state with an incoming call, and "Directed call pickup" is enabled, pressing the BLF or XML key can pick up the incoming call on the monitored extension.

REFERENCE

For more information about using the **AastraIPPhoneTextMenu** object, contact Mitel Customer Support regarding the ***XML Development Guide***.

DIRECTED CALL PICKUP PREFIX (OPTIONAL)

The optional "directed call pickup prefix" allows you to enter a specific prefix string (depending on what is available on your server), that the phone automatically dials when dialing the Directed Call Pickup number. For example, for BroadSoft servers, you can enter a value of *98 for the "directed call pickup prefix" (for sipXecs, *78 is used). When the phone performs the Directed Call Pickup after pressing a BLF or BLF/List softkey, the phone prepends the *98 value to the designated extension of the BLF or BLF/List softkey when dialing out.

How this Feature Works when Directed Call Pickup is Enabled with BLF or BLF/List

1. Phone A monitors Phone B via BLF/List.
2. Phone C calls Phone B; Phone B rings.
3. If you press the BLF/List softkey on Phone A, it picks up the ringing line on Phone B.
4. Phone C connects to Phone A.

How this Feature Works when Directed Call Pickup is Disabled with BLF or BLF/List

1. Phone A monitors Phone B via BLF/List.
2. Phone C calls Phone B; Phone B rings
3. If you press the BLF/List softkey on Phone A, it performs a speeddial to Phone B.
4. Phone C and Phone A are ringing Phone B on separate lines (if available).

Notes:

1. The default method for the phone to use is Directed Call Pickup over BLF if the server provides applicable information. If the Directed Call Pickup over BLF information is missing in the messages to the server, the Directed Call Pickup by Prefix method is used if a value for the prefix code exists in the configuration.
2. You can define only one prefix, which will be applicable to all BLF- or BLF/List-monitored extensions.
3. The phone that picks up displays the prefix code + the extension number (for example, *981234 where prefix key = *98, extension = 1234).

You can enable/disable “Directed Call Pickup” using the configuration files or the Mitel Web UI.

Note: The “Directed Call Pickup” feature is disabled by default.

ENABLING/DISABLING DIRECTED CALL PICKUP

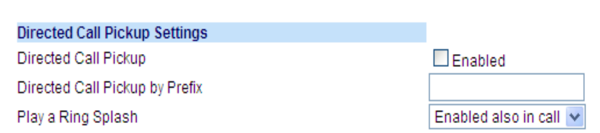
Use the following procedure to enable or disable the Directed Call Pickup feature on the IP phone.

CONFIGURATION FILES

To enable/disable Directed Call Pickup on the IP phone using the configuration files, see Appendix A, the section, “Directed Call Pickup (BLF or XML Call Interception) Settings” on page A-238.

MITEL WEB UI

1. Click on **Basic Settings->Preferences->Directed Call Pickup Settings.**



2. Enable the "**Directed Call Pickup**" field by checking the check box.
   (Disable this field by unchecking the box). Default is disabled.)
3. (Optional) Enter a prefix in the "**Directed Call Pickup Prefix**" field. For example, *98.
   This prefix is appended to the beginning of the Directed Call Pickup number when dialed from the BLF or BLF/List softkey.

4. Enable the "**Play a Ring Splash**" feature by selecting either Enabled (when idle) or Enabled also in call (when idle and in an active call state. (Default is disabled).
5. If the "**Play a Ring Splash**" parameter is enabled, the IP phone plays a short "ring splash" when there is an incoming call on the BLF monitored extension.
6. Click **Save Settings** to save your changes.

CONFIGURING BLF OR BLF/LIST FOR DIRECTED CALL PICKUP

Use the following procedure to configure BLF or BLF/List for Directed Call Pickup in the configuration files.

Note: You must enable Directed Call Pickup before performing these procedures. See "Enabling/Disabling Directed Call Pickup" on page 5-151

CONFIGURATION FILES

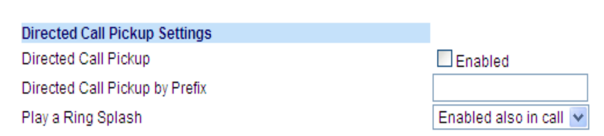
To set BLF or BLF/List in the configuration files for Directed Call Pickup, see Appendix A, the sections:

- "Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters" on page A-248.
- "BLF List URI Settings" on page A-292.

Use the following procedure to configure BLF or BLF/List for Directed Call Pickup in the Mitel Web UI.

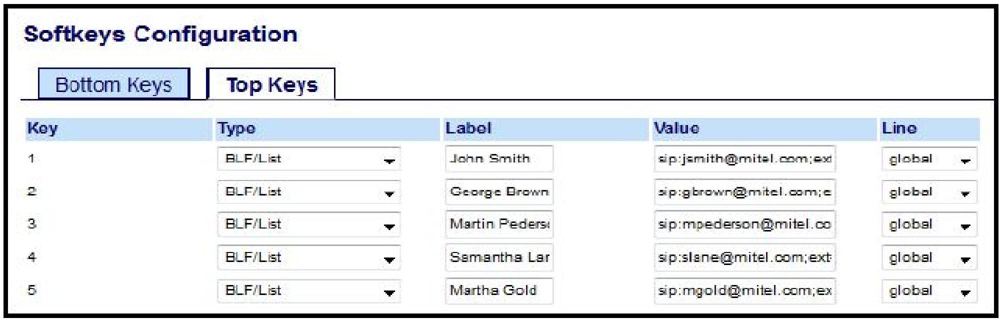
MITEL WEB UI

1. Click on **Basic Settings->Preferences->Directed Call Pickup Settings.**



2. Enable the "**Directed Call Pickup**" field by checking the check box.
3. (optional) Enter a prefix in the "**Directed Call Pickup Prefix**" field. For example, *98. This prefix is appended to the beginning of the Directed Call Pickup number when dialed from the BLF or BLF/List softkey.
4. Enable the "**Play a Ring Splash**" feature by selecting either Enabled (when idle) or Enabled also in call (when idle and in an active call state. (Default is disabled).
If the "**Play a Ring Splash**" parameter is enabled, the IP phone plays a short "ring splash" when there is an incoming call on the BLF monitored extension.

5. Click on **Operation->Softkeys and XML**
   or
   Click on **Operation->Programmable Keys**
   or
   Click on **Operation->Expansion Module <N>**



Note: Depending on your phone-model, the key configuration screen displays.

6. Select a softkey or programmable key to configure.
7. In the "**Type**" field, select "**BLF**" (Asterisk), "**BLF/List**" (BroadSoft BroadWorks).
8. (For the 6867i/6869i/6873i/6920/6930/6940/6970 softkeys) In the "**Label**" field, enter the name of the person who's extension you are monitoring.

Note: If BLF/List type is selected, the label value is optional. If a label is:

1. Configured, then the label name is shown and labels from SIP NOTIFY name are ignored.
2. Not configured, then the label name is shown based on SIP NOTIFY name. In some cases if a label is not configured, the label will be displayed as a series of question marks (i.e. ???) until it is updated with the appropriate data from the call manager.

9. In the "**Value**" field, enter a value to associate with the softkey or programmable key.
   For example, for BLF, the value is the extension you want to monitor.
   For BLF/List, enter the BLF/List target's resource URI, using the following syntax:
   `sip:username@domain.com;ext=extension number`
   whereby the "username@domain.com" is identical to the resource URI of the BLF/List key configured on the call manager and the "extension number" (an optional value) corresponds to the target's extension number.

Note: If a resource URI is not defined in the **Value** field, the key will be automatically populated using the first resource entry from the BLF/List NOTIFY data that has not already been populated (either manually or automatically).

10. Click **Save Settings** to save your changes.
11. In the "**Line**" field, select a line number that is actively registered to the appropriate SIP proxy you are using.

12. In the "**BLF List URI**" field, enter the name of the BLF list defined on the BroadSoft BroadWorks Busy Lamp Field page for your particular user.
    For example, sip:9@192.168.104.13.

> **Note:** The value of the BLF/List URI parameter must match the list name configured. Otherwise, no values display on the screen and the feature is disabled.

13. Select the line state (idle, connected, incoming, outgoing, busy) that you want to apply to the BLF softkey or programmable key.
14. Click **Save Settings** to save your changes.

CONFIGURING XML FOR DIRECTED CALL PICKUP

Use the following procedure to configure XML for Directed Call Pickup in the configuration files.

> **Notes:**
> 1. Before implementing this procedure, you must create an XML application that the phone uses when the XML softkey or programmable key is pressed. This XML application must be entered as a URI in the "Value" field of the XML key. For information about creating an XML script, see the ***XML Developer's Guide***.
> 2. You must enable Directed Call Pickup before performing these procedures. See "Enabling/Disabling Directed Call Pickup" on page 5-151.

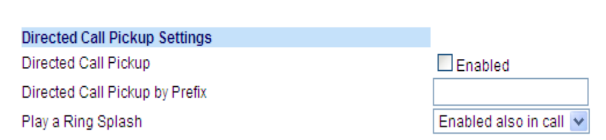
CONFIGURATION FILES

To set XML in the configuration files for Directed Call Pickup, see Appendix A, the section, "Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters" on page A-248.

Use the following procedure to configure XML for Directed Call Pickup in the Mitel Web UI.

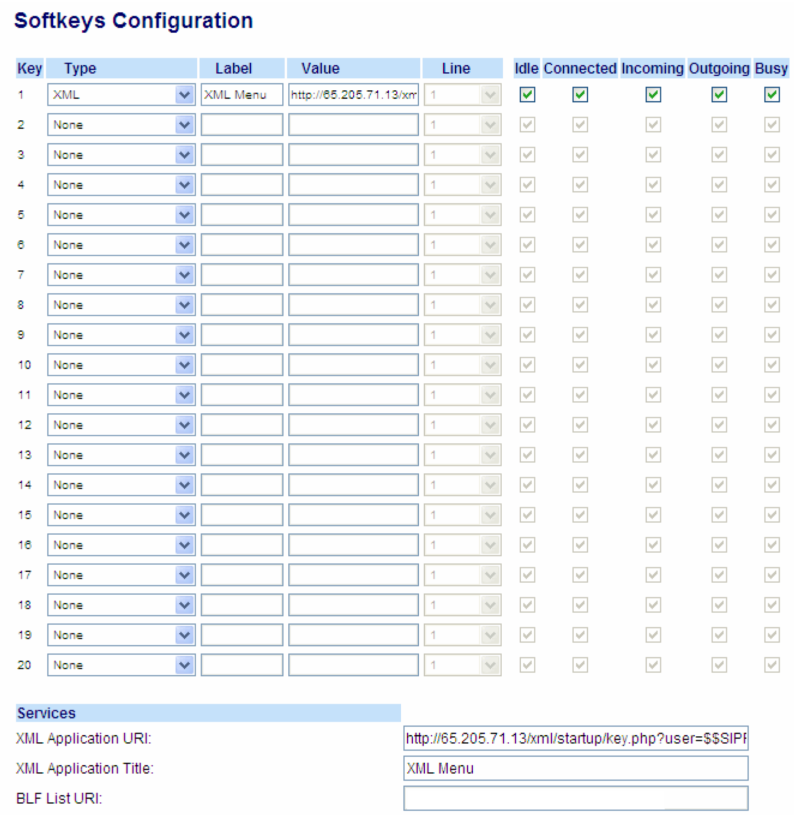
MITEL WEB UI

1. Click on **Basic Settings->Preferences->Directed Call Pickup Settings.**



2. Enable the "**Directed Call Pickup**" field by checking the check box.
3. (Optional) Enter a prefix in the "**Directed Call Pickup Prefix**" field. For example, *98. This prefix is appended to the beginning of the Directed Call Pickup number when dialed from the BLF or BLF/List softkey.
4. Enable the "**Play a Ring Splash**" feature by selecting either Enabled (when idle) or Enabled also in call (when idle and in an active call state. (Default is disabled).
   If the "**Play a Ring Splash**" parameter is enabled, the IP phone plays a short "ring splash" when there is an incoming call on the BLF monitored extension.

5. Click on **Operation->Softkeys and XML**
or
Click on **Operation->Programmable Keys**
or
Click on **Operation->Expansion Module <N>.**



Note: Depending on your phone-model, the key configuration screen displays

6. Select a softkey or programmable key to configure.

7. In the "**Type**" field, select "**XML**".

8. (For the 6867i/6869i/6873i Softkeys) In the "**Label**" field, enter the name of the person whose extension you are monitoring.

9. In the "**Value**" field, enter the URI that the phone uses to display the XML application to the LCD.
For example, http://65.205.71.13/xml/startup/key.php?user=$$SIPREMOTENUMBER$$.

Note: For more information about creating an XML script to use with Directed Call Pickup, see the ***XML Developer's Guide***.

10. Select the line state (idle, connected, incoming, outgoing, busy) that you want to apply to the XML softkey or programmable key.

11. Click **Save Settings** to save your changes.

TWO-STAGE BLF KEY DIRECTED CALL PICKUP SUPPORT

Notes:

1. Feature compatibility is dependent on your call manager. To display the caller details, your call manager must support the local and remote identity tags as described in RFC 4235, Section 4.1.1. Dialog Element (refer to Section 4.2. Sample Notification Body for an example NOTIFY body). To pick up the call after displaying the caller details, your call manager must support the SIP "Replaces" header as detailed in RFC 3891.
2. Applicable to the 6865i, 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones only.

With the directed call pickup feature configured, pressing on the ringing BLF softkey will simply pick up the ringing line on the BLF-monitored phone. Administrators can configure the "**enhanced directed call pickup**" parameter to change the behavior so that pressing the BLF softkey will first display the remote caller's information (i.e. name, number, and picture ID [if applicable]) on screen allowing users to review the remote caller's details before acting upon the call.

After checking the remote caller's information, users are able to press the BLF softkey again (or "Pickup" key) to pick up the ringing line on the BLF-monitored phone, or simply ignore/cancel the call.

Configuring the Two-Stage BLF Key Directed Call Pickup Feature

Use the following procedure to configure the two-stage BLF key directed call pickup feature in the configuration files.

CONFIGURATION FILES

To enable/disable the two-stage BLF key directed call pickup feature on the IP phone using the configuration files, see Appendix A, the section, "Directed Call Pickup (BLF or XML Call Interception) Settings" on page A-238.

MICLOUD TELEPO DIRECTED CALL PICKUP SUPPORT

Improvements have been made with regards to the directed call pickup feature specifically for interoperability with the MiCloud Telepo for Service Providers call manager.

For MiCloud Telepo interoperability, the directed call pickup feature must be enabled (i.e. the "**directed call pickup**" parameter must be defined as "**1**") and the "**enhanced directed call pickup**" parameter must be defined as "**3**".

In this enhanced directed call pickup mode, pressing a BLF key when the monitored extension is ringing will cause the phone use the dialog information sent in the NOTIFY message to form the INVITE request (the dialog information will be detailed in the "Replaces" header of the INVITE).

Enabling MiCloud Telepo Directed Call Pickup Support

Use the following procedure to enable MiCloud Telepo directed call pickup support in the configuration files.

CONFIGURATION FILES

To enable MiCloud Telepo directed call pickup support using the configuration files, see Appendix A, the section, "Directed Call Pickup (BLF or XML Call Interception) Settings" on page A-238.

SOFTKEYS/PROGRAMMABLE KEYS/EXPANSION MODULE KEYS

You can configure the softkeys, programmable keys, and expansion module keys that are applicable to a specific phone model, to perform specific functions on the IP phones.

Notes:

1. When entering definitions for softkeys in the configuration files, the "#" sign must be enclosed in quotes.
2. Use "topsoftkeyN" when defining top softkey parameters and "softkeyN" when defining bottom softkey parameters.

SOFTKEYS

The following table provides the number of softkeys you can configure, and the number of lines available for each phone model that has configurable softkeys.

IP PHONE MODEL	SOFTKEYS	EXPANSION MODULE KEYS	LINES AVAILABLE
6867i	6 top (maximum of 20 functions) 4 bottom (maximum of 18 functions)	16 to 48* (Model M680i) 84 to 252** (Model (M685i)	24
6869i	12 top (maximum of 44 functions) 5 bottom (maximum of 24 functions)	16 to 48* (Model M680i) 84 to 252** (Model (M685i)	24
6873i	12 top (maximum of 48 functions) 6 bottom (maximum of 30 functions)	16 to 48* (Model M680i) 84 to 252** (Model (M685i)	24

*The M680i expansion module consists of 16 softkeys. You can have up to 3 expansion modules on an IP phone totaling 48 softkeys. Valid for 6865i, 6867i, 6869i and 6873i phones.

**The M685i expansion module consists of 3 pages of 28 softkeys (for a total of 84). You can have up to 3 expansion modules on an IP phone totaling 252 softkeys. Valid for 6865i, 6867i, 6869i, 6873i phones.

STATE-BASED SOFTKEYS (BOTTOM SOFTKEYS ONLY)

Users and administrators can configure a specific state to display when a softkey is being used. Available states you can configure for each softkey include:

- **idle** - The phone is not being used.
- **connected** - The current line is in an active call (or the call is on hold)
- **incoming** - The phone is ringing.
- **outgoing** - The user is dialing a number, or the far-end is ringing.
- **busy** - The current line is busy because the line is in use or the line is set as “Do Not Disturb”.

The following table identifies the applicable default states for each type of softkey you can configure on the IP phone. Availability of the types is dependent on your IP phone model.

SOFTKEY TYPE	DEFAULT STATES
None	All states disabled.
Speeddial	idle, connected, incoming, outgoing, busy
DND	idle, connected, incoming, outgoing, busy
XML	idle, connected, incoming, outgoing, busy
Flash	All states disabled.
Sprecode	connected
Park	connected
Pickup	idle, outgoing
Last Call Return	idle, connected, incoming, outgoing, busy
Call Forward	idle, connected, incoming, outgoing, busy
Speeddial/Xfer	idle, connected, incoming, outgoing, busy
Speeddial/Conf	idle, connected, incoming, outgoing, busy
Directory	idle, connected, incoming, outgoing, busy
Filter	idle, connected, incoming, outgoing, busy
Received Callers List	idle, connected, incoming, outgoing, busy
Redial	idle, connected, incoming, outgoing, busy
Conference	idle, connected, incoming, outgoing, busy
Transfer	idle, connected, incoming, outgoing, busy
Icom (Intercom)	idle, connected, incoming, outgoing, busy
Phone Lock	All states disabled.
Paging	All states disabled.
Login	idle, connected, incoming, outgoing, busy
Discreet Ringing	idle, connected, incoming, outgoing, busy
Hold	idle, connected, incoming, outgoing, busy
Empty	idle, connected, incoming, outgoing, busy

You can enable or disable the softkey states using the configuration files or the Mitel Web UI. In the Mitel Web UI, you disable a state by unchecking the box for that operational state.

In the configuration files, you use the following parameters to enable and disable operational states:

- softkeyN states

You can enter multiple values (**idle, connected, incoming, outgoing, busy**) for the "**softkeyN state**" parameter. For example:

```
softkeyN states: idle connected
```

You must associate the softkeyN state parameter with a specific softkey. In the following example, the softkeyN states parameter is associated with softkey 12:

```
softkey12 type: speeddial
softkey12 label: voicemail
softkey12 value *89
softkey12 states: outgoing
```

Notes:

1. By default the IP phone idle screen collapses the softkeys. So in the previous example, softkey 12 will appear in position 1 if no other softkeys are set.
2. A softkey type of "empty" does not display on the idle screen at all. For more information about the softkey type of "empty" see Appendix A, the section, "Softkey Settings" on page 249.

CONFIGURATION EXAMPLE

The following example illustrates the use of the "**softkeyN states**" parameter, and the "**softkeyN type**" parameter with a value of **empty**. For clarity purposes, only the "**softkeyN type**" and "**softkeyN states**" parameters are shown.

```
softkey1 type: callers
softkey1 states: idle connected

softkey3 type: dnd
softkey3 states: idle

softkey4 type: redial

softkey5 type: empty
softkey5 states: connected

softkey6 type: speeddial
softkey6 states: connected
```

The following table shows how the keys in the example above would display on the IP Phone UI.

Note: The "**empty**" key type allows a softkey to be removed quickly by deleting the softkey information from the configuration file.

SOFTKEY	IDLE	CONNECTED	NOTES
softkey1	Key 1	Key 2	Received Callers List displays for softkey1. Key 1 in connected state is the Drop key. Idle and connected display as applicable.
softkey2	(not used)	(not used)	Softkey2 is not displayed.
softkey3	Key 2	(not used)	DND displays for softkey3. Idle displays as applicable.
softkey4	Key 3	Key 3	Redial displays for softkey4. Default state values (idle, connected, incoming, outgoing, busy) display as applicable.

softkey5	(not used)	Key 4 (blank)	A blank displays for softkey5. Connected displays as applicable.
softkey6	(not used)	Key 5	Speeddial displays for softkey6. Connected displays as applicable.

Softkeys and programmable keys are configurable using the Mitel Web UI or the configuration files.

PROGRAMMABLE KEYS

The following table provides the number of softkeys and programmable keys you can configure, and the number of lines available for each type of phone that has programmable keys.

IP PHONE MODEL	EXPANSION MODULE KEYS	PROGRAMMABLE KEYS	LINES AVAILABLE
6863i/ 6905	N/A	3	2
6865i/ 6910	16 to 48* (Model M680i) 84 to 252** (Model (M685i)	8	24

*The M680i expansion module consists of 16 softkeys. You can have up to 3 expansion modules on an IP phone totaling 48 softkeys.

**The M685i expansion module consists of 3 pages of 28 softkeys (for a total of 84). You can have up to 3 expansion modules on an IP phone totaling 252 softkeys.

SOFTKEY/PROGRAMMABLE KEY/EXPANSION MODULE KEY FUNCTIONS

You can configure the softkeys and programmable keys on the phones and any attached expansion module keys to perform specific functions using the configuration files or the Mitel Web UI. The following table identifies the available functions of the softkeys, programmable keys, and expansion module keys on the IP phones. Available functions may vary on each model phone.

Note: Availability of the functions is dependent on your IP phone model as well as whether the softkey is a top or bottom softkey. See your ***<Model-Specific> SIP Phone User Guide*** for details.

Key Functions Table

SOFTKEY/ PROGRAMMABLE KEY FUNCTION	CONFIGURATION FILE PARAMETER	MITEL WEB UI PARAMETER	DESCRIPTION
None	none	None	Indicates not setting for the key.
Line	line	Line	Indicates the key is configured for line use.
Speeddial	speeddial	Speeddial	Indicates the key is configured for speeddial use. You can configure a softkey to speeddial a specific number. Optionally, you can also configure a Speeddial key to dial prefix numbers. With this option, the prefix numbers automatically dial when you press the softkey, and the phone waits for you to enter the remaining numbers to dial out. For more information about speeddial prefixes, see "Speeddial Prefixes" on page 5-189. You can also create Speeddial keys and edit the keys using the IP Phone keypad. For more information about Speeddial keys and editing Speeddial keys, see your <Model-Specific> ***SIP Phone User Guide*** for more information.
Busy Lamp Field (BLF)	blf	BLF	Indicates the key is configured for Busy Lamp Field (BLF) use. A user can dial out on a BLF configured key. You can also set a BLF subscription period. For more information about BLF, see the section "Busy Lamp Field (BLF)" on page 5-190. For more information about BLF Subscription Period, see "BLF Subscription Period" on page 5-200.
Busy Lamp Field List	list	BLF/List	Indicates the key is configured for BLF list use. A user can dial out on a BLF/List configured key. For more information on BLF, see the section "Busy Lamp Field (BLF)" on page 5-190.

SOFTKEY/ PROGRAMMABLE KEY FUNCTION	CONFIGURATION FILE PARAMETER	MITEL WEB UI PARAMETER	DESCRIPTION
Auto Call Distribution (ACD)	acd	Auto Call Distribution	(For Sylantro/BroadWorks servers) Indicates the key is configured for automatic call distribution (ACD). ACD allows the Sylantro/BroadWorks server to distribute calls from a queue to registered IP Phones (agents). You can also set an ACD subscription period. For more information about ACD, see the section "Automatic Call Distribution (ACD) (for Sylantro/BroadWorks Servers)" on page 5-213. For more information about ACD subscription period, see "ACD Subscription Period" on page 5-217.
Do Not Disturb (DND)	dnd	Do Not Disturb	Indicates key is configured for "do not disturb" use. For more information on DND, see the section "Do Not Disturb (DND)" on page 5-218.
Extensible Markup Language) (XML)	xml	XML	Indicates the key is configured to accept an XML application for accessing customized XML services. You can also specify a URL for an XML key. For more information on XML, see the section "XML Customized Services" on page 5-316.
Flash	flash	Flash	Indicates the key is set to generate a flash event when it is pressed. The IP phone generates flash events only when a call is connected and there is an active RTP stream (for example, when the call is not on hold). For more information about the Flash key, see your <Model-Specific> ***SIP Phone User Guide***.
Sprecode	spre	Sprecode	Indicates the key is set to automatically activate specific services offered by the server. For example, if the sprecode value of *82 is configured, then by pressing the key, *82 automatically activates a service provided by the server. The value you enter for this field is dependent on the services provided by the server. For more information about the Sprecode key, see your <Model-Specific> ***SIP Phone User Guide***.

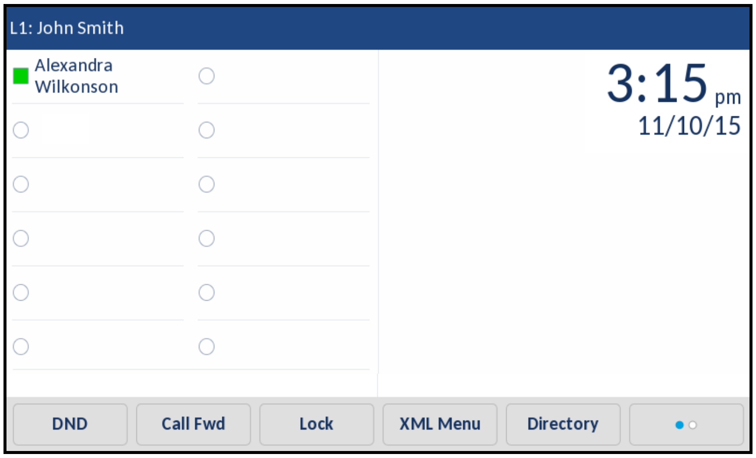
SOFTKEY/ PROGRAMMABLE KEY FUNCTION	CONFIGURATION FILE PARAMETER	MITEL WEB UI PARAMETER	DESCRIPTION
Park	park	Park	Indicates the key is set to be used as a park key to park an incoming call. For more information on park, see the section "Park/Pick Up Static and Programmable Configuration" on page 5-241.
Pickup	pickup	Pickup	Indicates the key is set to be used as a pickup key to pick up a parked call. For more information on pickup, see the section "Park/Pick Up Static and Programmable Configuration" on page 5-241.
Last Call Return (LCR)	lcr	Last Call Return	(For Sylantro Servers) Indicates the key is set to be used to dial the last call that came in on that line. For more information on lcr, see the section "Last Call Return (LCR) (Sylantro Servers)" on page 5-251.
Call Forward	callforward	Call Forward	Indicates the key is set to be used to access the Call Forward menus on the phone. For more information about call forwarding, see the section "Call Forwarding" on page 5-252.
BLF/Xfer	blfxfer	BLF/Xfer	Indicates the key is set to be used as a BLF key AND as a Transfer key. For more information about the BLF/Xfer feature, see the section "BLF/Xfer and Speeddial/Xfer Keys" on page 5-202.
Speeddial/Xfer	speeddialxfer	Speeddial/Xfer	Indicates the key is set to be used as a Speeddial key AND as a Transfer key. For more information about the Speeddial/Xfer feature, see the section "BLF/Xfer and Speeddial/Xfer Keys" on page 5-202.
Speeddial/Conf	speeddialconf	Speeddial/Conf	Indicates the key is set to be used as a Speeddial key AND as a Conference key. For more information about the Speeddial/Conf feature, see the section "Speeddial/Conference Key" on page 5-206.

SOFTKEY/ PROGRAMMABLE KEY FUNCTION	CONFIGURATION FILE PARAMETER	MITEL WEB UI PARAMETER	DESCRIPTION
Speeddial/MWI	speeddialmwi	Speeddial/MWI	Indicates the key is set to be used as a Speeddial key for a voicemail account. For more information about the Speeddial/MWI feature, see the section “Speeddial/MWI Key” on page 5-208.
Directory	directory	Directory	Indicates the key is set for accessing the Directory List. For more information about the Directory List, see the section “Enhanced Directory List” on page 5-290.
Filter	filter	Filter	Indicates the key is set for activating/deactivating Executive Call Filtering. For more information about the Executive and Assistant Services feature, see the section “BroadSoft BroadWorks Executive and Assistant Services” on page 6-94.
Received Callers List	callers	Callers List	Indicates the key is set for accessing the Received Callers List. For more information on the Received Callers List, see the section “Received Callers List” on page 5-281.
Outgoing Redial List	redial	Redial	Indicates the key is configured to access the Outgoing Redial List. For more information about the Outgoing Redial List, see your <Model-Specific> ***SIP Phone User Guide***.
Conference	conf	Conference	Indicates the key is configured as a Conference key (for local conferencing). (For Sylantro and BroadSoft Servers) An Administrator can also enable centralized conferencing on the IP Phones. For more information about using the Conference key, see your <Model-Specific> ***SIP Phone User Guide***. For information about enabling centralizing conferencing, see “Centralized Conferencing (for Sylantro and BroadSoft Servers)” on page 5-349.
Transfer	xfer	Transfer	Indicates the key is configured as a Transfer key for transferring calls. For more information about using the Transfer key, see your <Model-Specific> ***SIP Phone User Guide***.

SOFTKEY/ PROGRAMMABLE KEY FUNCTION	CONFIGURATION FILE PARAMETER	MITEL WEB UI PARAMETER	DESCRIPTION
Icom	icom	Intercom	Indicates the key is set to be used as the Intercom key. For more information about using the Intercom key, see your <Model-Specific> ***SIP Phone User Guide***. For information about other Intercom features, see "Incoming/Outgoing Intercom with Auto-Answer and Barge In" on page 5-117.
Services	services	Services	Indicates the key is set to access Services, such as, Directory List, Received Callers List, Voicemail, and any other XML applications configured on the phone. For more information about using the Services key, see your <Model-Specific> ***SIP Phone User Guide***.
Phone Lock	phone lock	Phone Lock	Indicates the key is configured as a phone lock key, allowing you to press this key to lock/unlock the phone. For more information about the lock/unlock key, see "Locking IP Phone Keys" on page 5-77.
Paging	paging	Paging	Indicates the softkey is set for Group Paging on the phone. Pressing this key automatically sends a Real Time Transport Protocol (RTP) stream to pre-configured multicast addresses without involving SIP signaling. For more information about the Paging key, see "Group Paging RTP Settings" on page 5-121.
Login	hotdesklogin	Login	Indicates the key is configured as a Visitor Desk Phone (VDP) Login key. For VDP feature availability and details, please contact your System Administrator. For more information about the Login key, see "Visitor Desk Phone Support" on page 6-102.
Discreet Ringing	discreetringing	Discreet Ringing	Indicates the key is configured to toggle Discreet Ringing on/off. For more information about the Login key, see "Discreet Ringing" on page 211.

SOFTKEY/ PROGRAMMABLE KEY FUNCTION	CONFIGURATION FILE PARAMETER	MITEL WEB UI PARAMETER	DESCRIPTION
Call History	callhistory	Call History	Indicates the key is configured as a Call History key, which allow users the ability to directly access the list of all calls in the Call History.
Call Center	callcenter	Call Center	Indicates the key is configured for Xsi call center functionality.
My Status	mystatus	My Status	Indicates the key is configured for My Status functionality. For more information about the My Status key, see "Interoperability Support for XMPP-Based BroadSoft UC-ONE Services" on page 6-80.
Contacts	contacts	Contacts	Indicates the key is configured for Contact List functionality. For more information about the Contacts key, see "Interoperability Support for XMPP-Based BroadSoft UC-ONE Services" on page 6-80.
Favorite	favorite	Favorite	Indicates the key is configured for favorite contacts functionality. For more information about the Favorite key, see "Interoperability Support for XMPP-Based BroadSoft UC-ONE Services" on page 6-80.
Hold	Hold	Hold	Indicates the key is configured for call hold functionality. For more information about the Hold key, see "Hold Softkey Support" on page 5-289
Empty (Not applicable to programmable keys or expansion module keys)	empty	Empty	Indicates the key is configured to force a blank entry on the IP phone display for a specific key. If a particular key is not defined, it is ignored. For more information about empty keys, see your <Model-Specific> ***SIP Phone User Guide***.

Many softkey functions allow you to customize the label of the softkey. For the 6873i, when you define a long top softkey label, the phone will attempt (if possible) to intelligently split the label on to two lines. You can also manually split any top softkey label on to two lines by using adding two vertical bar characters (i.e. ||) in between the characters you want to split. For example, defining a top softkey label as Alexandra||Wilkonson places a carriage return after Alexandra.



Reference

For more information about key functions for your model phone, see your <Model-Specific> ***SIP Phone User Guide***.

CONFIGURING SOFTKEYS AND PROGRAMMABLE KEYS

Use the following procedures to configure the softkeys and programmable keys on the IP phone.

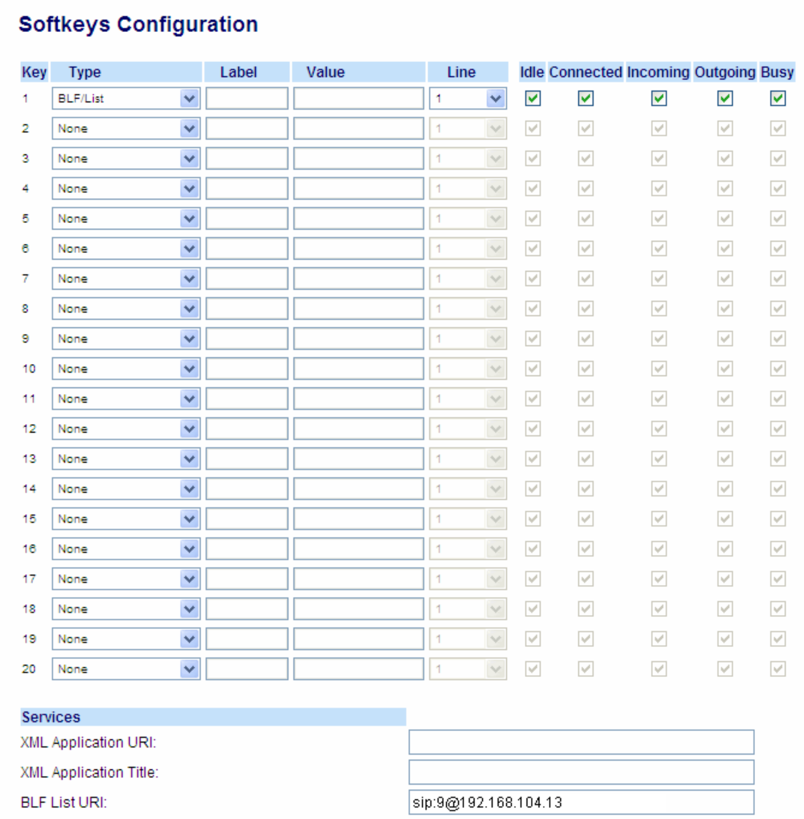
CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the sections, "Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters" on page A-248.

MITEL WEB UI

1. Click on **Operation->Softkeys and XML**
   or
   Click on **Operation->Programmable Keys**
   or

Click on **Operation->Expansion Module <N>.**
Depending on your phone-model, the key configuration screen displays.



2. Select a key to configure.

For Softkeys and Expansion Module Keys:

3. In the "**Type**" field, select the type of softkey you want to configure.

   Note: For available type values on each IP phone model, see Appendix A, the section, "Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters" on page A-248.

4. If applicable, enter a label in the "**Label**" field.

5. If applicable, in the "**Value**" field, enter a value to associate with the softkey. For example, for a Speeddial value, you can enter a number you want to use for the Speeddial key, or 12345+ as a Speeddial prefix.

6. If applicable, in the "**Line**" field, select the line for which you want to associate the softkey.

7. Some softkey types allow you to configure specific operational states.
   Operational states display to the IP phone when a softkey is used.
   To enable/disable an operational state, click the "**Idle**", "**Connected**", "**Incoming**", or "**Outgoing**" fields to check or uncheck the box.

   Note: Operational states are not applicable to expansion modules.

8. Click **Save Settings** to save your changes.

For Programmable Keys:

9. In the “**Hard Key**” field, select the programmable key type you want to configure.

Note: For available type values on each IP phone model, see Appendix A, the section, “Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters” on page A-248.

In the "**Value**" field, enter a value to associate with the programmable key. For example, for a Speeddial value, you can enter a number you want to use for the Speeddial key, or 12345+ as a Speeddial prefix.

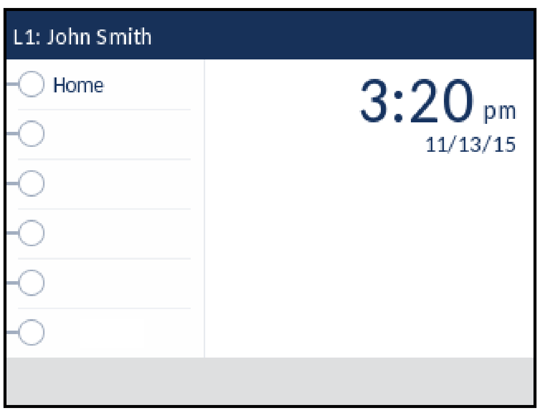
10. In the "**Line**" field, select the line for which you want to associate the programmable key.

11. Click **Save Settings** to save your changes.

CONFIGURABLE POSITIONING OF PROGRAMMED SOFTKEYS

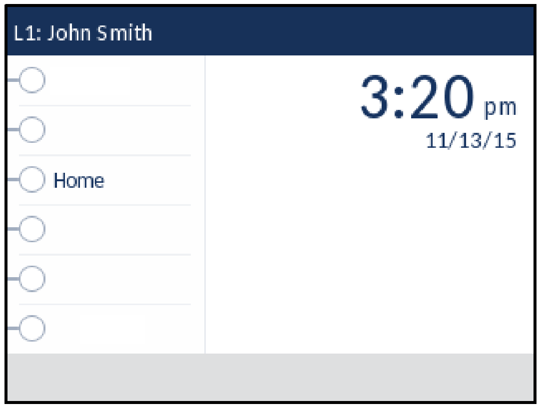
Note: Applicable to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones only.

By default, when programming softkeys for the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP phones, the softkey is automatically placed (i.e. collapses) into the first available softkey slot/position on the LCD display. For example, for the 6867i, if top softkeys 1 through 44 are set to ”None” on and top softkey 3 is programmed as a speeddial softkey with the label “Home”, after saving the settings, the “Home” speeddial softkey will appear on the first top softkey position on the LCD display.



6867i Example - Collapsed Mode (Default)

Administrators now have the option to configure programmed softkey positioning behavior. Enabling the “**collapsed softkey screen**” parameter (i.e. defining the parameter as “**1**” in the configuration files) will maintain the previous behavior (as per the example above) for the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970. Disabling the parameter (i.e. defining the parameter as “**0**”) will cause the IP phone to retain the defined position of the programmed softkey. Using the example above, if the “**collapsed softkey screen**” parameter is disabled, the “Home” speeddial softkey will retain its position appearing on the third top softkey position on the LCD display.



6869i Example - Non-Collapsed Mode

Notes:

1. The "**collapsed softkey screen**" parameter applies to both top and bottom softkeys and is enabled by default.
2. When the "**collapsed softkey screen**" parameter is disabled, bottom softkeys configured with a function that is to be displayed only in specific states will be displayed as a blank softkey in all other states. For example, if a bottom softkey is configured with speeddial functionality in the connected, incoming, outgoing, and busy states, when the phone is idle, the softkey will be blank (i.e. no label is displayed) and will not be functional.

OFFSET PARAMETERS

Complementing the "**collapsed softkey screen**" parameter are the following two additional parameters giving Administrators more control over softkey positioning:

- **collapsed softkey screen offset bottom**: Defines the offset for locking or collapsing the bottoms softkeys.
- **collapsed softkey screen offset top**: Defines the offset for locking or collapsing the top softkeys.

If the "**collapsed softkey screen**" parameter is enabled (i.e. defined as "**1**") and an offset parameter such as "**collapsed softkey screen offset bottom: 4**" is defined, the first four bottom softkeys will not be taken into consideration when collapsing (i.e. essentially locking the first four bottom softkeys and collapsing the rest).

Alternatively, the inverse is true whereby, if the "**collapsed softkey screen**" parameter is disabled (i.e. defined as "**0**") and an offset parameter such as "**collapsed softkey screen offset**

bottom: 4" is defined, all bottom softkeys except the first four will not be taken into consideration when collapsing (i.e. essentially collapsing the first four bottom softkeys and locking the rest).

Notes:

1. The range of the "offset" parameters is dependent on the SIP phone model. Values not in range will be ignored.
2. For the 6867i/6920, the range for the "**collapsed softkey screen offset bottom**" and "**collapsed softkey screen offset top**" parameters are 1 - 17 and 1 - 19 respectively.
3. For the 6869i/6930, the value for the "**collapsed softkey screen offset bottom**" and "**collapsed softkey screen offset top**" parameters are 1 - 23 and 1 - 43 respectively.
4. For the 6873i/6940/6970, the value for the "**collapsed softkey screen offset bottom**" and "**collapsed softkey screen offset top**" parameters are 1 - 23 and 1 - 47 respectively.

For example, the 6869i has a total of 24 bottom softkeys and 44 top softkeys. If the configuration file for the phone contains the following defined parameters:

```
collapsed softkey screen: 1
collapsed softkey screen offset top: 0
collapsed softkey screen offset bottom: 4
```

the phone would collapse all the top softkeys (i.e 1 - 44), lock bottom softkeys 1 - 4, and collapse the rest of the bottom softkeys (i.e. 5 - 24).

Alternatively, If the configuration file for the phone contains the following defined parameters:

```
collapsed softkey screen: 1
collapsed softkey screen offset top: 10
collapsed softkey screen offset bottom: 20
```

the phone would lock top softkeys 1 -10, collapse top softkeys 11 - 24, lock bottom softkeys 1 - 20, and collapse bottom softkeys 21 - 44.

With the collapsed softkey screen disabled the inverse would apply. If the configuration file for the phone contains the following defined parameters:

```
collapsed softkey screen: 0
collapsed softkey screen offset top: 0
collapsed softkey screen offset bottom: 4
```

the phone would lock all the top softkeys (i.e 1 - 44), collapse bottom softkeys 1 - 4, and lock the rest of the bottom softkeys (i.e. 5 - 24).

Alternatively, If the configuration file for the phone contains the following defined parameters:

```
collapsed softkey screen: 0
collapsed softkey screen offset top: 10
collapsed softkey screen offset bottom: 20
```

the phone would collapse top softkeys 1 -10, lock top softkeys 11 - 24, collapse bottom softkeys 1 - 20, and lock bottom softkeys 21 - 44.

CONFIGURING PROGRAMMED SOFTKEY POSITIONING OPTIONS

Use the following procedures to configure the programmed softkey positioning options.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Configurable Positioning of Programmed Softkeys" on page A-256.

SHIFTING OF SOFTKEY POSITIONS FOR BUSY STATES

Note: Applicable to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones only.

By default, user configured softkeys are automatically shifted from the first page of softkeys to the second page when the phone is in a busy state. Administrators have the option of "collapsing" the user configured softkeys to start on the first available softkey position after the context-sensitive softkeys during the following busy states:

- outgoing
- ringing
- connected
- hold

This feature is configured by defining the "**collapsed context user softkey screen**" parameter as "**0**" (disabled) or "**1**" (enabled) in the configuration files.

Note: The "**collapsed context user softkey screen**" parameter is disabled by default.

For Example:

During a call on a 6869i IP phone with the "**collapsed context user softkey screen**" parameter disabled and with softkey 1 configured as Park, the softkey will not appear on page 1. The user has to press the More key to access it on page 2.

During a call on a 6869i IP phone with the "**collapsed context user softkey screen**" parameter enabled Park appears on page 1 in softkey positions 4 (Drop, Conf, and Xfer situated in softkey positions 1, 2, and 3).

CONFIGURING COLLAPSED CONTEXT USER SOFTKEY SCREEN

Use the following procedures to configure the collapsed context user softkey screen.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Configurable Positioning of Programmed Softkeys" on page A-256.

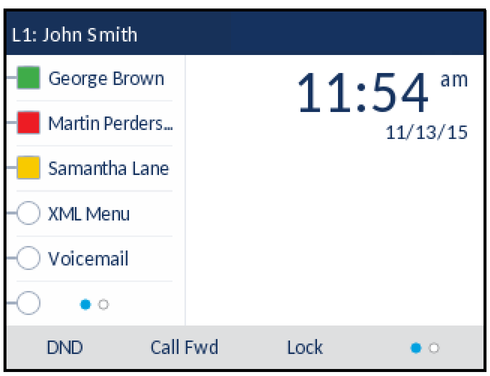
OPTION TO REMOVE THE "MORE" SOFTKEY WHEN NOT REQUIRED

Note: Applicable to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones only.

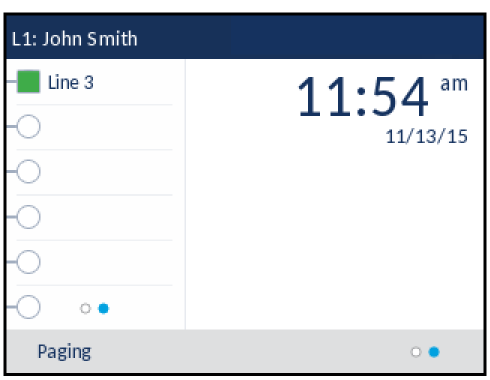
Administrators can control how softkeys are displayed on the IP phones' screens when the number of softkeys configured matches the exact number of softkey buttons on the phone.

For example, the 6867i/6920 has a total of six physical top softkey buttons and four physical bottom softkey buttons. By default, when a total of six top softkeys and four bottom softkeys are configured, the screen displays five top softkeys and three bottom softkeys along with "More" options to access the remaining softkeys.

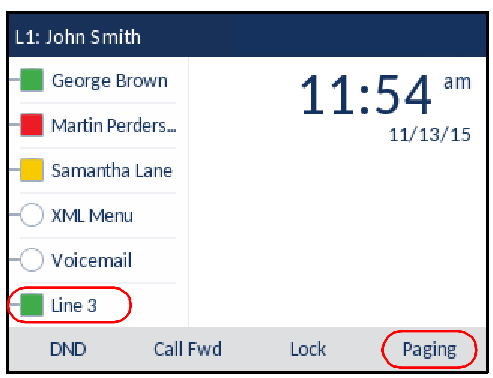
By enabling the "**collapsed more softkey screen**" parameter, in the scenario above, the "More" softkey is removed in both places allowing the phones to display all configured top and bottom softkeys on one screen.



Default Screen 1



Default Screen 2



Parameter Enabled

When the “**collapsed more softkey screen**” parameter is enabled for the 6869i/6930 IP phone, the phone will apply the same behavior if 12 top softkeys or five bottom softkeys are configured.

When the “**collapsed more softkey screen**” parameter is enabled for the 6873i/6940 IP phone, the phone will apply the same behavior if 12 top softkeys or six bottom softkeys are configured.

CONFIGURING THE COLLAPSED MORE SOFTKEY SCREEN OPTION

Use the following parameter to configure the collapsed more softkey screen option

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Programmable Key Settings” on page A-259.

PRESS-AND-HOLD SPEEDDIAL KEYPAD KEYS

The keypad keys on the IP phones can be used to store speeddial numbers that are dialed out when a user presses and holds the respective key. These press-and-hold speeddial numbers can be configured using the IP phone UI, the Mitel Web UI, or by defining the “**pnhkeypadN value**” and “**pnhkeypadN line**” parameters in the configuration files.

CONFIGURING PRESS-AND-HOLD SPEEDDIAL KEYPAD KEYS

You can program one speeddial number for each applicable keypad key (keys 1 through 9). For information on how to configure the press-and-hold keypad keys (as well as press-and-hold speeddial softkeys or programmable keys) using the IP phone UI, please refer to the respective phone model’s *SIP Phone User Guide*.

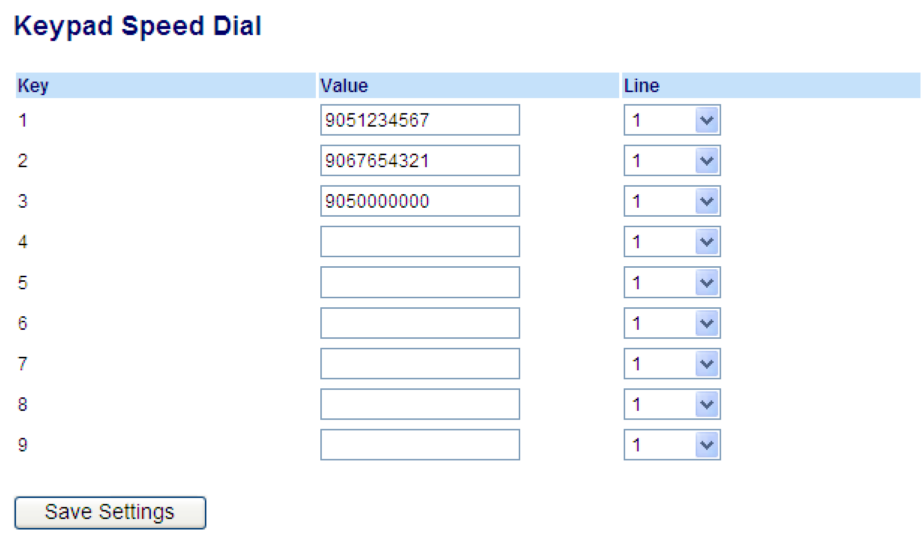
Use the following procedures to configure the press-and-hold keypad keys.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Press-and-Hold Speeddial Keypad Key Settings” on page A-273.

MITEL WEB UI

1. Click on **Operation->Keypad Speed Dial.**



2. Select the keypad key you want to program.
3. In the “**Value**” field, enter the speeddial number.
4. In the "**Line**" field, select the line number you want the phone to use when dialing the speeddial number.
5. Click **Save Settings**.

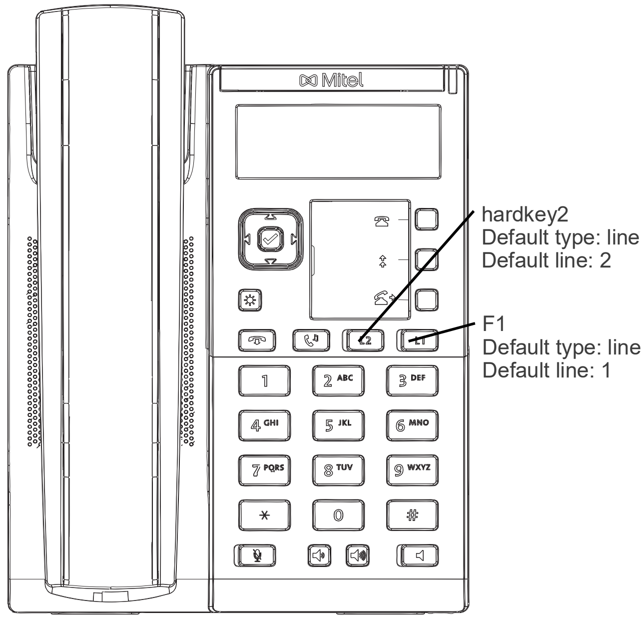
EDIT SPEED DIAL KEY

With release 5.0.0 SP1, users can edit the previously configured speed dial softkey using the "Press and Hold" feature.

HARD KEY REPROGRAMMING

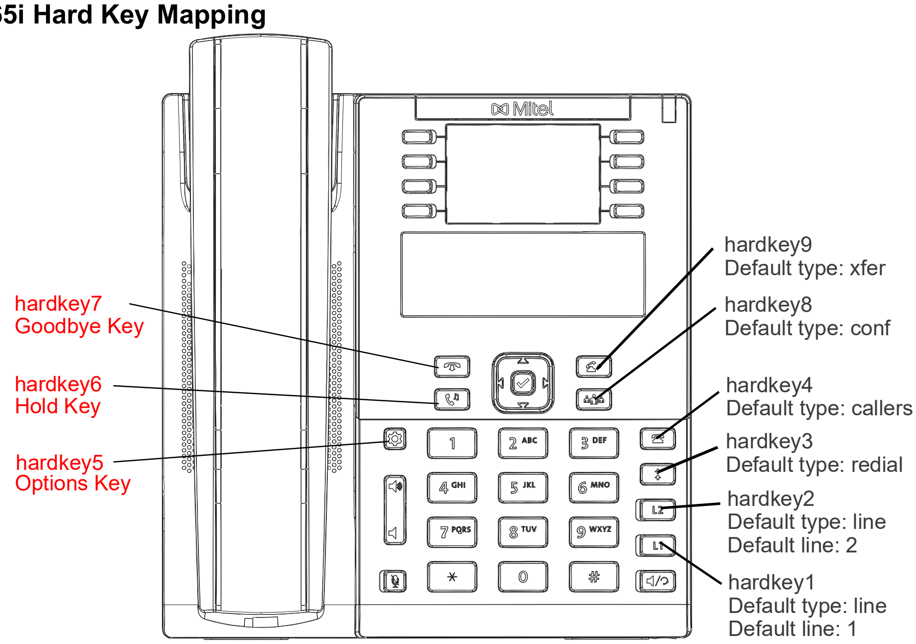
Administrators have the ability to reprogram a number of the IP phone’s hard keys (depending on the model) with any one of the phone’s softkey functions.

6863i Hard Key Mapping



Note: Hard keys are only configurable using the configuration files.

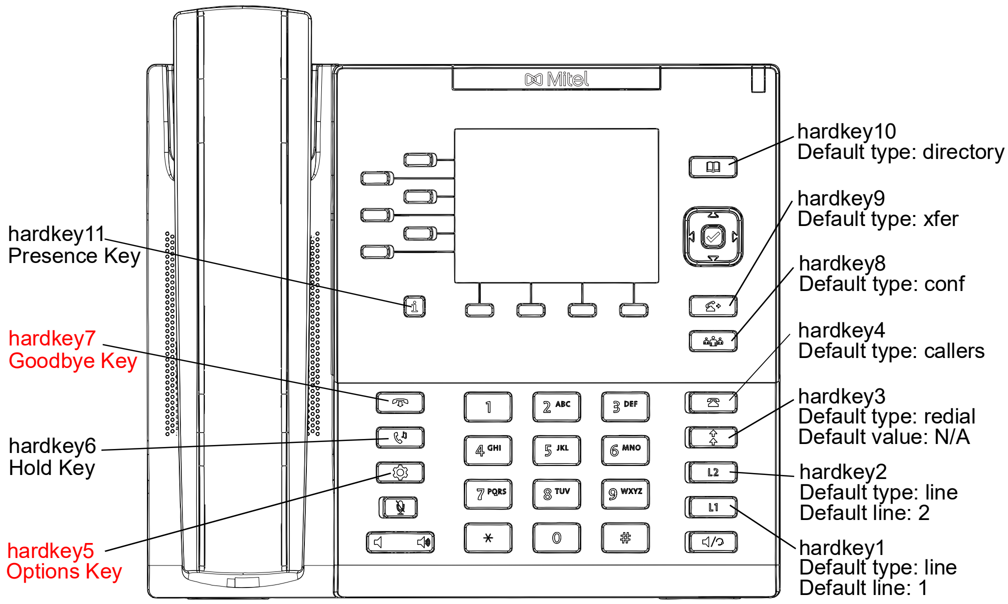
6865i Hard Key Mapping



Notes:

1. The reprogramming of hard keys 5, 6, and 7 (indicated above in red) is not supported.
2. Hard keys are only configurable using the configuration files.

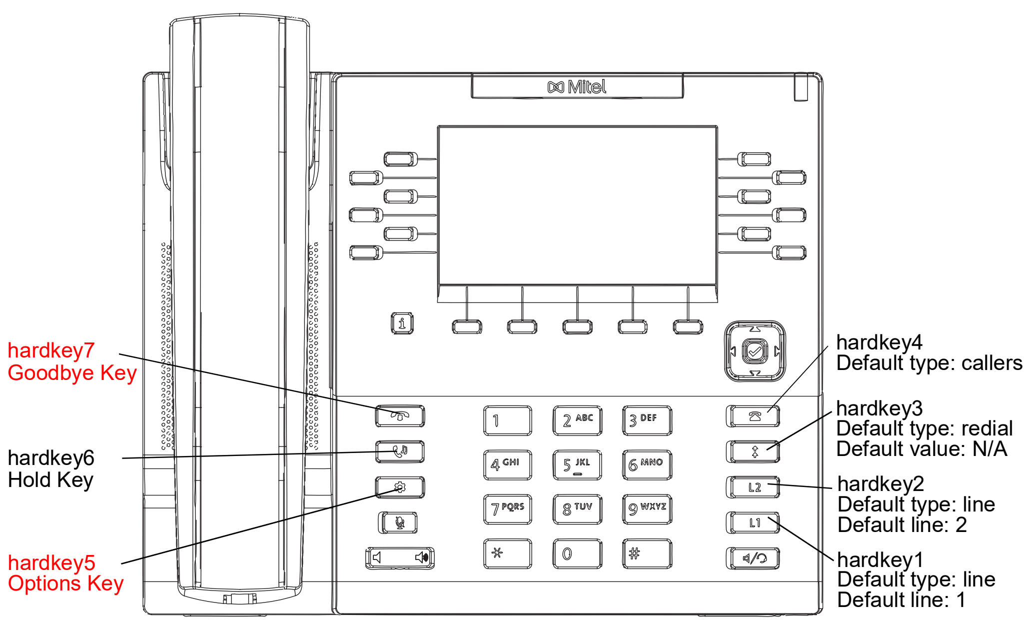
6867i Hard Key Mapping



Notes:

1. The reprogramming of hard keys 5 and 7 (indicated above in red) is not supported.
2. Hard keys are only configurable using the configuration files.

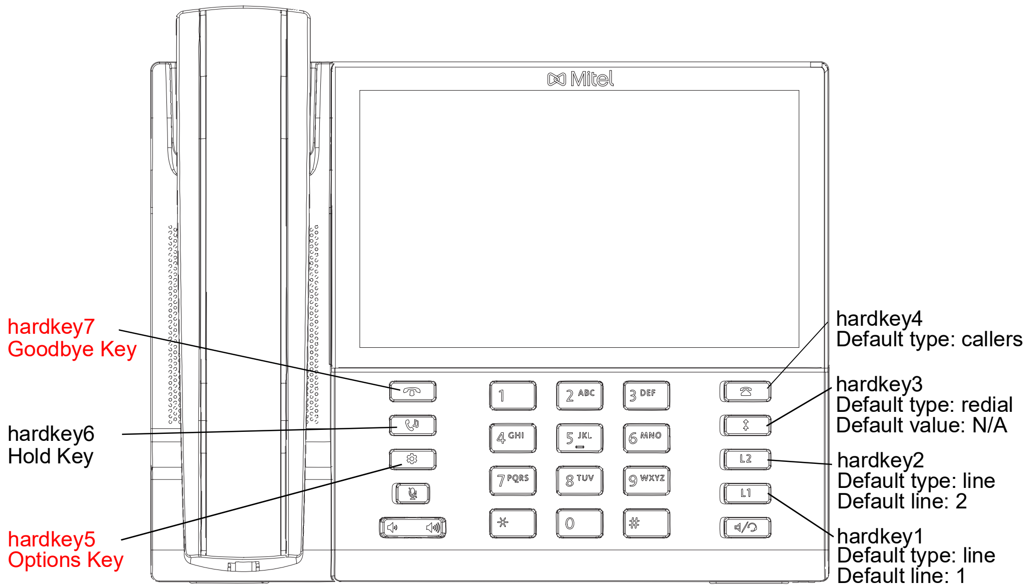
6869i Hard Key Mapping



Notes:

1. The reprogramming of hard keys 5 and 7 (indicated above in red) is not supported.
2. Hard keys are only configurable using the configuration files.

6873i Hard Key Mapping



Notes:

1. The reprogramming of hard keys 5 and 7 (indicated above in red) is not supported.
2. Hard keys are only configurable using the configuration files.

6900 HARD KEY REMAPPING

Note: The 6970 IP Phone does not support hard key reprogramming.

The hardkey layout for 6900 series SIP phones is redesigned and mapped as shown in the following graphical representations.

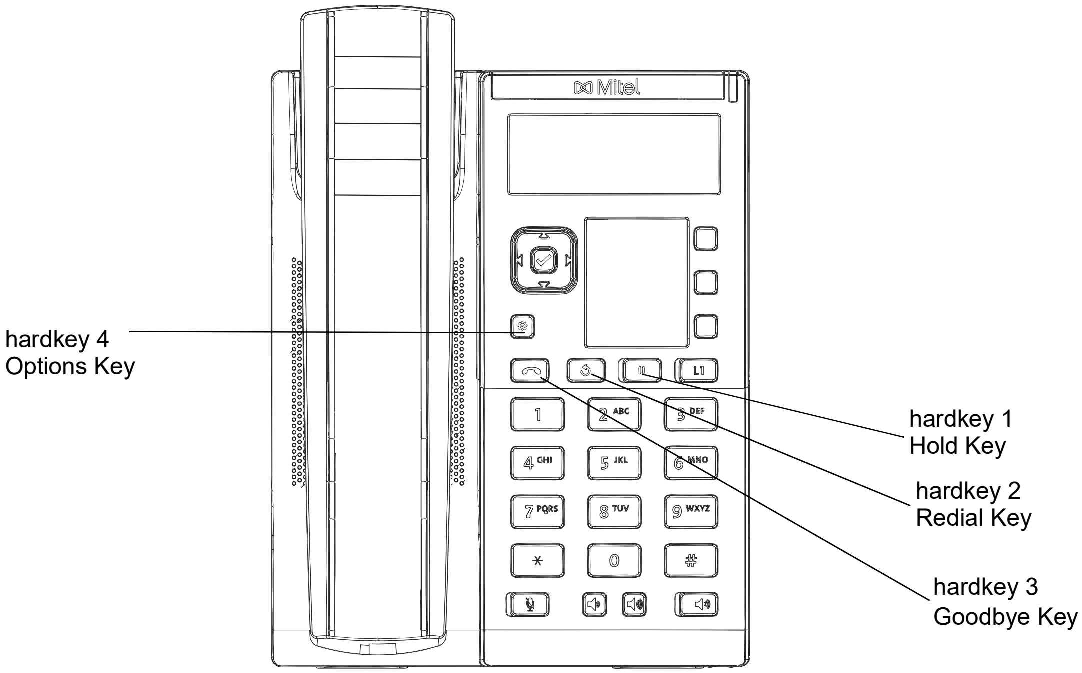
Notes:

1. The reprogramming of hard keys 3 and 4 (goodbye and options keys) is not supported.
2. Hard keys are only configurable using the configuration files.

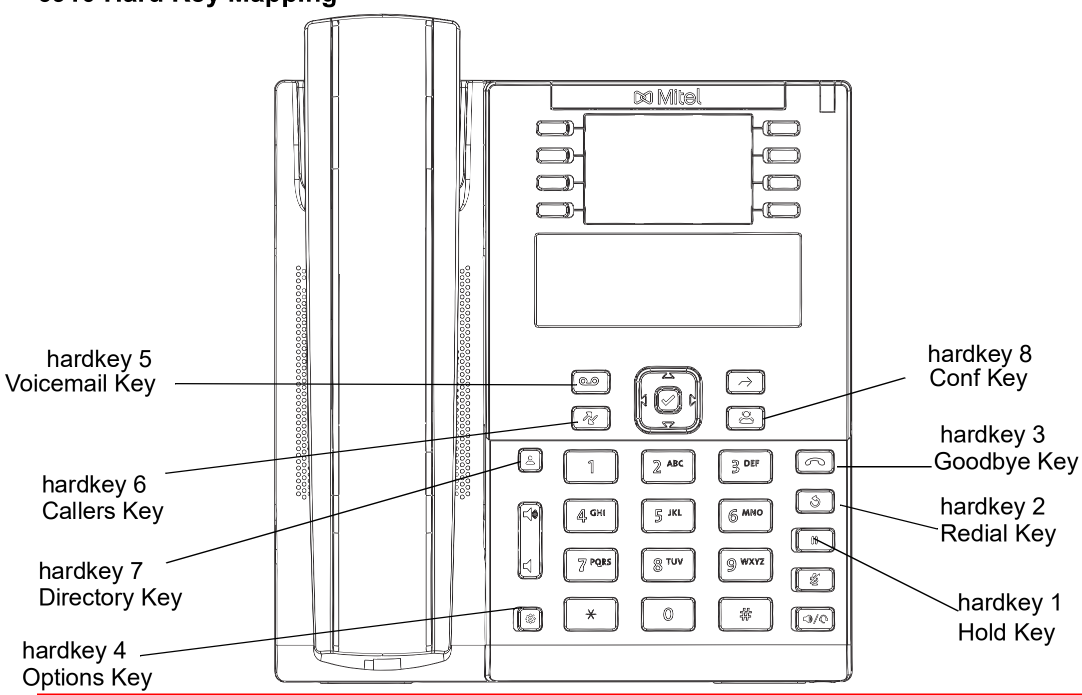
The default configuration parameter values for 6900 series SIP Phones are as follows:

- hardkey1 type: hold
- hardkey2 type: redial
- hardkey3 type: goodbye
- hardkey4 type: options
- hardkey5 type: voicemail
- hardkey6 type: callers
- hardkey7 type: directory
- hardkey8 type: conf

6905 Hard Key Mapping

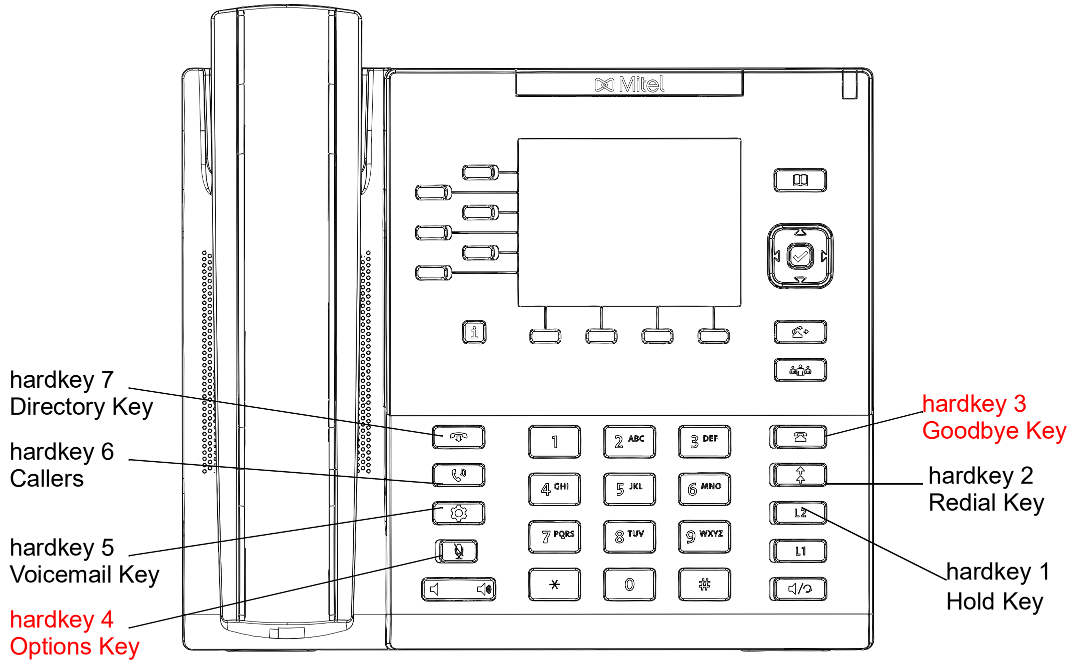


6910 Hard Key Mapping

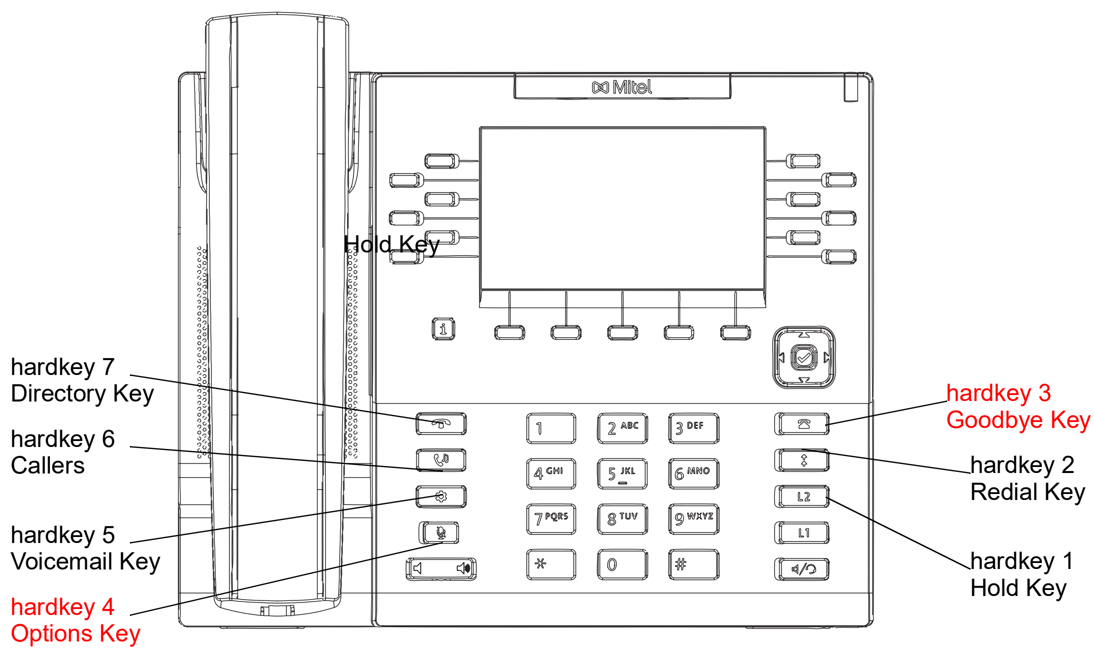


Note: The reprogramming of hard key 8 (i.e Conf key) is supported on 6910 IP Phone.

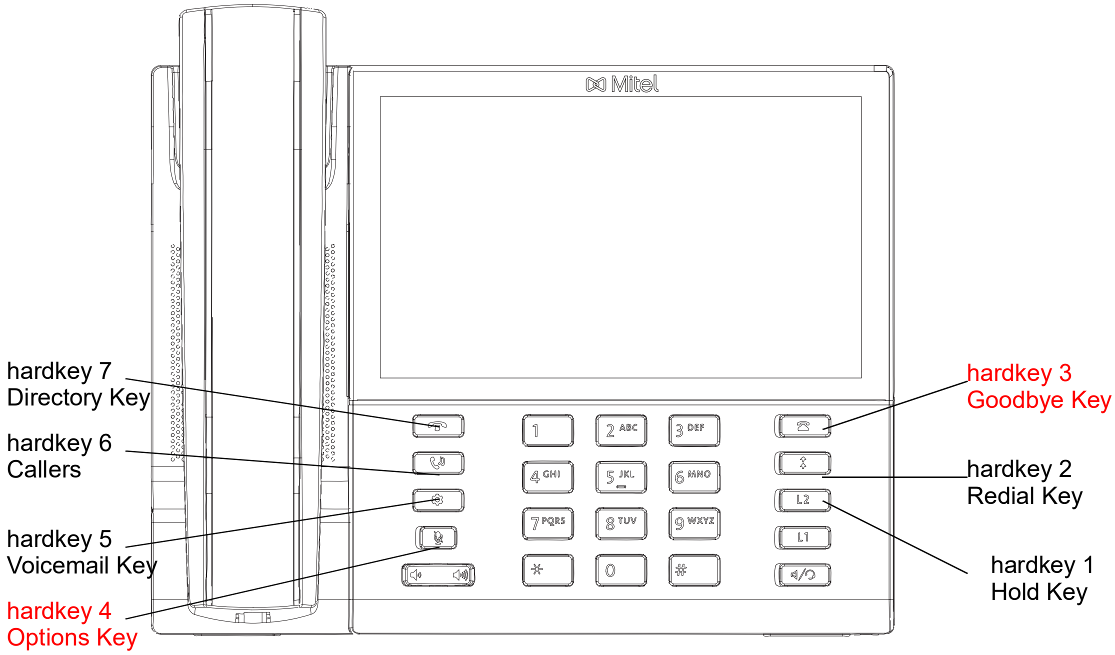
6920 Hard Key Mapping



6930 Hard Key Mapping



6940 Hard Key Mapping



The following parameters can be used to reprogram the hard keys:

CONFIGURATION PARAMETER	DESCRIPTION
hardkeyN type	The type of key to which you would like to change the hard key. Valid types (depending on the model) include: • none • line • speeddial • dnd • blf (6865i, 6867i, 6869i, 6873i, 6920, 6930, 6940 only) • list (6865i, 6867i, 6869i, 6873i, 6920, 6930, 6940 only) • acd (6865i, 6867i, 6869i, 6873i, 6920, 6930, 6940 only) • xml • flash • spre • park • pickup • lcr • callforward • blfxfer (6865i, 6867i, 6869i, 6873i, 6920, 6930, 6940 only) • speeddialxfer • speeddialconf • speeddialmwi (6865i, 6867i, 6869i, 6873i, 6920, 6930, 6940 only) • directory • filter (6865i, 6867i, 6869i, 6873i, 6920, 6930, 6940 only) • callers • redial • conf • xfer • icom • services • phonelock • paging • hotdesklogin • discreetringing • callhistory • callcenter

CONFIGURATION PARAMETER	DESCRIPTION
hardkeyN value	The value you would like to assign to the hard key you are configuring. The “hardkeyN value” parameter can be set for the following key types only: • speeddial • line • blf (6865i, 6867i, 6869i, 6873i, 6910, 6920, 6930, 6940 only) • spre • xml • park • pickup • blfxfer (6865i, 6867i, 6869i, 6873i, 6920, 6930, 6940 only) • speeddialxfer • speeddialconf • speeddialmwi (6865i, 6867i, 6869i, 6873i, 6910, 6920, 6930, 6940 only) • redial • filter (6865i, 6867i, 6869i, 6873i, 6910, 6920, 6930, 6940 only) • paging • callcenter
hardkeyN line	The line associated with the hard key you are configuring. The “hardkeyN line” parameter can be set for the following key types only: • speeddial • blf (6865i, 6867i, 6869i, 6873i, 6910, 6920, 6930, 6940 only) • list (6865i, 6867i, 6869i, 6873i, 6910, 6920, 6930, 6940 only) • acd (6865i, 6867i, 6869i, 6873i, 6910, 6920, 6930, 6940 only) • park • pickup • lcr • blfxfer (6865i, 6867i, 6869i, 6873i, 6910, 6920, 6930, 6940 only) • speeddialxfer • speeddialconf • speeddialmwi (6865i, 6867i, 6869i, 6873i, 6910, 6920, 6930, 6940 only) • redial • filter (6865i, 6867i, 6869i, 6873i, 6910, 6920, 6930, 6940 only)

In addition to the above basic parameters, the following supplementary parameters can also be used for the hard keys:

CONFIGURATION PARAMETER	DESCRIPTION
hardkeyN locked	Locks the specified hard key on the IP phones. When enabled, the phone locks the key with the provisioned local settings and prevents users from changing or configuring the key. **Note:** If no settings are configured locally but the "hardkeyN type" is defined in a configuration file, the phone will lock the key with the key type defined in the configuration file along with any values associated with the additional "hardkeyN" parameters (i.e. "hardkeyN value" and "hardkeyN line").

CONFIGURATION PARAMETER	DESCRIPTION
hardkeyN ring splash	When a key is configured for BLF or BLF/List functionality, this parameter controls the ring splash alert pattern per key. The following alerting patterns are available: 0. Silence (ring splash off). 1. Normal (same as current BLF ring splash). 2. Normal delayed (After a delay of [x] seconds, the ring signal that is the same as the current BLF ring splash is played [use the “ring splash delay” parameter to define the delay]). 3. Periodic (similar to the normal ring signal that is used by the phone itself. The actual ring melody is based on the current melody set for the line to which the BLF key is associated). 4. Periodic delayed (same as Periodic but after a delay of [x] seconds, the ring signal that is used by the phone is played [use the “ring splash delay” parameter to define the delay]). 5. Low volume (same as the current BLF ring splash but at a lower level to be less intrusive). 6. Low volume delayed (after a delay of [x] seconds, the ring signal that is the same as the current BLF ring splash is played at a lower level [use the “ring splash delay” parameter to define the delay]). 7. The behavior is determined by the global parameter “play a ring splash”. •If “play a ring splash” is defined as 0 then the feature is disabled. •If “play a ring splash” is defined as 1 then the behavior is the same as Normal. •If “play a ring splash” is defined as 2 then the behavior is the same as Normal but the ring splash plays when idle and also during the active call state. 8. In call delayed (same as Normal delayed but ring splash plays when idle and also during the active call state [use the “ring splash delay” parameter to define the delay]). 9. In call periodic (same as Periodic but ring splash plays when idle and also during the active call state [use the “ring splash frequency” parameter to define the ring splash frequency interval for the active call state]). 10.In call periodic delayed (same as Periodic delayed but ring splash plays when idle and also during the active call state [use the “ring splash delay” parameter to define the delay for the active and idle call state and the “ring splash frequency” parameter to define the ring splash frequency interval for the active call state]). 11. In call low volume (same as Low volume but ring splash plays when idle and also during the active call state). 12. In call low volume delayed (same as Low volume delayed but ring splash plays when idle and also during the active call state [use the “ring splash delay” parameter to define the delay]). **Note:** Ring tones are based on the current ring tone set configured on the SIP phone. Ring splashes will not be played if a custom ring tone has been selected by the user.

Notes:

1. The value of “N” in the above “hardkeyN” parameters corresponds to the hard key’s mapping number as per the “6863i Hard Key Mapping”, “6865i Hard Key Mapping”, “6867i Hard Key Mapping”, “6869i Hard Key Mapping”, “6873i Hard Key Mapping”, “”, “6930 Hard Key Mapping”, *and* “6940 Hard Key Mapping” figures.
2. Hard keys 1 and 2 on all 6800 Series SIP phones cannot be programmed as Line keys other than their default (Line 1 and Line 2).
3. When hard keys 1 and 2 on the 6863i and 6865i are remapped, if applicable, LED indication will follow the color/cadence of the corresponding feature when the key is reprogrammed.
4. When hard keys 1 to 4 on 6867i, 6869i, and 6873i are remapped, if applicable, LED indication will follow the color/cadence of the corresponding feature when the key is reprogrammed.
5. Hard keys 3, 4, 8, and 9 on the 6865i, hard keys 6, 8, 9, 10, and 11 on the 6867i, and hard keys 6 and 11 on the 6869i can be remapped to any key type except for the following: Line, BLF, BLF/List, Auto Call Distribution, and BLF/Xfer.
6. If a hard key is configured with the type “None”, functionality of the hard key (and its corresponding LED) is disabled.
7. Misconfiguration of the hard key will result in the key going back to its default function. For example, reprogramming hard key 3 (Redial) to:
   ```
   hardkey3 type: line
   hardkey3 line: 33
   ```
   will result in hard key 3 reverting back to its default Redial functionality as the “hardkey3 line: 33” definition is invalid.

REPROGRAMMING HARD KEY FUNCTIONALITY USING THE CONFIGURATION FILES

Use the following procedures to reprogram the functionality of hard keys on the 6867i, 6869i, 6873i, 6905, 6910, 6920, 6930 and 6940 IP phones.

CONFIGURATION FILES

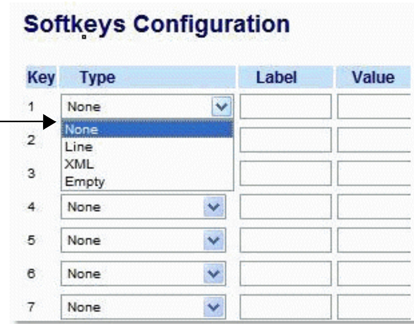
For specific parameters you can set in the configuration files, see Appendix A, the sections, “Hard Key Settings” on page A-281, “Locking Keys” on page A-288, and “Ring Splash Settings” on page A-297.

CUSTOMIZING THE KEY TYPE LIST IN THE MITEL WEB UI

An Administrator can configure which key types display in the Mitel Web UI list for a Softkey, Programmable Key, and/or Expansion Module Key,. Currently, in the Mitel Web UI for a phone, you can select a type of key from a list of more than 20 key types to assign to a softkey, programmable key, and/or expansion module key.

Using the configuration files, you can specify key types to display in the key type list that apply to a User's environment.

Example of a List of Configured Keys Types (None, Line, XML, Empty)



In addition to being able to specify which key types display in the list, the Administrator can also determine in which order the key types display.

You can use the following configuration file parameters to control which key types to display and specify in which order to display them in:

- softkey selection list

If no value is specified for the "softkey selection list" parameter, the key "Type" list displays all of the key types by default.

If an Administrator configures specific key types for a phone in the configuration file, and the phone for which he downloads the configuration to already has key types configured on it, those key types display in the key list for those keys, in addition to the key types specified by the Administrator. For example, a phone has a Park key and a Pickup key already configured on the phone, and the Administrator downloads a configuration file to the phone that has specific key types of None, Line, Speeddial, and XML. After the configuration file is downloaded, the Park key list will show None, Line, Speeddial, XML, and Park; the Pickup key list will show None, Line, Speeddial, XML, and Pickup; all other keys that were configured as None before the download will show only None, Line, Speeddial, and XML.

Notes:

1. Any key types configured that do not apply to the phone are ignored.
2. The SAVE and DELETE keys appear by default Keys 5 and 6 on the 6865i unless your Administrator configured these keys as other functions.
3. An Administrator must use the English value when configuring the key types in the configuration files.
4. After configuring specific key types for a phone, the key types in the Mitel Web UI display the same for both the User and Administrator Web interfaces for that phone.

CUSTOMIZING THE KEY TYPE LIST USING THE CONFIGURATION FILES

Use the following procedure to configure the Key Type List that displays in the Mitel Web UI.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Customizing the Key Type List" on page A-286.

SPEEDDIAL PREFIXES

The normal function of the **Speeddial** option allows you to configure a specific key on the phone to dial a number quickly by pressing the configured key. For example, if you had the following Speeddial configuration in the configuration files:

```
softkey1 type: speeddial
softkey1 label: Office
softkey1 value: 5552345
softkey1 line: 1
```

after you press softkey1 on the phone, it dials the Office number at 555-2345 on line 1.

A Speeddial option feature allows you to configure a preset string of numbers followed by a "+". This feature allows the phone to speeddial a prefix number and then pause to let you enter the remaining phone number. You can use this feature for numbers that contain long prefixes. For example, if you had the following Speeddial configuration in the configuration files:

```
softkey2 type: speeddial
softkey2 label: Europe Office
softkey2 value: 1234567+
softkey2 line: 2
```

after you press softkey2 on the phone, it dials the prefix number automatically and pauses for you to enter the remaining number using the keypad on the phone.

You can configure the Speeddial prefix using the configuration files or the Mitel Web UI.

ENABLING/DISABLING ABILITY TO ADD OR EDIT A SPEEDDIAL KEY

The IP Phones allow you to set a parameter, "**speeddial edit**" using the configuration files that allows you to enable or disable the ability to add a Speeddial key or edit a Speeddial key from the IP Phone UI. Disabling this parameter prevents a user from adding or editing a Speeddial key.

Notes: The ability to edit Speeddial keys on the phone using the Press-and-hold feature is only available with the firmware release 4.3.0 SP2, and not with earlier or later releases.

The default for this parameter is enabled, allowing you to create and edit Speeddial keys on the phone using the Press-and-hold feature, softkeys, programmable keys, expansion module keys and key pad, Speeddial menu in the IP Phone UI, and the SAVE TO key.

If this parameter is set to disabled, it blocks the user from using any of the features on the phone to create or edit a Speeddial key.

ENABLING/DISABLING THE ABILITY TO ADD OR EDIT A SPEEDDIAL KEY USING THE CONFIGURATION FILES

Use the following procedure to enable/disable the ability to add and edit a Speeddial key.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Enabling/Disabling Ability to Add/Edit Speeddial Keys" on page A-292.

BUSY LAMP FIELD (BLF)

The BLF feature on the IP phones allows a specific extension to be monitored for state changes. BLF monitors the status (busy, idle, ringing, and on hold) of extensions on the IP phone.

Notes:

1. Applicable to the 6865i, 6867i, 6869i, 6873i, 69210, 6920, 6930, 6940, and 6970 IP phones only.
2. BLF feature availability is dependent on your call manager.

Example

A Supervisor configures BLFs on his phone for monitoring the status of a worker's phone use. When the worker picks up his phone to make a call, a busy indicator on the Supervisor's phone shows that the worker's phone is in use and busy.

BLF SETTING

On the 6865i IP phone, the LED lights next to each BLF programmable key illuminate steady to indicate the monitored line is off-hook or unregistered. The LED goes off when the line is idle. When the monitored extension is ringing, the LED flashes.

On 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970, the busy and idle states are indicated by the color of the softkey button on screen (i.e. red for busy, green for idle, yellow for ringing, yellow hold icon for hold). On the 6867i, 6869, 6920 and 6930, the LEDs indicate the states as well (i.e. solid for busy, off for idle, blinking for ringing and on hold).

Note: You can configure a maximum of 50 BLFs shared between the phone and any attached expansion modules.

You can configure a BLF key on the IP Phones using the configuration files or the Mitel Web UI.

BLF/LIST SETTING

(For use with the BroadSoft BroadWorks Rel 13 or higher platform only)

The BLF/List feature on the IP phones is specifically designed to support the BroadSoft BroadWorks Rel 13 Busy Lamp Field feature. This feature allows the IP phone to subscribe to a list of monitored users defined through the BroadWorks web portal.

For the 6867i/6920, 6869i/6930, and 6873i/6940/6970, when the monitored user is idle, the corresponding softkey is green. When the monitored user's phone is ringing, the corresponding softkey turns yellow. When the monitored user on an active call or is attempting to make a call, the corresponding softkey turns red. Finally, when the monitored user's call is on hold, the corresponding softkey displays the BLF/List hold icon. On the 6867i/6920 and 6869i/6930 the LEDs indicate the states as well (i.e. solid for busy, off for idle, blinking for ringing and on hold).

On the 6865i IP hone, the LED lights next to each BLF programmable key illuminate steady to indicate the monitored line is off-hook or unregistered. The LED goes off when the is idle. When the monitored extension is ringing, the LED flashes.

Note: The BroadWorks BLF feature is not the same as the BroadWorks Shared Call Appearance (SCA) feature and does not permit call control over the monitored extension.

You can configure a BLF/List key on the IP Phones using the configuration files or the Mitel Web UI. You can also specify a BLF list URI that the phone uses to access the required BLF list. You can specify a BLF List URI using the "**list uri**" parameter in the configuration files or the BLF List URI field in the Mitel Web UI at the path *Operation->Softkeys/Programmable Keys/Expansion Module Keys->Services->BLF List URI*. For more information about the "list uri" parameter, see Appendix A, the section, "BLF List URI Settings" on page 292.

Example

A receptionist has an IP phone that subscribes to a list of extensions from the BroadWorks Application Server.

On 6865i IP phone, the programmable key LEDs illuminate either flashing, solid, or turn off depending on the state of the monitored extensions. On the 6867i/6920, 6869i/6930, and 6873i/6940/6970 the BLF states are indicated by the color of the softkey icon on screen (red for busy, yellow for ringing, green for idle, and a yellow hold icon for hold) and for the 6867i/6920 and 6869i/6930 the LEDs indicate the state as well (i.e. solid for busy, flashing for ringing and hold, and off for idle).

BLF BEHAVIOR IN FAILOVER SCENARIO

Previously, the "???" symbol was displayed next to the corresponding BLF key when the status of a monitored SIP extension was unreliable. In a failover scenario, the "???" symbol is displayed during a failover from the current to an alternative registrar.

An enhancement is made wherein the "???" symbol does not display next to the corresponding BLF key during a failover from the current to an alternative registrar, unless the registration to the alternative server fails.

ASTERISK BLF CONFIGURATION

You can enable the BLF feature on Asterisk to enable monitoring for specific extensions. BLF on Asterisk is possible through the "hint" extension parameter.

Add the following in the Asterisk *extensions.conf* file for each target extension being monitored.

For example:

```
exten -> 9995551212,hint,SIP/9995551212
```

Add the following in the Asterisk *sip.conf* file for each subscriber if it is not defined already.

For example:

```
[9995551212]

Subscribecontext=sip
```

BROADSOFT BLF CONFIGURATION

You can enable the BLF feature on BroadSoft BroadWorks Rel 13 or higher through the BroadWorks Web Portal. Each user must have the Busy Lamp Field service enabled for their user. The user must add each desired extension to the "Monitored Users List" on the Busy Lamp Field service page and also enter in a list name for the monitored users BLF list on the same page.

Changes to the "Monitored Users List" are dynamic and the Mitel IP phones are automatically updated without requiring a restart.

Reference

For sample BLF configurations, see Appendix D, "Sample BLF Softkey Settings."

CONFIGURING BLFS

Use the following procedures to configure BLF and BLF/List on the IP phone.

CONFIGURATION FILES

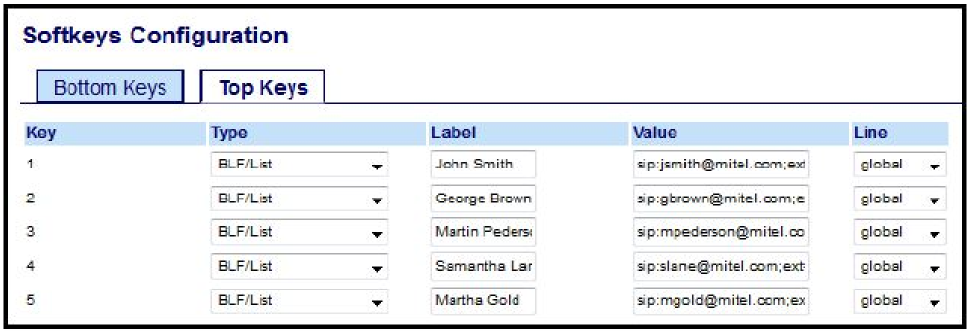
To set BLF or BLF/List in the configuration files, see Appendix A, the sections,

- "Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters" on page A-248.
- "BLF List URI Settings" on page A-292.

MITEL WEB UI

1. Click on **Operation->Softkeys and XML->Top Keys**
   or

Click on **Operation->Programmable Keys**
or
Click on **Operation->Expansion Module <N>.**
Depending on your phone-model, the key configuration screen displays.



2. Select a softkey, programmable, or expansion module key to configure.

3. In the "**Type**" field, select "**BLF**" (Asterisk), "**BLF/List**" (BroadSoft BroadWorks).

4. (For the 6867i/6869i/6873i/6920/6930/6940/6970 softkeys) In the "**Label**" field, enter the name of the person who's extension you are monitoring.

Note: If BLF/List type is selected, the label value is optional. If a label is:

1. Configured, then the label name is shown and labels from SIP NOTIFY name are ignored.
2. Not configured, then the label name is shown based on SIP NOTIFY name. In some cases if a label is not configured, the label will be displayed as a series of question marks (i.e. ???) until it is updated with the appropriate data from the call manager.

5. In the "**Value**" field, enter a value to associate with the softkey or programmable key.
For example, for BLF, the value is the extension you want to monitor.
For BLF/List, enter the BLF/List target's resource URI, using the following syntax:
`sip:username@domain.com;ext=extension number`
whereby the "username@domain.com" is identical to the resource URI of the BLF/List key configured on the call manager and the "extension number" (an optional value) corresponds to the target's extension number.

Note: If a resource URI is not defined in the **Value** field, the key will be automatically populated using the first resource entry from the BLF/List NOTIFY data that has not already been populated (either manually or automatically).

6. In the "**Line**" field, select a line number that is actively registered to the appropriate SIP proxy you are using.

7. In the "**BLF List URI**" field, enter the name of the BLF list defined on the BroadSoft BroadWorks Busy Lamp Field page for your particular user.
For example, sip:9@192.168.104.13.

Note: The value of the BLF/List URI parameter must match the list name configured. Otherwise, no values display on the screen and the feature is disabled.

8. Select the line state (idle, connected, incoming, outgoing, busy) that you want to apply to the BLF softkey or programmable key.
9. Click **Save Settings** to save your changes.
10. In the "**BLF List URI**" field, enter the name of the BLF list defined on the BroadSoft BroadWorks Busy Lamp field page for your particular user.
    For example, sip:9@192.168.104.13.

    Note: The value of the BLF/List URI parameter must match the list name configured. Otherwise, no values display on the screen and the feature is disabled.
11. Click **Save Settings** to save your changes.

BLF PAGE SWITCH FEATURE

Note: Applicable to the 6867i, 6869i, 6920, and 6930 IP Phones only. This feature is currently not supported on the 6873i, 6940, and 6970 IP phones.

The BLF page switch feature enables the 6867i, 6869i, 6920 and 6930 model phones to automatically switch the screen focus to a softkey page or M685i or M695 expansion module page that has an active Busy Lamp Field (BLF) key. Administrators can configure this feature using the "**blf activity page switch**" parameter.

If this parameter is set to "1", the screen will switch to a softkey page or an M685i or M695 expansion module page if a monitored extension transitions to a ringing (fast flashing) state. If this parameter is set to "2", the screen will switch if a monitored extension transitions to either a ringing (fast flashing) or a hold (slow flashing) state. Finally, if this parameter is set to "3", the screen will switch if a monitored extension transitions to either a ringing or hold state OR from an idle (off) state to an "in call" (solid) state.

The following can be observed with this new feature:

- If there is a lot of activity on the monitored extensions, the page will be shown on the screen for at least 5 seconds before switching again. When a user manually scrolls the pages by pressing the **More** key or the **Function** key (for the page you want to display) on the M685i or M695, no activity-triggered page flipping should occur for 5 seconds after the manual switch.
- If the phone softkeys are hidden by an overlay screen, such as an XML UI object, a menu (e.g. the Services, Directory, or Received Callers List menu), or if the phone is in an active call, the screen will not automatically switch focus to a softkey page with BLF activity (it will however for an expansion module page).
- When the phone is in Idle mode, the menu switches to the page with the BLF key when there is an incoming call to the monitored extension. The page is shown for 10 seconds if the call is answered. If the call is not answered by the BLF extension, the BLF key page will be shown as long as ringing is ongoing.
- When the BLF key page is shown and there is another incoming call on another BLF key on the same page, the new call is also shown on this BLF key.
- When the BLF key page is shown and there is another incoming call on another BLF key on another page, the switch to the other page will be done after 10 seconds.

- When the BLF key page is shown and there are several more incoming calls on BLF keys, after 10 seconds the next active BLF key will be shown in the key number order.

Notes:

1. This feature is not applicable to BLF/List keys.
2. To minimize the chance of a lot of switching between the Idle screen and the page(s) with BLF keys, it is recommended to have the BLF keys with most frequent traffic on one page. If the expansion module has several BLF keys, it is recommended to use an extra display panel unit.
3. The 6867i, 6869i, 6920, and 6930 IP phones (as well as the M685i or M695 Expansion Module) will automatically switch to the idle page (or the first page on the M685i Expansion Module) if no BLF activity is detected by the phone.

CONFIGURING BLF PAGE SWITCH

Use the following procedures to configure the BLF page switch feature on the IP phone.

CONFIGURATION FILES

To configure the BLF page switch on the IP phones using the configuration files, see Appendix A, the section, "BLF Page Switch" on page A-294.

CONFIGURABLE DISPLAY MODES FOR BLF AND BLF/LIST SOFTKEY LABELS

Note: Applicable to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones only.

The manner in which labels for BLF and BLF/List softkeys are displayed on the applicable IP phones (as well as the M685i or M695 Expansion Modules) can be configured by Administrators. By defining the "**blf display label to max**" parameter to either "**0**" or "**1**" in the configuration files, Administrators can choose between two distinct display modes.

In the primary (default) display mode (i.e. "**blf display label to max: 0"**), when a label exceeds the maximum characters the respective phone's screen can display, the phone adds an ellipsis (i.e. "...") at the end of the label indicating the label has been automatically truncated. In the secondary display mode (i.e. "**blf display label to max: 1"**), the phone does not automatically truncate the label and simply displays as many characters as the area reserved for the label allows.

CONFIGURING XMPP AVATAR

When the XMPP Avatar for picture ID is configured on the phone, the available image is displayed on the phone (it can be XMPP Avatar image as well).

And if the image is not available, the phone downloads it from the image server and displays the image of a blue man.

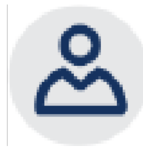
XMPP can be configured in these two scenarios:

If XMPP enabled

The phone checks for XMPP avatar and the image in the image database.

If XMPP not enabled

The phone only checks the availability of the image in the image database.
(XMPP avatar is not checked as it is not enabled.)



Generic Avatar image

CONFIGURABLE DISPLAY FOR BLANK BLF/LIST AND XMPP PRESENCE-RELATED FAVORITE SOFTKEYS

Note: Applicable to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones only.

When softkeys for the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP phones and the M685i and M695 Expansion Modules are configured as BLF/Listkeys on the phone but there are not enough members in the BLF/List on the BroadSoft server side, then a series of question marks (i.e. “???”) are displayed on screen beside some of the softkeys. The series of question marks are also displayed for unused XMPP presence-related Favorite softkeys on the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP phones when the number of Favorite softkeys exceeds the number of UC-ONE favorite contacts.

Administrators can simply choose to hide the series of question marks using the “**keys noname hidden**” parameter. If this parameter is set to “1” (enabled) then the series of question marks will be hidden and nothing will be shown on the screen beside the affected softkeys. If this parameter is set to “0” (disabled) then the series of question marks (or configured symbol) will be displayed on the screen indicating blank BLF/List and/or Favorite softkeys.

Alternatively, applicable only to BLF/List softkeys, Administrators can configure the phone to replace the series of question marks with a series of different symbols by defining the “**keys noname symbol**” parameter with a desired character. For example, if **keys noname symbol: “e”** is defined in the configuration files, the phone will display “eee” instead of “???”.

CONFIGURING THE DISPLAY FOR BLANK BLF/LIST AND FAVORITE SOFTKEYS

Use the following procedure to configure the display for blank BLF/List and Favorite softkeys:

CONFIGURATION FILES

To configure the display for blank BLF/List and Favorite softkeys on the IP phone using the configuration files, see Appendix A, the section, "Configurable Display for Blank BLF/List and XMPP Presence-Related Favorite Softkeys" on page A-295.

CONFIGURABLE BLF OR BLF/LIST KEY BEHAVIOR WHEN IN AN ACTIVE CALL

Note: Applicable to the 6865i, 6867i, 6869i, and 6873i IP Phones only.

Administrators can configure the phone's behavior when a BLF or BLF/List softkey is pressed during an active call. If the "**blf key mode**" parameter is defined as "0" (default), the BLF or BLF/List number will be sent as DTMF tones in the active call. If defined as "1", the active call will be placed on hold and the phone will place a call to the BLF or BLF/List number using the next available line.

CONFIGURING BLF KEY BEHAVIOR WHEN IN AN ACTIVE CALL

Use the following procedure to configure BLF and BLF/List key behavior when in an active call:

CONFIGURATION FILES

To configure BLF and BLF/List key behavior when in an active call, see Appendix A, the section, "Configurable BLF and BLF/List Key Behavior When in an Active Call" on page A-296.

RING SIGNAL TYPE FOR BLF AND BLF/LIST

Note: Applicable to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones only.

There is a global parameter "**play a ring splash**" that controls whether or not a ring splash is played when there is an incoming call on a BLF- or BLF/List-monitored extension. For the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP phones, you can configure the phone to play the ring splash when idle only or when idle and also in an active call state.

Notes:

1. When on an active call using a wired analog headset, the call's audio may be interrupted during the BLF/BLF-List ring splash.
2. When a mobile phone call is connected using an internal hands free speaker or microphone, a BT handset, BT headset, or BT Speaker phone, the call's audio might be interrupted during the BLF/BLF-List ring splash. Hence, while a mobile phone call is connected using any of these devices, the BLF-List ring splash does not occur for the BLF monitoring number.

In addition to this global ring splash control, administrators can control the ring splash alert pattern on a per key basis. Each type of key can have a different ring splash alerting pattern and volume. When the phone UI receives the event update from the line manager for BLF transitions to ringing state, the ring splash value is checked to take the appropriate action.

The following alerting patterns are available for all applicable phones:

- **0**: Silence (ring splash off).
- **1**: Normal (same as current BLF ring splash).
- **2**: Normal delayed (After a delay of [x] seconds, the ring signal that is the same as the current BLF ring splash is played [use the "**ring splash delay**" parameter to define the delay]).
- **3**: Periodic (similar to the normal ring signal that is used by the phone itself. The actual ring melody is based on the current melody set for the line to which the BLF key is associated).
- **4**: Periodic delayed (same as Periodic but after a delay of [x] seconds, the ring signal that is used by the phone is played [use the "**ring splash delay**" parameter to define the delay]).
- **5**: Low volume (same as the current BLF ring splash but at a lower level to be less intrusive).
- **6**: Low volume delayed (after a delay of [x] seconds, the ring signal that is the same as the current BLF ring splash is played at a lower level [use the "**ring splash delay**" parameter to define the delay]).
- **7**: The behavior is determined by the global parameter "**play a ring splash**".
  - If "**play a ring splash**" is defined as 0 then the feature is disabled.
  - If "**play a ring splash**" is defined as 1 then the behavior is the same as Normal.
  - If "**play a ring splash**" is defined as 2 then the behavior is the same as Normal but the ring splash plays when idle and also during the active call state.
- **8**: In call delayed (same as Normal delayed but ring splash plays when idle and also during the active call state [use the "**ring splash delay**" parameter to define the delay]).
- **9:** In call periodic (same as Periodic but ring splash plays when idle and also during the active call state [use the "**ring splash frequency**" parameter to define the ring splash frequency interval for the active call state]).
- **10:** In call periodic delayed (same as Periodic delayed but ring splash plays when idle and also during the active call state [use the "**ring splash delay**" parameter to define the delay for the active and idle call state and the "**ring splash frequency**" parameter to define the ring splash frequency interval for the active call state]).
- **11**: In call low volume (same as Low volume but ring splash plays when idle and also during the active call state).
- **12**: In call low volume delayed (same as Low volume delayed but ring splash plays when idle and also during the active call state [use the "**ring splash delay**" parameter to define the delay]).

The following parameters are available allowing administrators to set and pass the control of the ring splash to the key (instead of the phone using the global "**play a ring splash**" parameter).

- "**prgkeyN ring splash**"
- "**softkeyN ring splash**"
- "**topsoftkeyN ring splash**"

- "**expmodX KeyN ring splash**
- "**hardkeyN ring splash**"
- "**ring splash delay**" (applicable when the "...keyN ring splash" parameter is set to a "delayed" alerting pattern)
- "**ring splash volume**" (applicable when the "...keyN ring splash" parameter is set to a "low volume" alerting pattern)
- "**ring splash frequency**" (applicable when the "...keyN ring splash" parameter is set to a "in call periodic" alerting pattern)
- **"XXXkeyN ring splash**" (applicable when the "...**"**keyN ring splash" parameter value is set to control the ring splash alert pattern for both BLF and BLF/List.

The per key settings overwrite the global setting ("**play a ring splash**" parameter) on the phone. If the global parameter is *disabled*, a ring splash can still be enabled on a key basis. If the global parameter is *enabled*, all keys will have a ring splash unless the value "0" is configured explicitly for a key.

The following table details the ring splash behavior in the different call states/events when the feature is enabled for active calls states. The behavior is consistent for all audio sources and audio mode configurations.

STATE	BEHAVIOR
Idle	Ring splash played through the speaker.
Active Call	Ring splash played through the speaker.
Call Waiting	Ring splash played through speaker.
Mid-Conference/Transfer Establishment	Ring splash played through speaker.
Do Not Disturb (Idle/In Call)	No ring splash played.
Hold	Ring splash played through speaker.
Ringing - Outgoing	Ring splash played through speaker.
Ringing - Incoming	No ring splash played.
Initiating a direct call pickup of the BLF target	No ring splash played.
Initiating a speeddial of the BLF target	No ring splash played.

CONSIDERATIONS

The following considerations must be taken into account when using this feature:

- When a BLF or BLF/List softkeys ring splash parameter is dynamically changed, the change will not take effect until the BLF target becomes idle.
- The playing of a ring splash will be postponed if it is not allowed to be played in the current state and will start playing if the phone transitions to a state where the ring splash can be played. However, if the BLF target stops ringing before the transition, the ring splash will not be played.
- The playing of a delayed ring splash will be postponed until the delay expires. However, if the BLF target stops ringing before the delay expires, the ring splash will not be played.

- In scenarios where the BLF target goes into the ringing state while an initial in-call ring splash is playing or while a call hold or call waiting reminder is playing, the secondary in-call ring splash will be played 500ms after the current event has ended. The inverse is also true whereby call hold or call waiting reminders will be played 500ms after the BLF ring splash, if they occur while a BLF ring splash is playing.
- In scenarios where multiple keys are configured for periodic ring splashes and multiple BLF targets are ringing, only one periodic ring splash for one target will be played.
- While on an active call, if the “ring audibly enable” parameter is enabled and a call is incoming while a periodic ring splash is playing, the periodic ring splash will stop allowing the incoming call’s ring tone to be played, and then resume after the incoming call’s ring tone has ended.

CONFIGURING RING SPLASH SETTINGS

Use the following parameters to configure the ring splash settings:

CONFIGURATION FILES

To set the ring splash on a per key basis in the configuration files for BLF, see Appendix A, the sections “Ring Splash Settings” on page A-297.

BLF SUBSCRIPTION PERIOD

Note: Applicable to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones only.

On the IP phones, you can set the time period, in seconds, that the IP phone re-subscribes the BLF subscription service.

In the configuration files, enter the following parameter with a valid value to set the BLF subscription period:

```
sip blf subscription period: <value in seconds>
```

The minimum value for this parameter is 120 seconds (2 minutes) and the maximum is 2147483647 seconds. The default is 3600 (1 hour). The phone resubscribes to the BLF subscription service before the defined subscription period ends.

You can configure this feature using the configuration files or the Mitel Web UI.

Note: The “**sip blf subscription period**” parameter is not applicable to BLF/List subscriptions.

CONFIGURING BLF SUBSCRIPTION PERIOD

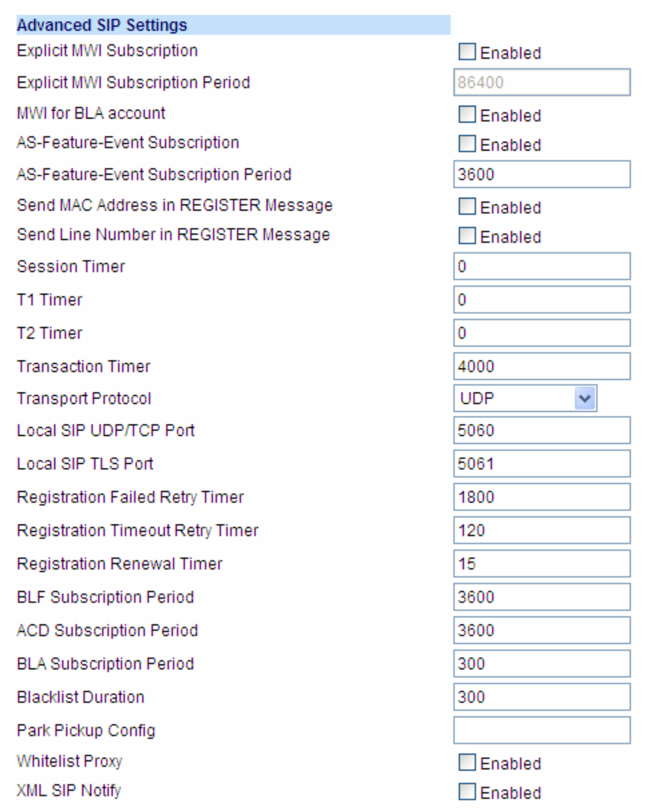
Use the following procedures to configure the BLF subscription period on the IP phone.

CONFIGURATION FILES

To configure the BLF subscription period on the IP phones using the configuration files, see Appendix A, the section, "Advanced SIP Settings" on page A-116.

MITEL WEB UI

1. Click on **Advanced Settings->Global SIP->Advanced SIP Settings.**



2. Enter a value, in seconds, from 120 to 2147483647 in the "**BLF Subscription Period**" field.
3. Click **Save Settings** to save your changes.

BLF/XFER AND SPEEDDIAL/XFER KEYS

The IP Phones have a transfer (Xfer) enhancement feature you can use with the BLF and Speeddial keys - **BLF/Xfer** (for 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 only) and **Speeddial/Xfer**.

The BLF key allows one or more extensions to be monitored, and once there is any state change with those extensions, the key shows the status of the monitored lines. The Xfer key allows a call to be transferred to other recipients blindly or consultatively.

The Speeddial key allows a number to be dialed quickly by pressing one key configured for speed-dialing. After answering a call, the recipient can transfer the call to an extension by:

1. Pressing Xfer key.
2. Entering the number of the extension or pressing Speeddial or BLF key.
3. Pressing Xfer key again

The BLF and Speeddial transfer enhancement feature provides a simpler way of transferring calls using the keys called **BLF/Xfer** and **Speeddial/Xfer**. The **BLF/Xfer** key combines the BLF and Xfer key's functionality together allowing the user to transfer calls or use BLF with one key. Similarly, the **Speeddial/Xfer** key combines the Speeddial key and Xfer key's functionality together allowing the user to press one key to speeddial and transfer calls.

Note: It is recommended that you enable the "**switch focus to ringing**" parameter when using the BLF and Speeddial Transfer key feature. For more information about this parameter, see "Switch Focus to Ringing Line" on page 5-98.

BLF/XFER KEY REQUIREMENTS AND FUNCTIONALITY

- **BLF/Xfer and BLF**
  A BLF/Xfer key can be configured for subscribing to an extension and monitor the status of the extension, similar to the BLF key functionality. Changes of the state of the monitored extension are indicated by a LED / Icon.
- **BLF/Xfer and Blind Transfer Calls**
  When the focused line is in the "Connected" state, pressing the BLF/Xfer key transfers the call to the extension unconditionally, disregarding the status of the monitored extension. If transferring a call to an extension fails, a message "*Transfer Failed*" displays on the phone, and you can reconnect the call (get the call back) by pressing the line key again.
- **BLF/Xfer and Call forward**
  When the focused line is in the "Ringing" state, pressing the BLF/Xfer key forwards the call to the extension unconditionally, disregarding the status of the monitored extension.
- **BLF/Xfer and Speeddial**
  When the focused line and the monitored extension are idle, pressing the BLF/Xfer key causes the phone to go offhook and dial the number of the extension.

SPEEDDIAL/XFER KEY REQUIREMENTS AND FUNCTIONALITY

The Speeddial/Xfer key has the following capabilities:

- **Speeddial/Xfer and Speeddial**
  When the phone is in the "**Idle**" state, pressing the Speeddial/Xfer key causes the phone to go offhook and dial the predefined extension.
- **Speeddial/Xfer and Blind Transfer**
  When the phone is connected to a call, pressing the Speeddial/Xfer key blind transfers the call to the predefined target.
  If transferring a call fails, a message "*Transfer Failed*" displays, and you can reconnect the call (get the call back) by pressing the line key again.
- **Speeddial/Xfer and Call Forward**
  When the phone is in the "**Ringing**" state, pressing the Speeddial/Xfer key forwards the call to the predefined extension.

CONFIGURING THE BLF/XFER KEY AND THE SPEEDDIAL/XFER KEY USING THE CONFIGURATION FILES

You use the following parameters in the configuration files to configure the BLF/Xfer key and/or Speeddial/Xfer key on the IP Phone.

SOFTKEY PARAMETERS	PROGRAMMABLE KEY PARAMETERS	EXPANSION MODULE PARAMETERS	TOP SOFTKEY PARAMETERS
softkeyN type	prgkeyN type	expmodX keyN type	topsoftkeyN type
softkeyN label	prgkeyN value	expmodX keyN label	topsoftkeyN label
softkeyN value	prgkeyN line	expmodX keyN value	topsoftkeyN value
softkeyN line		expmodX keyN line	topsoftkeyN line
softkeyN states			

Examples:

```
softkey1 type: speeddialxfer
softkey1 label: BX7801
softkey1 value: 7801
softkey1 line: 1
softkey1 states: idle connected incoming outgoing busy
```

```
prgkey1 type: blfxfer
prgkey1 value: 35
prgkey1 line: 1
```

Refer to the following in Appendix A to configure a BLF/Xfer and Speeddial/Xfer key on the IP phone using the configuration files.

CONFIGURATION FILES

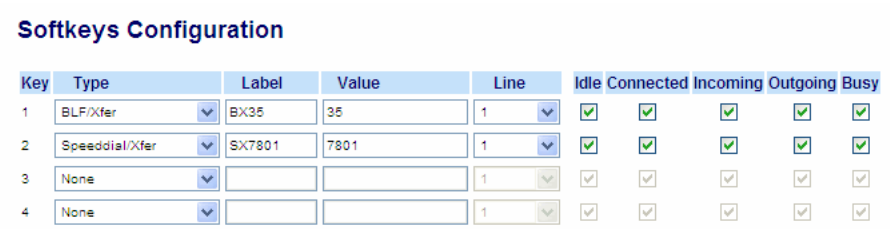
To set a BLF/Xfer and Speeddial/Xfer key using the configuration files, see Appendix A, "Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters" on page A-248.

CONFIGURING THE BLF/XFER KEY AND THE SPEEDDIAL/XFER KEY USING THE MITEL WEB UI

You configure the BLF/Xfer key and/or the Speeddial/Xfer Key on the IP phone similar to configuring a BLF key or Speeddial key using the Mitel Web UI. Use the following procedure to configure BLF/Xfer and/or Speeddial/Xfer.

MITEL WEB UI

1. Click on **Operation->Softkeys and XML.**
   or
   Click on **Operation->Programmable Keys.**
   or
   Click on **Operation->Expansion Keys.**



2. Choose a key that you want to assign the BLF/Xfer key or a Speeddial/Xfer key to, and select **BLF/Xfer** or **Speeddial/Xfer** from the "**Type**" field.
3. In the "**Label**" field, enter a key label to assign to the BLF/Xfer key (for example, "**BX35**").
4. In the "**Value**" field, enter the monitored extension (for example, "**35**").
5. In the "**Line**" field, select the line for which you want to use the key functionality.
6. Select the state(s) (idle, connected, incoming, outgoing, busy) for which you want to use on the key.

   Note: States are not applicable to programmable keys.

7. Click **Save Settings** to save your changes.

SPEEDDIAL/CONFERENCE KEY

The IP Phones allow you to configure a softkey/programmable key/expansion module key to be used as a Speeddial Conference key (**Speeddial/Conf** key) while remaining in the current call. This key allows a user on a call, to conference another party at a pre-defined number while remaining in the conference call.

For example, while on an active call, a user can use the Speeddial/Conf key to dial a recording service and have the resulting conference recorded.

Note: If currently in a conference, the Speeddial/Conf key is disabled on the active call.

HOW IT WORKS

If you configure a softkey/programmable key/expansion module as a **Speeddial/Conf** key, and you press this key while on an active call, the focused line changes to the dialing line. A **Cancel** softkey displays on the 6867i/6869i/6873i IP phones, allowing you to abort the conference speeddial if required. The message "*Ringing*..." displays below the number when the far end is ringing. The message "*Conf. Unavailable*" briefly displays when a conference is already in progress. The active call is not put on hold when the speeddial number is dialed. This feature is not compatible with centralized conferencing.

The softkey/programmable key is called "**Speeddial/Conf**" in the Web UI drop down list. In the configuration file, use "**speeddialconf**" as the softkey type.

CONFIGURING THE SPEEDDIAL/CONF KEY USING THE CONFIGURATION FILES

To configure the Speeddial/Conf key using the configuration files, you enter "**speeddialconf"** for the key type. The following parameters are examples you can use to configure the Speeddial/Conf key:

```
softkey1 type: speeddialconf
softkey1 label: Sales
softkey1 value: 5645
softkey1 line: 3

topsoftkey1 type: speeddialconf
topsoftkey1 label: Sales
topsoftkey1 value: 5645
topsoftkey1 line: 3

prgkey1 type: speeddialconf
prgkey1 value: 5645
prgkey1 line: 1

expmod1 key1 type: speeddialconf
expmod1 key1 label: Sales
expmod1 key1 value: 5645
expmod1 key1 line: 3
```

Refer to the following in Appendix A to configure a Speeddial/Conf key on the IP phone using the configuration files.

CONFIGURATION FILES

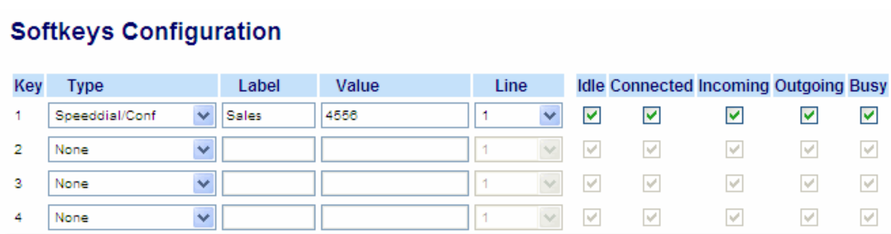
To set a Speeddial/Conf key using the configuration files, see Appendix A, "Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters" on page A-248.

CONFIGURING THE SPEEDDIAL/CONF KEY USING THE MITEL WEB UI

Use the following procedure to configure the Speeddial/Conf Key using the Mitel Web UI.

MITEL WEB UI

1. Click on **Operation->Softkeys and XML.**
   or
   Click on **Operation->Programmable Keys.**
   or
   Click on **Operation->Expansion Module Keys.**



2. In the "**Type**" field, select **Speeddial/Conf** from the list of options.
3. In the "**Label**" field, enter a key label to assign to the Speeddial/Conf key (for example, "**Sales**").
4. In the "**Value**" field, enter the number that the phone dials when the Speeddial/Conf key is pressed (for example, "**4556**").
5. In the "**Line**" field, select the line for which you want to use the key functionality.
6. For phones with softkeys:
7. In the States field, select the state(s) (idle, connected, incoming, outgoing, busy) for which you want to use on the key.

   Note: States are not applicable to programmable keys (6863i, 6865i, 6905, 6910).

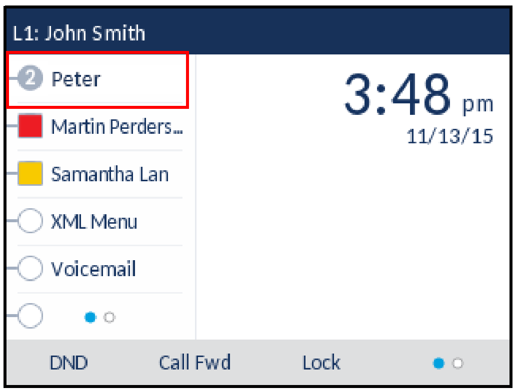
8. Click **Save Settings** to save your changes.

SPEEDDIAL/MWI KEY

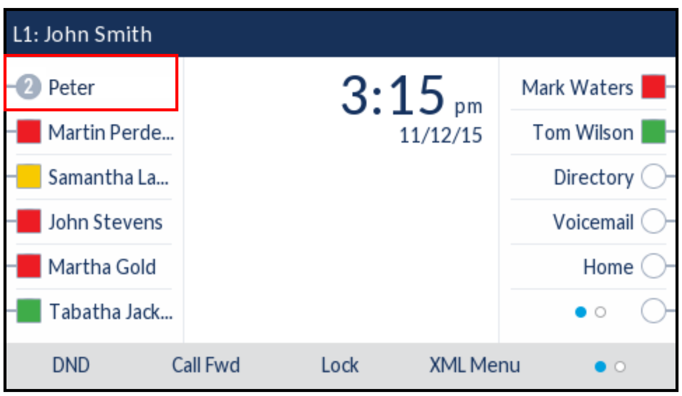
Multiple voicemail registration is supported on the 6865i, 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 SIP phones. This feature can be useful in scenarios where a user needs to monitor the voicemail accounts of his/her team members or an assistant requires access to his/her manager's voicemail messages.

By configuring a programmable key, top softkey, or expansion module softkey as "Speeddial/MWI" and defining call and voicemail URIs, users can monitor and listen to pending messages on multiple voicemail accounts. When new messages are pending on a monitored voicemail account the corresponding Speeddial/MWI key's LED will blink (6865i, 6867i, and 6869i) and the UI (for top softkeys on the 6867i, 6869i, and 6873i) will display a gray circle and the number of pending messages inside the circle.

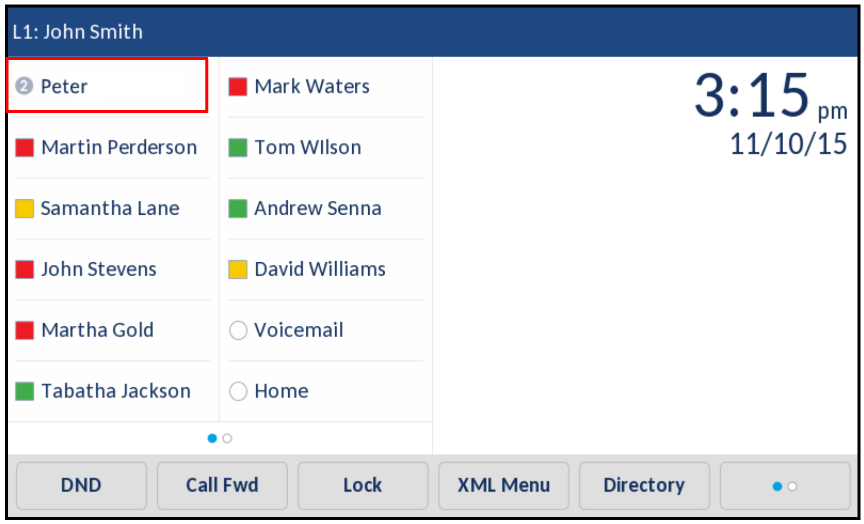
6867i/6920 Speeddial/MWI Key Example



6869i/6930 Speeddial/MWI Key Example



6873i/6940/6970 Speeddial/MWI Key Example



When a user presses the Speeddial/MWI key, the phone will send an INVITE to the configured call URI whereby the user will be able to listen to the new messages.

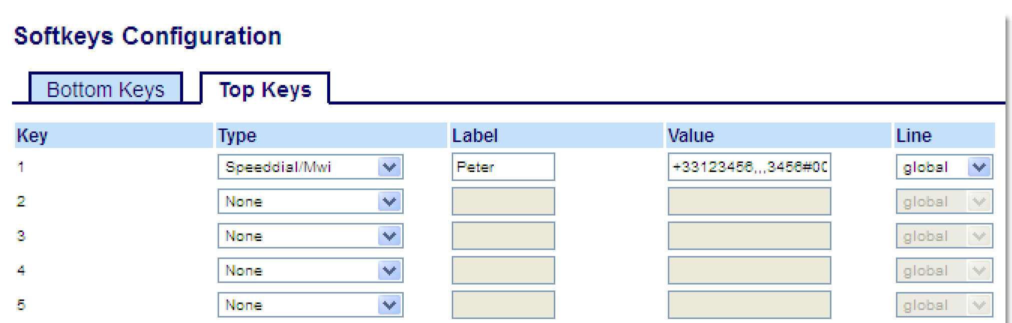
Users can configure the Speeddial/MWI key through the Mitel Web UI while Administrators can configure the key through the Mitel Web UI as well as the configuration files.

Configuring a Speeddial/MWI Key Using the Mitel Web UI

Use the following procedure to configure a Speeddial/MWI key using the Mitel Web UI:

MITEL WEB UI

1. Click on **Operation > Programmable Keys**
   or
   Click on **Operation > Softkeys and XML > Top Keys**
   or
   Click on **Operation > Expansion Module <N>**



2. Choose an available key and in the **Type** field, select **Speeddial/MWI**.
3. (If applicable) In the **Label** field, enter a label to apply to this key.

4. In the **Value** field, enter call URI and voicemail URI separated by a semi-colon, as per the following syntax: [call URI];[voicemail URI]. For example, +33123456,,,3456#0000#@domain;sip:voicemail_peter@domain.

> **Notes:**
> 1. As the example above illustrates, pauses and DTMF are supported for the call URI.
> 2. Ensure that no spaces are added between the call URI and the voicemail URI when defining the key value.
> 3. If only one URI is provided, the value will be used for the voicemail URI and the call URI will be left as undefined.

5. In the **Line** field, select the line for which you want to use the key functionality.
6. Click **Save Settings**.

Configuring a Speeddial/MWI Key Using the Configuration Files

To configure a Speeddial/MWI key using the configuration files, you must enter "**speeddialmwi**" for the key type. For the label (6867i/6869i/6873i/M685i only), enter a key label to assign to the Speeddial/MWI key (e.g. Peter). For the value, enter call URI and voicemail URI separated by a semi-colon, as per the following syntax: [call URI];[voicemail URI]. For example, +33123456,,,3456#0000#@domain;sip:voicemail_peter@domain.

> **Notes:**
> 1. As the example above illustrates, pauses and DTMF are supported for the call URI.
> 2. Ensure that no spaces are added between the call URI and the voicemail URI when defining the key value.
> 3. If only one URI is provided, the value will be used for the voicemail URI and the call URI will be left as undefined.

For the line, enter the line for which you want to use the key functionality (e.g. 3). The following parameters are examples you can use to configure a Speeddial/MWI key using the configuration files:

For Top Softkeys

```
topsoftkey1 type: speeddialmwi
topsoftkey1 label: Peter
topsoftkey1 value:
+33123456,,,3456#0000#@domain;sip:voicemail_peter@domain
topsoftkey1 line: 3
```

For Programmable Keys

```
prgkey1 type: speeddialmwi
prgkey1 value:
+33123456,,,3456#0000#@domain;sip:voicemail_peter@domain
prgkey1 line: 3
```

For Expansion Module Softkeys

```
expmod1 key1 type: speeddialmwi
expmod1 key1 label: Peter
expmod1 key1 value:
+33123456,,,3456#0000#@domain;sip:voicemail_peter@domain
expmod1 key1 line: 3
```

For Hard Keys

```
hardkey1 type: speeddialmwi
hardkey1 value:
+33123456,,,3456#0000#@domain;sip:voicemail_peter@domain
hardkey1 line: 3
```

Refer to the following in Appendix A to configure a Speeddial/MWI key on the IP phone using the configuration files.

CONFIGURATION FILES

To set a Speeddial/Conf key using the configuration files, see Appendix A, "Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters" on page A-248.

DISCREET RINGING

The discreet ringing feature has been implemented beginning with Release 4.0.0 SP1. When enabled, if a call is incoming, the phone will play the configured ring tone once only. All applicable visual indicators (LED for the corresponding Line key, Message Waiting Indicator [MWI], etc...) will behave normally.

Note: If a custom ring tone is selected and discreet ringing is enabled, the phone will not play the custom ring tone during an incoming call. Ring tone 1 will be played once instead.

Administrators can configure this feature by defining the "**discreet ringing**" parameter in the configuration files (i.e. "0", the default, disables this feature, while "1", enables discreet ringing). or by programming a key on the phone with the "Discreet Ringing" type feature using the Mitel Web UI. After the key has been programmed, users can simply toggle the feature on or off by pressing the programmed "Discreet" key.

Refer to the following in Appendix A to configure a Discreet Ringing key on the IP phone using the configuration files.

CONFIGURATION FILES

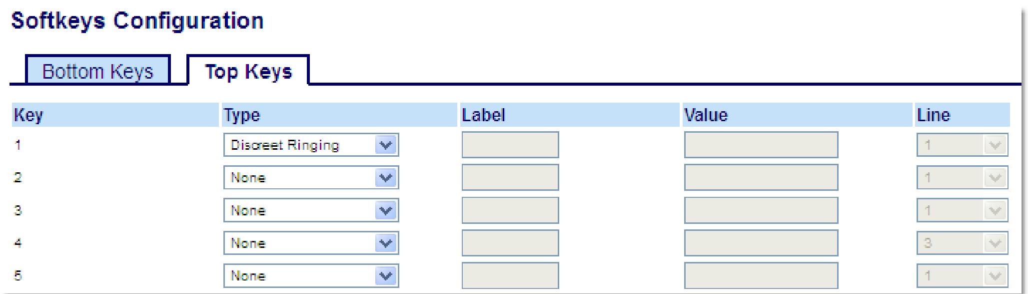
To enable the feature and set a Discreet Ringing key using the configuration files, see Appendix A, "Discreet Ringing Settings" on page A-309 and "Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters" on page A-248.

CONFIGURING THE DISCREET RINGING KEY USING THE MITEL WEB UI

Use the following procedure to configure the Discreet Ringing Key using the Mitel Web UI.

MITEL WEB UI

1. Click on **Operation**->**Softkeys and XML**.
   or
   Click on **Operation**-> **Programmable Keys**.
   or
   Click on **Operation**->**Expansion Module Keys**.



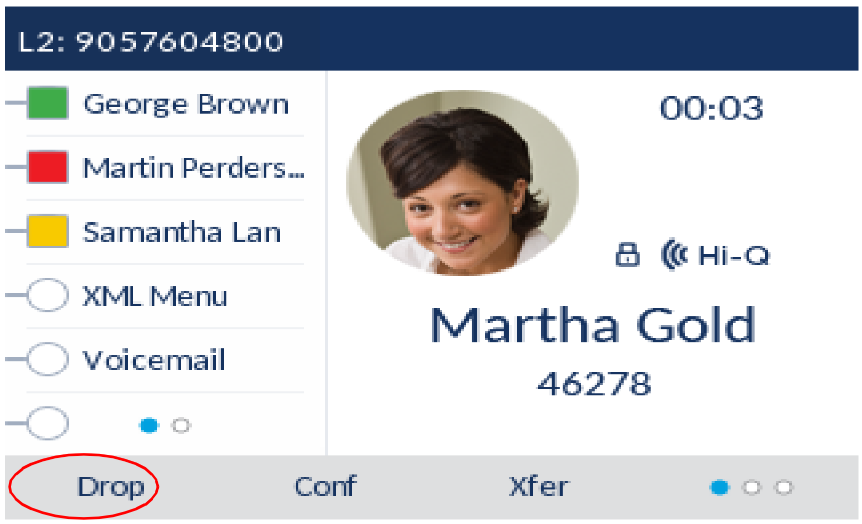
2. Select a key that you want to use as a Discreet Ringing key.
3. In the "**Type**" field, select "**Discreet Ringing**".
4. Click **Save Settings** to save your settings.

CONFIGURABLE REMOVAL OF THE "DROP" SOFTKEY

Note: This feature is applicable to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 SIP Phones.

Administrators have the ability to globally remove the contextual **Drop** softkey that is displayed when on any active call.

6873i Example



When the parameter "**drop context softkey**" is disabled (defined as "0"), the **Drop** softkey will not be displayed in any of the active call screens (e.g. for point-to-point calls, attended transfer and conference scenarios, conference calls, paging calls, etc...).

CONFIGURATION FILES

To enable or disable the **Drop** softkey using the configuration files, see Appendix A, "Drop Softkey Settings" on page A-309.

AUTOMATIC CALL DISTRIBUTION (ACD) (FOR SYLANTRO/BROADWORKS SERVERS)

Note: Applicable to the 6865i, 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones only.

The IP phones support an Automatic Call Distribution (ACD) feature for Sylantro/BroadWorks servers. The ACD feature allows the server to distribute calls from a queue to registered IP phone users (agents).

To use the ACD feature on an IP phone, the administrator must first configure an ACD softkey or programmable key. When an IP phone user wants to subscribe to a queue (in order to receive incoming calls), the user presses the ACD key. The IP phone UI prompts the user to log in.

When the IP phone user is ready to receive calls from the server, the user logs into a queue. Depending on the server configuration, the IP phone is either in an “unavailable” or “available” state. If the phone is set to “available” then the server begins to distribute calls to this phone immediately. If the phone is set to unavailable, then server waits until the IP phone user manually changes the phone status to “available” (using the IP phone UI) before distributing calls.

Whenever the IP phone user answers a call, or misses a call, the server automatically changes the phone’s status to unavailable. The server updates it database with this new information and no longer distributes calls to this phone. The IP phone will remain in this state until:

- the IP phone user makes himself “available” again.
- the ACD auto-availability timer expires. This occurs only if the administrator has configured an ACD auto-availability timer as described in “ACD Auto-Available Timer” on page 5-214.

The IP phone user can also choose to manually change the phone status to unavailable, using the IP Phone UI.

Note: It is recommended you configure no more than a single ACD softkey or programmable key per IP phone.

ACD AUTO-AVAILABLE TIMER

Whenever the IP phone user answers a call, or misses a call, the server automatically changes the phone’s status to unavailable. The administrator can control how long the IP phone remains in the unavailable state by configuring an auto-available timer. When the timer expires, the IP phone status is automatically changed to available. The default setting for the timer is 60 seconds.

You use the following parameters to configure an ACD Auto-Available Timer in the configuration files:

- acd auto available
- acd auto available timer

CONFIGURING AN AUTOMATIC CALL DISTRIBUTION (ACD) KEY

You can configure an ACD key on softkeys, programmable keys, and extension module keys.

The following table illustrates examples of configuring an ACD key on the phone.

TOP SOFTKEY EXAMPLES	PROGRAMMABLE KEY EXAMPLES	EXTENSION MODULE EXAMPLES
topsoftkey1 type: acd topsoftkey1 label: sales topsoftkey1 line: 1	prgkey1 type: acd prgkey1 line: 1	expmod1 key1 type: acd expmod1 key1 label: sales expmod1 key 1 line: 1

Use the following procedures to configure an ACD key on the IP phone.

CONFIGURATION FILES

To configure an ACD key using the configuration files, see Appendix A, the section, "Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters" on page A-248.

CONFIGURING THE ACD AUTO-AVAILABLE TIMER

CONFIGURATION FILES

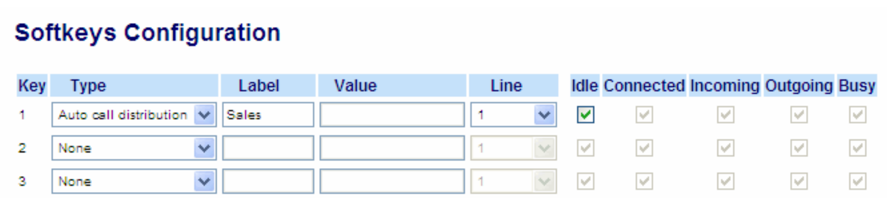
To configure the ACD Auto-Available Timer using the configuration files, see Appendix A, the section, "ACD Auto-Available Timer Settings" on page A-240.

CONFIGURING AN ACD KEY USING THE MITEL WEB UI

Use the following procedure to configure an ACD softkey, programmable key, or expansion module key using the Mitel Web UI.

MITEL WEB UI

1. Click on **Operation->Softkeys and XML**
   or
   Click on Operation->Programmable Keys
   or
   Click on Operation->Expansion Module <N>.
   Depending on your phone-model, the key configuration screen displays.



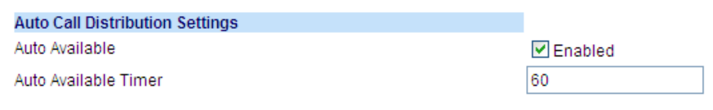
2. In the "**Type**" field, select **Auto Call Distribution**.
3. In the **"Label"** field, specify a name for this ACD softkey. The Label helps identify which queue you are subscribing to when you login. (This field does not apply to programmable keys).
   For example: **Sales**
4. In the **"Line"** field, select the line which the IP phone uses to subscribe to the queue.
   For example: **Line 1**
5. Click **Save Settings** to save your changes.

CONFIGURING THE ACD AUTO-AVAILABLE TIMER USING THE MITEL WEB UI

Use the following procedure to configure an ACD auto-available timer using the Mitel Web UI.

MITEL WEB UI

1. Click on **Basic Settings->Preferences->Auto Call Distribution Settings**.



2. In the "**Auto Available**" check-box, click **Enabled**.
3. In the **"Auto Available Timer"** field, specify the length of time (in seconds) before the IP phone state is automatically reset to "available." Valid values are 0 to 120 seconds. Default is 60.
   For example: **60**
4. Click **Save Settings** to save your changes.

USING THE ACD FEATURE ON YOUR IP PHONE

The ACD feature allows you to login to a phone queue in order to receive distributed calls on your IP phone. To login to a phone queue, your system administrator must preconfigure an ACD softkey or programmable key on your Mitel IP phone.

For the 6867i, 6869i, and 6873i IP phones, the ACD softkey is labeled according to your network requirements. The label usually describes which phone queue you are accessing when you press the ACD softkey.

For example, suppose the administrator wants to configure an ACD softkey to allow an IP phone user to log into the Customer Support phone queue. The administrator assigns the label "Support" to the softkey, so it is easily recognizable to the IP phone user. When the IP phone user wants to subscribe to the Customer Support queue, the user presses the Support key and can log in.

Once logged in to the queue, you can make yourself "available" or "unavailable" to take calls by pressing the Available/Unavailable key on the phone UI. The server monitors your IP phone status. When you set the IP phone to "available," the server begins distributing calls to your phone. When you set the IP phone to "unavailable," the server temporarily stops distributing calls to your phone.

For the 6865i, the programmable key LED reflects your current status. For the 6867i, 6869i, 6873i, 6920, 6930, 6940, and the 6970, the graphical button color reflects your current status along with text indication. The table below describes the meaning of the LED, and each icon, as they may appear on your IP phone:

PHONE MODEL	STATUS: LOGGED IN AND AVAILABLE	STATUS: UNAVAILABLE	LOGGED OUT
6865i	Solid Red LED	Blinking red LED	No LED

PHONE MODEL	STATUS: LOGGED IN AND AVAILABLE	STATUS: UNAVAILABLE	LOGGED OUT
6867i 6869i 6873i	Green Softkey	Yellow Softkey	Red Softkey

ACD SUBSCRIPTION PERIOD

On the IP phones, you can set the time period, in seconds, that the IP phone resubscribes the ACD subscription service after a software/firmware upgrade or after a reboot of the IP phone.

In the configuration files, you enter the following parameter with a valid value to set the ACD subscription period:

```
sip acd subscription period: <value in seconds>
```

The minimum value for this 120 seconds (2 minutes).

The default is 3600 (1 hour).

Setting this parameter to a value lower than 3600 allows the configured ACD feature to become active more quickly after a software/firmware upgrade or after a reboot of the IP phone. If you enter a value lower than 120 for this parameter, the default value (3600) will be used by the IP phone.

You can configure this feature using the configuration files or the Mitel Web UI.

CONFIGURING ACD SUBSCRIPTION PERIOD

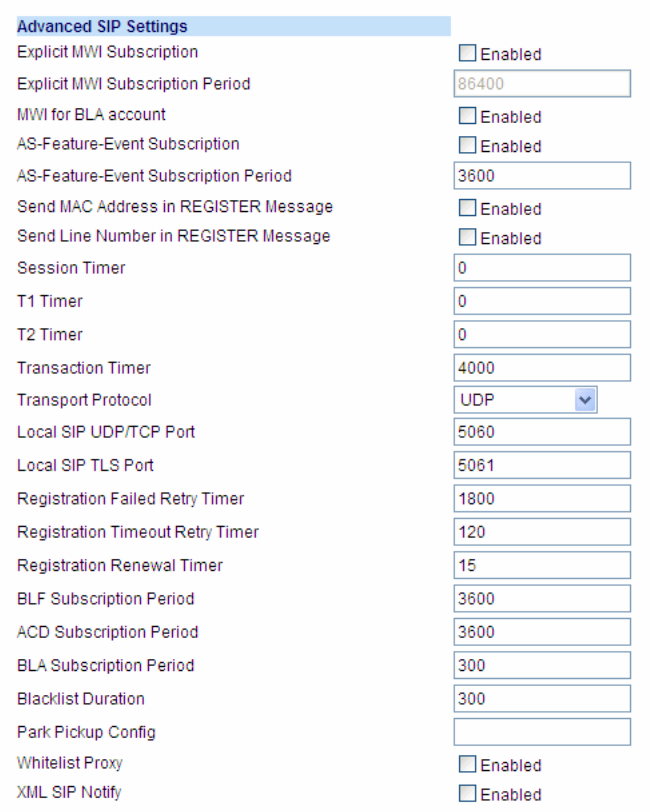
Use the following procedures to configure the ACD subscription period on the IP phone.

CONFIGURATION FILES

To configure the ACD subscription period on the IP phones using the configuration files, see Appendix A, the section, "Advanced SIP Settings" on page A-116.

MITEL WEB UI

1. Click on **Advanced Settings->Global SIP->Advanced SIP Settings.**



2. Enter a value, in seconds, from 120 (2 min) to 3600 (1 hour) in the "**ACD Subscription Period**" field.
3. Click **Save Settings** to save your changes.

DO NOT DISTURB (DND)

The IP phones have a feature you can enable called "Do Not Disturb (DND). An Administrator or User can set “Do Not Disturb” based on the accounts on the phone (all accounts or a specific account). You can set specific modes for the way you want the phone to handle DND. The three modes you can set on the phone for DND are:

- Account
- Phone
- Custom

DND ACCOUNT-BASED CONFIGURATION

An Administrator or User can configure DND on the phone-side by setting a mode for the phone to use (**account**, **phone**, or **custom**). Once the mode is set, you can use the IP Phone UI to use the DND feature.

Notes:

1. If there is only one account configured on the phone, then the mode setting is ignored and the phone behaves as if the mode was set to “Phone”.
2. You must configure a DND key on the phone to be able to use this feature via the phone’s keypad.

The following describes the DND key behavior for each DND mode.

- **Account** - DND key toggles the account in focus on the IP Phone UI, to ON or OFF if DND enabled for that account.
- **Phone** - DND key toggles all accounts on the phone to ON or OFF.
- **Custom** - DND key displays custom screens on the IP Phone UI. User can select whether to enable/disable DND per account, enable DND on all accounts, or disable DND on all accounts.

The following table describes the DND key and Message Waiting Indicator (MWI) LEDs when you enable DND on the IP Phone.

SOFTKEY LED BEHAVIOR FOR ALL MODES	MWI LED BEHAVIOR FOR ALL MODES
DND key LED RED if current account in focus has DND ON.	**MWI LED ON** if current account in focus has DND ON.
DND key LED OFF when current account in focus has DND disabled.	**MWI LED OFF** if current account in focus has DND OFF.

You can configure the DND softkey and the DND mode (**Account**, **Phone**, **Custom**) using the configuration files or the Mitel Web UI. Once you configure DND, you can access the DND screen on the IP Phone UI.

Notes:

1. In the Mitel Web UI, the “Account Configuration” page replaces the previous “Call Forward Settings” page.
2. In the IP Phone UI, the new DND key feature now has new menu screens.
3. If you make changes to the configuration for DND via the IP Phone UI, you must refresh the Mitel Web UI screen to see the changes.

CONFIGURING DND USING THE CONFIGURATION FILES

You use the following parameters to configure DND on the IP Phone:

- dnd key mode
- softkeyN type, topsoftkeyN type, prgkeyN type, or expmodX keyN type
- softkeyN states (optional)

Note: If there is no DND key configured or if it is removed, DND is disabled on the IP Phone.

Example

The following is an example of configuring the mode for DND in the configuration files:

```
dnd key mode: 2
softkey1 type: dnd
softkey1 states: idle connected incoming outgoing busy
```

In the above example, softkey 1 is configured for DND for line 1 only, with a "**custom**" configuration. Pressing softkey 1 displays DND screens for which you can customize on the phone.

CONFIGURATION FILES

To set DND in the configuration files, see Appendix A, the sections:

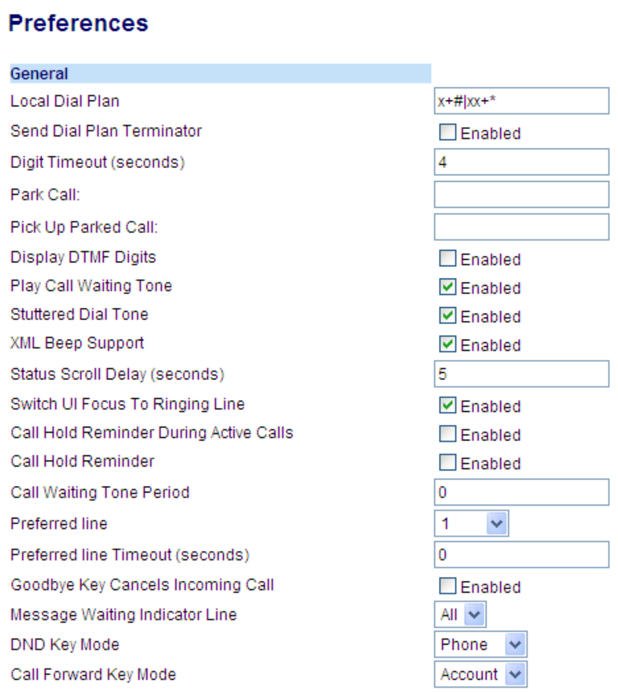
- "DND Key Mode Settings" on page A-206.
- "Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters" on page A-248.

CONFIGURING DND USING THE MITEL WEB UI

Use the following procedure to configure DND mode using the Mitel Web UI:

MITEL WEB UI

1. Click on **Basic Settings->Preferences->General.**



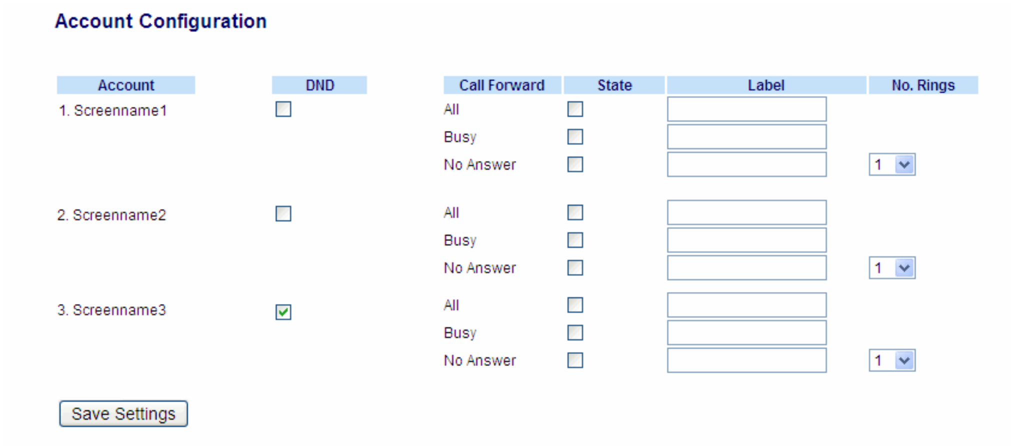
2. In the "**DND Key Mode**" field, select a "do not disturb" (DND) mode to use on the phone. Valid values are: Account, Phone, Custom. Default is **Phone**.
   - **Account** Sets DND for a specific account. DND key toggles the account in focus on the IP Phone UI, to ON or OFF.
   - **Phone** Sets DND ON for all accounts on the phone. DND key toggles all accounts on the phone to ON or OFF.
   - **Custom** Sets the phone to display custom screens after pressing the DND key, that list the
     account(s) on the phone. The user can select a specific account for DND, turn DND ON for all accounts, or turn DND OFF for all accounts.

Notes:

1. If there is only one account configured on the phone, then the mode setting is ignored and the phone behaves as if the mode was set to "Phone".
2. Using the Mitel Web UI, if you change the DND Key Mode to "phone", all accounts synchronize to the current setting of Account 1.

3. Click **Save Settings** to save your changes.
   The change takes effect immediately without a reboot.

4. Click on **Basic Settings->Account Configuration.**



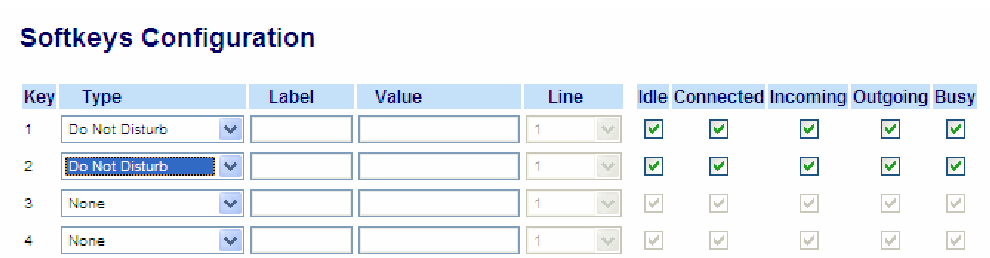
5. For each account, enable DND by placing a check mark in the box. Disable DND by unchecking the box.

Notes:

1. If you selected "**Account**" or "**Custom**" mode in step 2, you can enable/disable each account or all accounts as applicable.
   If you selected "**Phone**" mode, the first account allows you to change the DND status for all accounts.
2. Number and name of accounts that display to this screen are dependent on the number and name of accounts configured on the phone. In the screen in step 4, Screenname1 is configured on Line 1, Screenname2 is configured on Line 2, and Screenname3 is configured on Line 3. The name for the account is dependent on the name specified for the "**Screen Name**" parameter at the path *Advanced Settings->LineN*. If you do not specify a value for the "Screen Name" parameter, the account name is based on the "**Phone Number**" parameter at the path *Advanced Settings->LineN*. If neither the "Screen Name" nor the "Phone Number" parameters are specified, the account name shows "1", "2", "3", etc. only.

6. Click **Save Settings** to save your changes.
   The change takes effect immediately without a reboot.

7. Click on **Operation->Softkeys and XML**;
   or
   Click on **Operation->Programmable Keys;**
   or
   Click on **Operation->Expansion Module**.



Note: If there is no DND key configured or if it is removed, DND is disabled on the IP Phone.

8. Click **Save Settings** to save your changes.

CONFIGURING DND VIA THE IP PHONE UI (6863I/6865I/6905/6910 IP PHONES)

After you add a DND key to your phone, you can toggle the DND state using this key on the phone. Use the following procedure to enable/disable DND on the IP phone.

The following procedures assume you have already configured a DND key AND assumes there are two accounts configured on the phone.

Notes:

1. If there is no **DND** key configured or if it is removed, DND is disabled on the IP phone.
2. If there is only one account configured on the phone, then the mode setting is ignored and the phone behaves as if the mode was set to Phone.
3. Using the Mitel Web UI, if you change the DND key mode to Phone, all accounts synchronize to the current setting of Account 1.

DND in Account Mode

IP PHONE UI

1. Use the and navigation keys to scroll through each account.

```
L1     John Smith
         DND On
   Tue Aug 20 2:55pm
```

```
L2      J. Smith

   Tue Aug 20 2:55pm
```

2. With the account in focus on the IP phone UI, press the **DND** key to turn on/off DND for the account.

In the above example, two accounts are configured on the phone. Only account 1 has DND enabled while account 2 has DND disabled.

DND in Phone Mode (Default)

IP PHONE UI

1. Press the **DND** key to turn on/off DND for all accounts on the phone.

2. Use the and navigation keys to scroll through each account.

```
L1     John Smith
         DND On
   Tue Aug 20 2:55pm
```

```
L2      J. Smith
         DND On
   Tue Aug 20 2:55pm
```

In the above example, enabling DND for account 1 also enables DND for account 2.

DND in Custom Mode

IP PHONE UI

1. Press the **DND** key on the phone. The screen displays a list of the accounts on the phone and allows you to enable/disable a specific account or all accounts.
2. Use the and navigation keys to scroll through the accounts.

```
1  DND
   John Smith        ✓
   Done        Change
```

```
3  DND
   All Off
   Done        Change
```

```
2  DND
   J. Smith          X
   Done        Change
```

```
4  DND
   All On
   Done        Change
```

In the above example, account 1 has DND enabled as indicated by a check mark (✓). Account 2 has DND disabled as indicated by an **X**. The and keys allow you to disable or enable DND on all accounts, respectively.

3. Use the **Change** key to enable or disable DND for a specific account or to enable/disable DND for all accounts.
After making the change, press **Done** and then **# Confirm** to save the change. Pressing **0 Cancel** cancels the attempted change.

```
Apply Changes
0Cancel
#Confirm
```

CONFIGURING DND USING THE IP PHONE UI (6867I/6869I/6873I/6920/6930/6940)

After you add a DND key to your phone, you can toggle the DND state using this key on the phone. Use the following procedure to enable/disable DND on the IP phone.

The following procedures assume you have already configured a DND key AND assumes there are multiple accounts configured on the phone.

DND in Account Mode (6867i/6869i/6920/6930)

IP PHONE UI

1. From the Home screen press the ▶ navigation key to move to the **Line Selection** screen.
2. Highlight the desired account using the ▲ and ▼ navigation keys.
3. Press the 3 navigation key to go back to the **Home** screen
4. With the account in focus on **Home** screen, press the **DND** softkey to toggle DND on or off for the account.

DND in Account Mode (6873i/6940)

IP PHONE UI

1. From the Home screen swipe left to move to the **Line Selection** screen.
2. Press the desired account.
3. Swipe right to go back to the **Home** screen
4. With the account in focus on **Home** screen, press the **DND** softkey to toggle DND on or off for the account.

DND in Phone Mode (Default - 6867i/6869i/6873i)

IP PHONE UI

From the **Home** screen, press the **DND** softkey to toggle DND on or off for all accounts on the phone.

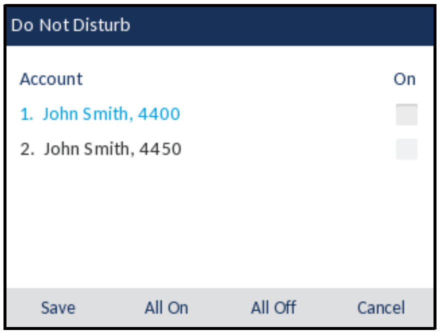
Note: Enabling DND in Phone mode toggles all accounts on the phone to DND on.

DND in Custom Mode (6867i/6869i/6920/6930)

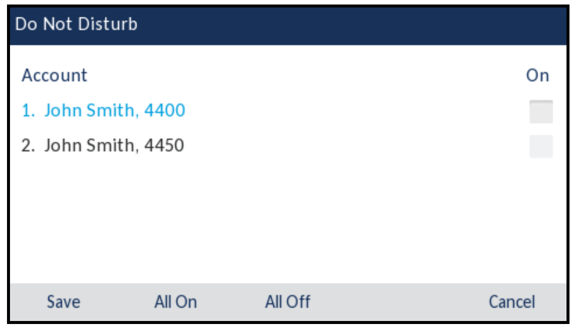
IP PHONE UI

1. From the Home screen, press the **DND** softkey.
   The screen displays a list of the accounts on the phone and allows you to enable/disable a specific account or all accounts.

6867i DND Custom Mode



6869i DND Custom Mode



2. Use the ▲ and ▼ navigation keys to scroll through the accounts and press the button to enable DND for the selected account.

> **Note:** Press the **All On** or **All Off** softkeys to quickly enable or disable DND for all accounts.

3. Press the **Save** softkey to save your changes.

DND in Custom Mode (6873i/6940)

IP PHONE UI

1. From the Home screen, press the **DND** softkey.
   The screen displays a list of the accounts on the phone and allows you to enable/disable a specific account or all accounts.

6873i DND Custom Mode

2. Press the checkbox to enable DND for the respective account.

   Note: Press the **All On** or **All Off** softkeys to quickly enable or disable DND for all accounts.

3. Press the **Save** softkey to save your changes.

BRIDGED LINE APPEARANCE (BLA)

A SIP bridge line appearance (BLA) on the IP phones allows multiple devices to share a single directory address (DA).

For example, people working at a technical support department could be located in different places. If their desktop phones are configured for BLA DA, when customer calls come in, all the phones with the BLA DA would ring but the call can only be answered by one of them.

Once the call is answered, the rest of the phones reflect the status of the call. If the call was put on "hold" by the original recipient, any one from the group can pick up the call.

Note: This feature is dependent on the IP telephony system to which the IP phone is registered and according to draft-anil-sipping-bla-02.txt.

You can apply BLA on the IP phones as follows:

- **As a single BLA group** - One BLA DA is shared among multiple phones. Only one phone at a time can pick up an incoming call or initiate an outgoing call on the BLA DA. All phones reflect the usage of the BLA DA. If the call is put on "hold", any one from the group can pick up the "held" call.
- **As a multiple BLA group** - On one single phone, multiple BLA DA can be associated with different line appearances. Every BLA DA is independent from each other and follows the same rules as "a single BLA group".
- **As multiple instances of a BLA DA** - A "x-line-id" parameter was defined in draft-anil-sipping-bla-02.txt to present the incoming call to or place an outgoing call on the specified line appearance instance. The parameter is carried in "Alert-Info" header field over the request-URI (INVITE e.g.) or in the NOTIFY messages to report the status of a dialog.

BLA DA can be configured on a global basis or on a per-line basis on the IP phones using the Mitel Web UI or the configuration files.

The following table shows the number of lines that can be set to BLA for each model phone.

IP PHONE MODEL	POSSIBLE # OF BLA LINES
6863i/ 6905	2
6865i/ 6910	24
6867i / 6920	24
6869i / 6930	24
6873i / 6940	24

CONFIGURING BLA

You can configure BLA on a global or per-line basis using the configuration files or the Mitel Web UI.

Global BLA

You configure BLA on a global basis in the configuration files using the following parameters:

- sip mode
- sip user name
- sip bla number

You configure BLA on a global basis in the Mitel Web UI using the following fields at **Advanced Settings->Global SIP->Basic SIP Authentication Settings**:

- Line Mode
- Phone Number
- BLA Number

Per-Line BLA

You configure BLA on a per-line basis in the configuration files using the following parameters:

- sip lineN mode
- sip lineN username
- sip lineN bla number

You configure BLA on a per-line basis in the Mitel Web UI using the following fields at **Advanced Settings->Line 1 thru Line N:**

- Line Mode
- Phone Number
- BLA Number

Sylantro servers and ININ servers require specific configuration methods for per-line configurations.

For Sylantro Server

When configuring the BLA feature on a per-line basis for a Sylantro server, the value set for the "sip lineN bla number" parameter shall be the same value set for the "sip lineN user name" parameter for all the phones in the group. For example, if sip lineN user name is 1010, you would configure BLA on a per-line basis for the Sylantro server as follows:

```
sip line 1 mode: 3
sip line1 user name: 1010 (# for all the phones)
sip line1 bla number: 1010
```

For ININ Server

When configuring the BLA feature on an ININ server, the value set for the sip lineN bla number parameter shall be the same value set for the sip lineN user name parameter without the incremented digit added to the phone #. For example, if the sip lineN user name for the first phone is 10101, and the sip lineN user name for the second phone is 10102, etc., you would configure BLA on a per-line basis for the ININ server as follows:

(# for phone 1 with appearance of phone 3)

```
sip line1 mode: 3
sip line1 user name: 10101 sip line1 bla number: 1010

(# for phone 2 with appearance of phone 3)

sip line1 mode: 3
sip line1 user name: 10102
sip line1 bla number: 1010

(# for phone 3)

sip line1 mode: 3
sip line1 user name: 1010
sip line1 bla number: 1010
```

Note: The original phone number which has the bridged line appearance on other phones, will have the "sip lineN user name" parameter the same as the "sip lineN bla number" (1010 in the above example on Phone 3).

Configuring Global BLA Using the Configuration Files

Use the following procedures to configure global BLA on the IP phone.

CONFIGURATION FILES

For specific **global** parameters you can set in the configuration files, see Appendix A, the section,
"SIP Basic, Global Settings" on page A-89.

Configuring Per-Line BLA Using the Configuration Files

Use the following procedures to configure per-line BLA on the IP phone.

CONFIGURATION FILES

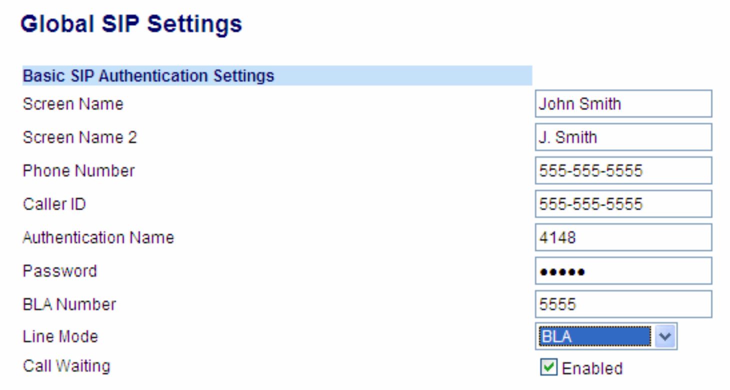
For specific **per-line** parameters you can set in the configuration files, see Appendix A, the section, "SIP Basic, Per-Line Settings" on page A-98.

Configuring BLA Using the Mitel Web UI

MITEL WEB UI

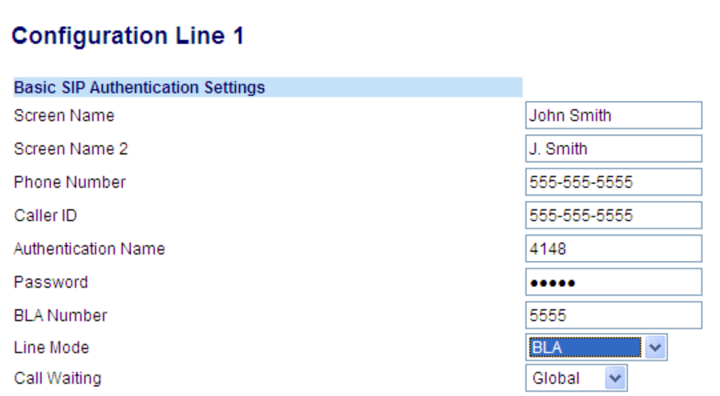
For global configuration of BLA:

1. Click on **Advanced Settings->Global SIP->Basic SIP Authentication Settings.**



For per-line configuration of BLA:

1. Click on **Advanced Settings->Line *N*.**



2. In the "**Line Mode**" field, select the **BLA** option.
3. In the "**Phone Number**" field, enter the phone number of the IP phone.
4. For global configuration of BLA:
   In the "**BLA Number**" field, enter the Bridge Line Appearance (BLA) number to be shared across all IP phones.
5. For per-line configuration of BLA:
   In the "**BLA Number**" field, enter the Bridge Line Appearance (BLA) number to be shared on a specific line.
6. Click **Save Settings** to save your changes.

BLA SUBSCRIPTION PERIOD

The IP Phones include a **SIP BLA subscription period** parameter that allows an Administrator to set the amount of time, in seconds, of the BLA subscription period.

If this parameter is set to zero (0), the phone uses the value specified for the BLA expiration in the subscribe message received from the server. If no value is specified in the Subscribe message received from the server, the phone uses the default value of 300 seconds.

You can configure this parameter using the configuration files or the Mitel Web UI.

Configuring the BLA Subscription Period

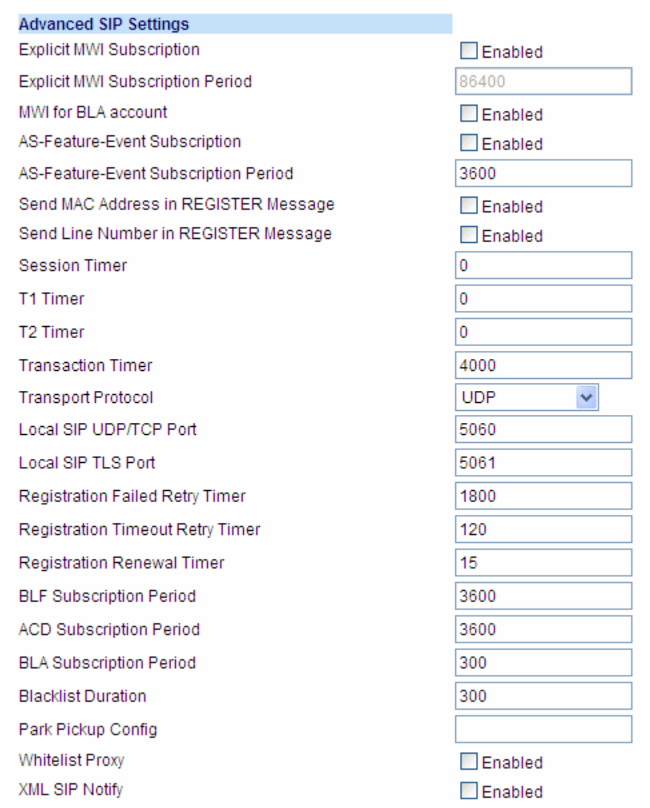
Use the following procedures to configure the BLA Subscription Period.

CONFIGURATION FILES

To configure the BLA subscription period on the IP phones using the configuration files, see Appendix A, the section, "Advanced SIP Settings" on page A-116.

MITEL WEB UI

1. Click on **Advanced Settings->Global SIP->Advanced SIP Settings.**



2. In the “**BLA Subscription Period**” field, enter a value, in seconds, that the phone waits to receive a BLA subscribe message from the server. If you specify zero (0), the phone uses the value specified for the BLA expiration in the subscribe message received from the server. If no value is specified, the phone uses the default value of 300 seconds. Valid values are 0 to 3700. Default is 300 seconds.

3. Click **Save Settings** to save your changes.

USING A BLA LINE ON THE IP PHONE

If you have either a global or per-line BLA configuration, and you want to share a call on the line with a BLA group, you need to press the Hold button before sharing the call with the group.

For example, if line 1 is configured for BLA, and you pick up a call on line 1, you must press the Hold button to share the call with the BLA group.

If you pick up a call on line 1 configured for BLA, and another call comes in on line 2, you can pick up line 2 without putting line 1 on hold. The line 1 call will be on hold automatically; however it is on hold locally only. The line 1 call cannot be shared with the BLA group.

Note: The Hold button must be pressed for a call on a BLA line to be shared with the BLA group.

BLA SUPPORT FOR THIRD-PARTY REGISTRATION

BLA allows an Address Of Record (AOR) to be assigned onto different line appearances for a group of SIP user agents (IP phones). When a call is made to this BLA number, the call is offered to all user agents that have mapping to this BLA. To support this, the IP phones need to support third party registration for the BLA along with the registration for its own primary appearance number. If the IP phone has the primary appearance as a BLA, then there is no need for third party registration.

When configuring the BLA feature on a per-line basis for third party registration and subscription, the third party name must be configured using the "**sip lineN bla number**" parameter. For third party registration to work effectively, one of the lines should register as generic with its own username.

For example, Bob has Alice's appearance on his phone. Bob's configuration is as follows:

```
#line 1 Bob

sip line1 auth name:4082272203
sip line1 password:
sip line1 mode: 0
sip line1 user name:4082272203
sip line1 display name:Bob
sip line1 screen name:Bob

#line 2 Alice

sip line2 auth name:4082272203
sip line2 password:

#BLA mode 3

sip line2 mode: 3
sip line2 user name:4082272203

#Alice phone number

sip line2 bla number:4085582868
sip line2 display name:Alice
sip line2 screen name:Alice

Alice's configuration is as follows:

#line 1

sip line1 auth name:4085582868
sip line1 password:
```

```
sip line1 mode: 3
sip line1 user name:4085582868
sip line1 display name: Alice
sip line1 screen name: Alice
```

P-PREFERRED IDENTITY HEADER FOR BLA ACCOUNTS

The IP Phones support the BLA specification, draft-anil-sipping-bla-02, which states that the P-Preferred-Identity header (RFC3325) gets added to the INVITE message to indicate the Caller-ID that is used for the call.

Note: The P-Preferred-Identity for BLA accounts is also sent for hold/unhold messages.

BLA SUPPORT FOR MESSAGE WAITING INDICATOR (MWI)

The IP Phones have an option for a Busy Line Appearance (BLA) configured line to send a SUBSCRIBE SIP message for a Message Waiting Indicator (MWI).

Notes:

1. If you change the setting on this parameter, you must reboot the phone for it to take affect.
2. Both the "**sip explicit mwi subscription**" and "**sip mwi for bla account**" parameters must be enabled in order for the MWI subscription for BLA to occur.
3. The MWI re-subscription for the BLA account uses the value set for the "**sip explicit mwi subscription period**" parameter to re-subscribe.
4.Whether or not the "**sip mwi for bla account**" parameter is enabled, the priority for displaying MWI does not change.

You can configure this feature using the configuration files or the Mitel Web UI.

Limitations

The following are limitations of the BLA Support for MWI feature:

- The phone shows MWI for the first matching identity if more than one line with different user names has the same BLA account.
- If a normal line has the same user name as the BLA user of another line, the phone shows MWI only for the normal line.

CONFIGURING BLA SUPPORT FOR MWI USING THE CONFIGURATION FILES

Use the following procedure to configure BLA support for MWI.

CONFIGURATION FILES

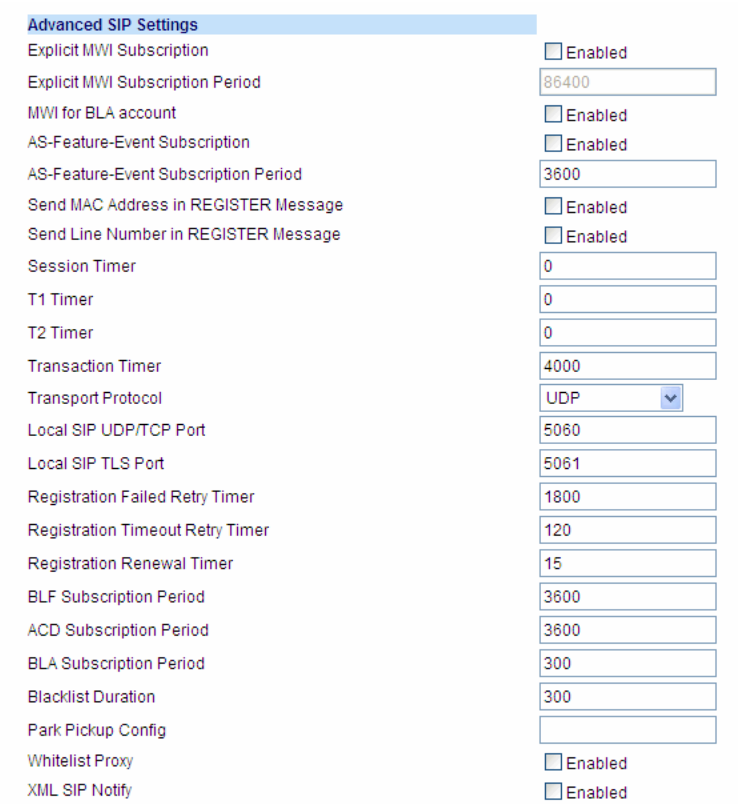
For specific parameters you can set in the configuration files, see Appendix A, the section, "BLA Support for MWI" on page A-109.

CONFIGURING BLA SUPPORT FOR MWI USING THE MITEL WEB UI

Use the following procedure to configure BLA support for MWI.

MITEL WEB UI

1. Click on **Advanced Settings->Global SIP->Advanced SIP Settings**.



2. The “**MWI for BLA Account”** field is disabled by default. To enable this feature, place a checkmark in the “**Enabled**” box.

Notes:

1. If you change the setting on this parameter, you must reboot the phone for it to take affect.
2. Both the “**sip explicit mwi subscription**” and “**sip mwi for bla account**” parameters must be enabled in order for the MWI subscription for BLA to occur.
3. The MWI re-subscription for the BLA account uses the value set for the "**sip explicit mwi subscription period**" parameter to re-subscribe.
4. Whether or not the "**sip mwi for bla account**" parameter is enabled, the priority for displaying MWI does not change

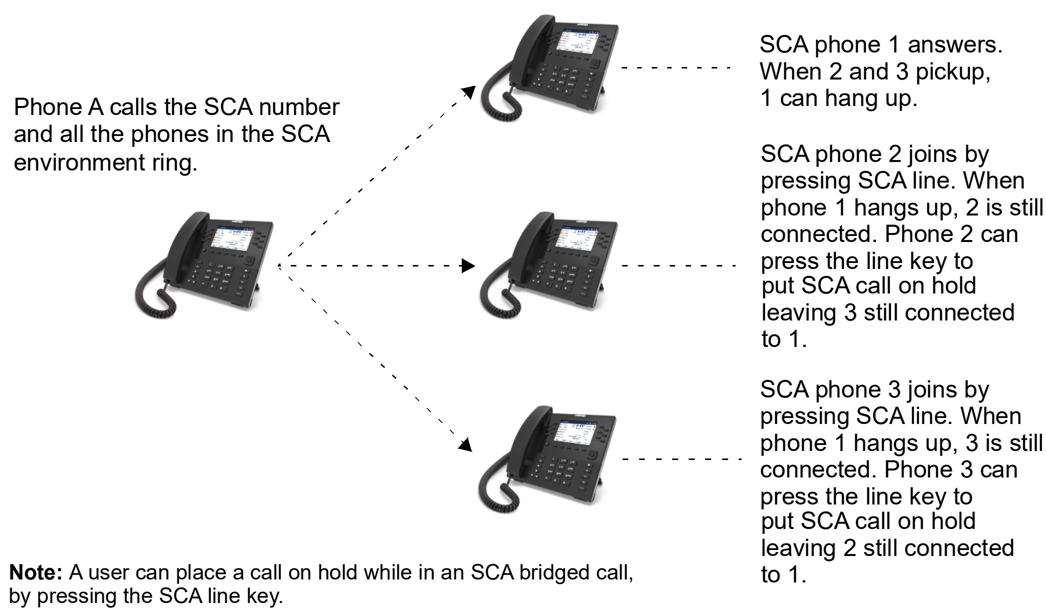
3. Click **Save Settings** to save your changes and reboot the phone for the change to take affect.

SHARED CALL APPEARANCE (SCA) CALL BRIDGING

Shared Call Appearance (SCA) is when incoming calls are presented to multiple phones simultaneously. For example, it is the ability to assign the boss' extension to a button on the secretary's phone. Calls can be transferred between two phones with the same extension button by simply putting the call on hold at one phone and picking it up on the other. Status LEDs light and flash in unison, allowing all people sharing the extension to see the status at a glance.

The IP Phones include an enhanced SCA for the servers that support call bridging and allows two or more SCA users to be connected in a call with a third party.

Refer to the following example.



Using the example above, when a call comes into Phone 1, Phone 2 and Phone 3 can pickup the same call by pressing the SCA line key. Phone 2 and 3 display the call they are bridging into on the LCD of the phones. Existing SCA parties in a bridge or one-to-one call hear an audible beep when another party has joined the call.

Note: Enabling/disabling the beep is configurable on the server-side.

If a phone is configured for SCA bridging and it attempts to join a call, but the account on the server does not have this functionality enabled, an error message displays to the LCD on the phone.

The SCA call bridging feature is disabled by default on all phones. You can enable this feature on a global or per-line basis using the configuration files only.

Note: A "Call-Info" header is included in the requests as well as the 200ok response to an INVITE, RE-INVITE, and UPDATE messages for SCA lines.

KEYS STATES AND LED BEHAVIOR

There are two new call states on the phones that support SCA bridging:

- **Bridge-active** - A bridged call is in progress
- **Bridge-held** - The 3rd-party (i.e. non-SCA party) in the bridge is on hold.

The following tables provide the key states and LED behavior in an SCA bridge call for users involved in an SCA call and users not involved in the SCA call.

Line Keys and Idle Screens

STATE	LED FOR LOCAL	CALLER ID FOR LOCAL	LED FOR REMOTE	CALLER ID FOR REMOTE
Idle	Off	N/A	Off	N/A
Seized	Solid Green	None	Solid Red	None
Progressing (outgoing call)	Green	Called Party	Solid Red	None
Alerting (incoming call)	Flashing Red	N/A	Off	N/A
Active	Solid Green	Far-end	Solid Red	Far-end
Held	Slow Flashing Green	Far-end	Slow Flashing Red	Far-end
Hold private	Slow Flashing Green	Far-end	Solid Red	Far-end
Bridge-active	Solid Green	Far-end	Solid Red	Far-end
Bridge-held	Slow Flashing Green	Far-end	Solid Red	Far-end

Softkey Line Keys

STATE	LED FOR LOCAL	LED FOR REMOTE
Idle	None	None
Seized	N/A	Solid Red
Progressing (outgoing call)	Solid Red	Solid Red
Alerting (incoming call)	Flashing Red	N/A
Active	Solid Red	Solid Red
Held	Slow Flashing Red	Slow Flashing Red
Hold private	Slow Flashing Red	Solid Red
Bridge-active	Solid Red	Solid Red
Bridge-held	Slow Flashing Red	Solid Red

Line Key Phone Behavior

STATE	LINE KEY PRESSED FOR LOCAL	LINE KEY PRESSED FOR REMOTE
Idle	N/A	Attempt to seize the line
Seized	Hang up	Ignore
Progressing	Hang up	Ignore
Alerting	answer	N/A
Active	Hold	Bridge
Held	Retrieve	Bridge
Hold private	Retrieve	Ignore
Bridge-active	Hold	Bridge
Bridge-held	Retrieve	Bridge

6867i/6869i/6873i/6920/6930/6940 Softkeys

STATE	SOFTKEY IMAGE FOR LOCAL	SOFTKEY LED FOR LOCAL (6867I/6869I ONLY)	SOFTKEY IMAGE FOR REMOTE	SOFTKEY LED FOR REMOTE (6867I/6869I ONLY)
Idle		Off		Off
Seized		Solid Red		Solid Red
Progressing (outgoing call)		Solid Red		Solid Red
Alerting (incoming call)		Flashing Red		N/A
Active		Solid Red		Solid Red
Held	(Blinking)	Slow Flashing Red	(Blinking)	Slow Flashing Red
Hold Private	(Blinking)	Slow Flashing Red	(Blinking)	Solid Red
Bridge-Active		Solid Red		Solid Red
Bridge-Held	(Blinking)	Slow Flashing Red	(Blinking)	Solid Red

LOCAL MODE SCA BEHAVIOR

If the phone is configured for Shared Call Appearance (SCA) functionality (the line mode is configured as BroadSoft SCA), the phone needs to send a SUBSCRIBE message to get a dial tone to make a call. If the network device the phone is connected to loses WAN Internet connectivity, the phone transitions into local mode.

In previous releases, the phone would continue to function (make/receive calls) locally when in local mode, but only until the SCA subscription expired. Once the subscription expired, the phone was no longer able to send a SUBSCRIBE message and therefore no dial tone was available to make a call.

Starting with Release 4.3.0 SP1. when the phone looses connection and is in local mode with the network device, the phone switches to the generic line mode instead of the BroadSoft SCA line mode. This ensures users are able to make and receive calls as the phone does not need to send the SUBSCRIBE message to get a dial tone to make a call. Once the phone is connected to the network device again, the phone leave local mode and switches back to its original BroadSoft SCA line mode.

ENABLING/DISABLING SCA CALL BRIDGING FEATURE

Use the following procedure to enable/disable SCA call bridging on the IP Phones.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section,"Shared Call Appearance (SCA) Call Bridging" on page A-109.

PARK/PICK UP STATIC AND PROGRAMMABLE CONFIGURATION

The IP phones have a park and pickup call feature that allows you to park a call and pickup a call when required. Administrators can configure call park and pickup using a static configuration (6867i/6869i/6873i/6920/6930/6940/6970) or by using a programmable configuration (all 6800 and 6900 series IP phones).

Notes:

1. The 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP phones accept both methods of configuration, however to avoid redundancy, Mitel recommends you configure either a static configuration or a programmable configuration.
2. For interoperability with the MiCloud Telepo for Service Providers call manager, Administrators must use the programmable configuration method.

Administrators can use configuration files or the Mitel Web UI to configure a park/pickup static or programmable configuration. Users can make changes to customize the label and the state of the park/pick up keys using the Web UI.

The IP phones support the Park/Pickup feature on the Asterisk, BroadWorks, Sylantro, and ININ PBX, and MiCloud Telepo servers.

The following paragraphs describe the static and programmable configuration of the call park and pickup feature.

PARK/PICKUP STATIC CONFIGURATION

Notes:

1. This feature does not work when the "collapsed context user softkey screen" parameter is enabled (see "Shifting of Softkey Positions for Busy States" on page 173).
2. For interoperability with the MiCloud Telepo for Service Providers call manager, Administrators must use the programmable configuration method.

The static method configures park and pickup on a global basis for all supported IP phones. You can use the configuration files or the Mitel Web UI to configure a park/pickup static configuration. In the configuration files, you use the following parameters to statically configure park/pickup: "**sprecode**" and "**pickupsprecode**".

In the Mitel Web UI, you use the following fields at **Basic Settings -> Preferences** to configure park/pickup statically:

- Park Call
- Pick Up Parked Call

How it Displays on the Phone

On the phone UI, the static configuration method displays the following:

- When a call comes in and you pickup the handset, the default label of “Park” displays on the first screen of the phone UI.
- After pressing the “Park” softkey to park the call, the default label of “Pickup” displays on the first screen of the phone UI.

Note: A "Drop" softkey is also offered when the "Park" softkey is pressed. Pressing the "Drop" softkey will cancel the park attempt and return the user to the original call.

The values you enter for the Park/Pickup feature are dependent on your type of server. The following table provides the values you enter for the “**sprecode”** and “**pickupsprecode”** parameters (configuration files), or "**Park Call**" and "**Pickup Parked Call**" fields (Mitel Web UI).

Park/Pickup Call Server Configuration Values

SERVER	PARK VALUES**	PICKUP VALUES**
Asterisk	70	70
Sylantro	*98	*99
BroadWorks	*68	*88
ININ PBX	callpark	pickup

**Leave "value" fields blank to disable the park and pickup feature.

Configuring Park/Pickup Static Configuration Using the Configuration Files

Use the following parameters to configure park/pickup static configuration:

- sprecode
- pickupsprecode

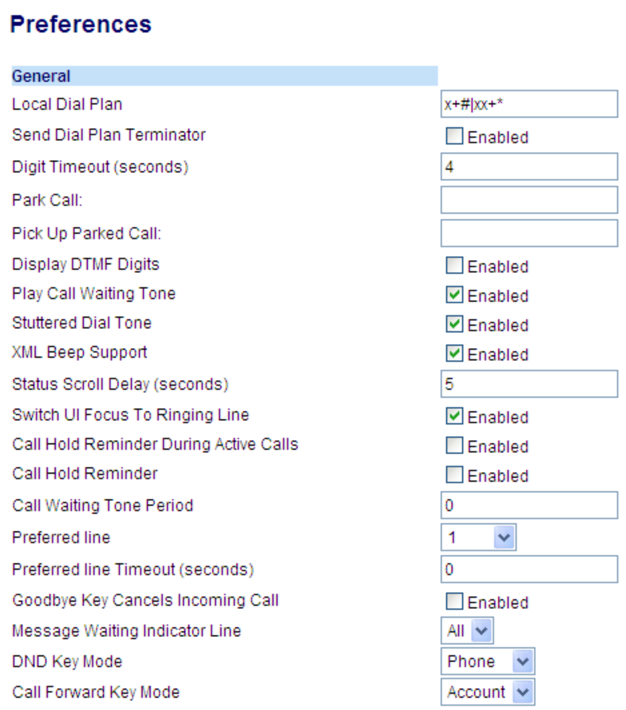
CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Park and Pickup Settings” on page A-243.

Configuring Park/Pickup Static Configuration Using the Mitel Web UI

MITEL WEB UI

1. Click on **Basic Settings ->Preferences ->General**



2. Enter a server value in the Park Call field to which incoming live calls will be parked.

Note: For values to enter in this field, see the table "Park/Pickup Call Server Configuration Values" on page 5-242.

3. Enter a server value in the Pick Up Parked Call field.

4. Click Save Settings to save your changes.

PARK/PICKUP PROGRAMMABLE CONFIGURATION (USING A SOFTKEY)

The programmable method of configuration creates park and pickup keys (softkeys, programmable keys, expansion module keys) that you can configure on the IP phones.

For the 6867i, 6869i, 6873i, 6920, 6930, and 6940 IP phones you can configure keys with park and pickup functionality and then:

- specify a customized label to display on the Phone UI
- specify the state of the park and/or pickup keys (not applicable for MiCloud Telepo interoperability)

For the 6863i, 6865i, 6905, and 6910 IP phones, you can configure programmable keys with park and pickup functionality.

On the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phone UIs

- When a call comes in, and you pickup the handset, the custom label that you configured for the park softkey displays on the Phone UI.
- After the call is parked, the label that you configured for the pickup softkey displays on other phones in the network. You can then press the pickup softkey, followed by the applicable value to pickup the call on another phone in your network.

Note: When using the MiCloud Telepo for Service Providers method of call park/pickup, the Park and Pickup softkeys will be displayed on the phone at all times.

On the 6863i, 6865i, 6905, and 6910 IP Phone UIs

When a call comes in, and you pickup the handset, you can press the applicable programmable key configured with park functionality to park the call.

After the call is parked, you can press the programmable key configured with pickup functionality, followed by the applicable value to pickup the call.

Configuring Park/Pickup Key Using Configuration Files

In the configuration files, you configure the park/pickup keys using the key parameters. You also must specify the "sip lineN park and pickup config" parameter for all applicable servers except when using the MiCloud Telepo for Service Providers call manager.

For the MiCloud Telepo call manager, two keys configured with BLF/Xfer functionality (one defined as "myCalls" and the other as "callPark") facilitates the call park/retrieve method. When the first BLF/Xfer key (defined as "myCalls") is pressed, the phone will subscribe to the myCalls@<domain>.com URI and users will be able to pick up any authorized calls. Pressing the second BLF/Xfer key (defined as "callPark") will transfer the active call to the callPark@<domain>.com URI (i.e. the park device)

The following examples show park/pickup configurations using specific servers.

Examples for 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970

SERVER	PARK CONFIGURATION	PICKUP CONFIGURATION
Asterisk	softkeyN type: **park** softkeyN label: **parkCall** softkeyN states: **connected*** sip lineN park pickup config: **70;70;asterisk**	softkeyN type: **pickup** softkeyN label: **pickupCall** softkeyN states: **idle, outgoing**** sip lineN park pickup config: **70;70;asterisk**
Sylantro	softkeyN type: **park** softkeyN label: **parkCall** softkeyN states: **connected*** sip lineN park pickup config:***98;*99;sylantro**	softkeyN type: **pickup** softkeyN label: **pickupCall** softkeyN states: **idle, outgoing**** sip lineN park pickup config: ***98;*99;sylantro**

BroadWorks	softkeyN type: **park** softkeyN label: **parkCall** softkeyN states: **connected*** sip lineN park pickup config:***68;*88;broadworks**	softkeyN type: **pickup** softkeyN label: **pickupCall** softkeyN states: **idle, outgoing**** sip lineN park pickup config: ***68;*88;broadworks**
ININ PBX	softkeyN type: **park** softkeyN label: **parkCall** softkeyN states: **connected*** sip lineN park pickup config: **callpark;pickup;inin**	softkeyN type: **pickup** softkeyN label: **pickupCall** softkeyN states: **idle, outgoing**** sip lineN park pickup config: **callpark;pickup;inin**
MiCloud Telepo for Service Providers	topsoftkeyN type: **blfxfer** topsoftkeyN label: **Park** topsoftkeyN value: **callPark**	topsoftkeyN type: **blfxfer** topsoftkeyN label: **Pickup** topsoftkeyN value: **myCalls**

*When you configure a softkey as "Park", you must configure the state of the softkey as "connected".

**When you configure a softkey as "Pickup", you can configure the state of the softkey as "idle, outgoing", or just "idle", or just "outgoing".

Examples for 6863i and 6865i

SERVER	PARK CONFIGURATION	PICKUP CONFIGURATION
Asterisk	prgkeyN type: **park** sip lineN park pickup config: **70;70;asterisk**	prgkeyN type: **pickup** sip lineN park pickup config: **70;70;asterisk**
Sylantro	prgkeyN type: **park** sip lineN park pickup config: ***98;*99;sylantro**	prgkeyN type: **pickup** sip lineN park pickup config: ***98;*99;sylantro**
BroadWorks	prgkeyN type: **park** sip lineN park pickup config: ***68;*88;broadworks**	prgkeyN type: **pickup** sip lineN park pickup config: ***68;*88;broadworks**
ININ PBX	prgkeyN type: **park** sip lineN park pickup config: **callpark;pickup;inin**	prgkeyN type: **pickup** sip lineN park pickup config: **callpark;pickup;inin**
MiCloud Telepo for Service Providers (not applicable to the 6863i)	prgkeyN type: **blfxfer** prgkeyN value: **callPark**	prgkeyN type: **blfxfer** prgkeyN value: **myCalls**

Note: The 6863i, 6865i, 6905, and 6910 do not allow for the configuration of labels and states for programmable keys.

Call Park/Pickup Configuration Precedence Rule

Note: Not applicable when using the MiCloud Telepo for Service Providers call manager for park/pickup functionality.

For users upgrading from Release 2.x firmware, the "**softkeyN value**" parameter will be used if the "**sip lineN park pickup config**" parameter is not set. If the per-line park pickup config parameter is set, the following precedence rule will apply:

1. "sip lineN park pickup config: <park_value>;<pickup_value>;<asterisk | sylantro | broadworks>" will override
   "sip park pickup config: <park_value>; <pickup_value>; <asterisk | sylantro | broadworks | inin>"
2. "sip park pickup config: <park_value>;<pickup_value>;<asterisk | sylantro | broadworks | inin>"
   will override
   "softkeyN value: <park_or_pickup_value>" (or topsoftkeyN, prgkeyN, or expmod1 keyN).
3. "softkeyN value: <asterisk|sylantro|broadworks|inin>;<park_or_pickup_value>"
   will have lowest priority.

For example, the following has been configured on the phone:

```
softkey1 type: park
softkey1 label: parkCall
softkey1 states: connected
softkey1 value: broadworks;*68
softkey2 type: pickup
softkey2 label: pickupCall
softkey2 states: idle, outgoing
softkey2 value: broadworks;*88
sip park pickup config: 70;70;asterisk
sip line1 park pickup config: *78;*98;broadworks
```

If the active call is using Line1, the phone will use the BroadWorks method for park (*78) and pickup (*98) since per-line has the highest precedence.

If the active call is using any other line except Line1, the phone will use the Asterisk method for park (70) and pickup (70) since it has precedence over the softkey value.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Expansion Module Key Settings for M680i and M685i" on page A-274, "Softkey Settings" on page A-249 and "Programmable Key Settings" on page A-259.

Configuring a Park/Pickup Key Using Mitel Web UI (for Asterisk, BroadWorks, Sylantro, and ININ Call Managers)

For all phones you first configure the park and pickup keys at **Advanced Settings -> Line 1-N** by entering the appropriate value based on the server in your network.

Note: Applicable values depend on the server in your network (Asterisk, BroadWorks, Sylantro, ININ). See the table below for applicable values.

For the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP phones, you can enter a key label and change the softkey states at **Operation->Softkeys and XML.** The default state of the park configuration is "**connected**". The default state of the Pickup configuration is "**idle, outgoing**". On the 6863i, 6865i, 6905, and 6910 IP phones, you can enter a key label at **Operation->Softkeys and XML**.

Park/Pickup Call Server Configuration Values

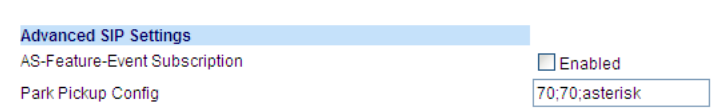
SERVER	PARK VALUES*	PICKUP VALUES*
Asterisk	70	70
Sylantro	*98	*99
BroadWorks	*68	*88
ININ PBX	callpark	pickup

Use the following procedure to configure the park/pickup call feature using the Mitel Web UI.

MITEL WEB UI

For the 6867i/6869i/6873i/6920/6930/6940/6970:

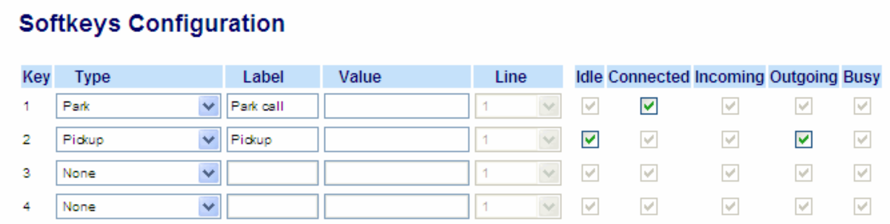
1. Click on **Advanced Settings ->Line 1** (you can select any line)
2. Under **Advanced SIP Settings** in the "**Park Pickup Config**" field, enter the appropriate value based on the server in your network.



Notes:

1. For values to enter in this field, see the table "Park/Pickup Call Server Configuration Values" on page 5-247.
2. Leave the park/pickup configuration field blank to disable the park and pickup feature.

3. Click on **Operation->Softkeys and XML.**



4. Pick a softkey to configure for parking a call.
5. In the "**Type**" field, select **Park**.
6. In the "**Label**" field, enter a label for the park softkey.

Notes:

1. The" **Value**" and "**Line**" fields are already configured from the "**Park Pickup Config**" field.
2. The park softkey has a default state of "**Connected**".
3. Leave this state enabled or to disable, uncheck the check box.

7. Pick a softkey to configure for Picking up a call.
8. In the "**Type**" field, select **Pickup**.
9. In the "**Label**" field, enter a label for the Pickup softkey.

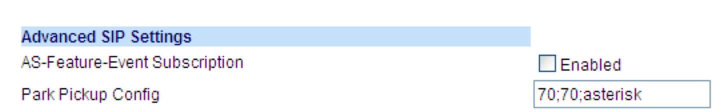
Notes:

1. The" **Value**" and "**Line**" fields are already configured from the "**Park Pickup Config**" field.
2. The pickup softkey has a default state of "**Idle**" and "**Outgoing**".
3. Leave these states enabled or to disable, uncheck the check boxes.

10. Click **Save Settings** to save your changes.
11. Click on **Reset**, then click **Restart** to restart the IP phone and apply the changes.

For the 6863i/6865i/6905/6910:

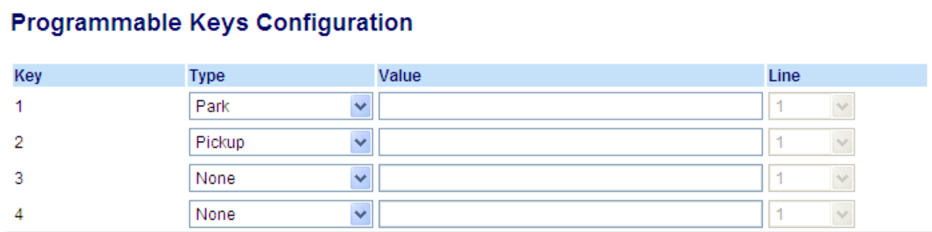
1. Click on **Advanced Settings -> Line 1** (you can select any line)
2. Under Advanced SIP Settings in the "**Park Pickup Config**" field, enter the appropriate value based on the server in your network.



Notes:

1. For values to enter in this field, see the table "Park/Pickup Call Server Configuration Values" on page 5-247.
2. Leave the park/pickup configuration field blank to disable the park and pickup feature.

3. Click on **Operation->Programmable Keys.**



4. Pick a key to configure for parking a call.
5. In the "**Type**" field, select **Park**.

Note: The" **Value**" and "**Line**" fields are already configured from the "**Park Pickup Config**" field.

6. Pick a key to configure for picking up a call.
7. In the "**Type**" field, select **Pickup**.

Note: The" **Value**" and "**Line**" fields are already configured from the "**Park Pickup Config**" field.

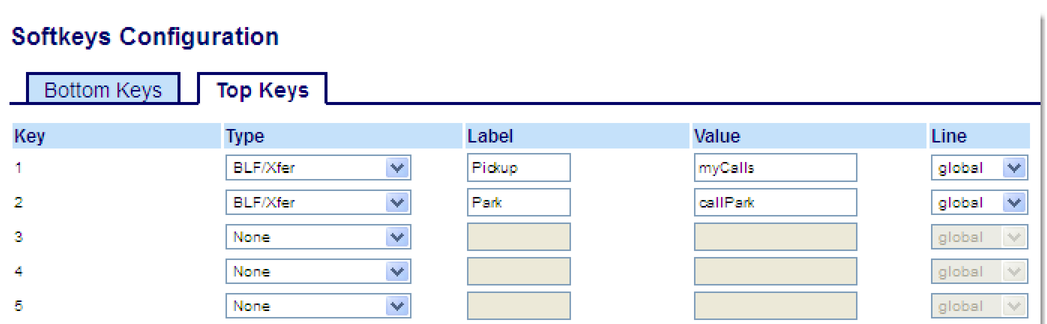
8. Click **Save Settings** to save your changes.
9. Click on **Operation->Reset**.
10. Click on **Reset**, then click **Restart** to restart the IP phone and apply the changes.

Configuring a Park/Pickup Key Using Mitel Web UI (for the MiCloud Telepo for Service Providers Call Manager)

Use the following procedure to configure a BLF/Xfer key will call park/pickup functionality using the Mitel Web UI.

MITEL WEB UI

1. Click on **Operation > Programmable Keys**
   or
   Click on **Operation > Softkeys and XML > Top Keys**
   or
   Click on **Operation > Expansion Module <N>**



2. Choose an available key that you want to use as a retrieve key and in the **Type** field, select **BLF/Xfer**.
3. (If available) In the **Label** field, enter a label to apply to this key (e.g. Pickup).
4. In the **Value** field, enter "myCalls".
5. Choose an available key that you want to use as park key and in the **Type** field, select **BLF/Xfer**.
6. (If available) In the **Label** field, enter a label to apply to this key (e.g. Park).
7. In the **Value** field, enter "callPark".
8. Click **Save Settings**.

USING THE PARK CALL/PICKUP PARKED CALL FEATURE

Use the following procedures on the IP phones to park a call and pick up a parked call.

IP PHONE UI

Parking a Call

1. While on a live call, press the "**Park**" softkey.
2. Perform the following for your specific server:

ASTERISK:
Server announces the extension number where the call has been parked. Once the call is parked, press the **Goodbye** key to complete parking.
BROADWORKS:
After you hear the greeting from the CallPark server, enter the extension where you want to park the call.
SYLANTRO:
Enter the extension number where you want to park the call, followed by "**#**" key.
NIN PBX:
Enter the extension number where you want to park the call, followed by "**#**" key.
MICLOUD TELEPO:
Not applicable to the MiCloud Telepo call park method.

If the call is parked successfully, the response is either a greeting voice confirming that the call was parked, or a hang up occurs.

3. If the call fails, you can pick up the call (using the next procedure) and press the "**Park**" softkey again to retry step 2.

Picking up a Parked Call

1. Pick up the handset on the phone.
2. Enter the extension number where the call was parked (not applicable to the MiCloud Telepo call pickup method).
3. Press the "**Pickup**" softkey.
   If the call pick up is successful, you are connected with the parked call.

LAST CALL RETURN (LCR) (SYLANTRO SERVERS)

Last call return (LCR) allows an administrator or user to configure a "last call return" function on a softkey or programmable key. This feature is for Sylantro servers only.

You can configure the "lcr" softkey feature via the configuration files or the Mitel Web UI.

HOW IT WORKS

If you configure "lcr" on a softkey or programmable key, and a call comes into your phone, after you are finished with the call and hangup, you can press the key configured for "lcr" and the phone dials the last call you received. When you configure an "lcr" softkey, the label "LCR" displays next to that softkey on the IP phone. When the Sylantro server detects an "lcr" request, it translates this request and routes the call to the last caller.

CONFIGURING LAST CALL RETURN

Use the following procedures to configure LCR on the IP phones.

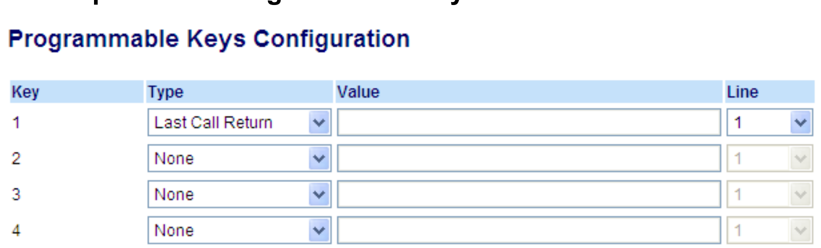
CONFIGURATION FILES

For specific last call return (lcr) parameters you can set in the configuration files, see Appendix A, the section, "Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters" on page A-248.

MITEL WEB UI

For the 6863i/6865i/6905/6910:

1. Click on **Operation->Programmable Keys.**



2. Pick a key to configure for Last Call Return.

3. In the "**Type**" field, select **Last Call Return**.
4. In the "**Line**" field, select a line for which to apply the lcr configuration.
5. Click **Save Settings** to save your changes.

CALL FORWARDING

Call Forward (CFWD) on the IP phone allows incoming calls to be forwarded to another destination. The phone sends the SIP message to the SIP proxy, which then forwards the call to the assigned destination.

An Administrator or User can configure CFWD on the phone-side by setting a mode for the phone to use (**Account**, **Phone**, or **Custom**). Once the mode is set, you can use the IP Phone UI to use the CFWD feature at *Options->Call Forward* or by pressing a configured Call Forward softkey/programmable key/extension module key.

The following describes the behavior for each CFWD mode.

- **Account mode** - The account mode allows you to configure CFWD on a per account basis. Pressing a configured CFWD key applies to the account in focus.
- **Phone mode** - The Phone mode allows you to set the same CFWD configuration for all accounts (**All**, **Busy**, and/or **No Answer**). When you configure the initial account, the phone applies the configuration to all other accounts. (In the Mitel Web UI, only the account you configured is enabled. All other accounts are grayed out but set to the same configuration.) Using the Mitel Web UI, if you make changes to that initial account, the changes apply to all accounts on the phone.
- **Custom mode** - The Custom mode allows you to configure CFWD for a specific account or all accounts. You can configure a specific mode (**All**, **Busy**, and/or **No Answer**) for each account independently or all accounts. You can set all accounts to **ALL On** or **ALL Off** or copy the configuration for the account in focus to all other accounts using a **CopytoAll** softkey (on the 6867i, 6869i, and 6873i IP phones).

Note: If there is only one account configured on the phone, then the mode setting is ignored and the phone behaves as if the mode was set to “Phone”.

You can enable different call forwarding rules/modes independently (for example, you can set different phone numbers for Busy, All, and NoAns modes and then turn them on/off individually).

The following table describes the key and Message Waiting Indicator (MWI) LEDs when you enable CFWD on the IP Phone.

KEY LED BEHAVIOR FOR ALL MODES	MWI LED BEHAVIOR FOR ALL MODES
CFWD key LED RED if any CFWD mode is enabled for the account in focus.	**MWI LED ON** if any CFWD mode is enabled for the account in focus.
CFWD key LED OFF if all CFWD modes are disabled for the account in focus.	**MWI LED OFF** if all CFWD modes are disabled for the account in focus.

You can enable/disable CFWD and set a CFWD key using the configuration files or the Mitel Web UI. You can set CFWD mode (**Account**, **Phone**, **Custom**) using the configuration files, Mitel Web UI or IP Phone UI.

Notes:

1. In the configuration files, the "**call forward key mode**" parameter in the section, "Call Forward Busy or Call Forward No Answer Option to Turn Off MWI LED" on page 5-253 is in addition to the previous call forward parameter (**call forward disabled**). You can still use the previous call forwarding parameter if desired in the configuration files.
2. In the IP Phone UI, you can access the Call Forwarding features at the path *Options->Call Forward* or by pressing a configured CFWD key.
3. If you make changes to the configuration for CFWD via the IP Phone UI, you must refresh the Mitel Web UI screen to see the changes.

Call Forward Busy or Call Forward No Answer Option to Turn Off MWI LED

With Release 5.0.0 SP1, when Call Forward is set to either "Call Forward Busy" or "Call Forward No Answer" options, the MWI LED on the SIP phone turns off. The LED turns on only when Call Forward is set to "Call Forward All".

CONFIGURING CALL FORWARDING

You use the following parameters to set CFWD on the IP Phone using the configuration files:

- call forward key mode
- softkeyN type, topsoftkeyN type, prgkeyN type, or expmodX keyN type
- **softkeyN states** (optional)

Notes:

1. If there is no CFWD key configured on the phone or it is removed, you can still set the CFWD modes via the IP Phone UI at the path *Options->Call Forward*.
2. If there is only one account configured on the phone, then the mode setting is ignored and the phone behaves as if the mode was set to "Phone".
3. When configuring a CFWD mode (**All**, **Busy**, **No Answer**) for an account, you must configure a CFWD number for that mode in order for the mode to be enabled.

Use the following procedures to configure Call Forwarding on the IP phones.

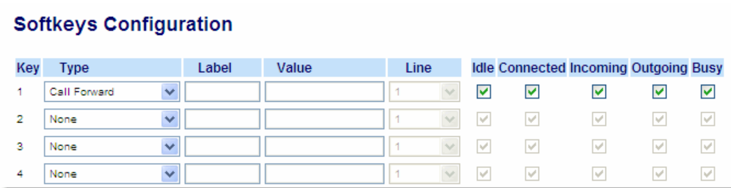
CONFIGURATION FILES

For specific call forwarding parameters you can set in the configuration files, see Appendix A, the sections,

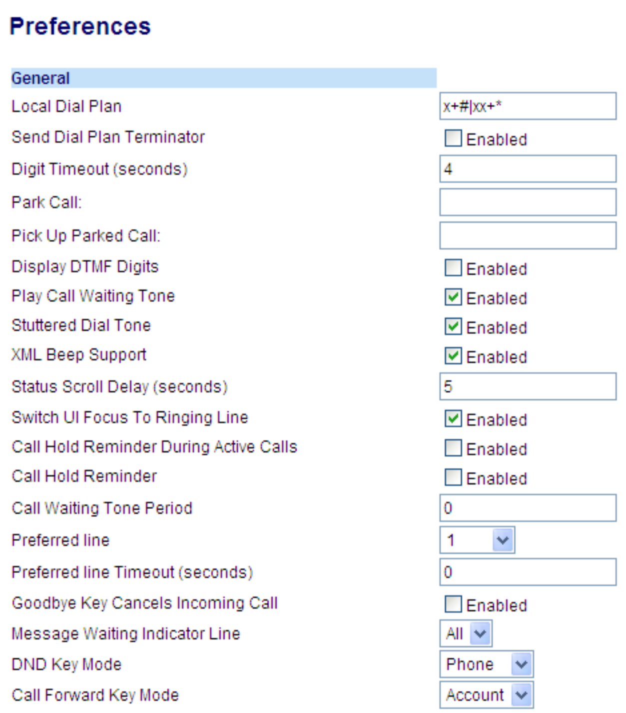
- "Call Forward Settings" on page A-180.
- "Call Forward Key Mode Settings" on page A-181.
- "Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters" on page A-248.

MITEL WEB UI

1. Click on **Operation->Softkeys and XML**;
   or
   Click on **Operation->Programmable Keys;**
   or
   Click on **Operation->Expansion Module**.



2. Click **Save Settings** to save your changes.
3. Click on **Basic Settings->Preferences->General.**



Note: If there is no CFWD key configured on the phone or it is removed, you can still set the CFWD modes via the IP Phone UI at the path *Options->Call Forward.*

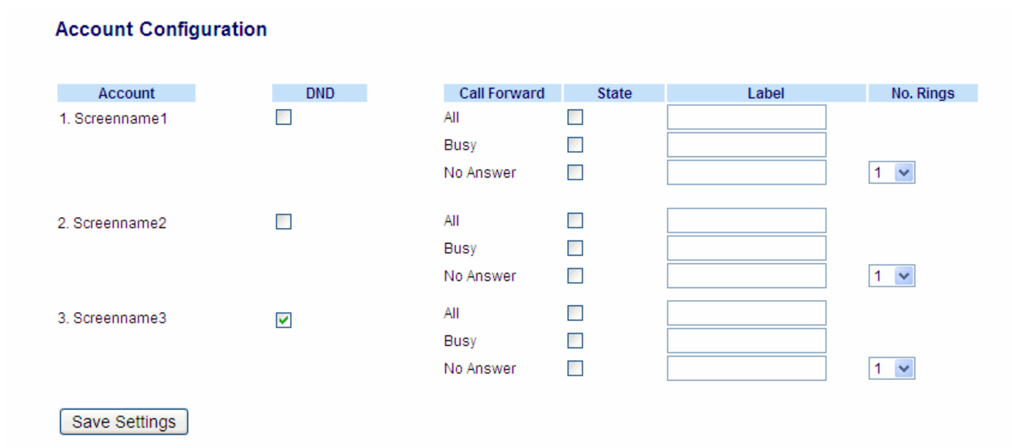
4. In the "**Call Forward Key Mode**" field, select a call forward mode to use on the phone. Valid values are: Account, Phone, Custom. Default is **Account**.
   - **Account**
     The account mode allows you to configure CFWD on a per account basis. Pressing a configured CFWD key applies to the account in focus.

- **Phone**
  The Phone mode allows you to set the same CFWD configuration for all accounts (**All**, **Busy**, and/or **No Answer**). When you configure the initial account, the phone applies the configuration to all other accounts. (In the Mitel Web UI, only the account you configured is enabled. All other accounts are grayed out but set to the same configuration.) Using the Mitel Web UI, if you make changes to that initial account, the changes apply to all accounts on the phone.
- **Custom**
  The Custom mode allows you to configure CFWD for a specific account or all accounts. You can configure a specific state (**All**, **Busy**, and/or **No Answer**) for each account independently or all accounts. On the 6863i/6865i IP phones, you can set all accounts to **ALL On** or **ALL Off**. On the 6867i/6869i/6873i IP phones, you can set all accounts to **All On**, **All Off**, or copy the configuration for the account in focus to all other accounts using a **CopytoAll** softkey.

Notes:

1. If there is no CFWD key configured on the phone or it is removed, you can still set the CFWD modes via the IP Phone UI at the path *Options->Call Forward.*
2. If there is only one account configured on the phone, then the mode setting is ignored and the phone behaves as if the mode was set to “Phone”.
3. When configuring a CFWD state (**All**, **Busy**, **No Answer**) for an account, you must configure a CFWD number for that state in order for the state to be enabled.

5. Click **Save Settings** to save your changes.
   The change takes effect immediately without a reboot.
6. Click on **Basic Settings->Account Configuration.**



Note: If the BroadSoft BroadWorks Executive and Assistant Services feature is enabled and your phone is configured with the Assistant’s role, an additional Forward Filtering option may be available on the Account Configuration page. For information on the BroadWorks Executive and Assistant Services feature, refer to “BroadSoft BroadWorks Executive and Assistant Services” on page 6-94. For details on how to configure and utilize Forward Filtering, please refer to the respective phone model’s ***Mitel SIP Phone User Guide***.

7. For each account, enable CFWD state by placing a check mark in one or more of the following "**State**" fields:
   - All
   - Busy
   - No Answer

   The "**All**" option forwards all incoming calls for this account to the specified phone number regardless of the state of the phone. The phone can be in the Busy or No Answer states, or can be in the idle state. The phone still forwards all calls to the specified number.

   The "**Busy**" option call forwards incoming calls only if the account is in the busy state. The calls are forwarded to the specified phone number.

   The "**No Answer**" option call forwards incoming calls only if the account rings but is not answered in the defined number of rings. The call gets forwarded to the specified number.

   Note: You can use the "**Busy**" and "**No Answer**" states together using different forwarding phone numbers. If these states are enabled for an account (the "**All**" state is disabled), and the phone is in the busy state when a call comes in, the phone can forward the call to the specified phone number (for example, voicemail). If there is no answer on the phone after the specified number of rings, the phone can forward the call to a different specified number, such as a cell phone number.

8. For each account, in the "**Number**" field, enter the phone number for which you want the incoming calls to forward to if the phone is in the specified state.

If using the “**Account**” mode or “**Custom**” mode, you can enter different phone numbers for each account.

Notes:

1. If you selected “Account” mode in step 4, you can enable/disable each account or all accounts as applicable. You can enter different phone number for each enabled state.
2. If you selected “Custom” mode, you can enable/disable each account or all accounts as applicable. You can enter different phone numbers for each enabled state.
3. If you selected “Phone” mode, all accounts are set to the same CFWD configuration (All, Busy, and/or No Answer) as Account 1 on the phone. (In the Mitel Web UI, only Account 1 is enabled. All other accounts are grayed out but use the same configuration as Account 1.)
4. Using the Mitel Web UI, if you make changes to Account 1, the changes apply to all accounts on the phone. Using the IP Phone UI, if you make changes to any other account other then Account 1, the changes also apply to all accounts on the phone. When enabling a CFWD state, you must specify a phone number for the phone to CFWD to. The number you specify applies to all accounts of the same mode.
5. Number and name of accounts that display to this screen are dependent on the number and name of accounts configured on the phone. In the screen in step 6, Screenname1 is configured on Line 1, Screenname2 is configured on Line 2, and Screenname3 is configured on Line 3. The name for the account is dependent on the name specified for the “**Screen Name**” parameter at the path *Advanced Settings->LineN*. If you do not specify a value for the “Screen Name” parameter, the account name is based on the “**Phone Number**” parameter at the path *Advanced Settings->LineN*. If neither the “Screen Name” nor the “Phone Number” parameters are specified, the account name shows “1”, “2”, “3”, etc. only.

9. For the **No Answer** state, in the “**No. Rings**” field, enter the number of times that the account rings before forwarding the call to the specified number. Valid values are 1 through 20. Default is 1.

   Note: When using the “**Account**” mode or “**Custom**” mode, you can enter a different number of rings for each account. If you use the Mitel Web UI to change the Call Forward Key Mode to “**Phone**”, all accounts synchronize to Account 1.

10. Click **Save Settings** to save your changes.
    The change takes effect immediately without a reboot.

CONFIGURING CFWD VIA THE IP PHONE UI (6863I/6865I/6905/6910)

Once CFWD is enabled on your phone, you can access and change the configuration using the IP phone UI or the Mitel Web UI. You can access the CFWD menus by pressing a pre-configured **CFWD** key, or by selecting *Options* > *Call Forward* from the IP phone UI.

Notes:

1. If there is no CFWD key configured on the phone or it is removed, you can still enable CFWD via the at the path *Options->Call Forward*.
2. If there is only one account configured on the phone, then the mode setting is ignored and the phone behaves as if the mode was set to “Phone”.
3. Using the Mitel Web UI, if you change the CFWD key mode to “**Phone**”, all accounts synchronize to the current setting of Account 1.
4. If the BroadSoft BroadWorks Executive and Assistant Services feature is enabled and your phone is configured with the Assistant’s role, an additional Forward Filtering option may be available on the CFWD Mode menu. For information on the BroadWorks Executive and Assistant Services feature, refer to “BroadSoft BroadWorks Executive and Assistant Services” on page 6-94. For details on how to configure and utilize Forward Filtering, please refer to the respective phone model’s ***Mitel SIP Phone User Guide***.

CFWD in Account Mode

IP PHONE UI

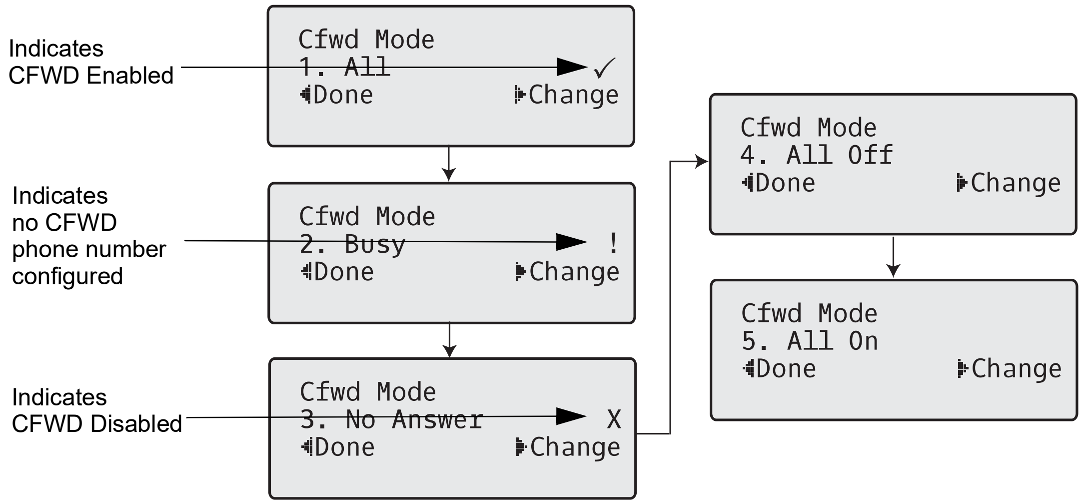
1. Use the ◀ and ▶ navigation keys to scroll through each account.

```
L1     John Smith
       CFWD All
   Tue Aug 20 2:55pm
```

```
L2       J. Smith
        CFWD Busy
   Tue Aug 20 2:55pm
```

In the above example, account 1 has CFWD All enabled and account 2 has CFWD Busy enabled.

2. Press the programmed **Call Forward** key. The Call Forward Mode screen displays. Use the ▲ and ▼ navigation keys to scroll through each state type.



In the above example, CFWD All is enabled as indicated by a check mark (✓), CFWD Busy is enabled but no call forward phone number configured as indicated by a **!**, and CFWD No Answer is disabled, as indicated by an **X**.

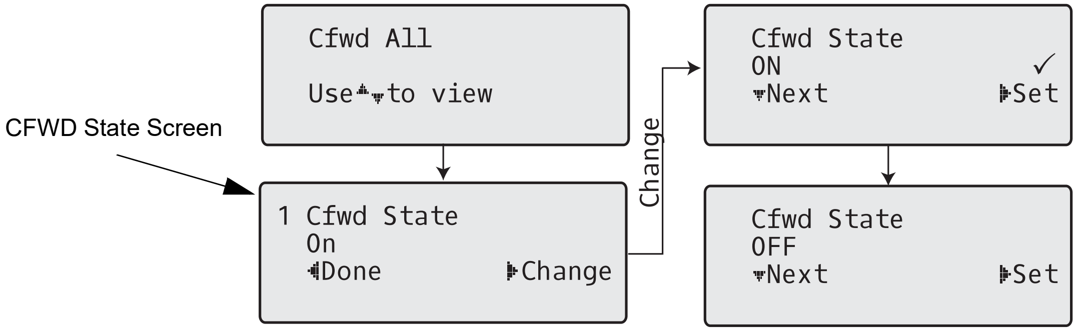
3. Select a state for the account(s) in focus using the ▲ and ▼ navigation keys.
   You can enable/disable any or all of the following states for an account:
   - All: Forwards all incoming calls for the respective account to the specified number.
   - Busy: Forwards incoming calls to a specified number if DND has been enabled for that account OR if the account is currently engaged in another call.
   - No Answer: Forwards incoming calls to a specified number if the call has not been answered for the specified number of rings.

Note: If CFWD All, CFWD Busy, and CFWD No Answer are all enabled (and/or if the account has DND enabled), the CFWD All settings take precedence over CFWD Busy and CFWD No Answer.

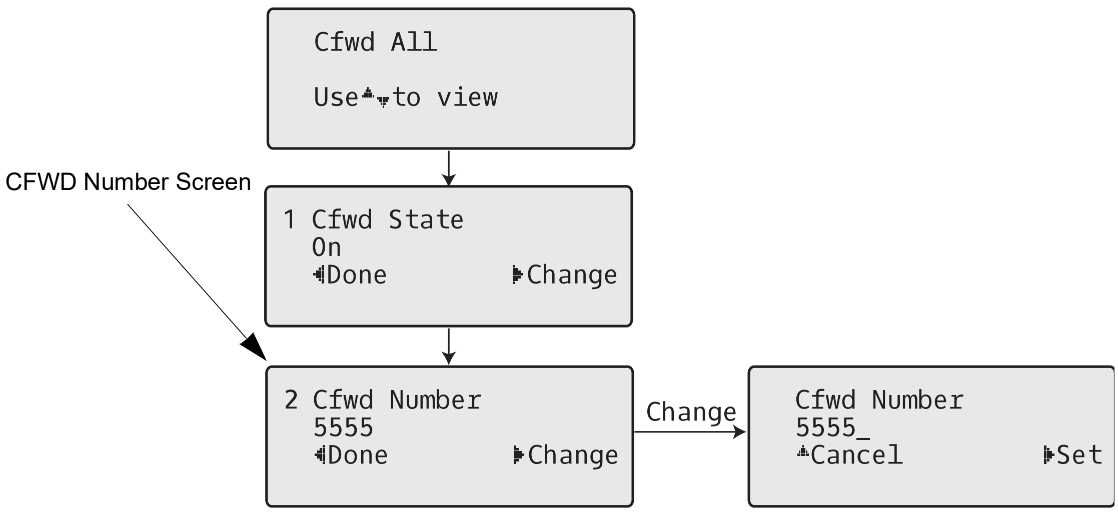
You can also use the following keys if required:

- All Off: Disables all CFWD states for the current account in focus
- All On: Enables all CFWD states for the current account in focus

4. Press the **Change** navigation key for the state you selected in Step 3. Scroll to the CFWD State screen. This displays the current state of the mode you selected. In the following example, the CFWD All state is ON.



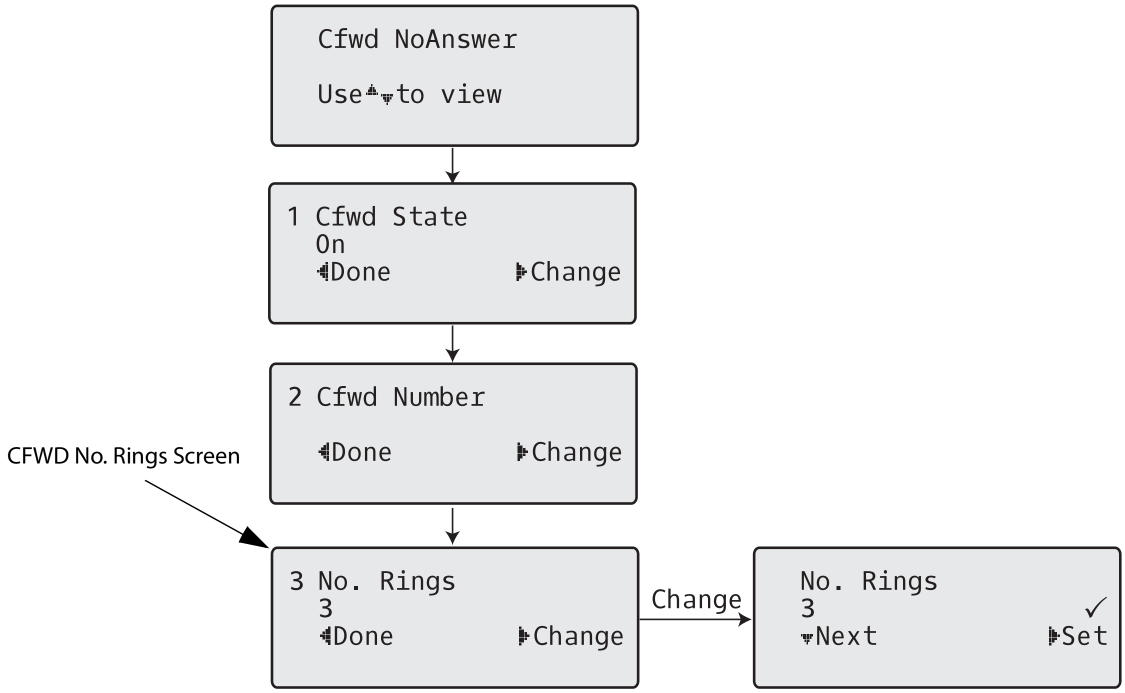
5. Press the **Change** navigation key in the CFWD State screen. Press 2 to toggle the state of the CFWD mode ON or OFF. In the example in Step 4, you press 2 to change the option to OFF.
6. Press **Set** to save the change.
7. In the CFWD State screen, press the ▲ navigation keys to scroll to the CFWD Number screen and press **Change.**



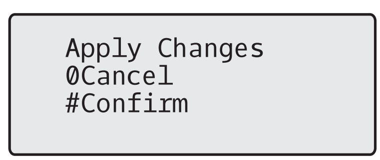
Enter a phone number to apply to the current state in focus. When the phone is in the state you specified, and a call comes into the phone, it forwards the call to the number you specify.

8. Press **Set** to save the change.

9. For the **CFWD No Answer** state, In the CFWD Number screen, press the navigation key to scroll to the CFWD No. Rings screen and press 4**Change**.



10. Press 2**Next** to select the number of rings to apply to the phone for call forwarding incoming calls. Valid values are 1 to 20. Default is 3.
    When the phone receives an incoming call, and call forward is configured on the phone, the phone rings the number of times you specify in the No. Rings screen, and then forwards the call if there is no answer.
11. Press 4**Set** to save the change.
12. Press 3**Done** to save all your changes.
    Each time you press **Done**, the following screen displays.

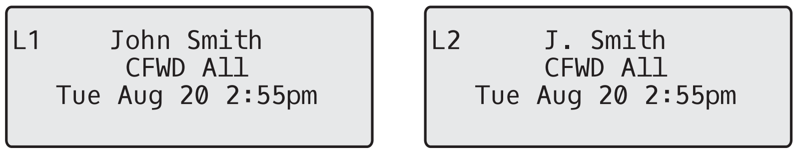


13. Press **# Confirm** to confirm the change(s) each time the Apply Changes screen displays. All changes are saved to the phone.

CFWD in Phone Mode

IP PHONE UI

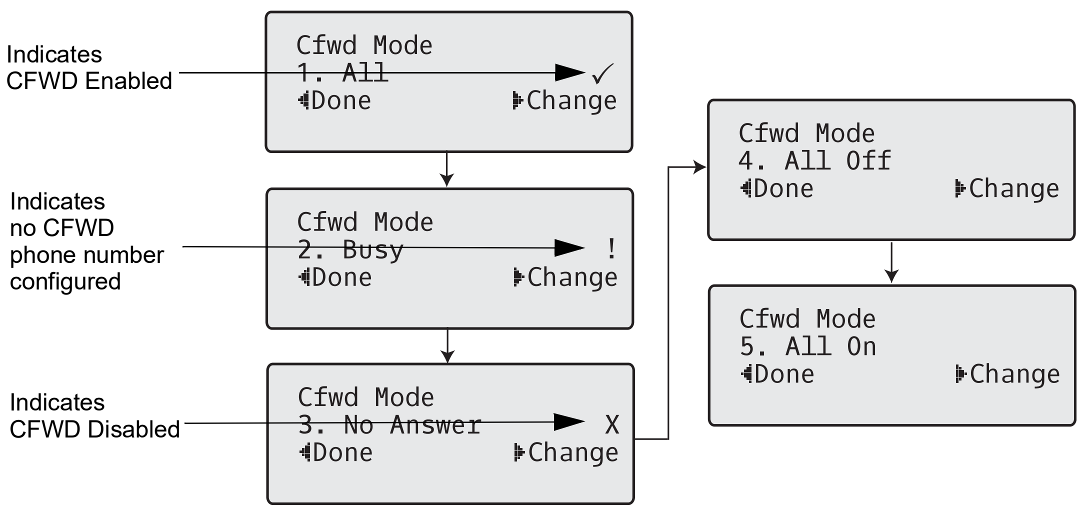
1. Use the ◄ and ► navigation keys to scroll through each account.



In the above example, account 1 and account 2 are the accounts configured on the phone. Both accounts have CFWD enabled as indicated by the **CFWD All** message.

> **Note:** In Phone mode, when you change the call forward configuration for an account, the change applies to all accounts.

2. Press the **Call Forward** key. The Call Forward menu displays. Use the ▲ and ▼ navigation keys to scroll through each state type.



In the above example, CFWD All is enabled as indicated by a check mark (✓), CFWD Busy is enabled but no call forward phone number configured as indicated by a **!**, and CFWD No Answer is disabled, as indicated by an **X**.

3. Select a state using the ▲ and ▼ navigation keys.
   You can enable/disable a specific account on the phone with any or all of the following states. However, the configuration you set will apply to all accounts on the phone.
   - All: Forwards all incoming calls for the respective account to the specified number.
   - Busy: Forwards incoming calls to a specified number if DND has been enabled for that account OR if the account is currently engaged in another call.

- No Answer: Forwards incoming calls to a specified number if the call has not been answered for the specified number of rings.

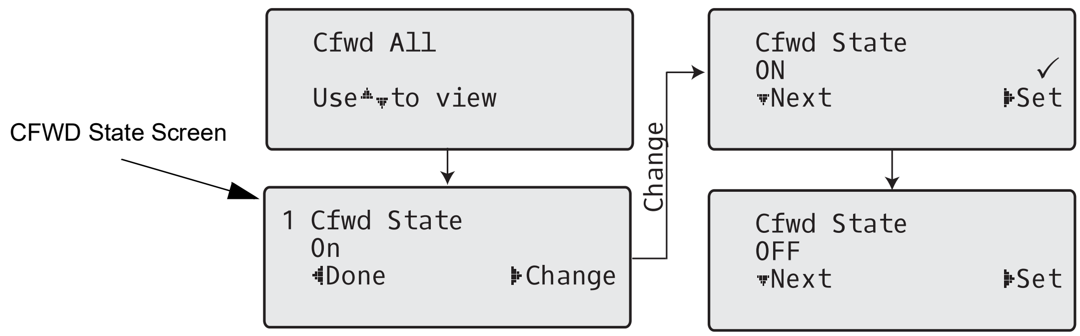
Note: If CFWD All, CFWD Busy, and CFWD No Answer are all enabled (and/or if the account has DND enabled), the CFWD All settings take precedence over CFWD Busy and CFWD No Answer.

You can also use the following keys if required:

- All Off: Disables all CFWD states for the current account in focus
- All On: Enables all CFWD states for the current account in focus

Note: In Phone mode, the initial configuration you set for an account applies to all the accounts on the phone.

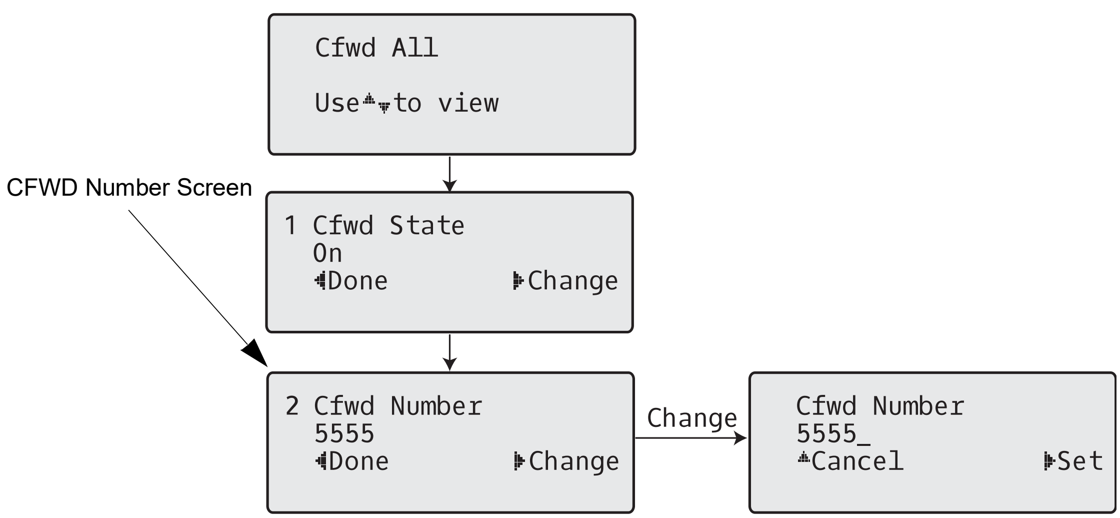
4. Press the 4**Change** key for the mode you selected in Step 2. Scroll to the CFWD State screen. This screen displays the current state of the mode you selected. In the following example, the CFWD All state is ON.



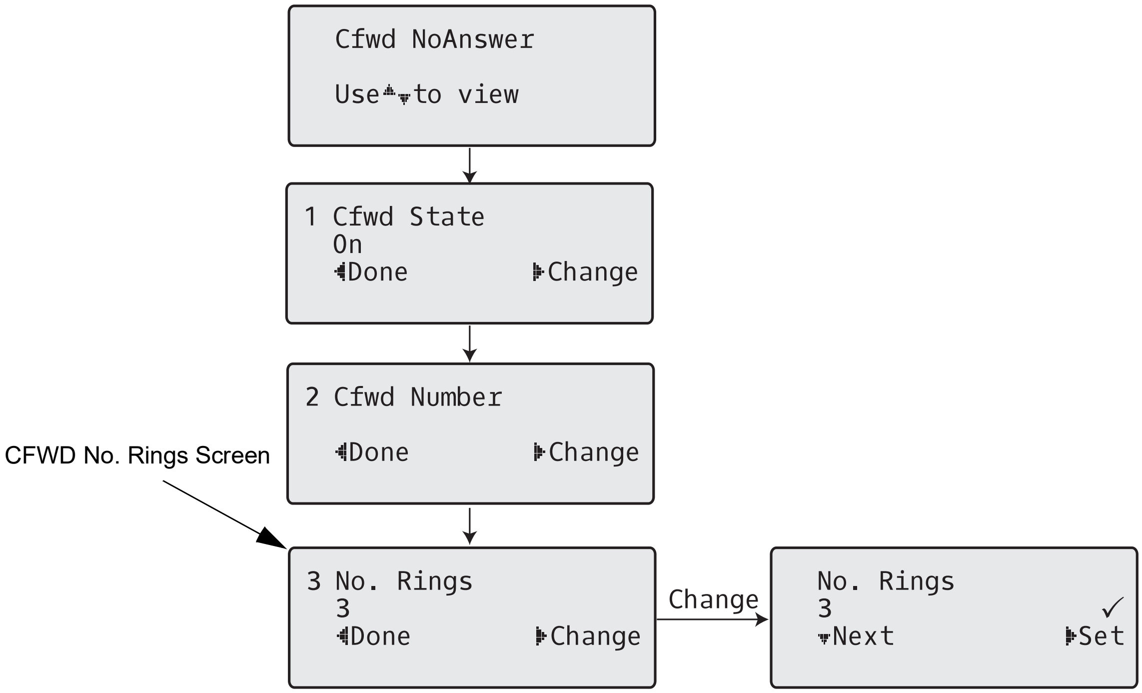
5. Press the 4**Change** key in the CFWD State screen. Press 2**Next** to toggle the state of the CFWD state ON or OFF. In the example in Step 4, you press 2**Next** to change the option to **Off**.

6. Press the 4**Set** key to save the change.

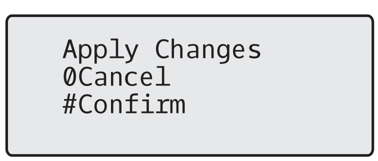
7. In the CFWD State screen, press the ▲ navigation key to scroll to the CFWD Number screen and press 4**Change.**



8. Enter a phone number to apply to the current state in focus. When the phone is in the state you specified, and a call comes into the phone, it forwards the call to the number you specify.
9. Press 4**Set** to save the change.
10. For the CFWD No Answer state, in the CFWD Number screen, press the ▲ navigation key to scroll to the CFWD No. Rings screen and press 4**Change.**



11. Press the 2**Next** key to select the number of rings to apply to the phone for call forwarding incoming calls. Valid values are 1 to 20. Default is 3.
When the phone receives an incoming call, and call forward is configured on the phone, the phone rings the number of times you specify in the No. Rings screen, and then forwards the call.
12. Press 4**Set** to save the change.
13. Press 3**Done** to save all your changes.
Each time you press 3**Done**, the following screen displays.

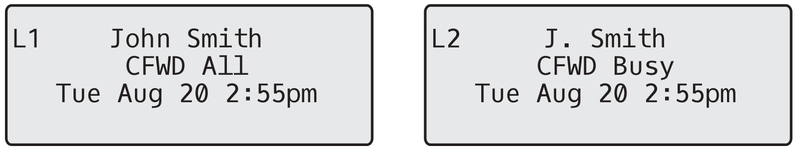


14. Press **# Confirm** to confirm the change(s) each time the Apply Changes screen displays. All the same changes are saved to all accounts on the phone.

CFWD in Custom Mode

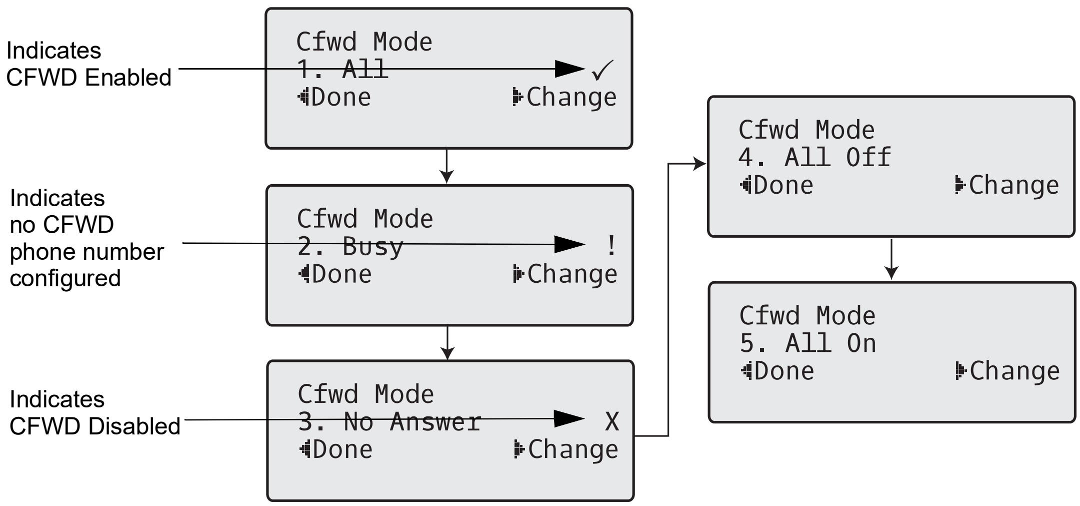
IP PHONE UI

1. Use the and navigation keys to scroll through each account.



In the above example, account 1 has CFWD All enabled and account 2 has CFWD Busy enabled.

2. Press the **Call Forward** key. The Call Forward menu displays. Use the and navigation keys to scroll through each state type.



In the above example, CFWD All is enabled as indicated by a check mark (✓), CFWD Busy is enabled but no call forward phone number configured as indicated by a **!**, and CFWD No Answer is disabled, as indicated by an **X**.

3. Select a state for the account(s) in focus using the and navigation keys.
You can enable/disable any or all of the following states for a specific account or for all accounts (with individual configurations):
   - All: Forwards all incoming calls for the respective account to the specified number.
   - Busy: Forwards incoming calls to a specified number if DND has been enabled for that account OR if the account is currently engaged in another call.
   - No Answer: Forwards incoming calls to a specified number if the call has not been answered for the specified number of rings.

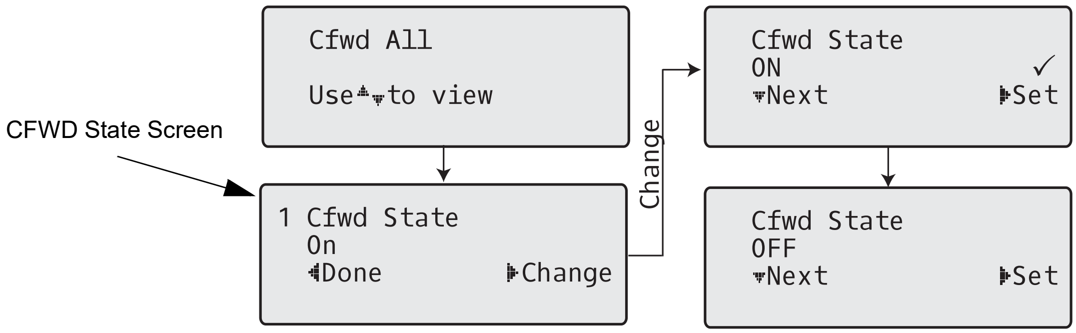
Note: If CFWD All, CFWD Busy, and CFWD No Answer are all enabled (and/or if the account has DND enabled), the CFWD All settings take precedence over CFWD Busy and CFWD No Answer.

You can also use the following keys if required:

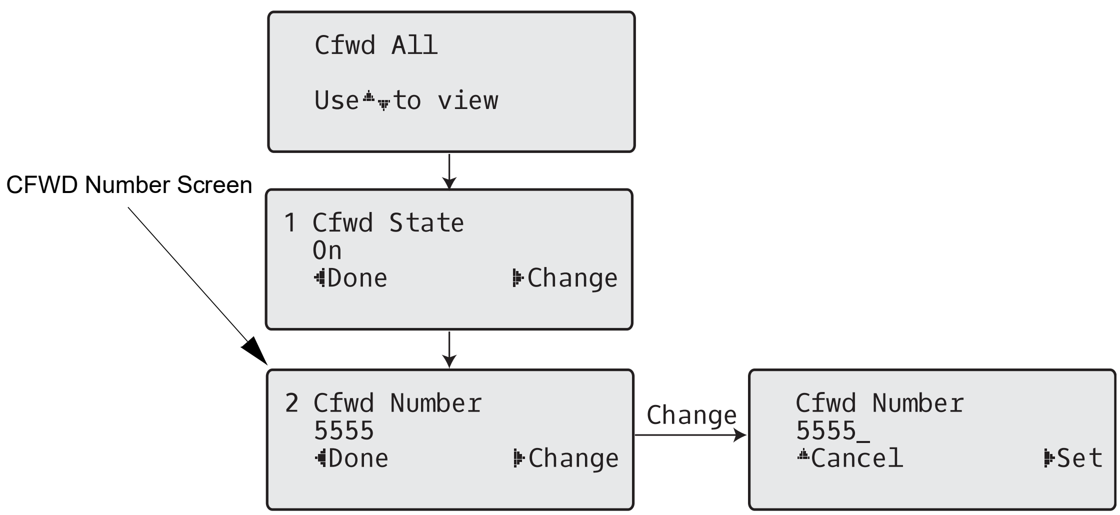
- All Off: Disables all CFWD states for the current account in focus

- All On: Enables all CFWD states for the current account in focus

4. Press the 4**Change** key for the mode you selected in step 2. Scroll to the CFWD State screen. This displays the current state of the mode you selected. In the following example, the CFWD All state is ON.

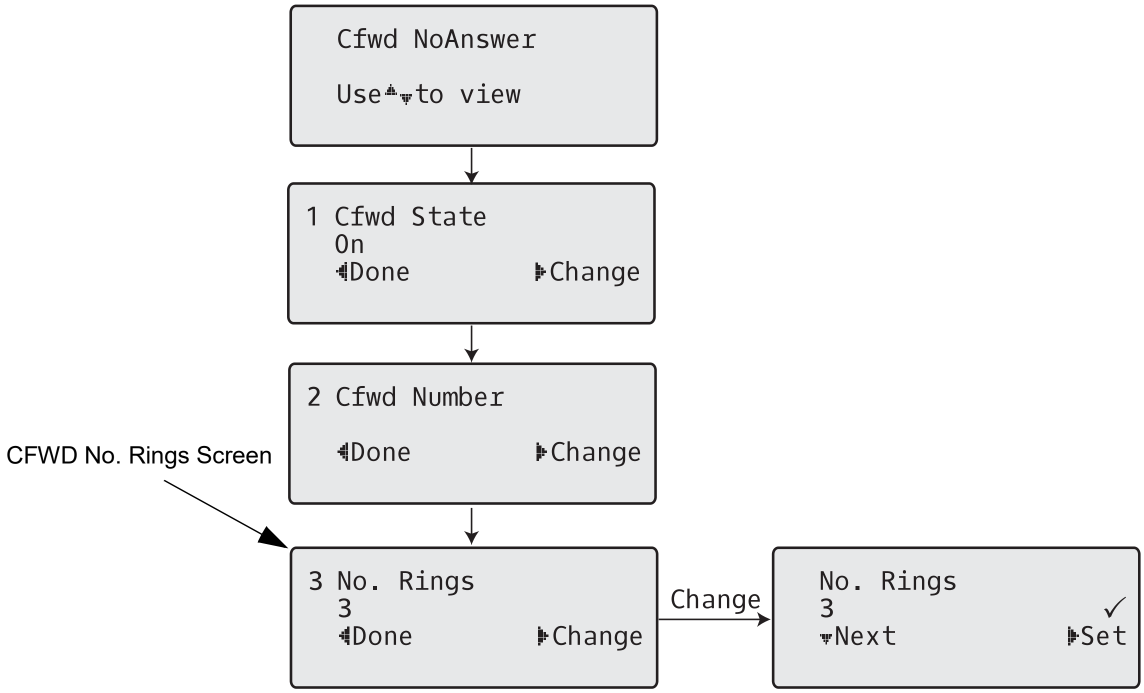


5. Press the 4**Change** key in the CFWD State screen. Press 2**Next** to toggle the state of the CFWD state ON or OFF. In the example in Step 4, you press 2**Next** to change the option to **Off**.
6. Press the 4**Set** key to save the change.
7. In the CFWD State screen, press the ▲ navigation key to scroll to the CFWD Number screen and press 4**Change**.



8. Enter a phone number to apply to the current state in focus. When the phone is in the state you specified, and a call comes into the phone, it forwards the call to the number you specify.
9. Press 4**Set** to save the change.

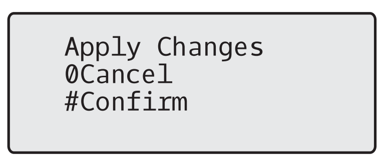
10. For the CFWD No Answer state, in the CFWD Number screen, press the navigation key to scroll to the CFWD No. Rings screen and press 4**Change**.



11. Press the key to select the number of rings to apply to the phone for call forwarding incoming calls. Valid values are 1 to 20. Default is 3.
When the phone receives an incoming call, and call forward is configured on the phone, the phone rings the number of times you specify in the No. Rings screen, and then forwards the call.

12. Press **Set** to save the change.

13. Press **Done** to save all your changes.
Each time you press **Done**, the following screen displays.



14. Press **# Confirm** to confirm the change(s) each time the Apply Changes screen displays. All changes are saved to the phone for all accounts.

CONFIGURING CALL FORWARD VIA THE IP PHONE UI

Once Call Forward is enabled on your phone, you can access the Call Forward menus by pressing a pre-configured **Call Forward** key, or by selecting *Options* > *Call Forward* from the IP phone UI.

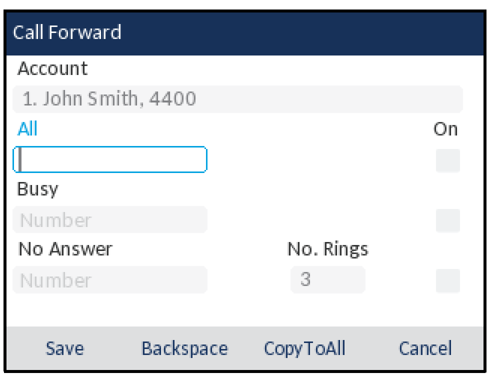
Note: If the BroadSoft BroadWorks Executive and Assistant Services feature is enabled and your phone is configured with the Assistant’s role, an additional Forward Filtering option may be available on the Call Forward menu. For information on the BroadWorks Executive and Assistant Services feature, refer to “BroadSoft BroadWorks Executive and Assistant Services” on page 6-94. For details on how to configure and utilize Forward Filtering, please refer to the respective phone model’s ***Mitel SIP Phone User Guide***.

CFWD in Account Mode (6867i/6869i/6920/6930)

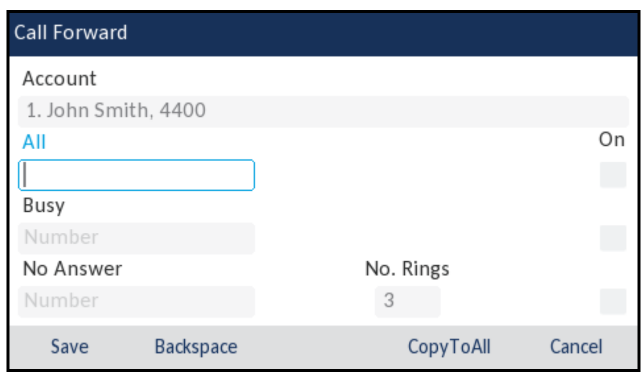
IP PHONE UI

1. From the Home screen press the ▶ navigation key to move to the **Line Selection** screen.
2. Highlight the desired account using the ▲ and ▼ navigation keys.
3. Press the 3 navigation key to go back to the **Home** screen
4. With the account in focus on **Home** screen, press the configured **Call Fwd** softkey or press ⚙, navigate to the **Call Forward** option and press the ✓ button or **Select** softkey. The Call Forward screen displays for the account you selected.

6867i CFWD Account Mode



6869i CFWD Account Mode



5. Enter forwarding numbers using the dialpad keys for any of the following states:
   - All: Forwards all incoming calls for the respective account to the specified number.
   - Busy: Forwards incoming calls to a specified number if DND has been enabled for that account OR if the account is currently engaged in another call.

- No Answer: Forwards incoming calls to a specified number if the call has not been answered for the specified number of rings.

Notes:

1. Pressing the navigation key moves the selection to the next field/checkbox.
2. If All and Busy and No Answer are all enabled (and/or if the account has DND enabled), the All settings take precedence over Busy and No Answer.
3. Pressing the **CopyToAll** key copies the call forward number of the Call Forward mode in focus to every Call Forward mode of that account. For example, if you have the cursor pointing at the All state and has a call forward phone number configured, pressing the **CopytoAll** key assigns the same phone number to the Busy and No Answer states as well.

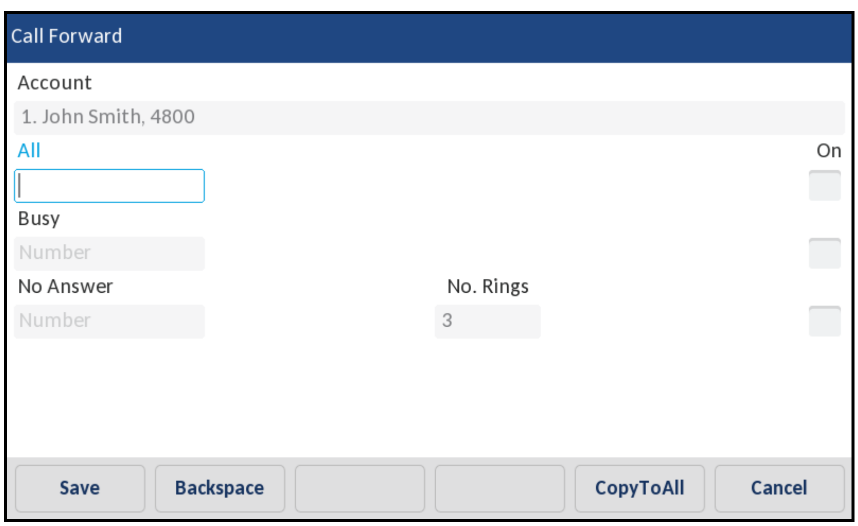
6. If configuring a forwarding number for the No Answer state, navigate to the **No. Rings** field and press the 3 or navigation keys to change the desired number of rings.
7. Using the navigation key, move to the **On** checkbox beside the respective Call Forward mode and press the button to enable the Call Forward mode.
8. Press the **Save** softkey to save your changes.

CFWD in Account Mode (6873i/6940/6970)

IP PHONE UI

1. From the Home screen swipe left to move to the **Line Selection** screen.
2. Choose the desired account.
3. Swipe right to go back to the **Home** screen
4. With the account in focus on **Home** screen, press the configured **Call Fwd** softkey or press and press the **Call Forward** icon.
   The Call Forward screen displays for the account you selected.

6873i CFWD Account Mode



5. Enter forwarding numbers using the dialpad keys for any of the following states:

- All: Forwards all incoming calls for the respective account to the specified number.
- Busy: Forwards incoming calls to a specified number if DND has been enabled for that account OR if the account is currently engaged in another call.
- No Answer: Forwards incoming calls to a specified number if the call has not been answered for the specified number of rings.

Notes:

1. If All and Busy and No Answer are all enabled (and/or if the account has DND enabled), the All settings take precedence over Busy and No Answer.
2. Pressing the **CopyToAll** key copies the call forward number of the Call Forward mode in focus to every Call Forward mode of that account. For example, if you have the cursor pointing at the All state and has a call forward phone number configured, pressing the **CopytoAll** key assigns the same phone number to the Busy and No Answer states as well.

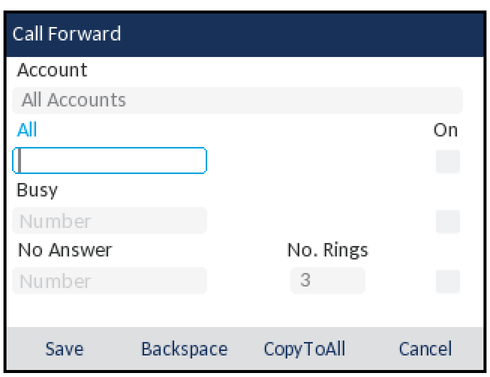
6. If configuring a forwarding number for the No Answer state, press the **No. Rings** field and press the left or right arrow keys to change the desired number of rings.
7. Press the checkbox beside the respective Call Forward mode to enable the Call Forward mode.
8. Press the **Save** softkey to save your changes.

CFWD in Phone Mode (6867i/6869i/6920/6930)

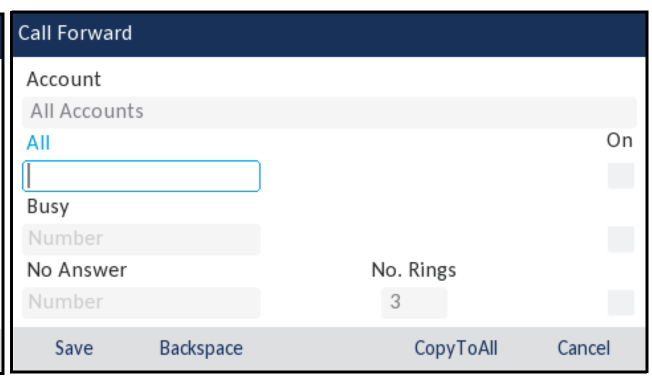
IP PHONE UI

1. Press the configured **Call Fwd** softkey or press , navigate to the **Call Forward** option and press the button or **Select** softkey.
The Call Forward screen displays and is applicable to all accounts configured on the phone.

6867i CFWD Phone Mode



6869i CFWD Phone Mode



2. Enter forwarding numbers using the dialpad keys for any of the following states:
   - All: Forwards all incoming calls for the respective account to the specified number.
   - Busy: Forwards incoming calls to a specified number if DND has been enabled for that account OR if the account is currently engaged in another call.

- No Answer: Forwards incoming calls to a specified number if the call has not been answered for the specified number of rings.

Notes:

1. Pressing the ▲ navigation key moves the selection to the next field/checkbox.
2. If All and Busy and No Answer are all enabled (and/or if the account has DND enabled), the All settings take precedence over Busy and No Answer.
3. Pressing the **CopyToAll** key copies the call forward number of the Call Forward mode in focus to every Call Forward mode of that account. For example, if you have the cursor pointing at the All state and has a call forward phone number configured, pressing the **CopytoAll** key assigns the same phone number to the Busy and No Answer states as well.

3. If configuring a forwarding number for the No Answer state, navigate to the **No. Rings** field and press the 3 or ▶ navigation keys to change the desired number of rings.
4. Using the ▲ navigation key, move to the **On** checkbox beside the respective Call Forward mode and press the button to enable the Call Forward mode.
5. Press the **Save** softkey to save your changes.

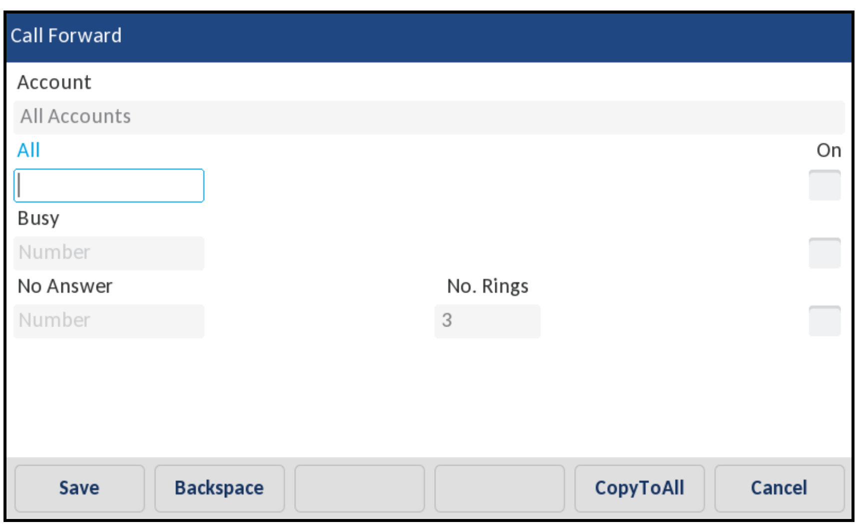
Note: In **Phone** mode, the configuration applies to all the accounts on the phone.

CFWD in Phone Mode (6873i/6940/6970)

IP PHONE UI

1. Press the configured **Call Fwd** softkey or press and press the **Call Forward** icon. The Call Forward screen displays and is applicable to all accounts configured on the phone.

6873i CFWD Phone Mode



2. Enter forwarding numbers using the dialpad keys for any of the following states:
   - All: Forwards all incoming calls for the respective account to the specified number.

- Busy: Forwards incoming calls to a specified number if DND has been enabled for that account OR if the account is currently engaged in another call.
- No Answer: Forwards incoming calls to a specified number if the call has not been answered for the specified number of rings.

Notes:

1. If All and Busy and No Answer are all enabled (and/or if the account has DND enabled), the All settings take precedence over Busy and No Answer.
2. Pressing the **CopyToAll** key copies the call forward number of the Call Forward mode in focus to every Call Forward mode of that account. For example, if you have the cursor pointing at the All state and has a call forward phone number configured, pressing the **CopytoAll** key assigns the same phone number to the Busy and No Answer states as well.

3. If configuring a forwarding number for the No Answer state, press the **No. Rings** field and press the left or right arrow keys to change the desired number of rings.
4. Press the checkbox beside the respective Call Forward mode to enable the Call Forward mode.
5. Press the **Save** softkey to save your changes.

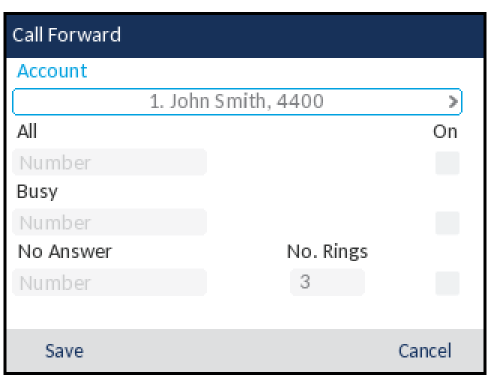
Note: In **Phone** mode, the configuration applies to all the accounts on the phone.

CFWD in Custom Mode (6867i/6869i/6920/6930)

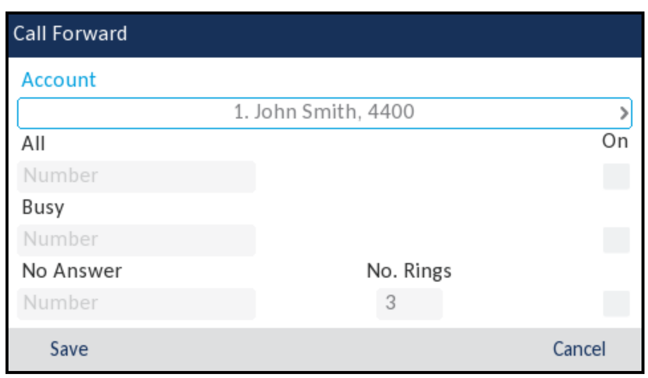
IP PHONE UI

1. Press the configured **Call Fwd** softkey or press , navigate to the **Call Forward** option and press the button or **Select** softkey.
   The Call Forward screen displays.

6867i CFWD Custom Mode



6869i CFWD Custom Mode



2. Press the 3 or navigation keys to change to the desired account.

Note: Select **All Accounts** if you want your changes to be made to all the accounts configured on the phone.

3. Enter forwarding numbers using the dialpad keys for any of the following states:

- All: Forwards all incoming calls for the respective account to the specified number.
- Busy: Forwards incoming calls to a specified number if DND has been enabled for that account OR if the account is currently engaged in another call.
- No Answer: Forwards incoming calls to a specified number if the call has not been answered for the specified number of rings.

Notes:

1. Pressing the ▲ navigation key moves the selection to the next field/checkbox.
2. If All and Busy and No Answer are all enabled (and/or if the account has DND enabled), the All settings take precedence over Busy and No Answer.
3. Pressing the **CopyToAll** key copies the call forward number of the Call Forward mode in focus to every Call Forward mode of that account. For example, if you have the cursor pointing at the All state and has a call forward phone number configured, pressing the **CopytoAll** key assigns the same phone number to the Busy and No Answer states as well.

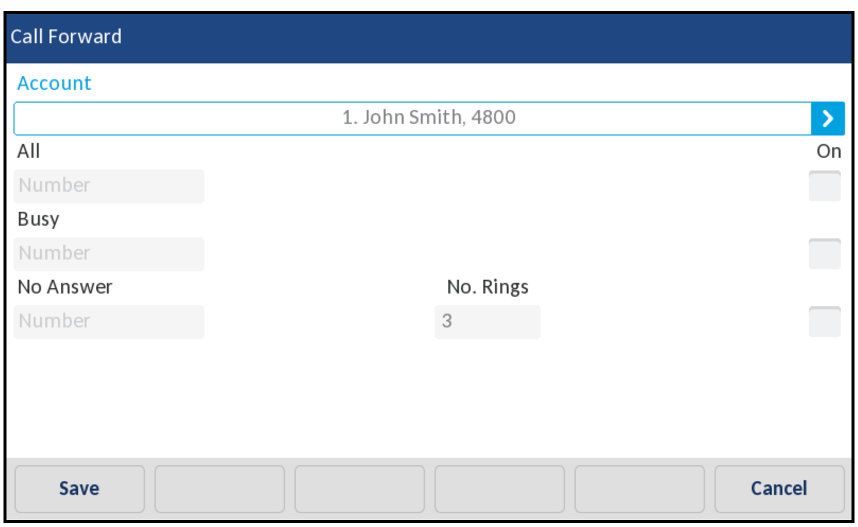
4. If configuring a forwarding number for the No Answer state, navigate to the **No. Rings** field and press the 3 or ▶ navigation keys to change the desired number of rings.
5. Using the ▲ navigation key, move to the **On** checkbox beside the respective Call Forward mode and press the button to enable the Call Forward mode.
6. Press the **Save** softkey to save your changes.

CFWD in Custom Mode (6873i/6940/6970)

IP PHONE UI

1. Press the configured **Call Fwd** softkey or press and press the **Call Forward** icon. The Call Forward screen displays.

6873i CFWD Custom Mode



2. Press the left or right arrow keys to change to the desired account.

Note: Select **All Accounts** if you want your changes to be made to all the accounts configured on the phone.

3. Enter forwarding numbers using the dialpad keys for any of the following states:
    - All: Forwards all incoming calls for the respective account to the specified number.
    - Busy: Forwards incoming calls to a specified number if DND has been enabled for that account OR if the account is currently engaged in another call.
    - No Answer: Forwards incoming calls to a specified number if the call has not been answered for the specified number of rings.

Notes:

1. If All and Busy and No Answer are all enabled (and/or if the account has DND enabled), the All settings take precedence over Busy and No Answer.
2. Pressing the **CopyToAll** key copies the call forward number of the Call Forward mode in focus to every Call Forward mode of that account. For example, if you have the cursor pointing at the All state and has a call forward phone number configured, pressing the **CopytoAll** key assigns the same phone number to the Busy and No Answer states as well.

4. If configuring a forwarding number for the No Answer state, press the **No. Rings** field and press the left or right arrow keys to change the desired number of rings.
5. Press the checkbox beside the respective Call Forward mode to enable the Call Forward mode.
6. Press the **Save** softkey to save your changes.

CALL DEFLECTION WITH NUMBER ENTRY

In Release 4.3.0 SP1, a new feature was implemented through which users can now deflect an incoming call to a number on a call-by-call basis without answering the call. Call deflection allows the users to manually determine a destination number during an incoming call (user has a choice to attend the call or deflect the call without answering).

The destination number can be entered using the dialpad keys or ’deflect a call quickly to a programmable key’ or ’softkey’ configured with Speeddial or BLF functionality. Applicable key types include:

- Speeddial
- Speeddial/Xfer
- Speeddial/Conf
- Speeddial/MWI
- BLF
- BLF/List

Notes:

1. Live dialpad is disabled when entering destination numbers using the call deflection feature.
2. When the "No Answer" Call Forward mode is configured and enabled on the phone, incoming calls are not forwarded to the defined "No Answer" number if the user is in the process of deflecting an incoming call.

   For example, during an incoming call, with the "No Answer" Call Forward mode configured to the forward incoming calls after five rings, if the user presses the Deflect softkey on their 6869i SIP phone (in the process of deflecting the call five ring elapse) the call is not forwarded. This is true even if the user decides not to deflect the call and cancels the deflection process after five rings. However, if the user cancels the deflection process before five rings, the call is forwarded per usual.
3. Users are able to transfer a call to Speeddial/Xfer and BLF /Xfer keys directly without answering an incoming call.
4. During an incoming when a call is deflected by pressing BLF/List or BLF key, it is treated same as a speeddial key disregarding other configuration options such as ‘directed call pickup', 'blf allow barg in', 'enhanced direct call pickup', 'blf key mode', and so on.
5. When the user wants to retain a behaviour defined by any of the above mentioned options after pressing the call deflect key, the call deflection can be cancelled by pressing the cancel key or by pressing the GoodBye key on the call deflect screen.

Users can enable or disable this feature using the "call deflect" parameter.

Enabling / Disabling Incoming Call Deflection with number entry Using Configuration Files.

Use the following parameter to enable or disable incoming call deflection with number entry on the 6873i/6940/6970 phone:

PARAMETER – *call deflect*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
DESCRIPTION	Enables or disables the ability to deflect a call to another number during a ringing state.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 - 1 0 (Disable) 1 (Enable)
EXAMPLE	call deflect: 1

Deflecting a Call

For the 6863i, 6865i, 6905, and 6910:

1. During an incoming call, press the key or programmable key configured with Transfer functionality.

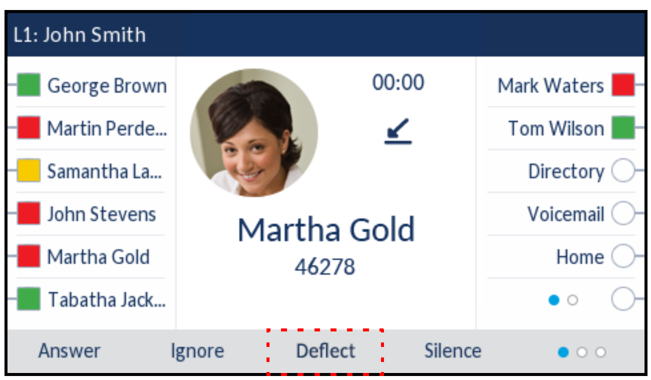
2. Using the dialpad keys, enter the destination number to which you wish to deflect the incoming call
   or
   Press a programmable key configured with Speeddial or BLF functionality.

3. If a destination number was entered manually, press the key, programmable key configured with Transfer functionality, or navigation key to deflect the call.

For the 6867i, 6869i, 6920, and 6930:

1. During an incoming call, press the **Deflect** softkey.

6869i Example

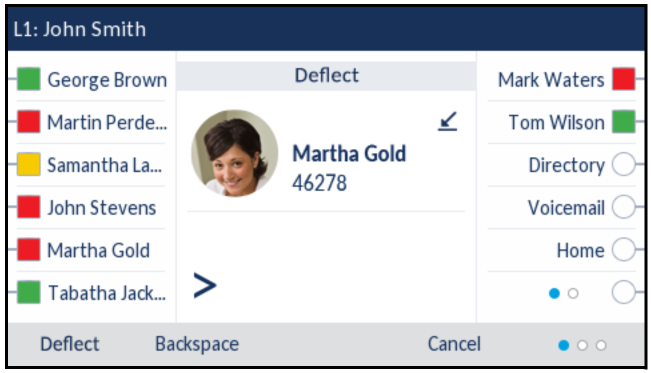


2. Using the dialpad keys, enter the destination number to which you wish to deflect the incoming call.

or

Press a softkey key configured with Speeddial or BLF functionality.

6869i Example

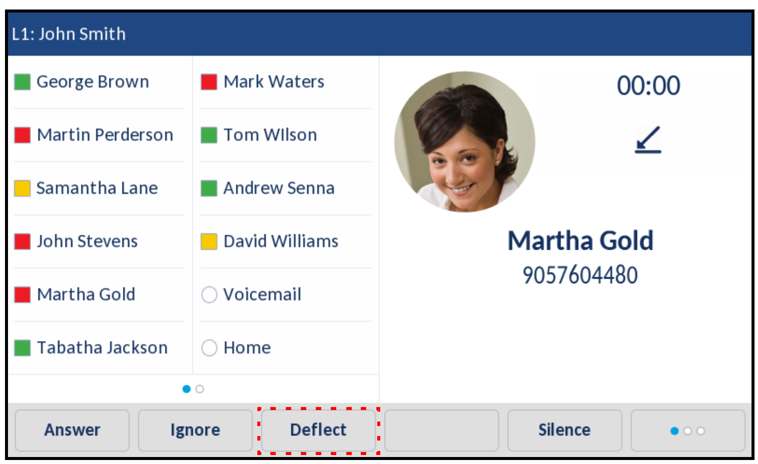


Note: Use the **Backspace** softkey to correct any errors and the **Cancel** softkey to cancel the call deflection process.

3. If a destination number was entered manually, press the **Deflect** softkey again to deflect the call.

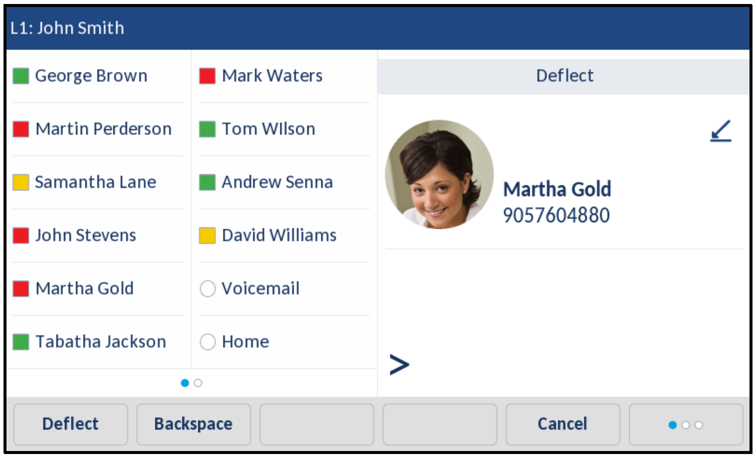
For the 6873i/6940/6970:

1. During an incoming call, tap the **Deflect** softkey.



2. Using the dialpad keys, enter the destination number to which you wish to deflect the incoming call

or
Tap a softkey key configured with Speeddial or BLF functionality.



Note: Use the **Backspace** softkey to correct any errors and the **Cancel** softkey to cancel the call deflection process.

If a destination number was entered manually, tap the **Deflect** softkey again to deflect the call.

SIP PHONE DIVERSION DISPLAY

When an outgoing call is being diverted to another destination (i.e. via call forward), the phone displays the Caller ID (phone number and/or caller name) of the new destination and the reason for the call diversion. Similarly, at the new destination, the Caller ID of the original call destination displays.

CALL DIVERSION EXAMPLE

1. Tim calls Mark at x400.
2. Mark's phone is busy.
3. Mark's phone diverts the incoming call to another destination (Roger @ x 464).
4. Tim's phone displays name and extension of where the call is being diverted to and reason for diverting the call.
5. Roger's phone accepts the call and displays the name and number of the incoming call (Tim) and the name (or number) of the original destination (Mark).

Note: If proxy servers exist in the network, it is possible that multiple diversions can take place on the phones. When multiple diversion headers are returned in a single 302 response back to the originating phone, the phone that originated the call (i.e.Tim's phone in the above example) displays the URI of the newest (first encountered) Diversion header, but displays the REASON of the oldest (last encountered) Diversion Header. The phone that receives the diverted call (i.e. Roger's phone in example above) displays the information of the oldest diverted call (last encountered).

You can enable or disable this feature on a global or per-line basis using the configuration files only.

CONFIGURING SIP DIVERSION DISPLAY ON THE PHONE

Use the following procedures to configure SIP diversion display on the IP phones.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “SIP Diversion Display” on page A-214.

LIMITATIONS

- The diversion header assumes that the ID of the 'diverted' caller is passed in a URI style manner.
- This feature relies on the server supporting and generating the Diversion header; the phone does not generate the header itself.
- Diversion header parameters such as counter, limit, privacy, screen, and extension are not recognized or supported by the phone. However, they are still passed along during the diversion process.

DISPLAY NAME CUSTOMIZATION

By default, if the IP phone receives an incoming call and the number of the incoming call matches an entry in directory, the IP phone will display the information stored in the directory instead of the display name of the INVITE. The “**directory lookup suppression pattern**” allows for the customization of the name displayed on the IP phone’s screen and suppression of the directory lookup.

This parameter is useful in such cases where a call manager will intentionally modify the display name according to a specific scenario. For example, if a Manager forwards an incoming call to an employee, the call manager may modify the display name to state “--> [Manager’s Name] Caller’s Name”. With the “**directory lookup suppression pattern**” parameter configured for “-->” pattern matching, the IP phone will bypass the directory lookup and the phone’s screen will display the call as intended by the call manager.

PATTERN RULES AND SYNTAX

The customized display name must start with the pattern. The patterns that can be configured include the following regular expressions:

- “-->x+”
- “==>x+”
- “@@@x+”
- “aaax+”

Additionally, the pattern syntax supports the regular expression | to specify multiple OR combined patterns (e.g. “-->x+|==>x+|aaax+”).

Notes:

1. Pattern matching is only applied for incoming calls and against the From header display name for incoming calls.
2. Pattern matching is applied to shared lines.
3. Pattern matching is not applied against the display name in the P-Asserted-Identity (PAI) header.

CONFIGURING THE DISPLAY NAME CUSTOMIZATION FEATURE

Use the following procedures to configure the display name customization feature.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Display Name Customization Settings” on page A-215.

DISPLAYING CALL DESTINATION FOR INCOMING CALLS

The IP Phones allow an Administrator to enable and disable the call destination name in the “TO” header of the INVITE message for incoming calls. When this feature is enabled, the call destination name displays on the LCD of the phone. This allows the user to easily determine the intended destination of an incoming call.

BEHAVIOR OF THE PHONE

When this feature is enabled, the phone behaves as follows:

IF	THEN
A value exists for the Display Name field in the “TO” header of the INVITE message for incoming calls...	the phone displays the call destination name.
Display Name field is empty...	the phone uses the name specified for the “Screen name 1” parameter.
“Screen name 1” parameter is empty...	the phone uses the name specified for the “Display Name” parameter.
“Display Name” parameter is empty...	the phone uses the name specified for the “SIP User Name” parameter.
“SIP User Name” parameter is empty...	the phone uses the name specified for the “Call Destination Number” parameter.

The call destination information displays on multiple screens that scroll every 3 seconds.

Note: When both call diversion and call destination are enabled, the formation displays to the phone's screens in the following order:

1. **Screen 1:** Caller info
2. **Screen 2**: Call destination
3. **Screen 3**: Call diversion

CONFIGURING THE DISPLAY OF CALL DESTINATION FOR INCOMING CALLS

Use the following procedures to configure the display of call destination for incoming calls on the IP Phones.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "Display of Call Destination for Incoming Calls" on page A-215.

LIMITATIONS

The following are limitations of this feature:

- Any call destination name exceeding the screen length is truncated by the phone.
- Page scrolling every 3 seconds is hard-coded and not configurable.

RECEIVED CALLERS LIST

The IP phones have a "Received Callers List" feature that store the name, phone number, and incremental calls, for each call received by the phone. You can enable and disable the Received Callers List feature using the configuration files. When disabled, the Received Callers List does not display on the IP phone UI and the Received Callers List key is ignored when pressed.

When enabled, you can view, scroll, and delete line items in the Received Callers List from the IP phone UI. You can also directly dial from a displayed line item in the Received Callers List. You can download the Received Callers List to your PC for viewing using the Mitel Web UI.

When you download the Received Callers List, the phone stores the *callerlist.csv* file to your computer in comma-separated value (CSV) format.

You can use any spreadsheet application to open the file for viewing. The file displays the phone number, name, and the line that the call came in on.

ENABLING/DISABLING MISSED/RECEIVED CALLERS LIST

You can enable and disable user access to the Missed/Received Callers List on the IP phones using the following parameter in the configuration files:

- callers list disabled

Valid values for this parameter are **0** (enabled) and **1** (disabled). If this parameter is set to **0**, the Missed/Received Callers List can be accessed by all users. If this parameter is set to **1**, the IP phone does not save any caller information to the Missed/Received Callers List. For any applicable phones, the "Callers List" option on the IP phone is removed from the Services menu, and the Callers List key is ignored if pressed by the user.

Use the following procedures to enable/disable the Missed/Received Callers List on the IP phones.

CONFIGURATION FILES

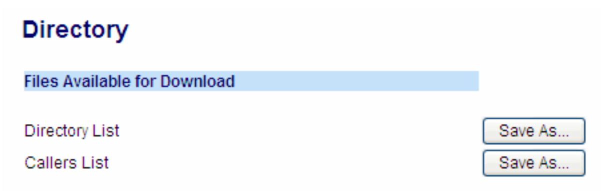
For specific parameters you can set in the configuration files for enabling/disabling the Missed/Received Callers List, see Appendix A, the section, "Missed/received Callers List Settings" on page A-179.

DOWNLOADING THE RECEIVED CALLERS LIST

Use the following procedure to download the Received Callers List using the Mitel Web UI.

MITEL WEB UI

1. Click on **Operation->Directory.**



2. In the Callers List field, click on **Save As**.
   A "*File Download*" message displays.
3. Click **Save**.
4. Enter the location on your computer where you want to download the Received Callers List and click **Save**.
   The *callerslist.csv* file downloads to your computer.
5. Use a spreadsheet application to open and view the Received Callers List.

CUSTOMIZABLE RECEIVED CALLERS LIST AND SERVICES KEYS

The IP phones may have a Received Callers List key and a Services key (as a hard key or softkey/programmable key) depending on your model phone. An Administrator can specify URI overrides for these keys using the following parameters in the configuration files:

- services script
- callers list script

Specifying URIs for these parameters cause the creation of an XML custom application instead of the standard function of the Received Callers List and Services keys.

An Administrator can configure these parameters using the configuration files only.

CREATING CUSTOMIZABLE RECEIVED CALLERS LIST AND SERVICES KEYS

Use the following procedure to create customized Received Callers List and Services keys on the IP Phone using the configuration files.

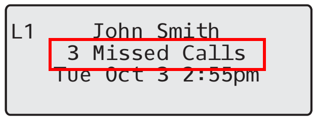
CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Customizable Received Callers List and Services Key" on page A-179.

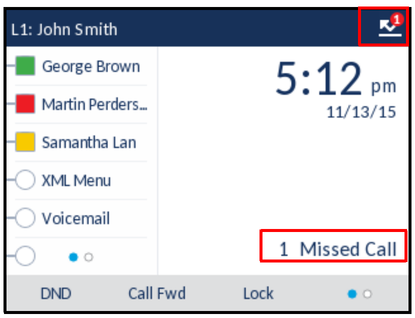
MISSED CALLS INDICATOR

The IP phone has a "missed calls" indicator that increments the number of missed calls to the phone.

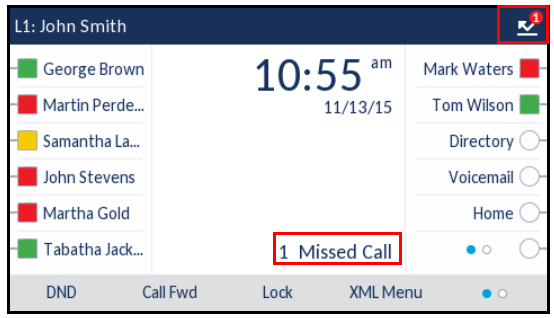
6863i/6865i/6905/6910 Missed Calls Indicator



6867i/6920 Missed Calls Indicator

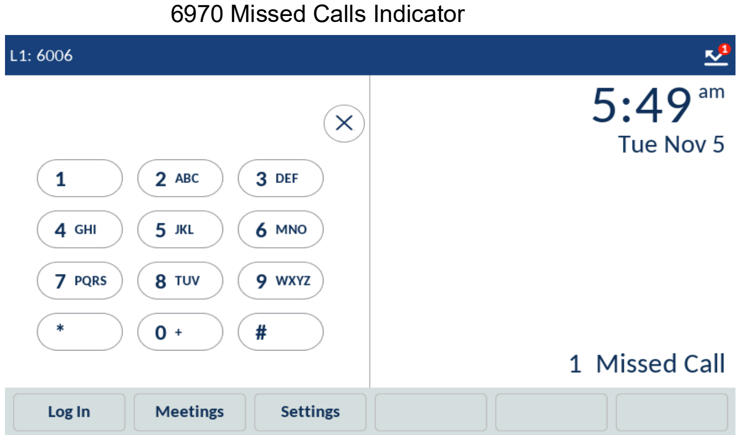


6869i/6930 Missed Calls Indicator



6873i/6940 Missed Calls Indicator

6970 Missed Calls Indicator



You can enable and disable the Missed Calls Indicator feature using the configuration files. When disabled, the Missed Calls Indicator does not increment as calls come into the IP phone.

When enabled, the number of calls that have not been answered increment on the phone's idle screen as "**<number> New Calls".** As the number of unanswered calls increment, the phone numbers associated with the calls are stored in the Missed Callers List. The user can access the Missed Callers List and clear the call from the list. Once the user accesses the Missed Callers List, the "<number> New Calls" on the idle screen is cleared.

ENABLING/DISABLING MISSED CALLS INDICATOR

You can enable (turn on) and disable (turn off) the Missed Calls Indicator on the IP phones using the following parameter in the configuration files:

- missed calls indicator disabled

Valid values for this parameter are **0** (enabled) and **1** (disabled). If this parameter is set to **0**, the indicator increments as unanswered calls come into the IP phone. If set to **1**, the indicator does not increment the unanswered calls.

Use the following procedures to enable/disable the Missed Calls Indicator on the IP phones.

CONFIGURATION FILES

For specific parameters you can set in the configuration files for enabling/disabling the Missed Calls Indicator, see Appendix A, the section, "Missed Calls Indicator Settings" on page A-185.

MISSED CALLS INDICATOR LINE APPLICABILITY

Administrators can also select the specific lines on the phone to which the missed calls indicator is applicable. This can be performed by defining the "**sip lineN missed calls enabled**" parameter in the configuration files ("0" for disabled, "1" for enabled) or through the Mitel Web UI.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Missed Calls Indicator Settings" on page A-185.

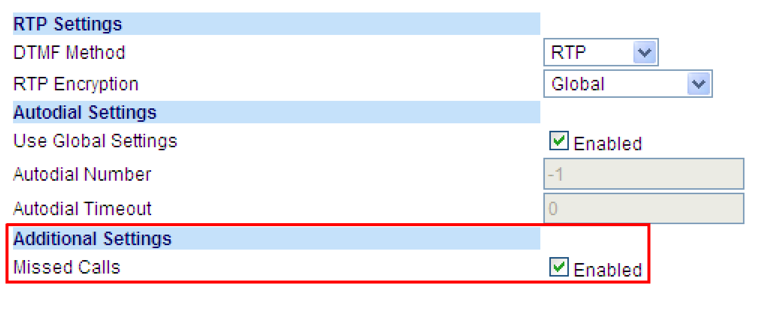
Configuring Missed Calls Indicator Applicability for Specific Lines Using the Mitel Web UI

Use the following procedure to configure missed calls indicator applicability for specific lines using the Web UI:

MITEL WEB UI

1. Click on **Advanced Settings > LineN** (where N = line number).

2. Under **Additional Settings**, for the **Missed Calls** option, enable by checking the checkbox or disable by unchecking the box (default is enabled).



3. Click **Save Settings**.

4. Repeat Steps 1 to 3 for any other lines you want to configure.

CALL HISTORY SOFTKEY SUPPORT

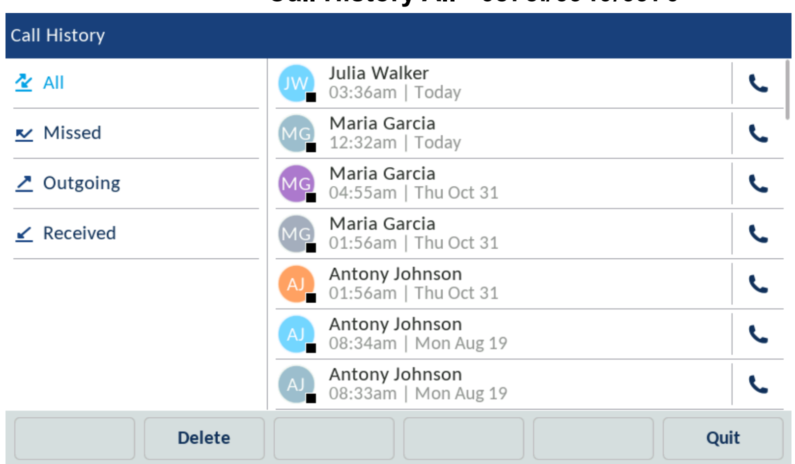
Note: This feature is applicable to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 SIP Phones.

A "Call History" softkey type is now available for the SIP phones. When pressed, the Call History softkey allows users the ability to directly access the list of all calls in the Call History.

Call History All - 6867i/6920

Call History All - 6869i/6930

Call History All - 6873i/6940/6970



Note: On 6873i, 6940 and 6970 IP Phone, from any of the folders of call history, you can directly make a call by tapping the Dial icon.

Users can configure a Call History key (on the top and bottom softkeys of the phone as well as expansion module softkeys) using the Mitel Web UI. Additionally, Administrators can configure a Call History key (on configurable hard keys and the top and bottom softkeys of the phone as well as expansion module softkeys) by defining a key as "callhistory" in the configuration files.

Refer to the following in Appendix A to configure a Call History key on the IP phone using the configuration files.

CONFIGURATION FILES

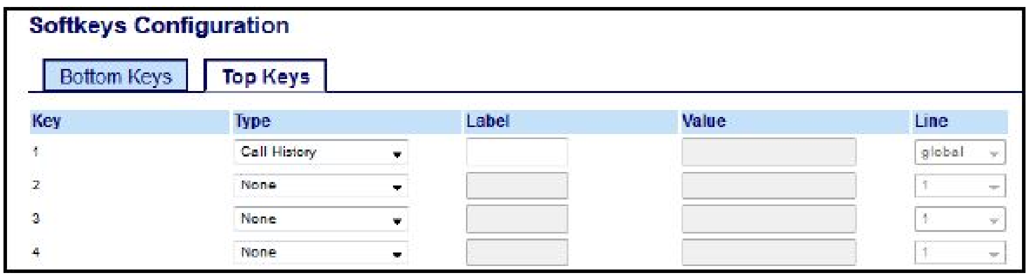
To set a Call History key using the configuration files, see Appendix A,"Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters" on page A-248.

CONFIGURING THE CALL HISTORY KEY USING THE MITEL WEB UI

Use the following procedure to configure a Call History key using the Mitel Web UI:

MITEL WEB UI

1. Click on **Operation > Softkeys and XML > Top Keys** (6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970)
   or
   Click on **Operation > Expansion Module <N>**. (M680i, M685i, and M695)



Top and Bottom Softkeys

2. Select a top or bottom softkey (6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970).
3. In the **Type** field, select **Call History**.
4. In the **Label** field, enter a label to display on the phone for the key (default is "Call History").
5. Click **Save Settings**.

Expansion Module Keys

6. Select from **Key 1** through **Key 16** (M680i) or **Key 84** (M685i and M695).
7. In the **Type** field, select **Call History**.
8. In the **Label** field, enter a label to display on the phone for the key (default is "Call History").
9. Click **Save Settings**.

HOLD SOFTKEY SUPPORT

Note: The Hold softkey is supported on the 6970 IP Phone only.

Users can configure a Hold softkey (on the top and bottom softkeys of the phone) using the Mitel Web UI. Additionally, Administrators can configure a Hold softkey (on the top and bottom softkeys of the phone) by defining a softkey as "hold" in the configuration files.

Refer to the following in Appendix A to configure a Hold softkey on the IP phone using the configuration files.

CONFIGURING THE HOLD SOFTKEY USING THE CONFIGURATION FILES

CONFIGURATION FILES

1. Open the configuration file for the conference phone.
2. Using the Softkey parameter in the configuration file, put in the data on the Hold softkey created. For example:

```
softkey5 type: hold
```

   Here you create bottom softkey No.5 of Hold type.

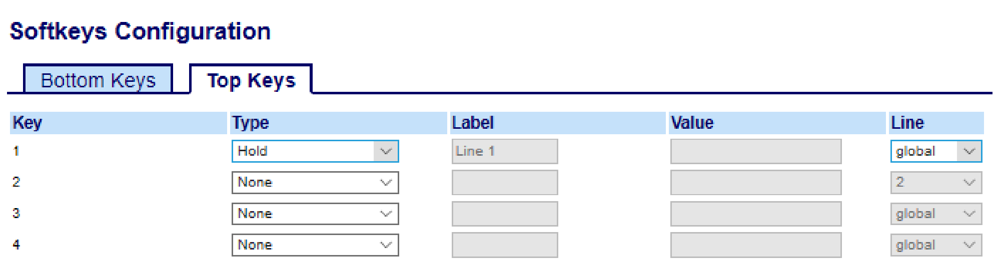
3. Save the changes in the file.
4. Download the configuration file into the phone for the change to become effective.

CONFIGURING THE HOLD SOFTKEY USING THE MITEL WEB UI

Use the following procedure to configure a Hold softkey using the Mitel Web UI:

MITEL WEB UI

1. Click on **Operation > Softkeys and XML**



2. Select a top or bottom softkey.
3. In the **Type** field, select **Hold**.
4. In the **Line** field, select the line for which you want to use the key functionality.

5. (For bottom keys only) In the **States** field, select the state(s) (idle, connected, incoming, outgoing, busy) for which you want to use on the key

6. Click **Save Settings**.

ENHANCED DIRECTORY LIST

Note: For more detailed information about user-related Directory functions, see your **Mitel <Model-Specific>** ***SIP Phone User Guide.***

The 6863i, 6865i, 6867i, 6869i, 6873i, 6905, 6910, 6920, 6930, 6940, and 6970 IP phones support enhanced Directory functionality allowing for interoperability with multiple directory sources (i.e. Local Directory, Corporate and Personal CSV directories, LDAP, Microsoft Exchange, Xsi Enterprise Directory, Xsi Personal Contacts, Xsi Enterprise Common Phone List, Xsi Group Directory, and Xsi Group Common Phone List,)

LOCAL DIRECTORY

The internal Local Directory contains the contacts that have been created or copied directly to the phone using the phone UI. If no external directory sources are available, pressing on the Directory key will open the Local Directory menu.

WARNING: WHEN UPGRADING A PHONE WITH A FIRMWARE VERSION PREVIOUS TO RELEASE 4.0.0 TO RELEASE 4.0.0 OR HIGHER, ALL LOCAL DIRECTORY ENTRIES WILL BE MIGRATED ACCORDINGLY. HOWEVER, IF DOWNGRADING BACK TO A FIRMWARE VERSION PREVIOUS TO RELEASE 4.0.0, ALL LOCAL DIRECTORY ENTRIES WILL BE LOST. IF YOU PLAN ON DOWNGRADING AT ANY TIME IN THE FUTURE AND WOULD LIKE TO RETAIN YOUR LOCAL DIRECTORY INFORMATION, IT IS RECOMMENDED TO SAVE YOUR LOCAL DIRECTORY ENTRIES BEFORE ANY UPGRADE OR DOWNGRADE BY USING THE PHONE'S WEB UI UNDER THE *OPERATION* > *DIRECTORY* MENU.

From the Local Directory menu, you can search for a contact, place a call to the selected contact, add new contacts to the Local Directory, delete all contacts, delete individual contacts, or edit existing contacts. Users can also view contact details (e.g. title, company name, numbers, work and home addresses, e-mail addresses, etc...).

Notes:

1. No configuration is required for the Local Directory.
2. Up to 1000 Directory contacts can be stored locally on the phone.

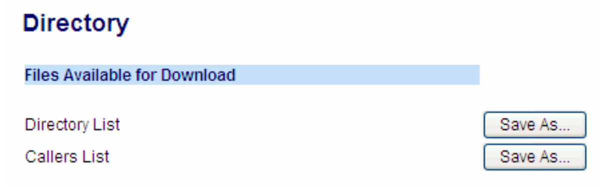
Downloading the Local Directory List Using the Mitel Web UI

You can use the Mitel Web UI to download the Local Directory List from the IP phone to the configuration server.

Use the following procedure to configure the download.

MITEL WEB UI

1. Click on **Operation->Directory.**



2. In the Directory List field, click on **Save As**.
   A "File Download" message displays.
3. Click **Save**.
4. Enter the location on your computer where you want to download the Directory List and click **Save**.
   The *directorylist.csv* file downloads to your computer.
5. Use a spreadsheet application to open and view the Directory List.

CSV-BASED DIRECTORIES

Two Comma-Separated-Value (CSV)-based directory files can be created and utilized on the phone as per previous releases but the number of fields the phone can parse has been greatly expanded. The phone can now handle CSV files with the following field values in the following order separated by commas:

- First Name (mandatory)
- Last Name
- Company
- Job Title
- Work Address Street
- Work Address City
- Work Address State/Province
- Work Address Zip/Postal Code
- Work Address Country
- Home Address Street
- Home Address City
- Home Address State/Province
- Home Address Zip/Postal Code
- Home Address Country
- Email1

- Email2
- Email3
- Number of Total Phone Numbers
- Phone Number 1 Type (mandatory)
- Phone Number 1 Line #
- Phone Number 1
- Phone Number 2 Type
- Phone Number 2 Line #
- Phone Number 2

Note: Phone Number N Type is defined as an integer as per the following list:

- 1 (Work1)
- 2 (Work2)
- 3 (Cell)
- 4 (Home1)
- 5 (Home2)
- 6 (Fax)
- 7 (Other)

The following example details a typical entry in the CSV directory file:

```
John,Smith,Acme Ltd.,Director of Marketing,123 Acme Rd.,Toronto,
Ontario,L4K 4N9,Canada,,,,,,jsmith@acme.com,,,2,1,1,9054804321,
3,1,9054801234
```

Administrators can fully configure CSV directories by defining the following parameters in the configuration files:

PARAMETER	DESCRIPTION
directory 1	The name/location of the first CSV-based directory list file that you can download from the configuration server.
directory 2	The name/location of the second CSV-based directory list file that you can download from the configuration server.
directory 1 name	Specifies the folder name of the directory defined in the “directory 1” parameter. Can also be configured through the Phone UI, see Enabling/Disabling Directories and Renaming Labels Using the Phone UI on page 5-307 for details.
directory 2 name	Specifies the folder name of the directory defined in the “directory 2” parameter. Can also be configured through the Phone UI, see Enabling/Disabling Directories and Renaming Labels Using the Phone UI on page 5-307 for details.
directory 1 enabled	Specifies whether or not the directory defined in the “directory 1” parameter should be enabled to be accessed on the phone. Can also be configured through the Phone UI, see Enabling/Disabling Directories and Renaming Labels Using the Phone UI on page 5-307 for details.

PARAMETER	DESCRIPTION
directory 2 enabled	Specifies whether or not the directory defined in the “directory 2” parameter should be enabled to be accessed on the phone. Can also be configured through the Phone UI, see Enabling/Disabling Directories and Renaming Labels Using the Phone UI on page 5-307 for details.

Note: CSV-based directories, directory 1 and directory 2 can now support 2000 contacts in each directory.

Configuring Interoperability with CSV-Based Directories Using the Configuration Files

Use the following procedures to configure interoperability with CSV-based directories.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “CSV Directory Settings” on page A-148.

MICROSOFT EXCHANGE CONTACTS

The 6800 and 6900 Series IP phones allow interoperability with Microsoft Exchange contacts (Exchange 2007 SP1 or greater interface supported [through the Exchange Web Server API]). Contact information is mapped seamlessly into the phone’s Directory menu whereby users can search for contacts, dial out to contacts, copy contacts to the Local Directory, or simply view the contact’s details (e.g. title, company name, numbers, work and home addresses, e-mail addresses, etc...).

Note: Microsoft Exchange contacts work only with on-premise exchange server.

Administrators can fully configure a Microsoft Exchange Directory by defining the following parameters in the configuration files:

PARAMETER	DESCRIPTION
exchange server	Specifies the user’s Microsoft Exchange server IP address or Fully Qualified Domain Name (FQDN).
exchange use ssl	Specifies whether SSL (Secure Sockets Layer) should be enabled or disabled.
exchange path	Configures a custom Exchange Web Services (EWS) path on the Exchange server hosting the EWS managed API. By default the path is "ews/exchange.asmx" on a typical Microsoft Exchange installation.
exchange user name	Specifies the user’s Microsoft Exchange user name. Can also be configured through the Phone UI, see Entering Usernames/Passwords and Connection Testing on page 5-308 for details.

PARAMETER	DESCRIPTION
exchange contacts enabled	Specifies whether or not the Microsoft Exchange directory should be enabled to be accessed on the phone. Can also be configured through the Phone UI, see Enabling/Disabling Directories and Renaming Labels Using the Phone UI on page 5-307 for details.
exchange contacts name	Specifies the folder name of the Microsoft Exchange directory when enabled. Can also be configured through the Phone UI, see Enabling/Disabling Directories and Renaming Labels Using the Phone UI on page 5-307 for details.
exchange contacts resync time	Sets the time of day in a 24-hour period for the IP phone to update the Microsoft Exchange directory.
exchange contacts resync days	Specifies the amount of days that the phone waits between Microsoft Exchange directory resync operations.
exchange contacts resync max delay	Specifies the maximum time, in minutes, the phone waits past the scheduled time before starting a Microsoft Exchange directory checksync.

Configuring Interoperability with a Microsoft Exchange Directory Using the Configuration Files

Use the following procedures to configure interoperability with a Microsoft Exchange Directory.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Exchange Directory Settings" on page A-151.

BROADSOFT XSI DIRECTORIES

The 6800 Series IP phones also support interoperability with BroadSoft Xsi directories such as Enterprise Directory, Personal Contacts, Enterprise Common Phone List, Group Directory, and Group Common Phone List. When configured, the IP phones will retrieve the respective BroadSoft Xsi directory and add folders to the Directory menu where they can be accessed by users.

Administrators can fully configure the Xsi directories by defining the following parameters in the configuration files:

PARAMETER	DESCRIPTION
xsi ip	Specifies the Xsi Enterprise Directory credentials (if applicable) and IP address or Fully Qualified Domain Name (FQDN) of the Xsi server in the following syntax: server or username:password@server **Note:** Xsi credentials defined through the "**xsi ip**" parameter are only applicable to the Xsi Enterprise Directory feature and not applicable to user-related Xsi features (such as Speed Dial 8, Basic Call Log, Hide Number, Remote Office, Simultaneous Ring Personal, Call Center, and BroadSoft Anywhere) and other Xsi directories. Credentials for the user-related Xsi features require encryption and therefore must be entered through the phone's Options List > Credentials menu.
xsi protocol	Specifies the protocol (either HTTP or HTTPs) used for communicating with the Xsi server.
xsi port	Specifies the port used for communicating with the Xsi server.
xsi user name	Specifies the user name used for authentication of the Xsi account when not using SIP authentication (see BroadSoft BroadWorks Xsi SIP Authentication on page 6-61 for information on XSI SIP authentication). Can also be configured through the Phone UI, see Entering Usernames/Passwords and Connection Testing on page 5-308 for details.
xsi personal contacts enabled	Specifies whether or not the BroadSoft Xsi Personal Contacts directory should be enabled to be accessed on the phone. Can also be configured through the Phone UI, see Enabling/Disabling Directories and Renaming Labels Using the Phone UI on page 5-307 for details.
xsi enterprise directory enabled	Specifies whether or not the BroadSoft Xsi Enterprise Directory should be enabled to be accessed on the phone. Can also be configured through the Phone UI, see Enabling/Disabling Directories and Renaming Labels Using the Phone UI on page 5-307 for details.
xsi enterprise common directory enabled	Specifies whether or not the BroadSoft Xsi Enterprise Common Directory should be enabled to be accessed on the phone. Can also be configured through the Phone UI, see Enabling/Disabling Directories and Renaming Labels Using the Phone UI on page 5-307 for details.
xsi group directory enabled	Specifies whether or not the BroadSoft Xsi Group Directory should be enabled to be accessed on the phone. Can also be configured through the Phone UI, see Enabling/Disabling Directories and Renaming Labels Using the Phone UI on page 5-307 for details.

PARAMETER	DESCRIPTION
xsi group common directory enabled	Specifies whether or not the BroadSoft Xsi Group Common Directory should be enabled to be accessed on the phone. Can also be configured through the Phone UI, see Enabling/Disabling Directories and Renaming Labels Using the Phone UI on page 5-307 for details.
xsi personal contacts name	Specifies the folder name of the BroadSoft Xsi Personal Contacts when enabled. Can also be configured through the Phone UI, see Enabling/Disabling Directories and Renaming Labels Using the Phone UI on page 5-307 for details.
xsi enterprise directory name	Specifies the folder name of the BroadSoft Xsi Enterprise Directory when enabled. Can also be configured through the Phone UI, see Enabling/Disabling Directories and Renaming Labels Using the Phone UI on page 5-307 for details.
xsi enterprise common directory name	Specifies the folder name of the BroadSoft Xsi Enterprise Common Directory when enabled. Can also be configured through the Phone UI, see Enabling/Disabling Directories and Renaming Labels Using the Phone UI on page 5-307 for details.
xsi group directory name	Specifies the folder name of the BroadSoft Xsi Group Directory when enabled. Can also be configured through the Phone UI, see Enabling/Disabling Directories and Renaming Labels Using the Phone UI on page 5-307 for details.
xsi group common directory name	Specifies the folder name of the BroadSoft Xsi Group Common Directory when enabled. Can also be configured through the Phone UI, see Enabling/Disabling Directories and Renaming Labels Using the Phone UI on page 5-307 for details.
xsi resync time	Sets the time of day in a 24-hour period for the IP phone to update the BroadSoft Xsi directories.
xsi resync days	Specifies the amount of days that the phone waits between BroadSoft Xsi directory resync operations.
xsi resync max delay	Specifies the maximum time, in minutes, the phone waits past the scheduled time before starting a BroadSoft Xsi directory checksync.

Configuring Interoperability with BroadSoft Xsi Directories

Use the following parameters to configure interoperability with BroadSoft Xsi directories.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "BroadSoft Xsi Directory Settings" on page A-155.

LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)

The 6800/6900 Series IP phones are able to use a Lightweight Directory Access Protocol (LDAP) server for reading directories over an IP network. When configured, users are able to search for contacts, dial out to contacts, copy contacts to the Local Directory, or simply view the contact's details (e.g. title, company name, numbers, work and home addresses, e-mail addresses, etc...).

Administrators can fully configure an LDAP Directory by defining the following parameters in configuration files.

Notes:

1. For compatibility purposes your LDAP database must be configured with a matching rule to ignore case (i.e. queries should be case-insensitive). Refer to RFC2252 for information on the LDAP attribute type EQUALITY and other settings related to matching rules.
2. Only the basic LDAP parameters are required to be configured for LDAP functionality.
3. Advanced LDAP parameters are optional and are not required for LDAP functionality. These advanced parameters can be used for advanced customization of the LDAP directory.

Basic LDAP Parameters

PARAMETER	DESCRIPTION
ldap server	Specifies the LDAP server hostname or IP address.
ldap user name	Specifies the user's LDAP user name. Can also be configured through the Phone UI, see Entering Usernames/Passwords and Connection Testing on page 5-308 for details.
ldap base dn	Specifies the LDAP server base DN. It is the description of the top level of the directory tree. Usually if a company domain is "company.com", the base DN (distinguished name) must be entered under the form "dc=company, dc=com".
ldap enabled	Specifies whether or not the LDAP Directory should be enabled to be accessed on the phone. Can also be configured through the Phone UI, see Enabling/Disabling Directories and Renaming Labels Using the Phone UI on page 5-307 for details.
ldap name	Specifies the folder name of the LDAP Directory when enabled. Can also be configured through the Phone UI, see Enabling/Disabling Directories and Renaming Labels Using the Phone UI on page 5-307 for details.
ldap resync time	Sets the time of day in a 24-hour period for the IP phone to update the LDAP directory.
ldap resync days	Specifies the amount of days that the phone waits between LDAP directory resync operations.
ldap resync max delay	Specifies the maximum time, in minutes, the phone waits past the scheduled time before starting an LDAP directory checksync.

Advanced LDAP Parameters

PARAMETER	DESCRIPTION
ldap cn attribute	Used when both the first and last name of a record are empty.
ldap dn attribute	Used to perform the search request for the detailed view of an LDAP contact.
ldap search filter	Used to set search filters. This parameter format must follow RFC 4515, for example (sn=%). This parameter must include a '%' character at the place where it will be replaced by a*, b*, etc...
ldap search scope	Used to set the search scope. A "base" search is performed only on the baseDN, a "onelevel" search is performed on the baseDN and the first sublevel, and a "subtree" search is performed on the whole tree under the base DN.
ldap search timeout	Used to set the request timeout for LDAP requests.
ldap network timeout	Used to set the network timeout for LDAP requests.
ldap use ISO-8859-1 encoding	Specifies whether or not the LDAP directory the phone is configured to use ISO-8859-1 or UTF-8 encoding. If the LDAP directory utilizes ISO-8859-1 encoding and the parameter is set to “1”, the phone will transcode any characters using diacritical marks from the ISO-8859-1 character set to the equivalent UTF-8 characters, correcting any character encoding issues.
ldap first name attribute list	Specifies the LDAP first name (e.g. John) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap last name attribute list	Specifies the LDAP last name (e.g. Doe) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap company attribute list	Specifies the LDAP company name (e.g. Mitel) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap job title attribute list	Specifies the LDAP job title (e.g. Vice President) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap business street attribute list	Specifies the LDAP business street (e.g. Snow Blvd.) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap business city attribute list	Specifies the LDAP business city (e.g. Concord) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap business state attribute list	Specifies the LDAP business state (e.g. Ontario) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap business postal code attribute list	Specifies the LDAP business postal code (e.g. L4K 4N9) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap business country attribute list	Specifies the LDAP business country (e.g. Canada) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.

PARAMETER	DESCRIPTION
ldap home street attribute list	Specifies the LDAP home street (e.g. Internet Blvd.) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap home city attribute list	Specifies the LDAP home city (e.g. Frisco) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap home state attribute list	Specifies the LDAP home state (e.g. Texas) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap home postal code attribute list	Specifies the LDAP home postal code (e.g. 75034) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap home country attribute list	Specifies the LDAP home country (e.g. U.S.A) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap business phone 1 attribute list	Specifies the LDAP business phone 1 (e.g. 1-905-760-4200) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap business phone 2 attribute list	Specifies the LDAP business phone 2 (e.g. 1-905-760-4201) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap home phone 1 attribute list	Specifies the LDAP home phone 1 (e.g. 1-416-468-3266) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap home phone 2 attribute list	Specifies the LDAP home phone 2 (e.g. 1-416-468-3267) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap mobile phone attribute list	Specifies the LDAP mobile phone (e.g. 1-416-468-3268) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap other phone attribute list	Specifies the LDAP other phone (e.g. 1-416-468-3269) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap business fax attribute list	Specifies the LDAP business fax (e.g. 1-905-760-4233) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap email 1 attribute list	Specifies the LDAP email 1 (e.g. john.doe@mitel.com) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap email 2 attribute list	Specifies the LDAP email 2(e.g. john.d@mitel.com) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap email 3 attribute list	Specifies the LDAP email 3 (e.g. j.doe@mitel.com) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.

When a 6800/6900 Series SIP phone detects it is connected to an Active Directory service of Exchange server through the LDAP interface, the following field mapping, scope, and search filters are used to perform the requests:

Field Mapping

- ldap cn attribute: cn
- ldap dn attribute: distinguishedName
- ldap first name attribute list: givenName
- ldap last name attribute list: sn
- ldap company attribute list: company
- ldap job title attribute list: title
- ldap business street attribute list attribute list: streetAddress
- ldap business city attribute list: l
- ldap business street attribute list: st
- ldap business postal code attribute list: postalCode
- ldap business country attribute list: co
- dap business phone 1 attribute list: telephoneNumber
- ldap business phone 2 attribute list: otherTelephone
- ldap home phone 1 attribute list: homePhone
- ldap home phone 2 attribute list: otherHomePhone
- ldap mobile phone attribute list: mobile
- ldap other phone attribute list: ipPhone
- ldap business fax attribute list: facsimileTelephoneNumbe
- ldap email 1 attribute list: mail
- ldap email 2 attribute list: otherMailBox

Scope

ldap search scope: subtree

Search filter

ldap search filter:
(&(objectCategory=Person)(objectClass=User)(!(msExchHideFromAddressLists=TRUE))(!(userAccountControl:1.2.840.113556.1.4.803:=2))(displayname=%)(|(telephonenumber=*)(mobile=*) (homephone=*)))

Configuring Interoperability with an LDAP Directory

Use the following parameters to configure interoperability with an LDAP Directory

CONFIGURATION FILES

For specific parameters that you can set in the configuration files, see Appendix A, "Basic LDAP Settings" on page A-161 and "Advanced LDAP Settings" on page A-167.

SECURE LDAP CONFIGURATION

Users can now enable a secure LDAP connection to connect to the Active Directory.

The following three approaches can be used to encrypt a non-secure LDAP connection.

- LDAPS over port 636
- LDAP with STARTTLS (port 389)
- LDAP mTLS

LDAP with STARTTLS is activated only if "ldap starttls" parameter is set to 1 in the configuration file.

LDAPS over port 636 is used only if *ldaps://server_address* is configured in the configuration parameter "ldap server".

The following LDAP/LDAPS configurations are supported:

```
ldap server:
CN=admin01,OU=toronto,DC=mitel,DC=com:1234@ldap_server_ip:389
```

```
ldap server:
CN=admin01,OU=toronto,DC=mitel,DC=com:1234@ldap://ldap_server_ip:389
```

```
ldap server:
CN=admin01,OU=toronto,DC=mitel,DC=com:1234@ldaps://ldaps_server_host
name:636
```

To connect to an LDAPS server, a CA certificate is required on the phone. By default, the certificate trust store "*/nvdata/certificates/rootCerts.pem*" is used. Alternative certificates can be downloaded from the configuration server and used if the "ldaps trusted certificates" parameter is configured. The file path of certificates on the configuration server is used as the value for the "ldaps trusted certificates" parameter. For example, *ldaps trusted certificates: cacert.pem*.

By default, a Fully Qualified Domain Name (FQDN) of the LDAPS server is required in the "ldap server" parameter if *ldaps://* is configured as following:

For LDAPS over port 636,

```
ldap server:
CN=admin01,OU=toronto,DC=mitel,DC=com:1234@ldaps://abc.mitel.com:636
```

For LDAP with STARTTLS,

```
ldap server:
CN=admin01,OU=toronto,DC=mitel,DC=com:1234@abc.mitel.com:389
```

Alternatively, an IP address can be used if a certificate with IP address configured in the Subject Alternative Name (SAN) field is used on the LDAPS server.

LDAP mTLS

Provides access to the LDAP server via mTLS (mutual Transport Layer Security). The LDAP server must support Mitel Root Certificate as the phone provides the MAC based device certificates when asked to send Client Certificate.

For specific parameters that you can set in the configuration files, see Appendix A, "Basic LDAP Settings" on page A-161.

ASYNCHRONOUS LDAP DIRECTORY LOOKUP MODE SUPPORT

In previous releases LDAP directories would be downloaded in full, cached in the directory database and updated daily. From Release 5.1.0 Asynchronous LDAP Directory Lookup Mode is supported for the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 SIP IP phones in which the LDAP directory is no longer cached but available through an LDAP lookup sub-application.

Note: The Mitel 6865i SIP IP phone model does not support Asynchronous LDAP directory lookup mode.

The new LDAP directory is accessible through the main Directory application. Users can now perform lookups via the LDAP server directly and access very large LDAP servers without overloading the SIP phones.

The existing LDAP parameters are shared in both cached and lookup modes. Two new configuration parameters have been added to supplement the lookup mode:

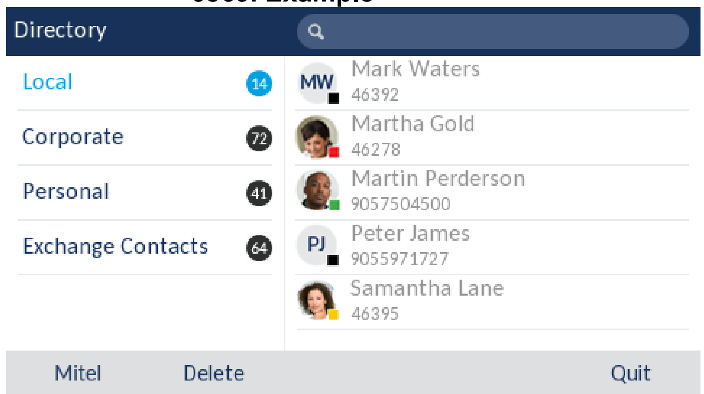
- **ldap downloaded**: Enables or disables the LDAP mode between cached and lookup. When defined as "0", LDAP directories are not cached on the phone (i.e. LDAP directories are available using the lookup method). When defined as "1" (default), LDAP directories are cached on the phone.
- **ldap lookup filter**: Represents the custom LDAP query sent for an LDAP lookup. Example: "ldap lookup filter: (|(givenName=%)(sn=%))". This parameter allows the query to be aligned to the LDAP server data scheme.

Note: This parameter is ignored if the LDAP server is an Exchange Server.

Example: If an LDAP directory is configured with an LDAP name of "Mitel" and the "ldap downloaded" parameter is defined as "0" in the configuration files, users can perform a lookup on the LDAP directory by accessing the Directory and then pressing or tapping the Mitel softkey.

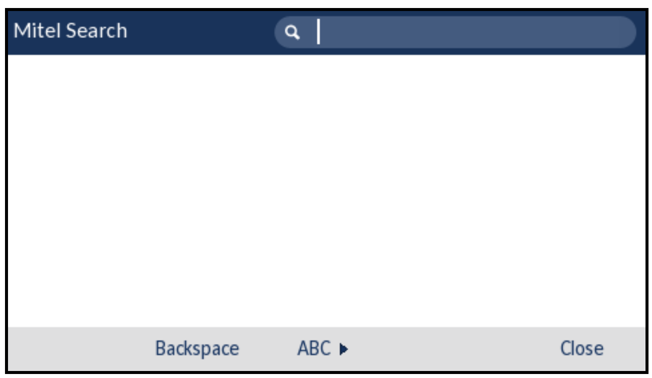
Users can then select a contact, dial, view the contact's Details page or copy to the Local Directory using the same methods as the cached LDAP directory.

6869i Example



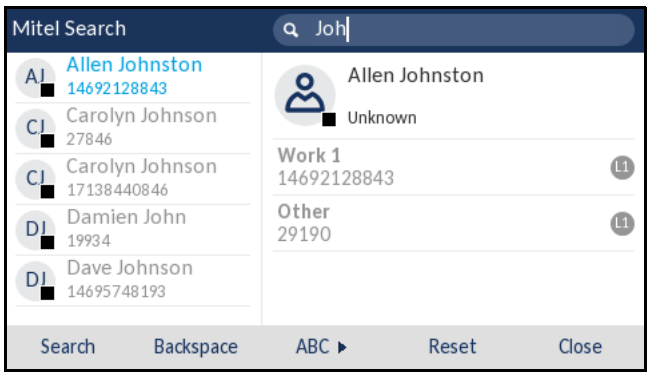
A sub-application for the LDAP directory is displayed whereby users can perform a lookup through the LDAP server.

6869i Example



Users must enter at least three characters in the search bar and then press or tap the **Search** softkey.

6869i Example



Users can then select a contact and dial, view the contact's Details page, or copy to the Local Directory using the same methods as the cached LDAP directory.

Limitations

There are two limitations when using the LDAP lookup mode:

- LDAP records are not used for caller ID lookups.
- Searches in the LDAP lookup mode are based on exact matches. Therefore, when searching for names with diacritical characters, the diacritical characters must be entered or the result will not be displayed. For example, a search for Stéphane using "Ste" will not result in a match; the search must be entered as "Sté". In cached mode, a search for "Ste" will still result in a match with "Stéphane".

Configuring Asynchronous LDAP Lookup Mode Using the Configuration Files

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, section "Asynchronous LDAP Directory Lookup Mode Support" on page A-175.

GENERAL DIRECTORY OPTIONS

Enabling/Disabling the Directory

You can enable and disable user access to the Directory List on the IP phones by defining "**directory disabled**" parameter in the configuration files. Valid values for this parameter are **0** (enabled) and **1** (disabled). If this parameter is set to **0**, the Directory List can be accessed by all users. If this parameter is set to **1**, the Directory List does not display on the IP phone and the Directory key is disabled.

Enabling/Disabling the Directory Using the Configuration Files

Use the following procedures to enable/disable the Directory List on the IP phones.

CONFIGURATION FILES

For specific parameters you can set in the configuration files for enabling/disabling the Directory List, see Appendix A, the section, "Asynchronous LDAP Directory Lookup Mode Support" on page A-175.

Display and Sorting

Administrators and users can configure the directory entries to display using the contact's first name and then last name or vice versa. Moreover, the option to sort contacts using either their first name or last name is available. These stings can be configured by defining the "**directory display name order**" and "**directory sort preference**" parameters in the configuration files or by navigating to the *Directory* options menu on the 6863i, 6865i, 6905, and 6910 or the *Directory > Settings* options menu on the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970.

Configuring Directory Display and Sorting Options Using the Configuration Files

Use the following procedures to configure display and sorting options for the Directory.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Asynchronous LDAP Directory Lookup Mode Support" on page A-175.

Configuring Directory Display and Sorting Options Using the Phone UI

Use the following procedure on the phone's UI to configure directory display and sorting options.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press the or key on the phone to enter the Option List.
2. Select **Directory**.

3. Navigate to the **Display Name Order** setting and press the ▶ **Enter** key.
4. Choose the order you wish to display the names in the Directory (**First Last** or **Last, First**).
5. Press the ☑ key or select ▶ **Set**.
   Your selection will be immediately applied to the phone.
6. Navigate to the **Sorting Preferences** setting and press the ▶ **Enter** key.
7. Choose the order you wish to sort the names in the Directory (**By First Name** or **By Last Name**).
8. Press the ☑ key or select ▶ **Set.**
   Your selection will be immediately applied to the phone.

For the 6867i/6869i/6920/6930:

1. Press ⚙ or ⚙ key on the phone to enter the Options List.
2. Navigate to the **Directory** > **Settings** option and press the ☑ button or **Select** softkey.
3. With **Display Name Order** highlighted press the ▶ key to move to selection column.
4. Use the ▲ and ▼ keys to and choose the desired display name order.
5. Press the ◀ key to move to back to the options column and press the ▲ key to highlight **Sorting Preferences**.
6. With **Sorting Preferences** highlighted press the ▶ key to move to selection column.
7. Use the ▲ and ▼ keys to and choose the desired sorting preference.
8. Press the **Save** softkey to save your changes.

For the 6873i/6940/6970:

1. Press ⚙ or the **Settings** softkey on the phone to enter the Options List.
2. Press the **Directory** icon.
3. Press the **Settings** icon.
4. With **Display Name Order** highlighted, choose the desired display name order.
5. Press **Sorting Preferences**.
6. With **Sorting Preferences** highlighted, choose the desired sorting preference.
7. Press the **Save** softkey to save your changes.

Enabling/Disabling Directories and Renaming Labels

Administrators have the option of enabling or disabling the respective directories on the phone as well as changing the default folder labels. These actions can be performed using the configuration files or through the phone’s UI.

Enabling/Disabling Directories and Renaming Labels Using the Configuration Files

Use the following procedures to enable/disable directories and rename directory folder labels.

CONFIGURATION FILES

For specific parameters you can set in the configuration files see Appendix A, the section, "Enhanced Directory Settings" on page A-148.

Enabling/Disabling Directories and Renaming Labels Using the Phone UI

Use the following procedure on the phone's UI to enable/disable directories and rename directory folder labels.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press the or key on the phone to enter the Option List.
2. Select **Directory**.
3. Select **External Sources.**
4. Navigate to the Directory Source you wish to enable/disable (e.g. LDAP) and press the **Enter** key.

   Note: CSV 1 and 2 are enabled by default. All other Directory sources are disabled by default.

5. Navigate to the **State** setting and press the **Enter** key.
6. Select a state (**ON** or **OFF**).
7. Press the key or select **Set.**
   Your selection will be immediately applied to the phone.
8. Navigate to the **Label** setting and press the **Enter** key.
9. Using the dialpad keys, enter in a name for the respective directory folder.
10. Select **Set.**
    Your selection will be immediately applied to the phone.

For the 6867i/6869i/6920/6930:

1. Press or on the phone to enter the Options List.
2. Navigate to the **Directory** > **External Sources** option and press the button or **Select** softkey.
3. Use the and keys to navigate through the list of Directory sources and press the button to enable or disable each one as per your preference.

   Note: CSV 1 and 2 are enabled by default. All other Directory sources are disabled by default.

4. Press the key to navigate to the **Enable/Disable** tab, and press the key to switch to the **Labels** tab.

5. Use the ▲ and ▼ keys to navigate through the list of Directory source labels and using the dialpad keys (or K680i Keyboard if available) enter in a name for the respective directory folders.
6. Press the **Save** softkey to save your changes.

For the 6873i/6940/6970:

1. Press ⚙ , ⚙ , or the **Settings** softkey on the phone to enter the Options List.
2. Press the **Directory** icon.
3. Press the **External Sources** icon.
4. Press the respective checkbox to enable or disable each directory source as per your preference.

> **Note:** CSV 1 and 2 are enabled by default. All other Directory sources are disabled by default.

5. Press the **Enable/Disable** tab, and press the right arrow key to switch to the **Labels** tab.
6. Press the Directory source label you wish to edit and enter in a new label.
7. Press the **Save** softkey to save your changes.

Entering Usernames/Passwords and Connection Testing

Before a specific Directory can be loaded, user credentials (i.e. username and password) for each respective external Directory source will need to be entered using the phone's UI by navigating to the *Options* > *Credentials* menu. For the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970, this menu also allows users to test their connection to the external Directory source.

> **Note:** Administrators may define a username and password in the "**ldap server**" configuration parameter. In such cases, a username and password does not have to be entered by the user. The fields under the LDAP tab will indicate that it already contains Administrator-defined credentials. If a username and password are entered by the user, the user-entered credentials take precedence over those defined by the Administrator.

Entering Username/Passwords and Testing Connections Using the Phone UI

Use the following procedure on the phone's UI to enter user credentials (and for the 6867i, 6869i, and 6873i, test the connection to an external source).

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press the ⚙ or ⚙ key on the phone to enter the Option List.
2. Select **Credentials**.
3. Use the ▲ and ▼ keys to navigate through the list of Directory sources and select ▶ **Enter**.
4. Press the ▲ key to navigate to the Enter Username screen and select ▶ **Enter**.

5. Using the dialpad keys, enter in your username and select ▶ **Set**.
6. Press the ▲ key to navigate to the Enter Password screen and select ▶ **Enter**.
7. Using the dialpad keys, enter in your password and press the ☑ button or select ▶ **Set.**

For the 6867i/6869i/6920/6930:

1. Press ⚙ on the phone to enter the Options List.
2. Navigate to the **Credentials** option and press the ☑ button or **Select** softkey.
3. Use the ◀ and ▶ key to navigate to the desired Directory source tab (e.g. LDAP, Microsoft Exchange, BroadSoft Xsi).
4. Press the ▲ key to highlight the **Username** field and using the dialpad keys enter in the username applicable to the Directory source.
5. Press the ▲ key to highlight the **Password** field and using the dialpad keys enter in the password applicable to the Directory source.
6. Press the ▼ key to navigate to the respective Directory source tab and repeat Steps 3 to 5 for any other sources you want to configure.
7. Press the ▼ key to navigate to the respective Directory source tab, and press the ▶ key until you get to the **Test Connection** tab.
8. Highlight the respective directory source and press the ☑ button to enable testing on that source.
9. Press the **Test** softkey to begin testing.
   A green ✔ will appear if there are no issues with the connection to the server.
   A red ! will appear if issues are found.
   If there are issues with your connection, please check your username, password, and/or server configuration.
10. Press the **Save** softkey to save your changes.

For the 6873i/6940/6970:

1. Press ⚙ on the phone to enter the Options List.
2. Press the **Credentials** icon.
3. Press the ◀ and ▶ arrow keys to navigate to the desired Directory source tab (e.g. LDAP, Microsoft Exchange, BroadSoft Xsi).
4. In the **Username** field enter in the username applicable to the Directory source.
5. In the **Password** field enter in the password applicable to the Directory source.
6. Press the Directory source tab and repeat Steps 3 to 5 for any other sources you want to configure.
7. Press the Directory source tab, and press the right arrow key until you get to the **Test Connection** tab.
8. Press the checkbox corresponding to the respective source.
9. Press the **Test** softkey to begin testing.
   A green ✔ will appear if there are no issues with the connection to the server.
   A red ! will appear if issues are found.
   If there are issues with your connection, please check your username, password, and/or server configuration.
10. Press the **Save** softkey to save your changes.

DIRECTORY SEARCH DYNAMIC THRESHOLD (6867I, 6869I, 6873I, 6920, 6930, 6940, AND 6970 ONLY)

On the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP phones, contacts are listed and updated dynamically on screen depending on the letters that are entered into the search field. This dynamic update is dependent on the "**directory search dynamic threshold**" configuration parameter. This parameter indicates the threshold value where the Directory search is no longer dynamic. By default, the search dynamic threshold is limited to 5000 entries That is, if any enabled Directory source holds more records than the configured value, users will need to manually press a Search softkey in order to trigger the search.

Configuring the Directory Search Dynamic Threshold Using the Configuration Files

Use the following procedures to configure the Directory search dynamic threshold.

CONFIGURATION FILES

For specific parameters you can set in the configuration files see Appendix A, the section, "Directory Search Dynamic Threshold" on page A-177.

DIRECTORY LOOSE NUMBER MATCHING

Default behaviour is to match the incoming call's number with the directory entry's number, after both of them were stripped from the country code, the national prefix or the trunk prefix. If the phone number is not identical, the directory lookup will fail and the phone will not display the stored directory entry's name.

However, the phone supports a directory loose number matching feature (using the "**directory digits match**" configuration parameter) whereby the Administrator can define how many digits of an incoming call's phone number the phone will use to perform a lookup in the various directories. For example, if a directory contains "1234567" as a phone number for an entry with the name defined as "John Smith", and the "**directory digits match**" parameter is defined as "**7**", the phone will take the last 7 digits of the incoming number and perform a lookup in the various directories. If an incoming call's phone number is 5551234567, as the last 7 digits are a match, the phone will display the directory entry's name (i.e. John Smith) on screen.

In previous releases, the value defined for the "**directory digits match**" parameter corresponded to the maximum number of digits the phone would take into account to perform the directory lookup. This means, using the example above, if an incoming call's phone number was 4567, the phone would still match the incoming call to the "John Smith" directory entry with the number "1234567". Starting with Release 4.3.0 SP1, the value defined for the "**directory digits match**" configuration parameter corresponds to the minimum number of digits the phone will take into account to perform a directory lookup. If the incoming call's phone number is less than the value defined for the "**directory digits match**" parameter, the phone will not perform a directory lookup and will display the information provided in the SIP header.

CONFIGURING DIRECTORY LOOSE NUMBER MATCHING

Use the following procedures to configure directory loose number matching on the IP phones.

CONFIGURATION FILES

For specific parameters you can set in the configuration files for configuring the directory loose number matching, see Appendix A, the section, "Directory Loose Number Matching" on page A-178.

CUSTOMIZABLE DIRECTORY LIST KEY

The IP phones may have a Directory List key (either a hard key or softkey/programmable key) depending on the model of the phone. An Administrator can specify a URI override for the Directory List key by defining the "**directory script"** parameter in the configuration files. Specifying a URI for this parameter causes the creation of an XML custom application instead of the standard function of the Directory List key. An Administrator can configure this parameter using the configuration files only.

CREATING A CUSTOMIZABLE DIRECTORY LIST KEY

Use the following procedure to create a customized Directory List key on the IP Phone using the configuration files.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Customizable Directory List Key" on page A-178.

VOICEMAIL

The Voicemail feature on the IP phones allow you to configure lines with phone numbers so the phone can dial out to connect to a voicemail server. You associate the Voicemail numbers with the phone numbers configured on each line.

For each assigned Voicemail number, there can be a minimum of 0 or a maximum of 1 Voicemail access phone number.

The Voicemail list displays a list of phone numbers assigned to the IP phone that has registered voicemail accounts associated with them.

Note: The Voicemail list does not display the voicemail access number.

The end of the Voicemail list displays the number of new voicemail messages (if any exist).

Note: Multiple voicemail registration and monitoring voicemail accounts is available on the IP phones. See "Speeddial/MWI Key" on page 208 for more information.

CONFIGURING VOICEMAIL

You configure Voicemail in the configuration files to dial a specific number to access an existing voicemail account. The user then follows the voicemail instructions for listening to voicemails.

Note: The phone must have a registered voicemail account from a server for this feature to be enabled. When no registered voicemail accounts are registered to the phone, the display shows "List Empty".

To configure the Voicemail feature on the IP phone, you must enter the following parameter in the configuration files:

- sip lineN vmail

You can enter a Voicemail number for each line on the phone.

For example:

```
sip line1 vmail: *97
sip line2 vmail: *95
```

Note: In the above example, the user would dial *97 to access the voicemail account for line 1, and *95 to access the voicemail account for line 2.

Use the following procedure to configure voicemail using the configuration files.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Voicemail Settings" on page A-146.

Note: You can also access your Voicemail via the "**Services**" Key on your phone if this has been setup by your System Administrator.

VISUAL INDICATORS FOR VOICEMAIL ON SCA-CONFIGURED LINES

Visual indicators for voicemail messages on Shared Call Appearance (SCA) lines have been implemented on the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 model IP phones. The parameter "**voice mail indicator**" is available allowing administrators the ability to configure what types of visual indicators the IP phones should display when voicemail messages are pending on a respective SCA line.

Administrators have three options when configuring the "**voice mail indicator**" parameter:

- 0: When a line has pending messages, the IP phone does not display any visual indicators.
- 1: When a line has pending messages, the line's corresponding softkey will display as a gray circle and the number of pending messages beside the softkey's label. Additionally, the softkey's LED will be illuminated (if available).
- 2: When a line has pending messages, the line's corresponding softkey will display as a gray circle only (i.e. no indication of the number of pending messages). Additionally, the softkey's LED will be illuminated (if available).

The parameter is set to 0 (no visual indicators) by default.

Notes:

1. The above behaviors are also applicable to expansion module softkeys representing SCA lines.
2. For programmable keys representing SCA lines, the respective programmable key's LED will flash when voicemail messages are pending.
3. The "**voice mail indicator**" parameter takes precedence over the "**line icon disabled**" parameter. If both "**voice mail indicator**" and "**line icon disabled**" are enabled, an envelope icon (and number of messages, if configured) will be displayed when voicemail messages are pending.
4. For information on SCA see "Shared Call Appearance (SCA) Call Bridging" on page 237.

CONFIGURING SCA VOICEMAIL VISUAL INDICATORS

Use the following procedure to configure the SCA voicemail visual indicators.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "SCA Voicemail Indicator Settings" on page A-147.

PIN AND AUTHORIZATION CODE SUPPRESSION

Certain features on MX-ONE require a PIN/Authorization code to be entered on the phone (for example: to register, for authorization, locking/unlocking, or accounting).

The number format is the following:

```
*<feature code>*PIN# or *<feature code>*PIN*<number>#
```

To deactivate features, the first star is replaced by #, for example:

```
#<feature code>*PIN#.
```

Administrators can now configure the "**pin suppression dial plan**" parameter so that if such a feature code with a PIN is entered, the PIN does not show up in any of the phone logs (i.e. the Outgoing Redial List) nor is it displayed on the screen during a call. The phone will dynamically mask the PIN on the display within a second of the code being entered by the user.

Note: The pin will be masked with wildcard characters (i.e. "*") on the display and in the logs.

The "**pin suppression dial plan**" parameter introduces new alphanumeric characters that control the masking of the PIN: "(" and ")".

The following is an example value of the new configuration parameter:

```
"*11*(1XXX)*5555+#|*72*(1XXX)#|#73*(1XXX)#"
```

where (1XXX) will mask any PINs that are 4 digits long and start with 1.

This parameter value should lead to the following masking:

- Entered digits *11*1234*5555# will lead to INVITE to this number but *11******5555# is shown on the display and in the Outgoing Redial List.
- Entered digits *72*1234# will lead to INVITE to this number but *72*****# is shown on the display and in the Outgoing Redial List.
- Entered digits #73*1234# will lead to INVITE to this number but #73*****# is shown on the display and in the Outgoing Redial List.

Use the following procedure to configure the pin suppression feature using the configuration files.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "PIN Suppression" on page A-182.

XML CUSTOMIZED SERVICES

Extensible Markup Language (XML) is a markup language much like HTML. HTML was designed to display data and to focus on how data looks. XML was designed to describe data and to focus on what data is.

The following are characteristics of XML:

- XML tags are not predefined. You must define your own tags.
- XML uses a Document Type Definition (DTD) or an XML Schema to describe the data.
- XML with a DTD or XML Schema is designed to be self-descriptive
- XML is a W3C Standard Recommendation

CREATING CUSTOMIZED XML SERVICES ON THE IP PHONES

The XML application for the IP phones allows users to create custom services they can use via the phone's keyboard and display. These services include things like weather and traffic reports, contact information, company info, stock quotes, or custom call scripts.

The IP phone XML application supports the following proprietary objects that allow for the customization of the IP phone's display.

XML OBJECT	DESCRIPTION
AastraIPPhoneTextMenu (for Menu screens)	Creates a numerical list of menu items on the IP phones.
AastraIPPhoneTextScreen (for Text screens) AastraIPPhoneFormattedTextScreen (for Text screens)	Creates a screen of text that wraps appropriately. Creates a formatted screen of text (specifies text alignment, text size, text static or scrolling)
AastraIPPhoneInputScreen (for User Input screens) AastraIPPhoneInputScreen Time and Date Attributes (for User Input screens)	Creates screens for which the user can input text where applicable. Allows you to specify US (HH:MM:SS am/pm and MM/DD/YYYY) or International (HH:MM:SS and DD/MM/YYYY) time/date formats for an XML user input screen.
AastraIPPhoneStatus (for Idle screen)	Creates a screen that displays status messages when applicable.
AastraIPPhoneExecute (for executing XML commands)	Allows the phone to execute commands (i.e. “reset”, “NoOp”, etc.) using XML.
AastraIPPhoneConfiguration (for pushing a configuration to the phone)	Allows the server to push a configuration to the phone.(See page 5-319 for more information).
AastraIPPhoneImageScreen (Standard Bitmap Image)	Creates a display with a single bitmap image according to alignment, height, and width specifications.
AastraIPPhoneImageMenu (Menu Image)	Creates a display with a bitmap image as a menu. Menu selections are linked to keypad keys (0-9, *, #).

XML OBJECT	DESCRIPTION
AastraIPPhoneTextMenu (Icon Menu) (Icon Menu Image)	Creates a display that has a small icon before each item in the menu.
AastraIPPhoneIconMenu	Creates a list of menu items on the IP phones just like TextMenu but in this case menus are represented by an icon or a sequence of text lines.
AastraIPPhoneSoftkey	Allows an external application to modify the configuration of an "xmladvanced" top softkey dynamically.

REFERENCE

For more information about creating customized XML applications, contact Mitel Customer Support regarding the ***XML Developer's Guide***.

You can also use the following attributes/options with the XML objects to further customize your XML applications:

ATTRIBUTE/OPTION	DESCRIPTION/USAGE	VALID VALUES
Beep	Enables or disables a BEEP option to indicate a status on the phone. Use with: XML object (See the ***XML Developer's Guide***) Configuration files (See page 5-318) Mitel Web UI (See page 5-318)	yes | no Default = no **Note:** This value is case sensitive.
xml status scroll delay (config files) Status Scroll Delay (seconds) (Web UI)	Allows you to set the time delay, in seconds, between the scrolling of each status message on the phone. Use with: Configuration files (See page 5-319) Mitel Web UI (See page 5-319)	1 to 25 Default = 5
XML Scroll Up and Scroll Down Tags	Supports the new tags "scrollUp" and "scrollDown" that are triggered when the scrolling reaches the top or the bottom of the menu items. Use with: XML object (See the ***XML Developer's Guide***)	some URI
Timeout	Specifies a timeout value for the LCD screen display. Use with: XML object (See the ***XML Developer's Guide***)	0, 30, 45, 60 Default =45

ATTRIBUTE/OPTION	DESCRIPTION/USAGE	VALID VALUES
XML Get Timeout	Specifies a timeout value, in seconds, that the phone waits for the far side to return a response after accepting the HTTP GET connection. Use with: Configuration Files (See page 5-320)	0 to 2147483647 seconds Default =0 (never timeout)
LockIn	Specifies whether or not the information on the LCD screen stays displayed when other events occur (such as pressing buttons on the keypad). Use with: XML object (See the ***XML Developer's Guide***)	yes | no Default = no
CancelAction	Specifies a URI that the phone executes a GET on when the user presses the default CANCEL key. Use with: XML object (See the ***XML Developer's Guide***)	Fully qualified URI **For example**: cancelAction= http://10.50.10.117/ft.xml

ENABLING/DISABLING A BEEP FOR STATUS MESSAGE DISPLAYS

You can enable or disable a BEEP option using the Status Message object (AastraIPPhoneStatus), the configuration files, or the Mitel Web UI.

Note: For enabling/disabling a status message beep using the Status Message object, see the ***XML Developer's Guide***.

When the phone receives a status message, the BEEP notifies the user that the message is displaying.

You can use the following to enable/disable a status message beep:

- **AastraIPPhoneStatus** object (via XML object; see the ***XML Developer's Guide*)**
- **xml beep notification** (via configuration files)
- **XML Beep Support** (via the Mitel Web UI)

Enabling the beep is an indication to the phone to sound a beep when it receives an AastraIPPhoneStatus object. If you disable the beep, or no AastraIPPhoneStatus object appears in the status message, then the default behavior is no beep is heard when the object arrives to the phone.

The value set in the configuration files and Mitel Web UI override the attribute you specify for the AastraIPPhoneStatus object.

For example, if the AastraIPPhoneStatus object has the attribute of **Beep="yes"**, and you uncheck (disable) the "**XML Beep Support**" in the Mitel Web UI, the phone does not beep when it receives an AastraIPPhoneStatus object.

Setting the BEEP option in the configuration files and the Mitel Web UI applies to the phone immediately.

REFERENCE

For information about enabling/disabling the XML beep in the Mitel Web UI, see "XML Beep Support" on page 5-95.

SCROLL DELAY OPTION FOR STATUS MESSAGES

The IP phones support a scroll delay option that allows you to set the time delay, in seconds, between the scrolling of each status message on the phone. The default time is 5 seconds for each message to display before scrolling to the next message. You can configure this option via the configuration files or the Mitel Web UI.

You can use the following to set the scroll delay for status messages:

- **xml status scroll delay** (via the configuration files)
- **Status Scroll Delay (seconds)** (via the Mitel Web UI)

Changes apply to the phone immediately.

REFERENCE

For more information about configuring status scroll delay, see "Status Scroll Delay" on page 5-97.

XML CONFIGURATION PUSH FROM THE SERVER

The IP phones provide an XML feature that allows you to make configuration changes to the phone that take affect immediately, without having to reboot the phone. This feature involves creating XML scripts that push the changed configuration parameter(s) from the server to the IP phones.

You can use the **AastraIPPhoneConfiguration** object in the XML scripts to change configuration parameters or configure new parameters. However, since the IP phone does not save **new** parameters created in XML scripts to the *local.cfg* file, when the phone reboots, it does not save the new parameters on the phone. In order for the phone to apply **new** configuration parameters, you have to enter the parameters via the user interfaces (Telephone User Interface, Web User Interface, or configuration files), or reapply the new parameters using the XML scripts after every boot.

Specific configuration parameters are dynamic on the phone when pushed from XML scripts on the server. See the ***XML Developer's Guide*** for more information about XML configuration scripts and dynamic configuration parameters.

For more information about creating XML configuration scripts and for XML script examples, see the ***XML Developer's Guide***.

CONFIGURING THE PHONE TO USE XML

You can configure the phone to request the XML objects you create by configuring specific parameters via the configuration files or the Mitel Web UI.

Users can access XML applications via softkeys configured on the IP phones. The phone performs an HTTP GET on the URI configured in the Mitel Web UI or configuration files.

You configure the following parameters for object requests:

- xml application URI
- xml application title

The xml application URI is the application you are loading into the IP phone.

The xml application title is the name of the XML application that displays on the Services menu in the IP Phone UI (as option #4).

XML GET TIMEOUT

The IP phone has a parameter called, "**xml get timeout**" that allows you to specify a timeout value, in seconds, that the phone waits for the far side to return a response after accepting the HTTP GET connection. If the far side accepts the GET connection but never returns a response, it blocks the phone until it is rebooted. If you enter a value greater than 0 for this parameter, the phone times out and will not be blocked.

For more information about configuring this parameter, see Appendix A, the section, "XML Settings" on page 186.

XML Push Requests

In addition to initiating a request to an XML application from a softkey, an HTTP server can push an XML object to the phone via HTTP Post. When the phone sees a PUSH request containing an XML object, it tries to authenticate the request. It does so by checking the IP address or host name of the requesting host against a list of trusted hosts (or domain names) configured via the Mitel Web UI (parameter called **XML Push Server List**) or the configuration files (parameter called **xml application post list**). If the request is authenticated, the XML object is handled by the IP phone accordingly, and displays the information to the screen.

Note: The HTTP Post must contain HTTP packets that have an "xml" line in the message body. For more information about adding "xml" lines in HTTP packets, see the ***XML Developer's Guide***.

Example Configuration of XML Application

The following example shows the parameters you enter in the configuration files to configure an XML application:

```
xml application URI: http://172.16.96.63/mitel/internet.php
xml application title: Mitel
xml application post list: 10.50.10.53, dhcp10-53.ana.mitel.com
```

CONFIGURING FOR XML ON THE IP PHONE

After creating an XML application, an administrator can configure the IP phone to use the application using the configuration files or the Mitel Web UI.

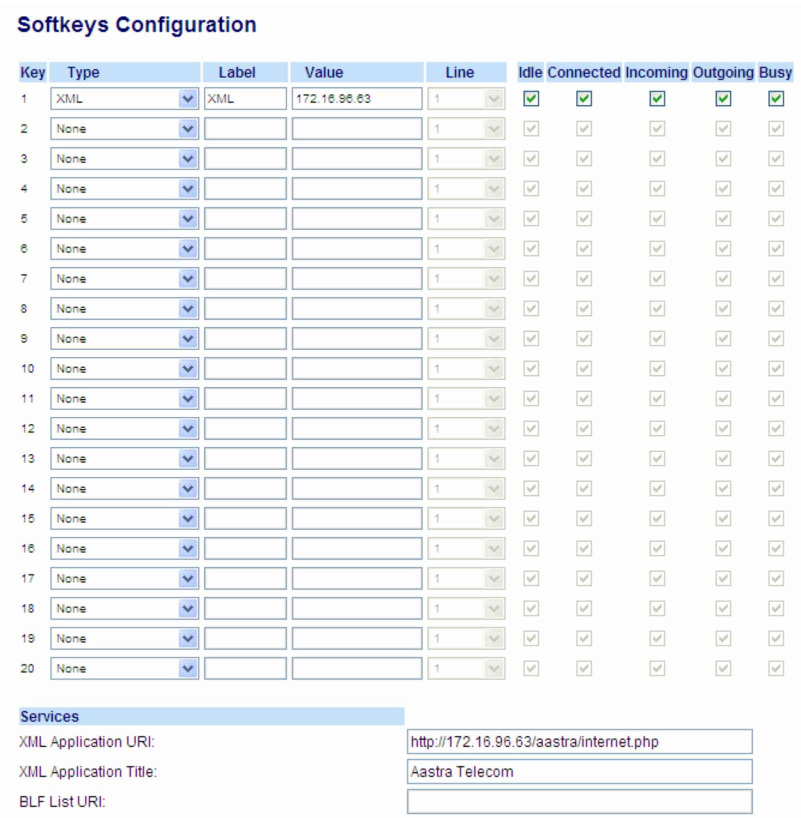
CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "XML Settings" on page A-186.

For the 6867i/6869i/6873i/6920/6930/6940/6970:

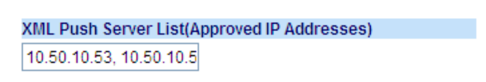
MITEL WEB UI

1. Click on **Operation->Softkeys and XML**.



2. Select a key.
3. In the "**Type**" field, select **XML** from the list box.
4. In the "**Label**" field, enter a label that displays on the IP phone for the softkey. For example, "**XML**".
5. In the "**Value**" field, enter the IP address or qualified domain name of the XML application.

6. In the "**XML Application URI**" field, enter the HTTP server path or qualified domain name of the XML application you want to load to the IP phone. For example, you could enter an XML application called "http://172.16.96.63/mitel/internet.php" in the applicable field.
7. In the "**XML Application Title**" field, enter the name of the XML application that you want to display on the IP phone Services Menu. ".
8. Click **Save Settings** to save your changes.
   The XML application is applied to the IP phone immediately.
   When the XML application is pushed to the phone via an HTTP POST, a host IP address or DNS server is required.
9. Click on **Advanced Settings->Configuration Server**.



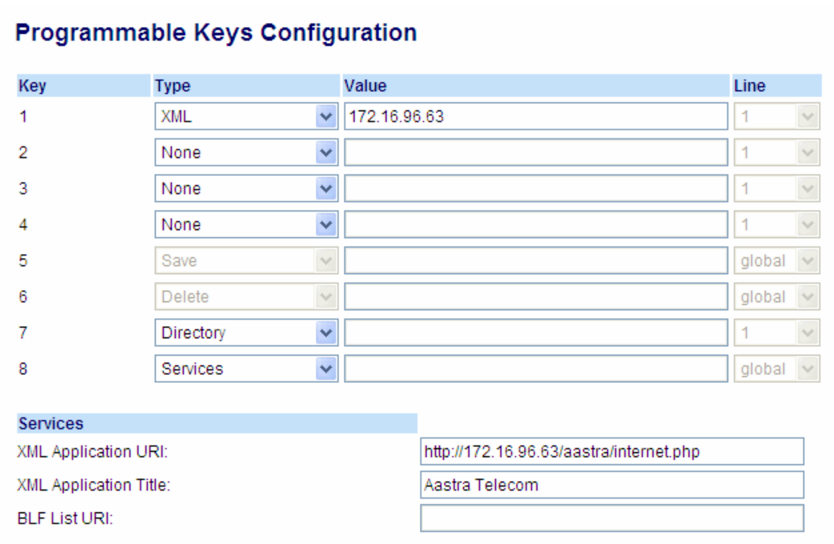
10. In the ***"XML Push Server List (Approved IP Addresses)"*** field, enter the host IP address and/or DNS server. You can enter multiple IP address and/or DNS servers (separated by commas). In the example in Step 8, the illustration shows a host IP address of "10.50.10.53, 10.50.10.54" in the applicable field.
11. Click **Save Settings** to save your changes.

Note: No posting is performed if a session times out.

For the 6863i/6865i/6905/6910:

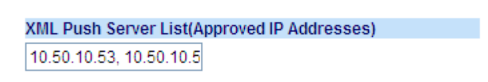
MITEL WEB UI

1. Click on **Operation->Programmable Keys.**



2. Select an available key.
3. In the "**Type**" field, select **XML** from the list box.

4. In the "**Value**" field, enter the IP address or qualified domain name of the XML application.
5. In the "**XML Application URI**" field, enter the HTTP server path or qualified domain name of the XML application you want to load to the IP phone. For example, you could enter an XML application called "http://172.16.96.63/mitel/internet.php" in the applicable field.
6. In the "**XML Application Title**" field, enter the name of the XML application that you want to display on the IP phone Services Menu.
7. Click **Save Settings** to save your changes.
   The XML application is applied to the IP phone immediately.
   When the XML application is pushed to the phone via an HTTP POST, a host IP address or DNS server is required.
8. Click on **Advanced Settings->Configuration Server**.



9. In the ***"*XML Push Server List (Approved IP Addresses)*"*** field, enter the host IP address and/or DNS server. You can enter multiple IP address and/or DNS servers (separated by commas). In the example in Step 6, the illustration shows a host IP address of "10.50.10.53, 10.50.10.54" in the applicable field.
10. Click **Save Settings** to save your changes.

> **Note:** No posting is performed if a session times out.

USING THE XML CUSTOMIZED SERVICE

After you create, save, and configure the IP phone with an XML application, the customized service is ready for you to use.

REFERENCE

For more information about customizing the phones using XML objects, contact Mitel Customer Support regarding the " ***XML Development Guide***."

Use the following procedure to use the XML feature on the IP phone.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press the programmable key configured on the phone for XML services.
   A "**Custom Features**" screen displays.
2. Use the ▲ and ▼ arrow keys to scroll through the customized features.
3. Select a service to display the information for that customized service.
   Message services display to the screen after pressing the programmable key.
   For user input services, follow the prompts as appropriate.

4. To exit from the "**Custom Features**" screen, press the XML programmable key again.

For the 6867i/6869i/6920/6930:

1. Press the **XML** softkey on the phone. An XML screen displays.
2. Use the ▲ and ▼ arrow keys to scroll through the customized features.
3. For menu and directory services, select a service to display the information for that customized service. Message services display to the screen after pressing the respective key. For user input services, follow the on-screen prompts.
4. To exit from the XML screen, press the **XML** softkey again or press the button.

For the 6873i/6940/6970:

1. Press the **XML** softkey on the phone. An XML screen displays.
2. For menu and directory services, select a service to display the information for that customized service. Message services display to the screen after pressing the respective key. For user input services, follow the on-screen prompts.
3. To exit from the XML screen, press the **XML** softkey again or press the button.

ACTION URIS

The IP phones have a feature that allows an administrator to specify a uniform resource identifier (URI) that triggers a GET when certain XML events occur. The Action URI feature prevents the phones from hanging if the Action URIs should fail. The phones also support transparent, non-blocking, XML post execute item URIs.

The IP phone XML events that support this feature are defined in the following table.

ACTION URI	DESCRIPTION
Startup	Specifies the URI for which the phone executes a GET on when a startup event occurs.
Successful Registration	Specifies the URI for which the phone executes a GET on when a successful registration event occurs.
Registration Event	Specifies the URI for when registration events occur or when there are registration state changes. **Note:** If defined, this action URI is also called upon at startup if the SIP registrar IP has not been configured (i.e. the IP is 0.0.0.0). **Note:** This action URI is not called when the same event is repeated (for example, a timeout occurs again when registration is already in a timeout state.)
Incoming Call	Specifies the URI for which the phone executes a GET on when an incoming call event occurs.
Outgoing Call	Specifies the URI for which the phone executes a GET on when an outgoing call event occurs.
Offhook	Specifies the URI for which the phone executes a GET on when an offhook event occurs.
Onhook	Specifies the URI for which the phone executes a GET on when an onhook event occurs.

ACTION URI	DESCRIPTION
Connected	Specifies the URI for which the phone executes an HTTP GET when it goes into the “connected” state. This includes regular phone calls, intercom calls, paging calls, RTP streaming, and the playing of a WAV file. It is also triggered when the phone establishes the second leg of a 3-way call. For more information, see “Action URI Connected” on page 5-333.
Disconnected	Specifies the URI that the phone executes a GET on, when it transitions from the incoming, outgoing, calling, or connected state into the idle state. For more information, see “Action URI Disconnected” on page 5-334.
XML SIP Notify	Specifies the URI to be called when an empty XML SIP NOTIFY is received by the phone. For more information, see “XML SIP Notify Events” on page 5-338.
Poll	Specifies the URI to be called every "action uri poll interval" seconds. For more information, see “Polling Action URIs” on page 5-331.
Poll Interval	Specifies the interval, in seconds, between calls from the phone to the "action uri poll". For more information, see “Polling Action URIs” on page 5-331.
Blf	Specifies the URI for which the phone executes a GET on when a BLF or BLF/Xfer key is pressed.

Note: For more information about the XML execute items, see the ***XML Developer’s Guide***.

The following table identifies the configurable action URI parameters in the configuration files and the Mitel Web UI. This table also identifies the variables that apply to specific parameters.

Action URIs and Associated Variables

CONFIGURATION FILE PARAMETERS	MITEL WEB UI PARAMETERS AT ADVANCED SETTINGS-> ACTION URI	APPLICABLE VARIABLES
action uri startup	Startup	$$DISPLAYNAME$$ $$SIPUSERNAME$$ $$SIPAUTHNAME$$ $$PROXYURL$$ $$LINESTATE$$ $$LOCALIP$$ $$REGISTRATIONSTATE$$ $$REGISTRATIONCODE$$
action uri registered	Successful Registration	$$SIPUSERNAME$$ $$SIPAUTHNAME$$ $$PROXYURL$$ $$LINESTATE$$ $$LOCALIP$$
action uri registration event	Registration Event	$$REGISTRATIONSTATE$$ $$REGISTRATIONCODE$$
action uri incoming	Incoming Call	$$REMOTENUMBER$$ $$DISPLAYNAME$$ $$SIPUSERNAME$$ $$INCOMINGNAME$ $$LINESTATE$$ $$CALLDURATION$$ $$CALLDIRECTION$$ $$LOCALIP$$ $$LINEINDEX$$
action uri outgoing	Outgoing Call	$$REMOTENUMBER$$ $$SIPUSERNAME$$ $$LINESTATE$$ $$LOCALIP$$ $$LINEINDEX$$
action uri offhook	Offhook	$$LINESTATE$$ $$LOCALIP$$
action uri onhook	Onhook	$$LOCALIP$$ $$CALLDURATION$$ $$CALLDIRECTION$$ $$LINESTATE$$

CONFIGURATION FILE PARAMETERS	MITEL WEB UI PARAMETERS AT ADVANCED SETTINGS-> ACTION URI	APPLICABLE VARIABLES
action uri connected	Connected	$$REMOTENUMBER$$ $$DISPLAYNAME$$ $$SIPUSERNAME$$ $$SIPAUTHNAME$$ $$INCOMINGNAME$ $$PROXYURL$$ $$LINESTATE$$ $$LOCALIP$$ $$DISPLAYNAME$$ $$CALLDURATION$$ $$CALLDIRECTION$$ $$REGISTRATIONSTATE$$ $$REGISTRATIONCODE$$
action uri disconnected	Disconnected	$$LINESTATE$$ $$LOCALIP$$ For more information, see "Action URI Disconnected" on page 5-334.
action uri blf	N/A	$$BLFNO$$ $$BLFSTATE$$ $$BLFTRANSFER$$
action uri xml sip notify	XML SIP Notify	$$LOCALIP$$ For more information, see "XML SIP Notify Events" on page 5-338.
action uri poll	Poll	For more information, see "Polling Action URIs" on page 5-331.
action uri poll interval	Interval	For more information, see "Polling Action URIs" on page 5-331.

Variable Descriptions

The following table provides a description of each variable.

VARIABLE	DESCRIPTION
$$SIPUSERNAME$$	Username associated with: • registered phone • incoming caller • outgoing caller
$$SIPAUTHNAME$$	Authentication name associated with: • registered phone

VARIABLE	DESCRIPTION
$$PROXYURL$$	Proxy URL associated with: • registered phone
$$LINESTATE$$	Current line state associated with: • registered phone • incoming caller • outgoing caller • offhook • onhook • disconnected
$$LOCALIP$$ **Note:** This variable allows for enhanced information in call records and billing applications.	IP Address associated with: • registered phone • onhook
$$REMOTENUMBER$$	Remote number associated with: • incoming caller • outgoing caller
$$DISPLAYNAME$$	Display name associated with: • incoming caller
$$SIPUSERNAME$$	Username associated with: • registered phone • incoming caller • outgoing caller
$$INCOMINGNAME$$	Name associated with: • incoming caller
$$CALLDURATION$$ **Note:** This variable allows for enhanced information in call records and billing applications.	Duration of last call. This variable is associated with: • onhook
$$CALLDIRECTION$$ **Note:** This variable allows for enhanced information in call records and billing applications.	Specifies whether the current/last call was incoming or outgoing. This variable is associated with: • onhook
$$REGISTRATIONSTATE$$	Specifies the state of the phone's registration. Registration states can be: • registered • unregistered • expired • refused • timeout

VARIABLE	DESCRIPTION
$$REGISTRATIONCODE$$	Specifies the code generated during the registration process. Registration code can be: "xxx" where xxx is the 3 digit code; for example, "403". Possible codes are: • 001 (registration successful) • 403 (registration failed)
$$LINEINDEX$$	Specifies Line Index of the focused line (SIP registration line number).

How it Works

When a startup, successful registration, incoming call, outgoing call, offhook, or onhook call event occurs on the phone, the phone checks to see if the event has an action URI configured. If the phones finds a URI configured, any variables configured (in the form $$VARIABLENAME$$) are replaced with the value of the appropriate variable. After all of the variables are bound, the phone executes a GET on the URI. The Action URI binds all variables and is not dependent on the state of the phone.

For example, if you enter the following string for the **action uri outgoing** parameter:

```
action uri outgoing:
http://10.50.10.140/outgoing.pl?number=$$REMOTENUMBER$$
```

and you dial out the number 5551212, the phone executes a GET on:

```
http://10.50.10.140/outgoing.pl?number=5551212
```

Notes:

1. If the phone cannot find the Action URI you specify, it returns a “NULL” response. For example,
`http://10.50.10.140/outgoing.pl?number=`
2. After executing a GET on the URI, the phone expects a valid XML response. If a valid XML response is not received, an error message is displayed on screen.

You can configure this feature via the configuration files or the Mitel Web UI.

Configuring XML Action URIs

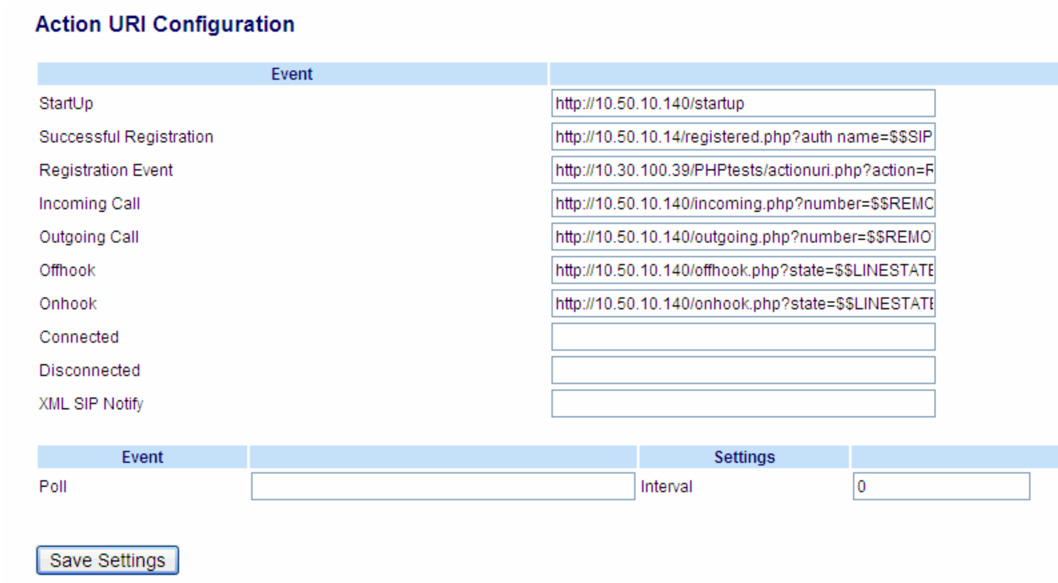
Use the following procedures to configure XML Action URIs using the configuration files or the Mitel Web UI.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Action URI Settings” on page A-188.

MITEL WEB UI

1. Click on **Advanced Settings->Action URI.**



2. Enter an XML URI for a startup event in the "**Startup**" field. For example:
   http://10.50.10.140/startup
   This parameter specifies the URI for which the phone executes a GET on when a startup event occurs.

3. Enter an XML URI for a successful registration in the "**Successful Registration**" field. For example:
   http://10.50.10.14/registered.php?auth name=$$SIPAUTHNAME$$
   This parameter specifies the URI for which the phone executes a GET on when a successful registration event occurs.

   Note: For a successful registration event, use the associated variables indicated in the table "Action URIs and Associated Variables" on page 5-326.

   The "**Successful Registration**" parameter executes on the first successful registration of each unique line configured on the phone.

4. Enter an XML URI in the "**Registration Event**" field, for when the phone performs registration. For example:
   http://10.30.100.39/PHPtests/actionuri.php?action=RegEvt&regstate=$$REGISTRATIONSTATE$$&regcode=$$REGISTRATIONCODE$$
   This parameter specifies the URI that the phone executes a GET on, when a registration event change occurs.

   Note: For a registration event, use the associated variables indicated in the table "Action URIs and Associated Variables" on page 5-326.

5. Enter an XML URI for an incoming call event in the "**Incoming Call**" field. For example:
http://10.50.10.140/incoming.php?number=$$REMOTENUMBER$$
This parameter specifies the URI for which the phone executes a GET on when an incoming call event occurs.

> **Note:** For an incoming call event, use the associated variables indicated in the table "Action URIs and Associated Variables" on page 5-326.

6. Enter an XML URI for an outgoing call event in the "**Outgoing Call**" field. For example:
http://10.50.10.140/outgoing.php?number=$$REMOTENUMBER$$
This parameter specifies the URI for which the phone executes a GET on when an outgoing call event occurs. .

> **Note:** or an outgoing call event, use the associated variables indicated in the table "Action URIs and Associated Variables" on page 5-326.

7. Enter an XML URI for an offhook event in the "**Offhook**" field. For example:
http://10.50.10.140/offhook.php?state=$$LINESTATE$$
This parameter specifies the URI for which the phone executes a GET on when an offhook event occurs.

> **Note:** For an offhook event, use the associated variables indicated in the table "Action URIs and Associated Variables" on page 5-326.

8. Enter an XML URI for an onhook event in the "**Onhook**" field. For example:
http://10.50.10.140/onhook.php?state=$$LINESTATE$$
This parameter specifies the URI for which the phone executes a GET on when an onhook event occurs.

> **Note:** For an onhook event, use the associated variables indicated in the table "Action URIs and Associated Variables" on page 5-326.

9. To configure a Connected event, see the section, "Action URI Connected" on page 5-333.

10. To configure a Disconnected event, see the section, "Action URI Disconnected" on page 5-334.

11. To configure an XML SIP Notify event, see the section, "XML SIP Notify Events" on page 5-338.

12. (Optional) You can poll a URI at specific intervals on the phones. For more information about polling Action URIs, see "Polling Action URIs" on page 5-331.

13. Click **Save Settings** to save your changes.

POLLING ACTION URIS

Another way to reach a phone behind a firewall is to have the phone make an XML call at periodic intervals. An Administrator can use the **action uri poll** parameter that commands the phone to perform an XML call at configurable intervals.

An Administrator can specify the URI to be called and specify the interval between polls using the configuration files or the Mitel Web UI. Configuration of this feature is dynamic (no reboot required).

Configuring Polling Action URI via the Configuration Files

Use the following parameters to configure the polling Action URI on the IP Phones.

- action uri poll
- action uri poll interval

CONFIGURATION FILES

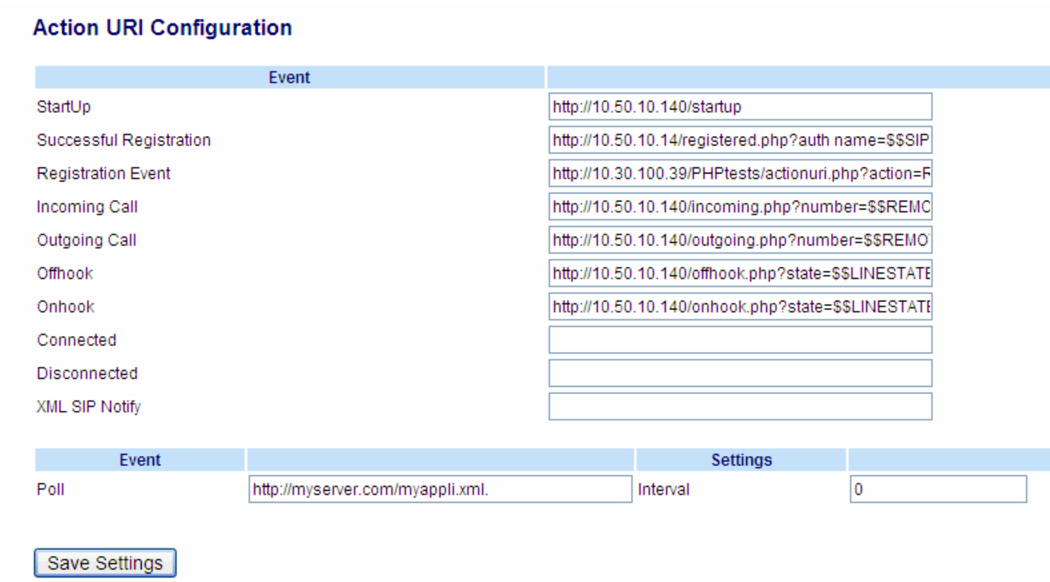
For the specific parameter you can set in the configuration files, see Appendix A, the section, "Polling Action URI Settings" on page A-194.

Configuring Polling Action URI via the Mitel Web UI

Use the following procedure to configure polling Action URI using the Mitel Web UI.

MITEL WEB UI

1. Click on **Advanced Settings->Action URI**.



2. In the "**Poll**" field, enter a URI to be called every "action uri pool interval" seconds. Enter the value in a URI format. For example, **http://myserver.com/myappli.xml**.
3. In the "**Interval**" field, enter the interval, in seconds, between calls from the phone to the "action uri poll". The value of "**0**" is disabled.
4. Click **Save Settings** to save your changes.

ACTION URI CONNECTED

A parameter called "**action uri connected**" (configuration files) and "**Connected**" (Mitel Web UI) now allows XML scripts to determine when a call is connected. When enabled, the phone triggers an HTTP GET when it goes into the "connected" state. This includes regular phone calls, intercom calls, paging calls, RTP streaming, and the playing of a WAV file. It is also triggered when the phone establishes the second leg of a 3-way call.

This parameter can use the following variables:

- $$REMOTENUMBER$$
- $$DISPLAYNAME$$
- $$SIPUSERNAME$$
- $$SIPAUTHNAME$$
- $$INCOMINGNAME$
- $$PROXYURL$$
- $$LINESTATE$$
- $$CALLDIRECTION$$
- $$LOCALIP$$
- $$DISPLAYNAME$$
- $$CALLDURATION$$
- $$REGISTRATIONSTATE$$
- $$REGISTRATIONCODE$$

If the Administrator enables this feature (by specifying a connect URI), when a call is connected, the phone checks to see if the event has a Connect URI configured. If the phones finds a configured URI it executes an XML script or the variable if defined.

Example

In the configuration files, you can enter the following:

```
action uri connected: http://www.example.com/connect.php
```

An Administrator can enable the "Connected" Action URI feature using the configuration files or the Mitel Web UI.

Limitations

- During SLA calls, the phone uses the Action URI Connected parameter when the line is seized before the caller dials out.
- SCA and BLA calls on hold trigger the Action URI Connected parameter, since the retrieval is a 2nd call by the phone, and the phone cannot link the retrieved call with the earlier held call.

For more information about the XML API objects, see the ***XML Developers Guide***.

Configuring the Action URI Connected Feature

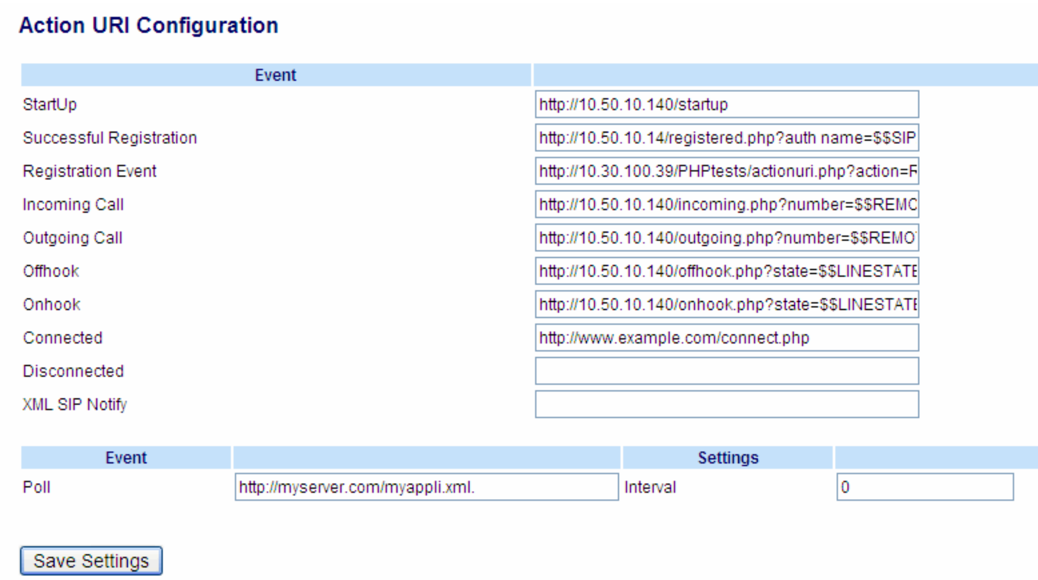
Use the following procedure to configure the Action URI Connected feature on the phone.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Action URI Settings" on page A-188.

MITEL WEB UI

1. Click on **Advanced Settings->Action URI.**



2. In the "**Connected**" field, enter a valid URI for which the phone executes a GET on, when it goes into the "connected" state. Leaving this field empty disables the Action URI Connected feature. For example,
   http://www.example.com/connect.php

3. Click **Save Settings** to save your settings.

ACTION URI DISCONNECTED

The phones have a parameter, "**action uri disconnected**" that allow a disconnect event to occur when the phone transitions from any active state (outgoing, incoming, connected, or calling) to an idle state. This parameter can use the variable "**$$LINESTATE$$**".

Note: The **$$LINESTATE$$** variable is optional and not required when enabling the "**action uri disconnected**" parameter.

If the Administrator enables this feature (by specifying a disconnect URI), when a call is disconnected, the phone checks to see if the event has a Disconnect URI configured. If the phones finds a configured URI with a $$LINESTATE$$ variable, it replaces the $$LINESTATE$$ variable with the appropriate line state of the current active line. After all of the variables are bound, the phone executes a GET on the URI. The following table lists the applicable values for the $$LINESTATE$$ variable.

$$LINESTATE$$ VALUE	DESCRIPTION	MEANING IN A DISCONNECTED URI
IDLE	Phone is idle.	N/A
DIALING	Phone is offhook and ready to dial.	N/A
CALLING	A SIP INVITE was sent but no response was received.	Error occurred during the call or the call was cancelled.
OUTGOING	Remote party is ringing.	Call was cancelled.
INCOMING	Local phone is ringing.	Call was missed or cancelled.
CONNECTED	Parties are talking.	Call was successful.
CLEARING	Call was released but not acknowledged.	N/A

The Action URI Disconnect feature allows an Administrator to determine the reason for the disconnect if required.

Note: If you enable the Action URI Disconnect feature by specifying a URI, the URI is called when any disconnect event occurs including an intercom call or a conference setup.

Example

If you enter the following string on Phone A for the "**action uri disconnected"** parameter:

```
action uri disconnected:
http://fargo.ana.mitel.com/disconnected.xml?state=$$LINESTATE$$
```

and then Phone A calls Phone B, Phone B answers and then hangs up, Phone A executes a GET on:

```
http://fargo.ana.mitel.com/disconnected.xml?state=CONNECTED
```

which is what the remote server receives.

An Administrator can enable the disconnect feature using the configuration files or the Mitel Web UI.

Configuring the Action URI Disconnected Feature

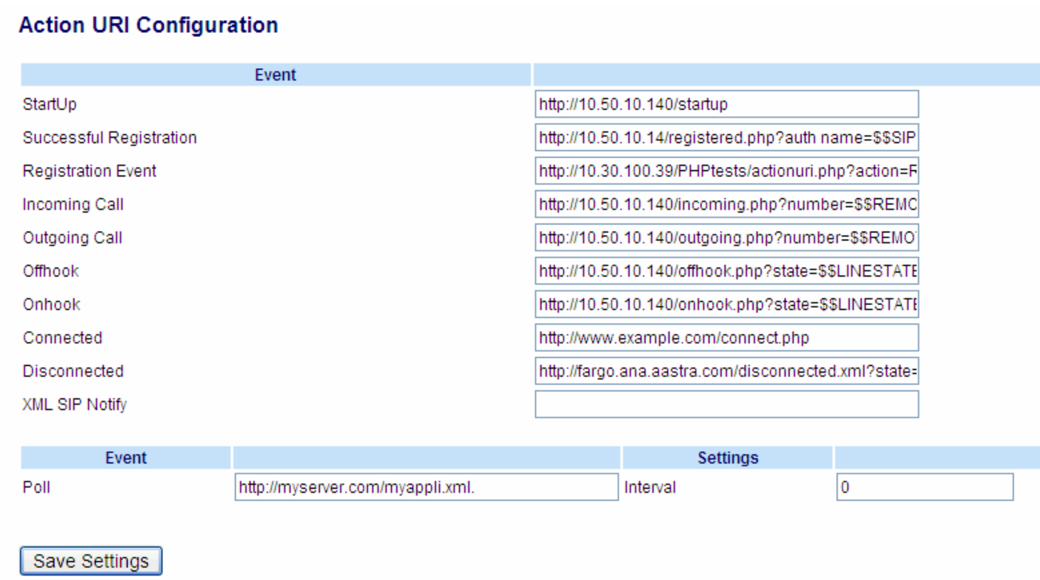
Use the following procedure to configure the Action URI Disconnected feature on the phone.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Action URI Settings" on page A-188.

MITEL WEB UI

1. Click on **Advanced Settings->Action URI->Event.**



2. In the "**Disconnected**" field, enter a valid URI for which the phone executes a GET on, when it transitions from the incoming, outgoing, calling, or connected state into the idle state. Leaving this field empty disables the Action URI Disconnected feature. For example,

http://fargo.ana.mitel.com/disconnected.xml?state=$$LINESTATE$$
The following table lists the applicable values and descriptions for the $$LINESTATE$$.

$$LINESTATE$$ VALUE	DESCRIPTION	MEANING IN A DISCONNECTED URI
IDLE	Phone is idle.	N/A
DIALING	Phone is offhook and ready to dial.	N/A
CALLING	A SIP INVITE was sent but no response was received.	Error occurred during the call.
OUTGOING	Remote party is ringing.	Call was canceled.
INCOMING	Local phone is ringing.	Call was missed or canceled.
CONNECTED	Parties are talking.	Call was successful.
CLEARING	Call was released but not acknowledged.	N/A

3. Click **Save Settings** to save your settings.

ACTION URI BLF

Notes:

1. This feature is applicable to the 6865i, 6867i, 6869i, 6873i, 6920, 6930, and 6940 SIP Phones.
2. The parameter "**blf key mode**" must be defined as "**2**" in the configuration files to use the BLF Action URI feature.
3. If the parameter "**blf key mode**" is defined as "**2**" but a BLF Action URI is not defined, pressing a BLF or BLF/Xfer key will follow the default BLF key mode behavior (DTMF in active call).

The action URI feature has been expanded to support BLF XML events whereby when a configured BLF or BLF/Xfer key is pressed, the phone checks to see if the event has an Action URI configured. If the phones finds a URI configured, any variables defined (in the form $$VARIABLENAME$$) are replaced with the value of the appropriate variable. After all of the variables are bound, the phone executes an HTTP GET on the URI.

The BLF Action URI can only be configured using the configuration files by defining the "**action uri blf**" parameter. The "**action uri blf**" parameter supports the following variables:

VARIABLE	DESCRIPTION
$$BLFNO$$	Indicates the monitored extension.
$$BLFSTATE$$	Indicates the monitored line state. Values include: • IDLE • BUSY • RINGING • ONHOLD • DND • UNKNOWN

VARIABLE	DESCRIPTION
$$BLFTRANSFER$$	Indicates if a BLF/Xfer key was pressed. Values include: • YES (BLF/Xfer) • NO (BLF)

For example, if you define the "**blf key mode**" as "**2**" and enter the following string for the "**action uri blf**" parameter:

```
action uri blf: http://192.168.0.50/blf.php?BLFNo=$$BLFNO$$
```

when you press a BLF key defined as 5000, an HTTP GET will be performed on:

```
http://192.168.0.50/blf.php?BLFNo=5000
```

Configuring the Action URI BLF Feature

Use the following procedure to configure the Action URI BLF feature on the phone.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Action URI Settings" on page A-188.

XML SIP NOTIFY EVENTS

In order for an XML push to bypass the firewall, the phone supports a proprietary SIP NOTIFY event (aastra-xml) with or without XML content. An Administrator can enable/disable the SIP NOTIFY event using a specific parameter in the configuration files (**sip xml notify event**) or the Mitel Web UI (**XML SIP Notify**).

If XML content is provided in the SIP NOTIFY, it is processed directly by the phone as it is done for an XML PUSH.

If the content is empty in the SIP NOTIFY, the phone automatically triggers a new pre-configured action uri (**action uri xml sip notify**).

Example of a SIP NOTIFY with XML Content

```
NOTIFY sip:200@10.30.100.103:5060 SIP/2.0

Via: SIP/2.0/UDP 10.30.100.103:5060;branch=z9hG4bK7bbc1fac;rport

From: <sip:201@10.30.100.103:5060>;tag=81be2861f3

To: Jacky200 <sip:200@10.30.100.103:5060>

Contact: <sip:201@10.30.100.103>

Call-ID: 59638f5d95c9d301

CSeq: 4 NOTIFY
```

```
Max-Forwards: 70

Event: aastra-xml

Content-Type: application/xml

Content-Length: 115

<AastraIPPhoneExecute><ExecuteItem
URI="http://10.30.100.39/XMLtests/SampleTextScreen.xml"/></Aastra
IPPhoneExecute>
```

When the phone receives the SIP NOTIFY, the XML content is processed as any XML object. In the above example, the phone calls http://10.30.100.39/XMLtests/SampleTextScreen.xml after reception of the SIP NOTIFY.

Note: The phone supports all the current XML objects with all the existing limitations. For example if an AastraIPPhoneExecute is used, the embedded URI(s) can not be HTTPS based.

Example of a SIP NOTIFY without XML Content

```
NOTIFY sip:200@10.30.100.103:5060 SIP/2.0

Via: SIP/2.0/UDP 10.30.100.103:5060;branch=z9hG4bK7bbc1fac;rport

From: <sip:201@10.30.100.103:5060>;tag=81be2861f3

To: Jacky200 <sip:200@10.30.100.103:5060>

Contact: <sip:201@10.30.100.103>

Call-ID: 59638f5d95c9d301

CSeq: 4 NOTIFY

Max-Forwards: 70

Event: aastra-xml

Content-Type: application/xml

Content-Length: 0
```

When the phone receives the SIP NOTIFY, it will trigger the **action uri xml sip notify** parameter, if it has been previously configured using the configuration files or the Mitel Web UI. If the **action uri xml sip notify** parameter is not configured, the phone does not do anything.

On the phone side, a System Administrator can enable or disable this SIP NOTIFY feature using the configuration files or the phone Web UI.

Also to ensure that the SIP NOTIFY is coming from a trusted source, it is recommended that you enable the Whitelist feature (Whitelist Proxy parameter) on the IP phone. If enabled, and the phone receives a SIP NOTIFY from a server that is NOT on the whitelist, the phone rejects the message.

Enabling/Disabling XML SIP NOTIFY using the Configuration Files

To enable/disable the SIP NOTIFY event, you can set the following parameter in the configuration files:

- sip xml notify event

If the content is missing in the SIP NOTIFY message received by the phone, the phone automatically uses the value you specify for the following parameter:

- action uri xml sip notify

CONFIGURATION FILES

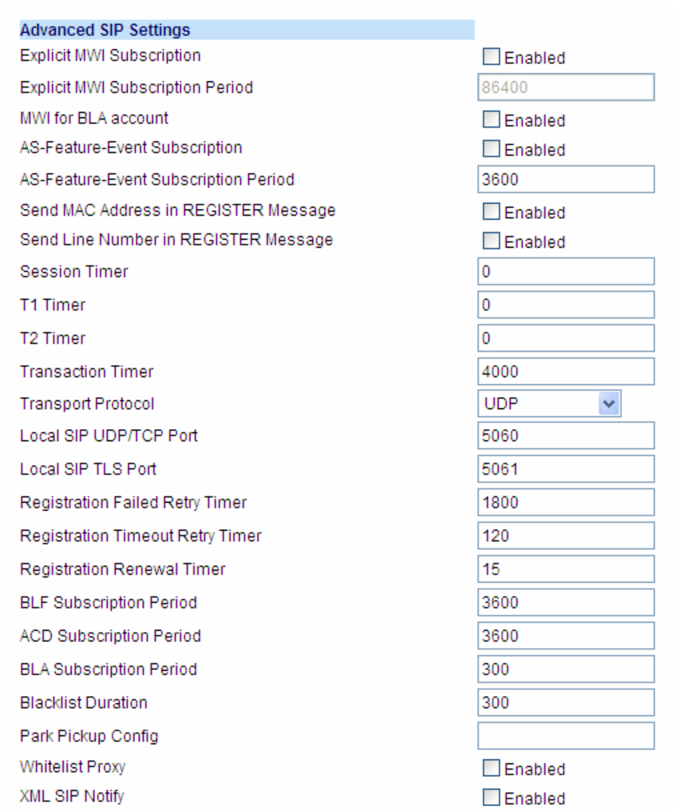
For the specific parameter you can set in the configuration files, see Appendix A, the section, "Polling Action URI Settings" on page A-194.

Enabling/Disabling XML SIP NOTIFY Using the Mitel Web UI

Use the following procedure to enable/disable the XML SIP NOTIFY feature in the Mitel Web UI.

MITEL WEB UI

1. Click on **Advanced Settings->Global SIP->Advanced SIP Settings**.



2. The “**XML SIP Notify**" field is disabled by default. To enable this field, check the box. This field enables or disables the phone to accept or reject an aastra-xml SIP NOTIFY message.

> **Note:** To ensure the SIP NOTIFY is coming from a trusted source, it is recommended that you enable the Whitelist feature (**Whitelist Proxy** parameter) on the IP phone. If enabled, and the phone receives a SIP NOTIFY from a server that is NOT on the whitelist (i.e. untrusted server), the phone rejects the message.

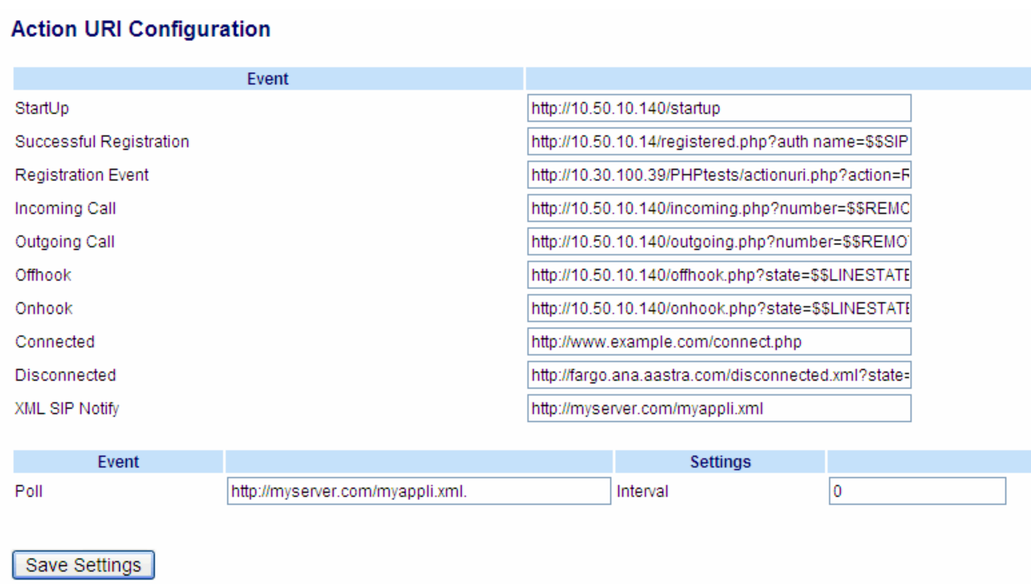
3. Click **Save Settings** to save your changes.

Configuring XML SIP NOTIFY using the Mitel Web UI if an Empty SIP NOTIFY Message Received by the Phone

Use the following procedure in the Mitel Web UI to configure the XML SIP NOTIFY parameter when the phone receives an empty SIP NOTIFY message.

MITEL WEB UI

1. If the content is missing in the SIP NOTIFY message received by the phone, the phone automatically uses the value you specify for the Action URI **XML SIP Notify** parameter at the path *Advanced Settings->Action URI*.
Click on **Advanced Settings->Action URI.**



2. Specify a URI to be called when an empty XML SIP NOTIFY is received by the phone.
For example:
http://myserver.com/myappli.xml

> **Note:** The **sip xml notify event** parameter at the path *Advanced Settings->Global SIP->Advanced SIP Settings* must be enabled.

3. Click **Save Settings** to save your changes.

XML SOFTKEY URI

In addition to specifying variables for the Action URIs, you can also specify variables in the XML softkey URIs that are bound when the key is pressed. These variables are the same as those used in the Action URIs.

When an administrator enters an XML softkey URI either via the Mitel Web UI or the configuration files, they can specify the following variables:

- $$SIPUSERNAME$$
- $$SIPAUTHNAME$$
- $$PROXYURL$$
- $$LINESTATE$$
- $$LOCALIP$$
- $$REMOTENUMBER$$
- $$DISPLAYNAME$$
- $$SIPUSERNAME$$
- $$INCOMINGNAME$$
- $$CALLDURATION$$
- $$CALLDIRECTION$$

Note: For a description of each variable in the above list, see “Variable Descriptions” on page 5-327

When the softkey is pressed, if the phone finds a URI configured with variables (in the form $$VARIABLENAME$$), they are replaced with the value of the appropriate variable. After all of the variables are bound, the softkey executes a GET on the URI.

Example

For example, if the administrator specifies an XML softkey with the value:

```
http://10.50.10.140/script.pl?name=$$SIPUSERNAME$$
```

This softkey executes a GET on:

```
http://10.50.10.140/script.pl?name=42512
```

assuming that the sip username of the specific line is 42512.

You can configure the XML softkey URI variables via the configuration files or the Mitel Web UI.

Configuring XML Softkey URIs

Use the following procedures to configure XML Softkey URIs using the configuration files or the Mitel Web UI.

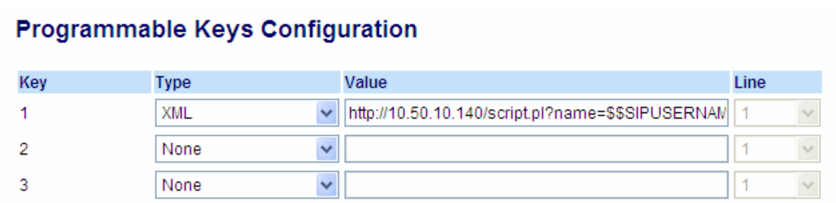
CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section,"Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters" on page A-248.

MITEL WEB UI

For the 6863i/6865i/6905/6910:

1. Click on **Operation->Programmable Keys.**



2. Select an available key.
3. In the "**Type**" field, select **XML** from the list box.
4. In the "**Value**" field, enter the URI that the phone performs a GET on when the key is pressed. For example:
http://10.50.10.140/script.pl?name=$$SIPUSERNAME$$

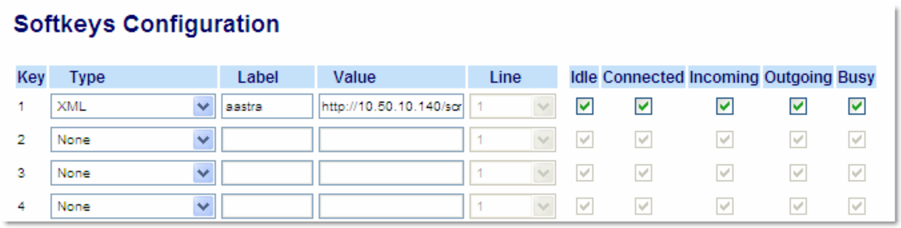
Note: You can use the following variables in the URI:

- $$SIPUSERNAME$$
- $$SIPAUTHNAME$$
- $$PROXYURL$$
- $$LINESTATE$$
- $$LOCALIP$$
- $$REMOTENUMBER$$
- $$DISPLAYNAME$$
- $$SIPUSERNAME$$
- $$INCOMINGNAME$$
- $$CALLDURATION$$
- $$CALLDIRECTION$$

5. Click **Save Settings** to save your changes.

For the 6867i/6869i/6873i:

1. Click on **Operation->Softkeys and XML**.



2. Select a key.
3. In the "**Type**" field, select **XML** from the list box.
4. In the "**Label**" field, enter a label that displays on the IP phone for the XML softkey. For example, "**mitel**".
5. In the "**Value**" field, enter the URI that the phone performs a GET on when the key is pressed. For example:
   http://10.50.10.140/script.pl?name=$$SIPUSERNAME$$

> **Note:** You can use the following variables in the URI:
> - $$SIPUSERNAME$$
> - $$SIPAUTHNAME$$
> - $$PROXYURL$$
> - $$LINESTATE$$
> - $$LOCALIP$$
> - $$REMOTENUMBER$$
> - $$DISPLAYNAME$$
> - $$SIPUSERNAME$$
> - $$INCOMINGNAME$$
> - $$CALLDURATION$$
> - $$CALLDIRECTION$$

6. Click **Save Settings** to save your changes.

XML KEY REDIRECTION

The IP phones allow the redirecting of phone-based hard keys to XML scripts. This allows the server to provide the phone with Redial, Transfer (Xfer), Conference (Conf), Intercom (Icom), and Directory key features and the Voicemail option feature, rather then accessing them from the phone-side. This feature allows you to access the redirected keys and voicemail option from the server using the IP Phone’s Services Menu. By default, the server-side keys function the same as the phone-side key features.

When configured, the configuration parameter "keyboard script" launches the XML app instead of the local directory.

The following table identifies the phone states that apply to each key redirection.

HARD KEYS/OPTIONS	REDIRECTS IN
Conference (Conf)	the connected state
Transfer (Xfer)	the connected and dialing states
Redial	all states
Intercom (Icom)	all states
Voicemail	all states

Notes:

1. Key remapping takes precedence over redirecting.
2. Disabling the redial, conference, or transfer features on the phone also disables the redirection of these keys

The following URI configuration parameters control the redirection of the keys and the voicemail option:

- redial script
- xfer script
- conf script
- icom script
- directory script
- voicemail script

An Administrator can configure the XML key, redirection URI parameters using the configuration files only.

Configuring XML Redirection of the Redial, Xfer, Conf, and Icom Keys, and the Voicemail Option

Use the following procedure to configure XML redirection of the Redial, Xfer, Conf, and Icom keys, and the Voicemail option.

CONFIGURATION FILES

For the specific parameters you can set in the configuration files, see Appendix A, the section, "XML Key Redirection Settings (for Redial, Xfer, Conf, Icom, Voicemail)" on page A-317.

OPTIONS KEY REDIRECTION

The IP phones allow the redirecting of the Options Key to an XML script. This allows the server to provide the phone with available options, rather then accessing them from the phone-side. You access the Options Key XML script by pressing the Options Key. You can still access the Options Menu from the phone-side by pressing and holding the Options key to display the phone-side Options Menu.

The following URI configuration parameter controls the redirection of the Options Key:

- options script

Notes:

1. If no Options URI script is configured, the local Options Menu on the phone displays as normal.
2. If you configure password access to the Options Menu, this password is required when accessing the local Option Menu, but is not required for the Options Key redirection feature.
3. Pressing the Options Menu for redirection from the server does not interfere with normal operations of the phone (for example, pressing the options menu when on a call does not affect the call).
4. If the phone is locked, you must unlock the phone before accessing the Options Menu redirect feature. After pressing the Options Key, the phone displays a screen that allows you to unlock the phone before continuing.

An Administrator can configure the XML Options Key, redirection URI parameter using the configuration files only.

Configuring XML Redirection of the Options Key

Use the following procedure to configure XML redirection of the Options key.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "Options Key Redirection Setting" on page A-319.

XML APPLICATIONS AND OFF-HOOK INTERACTION

A feature on the IP phone allows you to specify whether the phone is prevented from going into the off-hook/dialing state when the handset is off-hook and the call ends.

By default, the phone behaves as follows:

You are in a call using the handset and the phone displays an XML application. The far-end terminates the call, and a new XML application gets pushed/pulled onto the display. Since the handset is off-hook and in idle mode, the "offhook idle timer" starts. When this timer expires, the phone applies dial tone and moves to the off-hook/dialing state, which then destroys the XML application that was being displayed.

With the "off-hook interaction" feature you can set an "**auto offhook**" parameter that determines whether or not the phone is prevented from entering the off-hook/dialing state, if the handset is off-hook and the call ends.

An Administrator can enable (allow phone to enter the off-hook dialing state) or disable (prevent the phone from entering the off-hook dialing state) using the "**auto offhook**" parameter in the configuration files only.

Configuring the Off-Hook Interaction Feature

Use the following procedure to configure the XML application and off-hook interaction feature.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "Off-Hook and XML Application Interaction Setting" on page A-319.

XML URI FOR KEY PRESS SIMULATION

The Phones provide a feature that allow an XML Developer or Administrator to define XML Key URIs that can send key press events to the phone, just as if the physical hard key, softkey, or programmable key were pressed on the phone.

For more information about this feature, see Chapter 6, the section, "XML URI for Key Press Simulation" on page 6-45.

XML OVERRIDE FOR A LOCKED PHONE

The IP phones have a feature that allows a locked phone to be overridden when an XML application is sent to the phone. This feature also allows you to still use any softkeys/programmable key/Extension Module Keys applicable to the XML application even though the phone is locked. However, any keys NOT associated with the XML application cannot be used when the phone is locked.

Also, XML Get Requests override the locked feature on the phone so that any softkey pressed by the user that initiates a Get Request continues to get sent.

To allow the overriding of the locked phone for XML applications, the System Administrator must enter the following parameter in the configuration files:

- xml lock override

CONFIGURING XML OVERRIDE FOR A LOCKED PHONE USING THE CONFIGURATION FILES

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "XML Override for a Locked Phone Setting" on page A-320.

Note: A System Administrator can also lock and unlock a remote phone using the "**lock**" and "**unlock**" commands with the **AastraIPPhoneExecute** object in an XML application. For more information about this feature, contact Mitel Customer Support regarding the ***XML Development Guide***.

CONFIGURABLE INDICATION OF TERMINATED CALLS

An Administrator can configure a parameter called, "**far-end disconnect timer**" which allows you to enable or disable whether or not the near-end phone displays a disconnected screen with a "Call Terminated" message when the far-end hangs up. An audible busy signal is also heard on the phone. If enabled with a maximum time interval value, this parameter also specifies the interval of time that the busy signal is audible.

You can enable/disable this new parameter using the configuration files only.

The following table identifies when a call terminated screen displays on the phone for different scenarios.

IF	THEN
1 line active and far-end disconnects,	the line in focus: • displays disconnected screen. • plays busy tone. • displays "Call Terminated" message on the screen. the line not in focus: • plays busy tone.
2 or more lines active, and far-end disconnects,	the line in focus: • displays disconnected screen. • plays busy tone. • displays "Call Terminated" message on the screen for 5 seconds. When 5 second times out: • - the busy tone stops • - the disconnected screen disappears.
2 or more lines active, and a line NOT in focus is disconnected by the far-end,	• no busy tone plays • no disconnected screen displays • no "Call Terminated" message displays
An incoming call comes in on the line in focus that has a disconnected screen displaying,	• the line in focus with no calls on hold: • - displays a ringing screen • the line in focus WITH calls on hold: • - flashes its Line LED
An incoming call comes in on another line (NOT in focus), and the disconnected screen is displaying on the line in focus,	• the disconnected screen no longer displays on the line in focus.
A phone application is NOT in focus,	• busy tone plays • no disconnected screen displays • When the phone application in focus on screen stops: • - busy tone plays • - disconnected screen displays

Note: This “indication of terminated calls” feature does not affect parked calls on the phone or the conference call feature.

CONFIGURING INDICATION OF TERMINATED CALLS

You can enable or disable whether or not the phone displays an indication of a terminated call using the parameter, “**far-end disconnect timer**.” This parameter also specifies the maximum time interval that the busy tone is audible on the phone. You can configure the indication of terminated calls using the configuration files only.

Use the following procedure to configure this feature.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Terminated Calls Indicator” on page A-237.

Handling Call Termination Screens on the Phone UI

The following procedure describes how to handle the call terminated screens on your phone.

IP PHONE UI

1. Press the Goodbye key.
   The busy tone stops and the call terminated screen no longer displays.
   or
   Select any Line key.
   The busy tone stops and the call terminated screen no longer displays.
   A dial screen displays.

CENTRALIZED CONFERENCING (FOR SYLANTRO AND BROAD-SOFT SERVERS)

The IP phones include support for centralized conferencing (Ad-Hoc conferencing) for Sylantro and BroadSoft servers. This feature provides centralized conferencing on the SIP server (versus localized, on the phone) and allows IP phone users to do these tasks:

- Conference two active calls together into a conference call.
- When on an active conference call, invite another party into the call.
- Create simultaneous conference calls on the same IP phone (Sylantro servers only). For example, the IP phone user at extension 2005 could create these two conferences, and put one conference on hold while conversing with the other party:
  - Line 1: conference together extensions 2005, 2010, and 2020.
  - Line 2: conference together extensions 2005, 2011 and 2021.

When an IP phone user is connected to multiple conference calls, some outbound proxies have maximum call “hold” time set from 30-90 seconds. After this time, the call that is on hold is disconnected.

- Disconnect from an active conference call while allowing the other callers to remain connected.
- Ability to create N-way conference.
- Join two active calls together into a conference call.
- Incoming or outgoing active call can join any of the existing conferences.

If the administrator does not configure centralized conferencing, then the IP phone uses localized conferencing by default.

Note: When you configure centralized conferencing globally for an IP Phone, the global settings apply to all lines. Although, for the global setting to work on soft lines, the user must configure the lines with the applicable phone number.

An Administrator can configure centralized conferencing on a global or per-line basis using the configuration files or the Mitel Web UI.

To use the centralized conferencing after it is enabled, see your <Model-Specific> ***SIP Phone User Guide***.

CONFIGURING CENTRALIZED CONFERENCING USING THE CONFIGURATION FILES

You use the following parameters to configure centralized conferencing in the configuration files:

Global Parameter

- sip centralized conf

Per-Line Parameter

- sip lineN centralized conf

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Centralized Conferencing Settings” on page A-110.

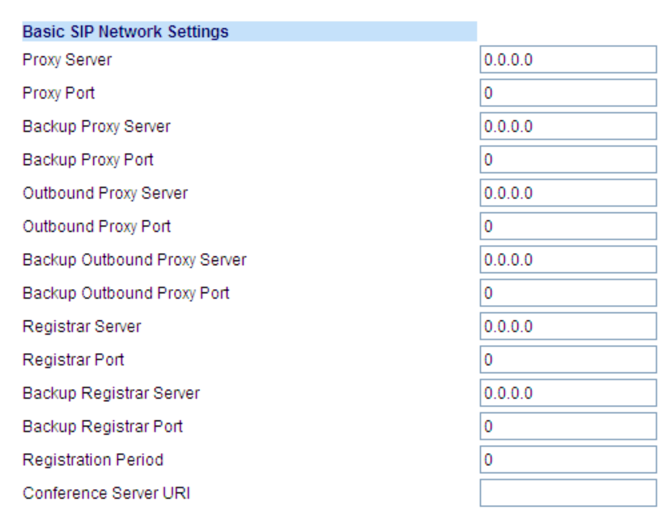
CONFIGURING CENTRALIZED CONFERENCING USING THE MITEL WEB UI

Use the following procedure to configure centralized conferencing using the Mitel Web UI.

MITEL WEB UI

Global Configuration

1. Click on **Advanced Settings->Global SIP Settings->Basic SIP Network Settings.**



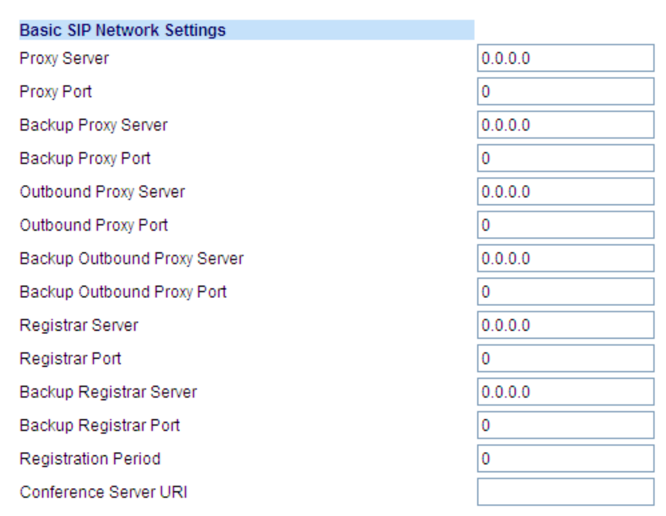
2. In the "**Conference Server URI**" field, do one of the following actions:

- To disable centralized conferencing on the IP phone, leave this field empty (blank).
- To enable SIP centralized conferencing on the IP phone, do one of the following actions:
  - If you have specified a proxy server/registrar server, then to reach the media server via the proxy server, set this field to one of the following:
    conf (Sylantro server), or
    Conference (BroadSoft server)
    By setting this field to **conf** or **Conference**, you specify conf@<proxy_server _address>: <proxy_port>. For example, if the proxy server address is 206.229.26.60 and the port used is 10060, then by setting this parameter to **conf**, you are specifying the following: conf@206.229.26.60:10060.
  - To reach the media server using a different address/port than that specified by the proxy, set this field to the following:
    conf@<media_server _address>: <media_port>

3. Click **Save Settings** to save your changes.

Per-Line Configuration

1. Click on **Advanced Settings->Line <#>->Basic SIP Network Settings**



2. In the "**Conference Server URI**" field, do one of the following actions:
   - To disable centralized conferencing on this line, leave this field empty (blank).
   - To enable SIP centralized conferencing on this line, do one of the following actions:
     - If you have specified a proxy server/registrar server, then to reach the media server via the proxy server, set this field to one of the following:
       conf (Sylantro server), or
       Conference (BroadSoft server)
       By setting this field to **conf** or **Conference**, you specify conf@<proxy_server _address>: <proxy_port>.
     - To reach the media server using a different address/port than that specified by the proxy, set this field to the following:
       conf@<media_server _address>: <media_port>
3. Click **Save Settings** to save your changes.

CUSTOM AD-HOC CONFERENCE

Previously, the phone will wait for server response prior to completing the ad-hoc and centralized conference feature. This results in an interoperability issue with certain call managers, such as Genband. Now the phone no longer waits for server response before referring the call to the conference host when the "**custom adhoc conference**" parameter is enabled.

CONFIGURING THE “CUSTOM AD-HOC CONFERENCE” FEATURE USING THE CONFIGURATION FILES

You use the following parameters to configure the “Custom AD- Hoc Conference” feature in the configuration files:

- custom adhoc conference

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, “Custom Ad-Hoc Conference” on page A-112.

“SIP JOIN” FEATURE FOR 3-WAY CONFERENCE

The IP Phones support a feature referenced in RFC 3911, which allows an additional caller to join an active call between two parties if the caller knows the dialog information. This feature begins a conference using a join header as described in RFC 3911.

The “SIP Join“ feature provides the following:

- Security via the whitelist (which is a feature that already exists on the phone).
- Initiates an offhook action uri when it is answered.
- Initiates an onhook action uri at call termination.
- Creates a caller list entry.

This feature is disabled by default. You can enable the “SIP Join” feature by setting the “sip join support” parameter in the configuration files.

LIMITATIONS OF THE “SIP JOIN” FEATURE

The following are limitations of the “SIP Join” feature:

- Not applicable to a conference call already in progress.
- Not applicable to a phone mixing RTP.
- Allows secondary parties to join calls if they can determine the dialog parameters. In order to provide security, it is recommended that the Administrator configure the SIP whitelist.
- Not applicable while the active call between two parties is in the early dialog state.

CONFIGURING THE "SIP JOIN" FEATURE USING THE CONFIGURATION FILES

You use the following parameters to configure the "SIP Join feature in the configuration files:

sip join support

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "SIP Join Feature for 3-Way Conference" on page A-112.

CONFERENCE/TRANSFER SUPPORT FOR LIVE DIAL MODE

By default, when users are initiating a conference call or transfer, they will not hear a dial tone before dialing begins (pre-dial mode). The phone does not automatically dial out the number until the user presses the "Conf" or "Transfer" key. This allows the users to make changes to the dialing number before initiating the call.

Administrators can enable live dial mode in a conference call or transfer scenario by configuring the "**confxfer live dial**" parameter. Two live dial mode options are available:

- **Live dial mode with dial plan matching**: When a user initiates a conference call or transfer, they hear a dial tone before dialing begins. The phone automatically dials out if the number matches the local dial plan or if it reaches the set digit timeout.
- **Live dial mode without dial plan matching**: When a user initiates a conference call or transfer, they hear a dial tone before dialing begins. The phone does not match the number to the local dial plan and automatically dials out only if it reaches the set digit timeout (or if the number matches a number defined in the emergency dial plan).

In the default pre-dial mode, users are able to edit the destination number prior to dialing, whereas in live dial mode they are not able to; however, the "Dial" and "Cancel" softkeys are provided while the user inputs the number.

Note: In a transfer scenario, when the "**confxfer live dial**" parameter is defined as "**2**", if the number of the transfer recipient is entered and the "Xfer" key is pressed before the set digit time out, the phone will attempt a blind transfer.

CONFIGURING CONFERENCE/TRANSFER IN LIVE DIAL MODE

You use the following parameters to configure conference/transfer feature in live dial mode:

- confxfer live dial

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "Conference/Transfer in Live Dial Mode" on page A-113.

AUTHENTICATION SUPPORT FOR HTTP/HTTPS DOWNLOAD METHODS, USED WITH BROADSOFT CLIENT MANAGEMENT SYSTEM (CMS)

The SIP phones support HTTP/HTTPS digest authentication as defined in RFC 2617. (The HTTP client supports digest authentication; the HTTP server does not; the HTTP server supports basic authentication). This feature allows the phones to interoperate with BroadSoft's CMS phone configuration tool.

Using the configuration files, you can enable/disable the following parameter to display a LOG IN softkey which allows the HTTP/HTTPS server to perform digest authentication:

- **http digest force login** - specifies whether or not to display the LOG IN softkey on the IP Phone UI screen. Valid values are 0 (disabled) or 1 (enabled). Default is 0 (disabled).

If the "**http digest force login**" parameter is set to **1** (enabled), after the phone boots, the LOG IN softkey displays on the phone's LCD. On pressing this softkey, the screen displays the following fields:

- Username (by default "aastra")
- Password (by default "aastra")

You can enter the field values in two ways:

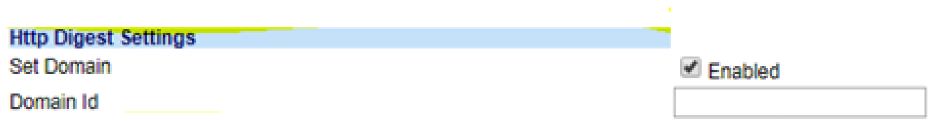
- Using the configuration files, you can change the default values for the following parameters:
  - **http digest username -** specifies the username to use for HTTP/HTTPS digest authentication.
  - **http digest password** - specifies the password to use for HTTP/HTTPS digest authentication.
- By enabling the "**http digest force login**" parameter (setting to 1) - the phone displays the LOG IN key so the user can enter the default username/password via the IP Phone UI.

An Administrator can configure the following domain fields from the Mitel Web UI:

- Set Domain - A check box to indicate whether Domain is enabled or disabled (by default disabled)
- Domain ID

Use the following procedure to configure domain fields using the Mitel Web UI.

1. Click on **Basic Settings**->**Preferences**->**Http Digest Settings**.
2. In the **Set Domain** field, enable or disable the check box.
3. In the **Domain ID** text box, enter the domain for HTTP/HTTPS digest authentication.
4. Click **Save Settings** to save your changes.



Alternatively, the domain field values can be set using the following parameters in the configuration files:

- **http digest domain enable** - Check box which specifies whether Domain is enabled or disabled.
- **http digest domain**- specifies the domain for HTTP/HTTPS digest authentication.

After user enters the configured values, it is sent to the HTTP/HTTPS server for digest authentication by the server.

CONFIGURING BROADSOFT CMS SUPPORT VIA THE CONFIGURATION FILES

Configure BroadSoft CMS support on the IP Phone using the following parameters in the configuration files:

- http digest force login
- http digest username
- http digest password
- http digest domain enable
- http digest domain

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section, "HTTP/HTTPS Authentication Support for BroadSoft CMS" on page A-113.

USING THE IP PHONE WHEN BROADSOFT CMS IS ENABLED

If you enable the HTTP/HTTPS digest authentication feature, the phone behaves as follows with the BroadSoft CMS tool:

1. Factory default the phone.
2. Configure the HTTP or HTTPS server (specify the HTTP or HTTPS server, path, and port).
3. Restart the phone.
   The first time the phone reboots, the phone is challenged by the server. The phone sends the default username of "**aastra**" and the default password of "**aastra**" to the server.By default, "http digest domain enable: 0" i.e. disabled and domain is empty.
   The server sends the default profile to the phone. This profile includes the information "**http digest force login: 1**". When the phone receives the profile, it displays the "**Log In**" key on the IP Phone's idle screen.

4. Press the "**Log In**" key to display the username, password and domain screen.

   Note: On the 6867i, 6869i, and 6873i you use the **Log In** softkey to log in. On 6863i and 6865i, you press the **right arrow** key to log in.

5. Enter a username in the "Username" field (up to 40 characters) and a password in the "Password" field (up to 20 characters). If Domain checkbox is disabled, then leave the Domain field empty. If Domain checkbox is enabled, then enter in the "Domain" field.

   Note: The "**Username"**, "**Password"** and "**Domain**" fields accept special characters, such as, @, #, %, =, _, etc.

6. After entering the username, password and domain, press **Submit**.
   The phone attempts to authenticate with the server. If successful, the phone reboots and loads the user configuration. If unsuccessful, then the phone displays "*Authentication Failed*".

   1. If Domain checkbox is disabled, then the authentication is based on Username and Password only.
   2. If Domain checkbox is enabled, then the authentication is based on Username, Password and Domain. If "http digest domain enable" is set to 1, the server challenges a "HTTP GET" request from the phone. The phone sends GET request to the server with a Authorization header with Username in the format <Username><Domain>. For example, if "Username" is 4005 and "Domain" is @8280001.com, the phone sends 4005@8280001.com for authorization.

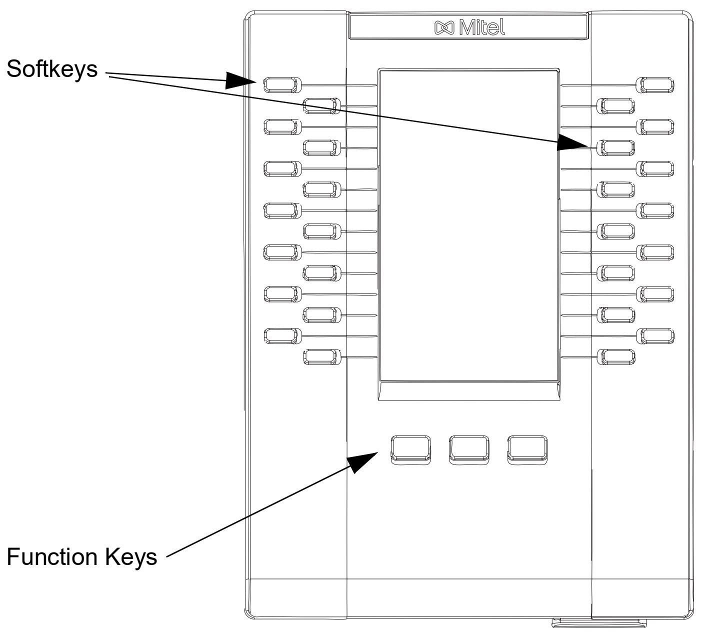
CUSTOMIZING THE DISPLAY COLUMNS ON THE M685I/M695 EXPANSION MODULE

The M685i/M695 Expansion Module screen displays softkeys in column format. The function keys on the bottom left of the Module allow you to display 3 full screens of softkeys. Each screen consists of 2 columns with the following default headings on each page:

- Page 1: "List 1" and "List 2"
- Page 2: "List 3" and "List 4"
- Page 3: "List 5" and "List 6"

Note: Headings for the M685i/M695 are only viewable on the *Operation > Expansion Module <N>* page of the Web UI.

M685i/M695 Expansion Module Keys



To use the M685i/M695, press the function key for the page you want to display to the LCD (page 1, page2, or page 3), and press the applicable softkey.

You can customize the headings on each M685i/M695 Expansion Module screen using the configuration files by defining the following parameters:

Expansion Module 1 (3 pages)

- expmod1page1left
- expmod1page1right
- expmod1page2left
- expmod1page2right

- expmod1page3left
- expmod1page3right

Expansion Module 2 (3 pages)

- expmod2page1left
- expmod2page1right
- expmod2page2left
- expmod2page2right
- expmod2page3left
- expmod2page3right

Expansion Module 3 (3 pages)

- expmod3page1left
- expmod3page1right
- expmod3page2left
- expmod3page2right
- expmod3page3left
- expmod3page3right

The following is an example of configuring Expansion Module 1 column headings.

```
expmod1page1left: Personnel Ext

expmod1page1right: Operations Ext

expmod1page2left: Marketing Ext

expmod1page2right: Logistics Ext

expmod1page3left: Engineering Ext

expmod1page3right: Shipping Ext
```

CUSTOMIZING THE M685I/M695 EXPANSION MODULE COLUMN DISPLAY

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see Appendix A, the section,"Customizing M685i/M695 Expansion Module Column Display" on page A-310.

PERSONAL MODE

Note: Applicable to the 6970 IP Phone only.

The 6970 IP Conference Phone supports a security feature to automatically log Hotdesk users out after every call when a timeout expires. This prevents user forgetting to log out after using the 6970 IP Conference Phone in a public room. If the 6970 IP Conference Phone is used in a secure location, this feature can be disabled via configuring the Personal mode parameter.

Note: The Personal mode is disabled by default.

CONFIGURING THE PERSONAL MODE USING THE CONFIGURATION FILES

Use the following information to set the Personal mode on the 6970 IP Phone.

CONFIGURATION FILES

You can enable or disable the Personal mode using the configuration file applicable to the conference phone. For example:

```
personal mode: 1
```

For specific parameters you can set in the configuration files, see Appendix A, the section, "Personal Mode Settings" on page A-115.

Chapter 6

CONFIGURING ADVANCED OPERATIONAL FEATURES

ABOUT THIS CHAPTER

The IP phones have advanced operational features you can configure using the configuration files and/or the Mitel Web UI. This chapter describes each of these features and provides procedures for configuring each feature.

TOPICS

This chapter covers the following topics:

ADVANCED OPERATIONAL FEATURES

DESCRIPTION

This section provides the following information about advanced features of the IP phones:

FEATURE	DESCRIPTION
TR-069 Support	The IP Phones support the Technical Report (TR) 069 Protocol, a Protocol that provides the communication between Customer-Premises Equipment (CPE) (like the IP Phones) and Auto Configuration Servers (ACS) over DSL/broadband connections.
User Agent Computer Supported Telecommunications Applications (uaCSTA) Support	uaCSTA is supported by the 6800 series SIP phones. uaCSTA refers to the mechanism of transporting CSTA XML messages over a SIP session allowing for compatibility with SIP phone user agents.
MAC Address/Line Number in REGISTER Messages	Allows you to enable or disable the sending of the MAC address and line number from the IP phone to the call server, in a REGISTER message.
SIP Message Sequence for Blind Transfer	Allows you to enable or disable the phone to use the Blind Transfer method available in software prior to release 1.4.
Update Caller ID During a Call	Allows you to enable or disable the updating of the Caller ID information during a call.
Boot Sequence Recovery Mode	Allows you to enable or disable Web recovery mode and set the maximum boot count on the IP phone.
Auto-discovery Using mDNS	The IP phones automatically perform an auto-discovery of all servers on a network using mDNS. When the IP phone discovers a TFTP server, it is automatically configured by that TFTP server.
As-Feature-Event Subscription	Allows you to enable or disable a specific line on the phone with the BroadSoft's server-side DND, CFWD, or ACD features.
Blacklist Duration	Allows you to specifies the length of time, in seconds, that a failed server remains on the server blacklist. The IP phone avoids sending a SIP message to a failed server (if another server is available) for this amount of time.
Whitelist Proxy	Allows you to configure the phone to either accept or reject call requests from a trusted proxy server.
Transport Layer Security (TLS)	Allows you to enable or disable the use of Persistent Transport Layer Security (TLS). Persistent TLS sets up the connection to the server once and re-uses that connection for all calls from the phone. The setup connection for Persistent TLS is established during the registration of the phone. If the phones are set to use Persistent TLS, and a call is made from the phone, this call and all subsequent calls use the same authenticated connection. This significantly reduces the delay time when placing a call.

FEATURE	DESCRIPTION
802.1x Configuration	Allows you to enable or disable the 802.1x Protocol support on the IP Phones.
Symmetric UDP Signaling	Allows you to enable or disable the phone to use port 5060 to send SIP UDP messages.
Symmetric TLS Signaling	Allows you to enable or disable the phone to use port 5061 to send SIP TLS messages.
Removing UserAgent and Server SIP Headers	Allows you to enable or disable the addition of the User-Agent and Server SIP headers in the SIP stack.
GRUU and sip.instance Support	The IP phones provide GRUU support using draft-ietf-sip-gruu-15. A sip.instance is added to all non-GRUU contacts.
Multi-Stage Digit Collection (Billing Codes) Support (for Sylantro Servers)	IP Phones support Sylantro Server features, like mandatory and optional billing codes that require the application server to notify the phone to collect more digits before completing the call. The IP phone is able to collect digits in two stages to support the billing code feature.
Configurable DNS Queries	Allows you to specify the Domain Name Service (DNS) query method to use when the phone performs a DNS lookup.
Ignore Out of Sequence Errors	Allows you to configure the phone to ignore CSeq number errors on all SIP dialogs on the phone.
“Early-Only” Parameter in Replaces Header RFC3891	The phones support the “early-only” parameter in the “Replaces” header as referenced in RFC3891.
Switching Between Early Media and Local Ringing	The phones support switching between early media and local ring tone.
Configurable Codec Negotiation Behavior	Allows you to enable or disable the microphone during early media.
Configurable Codec Negotiation Behavior	Allows Administrators to change the phone’s codec negotiation behavior so that the phone will indicate only one preferred codec in the SDP when replying to an SDP offer (as per 3GPP TS 24.229).
“Call-Info” Header to 200ok Responses for Shared Call Appearance (SCA) Lines	A “Call-Info” header is included in the 200ok response to an INVITE, RE-INVITE, and UPDATE messages for SCA lines. No configuration is required for this feature.
Reason Header Field in SIP Message	The IP Phones support the receiving of the Reason Header Field in a SIP CANCEL message, as described in RFC3326.
Configurable “Allow” and “Allow-Event” Optional Headers	On the IP Phones, an Administrator can enable or disable whether or not the optional “Allow” and “Allow-Events” headers are included in the NOTIFY message from the phone.
Configurable SIP P-Asserted Identity (PAI)	The IP Phones support a private extension to SIP for Asserted Identity within trusted networks (as defined in RFC 3325).
Configurable Route Header in SIP Packet	The IP Phones support a parameter that enables or disables the addition of the Route header in a SIP packet.
Configurable Compact SIP Header	The phones provide a feature that allows an Administrator to shorten the length of a SIP packet by using the compact form. This feature is in accordance with Compact SIP Headers defined in RFC 3261.

FEATURE	DESCRIPTION
Reject INV or BYE when Unsupported Value in REQUIRE Header	The IP Phones support a parameter that allows you to enable or disable the rejection of an INV or BYE with a "420 Bad Extension" if the INV or BYE contains an unsupported value in the REQUIRE header.
XML URI for Key Press Simulation	The phones provide a feature that allow an XML Developer or Administrator to define XML Key URIs that can send key press events to the phone, just as if the physical hard key, softkey, or programmable key were pressed on the phone.
Domain Name System (DNS) Server Pre-caching Support	This feature allows administrators to configure the phone to download a text file which contains persistent DNS "A record" hostname to IP address mappings. In addition, support for persistent DNS "SRV records" has been added to permit SRV based high availability of services.
Configurable Transport Protocol for SIP Services and RTCP Summary Reports	The IP Phones support a parameter that allows administrators to ability to configure the transport protocols used for SIP services and RTCP summary reports.
Configurable Alphanumeric Input Order for Username Prompts	This feature allow administrators the ability to change the default behavior of the keypad input order during username prompts from uppercase letters > digit > lower case letters to digit > uppercase letters > lower case letters.
Active Voice-over-IP (VoIP) Recording	When using the IP phones with a Mitel call manager supporting voice recording and a recording system with the predefined subset of the SIP interface, administrators can configure the phones to send duplicate copies of the transmit and receive RTP or SRTP voice packets to the voice recording system.
BroadSoft Xsi Features	Interoperability support for the BroadSoft Xsi Speed Dial 8, Basic Call Log, Hide Number, Remote Office, Simultaneous Ring Personal, Call Center, and BroadSoft Anywhere services has been implemented.
Feature Re-Branding Support for BroadSoft-Based Service Providers	The 6800 series SIP phones support the configuration of a number of BroadSoft features through the native phone UI as well as the phone's Web UI. References to these features in the respective UI may contain the strings "BroadSoft", "BSFT", or "BroadWorks". This feature allows service providers the ability to replace these BroadSoft-related strings in the UI with their own custom branding names.
Interoperability Support for XMPP-Based BroadSoft UC-ONE Services	The SIP phones are interoperable with the following Extensible Messaging and Presence Protocol (XMPP)-based BroadSoft UC-ONE services and features: • Presence • Contact List • Favorites • My Status • Free Text Display • Avatar Support

FEATURE	DESCRIPTION
BroadSoft BroadWorks Executive and Assistant Services	The Executive and Assistant Services feature allows Administrators to create an inter-network relationship between Executives and Assistants allowing calls to the Executive's phone to be screened, filtered, and routed to an Assistant, whereby the Assistant can answer, divert, or push the filtered call back to the Executive.
Visitor Desk Phone Support	The Visitor Desk Phone feature allows users to log in to any VDP-configured phone and thus use that respective phone as his/her personal device for the duration of the logged in session.
Option to Enable/Disable RTCP	Allows Administrators the ability to manually enable or disable RTCP.
Configurable SIP No RTP Packet Timeout Period	Allows Administrators the ability to define a timeout period whereby if no RTP packets are received in the defined amount of time, the phone will send a BYE request, thus releasing the call and returning the home/idle screen
Option to Parse or Ignore REFER Event IDs	Allows Administrators the ability to set whether or not event IDs (i.e. Event: refer:id=xxxxx) in REFER NOTIFY event headers received by the phone should be ignored.
Remote Rebooting and Dynamic Reloading of the Configuration Files	Allows Administrators the ability to immediately reboot the phone or reload all the parameter settings in the configuration files without rebooting based upon a check sync NOTIFY message with a "reboot" variable defined.
MiCloud Telepo Music on Hold Support	Allows Administrators the ability to configure the phones to utilize music on hold functionality when using the MiCloud Telepo for Service Providers call manager.
UAC Session Refresh Support	With certain networks, a Session Refresh is required to be performed by the User Agent Client (UAC). To accommodate this, a new configuration parameter "**sip force uac session refresh**" has been introduced. When the parameter is enabled and an incoming initial INVITE with a Session-Expires header with no refresher parameter is received, the Session-Expires header and the refresher=uac parameter are added to the 200 OK response, ensuring the refresh is performed by the call initiator.
Configurable SRTP Rollover Counter (ROC) RESET Behavior	In a Secure Real-time Transport Protocol (SRTP) environment, when a re-INVITE is sent but there is no change to the media Synchronization Source (SSRC) identifier, as per RFC3711 the phone must not reset its Rollover Counter (ROC) to zero. Certain call managers do not adhere to RFC3711 and with these call managers one-way audio may be observed after a re-INVITE is sent (e.g. in a call hold/unhold scenario). To allow interoperability with these call managers that do not adhere to RFC3711 ROC processing, the "srtp loose roc" parameter has been introduced.

TR-069 SUPPORT

The IP Phones support the Technical Report (TR)-069 Protocol. This Protocol is a bi-directional HTTP based protocol that provides the communication between Customer-Premises Equipment (CPE) (like the IP Phones) and Auto Configuration Servers (ACS) over DSL/broadband connections. It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework.

Service providers can, through TR-069, use one common platform to manage (through the Internet) all of their customer premise devices, regardless of the device or manufacturer. If TR-069 is enabled on the phones, when the remote ACS boots the phones, they contact the ACS and establish the configuration automatically.

In addition to configuring the phone with TR-069, you can also do the following:

- Reboot the phone
- Reset to factory defaults
- Update the firmware of the device
- Backup/restore configuration
- Upload the log file

REFERENCE

For more information about TR-069, see the ***TR-069 Configuration Guide***.

USER AGENT COMPUTER SUPPORTED TELECOMMUNICATIONS APPLICATIONS (UACSTA) SUPPORT

uaCSTA refers to the mechanism of transporting CSTA XML messages over a SIP session allowing for compatibility with SIP phone user agents.

The 6800 series SIP phones currently support the following requests:

- RequestSystemStatus
- MonitorStart
- MonitorStop
- SystemRegister
- MakeCall
- AnswerCall
- ClearConnection
- HoldCall
- RetrieveCall
- GetSwitchingFunctionDevices
- TransferCall

- ConferenceCall
- GenerateDigits
- GetDoNotDisturb
- SetDoNotDisturb
- GetForwarding
- SetForwarding
- SnapshotDevice
- DeflectCall
- ConsultationCall

The 6800 series SIP phones currently support the following events:

- ServiceInitiated
- Originated
- Delivered
- Established
- ConnectionCleared
- Held
- Retrieved
- Conference
- Transfered
- DigitsGenerated
- OutOfService
- BackInService
- DoNotDisturb
- Forwarding
- Failed
- Diverted

Note: For detailed information and examples regarding the above requests and events, refer to "*Using CSTA for SIP Phone User Agents (uaCSTA)*" (TR/87) June 2004, ECMA International.

To enable uaCSTA support, Administrators must define the "**csta**" parameter as "1" in the configuration files as well as define the "**csta proxy**", "**csta port**", and "**csta password**" parameters. The "**csta proxy**" corresponds to the IP address or FQDN of the CTSA proxy server, the "**ctsa port**" corresponds to the CTSA proxy server's port number, and the "**ctsa password**" corresponds to the password used for authentication with the CSTA proxy server.

ENABLING UACSTA SUPPORT USING THE CONFIGURATION FILES

CONFIGURATION FILES

For specific parameters you can set in the configuration files for enabling uaCSTA support see Appendix A, the section, "uaCSTA Settings" on page 312.

MAC ADDRESS/LINE NUMBER IN REGISTER MESSAGES

The IP phones can send the MAC address and line number in the REGISTER packets making it easier for the call server when a user configures the phones via the Mitel Web UI or the IP Phone UI. The following two configurable headers send this information to the call server:

```
Aastra-Mac: <mac address>
Aastra-Line: <line number>
```

The MAC address is sent in uppercase hex numbers, for example, 00085D03C792. The line number is a number between 1 and 24.

The following parameters allow you to enable/disable the sending of MAC address and line number to the call server:

- sip send mac
- sip send line

These parameters are disabled by default. The parameters are configurable via the configuration files or the Mitel Web UI.

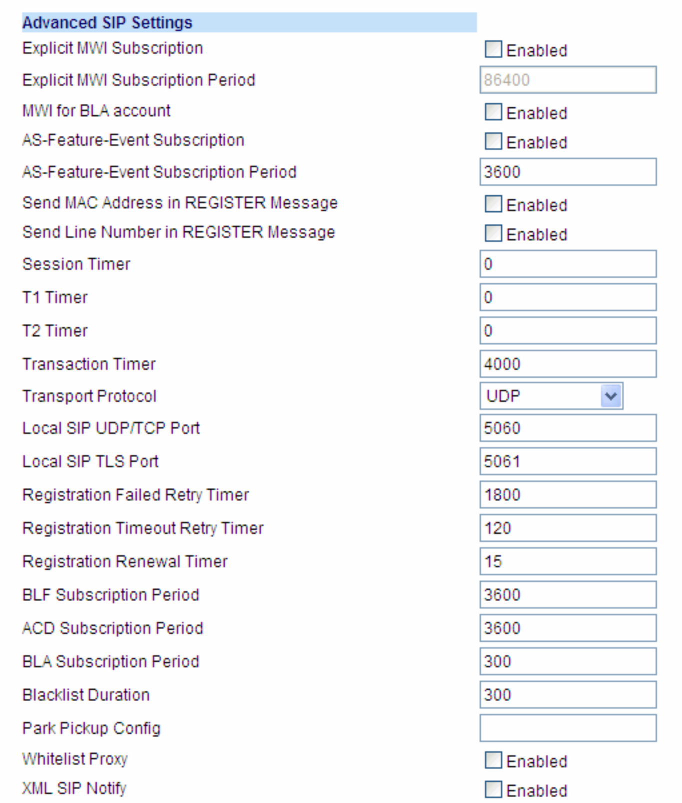
CONFIGURING THE MAC ADDRESS/LINE NUMBER IN REGISTER MESSAGE

CONFIGURATION FILES

For specific parameters you can set in the configuration files for enabling/disabling MAC address and line number, see Appendix A, the section, "Advanced Operational Parameters" on page A-312.

MITEL WEB UI

1. Click on **Advanced Settings->Global SIP->Advanced SIP Setting.**



2. Enable the "**Send MAC Address in REGISTER Message**" field by checking the check box. (Disable this field by unchecking the box).
3. Enable the "**Send Line Number in REGISTER Message**" field by checking the check box. (Disable this field by unchecking the box).
4. Click **Save Settings** to save your settings.

Note: The session prompts you to restart the IP phone to apply the configuration settings.

5. Select **Operation->Reset** and click **Restart**.

SIP MESSAGE SEQUENCE FOR BLIND TRANSFER

The SIP message sequence for Blind Transfer avoids the transfer target having two simultaneous calls. Prior to release 1.4, a CANCEL message was sent to the transfer target (if it was in a ringing state) after sending a REFER to the transferee to complete the transfer. In the 1.4 and later releases, the CANCEL is now sent before the REFER message.

The following parameter allows the system administrator to force the phone to use the Blind Transfer method available in software versions prior to 1.4:

- sip cancel after blind transfer

This parameter is configurable via the configuration files only.

CONFIGURING SIP MESSAGE SEQUENCE FOR BLIND TRANSFER

CONFIGURATION FILES

For the specific parameter you can set in the configuration files for enabling/disabling the blind transfer method, see Appendix A, the section, "Blind Transfer Setting" on page A-313.

SIP SETTINGS FOR SEMI-ATTENDED TRANSFERS

SIP MESSAGE SEQUENCE

The SIP message sequence for a Semi-Attended Transfer allows the transferor to start the transfer while the target phone is still ringing.

The following parameter supports different behaviors of a semi-attended transfer:

- sip refer-to with replaces

This parameter is configurable via the configuration files only.

The combination of this new parameter (**"sip refer-to with replaces"**) and the existing parameter (**"sip cancel after blind transfer"**) determines how the semi-attended transfer is completed. The following table shows how the old and new parameters work together:

IF	THEN
The "sip cancel after blind transfer" parameter is set to 0 and the "sip refer-to with replaces" parameter is set to 0	The phone sends CANCEL before REFER for semi-attended transfer.
The "sip cancel after blind transfer" parameter is set to 1 and the "sip refer-to with replaces" parameter is set to 0	The phone sends CANCEL after REFER for semi-attended transfer.
The "sip cancel after blind transfer" parameter is set to 0 and the "sip refer-to with replaces" parameter is set to 1	The phone sends REFER with Replaces for semi-attended transfer and NO CANCEL.
The "sip cancel after blind transfer" parameter is set to 1 and the "sip refer-to with replaces" parameter is set to 1	The phone sends REFER with Replaces for semi-attended transfer and NO CANCEL.

On the transferor phone, the REFER request will always be sent to the transferee.

IGNORING PAI HEADER FOR SEMI-ATTENDED TRANSFERS

In previous releases, when used in conjunction with the Mitel Clearspan call manager and a remote phone was defined with an overriding caller ID, semi-attended transfers to the remote phones would be sent to the destinations of the overriding caller ID and not the intended remote phones. Administrators utilizing the phones with the Mitel Clearspan platform can correct this by defining the "**sip refer-to from contact**" parameter as "**1**" (i.e. enabled) in the respective configuration files. When enabled, the phone will check the user name from the contact header received in 180 response and:

- if the contact header has user name, blind transfer the call to the user name
  or
- if there is no contact header found or the contact header has no user name, put the remote address of the original INVITE to the Refer-To header.

CONFIGURING SIP SETTINGS FOR SEMI-ATTENDED TRANSFERS

CONFIGURATION FILES

For the specific parameters you can set in the configuration files for customizing the semi-attended transfer method, see Appendix A, the section, "“Semi-Attended Transfer Settings”" on page A-313.

UPDATE CALLER ID DURING A CALL

It is possible for a proxy or call server to update the Caller ID information that displays on the phone during a call, by modifying the SIP Contact header in the re-INVITE message. The phone displays the updated name and number information contained within the Contact header.

The following parameter allows the system administrator to enable or disable this feature:

- sip update callerid

This parameter is configurable via the configuration files only.

CONFIGURING UPDATE CALLER ID DURING A CALL

CONFIGURATION FILES

For the specific parameter you can set in the configuration files for enabling/disabling the update of caller ID during a call, see Appendix A, the section, "Update Caller ID Setting" on page A-314.

SIP UNREGISTER ON BOOT

The SIP phones already support unregister on soft reboot. Enhancements are made to support SIP unregister at electrical reboot.

A new configuration parameter "**sip unregister on boot**" is introduced to enable or disable unregistering of SIP phones at boot or reboot (manual, remote or electrical).

CONFIGURE SIP UNREGISTER ON BOOT

Administrators can enable this functionality by defining the "**sip unregister on boot**" parameter as 1 in the configuration file. By default, this feature is disabled.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files for enabling/disabling the update of caller ID during a call, see Appendix A, section "SIP Unregister on Boot" on page A-314.

BOOT SEQUENCE RECOVERY MODE

You can force the IP phone into recovery mode by pressing the **1** and **#** keys during boot up when the logo displays. This feature is enabled by default on the IP phone.

You can disable this feature using the following parameter in the configuration files:

- force web recovery mode disabled

Valid values for this parameter are 0 (false) and 1 (true). Default is 0 (false).

A boot counter increments after each faulty boot. When the counter reaches a predetermined value, it forces Web recovery mode. The counter is reset to zero upon a successful boot.

The predetermined value is set using the following parameter in the configuration files:

- max boot count

A zero (0) value disables this feature. The default value is 10.

You can configure the boot sequence recovery mode parameters using the configuration files only.

Note: After the phone has been successfully recovered through the web recovery mode, the phone will fully download and upgrade to the firmware defined in the configuration files (upon reboot) or pushed through the Web UI even if the defined/pushed firmware's version is identical to the version already loaded on the phone.

Note: For **Web Recovery Mode** on 6970 IP Phone:

1. Tap **Settings > Advanced > Reset** and choose **Factory Default**.
1. Open **Recovery** mode by pressing **Directory** and **End** button during reboot.

CONFIGURING BOOT SEQUENCE RECOVERY MODE

CONFIGURATION FILES

For the specific parameters you can set in the configuration files for boot sequence recovery mode, see Appendix A, the section, "Boot Sequence Recovery Mode Settings" on page A-315.

AUTO-DISCOVERY USING MDNS

The IP phones can perform an auto-discovery of all servers on a network using mDNS. When the IP phone discovers a TFTP server, it is automatically configured by that TFTP server.

An unconfigured phone (phone right out of the box) added to a network, attempts to auto-discover a configuration server on the network without any end-user intervention. When it receives DHCP option 66 (TFTP server), it automatically gets configured by the TFTP server.

An already configured phone (either previously configured by auto-discovery or manually configured) added to a network, uses its predefined configuration to boot up.

Notes:

1. Configuration parameters received via DHCP do not constitute configuration information, with the exception of a TFTP server. Therefore, you can plug a phone into a DHCP environment, still use the auto-discovery process, and still allow the use of the TFTP server parameter to set the configuration server.
2. DHCP option 66 (TFTP server details) overrides the mDNS phase of the auto-discovery. Therefore, the DHCP option takes priority and the remaining process of auto-discovery continues.
3. As the phone performs auto-discovery, all servers in the network (including the TFTP server), display in the phone window. However, only the server configured for TFTP automatically configures the phone.

AS-FEATURE-EVENT SUBSCRIPTION

The IP phones support server-side Do Not Disturb (DND), Call Forward (CFWD), and Automatic Call Distribution (ACD) feature events. This feature is called “as-feature-event” and works with the DND, CFWD, and ACD keys.

This feature is configurable using the configuration files or the Mitel Web UI.

HOW IT WORKS ON THE PHONE UI

When you enable the “as-feature-event” on the phone, AND you activate a DND, CFWD, and/or ACD key, pressing the key performs as follows:

- If the key is configured for an account on the phone, the server applies DND, CFWD or ACD to that account. (For information about CFWD and DND account configuration, see Chapter 3, the section, “Account Configuration” on page 3-40).
- If the key is “custom” configured, a screen displays on the phone allowing the user to choose the account to apply DND or CFWD. (For information about CFWD and DND custom configuration, see Chapter 3, the section, “Account Configuration” on page 3-40).
- A solid “Message Waiting Indicator” (MWI) indicates if one line/account has DND or CFWD enabled, and the LED next to the DND/CFWD key is ON. A status displays on the LCD that indicates the status of the line in focus (for example, the status of CFWD could be “Call Forward Busy” (CFWDB) or “Call Forward No Answer” (CFWDNA).

Note: If the ACD key is configured on the phone, and the “as-feature-event” is not enabled, the phones uses the ACD icons and LED behavior from a Sylantro/BroadWorks server instead.

When you press the DND, CFWD, or ACD key, only one attempt is made to enable/disable the “as-feature-event” feature on the server. The message “*Trying*” displays on the phone’s LCD after pressing the key. If the attempt is successful, the idle screen displays. If the attempt is unsuccessful, the message “*Failed*” displays. The user can press the softkey again to re-attempt the feature if required.

For server-side ACD, when you press the ACD softkey, the screen that displays is dependent on the state of the ACD subscription. Possible state for ACD are:

- **Logged Out** - User has the option of logging in.
- **Logged In** - User has the option of logging out or making the phone unavailable.
- **Unavailable** - User has the option of logging out or making the phone available.

Notes:

1. f DND and CFWD are configured to use "Account" mode on the IP Phone, pressing the DND and CFWD keys apply to the account in focus as described in Chapter 3, the section, "Account Configuration" on page 3-40.
2. If ACD is configured on the phone, the ACD softkey applies to the line for which the key is configured. The ACD softkey must be configured for the first line of an account. For example, if account 2 has line 3 and line 4 you must configure the ACD softkey for line 3.

CONFIGURING AS-FEATURE-EVENT SUBSCRIPTION USING THE CONFIGURATION FILES

If the phone-side features of the DND, CFWD, and ACD keys are enabled, the phone uses the existing parameter values for these keys. If the server-side features are enabled, the phone saves the state of the features from the server on the phone.

Use the following parameters to enable/disable the server-side "as-feature-event" on the IP Phone:

- **sip lineN as-feature-event subscription**
- **sip as-feature-event subscription period**

CONFIGURATION FILES

For the specific parameters you can set in the configuration files, see Appendix A, the section, "As-Feature-Event Subscription Settings" on page A-123.

Configuring As-Feature-Event Subscription Using the Mitel Web UI

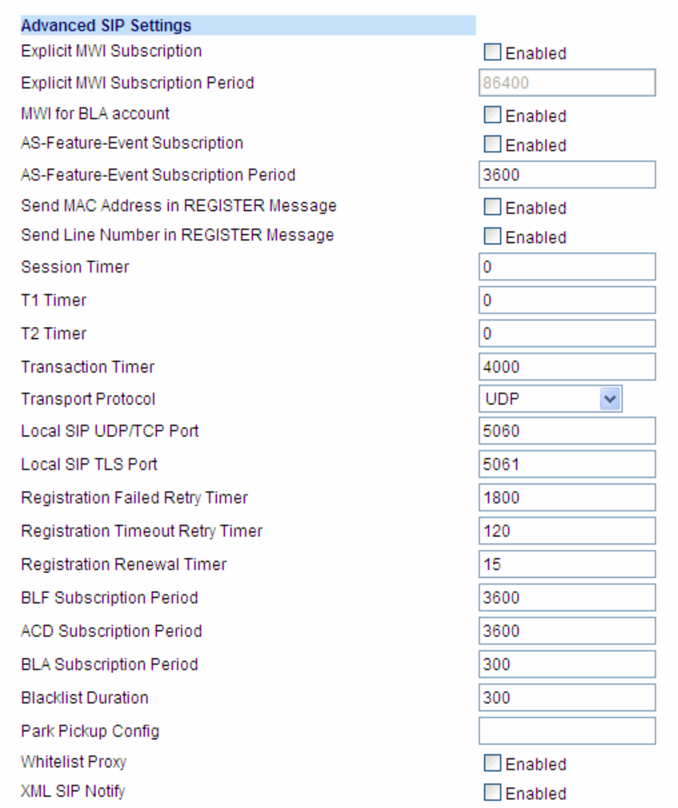
Use the following procedure to enable/disable the server-side "as-feature-event" on the IP Phone using the Mitel Web UI.

MITEL WEB UI

1. Click on **Advanced Settings->LineN->Advanced SIP Settings**.

2. Enable the "**As-Feature-Event Subscription**" field, by checking the check box. (Disable this field by unchecking the box).
3. Click **Save Settings** to save your changes.

4. Click on **Advanced Settings->Global SIP->Advanced SIP Settings**.



5. In the "**As-Feature-Event Subscription Period**" field, enter the amount of time, in seconds, that the phone waits after sending a SUBSCRIBE, to receive a NOTIFY response from the server side. Default is 3600.

6. Click **Save Settings** to save your changes.

BLACKLIST DURATION

The Blacklist Duration feature helps to reduce unnecessary delays during proxy/registrar server failures, caused by the IP phone repeatedly sending SIP messages to a failed server. If you enable this feature, then whenever the IP phone sends a SIP message to a server, and does not get a response, the phone automatically adds the server to the blacklist. The IP phone avoids sending messages to any servers on the blacklist. If all servers are on the blacklist, then the IP phone attempts to send the message to the first server on the list.

You can specify how long failed servers remain on the blacklist in the IP phone's configuration file or in the Mitel Web UI. The default setting is 300 seconds (5 minutes). If you set the duration to 0 seconds, then you disable the blacklist feature.

CONFIGURING BLACKLIST DURATION USING THE CONFIGURATION FILES

Use the following parameter to configure the Blacklist Duration in the configuration files:

- **sip blacklist duration**

CONFIGURATION FILES

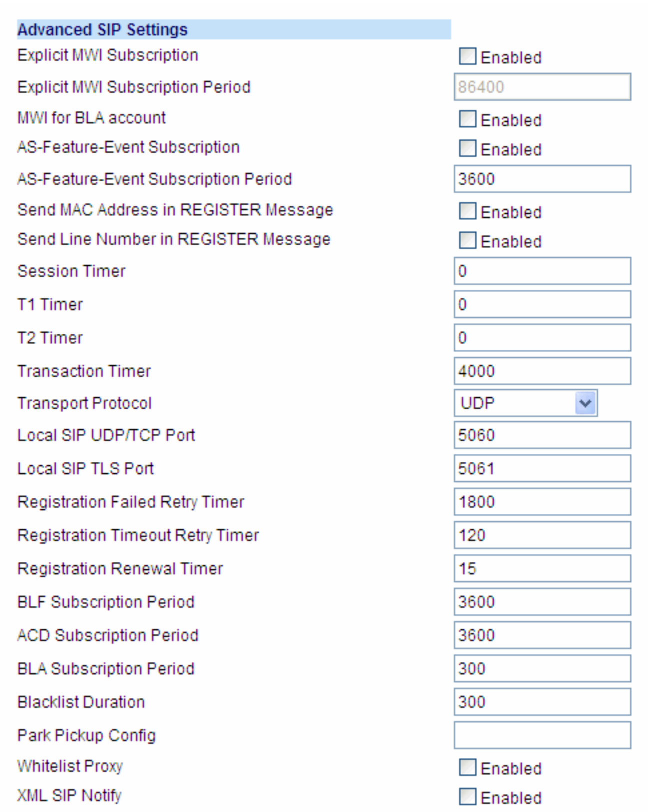
For the specific parameters you can set in the configuration files for setting Blacklist Duration, see Appendix A, the section, "Blacklist Duration Setting" on page A-316.

CONFIGURING A SERVER BLACKLIST USING THE MITEL WEB UI

You use the following procedure to configure Blacklist Duration using the Mitel Web UI.

MITEL WEB UI

1. Click on **Advanced Settings->Global SIP->Advanced SIP Settings**



2. In the "**Blacklist Duration**" field, specify the length of time, in seconds, that a failed server remains on the server blacklist. The IP phone avoids sending a SIP message to a failed server (if another server is available) for this amount of time. Valid values are 0 to 9999999. Default is 300 seconds (5 minutes).
For example: **600**

Note: The value of "**0**" disables the blacklist feature.

3. Click **Save Settings** to save your changes.

WHITELIST PROXY

To protect your IP phone network, you can configure a "**Whitelist Proxy**" feature that screens incoming call requests received by the IP phones. When this feature is enabled, an IP phone accepts call requests from a trusted proxy server *only*. The IP phone rejects any call requests from an untrusted proxy server.

The whitelist is dynamically updated (i.e. the phones are able to refresh and resync the whitelist [without a reboot] if the IP addresses corresponding to the proxy FQDNs are changed on the DNS server).

The IP phone monitors the following events and an update is triggered if required:

- 200 OK responses to REGISTER requests if the peer's IP address is not currently in the whitelist.
- 200 OK responses to INVITE requests if the peer's IP address is not currently in the whitelist.
- INVITE requests from untrusted proxy servers.

Notes:

1. 200 OK responses to INVITE requests for an IP call.
2. When more than one INVITE requests are received from the same untrusted proxy server.

CONFIGURING WHITELIST PROXY USING THE CONFIGURATION FILES

You use the following parameter to configure the whitelist proxy feature using the configuration files:

- sip whitelist

CONFIGURATION FILES

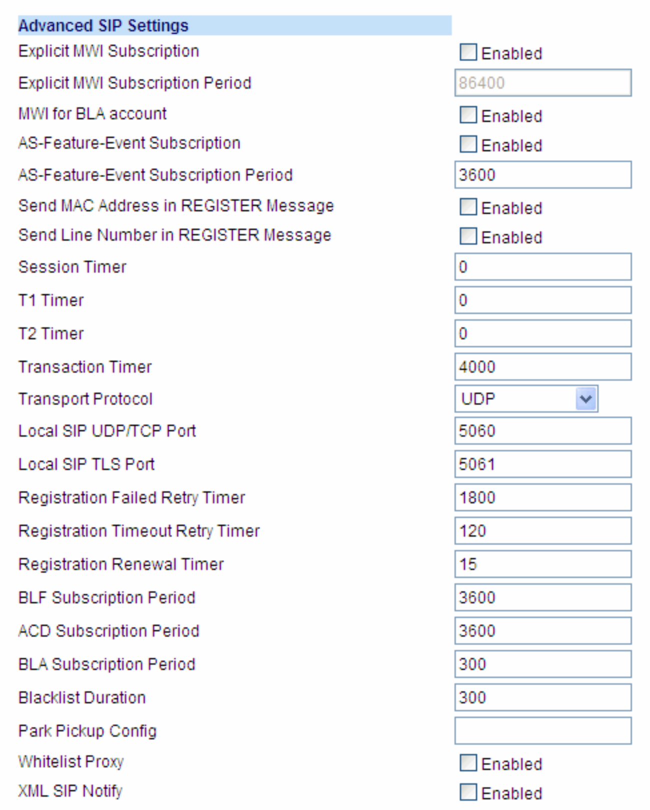
For the specific parameters you can set in the configuration files for setting Whitelist Proxy, see Appendix A, the section, "Whitelist Proxy Setting" on page A-316.

CONFIGURING WHITELIST PROXY USING THE MITEL WEB UI

Use the following procedure to configure the Whitelist Proxy feature using the Mitel Web UI.

MITEL WEB UI

1. Click on **Advanced Settings->Global SIP->Advanced SIP Settings**



2. The "**Whitelist Proxy**" field is disabled by default. To enable this field, check the box. When this feature is enabled, an IP phone accepts call requests from a trusted proxy server *only*. The IP phone rejects any call requests from an untrusted proxy server.

3. Click **Save Settings** to save your changes.

IP WHITELIST CONFIGURATION

To protect your IP Phone from a DoS attack, you may use software packet filtering rules by configuring the iptables to limit the number of incoming IP packets into the phone. To set up software packet filtering rules, use the following configuration parameter:

ip whitelist: <list of commas separated ipv4 address>

Notes:

1. The ip whitelist parameter supports up to 100 IP addresses.
2. The SIP proxy/registrar/outbound addresses are automatically populated into the iptables. If the proxy/registrar IPs are coming from the user.cfg, then the iptables do not get populated. This implies that either the sip proxy information is available in the startup.cfg or it should be manually added in the ip whitelist.
3. Ensure to manually add the user config IP and backup user config IP into the whitelist.

CONFIGURING IP WHITELIST USING THE CONFIGURATION FILES

CONFIGURATION FILES

For the specific parameters you can set in the configuration files for setting ip whitelist, see Appendix A, the section, "IPWhitelist Setting" on page A-316.

TRANSPORT LAYER SECURITY (TLS)

The IP Phones support a transport protocol called **Transport Layer Security (TLS)** and **Persistent TLS**. TLS is a protocol that ensures communication privacy between the SIP phones and the Internet. TLS ensures that no third party may eavesdrop or tamper with any message.

The 6800/6900 Series SIP phones support TLS versions 1.0, 1.1, and 1.2. TLS 1.1 and 1.2 introduce added security enhancements including (in TLS 1.2) the use of SHA-2 cryptographic hash functions. When TLS is being used for SIP messages the phone will always negotiate the highest possible TLS version in the handshaking process.

An NTP server is required to establish a successful TLS connection between an IP phone and a RCS server. If the phone cannot access the NTP server, the system is unable to check for the expiry of the RCS certificate, and therefore cannot validate the certificate and establish connection to RCS.

Note: Ensure that a default NTP server is accessible to all the phones in your network or that you have your own NTP server configured (using DHCP server options) and it is accessible to all the phones.

TLS is composed of two layers: the TLS Record Protocol and the TLS handshake protocol. The TLS Record Protocol provides connection security with some encryption method such as the Data Encryption Standard (DES). The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged. TLS requires the use of the following security certificate files to perform TLS handshake:

- Root and Intermediate Certificates
- Local Certificate
- Private Key
- Trusted Certificate

When the phones use **TLS** to authenticate with the server, each individual call must setup a new TLS connection. This can take more time when placing each call. Thus, the IP phones also have a feature that allows you to setup the connection to the server once and re-use that one connection for all calls from the phone. It is called **Persistent TLS**. The setup connection for Persistent TLS is established during the registration of the phone. If the phones are set to use Persistent TLS, and a call is made from the phone, this call and all subsequent calls use the same authenticated connection. This significantly reduces the delay time when placing a call.

Notes:

1. There can be only one persistent TLS connection created per phone.
2. If you configure the phone to use Persistent TLS, you must also specify the Trusted Certificate file to use. The Root and Intermediate Certificates, Local Certificate, and Private Key files are optional.

On the IP phones, an Administrator can configure TLS and Persistent TLS on a global-basis only, using the configuration files or the Mitel Web UI.

There is a keep-alive feature for persistent TLS connections only. Administrators can configure this keep-alive feature using the parameter called "**sip persistent tls keep alive**". When this feature is configured, the phone will send keep-alive pings to the proxy server at configured intervals. The keep-alive feature for persistent TLS connections performs the following functionalities:

- After a persistent TLS connection is established or re-established, activate the keep-alive, which will send CRLF to peer periodically.
- The phone will retry the connection automatically when a persistent TLS connection is down.
- When a persistent TLS connection is re-established (primary is up or primary is down and backup is up), refresh registration of the accounts associated with the connection.
- When a persistent TLS connection to primary is down, switch to backup if connection to backup is working.

Note: The real time interval will vary between 80% and 100% of the configured value.

Additionally the "**sip send sips over tls**" parameter allows administrators the ability to manually configure the IP phones to use either the SIP or SIPS URI scheme when TLS or persistent TLS is enabled. Disabling the "**sip send sips over tls**" parameter (i.e. defining the parameter as "**0**" in the configuration files) ensures the IP phones use the SIP URI scheme when TLS or persistent TLS is enabled. Enabling the parameter (i.e. defining the parameter as "**1**") ensures the phones use the SIPS URI scheme in such scenarios. The SIPS URI scheme is used by default.

The following ciphers and cipher suites are supported by SIP TLS client on the phone:

CIPHER	CIPHER SUITES
AES128	ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA256, ECDHE-RSA-AES128-SHA256 ECDHE-ECDSA-AES128-SHA, ECDHE-RSA-AES128-SHA AES128-GCM-SHA256, AES128-SHA256, AES128-SHA
AES256	ECDHE-ECDSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-SHA384, ECDHE-RSA-AES256-SHA384 ECDHE-ECDSA-AES256-SHA, ECDHE-RSA-AES256-SHA AES256-GCM-SHA384, AES256-SHA256,AES256-SHA
DES	DES-CBC3-SHA

CONFIGURING TLS USING THE CONFIGURATION FILES

You use the following parameters to configure TLS in the configuration files:

- sip transport protocol
- sips persistent tls
- sip persistent tls keep alive
- sip send sips over tls

- sips root and intermediate certificates
- sips local certificate
- sips private key
- sips trusted certificates

CONFIGURATION FILES

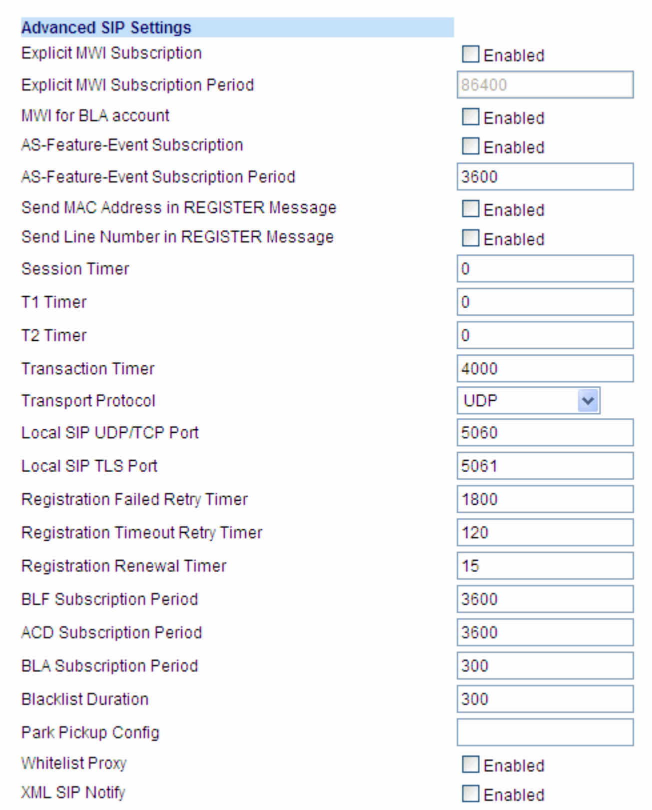
For the specific parameters you can set in the configuration files for setting TLS, see Appendix A, the section, "Transport Layer Security (TLS) Settings" on page A-124.

CONFIGURING TLS USING THE MITEL WEB UI

To configure TLS using the Mitel Web UI, you must enable TLS or Persistent TLS first. Then you must define the TLS certificate file names that you want the phone to use. Use the following procedure to configure TLS using the Mitel Web UI.

MITEL WEB UI

1. Click on **Advanced Settings->Global SIP->Advanced SIP Settings**.

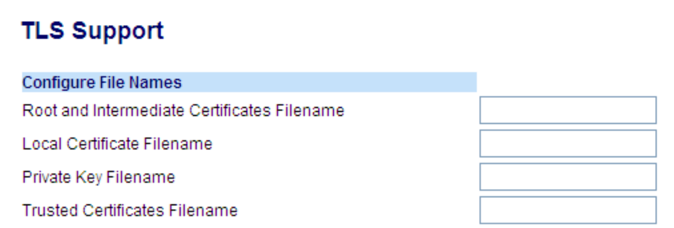


2. In the "**Transport Protocol**" field, select **TLS** or **Persistent TLS**.

> **Note:** If configuring **Persistent TLS**, you must go to *Advanced Settings->Global SIP->Basic Network Settings* and configure the "**Outbound Proxy Server**" and "**Outbound Proxy Port**" parameters.

3. Click **Save Settings** to save your changes.

4. Click on **Advanced Settings->TLS Support.**



5. Enter the certificate file names and the private key file name in the appropriate fields. The Root and Intermediate Certificate files contain one root certificate and zero or more intermediate certificates which must be placed in order of certificate signing with root certificate being the first in the file. If the local certificate is signed by some well known certificate authority, then that authority provides the user with the Root and Intermediate Certificate files (most likely just CA root certificate).
   The Trusted Certificate files define a list of trusted certificates. The phone's trusted list must contain the CA root certificates for all the servers it is connecting to. For example, if the phone is connecting to server A which has a certificate signed by CA1, and server B, which has a certificate signed by CA2, the phone must have CA1 root certificate and CS2 root certificate in its Trusted Certificate file.

   Notes:

   1. If configuring TLS, you must specify the files for Root and Intermediate Certificates, the Local Certificate, the Private Key, and the Trusted Certificates in order for the phone to receive calls.
   2. If configuring Persistent TLS, you must specify the Trusted Certificates (which contains the trusted certificate list). All other certificates and the Private Key are optional.
   3. The certificate files and Private Key file names must use the format ".pem".
   4. To create custom certificate files and private key files to use on your IP phone, contact Mitel Technical Support.

6. Click **Save Settings** to save your changes.

TLS V1.2 SUPPORT FOR 802.1X EAP

The 6800/6900 series SIP phones support TLS 1.2 for 802.1x EAP.

At reboot, the phone processes 802.1xEAP and sends client hello with TLS v1.2. The Radius server sends back server hello and the phone processes it with TLS v1.2.

Note:

1. Install Radius server with 802.1x TLS v1.2 support on the user network.
2. If the radius server does not support TLS v1.2, the phone automatically uses the TLS version (802.1x EAP TLS v1.1 or 802.1x EAP TLS v1.0) supported by the server.

The following TLS 1.2 cipher suites are supported for this feature:

- Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
- Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
- Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
- Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
- Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
- Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)

- Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
- Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
- Cipher Suite: TLS_RSA_WITH_RC4128MD5 (0x0004)

TELIA CA CERTIFICATE ADDITION

The Telia CA certificate is added to the Mitel repository for 6800/6900 Series SIP phones.

The SIP phone includes the CA to the root certificates in certificates.c file. After addition of the certificate, it is automatically made available for users to use.

Note: Reboot the phone to download all configuration files added to the server.

802.1X CONFIGURATION

If 802.1x on the phone is enabled, a "**802.1x Authenticating...**" message displays during startup of the phone.

If 802.1x fails to authenticate with the server, the phone continues its normal startup process using DHCP. However, the network port on the phone may or may not be disabled, depending on the switch configuration.

The 6800 and 6900 series SIP phones support the following versions of 802.1x protocol:

- 802.1x-2001
- 802.1x-2004

CERTIFICATES AND PRIVATE KEY INFORMATION

- If the certificates and private key are NOT stored in the phone, 802.1x authentication is disabled.
- If the certificates and private key ARE stored in the phone, the phone uses them during the authentication process
- If the phone uses EAP-TLS for successful authentication, the phone downloads the latest certificates and private key files, and then reboots.
- The private key uses AES-128 to encrypt the private key file.
- Switch Supplicant Mode - The switch supports the following 2 modes:
  - **Single supplicant** - This mode enables the port once any machine connected to this port is authenticated. For security reasons, the IP phone has the option to disable the pass-through port.
  - **Multiple supplicants** - Using this mode, the switch can support multiple clients connected to same port. The switch distinguishes between the clients based on their MAC address.
- Factory default and recovery mode deletes all certificates and private keys, and sets the EAP type to **disabled**.

You can configure the 802.1x feature on the IP phone using the configuration files, the IP Phone UI, or the Mitel Web UI.

CONFIGURING THE 802.1X PROTOCOL USING THE CONFIGURATION FILES

You use the following parameters to configure the 802.1x Protocol on your phone using the configuration files.

For EAP-MD5 use:

- eap type
- identity
- md5 password
- pc port passthrough enabled

For EAP-TLS use:

- eap type
- identity
- 802.1x root and intermediate certificates
(use 1 root and 0 or more intermediate certificates)
- 802.1x local certificate
(use 1 local certificate)

Notes:

1. The 802.1x local certificate configuration file must have only one client certificate for the phone.
2. If a certificate bundle or multiple certificates are found in the configuration file, the first certificate from the bundle is read and loaded to the phone.

- 802.1x private key
(1 private key that corresponds to local certificate)
- 802.1x trusted certificates
(0 or more trusted certificates)
- 802.1x mutual authentication
(Enables or disables mutual authentication for EAP-TLS for 802.1x setup)

CONFIGURATION FILES

For the specific parameters you can set in the configuration files for setting 802.1x support, see Appendix A, the section, "802.1x Support Settings" on page A-131.

CONFIGURING THE 802.1X PROTOCOL USING THE IP PHONE UI

Use the following procedure to configure the 802.1x Protocol on your phone using the IP Phone UI.

Note: If configuring 802.1x using the IP Phone UI, the certificates and private keys must already be configured and stored on the phone. Use the configuration files or the Mitel Web UI to load certificates and private keys

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press ⚙ or ⚙ on the phone to enter the Options List.
2. Select **Administrator Menu.**
3. Select **Network Settings->Ethernet & VLAN->802.1x Settings**.
4. Select **802.1x Settings.**
5. Select **802.1x Mode.**
6. Select **EAP-MD5** to configure the phone to use MD5 authentication;
   or
   Select **EAP-TLS** to configure the phone to use TLS authentication.

   Note: The 802.1x Protocol is disabled by default. If you select EAP-TLS authentication, you must use the configuration files or the Mitel Web UI to configure the certificates and private key for the phone.
7. Press **Set**.
8. To configure MD5, select **EAP-MD5 Settings**.
9. Select **Identity**.
10. Enter the identity or **username** used for authenticating the phone.
11. Press **Set**.
12. Enter the password used for authenticating the phone.
13. Press **Set**.

For the 6867i/6869i/6920/6930:

IP PHONE UI

1. Press ⚙ or ⚙ to enter the Options List.
2. Press the **Advanced** softkey.
3. Enter the Administrator password using the keypad. Default is “**22222**”.
4. Select **Network > 802.1x**.
5. In the **Basic Settings > EAP Type** select one of the following:
   - **Disabled** (Default)
   - **EAP-MD5** (phone uses MD5 authentication)
   - **EAP-TLS** (phone uses TLS authentication)

   Note: The 802.1x Protocol is disabled by default. If you select EAP-TLS authentication, you must use the configuration files or the Mitel Web UI to configure the certificates and private key for the phone.

6. In the **EAP-TLS Settings > Identity** field, enter a username used for authenticating the phone.
7. In the **EAP-TLS Settings > MD5 Password** field, enter the password used for authenticating the phone.

   Note: You must restart the phone for the 802.1x authentication parameters to take affect.

8. Press the **Save** softkey.
9. Restart the phone for the selection to take affect.

For the 6873i/6940:

IP PHONE UI

1. Press ⚙ or ⚙ to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password and press the blue Enter key. Default is “**22222**”.
4. Tap the **Network** icon.

> **Note:** If required, swipe left on the screen to navigate to the second page of options.

5. Tap the **802.1x** icon**.**
6. In the **Basic Settings > EAP Type** field select one of the following:
   - **Disable** (Default)
   - **EAP-MD5** (phone uses MD5 authentication)
   - **EAP-TLS** (phone uses TLS authentication)

> **Note:** The 802.1x Protocol is disabled by default. If you select EAP-TLS authentication, you must use the configuration files or the Mitel Web UI to configure the certificates and private key for the phone.

7. In the **EAP-TLS Settings > Identity** field, enter a username used for authenticating the phone.
8. In the **EAP-TLS Settings > MD5 Password** field, enter the password used for authenticating the phone.

> **Note:** You must restart the phone for the 802.1x authentication parameters to take affect.

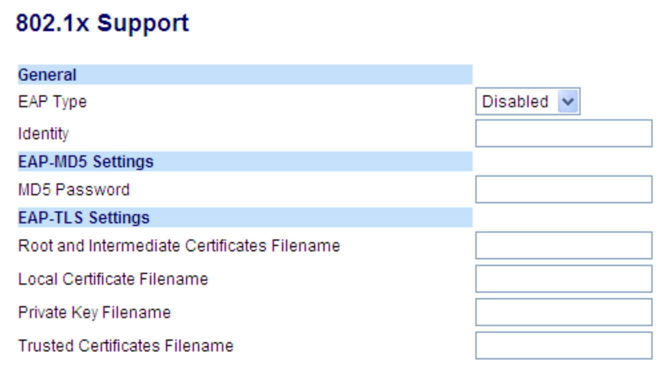
9. Tap the **Save** softkey.
10. Restart the phone for the selection to take affect.

CONFIGURING THE 802.1X PROTOCOL USING THE MITEL WEB UI

Use the following procedure to configure the 802.1x Protocol on your phone using the Mitel Web UI.

MITEL WEB UI

1. Click on **Advanced Settings->802.1x Support**.

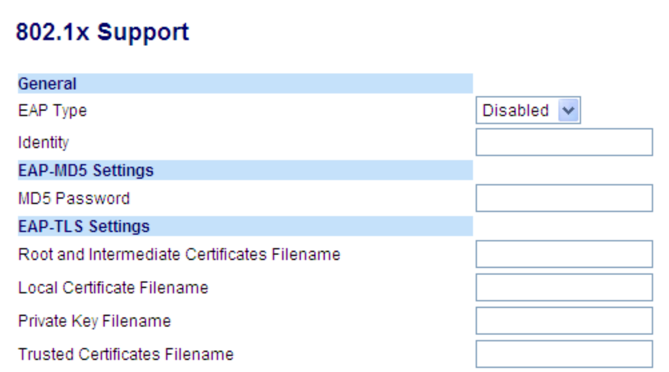


To configure EAP-MD5:

2. In the **“EAP Type**” field, select **EAP-MD5**.
   Valid values are: **Disabled** (Default), **EAP-MD5**, and **EAP-TLS**.
3. In the “**Identify**” field, enter an Identity for the IP phone for which you are configuring 802.1x.
4. For example, **phone1**.
5. In the “**MD5 Password**” field, enter a password used for the MD5 authentication of the phone.
6. For example, **password1**.
7. Click **Save Settings** to save your changes.

To configure EAP-TLS:

1. Click on **Advanced Settings->802.1x Support**.



2. In the **“EAP Type**” field, select **EAP-TLS**.
   Valid values are: **Disabled** (Default), **EAP-MD5**, and **EAP-TLS**.
3. In the “**Identity**” field, enter an Identity for the IP phone for which you are configuring 802.1x. For example, **phone1**.
4. In the “**Root and Intermediate Certificates Filename**” field, enter the filename that contains the root and intermediate certificates related to the local certificate. For example: **root_Intermed_certifi.pem**.
5. In the “**Local Certificate Filename**” field, enter the filename that contains the local certificate. For example: **localcertificate.pem**.
6. In the “**Private Key Filename**” field, enter the filename that contains the private key. For example: **privatekey.pem**.
7. In the “**Trusted Certificates Filename**” field, enter the filename that contains the trusted certificates. For example: **trusted_certificates.pem**.
8. Click **Save Settings** to save your changes.

SYMMETRIC UDP SIGNALING

By default, the IP phones use symmetric UDP signaling for outgoing UDP SIP messages. When symmetric UDP is enabled, the IP phone generates and listens for UDP messages using port 5060.

You can manually disable symmetric UDP signaling using the IP phone’s configuration file. When you disable symmetric UDP signaling, then the IP phone chooses a random source port for UDP messages.

The IP phone also chooses a random source port for UDP messages to the registrar if you configure a backup registrar server. Likewise, the IP phone chooses a random source port for UDP messages with regards to communication with the respective proxy server if you configure a backup proxy server or backup outbound proxy server. If you configure a backup registrar server as well as a backup proxy server and/or a backup outbound proxy server, one random source port will be used for all UDP messages (i.e. for communication with the proxy server[s] and for registration).

An Administrator can configure symmetric UDP signaling using the configuration files only.

CONFIGURING SYMMETRIC UDP SIGNALING USING THE CONFIGURATION FILES

You use the following parameter to enable or disable Symmetric UDP Signaling in the configuration files:

- sip symmetric udp signaling

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, “Symmetric UDP Signaling Setting” on page A-320.

SYMMETRIC TLS SIGNALING

The IP phones also use symmetric TLS signaling for outgoing TLS SIP messages by default. When symmetric TLS is enabled, the IP phone uses port 5061 as the persistent TLS connection source port. A configuration parameter enables or disables the usage of the port.

The following values can be set to the configuration parameter:

- 0 - disables the phone from using port 5061 and allows the phone to choose a random persistent TLS connection source port from the TCP range (i.e. 49152...65535) regardless of whether the parameter “sip outbound support” is enabled or disabled.
- 1 - enables the phone to use port 5061, by default.
- 2 - phone uses a random new port for reconnecting to the server over persistent TLS and forces close connection.
- 3 - phone uses a random new port for reconnecting to the server over persistent TLS but does not force close connection.

Note: If multiple persistent TLS connections are required, the persistent TLS connection source ports will follow the structure of random_port, random_port + 1, random_port + 2, etc....

An Administrator can configure symmetric TLS signaling using the configuration files only.

CONFIGURING SYMMETRIC TLS SIGNALING USING THE CONFIGURATION FILES

You use the following parameter to enable or disable Symmetric TLS Signaling in the configuration files:

- sips symmetric tls signaling

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, “Symmetric TLS Signaling Setting” on page A-321.

REMOVING USERAGENT AND SERVER SIP HEADERS

Currently, the phone always configures the SIP UserAgent/Server headers to contain:

Aastra <PhoneModel>/<FirmwareVersion>

You can suppress the addition of these headers by using the following parameter in the configuration files:

- sip user-agent

Setting this parameter allows you to enable or disable the addition of the User-Agent and Server SIP headers from the SIP stack.

You can configure this feature using the configuration files only.

CONFIGURING USERAGENT/SERVER SIP HEADERS

You use the following parameter to specify whether the UserAgent and Server SIP header is added to the SIP stack.

- sip user-agent

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "User-Agent Setting" on page A-321.

GRUU AND SIP.INSTANCE SUPPORT

Globally Routable User-Agent URIs (GRUUs) provide a way for anyone on the Internet to route a call to a specific instance of a User-Agent.

The IP phones provide GRUU support using draft-ietf-sip-gruu-15. A sip.instance is added to all non-GRUU contacts. By default, this feature is enabled. You can enable or disable this support using the configuration files.

Limitations of the GRUU Feature

The following are limitations of the GRUU feature on the phones:

- GRUU-Draft-15 is not compatible with versions prior to GRUU-Draft-10.
- Phones do not support temporary or phone-created GRUUs.

Enabling/Disabling GRUU and sip.instance Support

Use the following procedure to enable/disable GRUU and sip.instance support.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "GRUU and sip.instance Support" on page A-321.

MULTI-STAGE DIGIT COLLECTION (BILLING CODES) SUPPORT (FOR SYLANTRO SERVERS)

The IP Phones support Multi-Stage Digit Collection (billing codes) for Sylantro Servers. Sylantro Server features, like mandatory and optional billing codes, requires that the application server notify the phone to collect more digits before completing the call. The IP phone is able to collect digits in two stages to support the billing code feature.

Mitel IP Phone users are prompted to enter the correct billing code when they dial these numbers:

- External numbers.
- Eternal numbers dialed using a Speeddial key.

BILLING CODES IMPLEMENTATION NOTES

Note the following implementation information:

- IP phone users may enter a 2-9 digit billing code. Billing codes may not start with either 0 (Operator) or 9 (external calls).
- When using Sylantro Click-to-Call, IP phone users select a billing code from a pull-down menu.
- When placing a call, a secondary dial tone alerts IP phone users to enter the billing code. The IP phone UI also displays a “Enter Billing Code” message.
- If an IP phone user redials a number, they do not have to re-enter the billing code. The billing code information is maintained and processed accordingly.
- If an IP phone user enters an invalid billing code, the call fails.

MANDATORY VERSUS OPTIONAL BILLING CODES

This release of the Mitel IP phones supports two types of billing codes: Mandatory and Optional. The Sylantro server configuration determines which type of billing code is used on the IP phones.

- **Mandatory billing codes**: Calls are not connected until the user enters a valid billing code. The user dials the phone number. When prompted for billing codes, user dials the billing code.
  For example, suppose the IP phone user is using billing code 300, and dialing the external number 617-238-5500. The IP user then enters the number using the following format:
  - 6172385000#300

  Using mandatory billing codes, if the user is configuring a Speeddial number, then they enter the number using the following format:
  - <phonenumber>%23<billingcode>

  To use this format with the default dial plan terminator (#), the # sign required by Sylantro as a delimiter should be represented as an escaped character by using the sequence %23. The speeddial format for an external number that includes a mandatory billing code becomes:
  - <phonenumber>%23<billing code>
- **Optional billing codes:** The user dials an optional billing code by dialing *50, followed by the billing code digits. When prompted for additional digits, user enters the phone number. For example, suppose the IP phone user is using billing code 500, and dialing the external number 617-238-5000. The IP user then enters the number using the following format:
  - *50500#6172385000

  If the user is dialing configuring a Speeddial number, then they enter the number using the following format:
  - *50<billingcode>#<phonenumber>

To use this format with the default dial plan terminator (#), the # sign required by Sylantro as a delimiter should be represented as an escaped character by using the sequence %23. The speeddial format for an external number that includes an optional billing code becomes:

- *50<billing code>%23<phone number>

NUMBERS NOT REQUIRING BILLING CODES

Billing codes are not required for the following two types of calls:

- Emergency calls (E911)
- Calls between extensions

CONFIGURABLE DNS QUERIES

The Domain Name System (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to remember identifier for an Internet address.

The lists of domain names and IP addresses are distributed throughout the Internet in a hierarchy of authority within a database of records. There is usually a DNS server within close proximity to your geographic location that maps the domain names in your Internet requests or forwards them to other servers in the Internet.

The IP Phones may be configured to issue requests for DNS records using one of three methods. In the first method, the IP phones issue requests for “**A**” records from the DNS server. In the second method, the IP phones issue requests for “**SRV**” records from the DNS server. In the third method, the IP phones issue requests for **NAPTR** records from the DNS server. However, the IP phones do not use the **NAPTR** record to determine whether to use a secure or insecure communication path (see the following table for a description of each method).

When the IP phone accesses the IP network, it issues a DNS lookup request to find the IP address and port and then waits for a response from the DNS service that provides the IP address and port.

Note: Whether or not the phone will operate/communicate in a secure or insecure mode is ONLY determined by the pre-provisioning of the phone (i.e. the .cfg file).

You can configure the phone to use any one of these methods by entering the applicable value in the configuration files:

CONFIGURATION FILE VALUE	DNS SERVER METHOD USED	DESCRIPTION
0	A only	The phone issues requests for “**A**” (Host IP Address) records from the DNS server to get the IP address, and uses the default port number of 5060.

CONFIGURATION FILE VALUE	DNS SERVER METHOD USED	DESCRIPTION
1	SRV & A	The phone issues requests for “**SRV**” (Service Location Record) records from the DNS server to get the port number. Most often, the IP address is included in the response from the DNS server to avoid extra queries. If there is no IP address returned in the response, the phones send out the request for “**A**” records from the DNS server to find the IP address.
2	NAPTR & SRV & A	First, the phone sends "**NAPTR**" (Naming Authority Pointer) lookup to get the “**SRV**” pointer and service type. For example, if Global SIP transport protocol on the phone is “UDP”, and Proxy server on the phone is “test.mitel.com”, then: 1. If the NAPTR record is returned empty, the phone will use the default value “_sip._udp.test.mitel.com" for the “**SRV**” lookup. 2. If the NAPTR record is returned "test.mitel.com SIP+D2U .... _sip._udp.abc.mitel.co m", the phone will use “_sip._udp.abc.mitel.com" for the “**SRV**” lookup. 3. If the NAPTR record is returned "test.mitel.com SIP+D2T .... _sip._tcp.test.mitel.com", where the service type TCP mismatches the phone configured transport protocol “UDP”, the phone will ignore this value and use the default value “_sip._udp.test.aastra.com" for the “**SRV**” lookup. **Note:** The phone does not use the service type sent by the **NAPTR** response to switch its transport protocol, nor does it use the **NAPTR** response to determine whether to use a secure or insecure communication path. The phone will always use a global sip protocol that is configured on the phone via configuration files or the web user interface. After performing **NAPTR**, the phone sends “**SRV**” lookup to get the IP address and port number. If there is no IP address in the “**SRV**” response, then it sends out an “**A**” lookup to get it.

Note: On the phone side, if you configure the phone with a Fully- Qualified Domain Name (FQDN) proxy and specified port, the phone always sends “**A only**” lookups to find the Host IP Address of the proxy.

CONFIGURING THE DNS QUERY METHOD

You can configure the DNS query method for the phone to use for performing DNS lookups using the following parameter in the configuration files:

- sip dns query type

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "DNS Query Setting" on page A-323.

IGNORE OUT OF SEQUENCE ERRORS

An Administrator can configure the phone via the "**sip accept out of order requests**" parameter to ignore CSeq number errors on all SIP dialogs on the phone. When this parameter is enabled, the phone no longer verifies that the sequence numbers increase for each message within a dialog, and does not report a "CSeq Out of Order" error if they do not increase.

Note: As the default Asterisk configuration does not fully track dialogs through a reboot, it is recommended that this parameter be enabled when using the BLF feature with an Asterisk server. If you do not enable this feature, then rebooting the Asterisk server may cause BLF to stop working. With this parameter enabled, the BLF key starts working again when the phone re-subscribes, which by default, are one hour apart.

An Administrator can enable/disable this feature using the configuration files only.

ENABLING/DISABLING "OUT OF ORDER SIP REQUESTS"

Use the following procedure to enable/disable "out of order SIP requests".

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "Ignore Out of Order SIP Requests" on page A-324.

"EARLY-ONLY" PARAMETER IN REPLACES HEADER RFC3891

The phones support the "early-only" parameter in the "Replaces" header as referenced in RFC3891. When the phone receives a Replaces header with the early-only parameter, it replaces the existing dialog if the call is still in the early state. If the call has been answered, then the Replaces request is rejected.

Note: This feature is not supported in outgoing requests.

SWITCHING BETWEEN EARLY MEDIA AND LOCAL RINGING

The phone supports switching between early media and local ring tone. Upon receiving a 180 response, the phone generates a local ring tone unless it is receiving an early media flow. If the phone receives any subsequent 180 responses, it regenerates the local ring tone unless it is receiving early media flow.

ENABLE MICROPHONE DURING EARLY MEDIA

The phones now allow Administrators to enable or disable the microphone during early media by configuring the "**sip early media mute mic**" parameter. Early media indicates the period when a call has not fully established (i.e. the far end has not answered the call). By enabling this parameter, Administrators can mute the microphone during early media to prevent the far end from listening into the call prior to answering it.

ENABLING/DISABLING "MICROPHONE DURING EARLY MEDIA"

Use the following procedure to enable/disable "microphone during early media:

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "Enable Microphone During Early Media" on page A-233.

CONFIGURABLE CODEC NEGOTIATION BEHAVIOR

By default, when the phone receives an SDP Offer with several codecs defined for the media stream, the phone will reply with an SDP Answer containing all the codecs present in the Offer (as per RFC 3264).

A configuration parameter ("**sip single codec reply in sdp**") is available that allows Administrators to change the phone's codec negotiation behavior so that the phone will indicate only one preferred codec in the SDP when replying to an SDP offer (as per 3GPP TS 24.229).

Defining the "**sip single codec reply in sdp**" as "**0**" (disabled) will maintain the default behavior of the phone (as per RFC3264). Defining the "**sip single codec reply in sdp**" as "**1**" (enabled) will change the phone's behavior to indicate only one preferred codec (as per 3GPP TS 24.229).

Note: The first codec on the compatible codecs list will be selected as the single preferred codec when the "**sip single codec reply in sdp**" parameter is enabled.

CONFIGURING CODEC NEGOTIATION BEHAVIOR

Use the following procedure to configure codec negotiation behavior:

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "Codec Negotiation Behavior" on page A-233.

"CALL-INFO" HEADER TO 200OK RESPONSES FOR SHARED CALL APPEARANCE (SCA) LINES

A "Call-Info" header is included in the 200ok response to an INVITE, RE-INVITE, and UPDATE messages for SCA lines. No configuration is required for this feature.

REASON HEADER FIELD IN SIP MESSAGE

The IP Phones support the receiving of the Reason Header Field in a SIP CANCEL message, as described in RFC3326. This allows a call that is answered from somewhere else to still display in the Received Callers List. Also, the missed calls indicator and counter do not change.

LIMITATION

If the call is answered somewhere else, the duration of the call does not display in the Received Callers List.

CALL FAILED MESSAGE

Administrators can place certain restrictions on users for making outgoing calls (for example, only allow national calls, only allow internal calls, only allow emergency calls, etc.). Previously when a restriction was active and a user dialed a number that was not allowed, the PBX sent a certain status code 4xx and the phone displayed "Call Failed" or "Busy", which was not very informative to the user.

Now when an outgoing call fails with a status code 4xx or 5xx, the phone will look for the Reason Header (RFC 3326) in the status message and display the Reason Header to the user. The reason text is displayed in the center of the screen and is limited to 20 characters.

If *there is* a Reason Header in the status code message, the reason text (if any) will be displayed on the phone. The tone that is played follows the status code (i.e. the busy tone for 486 and the call failed tone for all others).

If *there is no* Reason Header in the status message, the behavior of the phone should be unchanged:

- "Busy" is displayed for the status code 486 and the busy tone will be played,
- or "Call Failed" is displayed for status codes 4xx to 5xx and the call failed tone will be played,
- or "Not Configured" or "Seize Failed" is displayed in case of an internal error,
- or "Unavailable" is displayed in case of code less support (6867i, 6869i, 6873i, 6920, 6930, 6940).

CONFIGURABLE "ALLOW" AND "ALLOW-EVENT" OPTIONAL HEADERS

On the IP Phones, an Administrator can enable or disable whether or not the optional "Allow" and "Allow-Events" headers are included in the NOTIFY message from the phone.

SIP NOTIFY messages from the phone may contain optional headers called "Allow" and "Allow-events". If the NOTIFY message contains these headers, the UDP packet returned by the server may be too large and may fragment the packet. To prevent the fragmenting of the UDP packet, the "Allow" and "Allow-events" headers may be removed using the parameter, "**sip notify opt headers**". If this parameter is set to "**0**" (disabled), the optional headers are not included in the SIP NOTIFY message which reduces the size of the packet returned by the server, and prevents fragmentation of the packet.

The value set for this parameter specifies whether or not to include the optional headers in the SIP NOTIFY message from the phone.

An Administrator can enable/disable the optional "Allow" and "Allow-Event" headers using the following parameter in the configuration files:

- sip notify opt headers

ENABLING/DISABLING OPTIONAL "ALLOW" AND "ALLOW-EVENT" HEADERS

Use the following procedure to enable/disable "Allow" and "Allow-Event" headers.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "Optional "Allow" and "Allow-Event" Headers" on page A-324.

CONFIGURABLE SIP P-ASSERTED IDENTITY (PAI)

The IP Phones support a private extension to SIP for Asserted Identity within trusted networks (as defined in RFC 3325). This feature allows a network of trusted SIP servers to assert the identity of authenticated users, and verify that phone messages originate from a Trusted Identity. Upon receiving a message from a caller in the Trusted Network, the IP phone reads the contents of the P-Asserted-Identity (PAI) header field and displays it on the phone UI. This field contains a more accurate description of the caller identity (extension/phone number) than is contained in the SIP message.

Notes:

1. The phones support PAI header in the UPDATE message, according to draft-ietf-sipping-update-pai-00. This feature is always enabled.
2. If an UPDATE is received with a PAI header from a trusted source, the phone updates the display with this information. The phone ignores any PAI received from untrusted entities.

When an IP phone receives an incoming call, the IP phone performs the following actions:

- Checks to see if the incoming call is from a registered proxy server.
- If the call is forwarded via a registered proxy server, then the message has already been verified and authenticated by the server. The caller is part of the Trusted Network. The IP phone UI displays the caller information contained in the PAI header.
- If the call is not forwarded via a registered proxy server - and therefore is not a “Trusted Entity” - the IP phone UI does not display any trust information contained in the PAI header.

Using the "**sip pai**" parameter, Administrators are able to select which URI field ("sip" or "tel") the phone should use when displaying the PAI URI information. Valid options include:

0: Disabled: PAI information is ignored.

1: Use sip URI only: (Default) The phone will use the URI information contained in the "sip" URI field (if available) and ignore the information contained in the "tel" URI field (if available).

2: sip URI preferred: The phone will use the URI information contained in the "sip" URI field. If the "sip" URI field is unavailable, the phone will use the URI information contained in the "tel" URI field.

3: Use tel URI only: The phone will use the URI information contained in the "tel" URI field (if available) and ignore the information contained in the "sip" URI field (if available).

4: tel URI preferred: The phone will use the URI information contained in the "tel" URI field. If the "tel" URI field is unavailable, the phone will use the URI information contained in the "sip" URI field.

Note: The default value (i.e. "1") will be enforced if this parameter is defined with any unsupported value.

ENABLING/DISABLING P-ASSERTED IDENTITY (PAI)

Use the following procedure to enable/disable PAI.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, “P-Asserted Identity (PAI)” on page A-325.

CONFIGURABLE ROUTE HEADER IN SIP PACKET

The IP Phones support the following parameter:

- sip remove route

This parameter enables or disables the addition of the Route header in a SIP packet. Enable this parameter for outbound proxies that do not support Route headers.

Note: When enabled this will break all support for SIP routing, so if some other device in the network attempts to add itself to the route it will fail.

ENABLING/DISABLING THE ROUTE HEADER IN THE SIP PACKET

Use the following procedure to enable/disable the addition of the Route header in the SIP packet.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "Route Header in SIP Packet" on page A-325.

CONFIGURABLE COMPACT SIP HEADER

The phones provide a feature that allows an Administrator to shorten the length of a SIP packet by using the compact form. This feature is in accordance with Compact SIP Headers defined in RFC 3261.

For example, the following SIP header is the long format:

```
Via: SIP/2.0/UDP
10.50.91.2:5060;branch=z9hG4bK571ebe0c;rport=5060;received=10.50.
91.2
From: "Unknown" <sip:Unknown@10.50.91.2>;tag=as19d00fc8
To: <sip:1106@10.50.110.54:5060;transport=udp>;tag=916699998
Call-Id: 73cad5456806f3a7768d17e8617279d7@10.50.91.2
CSeq: 102 OPTIONS
```

The following SIP header is equivalent to the above SIP header, but uses the short (compact) format instead:

```
v: SIP/2.0/UDP
10.50.91.2:5060;branch=z9hG4bK571ebe0c;rport=5060;received=10.50.
91.2
f: "Unknown" <sip:Unknown@10.50.91.2>;tag=as19d00fc8
t: <sip:1106@10.50.110.54:5060;transport=udp>;tag=916699998
i: 73cad5456806f3a7768d17e8617279d7@10.50.91.2
CSeq: 102 OPTIONS
```

By default, the IP Phones use the long format. However, an Administrator can provision the short (compact) format using the configuration files. The Mitel Web UI does not support this configuration feature.

ENABLING/DISABLING THE COMPACT SIP HEADERS FEATURE

Use the following procedure to enable/disable the Compact SIP Header in the SIP packet.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "Compact SIP Header" on page A-326.

REJECT INV OR BYE WHEN UNSUPPORTED VALUE IN REQUIRE HEADER

The IP Phones support the following parameter:

- sip enforce require hdr

This parameter allows you to enable (1) or disable (0) the rejection of an INV or BYE with a "420 Bad Extension" if the INV or BYE contains an unsupported value in the REQUIRE header.

ENABLING/DISABLING A REJECTION OF THE INV OR BYE

Use the following procedure to enable/disable the rejection of the INV or BYE if the INV or BYE contains an unsupported value in the REQUIRE header.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "Rejection of INV or BYE" on page A-326.

XML URI FOR KEY PRESS SIMULATION

The phones provide a feature that allow an XML Developer or Administrator to define XML Key URIs that can send key press events to the phone, just as if the physical hard key, softkey, or programmable key were pressed on the phone.

When the Key URI event is sent from the server to the phone, the phone initiates the event as if the key was physically pressed. If the key is not present on the phone (hard key) or not available (softkey or programmable key), when the phone receives the URI, the event is discarded. If you are in the process of changing the softkey or programmable key setting, or the key is disabled while the event is being processed, the request is discarded. The phone maps key events to its physical keys and not to its mapped logical keys.

The following table identifies the XML URIs for pressing buttons on the phone..

XML KEY URI	DESCRIPTION
LINE KEYS	
Key:Line1 to Key:Line<n>	Line 1 to <n>Keys **Note:** The phone ignores URI line key events if the line keys are not physically present on the phone.
KEYPAD KEYS	
Key:KeyPad0 to Key:KeyPad9	Numeric Keypad Keys 0-9
Key:KeyPadStar	* - Star Key
Key:KeyPadPound	# Hash Key
SOFTKEYS	

XML KEY URI	DESCRIPTION
Key:SoftKey1 to Key:SoftKey<n>	Softkey 1 to <n> (valid softkeys depend on the number of physical softkeys on the phone)
Key:TopSoftKey1 to Key:TopSoftKey<n> top	Top softkeys 1 to <n> ((valid top softkeys depend on the number of physical top softkeys on the phone)
PROGRAMMABLE KEYS	
Key:PrgKey1 to Key:PrgKey<n>	Programmable keys 1 to <n> (valid programmable keys depend on the number of physical programmable keys on the phone)
EXPANSION MODULE KEYS	
Key:ExpMod1SoftKey1 to Key:ExpMod1SoftKey<n>	Expansion module 1 softkeys 1 to <n> (valid softkeys depend on the number of physical softkeys on the expansion module) **Note:** The phone ignores URI expansion module key events if the keys are not physically present on the expansion module.
Key:ExpMod2SoftKey1 to Key:ExpMod2SoftKey<n>	Expansion module 2 soft keys 1 to <n> (valid softkeys depend on the number of physical softkeys on the expansion module)
Key:ExpMod3SoftKey1 to Key:ExpMod3SoftKey<n>	Expansion module 3 soft keys 1 to <n> (valid softkeys depend on the number of physical softkeys on the expansion module)
VOLUME KEY	
Key:VolDwn	Volume Decrease Key
Key:VolUp	Volume Increase Key
FEATURE KEYS	
Key:Xfer	Transfer Key
Key:Conf	Conference Key
Key:Services	Services Key
Key:Intercom	Intercom Key
Key:Headset	Headset Key **Note:** For Headset URI key, the behavior will be as if the "speaker/headset" key is pressed; and does not switch to headset for headset key event or to speaker for speaker key event.
Key:Speaker	Speaker Key **Note:** For Speaker URI key, the behavior will be as if the "speaker/headset" key is pressed; and does not switch to headset for headset key event or to speaker for speaker key event.
Key:Mute	Mute Key

XML KEY URI	DESCRIPTION
Key:Hold	Hold Key
Key:Redial	Redial Key
Key:Callers	Callers Key
Key:Directory	Directory Key
Key:Options	Options Key
Key:Save	Save Key
Key:Delete	Delete Key
Key:Swap	Swap Key
Key:Goodbye	GoodBye Key
NAVIGATION KEYS	
Key:NavUp	Navigation Up Key
Key:NavDwn	Navigation Down Key
Key:NavLeft	Navigation Left Key
Key:NavRight	Navigation Right Key
FUNCTION KEYS (ONLY IF PHYSICALLY CONFIGURED ON THE PHONE OR EXPANSION MODULE)	
KeyPark	Park Softkey
KeyPickup	Pickup Softkey

Notes:

1. If the URI key is a valid key, the phone executes the key regardless of the current state on the phone.
2. Park and Pickup XML URI softkeys are available **ONLY** if these features are physically configured on the phone or expansion module.

EXAMPLES

There are two ways to format the XML key URI:

For XML Post Messages

<ExecuteItem URI="<XML Key URI>" />

Example:

```
<ExecuteItem URI="Key: Line1" />
```

For XML Key Scripts

<URI><XML Key URI></URI>

Example:

```
<URI>Key: Line1</URI>

<SoftKey index="1">
<Label>Keypad1</Label>
<URI>Key: Line1</URI>
</SoftKey>
```

DOMAIN NAME SYSTEM (DNS) SERVER PRE-CACHING SUPPORT

The IP phones now support the use of a local DNS host file to resolve DNS queries, and supports pre-provisioning of DNS SRV records. This feature allows administrators to configure the phone to download a text file which contains persistent DNS “A record” hostname to IP address mappings. In addition, support for persistent DNS “SRV records” has been added to permit SRV based high availability of services.

There are two methods used to configure DNS pre-caching on the IP phone:

- Configure a unix style “host” file used instead of a DNS “A query” to resolve hostnames to IP addresses. The host file is downloaded and cached on the IP phone.
- Configure DNS “SRV queries” for geographic redundancy and failover. The configured SRV entries are used to pre-load the DNS cache on the IP phone.

Both these methods are configurable using the configuration files only, and are primarily intended for use when a third party hosting provider delivers SIP services but does not have local access or control of the LAN side DNS infrastructure.

Note: Time-to-Live (TTL) used in this feature is hard-coded for each server and not configurable.

CONFIGURING DNS “HOST FILE” PRE-CACHING FROM THE CONFIGU-RATION SERVER

The DNS host file must reside on the same server as the configuration files (*startup.cfg/.tuz*, etc.) and the filename to download is specified within the configuration.

Use the following parameter to configure the phone to use the host file for host IP address lookups.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, “DNS Host File” on page A-327.

The following procedure is an example of how to use the “sip dns host file” parameter to configure DNS lookup pre-caching from the configuration server.

CONFIGURING “DNS HOST” PRE-CACHING

1. Using a text-based editing application, create a blank text file

2. Enter the IP addresses of the DNS servers in your local network. For example:
   1.2.3.4 server1
   5.6.7.8 server2
   9.0.1.2 server3

   Note: Ensure each line uses a Carriage Return (CR) or Carriage Return + Line Feed (CRLF) to terminate the line.

3. Save the file as "*<filename>.txt*". For example, "***hostfile.txt***".
4. Using a text-based editing application, open the *startup.cfg* file for the phone(s) for which you want to apply the DNS hostfile.
5. Enter the following parameter in the *startup.cfg* file followed by the host file name as the value: sip dns host file: <filename>.txt
   For example:
   sip dns host file: hostfile.txt

   Note: If using a text file on a PC to enter this value, you must enter a carriage return (CR) after entering the host file name.

6. Save the file. Make sure the *startup.cfg* and the *hostfile.txt* files are on the configuration server in your network before downloading to the phone(s).
7. Restart the phone(s) in your network.
   The phone(s) downloads the specified host text file and stores it locally on the phone's flash memory. Upon each subsequent boot of the phones, if the host text file is available on the configuration server, it is downloaded to replace the locally cached copy; otherwise, the previously cached copy is retained and used unchanged.
   The configuration of the phone(s) can now use server1, server2, or server3 for SIP or other services instead of using the IP addresses. The phones will continue resolving the host names even if DNS on the network has conflicting or missing entries for server1, server2, or server3, or if the local LAN DNS server fails to respond.

CONFIGURING DNS "SERVICE (SRV) RECORDS" PRE-CACHING

In addition to using a host file to resolve host names to IP addresses, an Administrator can also configure DNS "SRV records" (Service Records) for geographic redundancy and failover between application servers in the network.

The SIP registration and SIP proxy features on the phones previously allowed the use of server queries only to live DNS servers. Using the host file and specific DNS SVR parameters extends this mechanism to allow pre-configuration of server values in the *startup.cfg* file. The following new parameters are used for this feature:

- sip dns srvX name
- sip dns srvX priority
- sip dns srvX port

- sip dns srvX target

Note: The “X” indicates a DNS SRV with a value from 1 to 4.

You can configure up to 4 DNS SRV records, with each server having a **priority** which tells the phone which server to use, and a host name or **target**. The IP phone will use the DNS SRV record with the lowest-numbered priority value first, and will only failover to other records if the connection with this record's host fails. Thus a service may have a designated failover server, which is only used if the primary server fails.

If a service has multiple SRV records with the same priority value, the IP phone(s) use the weight field to determine which host to use. The weight value is a ratio compared to the weight of other records with the same name and priority value.

In the following example, both the priority and weight fields are used to provide a combination of load balancing and backup service.

Example

```
sip dns srv1 name: _sip._udp.example.com
sip dns srv1 priority: 10
sip dns srv1 weight: 60
sip dns srv1 port: 5060
sip dns srv1 target: bigbox.example.com

sip dns srv2 name: _sip._udp.example.com
sip dns srv2 priority: 10
sip dns srv2 weight: 20
sip dns srv2 port: 5060
sip dns srv2 target: smallbox1.example.com

sip dns srv3 name: _sip._udp.example.com
sip dns srv3 priority: 10
sip dns srv3 weight: 20
sip dns srv3 port: 5060
sip dns srv3 target: smallbox2.example.com

sip dns srv4 name: _sip._udp.example.com
sip dns srv4 priority: 20
sip dns srv4 weight: 10
sip dns srv4 port: 5060
sip dns srv4 target: backupbox.example.com
```

The first three records (SRV 1, 2, and 3) share a priority of 10, so the weight field's value is used by the phones to load balance across the three target host names.
Bigbox will get 60% of the load, and smallbox1 and smallbox2 will each get 20% load.

If all three servers with priority 10 are unavailable, the next highest priority record is selected, in this case backupbox. This could be a server in another physical location.

The server entries in the *startup.cfg* file can use DNS hostnames or can use IP addresses. If hostnames are used, any pre-cached DNS A records via the host file mechanism are used before resorting to live DNS query if there is no local match.

For example, the following hostfile.text uses IP addresses that are used in the DNS server queries:

```
hostfile.txt

192.168.2.3 bigbox.example.com
192.168.3.4 smallbox1.example.com
192.168.8.1 smallbox2.example.com
47.28.05.69 backupbox.example.com
```

Use the following procedure in the configuration files to configure DNS server query support for the phones.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "DNS Server Query" on page A-327.

Use the following procedure to configure DNS SRV record pre-caching.

CONFIGURING DNS SRV RECORD PRE-CACHING

1. Using a text-based editing application, open the *startup.cfg* file.
2. Enter the parameter, "**sip dns srvX name**", where "X" is a value from 1 to 4.
   Enter a value for the DNS SRV service URI. For example:
   sip dns srv1 name: _sip._udp.example.com
3. Enter the parameter, "**sip dnx srvX priority**, where "X" is a value from 1 to 4.
   Enter a value for the DNS server priority. Valid values are 0 to 65535. Default is 0. For example:
   sip dns srv1 priority: 10
   After this parameter is downloaded from the configuration server to the phone, the phone uses the DNS server with the lowest numbered priority first to perform DNS lookups.
4. Enter the parameter, "**sip dnx srvX weight**, where "X" is a value from 1 to 4.
   Enter a value for the DNS server weight. Valid values are 0 to 65535. Default is 0. For example:
   sip dns srv1 weight: 60

   Note: The "sip dns srv1 weight" parameter must be configured but will be supported in a future release.
5. Enter the parameter, "**sip dnx srvX port**, where "X" is a value from 1 to 4.
   Enter a value for the port number on the target host. Valid values are 0 to 65535. Default is 0. For example:
   sip dns srv1 port: 5060

6. Enter the parameter, "**sip dnx srvX target**, where "X" is a value from 1 to 4.
   Enter a value for the DNS server target. Valid values are the host name or a fully qualified domain name. For example:
   sip dns srv1 target: bigbox.example.com
7. Save and close the file.
8. Place the *startup.cfg* file on the configuration server and download to the phones.

DNS-SRV HANDLING FOR DIFFERENT 5XX ERROR CONDITIONS

Previously SIP phone models allowed any SIP request to trigger DNS SRV failover and treated only 503 status code in 5xx class of response as service unavailable.

The 6800/6900 Series SIP phones now perform DNS-SRV failover for all SIP messages when a 5xx is received. A new DNS SRV failover mode named DNS-SRV failover-follow-registration is added to the SIP engine. Also the service unavailable response fail over rule is now configurable in the SIP stack.

The key point of the feature is DNS SRV failover follows registration. The following configurations are specified for the SIP phone to ensure DNS SRV failover follows registration:

- "proxy server", "registrar server" and "sip outbound proxy" (in SBC scenario) are set to DNS SRV FQDN
- "sip proxy port", "sip registrar port" and "sip outbound proxy port" are set to 0
- no backup proxy or registrar is configured
- no backup outbound is configured

SERVICE UNAVAILABLE STATUS CODES

Service unavailable status codes indicate that the server service is unavailable. The SIP phone switches server when a SIP response with one of the status codes is received.

Define Service Unavailable Status Codes Using Configuration Files

CONFIGURATION FILES

Administrators can define the service unavailable status codes rule by defining a new parameter "**sip service unavailable status codes**" in the configuration files.

Note: 408 and 503 are not included in the parameter list but yet treated as service unavailable status codes.

For the specific parameter you can set in the configuration files, see Appendix A, section "Service Unavailable Status Codes" on page A-329.

SERVICE UNAVAILABLE RESPONSE FAILOVER RULE

A service unavailable response is a SIP response with one of the defined service unavailable status codes. The following are the two failover rule options:

- option1: failover only if the service unavailable response is the first response received.
- option2: failover when the service unavailable response is received and no response other than 100 trying responses are received for the SIP request.

Define Service Unavailable Response Failover Rule Using Configuration Files

CONFIGURATION FILES

Administrators can configure the service unavailable response failover rule by defining a new parameter "**sip service unavailable failover rule**" as "**1**" in the configuration files. By default this feature is disabled.

For the specific parameter you can set in the configuration files, see Appendix A, section "Service Unavailable Response Failover Rule" on page A-329.

DNS SRV FAILOVER MODE

Administrators can configure the DNS SRV failover mode by defining the parameter "**sip srv failover enabled**" as "**2**" in the configuration files.

Define DNS SRV Failover Mode Using Configuration Files

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, section "DNS SRV Failover Mode" on page A-329.

CONFIGURABLE DNS MAXIMUM CACHE TTL

Administrators can manually set the DNS maximum cache TTL settings for both negative and positive responses on the phone by defining the "**sip dns cache negative max ttl**" and "**sip dns cache positive max ttl**" parameters in the configuration files. Setting these parameters will help alleviate issues regarding the phone not considering the DNS retry time settings defined by the DNS server.

CONFIGURING THE DNS MAXIMUM CACHE TTL

Use the following procedure to configure the DNS maximum cache TTL settings.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "DNS Maximum Cache TTL Settings" on page A-330.

CONFIGURE REUSE OF EXPIRED DNS RECORDS

An Administrator can configure the usage of expired DNS SIP records by defining the "**sip dns use cached expired response**" parameter in the configuration files. By default, this feature is disabled. When enabled, the previously resolved FQDN records can be reused beyond the TTL expiry. And even if expired, the previously resolved records can be reused whenever DNS server errors occur during DNS queries.

CONFIGURING REUSE OF EXPIRED DNS RECORDS

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "Reuse of Expired DNS Record Settings" on page A-330.

CONFIGURABLE TRANSPORT PROTOCOL FOR SIP SERVICES AND RTCP SUMMARY REPORTS

Parameters have been implemented allowing administrators the ability to independently configure the transport protocols used by SIP services (e.g. the SIP XML Notify service) and RTCP summary reports. The following parameters are available to be defined in the configuration files:

SIP SERVICES

- sip services transport protocol
- sip services port

The above parameters are used to specify the transport protocol and port used for SIP services.

RTCP SUMMARY REPORTS

- sip rtcp summary reports transport protocol

The above parameter is used to specify the transport protocol used for RTCP summary reports.

Notes:

1. The parameter "sip symmetric udp signaling" is effective when the transport protocol for RTCP summary reports is set to be UDP. For more information on symmetric udp signaling, refer to "Symmetric UDP Signaling," on page 33.
2. When the SIP transport protocol is set to TCP and the RTCP summary reports transport protocol is set to UDP, if an outbound proxy is configured, all SIP requests including RTCP summary reports will be sent over TCP.
3. In cases where the SIP services transport protocol is the same as the SIP transport protocol or RTCP summary reports transport protocol, only the SIP services port is enabled (the phone listens on the SIP services port as well as the local SIP port if they are different [if they are the same, no extra action is needed]).

Use the following procedure in the configuration files to configure the transport protocol for SIP services and RTCP summary reports.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "SIP Services/RTCP Summary Reports Transport Protocol Settings" on page A-331.

CONFIGURABLE ALPHANUMERIC INPUT ORDER FOR USERNAME PROMPTS

A configuration parameter **username alphanumeric input order** is available for the 6863i and 6865i IP phones allowing administrators the ability to change the default behavior of the keypad input order during username and password prompts. By default, keypad input order during username and password prompts changes from uppercase letters to the respective digit and then to lowercase letters with each successive press of the key. For example, when pressing "2" on the keypad, the following will be input with each successive press:

# OF PRESSES	LETTER/NUMBER
1	A
2	B
3	C
4	2
5	a
6	b
7	c

When the **username alphanumeric input order** parameter is defined as "**1**", the respective digit will be available as the first input option followed by upper case and then lower case letters. For example, when pressing "2" on the keypad with this parameter enabled, the following will be input with each successive press:

# OF PRESSES	LETTER/NUMBER
1	2
2	A
3	B
4	C
5	a
6	b
7	c

The behavior of the **username alphanumeric input order** parameter is applicable to the following username prompts as displayed on the phone's UI:

- HTTPS Login User Name

- SIP User Name
- SIP Display Name
- SIP Auth. Name
- FTP User Name

Note: The parameter is set to “1” (Digit first) by default.

Use the following procedure in the configuration files to configure the keypad input order for username and password prompts.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, “Alphanumeric Input Order for Username Prompts” on page A-332.

ACTIVE VOICE-OVER-IP (VOIP) RECORDING

Active VoIP recording is supported by the IP phones. When using the IP phones with a Mitel call manager supporting voice recording and a recording system with the predefined subset of the SIP interface, administrators can configure the phones to send duplicate copies of the transmit and receive RTP or SRTP voice packets to the voice recording system.

Notes:

1. Currently, the active VoIP recording feature is only supported when using the MiVoice MX-ONE call manager (v4.1 or 5.0) in conjunction with ASC’s EVO*ip* 10.0 voice recording system. Support for additional call managers and voice recording systems will be implemented in future releases.
2. The active VoIP recording feature is disabled by default.

Both dynamic (i.e. per call) and static (i.e. per the duration that the phone is registered) recording sessions are supported by the IP phones. Additionally, administrators have the option of enabling a Record-On-Demand feature allowing users to initiate and terminate a call recording session at their discretion. The call recording sessions are initiated by the voice recording system and when the session is established, the IP phone will duplicate all of its incoming and outgoing RTP/SRTP packets and send them to the voice recording system where they can be archived and analyzed as required.

Notes:

1. Please contact your MiVoice MX-ONE account manager for details on how to configure and utilize the Record-On-Demand feature.
2. As the RTP/SRTP packets sent to the voice recording system are duplicate copies, the codec used for the original call as well as the recording are identical as well. If active VoIP recording is required, ensure that the IP phone is configured to use the G.711 or G.729 codec as these are currently the only two codecs supported by ASC’s EVO*ip* 10.0 voice recording system.

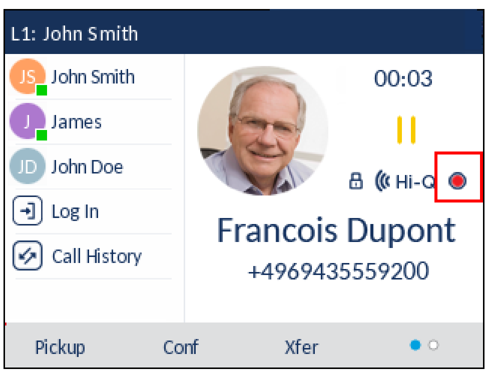
Administrators must configure a whitelist for voice recording system authentication using the “**recorder addressN**” parameters (where N is a number from 1 to 6). These parameters are used to specify trusted IP addresses corresponding to the voice recording system. The IP phone will check and respond to SIP messages coming from these IP addresses. If all of these parameters are left undefined, the active VoIP recording feature is disabled.

A whitelist can also be configured for RTP/SRTP packet destination authentication using the "**recording destinationN**" parameters (where N is a number from 1 to 6). These parameters are used to specify trusted IP addresses corresponding to the destination where the RTP/SRTP packets should be sent. The IP phone will check to see if the destination IP addresses are trusted before sending the duplicated RTP/SRTP packets. If all of these parameters are left undefined, no authentication checks will be performed.

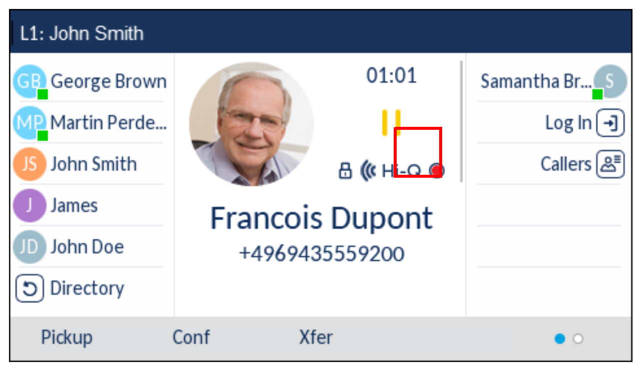
When a recording session is in progress, the respective IP phones display the following recording icons on screen:

6863i/6865i/6905/6910

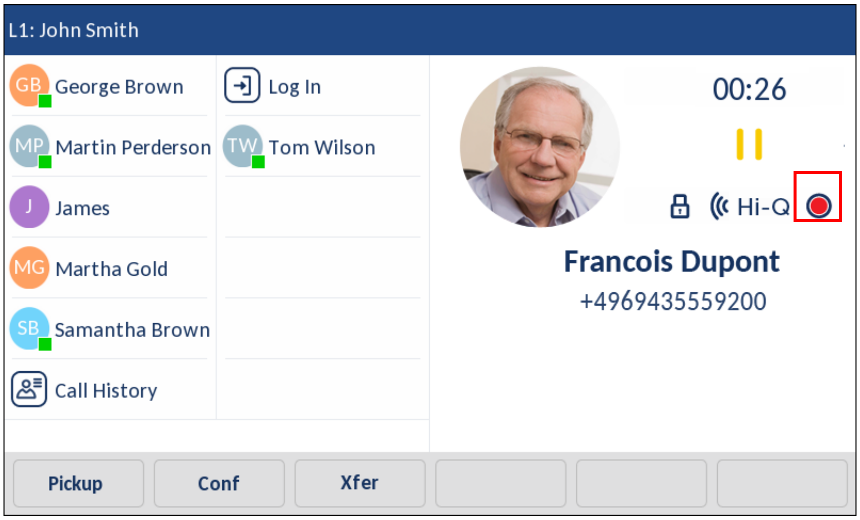
6867i



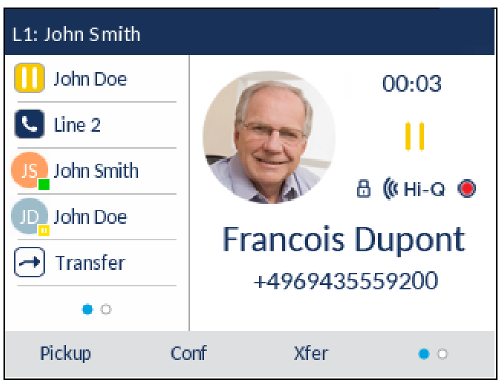
6869i



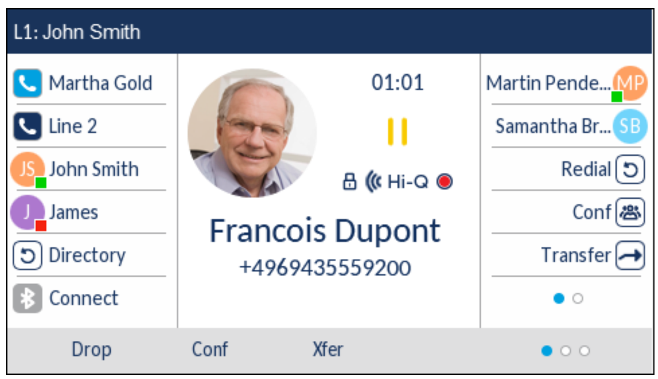
6873i



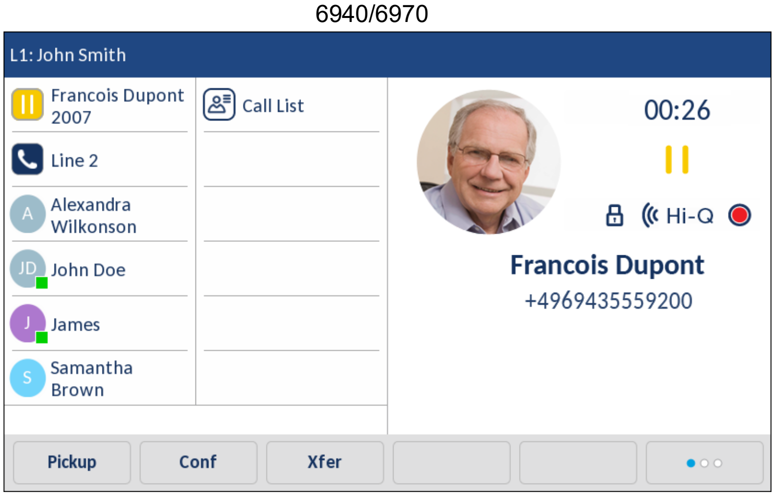
6920



6930



6940/6970



WARNING:THE RECORDING ICON IS DISPLAYED ON THE IP PHONES TO INDICATE THE RECORDING SESSION IS ACTIVE AND THAT A DUPLICATE COPY OF THE RTP/SRTP STREAM IS TO BE SENT FROM THE PHONE TO THE RECORDING SERVER. THE OVERALL RECORDING AND ITS QUALITY IS DEPENDENT ON THE RECORDING SERVER AND THE NETWORK.

Moreover, the phone will, by default, play a periodic audible beep tone through the selected audio path notifying users that their call is being recorded. Playback of the beep tone is configurable and if required, administrators can disable or set the playback interval of the beep tone by defining the "**recording periodic beep**" parameter in the configuration files. Additionally, by utilizing the "**recording beep direction**" parameter, administrators can define whether the beep tone is audible locally, remotely, or both.

Note: In addition to the aforementioned parameters corresponding to the active IP voice recording feature, the transport protocol parameters for SIP services (i.e. "**sip services transport protocol**" and "**sip services port**") must also be defined in the configuration files. See "Configurable Transport Protocol for SIP Services and RTCP Summary Reports" on page 6-54 for more information.
To use TLS transport for voice recording, "sip services transport protocol" parameter should be set to value 4, See SIP Services/RTCP Summary Reports Transport Protocol Settings See on page A-331for more information. In order to establish TLS connection with the phone, voice recording server must install a Mitel provided root certificate so that it can trust the certificate offered by the phone during SSL handshake. This certificate may be downloaded from the Software Download Center accessible through Mitel MiAccess Portal.

Use the following procedure in the configuration files to configure the active VoIP recording feature.

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, "Active VoIP Recording Settings" on page A-333.

BROADSOFT XSI FEATURES

XSI BASIC CONFIGURATION

Xsi features must first be configured using the Xtended Services Platform.

Note: Refer to the respective Xtended Services Platform documentation for information on how to configure the respective Xsi features on the BroadSoft BroadWorks call manager.

After configuring the desired Xsi feature information using the Xtended Services Platform, Administrators must enable basic Xsi interoperability on the phone by defining the following Xsi credential parameters:

- xsi user name (can also be entered using the Phone UI)
- xsi ip

- xsi port
- xsi protocol

Entering Usernames/Passwords and Connection Testing

Before the BroadSoft Xsi features can be utilized, user credentials (i.e. username and password) for BroadSoft Xsi will need to be entered using the phone's UI by navigating to the *Options* > *Credentials* menu. For the 6867i, 6869i, and 6873i this menu also allows users to test their connection to the Xsi server.

Use the following procedure on the phone's UI to enter user credentials and test the connection to the Xsi server.

IP PHONE UI

For the 6863i/6865i:

1. Press on the phone to enter the Options List.
2. Navigate to the **Credentials** option and press the **Enter** key.
3. Use the key to navigate to the **BroadSoft Xsi** option and press the **Enter** key.
4. Press the key to highlight the **Username** field and press the **Enter** key.
5. Use the dialpad keys to enter in your username and press the **Set** key when finished.
6. Press the key to highlight the **Password** field and press the **Enter** key.
7. Use the dialpad keys to enter in your password and press the **Set** key when finished.
8. Press the key to exit the Options List.

For the 6867i/6869i:

1. Press on the phone to enter the Options List.
2. Navigate to the **Credentials** option and press the button or **Select** softkey.
3. Use the key to navigate to the **BroadSoft Xsi** tab.
4. Press the key to highlight the **Username** field and using the dialpad keys (or K680i Keyboard if available) enter in your username.
5. Press the key to highlight the **Password** field and using the dialpad keys (or K680i Keyboard if available) enter in your password.
6. Press the key to navigate back to **BroadSoft Xsi** tab, and press the key until you get to the **Test Connection** tab.
7. Press the key to highlight **BroadSoft Xsi** and press the button to enable testing on that source.
8. Press the **Test** softkey to begin testing.
   A green ✔ will appear if there are no issues with the connection to the server.
   A red **!** will appear if issues are found.

If there are issues with your connection, please check your username, password, and/or server configuration.

9. Press the **Save** softkey to save your changes.

For the 6873i:

1. Press ⚙ on the phone to enter the Options List.
2. Press the **Credentials** icon.
3. Use the right arrow key to navigate to the **BroadSoft Xsi** tab.
4. In the **Username** field enter in the username applicable to the Directory source.
5. In the **Password** field enter in the password applicable to the Directory source.
6. Press the **BroadSoft Xsi** tab, and press the right arrow key until you get to the **Test Connection** tab.
7. Press the **BroadSoft Xsi** checkbox.
8. Press the **Test** softkey to begin testing.
   A green ✔ will appear if there are no issues with the connection to the server.
   A red **!** will appear if issues are found.
   If there are issues with your connection, please check your username, password, and/or server configuration.
9. Press the **Save** softkey to save your changes.

BROADSOFT BROADWORKS XSI SIP AUTHENTICATION

Users wanting to use BroadSoft BroadWorks Xsi features can authenticate to the respective Xsi account by manually entering in their credentials or authentication be automated by using the user's SIP credentials.

Notes:

1. To support Xsi SIP authentication, the BroadSoft BroadWorks call manager must have the "**allowSIPauthentication**" feature enabled. This can be verified by running the below CLI command:

```
XSP_CLI/Applications/Xsi-Actions/BWIntegration/get
allowSIPAuthentication
```

   and can be enabled by entering the following command:

```
XSP_CLI/Applications/Xsi-Actions/BWIntegration/set
allowSIPAuthentication true
```

2. Refer to the respective Xtended Services Platform documentation for information on how to configure the respective Xsi features on the BroadSoft BroadWorks call manager.

By enabling the "**xsi allow sip authentication**" parameter and defining "**sip xsi user name"** (global parameter) or "**sip lineN xsi user name**" (per-line parameter where N = line number), the phone will send the configured (global or per-line) BroadWorks Xsi user name along with the (global or per-line) SIP authentication user name and password to authenticate the Xsi account. Users will not need to manually enter a separate user name or password to use the Xsi-related features and services.

Global example:

```
xsi allow sip authentication: 1
sip xsi user name: 5553456@xsi.broadworks.net
sip auth name: 5553456
sip password: 123456
```

Per-line example:

```
xsi allow sip authentication: 1
sip line1 xsi user name: 5553456@xsi.broadworks.net
sip line1 auth name: 5553456
sip line1 password: 123456
sip line2 xsi user name: 5551234@xsi.broadworks.net
sip line2 auth name: 5551234
sip line2 password: 654321
```

Notes:

1. The “**xsi allow sip authentication**” parameter is disabled by default.
2. As detailed in the examples above, the user name portion of the "**sip xsi user name**" and "**sip lineN xsi user name**" parameters corresponds to the same value as the "**sip auth name**" and "**sip lineN auth name**".
3. If using a per-line XSI SIP authentication configuration, depending on which line is in focus on the phone, the Xsi features will reflect the account that has been configured for that line. For example, with Xsi Basic Calls Logs enabled, pressing the Callers List key on the phone when Line 3 is in focus on the phone will display the call logs for the account configured for Line 3.

XSI APPLICATION UPDATE FOR CALL ID BEHAVIOR WITH MULTIPLE ACCOUNTS

An enhancement is made to the existing XSI application (directory, call log and speeddial8) to consider screen focus while dialing out as opposed to using the first idle line with multiple accounts or XSI directories.

Screen focus is only considered when xsi is configured per line. This feature is supported only when “**xsi allow sip authentication**” is enabled.

In case of speeddial8, user can specify the line number as part of the speeddial8 softkey configuration. If the line number is configured as 'global', then the screen focus is used as the line for dialing out.

SPEED DIAL 8

Interoperability support for the BroadSoft Xsi Speed Dial 8 service has been introduced for the SIP phones. When the respective speed dial information is configured on the BroadSoft BroadWorks call manager and the phone is configured for Xsi interoperability, users can simply place an outgoing call to a speed dial number by pressing the Speed Dial 8 key and then pressing and holding the corresponding speed dial key on the dialpad. Alternatively, users can select the desired number and then press the Dial softkey (for the 6867i/6869i/6873i), button (if applicable), Line button, button, or simply pick up the handset.

To specifically enable the Speed Dial 8 service, Administrators must define the “**xsi speeddial8 enabled**” parameter in the respective configuration file and users must enter in their username (if required) and password on the phone through the *Options* > *Credentials* menu.

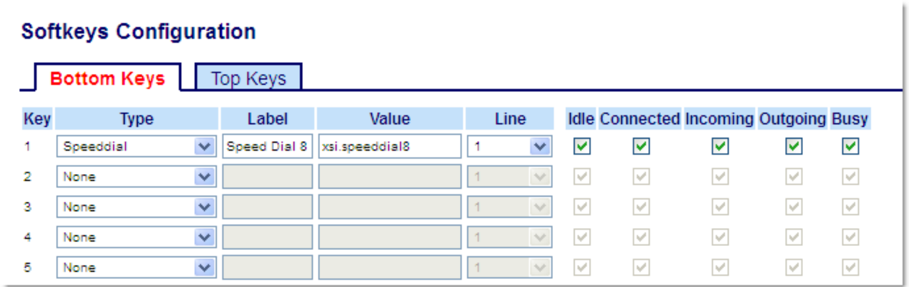
For Speed Dial 8 functionality, a Speed Dial 8 key should be configured for easy access to the Speed Dial 8 menu. Users and Administrators can configure a Speed Dial 8 key using the Web UI, selecting a desired key, changing the type to “Speeddial” and then entering “xsi.speeddial8” in the Value field.

Creating a Speed Dial 8 key Key Using the Mitel Web UI

Use the following procedure to create a Speed Dial 8 softkey using the Mitel Web UI:

MITEL WEB UI

1. Click on **Operation > Programmable Keys.**
   or
   Click on **Operation->Softkeys and XML**.



2. Select the key you want to use as a Speed Dial 8 key.
3. In the **Type** field, select **Speeddial** to apply to the key.
4. (Optional for the 6867i/6869i/6873i) In the **Label** field, enter a label to apply to this key.
5. In the **Value** field, enter “**xsi.speeddial8**”.
6. (Optional) In the **Line** field, select a line to apply to this key.
7. Click **Save Settings**.

Administrators also have the added option of configuring a Speed Dial 8 key by defining the "**prgkeyN type**", “**softkeyN type**” or “**topsoftkeyN type**” parameter as “speeddial” and "**prgkeyN value**", “**softkeyN value**” or “**topsoftkeyN value”** to “xsi.speeddial8” in the respective configuration file.

Notes:

1. Speed Dial 8 key Label and Line values are optional.
2. For details on how to configure speeddial keys using the configuration files see "Programmable Key Settings," on page 259, "Softkey Settings," on page 249, and "Top Softkey Settings," on page 265.

BASIC CALL LOGS

The BroadSoft Xsi Basic Call Log service is interoperable with the 6800 SIP phones. When configured on the BroadSoft BroadWorks call manager and enabled on the phone, the phone’s native Received Callers List and Outgoing Redial List are replaced with call information provided by the Xsi server.

The Received Callers List for all phones will show the name and number of the incoming caller, and specifically for the 6867i, 6869i, and 6873i the date and time of the call. 6867i, 6869i, and 6873i users are able to copy an entry to the Local Directory or edit an entry in the Received Callers List using the Copy and Edit softkeys exactly the same way as in the phone’s native Received Callers List.

The Outgoing Redial List for all phones will show the name and number of the outgoing call recipient, and the date and time of when the call was placed. 6867i, 6869i, and 6873i users are able to copy an entry to the Local Directory using the Copy softkey exactly the same way as in the phone’s native Outgoing Redial List.

Moreover, both lists for the 6867i, 6869i, and 6873i allow users to view more details of the respective call by pressing the right navigation key (or for the 6873i, pressing the right arrow button or Details softkey). All phone users can dial out by pressing the ✓ button, Line button, 🔈/🎧 button, or simply by picking up the handset (the Outgoing Redial List for the 6867i, 6869i, and 6873i also offers a Dial softkey).

Note: For more information regarding general Received Callers and Outgoing Redial List functionality (copy, edit, dialing, navigation, etc...) please see your model-specific *SIP Phone User Guide*.

To specifically enable the Basic Call Log service, Administrators must define the "**xsi calllogs enabled**" parameter in the respective configuration file and users must enter in their username (if required) and password on the phone through the *Options* > *Credentials* menu.

HIDE NUMBER

The BroadSoft BroadWorks Xsi Hide Number feature is supported by the SIP phones. By turning the Hide Number feature on (found in Options > BroadSoft Call Settings > Hide Number), users are able to place anonymous calls whereby the user's caller ID will not be displayed on the called party's phone.

To specifically enable the Hide Number feature, Administrators must define the "**xsi hide number enabled**" parameter in the respective configuration file and users must enter in their username (if required) and password on the phone through the *Options* > *Credentials* menu.

Enabling/Disabling the Hide Number Feature Using the Phone UI

IP PHONE UI

Use the following procedure on the phone's UI to enable/disable the Hide Number feature.

For the 6863i/6865i:

1. Press the ⚙ key on the phone to enter the Option List.
2. Select **BroadSoft Call Settings**.
3. Select **Hide Number.**
4. Use the ▲ and ▼ keys to select either **Disable** or **Enable**
5. Press the ✓ key or select 4**Set.**
   Your selection will be immediately applied to the phone.

For the 6867i/6869i:

1. Press ⚙ on the phone to enter the Options List.
2. Navigate to the **BroadSoft Call Settings > Hide Number** option and press the ✓ button or **Select** softkey.
3. With **Hide Number** highlighted press the 4 key to move to selection column.
4. Use the ▲ and ▼ keys to select either **Disable** or **Enable**.
5. Press the **Save** softkey to save your changes.

For the 6873i:

1. Press on the phone to enter the Options List.
2. Press the **BroadSoft Call Settings** icon.

> **Note:** For more information regarding general Received Callers and Outgoing Redial List functionality (copy, edit, dialing, navigation, etc...) please see your model-specific *SIP Phone User Guide*.

3. Press the **Hide Number** icon.
4. Select either **Disable** or **Enable**.
5. Press the **Save** softkey to save your changes.

INTEROPERABILITY SUPPORT FOR JOINING/UNJOINING BROADSOFT BROADWORKS XSI CALL CENTERS

The 6800 series SIP phones support the joining and unjoining of BroadSoft BroadWorks call centers using the BroadSoft BroadWorks Xsi API. To specifically enable call center join/unjoin capabilities on the phone, Administrators must define the "**xsi call center**" parameter in the respective configuration file as "1".

Keys (programmable keys [6865i], top softkeys [6867i, 6869i, and 6873i], hard keys [all phone models], and expansion module keys [M680i and M685i]) must then be configured (either through the configuration files or through the phone's Web UI) with call center functionality. Administrators can define the key type as "callcenter" (configuration files) or "Call Center" (Web UI) and, for the 6867i, 6869i, and expansion modules, define the key label with any desired label. A value for the key must be defined and must be identical to the call center ID value configured for the specific user in the BroadSoft BroadWorks call manager software. The following parameters are examples you can use to configure the call center keys:

For programmable keys (6865i)

prgkey1 type: callcenter
prgkey1 value: salesCC

prgkey2 type: callcenter
prgkey2 value: supportCC

For top softkeys (6867i, 6869i, and 6873i)

topsoftkey1 type: callcenter
topsoftkey1 label: Sales CC
topsoftkey1 value: salesCC

topsoftkey2 type: callcenter
topsoftkey2 label: Support CC
topsoftkey2 value: supportCC

For hard keys (6863i, 6865i, 6867i, 6873i, and 6869i)

hardkey1 type: callcenter
hardkey1 value: salesCC

hardkey2 type: callcenter
hardkey2 value: supportCC

For expansion module keys (M680i and M685i)

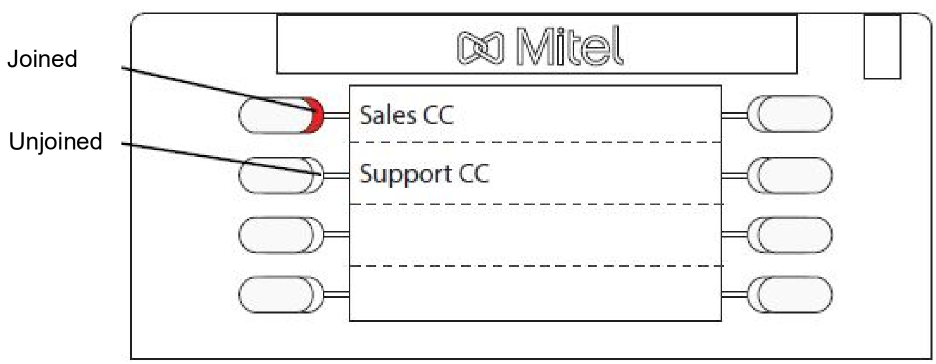
expmod1 key1 type: callcenter
expmod1 key1 label: Sales CC
expmod1 key1 value: salesCC

expmod1 key2 type: callcenter
expmod1 key2 label: Support CC
expmod1 key2 value: supportCC

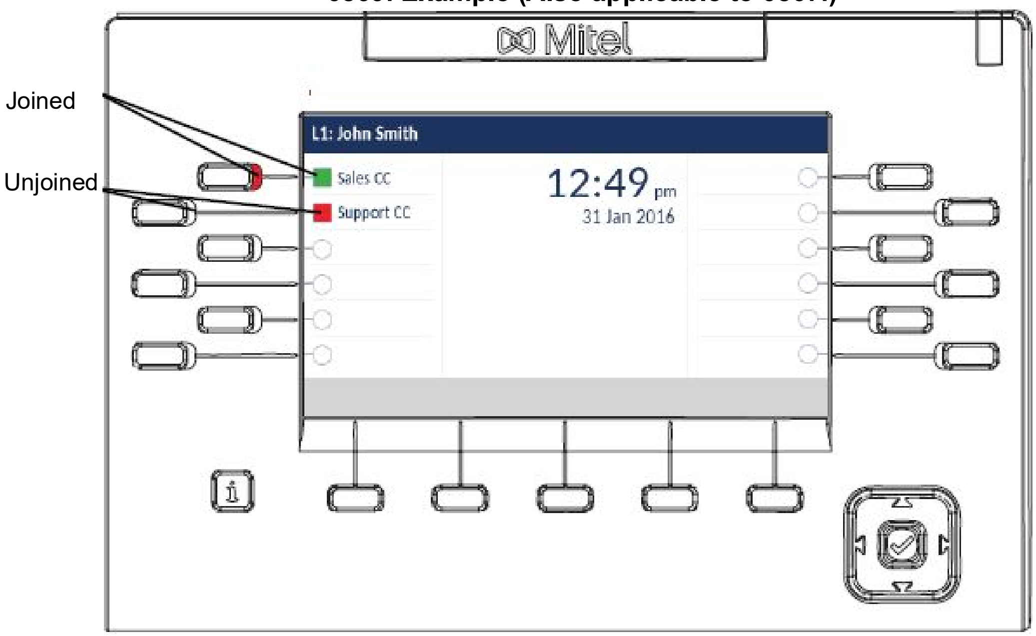
When the keys have been configured using the configuration files and the phone has been booted, the phone will indicate the Call Center join status through the configured keys' LEDs (not applicable to the 6873i). The 6867i, 6869i, and 6873i SIP phones will also provide indication of the join status through the color of the softkey's icon.

Note: If you are using the phone's Web UI to configure call center keys, after saving your changes, a reboot will be required to ensure that the join status of the call center key on the phone is synchronized with the call center join status configured on the BroadSoft BroadWorks call manager.

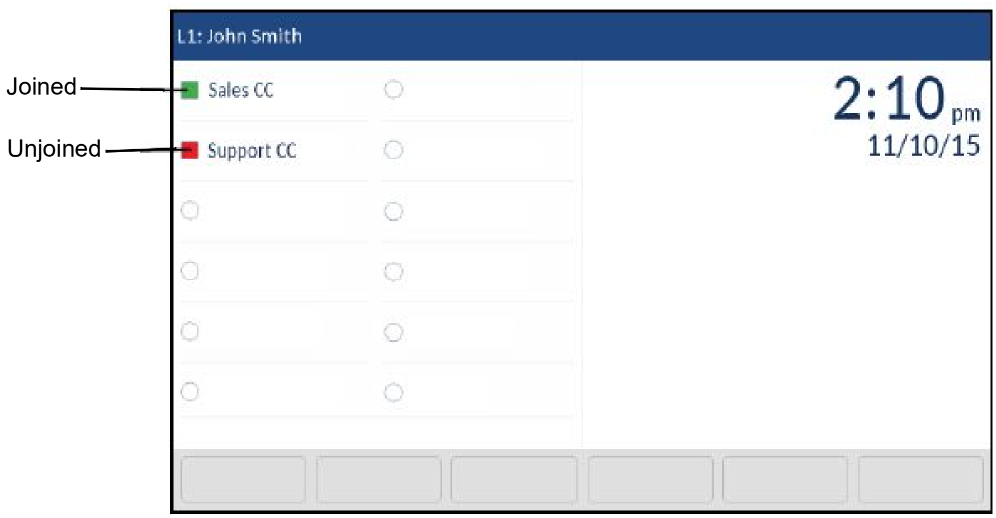
6865i Example



6869i Example (Also applicable to 6867i)



6873i Example



Join status indications for the phones are as follows:

STATUS	LED STATE (M680i AND ALL PHONES EXCEPT 6873i)	SOFTKEY ICON STATE (6867i, 6869i, 6873i, AND M685i)
Joined	On	
Unjoined	Off	

STATUS	LED STATE (M680i AND ALL PHONES EXCEPT 6873i)	SOFTKEY ICON STATE (6867i, 6869i, 6873i, AND M685i)
Status Not Synchronized	Off	
Call Center ID Misconfigured	Off	

Pressing the desired call center key will toggle between joining and unjoining the respective call center.

BROADSOFT BROADWORKS REMOTE OFFICE SUPPORT

Note: This service is applicable to the 6867i, 6869i, and 6873i SIP Phones.

The BroadSoft BroadWorks Remote Office service is supported by the 6800 series SIP phones. The BroadWorks Remote Office service allows users the ability to use any remote end-point device as their office phone. Users can define a remote office number or SIP-URI whereby all incoming calls to their SIP phone will be automatically forwarded to the defined remote office number/SIP-URI.

To specifically enable Remote Office support on the phone, Administrators must define the "**xsi remote office**" parameter in the respective configuration file as "1". When enabled, users have the ability to enable and disable Remote Office functionality as well as change the Remote Office number/SIP-URI through the phone's native UI.

Configuring the Remote Office Service Using the Phone UI

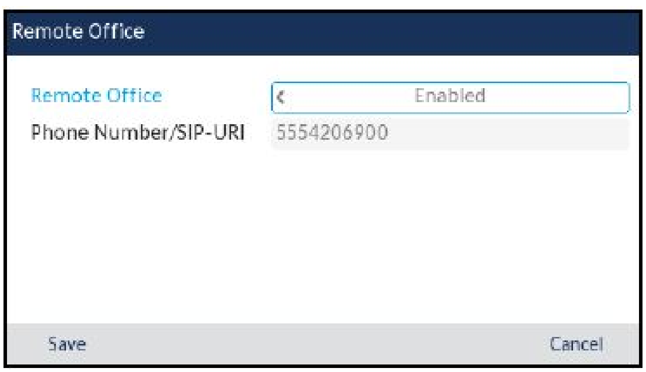
IP PHONE UI

Use the following procedure on the phone's UI to configure Remote Office service.

For the 6867i/6869i:

1. Press on the phone to enter the Options List.
2. Navigate to the **BroadSoft Call Settings > Remote Office** option and press the button or **Select** softkey.

6869i Example



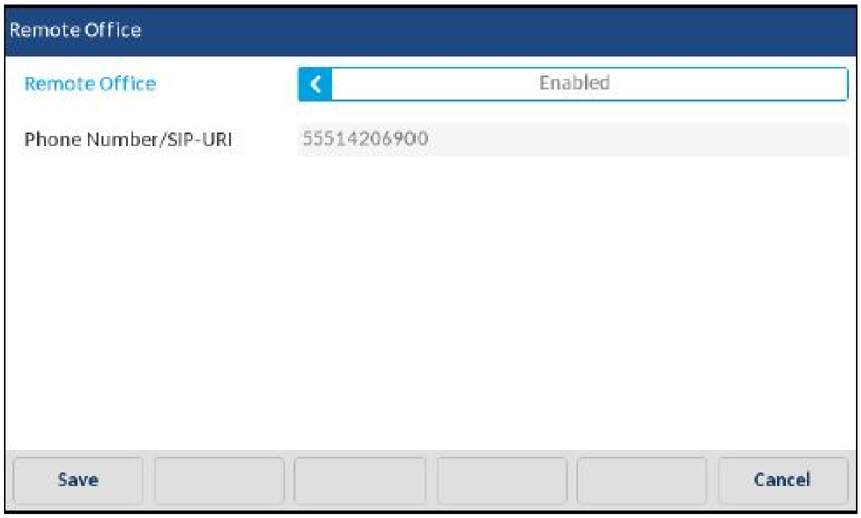
3. In the **Remote Office** field press the 3 or 4 key enable or disable the service.
4. Press the key to highlight the **Phone Number/SIP-URI** field and using the dialpad keys enter the phone number or SIP-URI you want all incoming calls to be forwarded to.
5. Press the **Save** softkey to save your changes.

For the 6873i:

1. Press on the phone to enter the Options List.
2. Press the **BroadSoft Call Settings** icon.

Note: If required, swipe right to switch pages in the Options List.

3. Press the **Remote Office icon**.



4. Press the and arrow buttons in the **Remote Office** field to enable or disable the service.
5. Press the **Phone Number/SIP-URI** field and using the on-screen keyboard or dialpad keys enter the phone number or SIP-URI you want all incoming calls to be forwarded to.
6. Press the **Save** softkey to save your changes.

BROADSOFT BROADWORKS SIMULTANEOUS RING PERSONAL SUPPORT

Note: This service is applicable to the 6867i, 6869i, and 6873i SIP Phones.

The BroadSoft BroadWorks Simultaneous Ring Personal service is supported by the 6800 series SIP phones. The BroadWorks Simultaneous Ring Personal service allows users the ability to define up to 10 phone numbers or SIP-URIs and independently set which phone numbers should ring when a call is incoming to their primary phone.

To specifically enable Simultaneous Ring Personal support on the phone, Administrators must define the "**xsi simultaneous ring personal**" parameter in the respective configuration file as "1". When enabled, users have the ability to enable and disable simultaneous ring functionality for up to 10 phone numbers. Users can also specify whether or not simultaneous ringing should occur when on an active call.

Configuring the Simultaneous Ring Personal Service Using the Phone UI

IP PHONE UI

Use the following procedure on the phone's UI to configure Simultaneous Ring Person service.

For the 6867i/6869i:

1. Press on the phone to enter the Options List.
2. Navigate to the **BroadSoft Call Settings > Simultaneous Ring** option and press the button or **Select** softkey.

6869i Example

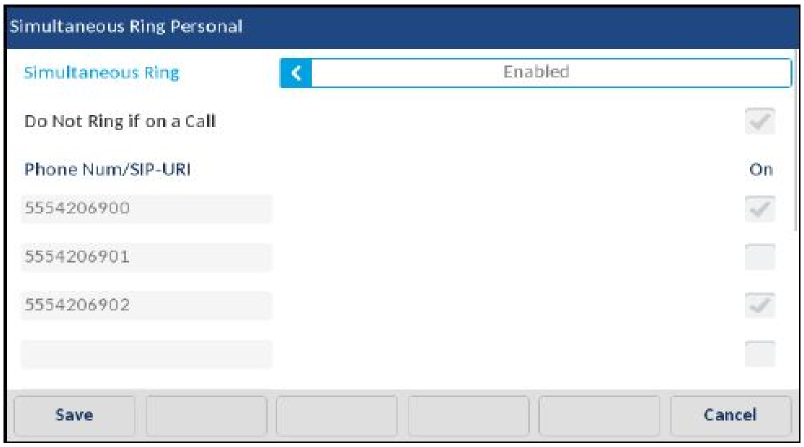
3. In the **Simultaneous Ring** field press the 3 or 4 key enable or disable the service.
4. Press the key to highlight the **Do Not Ring if on a Call** field and press the button to enable this functionality.
5. Press the key to highlight the **Phone Num/SIP URI** field and using the dialpad keys enter the phone number or SIP-URI you want to apply simultaneous ring functionality to.
6. Press the key to highlight the corresponding **Phone Num/SIP URI** checkbox and press the button to enable simultaneous ring functionality for the respective phone number/SIP URI.
7. Repeat Steps 5 and 6 for any additional phone numbers or SIP URIs you want to configure.
8. Press the **Save** softkey to save your changes.

For the 6873i:

1. Press on the phone to enter the Options List.
2. Press the **BroadSoft Call Settings** icon.

Note: If required, swipe right to switch pages in the Options List.

3. Press the **Simultaneous Ring** icon.



4. Press the ◀ and ▶ arrow buttons in the **Simultaneous Ring** field to enable or disable the service.
5. Press a **Phone Num/SIP-URI** field and using the on-screen keyboard or dialpad keys enter the phone number or SIP-URI you want to apply simultaneous ring functionality to.
6. Repeat Step 5 for any additional phone numbers or SIP URIs you want to configure.
7. Press the checkboxes beside any desired **Phone Num/SIP-URI** fields to enable simultaneous ring functionality for the respective phone numbers/SIP URIs.
8. Press the **Save** softkey to save your changes.

BROADSOFT BROADWORKS ANYWHERE SUPPORT

Note: This service is applicable to the 6867i, 6869i, and 6873i SIP Phones.

The BroadSoft BroadWorks Anywhere service is supported by the 6800 series SIP phones. The BroadWorks Anywhere service allows users the ability to make and receive calls using one number, regardless of the device being used. When enabled on the phone, users are able to configure the BroadWorks Anywhere service directly through the phone's native UI.

To specifically enable BroadWorks Anywhere support on the phone, Administrators must define the "**xsi broadworks anywhere**" parameter in the respective configuration file as "1". When enabled, users are able to view the BroadWorks Anywhere settings on the phone through the Options List > BroadSoft Call Settings > BroadWorks Anywhere menu. Settings that can be viewed or configured on the main BroadWorks Anywhere menu include:

- **Portal Number**: The read-only access number to the BroadWorks Anywhere portal. Users dial the portal number before the destination number so that their call is routed through the BroadWorks Anywhere service. The called party will see the user's office caller ID information instead of the caller ID of the device they are actually calling from.
- **Alert Locations for Click-to-Dial**: Enable/disable the feature whereby the user's BroadSoft Anywhere devices will be alerted when a click-to-dial button on a webpage or toolbar is pressed.
- **Alert Locations for Group Paging**: Enable/disable the feature whereby the user's BroadSoft Anywhere devices will be alerted when a group page is incoming.
- **Phone Numbers**: The list of phone numbers/locations the respective user will use to call the BroadWorks Anywhere portal. The portal will allow users to route calls only if it is accessed by one of the configured known numbers/locations. These numbers/locations can be defined and enabled/disabled individually by navigating to the phone number field and pressing the **Edit** softkey. By default, 10 numbers/locations can be viewed/configured on the phone. Administrators can define the number of phone numbers/locations that can be viewed/configured through the phone's UI by using the "**xsi broadworks anywhere locations**" parameter (the range being from 1 to 25).

  Note: In scenarios where the BroadWorks call manager has more numbers defined than the number of locations configured to be displayed on the phone, the phone will display the configured number of locations starting from the first defined in the call manager. For example, if the call manager has 25 numbers defined and the "**xsi broadworks anywhere locations**" parameters is defined as 10 for the phone, the first 10 locations defined in the call manager will be displayed on the phone.

When adding or editing the phone numbers/locations, the following settings can be defined:

- **Phone Number**: A phone number the respective user will use to call the BroadWorks Anywhere portal.
- **Description**: A description of the phone number, usually a location or type of number (e.g. "Home" or "Cell").
- **On**: Sets whether the number/location should be enabled for the BroadWorks Anywhere service.

- **Alternate Number**: An outbound alternate phone number or SIP-URI that when defined will ring when the SIP phone rings.
- **Call Control**: When enabled, call control services will be performed by the BroadWorks Anywhere location.
- **Diversion Inhibitor**: When enabled, the respective location will be prevented from redirecting or forwarding incoming calls to another even if call forward is activated.
- **Answer Confirmation**: When enabled, the BroadWorks call manager will prompt for an answer confirmation when an incoming call is answered by the respective location.

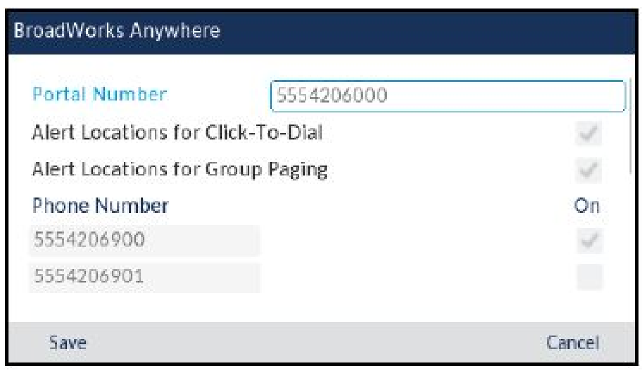
Configuring the BroadSoft Anywhere Service Using the Phone UI

Use the following procedure on the phone's UI to configure the BroadSoft Anywhere service.

For the 6867i/6869i:

1. Press on the phone to enter the Options List.
2. Navigate to the **BroadSoft Call Settings > BroadSoft Anywhere** option and press the button or **Select** softkey.

6869i Example

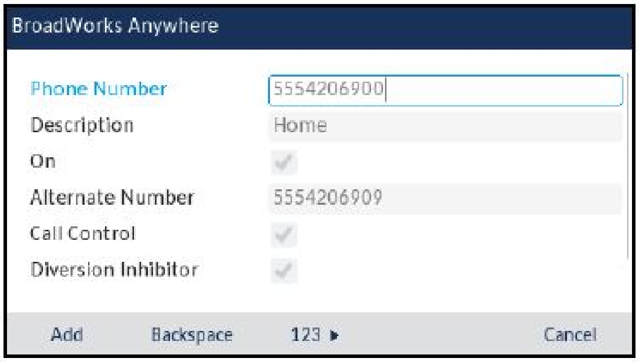


3. Press the key to highlight the **Alert Locations for Click-to-Dial** checkbox and if desired press the button to enable this functionality.
4. Press the key to highlight the **Alert Locations for Group Paging** checkbox and if desired press the button to enable this functionality.

To add or edit a phone number:

5. Press the ▲ key to highlight the desired **Phone Number** field and press the **Edit** softkey.

6869i Example



6. Using the dialpad keys enter or edit the phone number.

> **Note:** To move the cursor one digit/character to the right, press the ▶ navigation key. To erase one digit/character to the left of the cursor, press the **Backspace** softkey.

7. Press the ▲ key to highlight the **Description** field and using the dialpad keys enter or edit the description.

8. Press the ▲ key to highlight the **On** checkbox and press the ☑ button to enable the location for BroadSoft Anywhere.

9. Press the ▲ key to highlight the **Alternate Number** field and using the dialpad keys enter or edit the alternate number.

> **Note:** To move the cursor one digit/character to the right, press the ▶ navigation key. To erase one digit/character to the left of the cursor, press the **Backspace** softkey.

10. Press the ▲ key to highlight the **Call Control** checkbox and press the ☑ button to enable the feature. When enabled, call control services will be performed by the BroadWorks Anywhere location.

11. Press the ▲ key to highlight the **Diversion Inhibitor** checkbox and press the ☑ button to enable the feature. When enabled, the respective location will be prevented from redirecting or forwarding incoming calls to another even if call forward is activated.

12. Press the ▲ key to highlight the **Answer Confirmation** checkbox and press the ☑ button to enable the feature. When enabled, the BroadWorks call manager will prompt for an answer confirmation when an incoming call is answered by the respective location.

13. Press the **Add** softkey to save your changes.

14. Repeat Steps 5 to 13 for any additional phone numbers you want to configure.

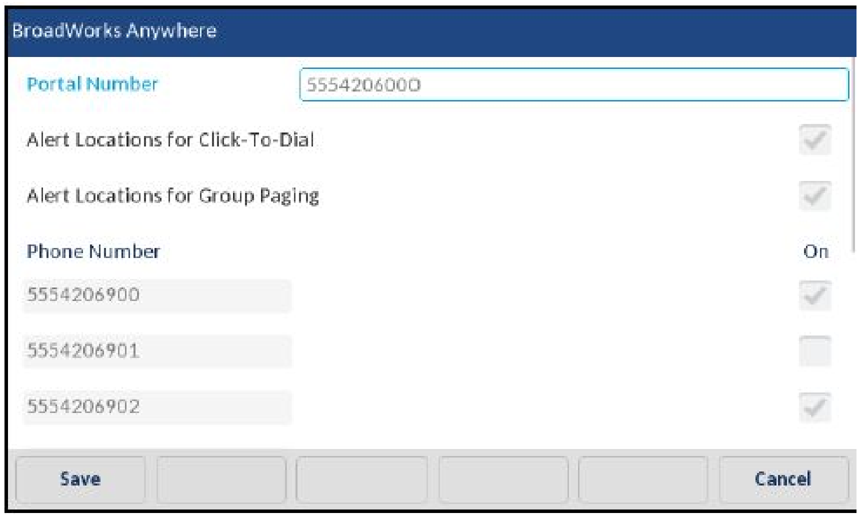
15. Press the **Save** softkey to save your changes.

For the 6873i:

1. Press  on the phone to enter the Options List.
2. Press the **BroadSoft Call Settings** icon.

Note: If required, swipe right to switch pages in the Options List.

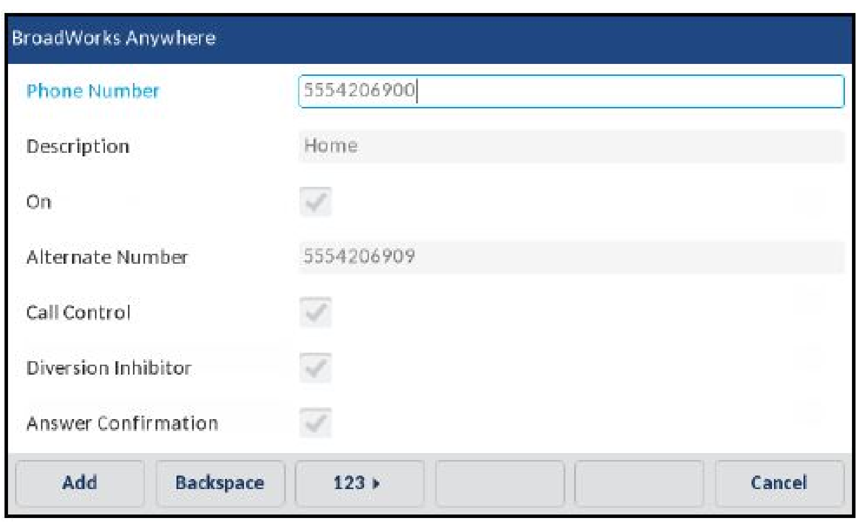
3. Press the **BroadWorks Anywhere** icon.



4. Press the **Alert Locations for Click-to-Dial** checkbox if desired to enable this functionality.
5. Press the **Alert Locations for Group Paging** checkbox if desired to enable this functionality.

To add or edit a phone number:

6. Press the desired **Phone Number** field and press the **Edit** softkey.



7. Using the on-screen keyboard or dialpad keys enter or edit the phone number.

8. Press the **Description** field and using the on-screen keyboard or dialpad keys enter or edit the description.
9. Press the **On** checkbox to enable the location for BroadSoft Anywhere.
10. Press the **Alternate Number** field and using on-screen keyboard or dialpad keys enter or edit the alternate number.
11. Press the **Call Control** checkbox if desired to enable the feature. When enabled, call control services will be performed by the BroadWorks Anywhere location.
12. Press the **Diversion Inhibitor** checkbox if desired to enable the feature. When enabled, the respective location will be prevented from redirecting or forwarding incoming calls to another even if call forward is activated.
13. Press the **Answer Confirmation** checkbox desired to enable the feature. When enabled, the BroadWorks call manager will prompt for an answer confirmation when an incoming call is answered by the respective location.
14. Press the **Add** softkey to save your changes.
15. Repeat Steps 6 to 14 for any additional phone numbers you want to configure.
16. Press the **Save** softkey to save your changes.

ENABLING XSI FEATURES USING THE CONFIGURATION FILES

You use the following procedure to enable Xsi feature support:

CONFIGURATION FILES

For the specific parameter you can set in the configuration files, see Appendix A, the section, “Xsi Feature Settings” on page A-335.

FEATURE RE-BRANDING SUPPORT FOR BROADSOFT-BASED SERVICE PROVIDERS

The 6800 series SIP phones support the configuration of a number of BroadSoft features through the native phone UI as well as the phone’s Web UI. References to these features in the respective UI may contain the strings "BroadSoft", "BSFT", or "BroadWorks" (e.g. "BroadSoft SCA", "BSFT Call Settings", or "BroadWorks Anywhere"). Starting with Release 4.3.0 SP1, service providers are able to replace these BroadSoft-related strings in the UI with their own custom branding names.

BroadSoft-related references on the phone can be categorized into three types:

- References using a full service provider name:
  - Used on the SIP phones when referencing a feature or option that encompasses the full service provider’s name.
  - The default string that is replaced when this value is defined is "BroadSoft".
  - For example, "BroadSoft Call Settings" on the 6867i, 6869i, and 6873i SIP phones as well as "BroadSoft SCA" and "BroadSoft Xsi" on all the 6800 series SIP phones.

- References using a short service provider name:
  - Used on the SIP phones when referencing a feature or option that encompasses a shortened version of the service provider's name.
  - The default string that is replaced when this value is defined is "BSFT".
  - For example, "BSFT Call Settings" on the 6863i and 6865i (as opposed to "BroadSoft Call Settings" on the 6867i, 6869i, and 6873i).
- References using a platform name:
  - Used on the SIP phones when referencing a feature or option that encompasses the name of the service provider's platform.
  - The default string that is replaced when this value is defined is "BroadWorks".
  - For example, "BroadWorks Anywhere" on the 6867i, 6869i, and 6873i SIP phones.

Service providers can re-brand these feature UI strings by defining the "broadsoft branding" parameter in the desired configuration file. The syntax of the parameter is as follows:

```
broadsoft branding: "<full name>;<short name>;<platform name>"
```

whereby the full, short, and platform name values are delimited by a semi-colon.

Note: To ensure the applicable UI strings are not truncated on the 6863i and 6865i, it is recommended to limit the character length of the short name value to four when the screen language is configured as English. Maximum character lengths may vary when a different screen language is configured.

For example, defining the parameter as:

```
broadsoft branding: "Mitel;MTL;MiVoice"
```

would result in the references "BroadWorks SCA", "BSFT Call Settings", and "BroadWorks Anywhere" being displayed as "Mitel SCA", "MTL Call Settings", and "MiVoice Anywhere" respectively.

If any or all of the three name values are not defined, the corresponding references will be left blank on the UI. For example, defining the parameter as:

```
broadsoft branding: ";MTL;"
```

would result in the references "BroadWorks SCA", "BSFT Call Settings", and "BroadWorks Anywhere" being displayed as "SCA", "MTL Call Settings", and "Anywhere" respectively.

As an alternate example, defining the parameter as:

```
broadsoft branding: ";;"
```

would result in the references "BroadWorks SCA", "BSFT Call Settings", and "BroadWorks Anywhere" being displayed as "SCA", "Call Settings", and "Anywhere" respectively.

Re-branding BroadSoft-Related Feature UI Strings

Use the following procedure to re-brand BroadSoft-related feature UI strings:

CONFIGURATION FILES

For the specific parameters you can set in the configuration files, see Appendix A, the section, "Settings for Re-Branding BroadSoft-Related Feature UI Strings" on page 340.

INTEROPERABILITY SUPPORT FOR XMPP-BASED BROADSOFT UC-ONE SERVICES

Note: This feature is applicable to the 6867i, 6869i, and 6873i SIP phones.

The 6867i, 6869i, and 6873i SIP phones are now interoperable with various Extensible Messaging and Presence Protocol (XMPP)-based BroadSoft UC-ONE services. The following UC-ONE services and features are supported by the SIP phones in Release 4.3.0 SP1 and greater:

- **Presence**: Users are able to see the presence information (i.e. state indicators and status text) for their UC-ONE contacts in various locations on the phone. The following presence states and corresponding indicators are as follows:

PRESENCE STATES	INDICATOR (COLOR)
Available	Green
Away	Orange
Busy	Yellow
Offline	Grey
Unknown	N/A

- **Contact List**: Users are able to view all their UC-ONE contacts by accessing a Contacts List. If applicable, contacts are categorized into groups that are definable through the UC-ONE desktop client. Contact details (e.g. presence information, names and user IDs, phone numbers, addresses, etc...) are also viewable through the Contacts List by navigating to the Details screen of the respective contact.
- **Favorites**: UC-ONE contacts that are defined as favorites can be viewed through the Contact List or can be assigned to specific softkeys so that their presence information can be seen on the idle/home screen.
- **My Status**: Users are able to see their own presence information on the phone and can change their presence states using the phone's native UI by accessing the My Status menu.
- **One Touch Dialing**: Pressing a Favorite softkey automatically dials out to the UC-ONE contact. Outgoing calls to any UC-ONE contact can also be made through the Contacts List.

- **Free Text Display**: Free status text that UC-ONE contacts have defined through their UC-ONE desktop client can be viewed in various locations on the phone.
- **Avatar Support**: Your own avatar can be viewed on the My Status softkey and avatars for UC-ONE contacts can be viewed on Favorite softkeys and within the Contacts List.

Notes:

1. Aside from changing your own presence state/status using the My Status feature, any other changes that need to be made (e.g. adding, removing, or editing contacts or groups, editing free text, uploading avatar images, etc...) must be made using the BroadSoft UC-ONE desktop client. Release 4.3.0 SP1 may be compatible with various versions of the UC-ONE desktop client, but has been tested and verified using Version 21.2.2.24.
2. The M680i and M685i expansion modules currently do not support this feature.
3. Integration of presence-related features with the phone’s Call History application is currently not supported.
4. Free text for both you and your contacts is not initially updated on the phone upon a reboot. The phone will reflect free text after a state change is made by you or your contacts using the UC-ONE desktop client.
5. Changes to avatars are displayed on the phone only after the phone has been rebooted.

CONFIGURING THE SIP PHONES FOR BASIC BROADSOFT UC-ONE INTEROPERABILITY

Before configuring the SIP phones for BroadSoft UC-ONE interoperability, ensure the BroadSoft BroadWorks call manager is configured and the BroadWorks BroadCloud and UC-ONE-related services are enabled. Additionally, ensure the SIP phones are registered with the proper proxy and registrar servers and configured with the proper SIP credentials.

Note: Refer to the respective BroadSoft documentation for information on how to configure the UC-ONE services on the BroadSoft BroadWorks call manager and the *6800 Series SIP Phone Administrator Guide* for information on how to configure basic SIP settings.

After the BroadSoft BroadWorks call manager has been configured and the BroadWorks BroadCloud and UC-ONE-related services have been enabled, Administrators must enable basic UC-ONE interoperability on the phone by defining the following parameters:

- **instant messaging and presence**
- **imp user name**
- **imp password**
- **imp ip**
- **imp port**

Enabling Basic UC-ONE Interoperability

Use the following procedure to enable basic UC-ONE interoperability:

CONFIGURATION FILES

For the specific parameters you can set in the configuration files, see Appendix A, the section, "UC-ONE Interoperability Settings" on page 341.

CONFIGURING UC-ONE CONTACTS, MY STATUS, AND FAVORITE SOFTKEYS

To access your UC-ONE Contacts List and to be able to see your own presence information along with the presence information of your UC-ONE favorite contacts on the idle/home screen, **Contacts**, **My Status**, and **Favorite** softkeys must be configured.

Contacts, My Status, and Favorite Softkeys - 6869i Example

Contacts, My Status, and Favorite Softkeys - 6873i Example

Any number of favorite softkeys can be configured (limited only by the number of available top softkeys on the respective phone). If the number of UC-ONE favorite contacts exceed the number of Favorite softkeys, the Favorite softkeys will be populated with as many of the user's UC-ONE favorite contacts. If the number of Favorite softkeys exceeds the number of UC-ONE favorite contacts, by default, the unused Favorite softkeys will not be populated and "???" labels will be displayed.

> **Note:** The **"keys noname hidden"** parameter, originally applicable to BLF/List softkeys, is also applicable to Favorite softkeys. When this parameter is enabled, the labels for the unused Favorite softkeys will be left blank instead of question marks being displayed. For more information on the **"keys noname hidden"** parameter, see "Configurable Display for Blank BLF/List and XMPP Presence-Related Favorite Softkeys" on page 196.

The phone assigns UC-ONE favorite contacts to the Favorite softkeys alphabetically based on the first name of the contact.

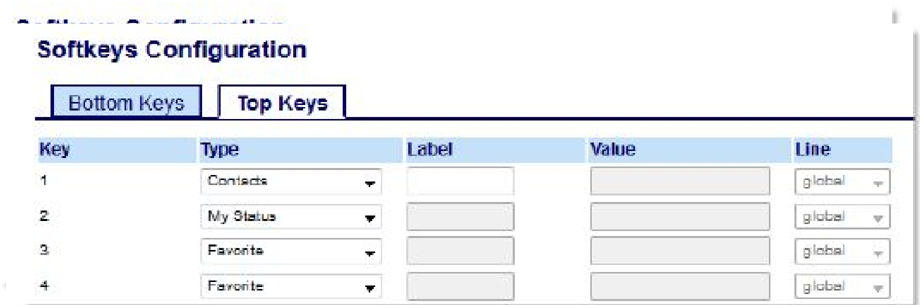
Users and Administrators can configure these softkeys using the phone's Web UI. Administrators have the additional capability of configuring these softkeys using the configuration files.

Configuring a Contacts Key Using the Mitel Web UI

Use the following procedure to configure a Contacts key using the Mitel Web UI.

MITEL WEB UI

1. Click on **Operation > Softkeys and XML > Bottom Keys** or **Top Keys**



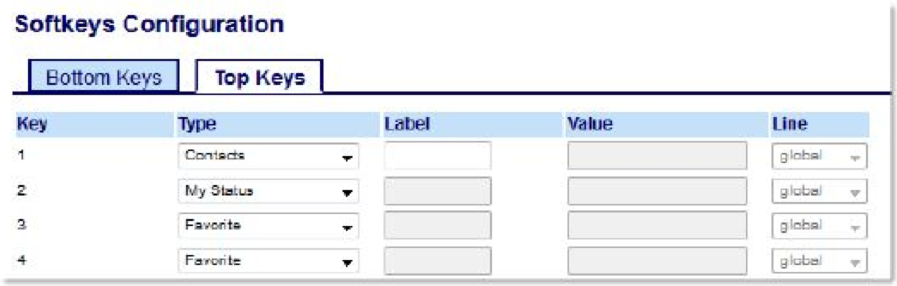
2. Select a top or bottom softkey.
3. In the **Type** field, select **Contacts**.
4. In the **Label** field, enter a label to display on the phone for the key (default is "Contacts").
5. Click **Save Settings**.

Configuring a My Status Key Using the Mitel Web UI

Use the following procedure to configure a Contacts key using the Mitel Web UI.

MITEL WEB UI

1. Click on **Operation > Softkeys and XML > Top Keys**



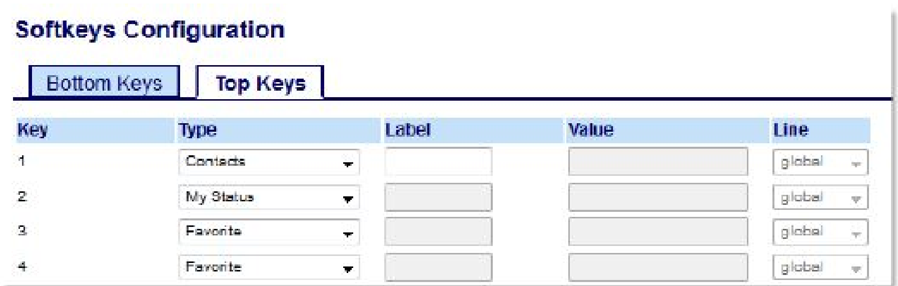
2. Select a top softkey.
3. In the **Type** field, select **My Status**.
4. Click **Save Settings**.

Configuring a Favorite Key Using the Mitel Web UI

Use the following procedure to configure a Contacts key using the Mitel Web UI.

MITEL WEB UI

1. Click on **Operation > Softkeys and XML > Top Keys**



2. Select a top softkey.
3. In the **Type** field, select **Favorite**.
4. Repeat Steps ▲ and ▼ navigation key for any other softkeys you would like to configure as a Favorite softkey.
5. Click **Save Settings**.

Use the following procedures to configure My Status, Contacts, and Favorite softkeys on the IP phone.

CONFIGURATION FILES

To configure a My Status, Contact, or Favorite softkey using the configuration files, see Appendix A, the section, “Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters” on page A-248.

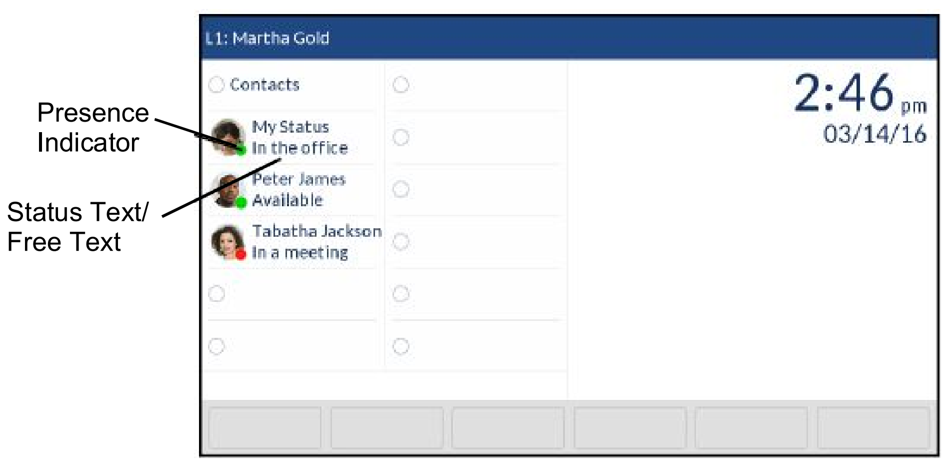
VIEWING AND CHANGING YOUR OWN PRESENCE INFORMATION ON THE PHONE

If a My Status softkey has been configured on your phone, the softkey will reflect your current presence state/status. On the 6867i and 6869i, the label and presence state indicator can be seen from the idle/home screen.

6869i Example

On the 6873i, in addition to the presence state indicator and the label, the My Status softkey will also display status text (either the default status text or the free text that has been entered in the UC-ONE desktop client).

6873i Example



If you press the My Status softkey, a menu appears whereby you can select the presence state you want to present to your UC-ONE contacts as well as any status text or free text that has been defined using the UC-ONE desktop client, if applicable.

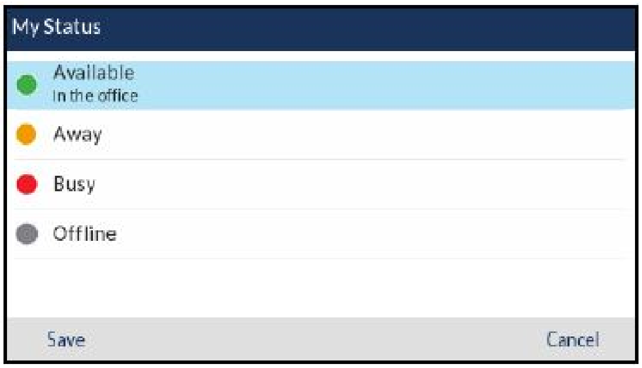
To Change Your Presence Status Using the IP Phone UI:

IP PHONE UI

For the 6867i and 6869i:

1. Press the softkey configured with My Status functionality.

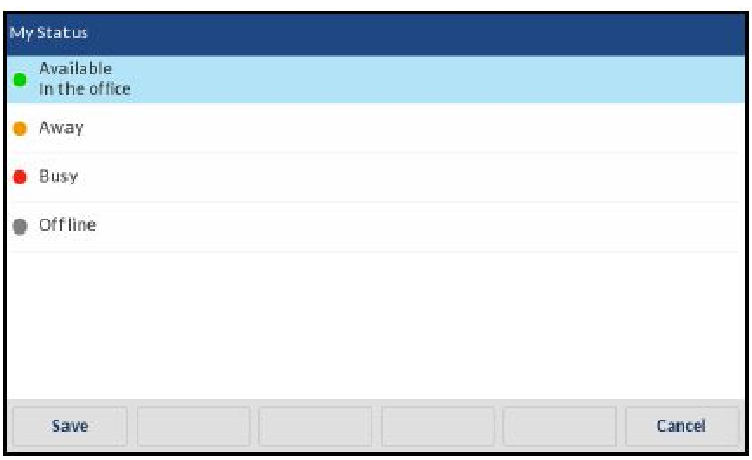
6869i Example



2. Use the ▲ and ▼ navigation keys to select the desired presence state/status.
3. Press the **Save** softkey.

For the 6873i:

1. Press the softkey configured with My Status functionality.



2. Press the desired presence state/status.
3. Press the **Save** softkey.

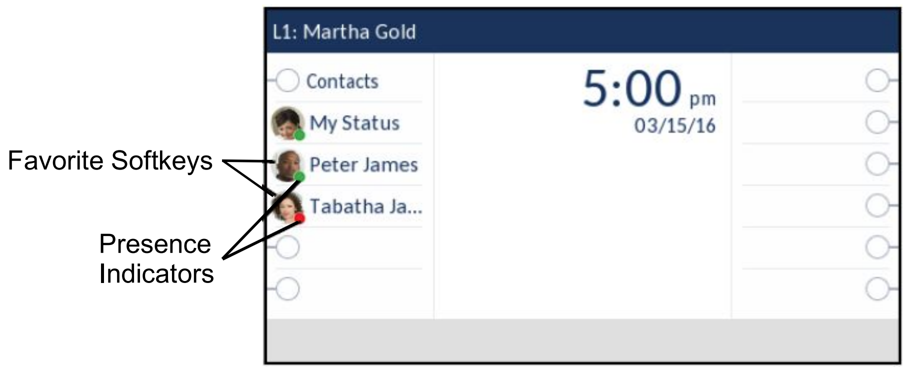
VIEWING AND DIALING FAVORITE CONTACTS USING YOUR FAVORITE SOFTKEYS

If you have configured Favorite softkeys, your UC-ONE contacts tagged as favorites will be populated to those softkeys and subsequently their presence information will be viewable on the idle/home screen.

Note: You cannot tag UC-ONE contacts as favorites using your phone. Favorites must be configured using your UC-ONE desktop client.

The Favorite softkeys display the same presence information as the My Status softkey, but for your favorite UC-ONE contacts. On the 6867i and 6869i, the names of your favorite contacts and their presence status indicators can be seen from the idle/home screen.

6869i Example



On the 6873i, in addition to the presence status indicators and the names, the Favorite softkeys will also display status text (either the default status text or the free text that has been entered in the UC-ONE desktop client by your favorite contacts).

At any time, pressing a populated Favorite softkey will initiate a call to the respective UC-ONE contact using the contact’s Work Extension number. If a Work Extension number is not defined, the phone will dial out using the Work Phone number, then the Mobile Phone number, and then lastly the Personal Phone number (whichever is defined first based on the described order).

USING THE CONTACTS LIST

The Contact List is a personal phone book that allows you to dial out quickly to any of your UC-ONE contacts as well as view all of your UC-ONE contacts' presence information within one application. If you have organized your UC-ONE contacts into different groups and tagged contacts as favorites using the UC-ONE desktop client, the same organizational structure is reflected in your Contact List on your phone. You can also view more detailed information for each individual contact (e.g. defined names, work/home address, Email address) by accessing the contact's Details screen. The Details screen also allows you to view and dial out to any additional phone numbers that a UC-ONE contact may have.

Notes:

1. The Contacts List is a read-only application. The UC-ONE desktop client must be used if you would like to make any changes to your contacts or your Contact List (e.g. add/edit/delete groups, add/edit/delete contact, tag favorites, edit free text, upload avatar images, etc...).
2. Favorite contacts are denoted by the yellow star icon in the Contacts List.
3. The Display Name Order setting found in the Options menu under Directory > Settings is applicable to the Contacts List. For example, setting the Display Name Order as "First Last" will display your contacts with their first name first and sort alphabetically using their first name. Setting the Display Name Order as "Last, First" will display your contacts with their last name first and sort alphabetically using their last name.

To View Your UC-ONE Contacts' Presence Information and Call a Contact Using the Contacts List

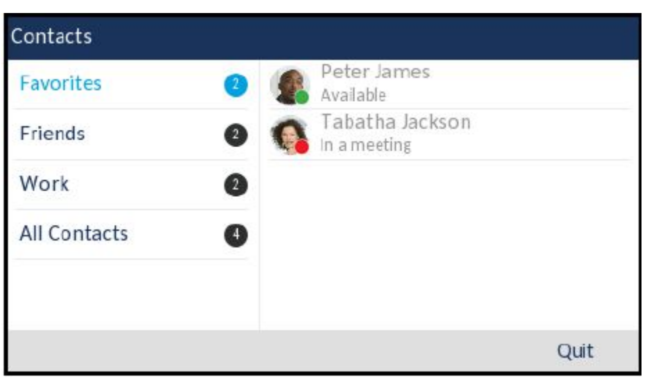
Use the following IP Phone UI procedure to view your UC-ONE contacts' presence information and call a contact using the Contacts List.

IP PHONE UI

For the 6867i and 6869i:

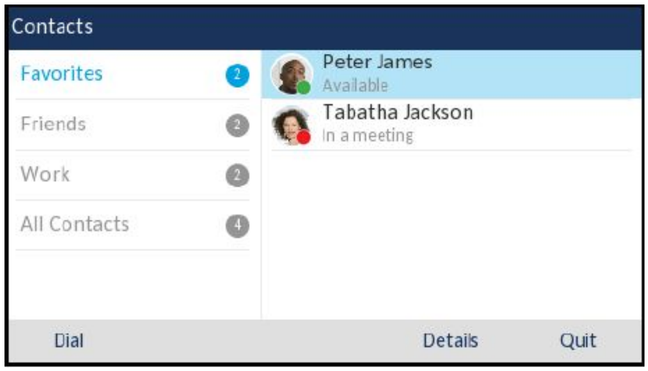
1. Press the softkey configured with Contact List functionality.

6869i Example



2. Use the ▲ and ▼ navigation keys to select the desired group.
   The avatars, names, presence state indicators, and presence status/free text for your UC-ONE contacts assigned to the desired group are displayed in the right contact column.
3. With the desired group highlighted, press the ▶ navigation key to move to the contact column.

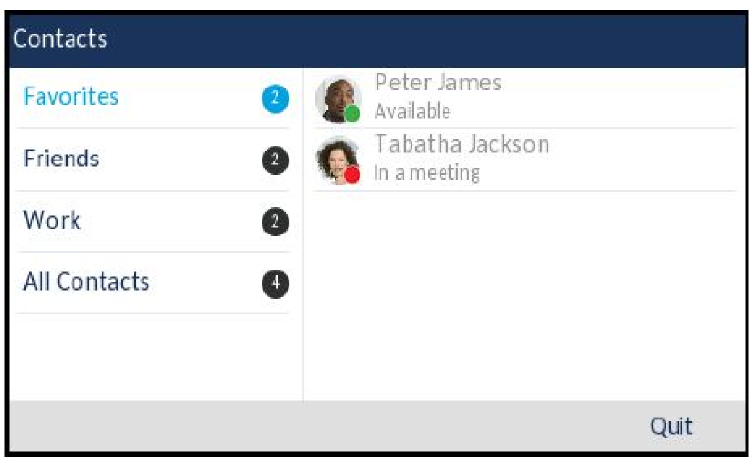
6869i Example



4. Use the ▲ and ▼ navigation keys to scroll through the list of contacts.
5. At any time, press the **Dial** softkey to initiate a call to the selected contact's Work Extension number. If a Work Extension number is not defined, the phone will dial out using the Work Phone number, then the Mobile Phone number, and then lastly the Personal Phone number (whichever is defined first based on the described order).
6. Press the **Quit** softkey to exit the Contacts List.

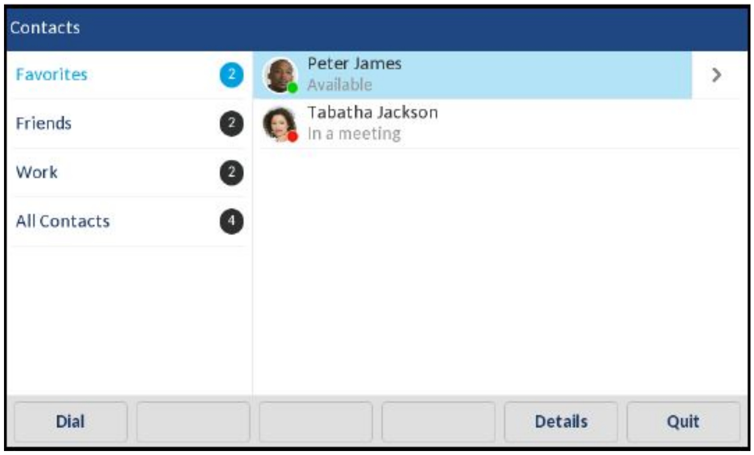
For the 6873i:

1. Press the softkey configured with Contact List functionality.



2. In the left group column, press a group to view the contacts within the selected group.
   The avatars, names, presence state indicators, and presence status/free text for your UC-ONE contacts assigned to the desired group are displayed in the right contact column.
3. At any time, press a contact and press the **Dial** softkey to initiate a call to the selected contact's Work Extension number. If a Work Extension number is not defined, the phone

will dial out using the Work Phone number, then the Mobile Phone number, and then lastly the Personal Phone number (whichever is defined first based on the described order).



4. Press the **Quit** softkey to exit the Contacts List.

To View Your UC-ONE Contacts' Detailed Information and Call a Contact's Secondary Phone Number

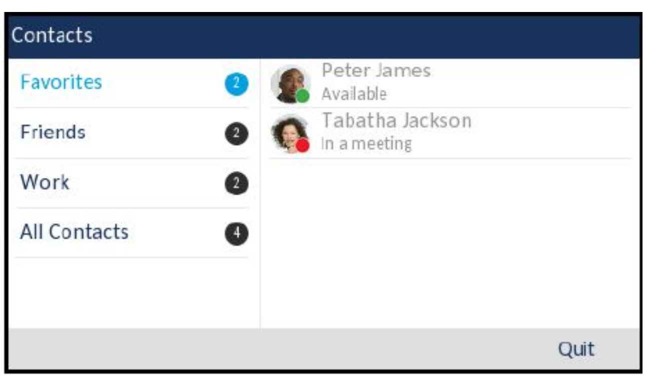
Use the following IP Phone UI procedure to view your UC-ONE contacts' detailed information and call a contact's secondary phone number using the Contacts List.

IP PHONE UI

For the 6867i and 6869i:

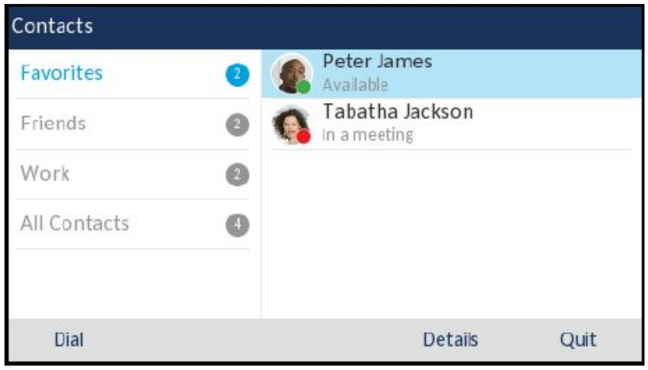
1. Press the softkey configured with Contact List functionality.

6869i Example



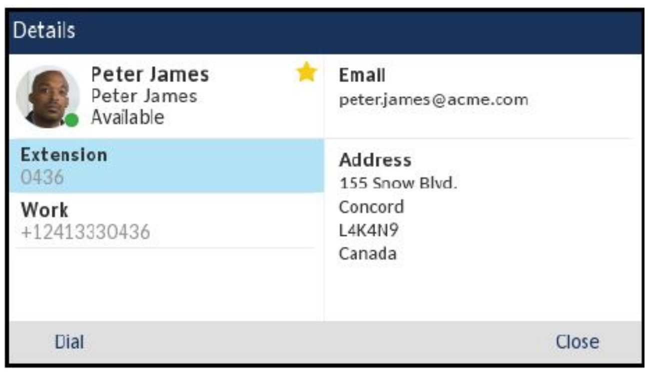
2. Use the ▲ and ▼ navigation keys to select the desired group.
3. With the desired group highlighted, press the Right navigation key to move to the contact column.

6869i Example



4. Use the ▲ and ▼ navigation keys to scroll through the list of contacts.
5. Press 4 or the **Details** softkey to see more detailed information about the selected contact. If available, the contact's display name, first and last name, presence information, phone numbers, address, and Email address are displayed.

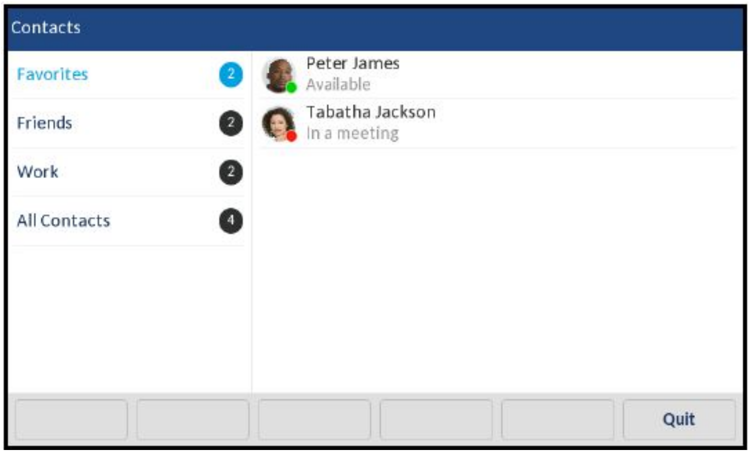
6869i Example



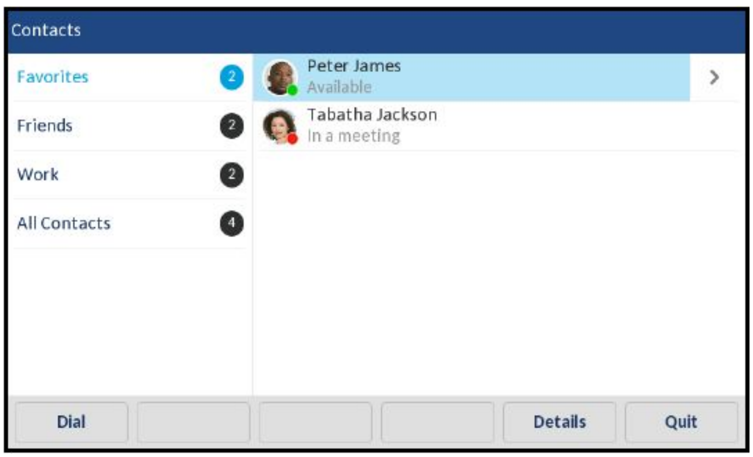
6. To call the contact use the ▲ and ▼ navigation keys to scroll through the list of phone numbers and then press the **Dial** softkey to initiate a call to the selected phone number.
7. Press the **Close** softkey to exit the **Details** screen.

For the 6873i:

1. Press the softkey configured with Contact List functionality.

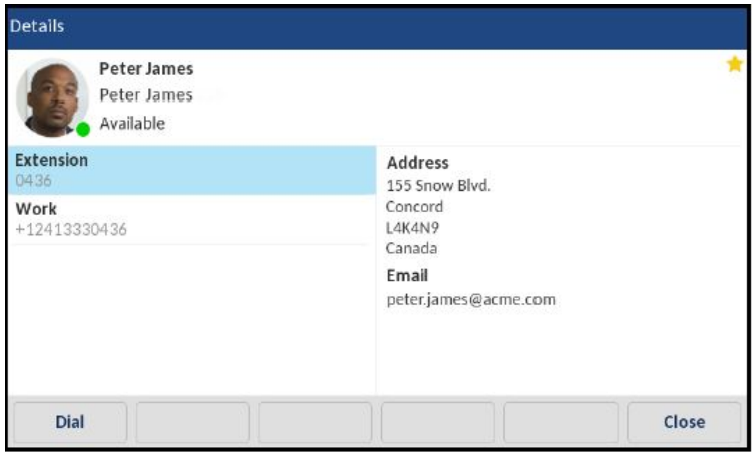


2. In the left group column, press a group to view the contacts within the selected group and then press a contact to select the desired contact.



3. Press the right arrow button or the **Details** softkey to display more detailed information about the selected contact.

If available, the contact's display name, first and last name, presence information, phone numbers, address, and Email address are displayed.



4. To call the contact, press the desired phone number and then press the **Dial** softkey to initiate a call to the selected phone number.
5. Press the **Close** softkey to exit the **Details** screen.

BROADSOFT BROADWORKS EXECUTIVE AND ASSISTANT SERVICES

The Executive and Assistant Services feature allows Administrators to create an inter-network relationship between Executives and Assistants allowing calls to the Executive's phone to be screened, filtered, and routed to an Assistant, whereby the Assistant can answer, divert the filtered call, or push the call back to the Executive.

Notes:

1. The inter-network relationship is created dynamically through the BroadSoft BroadWorks call manager Web portal. For BroadSoft BroadWorks Executive and Assistant Services Web portal configuration details and procedures, please refer to the respective BroadSoft documentation.
2. For details on how to configure and utilize the BroadSoft BroadWorks Executive and Assistant Services feature from a user's perspective, please refer to the respective phone model's ***Mitel SIP Phone User Guide***.

CONFIGURATION PARAMETERS

After configuring the applicable options on the BroadSoft Broadworks call manager Web portal, Administrators must define the "**sip execassist filter call prefix**", "**sip execassist fac call push**", and "**sip execassist fac initiate call**" parameters for the phone.

The "**sip execassist filter call prefix**" parameter is used to identify the prefix of the Alerting Custom Calling Line ID Name of a filtered call. The Alerting Custom Calling Line ID Name as configured in the BroadWorks Web portal should follow the format:

[prefix] [Identifier] -> [Executive Name]

The Executive Name must match the name that is configured in the user's profile, separated by a space or comma.

Note: The Alerting Calling Line ID Number can either be configured as the Executive's Number or Originator's Number.

For example, if the "Alerting Custom Calling Line ID Name" setting in the BroadWorks Web portal is defined as "[F] Filtrage -> Dupont, Francois", the From header of a filtered call sent by the BroadWorks SIP INVITE message will look similar to:

From:"[F] Filtrage -> Dupont, Francois"
<sip:5551234567@as.aastra.com;user=phone>

The "**sip execassist filter call prefix**"parameter in this scenario could be defined as:

sip execassist filter call prefix: "[F]"

The Assistant's phone will parse the From header of the SIP INVITE message of an incoming call sent by the call manager and will identify whether or not the call is a filtered call by the prefix. The prefix itself is not displayed on the phone's screen (e.g. in the case outlined above, the phone will only display "Filtrage -> Dupont, Francois").

The “**sip execassist fac call push**” parameter is used to specify the Feature Access Code (FAC) that is used to push a filtered call from the Assistant’s phone back to the Executive’s phone. The FAC should correspond to the value configured for the “Executive-Assistant Call Push” setting defined in the BroadSoft Web portal.

The “**sip execassist fac initiate call**” parameter is used to specify the FAC that is used by Assistants to initiate a call on behalf of the Executive. The FAC should correspond to the value configured for the “Executive-Assistant Initiate Call” setting defined in the BroadSoft Web portal.

Use the following parameters to configure the BroadSoft Executive and Assitant Services feature:

CONFIGURATION FILES

For the specific parameters you can set in the configuration files, see Appendix A, the section, “BroadSoft BroadWorks Executive and Assitant Services Settings” on page A-343.

FILTER SOFTKEY

In addition to the new parameters, a “Filter” softkey type has been introduced allowing both Executives and Assistants the ability to easily activate and deactivate the Executive Call Filtering feature.

> **Note:** The **As-Feature Event Subscription** option must also be enabled for the Filter softkey to function. This feature can be enabled by defining the “**sip lineN as-feature-event subscription**” parameter as “**1**” in the configuration files (where “N” corresponds to the applicable line) or through the phone’s Web UI under **Advanced Settings > LineN > Advanced SIP Settings > As-Feature-Event Subscription**. Refer to “As-Feature-Event Subscription” on page 6-15 for additional details on the As-Feature Event Subscription feature.

Filter Softkey for the Executive’s Phone

The Executive’s phone requires that only one Filter softkey be configured. The Filter softkey’s value can either be left undefined (which will toggle the Executive Call Filtering settings on the call manager via the SIP SUBSCRIPTION/NOTIFY mechanism) or, it can be defined using the following values (which will toggle the settings via an FAC call):

- Executive Call Filtering Activation FAC (e.g. "#61")
  - Used when the Deactivation FAC is in the same format as the Activation FAC but sequentially one number above the Activation FAC. For example, if the softkey value is defined as "#61" (the Activation FAC), the phone will automatically assume that the Deactivation FAC is "#62" and will use that code to deactivate Executive Call Filtering.
- Executive Call Filtering Activation FAC followed by a semi-colon and then Executive Call Filtering Deactivation FAC (e.g. "#61;*61" or "#61;#71")
  - Used when the Activation and Deactivation FACs are not in the same format or when they are not sequential. For example, if the Activation FAC is configured in the BroadSoft BroadWorks Web portal is "#61" and the Deactivation FAC is configured as "*61" or

"#71", the softkey value should be defined with the two specific FACs separated by a semi-colon (i.e. "#61;*61" or "#61;#71" respectively).

Notes:

1. If the Deactivation FAC is not specified after the semi-colon (e.g. "#61;"), the phone will ignore the semi-colon and behave as if only the Activation FAC was defined (i.e. the phone will automatically assume that the Deactivation FAC is in the same format but sequentially one number above the Activation FAC.
2. The IP phones support Executive Call Filtering Activation/Deactivation FACs that contain the prefix “#” or “*”.

Irrespective of a defined or undefined key value, when the Filter softkey is pressed, Executive Call Filtering will be activated and the softkey’s corresponding LED will be lit. When the Filter softkey is pressed again, Executive Call Filtering will deactivate and the softkey’s corresponding LED will turn off.

Note: Upon a reboot, the initial state of the Filter softkey LED will correspond to the Executive Call Filtering state configured on the call manager.

Configuring the Filter Softkey on the Executive’s Phone Using the Mitel Web UI

Use the following procedure to configure the Filter Softkey on the Executive’s phone using the Mitel Web UI:

1. Click on **Operation**->**Softkeys and XML**.
   or
   Click on **Operation**-> **Programmable Keys**.
   or
   Click on **Operation**->**Expansion Module Keys**.
2. Select a key that you want to use as a Filter activate/deactivate key.
3. In the "**Type**" field, select "**Filter**".
4. In the "**Label**" field (6867i, 6869i, 6873i only), enter a label to apply to this key (e.g. Filter).
5. (Optional) In the "**Value**" field, enter the Executive Call Filtering Activation FAC (e.g. #61) or both the Executive Call Filtering Activation and Deactivation FACs followed by a semi-colon (e.g. #61;*61).
6. In the “**Line**” field, select the line for which you want to use the key functionality.
7. Click **Save Settings** to save your settings.

Configuring the Filter Softkey on the Executive’s Phone Using the Configuration Files

To configure the Filter softkey on the Executive’s phone using the configuration files, you must enter “**filter**” for the key type. For the label (6867i, 6869i, and 6873i only), enter a key label to assign to the Filter key (e.g. “Filter”). Defining the value is optional. If you prefer to toggle Executive Call Filtering using an FAC call, enter in the Executive Call Filtering Activation FAC (e.g. "#61") or both the Executive Call Filtering Activation and Deactivation FACs followed by a semi-colon (e.g. "#61;*61") for the value. For the line setting, enter the line number for which you want to use the key functionality.

The following parameters are examples you can use to configure the Filter softkey on the Executive's phone:

For Bottom Softkeys
softkey1 type: filter
softkey1 label: Filter
softkey1 value: "#61;*61"
softkey1 line: 1

For Top Softkeys
topsoftkey1 type: filter
topsoftkey1 label: Filter
topsoftkey1 value: "#61;*61"
topsoftkey1 line: 1

For Programmable Keys
prgkey1 type: filter
prgkey1 value: "#61;*61"
prgkey1 line: 1

For Expansion Module Softkeys
expmod1 key1 type: filter
expmod1 key1 label: Filter
expmod1 key1 value: "#61;*61"
expmod1 key1 line: 1

Filter Softkey for the Assistant's Phone

As an Assistant can be associated with multiple Executives simultaneously, the Assistant's phone can be configured with multiple Filter softkeys; one softkey for each Executive. In this case, the value of each Filter softkey should correspond to the phone number or extension of the respective Executive as per configured in the user's profile.

When Filter softkeys are configured with key values, pressing the respective Filter softkey will activate Executive Call Filtering for the applicable Executive and the softkey's corresponding LED will be lit. When the same Filter softkey is pressed again, Executive Call Filtering for the applicable Executive will deactivate and the softkey's corresponding LED will turn off.

Alternatively, a single Filter softkey can be configured without a defined key value. If this is the case, the Assistant will be able to manually activate and deactivate Executive Call Filtering for each associated Executive through the phone's UI. In this scenario, as only one Filter softkey is utilized, the softkey's corresponding LED will be lit when Executive Call Filtering is activated for even one associated Executive. If Executive Call Filtering is disabled for all associated Executives, the softkey's corresponding LED will turn off.

Note: If Call Forward is enabled for filtered calls, LEDs for all Filter softkeys will be turned off.

Configuring the Filter Softkey on the Assistant's Phone Using the Mitel Web UI

Use the following procedure to configure the Filter Softkey on the Assistant's phone using the Mitel Web UI:

1. Click on **Operation**->**Softkeys and XML**.
   or
   Click on **Operation**-> **Programmable Keys**.
   or
   Click on **Operation**->**Expansion Module Keys**.
2. Select a key that you want to use as a Filter activate/deactivate key.
3. In the "**Type**" field, select "**Filter**".
4. In the "**Label**" field (6867i, 6869i, and 6873i only), enter a label to apply to this key (e.g. "Filter-Stefan" for a specific Executive or simply "Filter" for a generic Filter key with no defined value).

   Note: To utilize a single Filter softkey without a defined key value (so that you can manually activate and deactivate Executive Call Filtering through the phone's UI) skip to Step 8.
5. In the "**Value**" field, enter the Executive's phone or extension number (e.g. 4100)
6. In the "**Line**" field, select the line for which you want to use the key functionality.
7. Repeat Steps 2 to 6 for each respective Executive for whom you would like to assign a Filter key.
8. Click **Save Settings** to save your settings.

Configuring the Filter Softkey on the Assistant's Phone Using the Configuration Files

To configure the Filter softkeys on the Assistant's phone using the configuration files, you must enter "**filter**" for the key types. For the labels (6867i, 6869i, and 6873i only), enter key labels to assign to the Filter key (e.g. "Filter-Stefan" for a specific Executive or simply "Filter" for a generic Filter key with no defined value). Defining the value is optional. If you choose to assign a Filter softkey and define values for each Executive, enter in the respective Executive's phone or extension number (e.g. 4100). For the line setting, enter the line number for which you want to use the key functionality. If you prefer to utilize a single Filter softkey without a defined value you will be able to manually activate and deactivate Executive Call Filtering for each Executive to whom the Assistant is assigned through the phone's UI.

The following parameters are examples you can use to configure multiple Filter softkeys corresponding to multiple Executives on the Assistant's phone:

For Bottom Softkeys
softkey1 type: filter
softkey1 label: Filter-Stefan
softkey1 value: 4100
softkey1 line: 1

softkey2 type: filter
softkey2 label: Filter-John
softkey2 value: 4101
softkey2 line: 1

For Top Softkeys
topsoftkey1 type: filter

topsoftkey1 label: Filter-Stefan
topsoftkey1 value: 4100
topsoftkey1 line: 1

topsoftkey2 type: filter
topsoftkey2 label: Filter-John
topsoftkey2 value: 4101
topsoftkey2 line: 1

For Programmable Keys
prgkey1 type: filter
prgkey1 value: 4100
prgkey1 line: 1

prgkey2 type: filter
prgkey2 value: 4101
prgkey2 line: 1

For Expansion Module Softkeys
expmod1 key1 type: filter
expmod1 key1 label: Filter-Stefan
expmod1 key1 value: 4100
expmod1 key1 line: 1

expmod1 key2 type: filter
expmod1 key2 label: Filter-John
expmod1 key2 value: 4101
expmod1 key2 line: 1

SPEEDDIAL SOFTKEY WITH INITIATE CALL FUNCTIONALITY (ASSISTANTS ONLY)

Speeddial softkeys can be configured to efficiently utilize the Executive-Assistant Initiate Call function. With a Speeddial softkey configured for this feature, Assistants can initiate a call on behalf of an Executive, whereby the call will appear to the target as one originated by the Executive himself/herself. The Speeddial softkey's value can be defined using the following syntax:

- Executive-Assistant Initiate Call FAC (e.g. "#64"):
  - In such scenarios, the call manager will play an audible prompt asking you to enter the Executive's Address and Destination Address manually using the keypad.
- Executive-Assistant Initiate Call FAC followed by the Executive's Address (e.g. "#644052"):
  - In such scenarios, only the Destination Address will need to be manually entered using the keypad.
- Executive-Assistant Initiate Call FAC, followed by the Executive's Address, an asterisk, and then the Destination Address (e.g. "#644052*4059"):

- In such scenarios, addresses will not need to be manually entered and the phone will automatically initiate the call to the target phone on behalf of the Executive.

Note: The Speeddial softkey type can be utilized for additional functions related to the Executive and Assistant Services feature that rely on FAC calls (i.e. opting in to an Executive's filtered call pool, opting out of an Executive's filtered call pool, etc...). Administrators simply need to configure the Speeddial key value as the FAC and label accordingly.

Configuring the Initiate Call Softkey on the Assistant's Phone Using the Mitel Web UI

Use the following procedure to configure the Initiate Call Softkey on the Assistant's phone using the Mitel Web UI:

1. Click on **Operation**->**Softkeys and XML**.
   or
   Click on **Operation**-> **Programmable Keys**.
   or
   Click on **Operation**->**Expansion Module Keys**.
2. Select a key that you want to use as an Initiate Call key.
3. In the "**Type**" field, select "**Speeddial**".
4. In the "**Label**" field (6867i, 6869i, and 6873i only), enter a label to apply to this key (e.g. Init).
5. In the "**Value**" field, enter the Initiate Call FAC (e.g. #64)
   or
   In the "**Value**" field, enter the Initiate Call FAC, followed by the Executive's Address (e.g. #644052)
   or
   In the "**Value**" field, enter the Initiate Call FAC, the Executive's Address, followed by an asterisk, and then the Destination Address (e.g. #644052*4059)
6. In the "**Line**" field, select the line for which you want to use the key functionality.
7. Click **Save Settings** to save your settings.

Configuring the Initiate Call Softkey on the Assistant's Phone Using the Configuration Files

To configure the Initiate Call Speeddial softkeys on the Assistant's phone using the configuration files, you must enter "**speeddial**" for the key types. For the labels (6867i, 6869i, and 6873i only), enter key labels to assign to the Speeddial key (e.g. "Init"). For the values, enter one of the following:

- Executive-Assistant Initiate Call FAC (e.g. "#64")
- Executive-Assistant Initiate Call FAC followed by the Executive's Address (e.g. "#644052")
- Executive-Assistant Initiate Call FAC, followed by the Executive's Address, an asterisk, and then the Destination Address (e.g. "#644052*4059")

For the line setting, enter the line number for which you want to use the key functionality.

The following parameters are examples you can use to configure multiple Initiate Call Speeddial softkeys:

For Bottom Softkeys
softkey1 type: speeddial
softkey1 label: Init
softkey1 value: "#64"
softkey1 line: 1

softkey2 type: speeddial
softkey2 label: Init2
softkey2 value: "#644052"
softkey2 line: 1

softkey3 type: speeddial
softkey3 label: Init3
softkey3 value: "#644052*4059"
softkey3 line: 1

For Top Softkeys
topsoftkey1 type: speeddial
topsoftkey1 label: Init
topsoftkey1 value: "#64"
topsoftkey1 line: 1

topsoftkey2 type: speeddial
topsoftkey2 label: Init2
topsoftkey2 value: "#644052"
topsoftkey2 line: 1

topsoftkey3 type: speeddial
topsoftkey3 label: Init3
topsoftkey3 value: "#644052*4059"
topsoftkey3 line: 1

For Programmable Keys
prgkey1 type: speeddial
prgkey1 value: "#64"
prgkey1 line: 1

prgkey2 type: speeddial
prgkey2 value: "#644052"
prgkey2 line: 1

prgkey3 type: speeddial
prgkey3 value: "#644052*4059"
prgkey3 line: 1

For Expansion Module Softkeys
expmod1 key1 type: speeddial
expmod1 key1 label: Init
expmod1 key1 value: "#64"
expmod1 key1 line: 1

expmod1 key2 type: speeddial
expmod1 key2 label: Init2
expmod1 key2 value: "#644052"
expmod1 key2 line: 1

expmod1 key2 type: speeddial
expmod1 key2 label: Init3
expmod1 key2 value: "#644052*4059"
expmod1 key2 line: 1

VISITOR DESK PHONE SUPPORT

GENERAL OVERVIEW AND CONFIGURATION

A Visitor Desk Phone (VDP) feature has been implemented allowing users the ability to log in to any VDP-configured phones and thus use that respective phone as his/her personal device for the duration of the logged in session.

Note: For VDP functionality, the phone must be configured to accept XML SIP NOTIFY messages. This can be enabled by defining the “sip xml notify event” parameter as “1” in the respective configuration file, or by placing a checkmark in the “XML SIP Notify” option found under the Advanced Settings > Global SIP > Advanced SIP Settings section in the Web UI. See “XML SIP Notify Events and Action URIs” on page 3-71 for more information.

Using the “startup.cfg”, “<mac>.cfg”, or “<model>.cfg” file, Administrators can provision each of the respective phones with a generic visitor account that has been configured for the specific environment and then simply define the “**user config url**” parameter, which specifies the configuration server URL where the <user>.cfg is located when utilizing the Visitor Desk Phone (VDP) feature.

Notes:

1. If an HTTP/HTTPS server is being used to store the <user>.cfg file, then the following two files need to reside in the folder specified by the "**user config url**" parameter:
   - upload.html
   - upload_file.php

   To obtain these two files, please contact Mitel Technical Support.
2. The Visitor Desk Phone feature will not be functional when using the HTTP/HTTPS protocol without these two files properly installed on the HTTP/HTTPS configuration server.
3. PHP must be installed on the HTTP/HTTPS server and the folder must have read and write permissions.

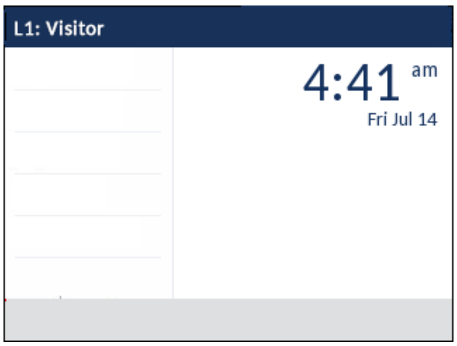
For example, the respective configuration file for a simple visitor account could contain the following:

```
sip auth name: 5000
sip display name: Acme Inc.
sip password: 12345
sip proxy ip: 100.200.50.60
sip proxy port: 5060
sip registrar ip: 100.200.50.60
sip registrar port: 5060
sip screen name: Visitor
sip user name: 5000
sip dtmf method: 1
sip xml notify event: 1
user config URL: http://100.200.50.79/vdp/
```

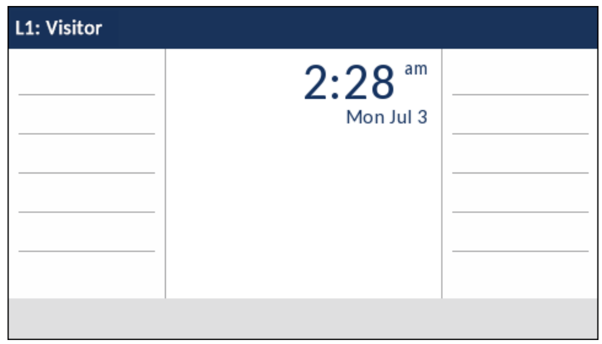
This visitor account is the default account that the phone uses when a user is not logged in his/her specific account. In the above configuration example, the user would see the following initial screen:

6863i/6865i/6905/6910 Visitor Account Example

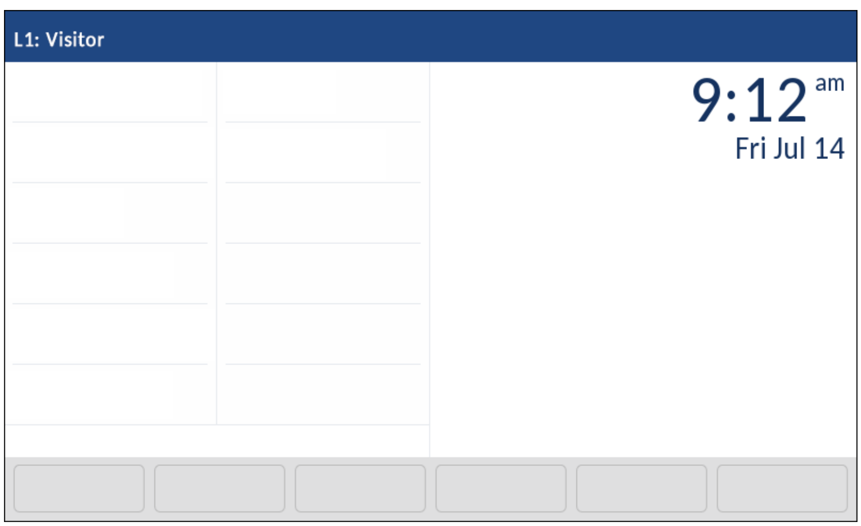
6867i Visitor Account Example



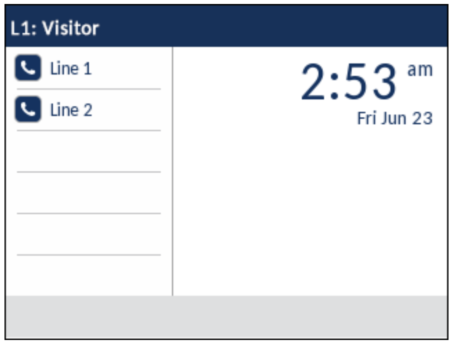
6869i Visitor Account Example



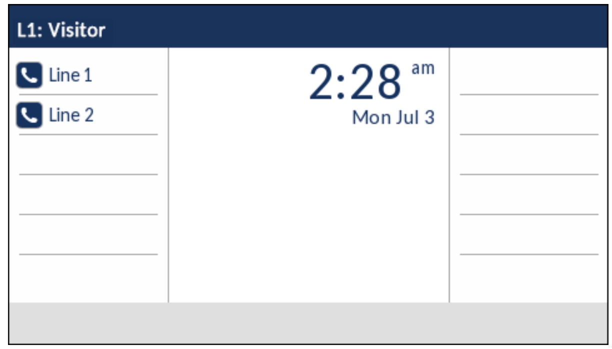
6873i Visitor Account Example



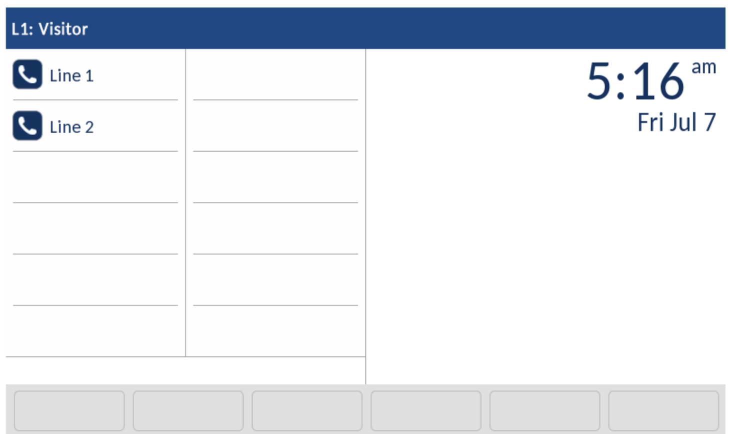
6920 Visitor Account Example



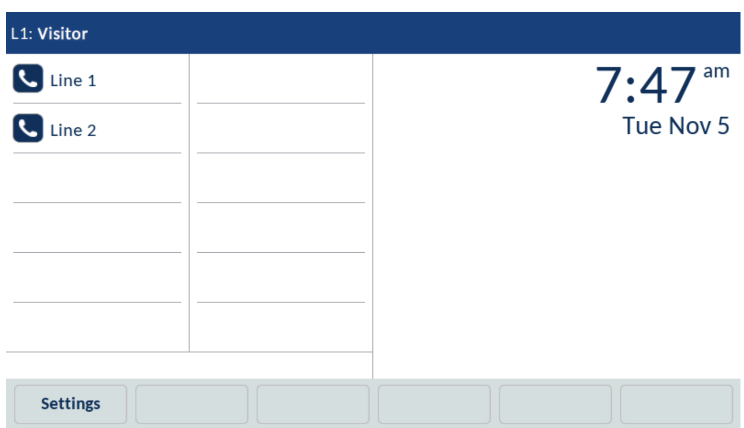
6930 Visitor Account Example



6940 Visitor Account Example



6970 Visitor Account Example



Configuring the User Configuration Server URL

CONFIGURATION FILES

For specific parameters that you can set in the configuration files, see Appendix A, section "Visitor Desk Phone Settings" on page A-344.

To configure the phone with a secondary server for downloading and uploading the user configuration server URL, define the **backup user config url** parameter.

When this configuration parameter is defined,

- the phone attempts to download the user configuration from the backup server if the configuration files could not be downloaded from the primary server at user login
- the phone attempts to upload the user configuration to the backup server when the primary server is down and the user configuration must be uploaded.

Configuring the Backup User Configuration Server URL

CONFIGURATION FILES

For specific parameters that you can set in the configuration files, see Appendix A, section "Visitor Desk Phone Settings" on page A-344.

LOGGING IN AND LOGGING OUT

For logging in and logging out, a NOTIFY message containing an XML body that includes the parameter "subscriberLogin" or "subscriberLogout" messageType (with valid username and password values if logging in) to the phone must be triggered. The method of triggering this NOTIFY message can be phone-initiated (by configuring a "Login" key) or initiated through a different method (e.g. through use of an Interactive Voice Response [IVR] system).

To log in to a specific user profile, the user could, if configured, press the "Login" key on the phone or call an IVR set up for the VDP log in/log out process (or any other alternative method configured).

If the "Login" key is pressed, the phone will prompt the user for the username and password. If the server does not support authentication or if the server is set up for anonymous connections, the username is all that is required and corresponds to the filename of the <user>.cfg file (e.g. john). If the server is configured with login credentials, both the username and password are required. The username in this case corresponds to both the server username credential and <user>.cfg file (i.e. the server username and <user>.cfg file name must match) and the password corresponds to the server password credential.

Note: The default input mode for password entry during hotdesk login is numeric.

When the user's credentials are confirmed, this triggers the call manager to send an unsolicited NOTIFY message containing an XML body that includes the "subscriberLogin" messageType with valid username and password values. The phone then contacts the configuration server (defined by the “user config url” parameter) and downloads the subscribers profile contained in the “<user>.cfg” and “<user>_local.cfg” files.

Note: The “<user>.cfg” file contains read-only server-related configuration information that is not configurable by the user and the “<user>_local.cfg” file contains the user configuration information that has been changed by the user locally either through the phone’s UI or through the Web UI.

For example, if the “**user config url**” parameter is defined with valid HTTP, HTTPS, FTP, or TFTP server credentials and an unsolicited NOTIFY message containing the following XML body is received by phone:

```
<?xml version="1.0" encoding="UTF-8"?>
<visitorDesk>
  <messageType>subscriberLogin</messageType>
  <subscriber>
     <username>john</username>
     <password>mitel</password>
  </subscriber>
</visitorDesk>
```

the phone connects to the defined server, downloads the “john.cfg” and “john_local.cfg” files containing all the applicable saved settings and information for that particular user, and configures the phone according to the “john.cfg” and “john_local.cfg” files.

The phone is updated with the respective user’s profile, which contains the user’s phone preferences (e.g. key configuration as well as settings configurable through the Options List), Received Callers and Outgoing Redial Lists, Directory contents, etc...

Note: Screen language settings are also updated to match the user’s configuration, but the language file must be loaded on the phone for the screen language setting to take effect.

When the user logs out (through an IVR for example, or by pressing the “Log Out” softkey), the “<user>_local.cfg” file is saved and another unsolicited NOTIFY message (containing an XML body that includes the “subscriberLogout” messageType) as per the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<visitorDesk>
   <messageType>subscriberLogout</messageType>
</visitorDesk>
```

is sent by the call manager to the phone. When the phone receives the NOTIFY, the user is logged out and the phone reverts back to the generic visitor account.

If using the “Login” key method, Administrators can define in the configuration files a programmable key, top or bottom softkey, or expansion module key type as “**hotdesklogin**” or configure a “Login” key using the Web UI.

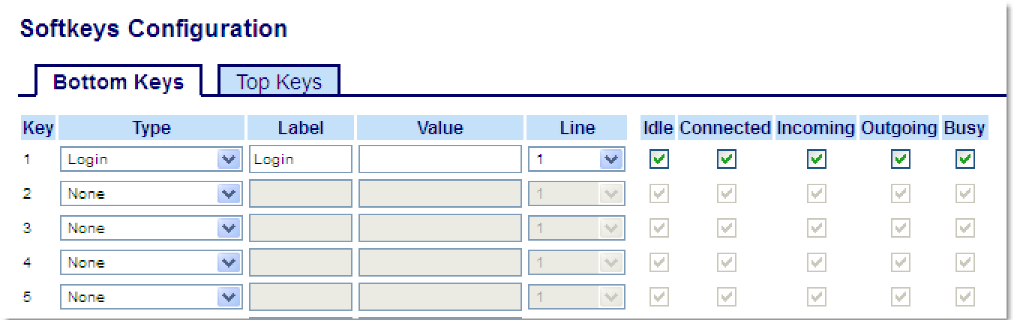
Note: For details on how to configure softkeys and programmable keys using the configuration files see "Softkey Settings," on page 249, "Programmable Key Settings," on page 259, and "Top Softkey Settings," on page 265.

Creating a Login Key Using the Mitel Web UI

Use the following procedure to create a Login key using the phone's Web UI:

MITEL WEB UI

1. Click on **Operation > Programmable Keys (6863i/6865i/6905/6910)** or **Softkeys and XML (6867i/6869i/6873i/6920/6930/6940/6970)**



2. Select from **Key 1** through **Key 3** (6863i) or **Key 8** (6865i) on the programmable keys
   or
   Select from **Key 1** through **Key 20** (6867i/6920) or **Key 44** (6869i/6930) or **Key 48** (6873i/6940/6970) on the top keys
   or
   Select from **Key 1** through **Key 18** (6867i/6920) or **Key 24** (6869i/6873i/6930) or **Key 30** (6940/6970) on the bottom keys.
3. In the **Type** field, select **Login** to apply to the key.
4. (If available/optional) In the **Label** field, enter a label to apply to this key (e.g. Login)
5. Click **Save Settings**.

Configurable Login/Logout Security Behavior

Using the "**hot desk high security**" parameter, Administrators are able define whether or not VDP users have to enter their credentials every time they want to log in and log out of the phone.

When the "**hot desk high security**" parameter is defined as "0" (disabled) and a user is logged in to their VDP account, if a power loss occurs, upon recovery the phone will attempt to automatically log in using the last set of credentials recorded by the phone.

Note: The last user name and password used to log in to a VDP account is encrypted and stored on the phone.

Additionally, users can press the "Logout" key to immediately log out of their VDP account without the need to enter their password.

When the "**hot desk high security**" parameter is defined as "1" (enabled), no automatic login attempts are made by the phone even after a power loss. Users are required to enter their credentials to log in to their VDP account at all times. Additionally, users must enter their password to log out of their account. These security features ensure that accounts are only logged in to and logged out of when initiated by the respective user.

Note: The "**hot desk high security**" parameter is enabled by default.

FILTER VDP PARAMETERS

When a hotdesk user logs in, all configuration changes made prior to log out need to be either uploaded to network, or saved to local config. Previously, all hotdesk user's configurations were synchronized to the server, including the network dependency parameters such as IP address, DHCP setting, TLS certificate settings, and so on.

Since the hotdesk user configuration is required to be independent of the network, a change was implemented, to have a list of network parameters stay on the phone (saved in local.cfg instead of user-local.cfg). This helps in avoiding mal-configurations when the VDP user switches networks.

In release 5.0.0 SP1, additional VDP filtering parameters are added to the list of configuration parameters. The firmware implements this feature automatically in the background and no parameter or configuration is required.

The following are the list of blacklisted configuration parameters stored locally on the phone:

- Advanced network settings
  - lldp
  - lldp interval
  - sip rport
- Troubleshooting parameter page
  - log server ip
  - log server port
  - log mac
  - log module
    - log module linemgr
    - log module audiomgr
    - log module user interface
    - log module misc
    - log module sip
    - log module dis
    - log module dstore
    - log module ept
    - log module ind
    - log module kbd
    - log module net
    - log module provis

  - log module rtpt
  - log module snd
  - log module prof
  - log module xml
  - log module stun
  - log module lldp
- Watchdog setting
  - watchdog enable
- Crash file retrieval
  - upload system info server
  - upload system info on crash
  - upload system info manual option
- Configuration server settings page
- Download protocol
- TFTP
  - tftp server
  - tftp path
  - alternate tftp server
  - alternate tftp path
  - use alternate tftp
- FTP
  - ftp server
  - ftp path
  - ftp username
  - ftp password
- HTTP
  - http server
  - http path
  - http port
- HTTPS
  - https server
  - https path
  - https port
- Auto resync
  - auto resync mode
  - auto resync time
  - auto resync max delay
  - auto resync days

- TLS Support
  - sips root and intermediate certificates
  - sips local certificate
  - sips trusted certificates
  - sips private key
- Action uri
  - action uri poll
  - action uri poll interval
  - action uri startup
  - action uri registered
  - action uri registration event
  - action uri xml sip notify
  - action uri blf
  - action uri incoming
  - action uri outgoing
  - action uri offhook
  - action uri onhook
  - action uri connected
  - action uri disconnected
- Paging
  - paging group listening
- HTTPS Client Method
- dhcp
- ip
- subnet mask
- default gateway
- dns1
- dns2
- ethernet port 0
- ethernet port 1
- eap type
- identity
- 802.1x root and intermediate certificates
- 802.1x local certificate
- 802.1x private key
- 802.1x trusted certificates

- tagging enabled
- vlan id
- vlan id port 1
- tos sip
- tos rtp
- tos rtcp
- tos priority map
- priority non-ip
- dhcp option 132 vlan id enabled
- dhcp config option override
- https user certificates

USER CONFIGURATION UPLOAD FUNCTIONALITY

Any changes made to a user's profile while he/she is logged in are saved to the "<user>_local.cfg" file periodically. The time period between the saves is configurable using the "**user config upload**" and "**user config upload delta**" parameters.

The "**user config upload**" parameter specifies the time period (in seconds) between the "<user>_local.cfg" saves (while the user is logged in). To help distribute the file transfers to the configuration server in a more even manner (i.e. so that the server does not get bombarded by file transfer requests all at the same time) after the initial save, the "<user>_local.cfg" is saved at a random time period between the values defined in the "**user config upload**" parameter and the "**user config upload delta**" parameter. This latter parameter specifies the upper limit of the extra random time (in seconds) added to the time defined in the "user config upload" parameter.

Additionally, a "**user config upload control**" parameter has been implemented that can be used to fine tune when the "<user>_local.cfg" file should be saved. Administrators can define the parameter as the following:

- **0:** Every time the "user config upload" time period expires and at every logout regardless of if the <user>_local.cfg has changed or not.
- **1:** When the "user config upload" time period expires but only if the <user>_local.cfg has changed, and at every logout regardless of if the <user>_local.cfg has changed or not.
- **2:** Only if the <user>_local.cfg has changed. Checked when the "user config upload" time period expires and at logout.

Configuring User Configuration Upload Functionality Using the Configuration Files

Use the following parameters to configure user configuration upload functionality:

CONFIGURATION FILES

For the specific parameters you can set in the configuration files, see Appendix A, the section, “Visitor Desk Phone Settings” on page A-344.

HANDLE 5XX RESPONSE DURING VDP LOGIN

Previously, when a VDP user attempts to log in and receives a 503 or 500 response from VDP configuration server (HTTP or HTTPS only), the phone fails to send further requests and no longer auto logs in. This scenario is only applicable when high security is disabled.

In Release 4.5.0, an enhancement is made wherein during a VDP auto login procedure, when the phone receives a 500 or 503 response, the VDP user retries to auto login after every 300 seconds. The phone continues to retry until a positive response is received from the server.

OPTION TO ENABLE/DISABLE RTCP

The "**rtcp enable**" parameter is available allowing Administrators the ability to manually enable or disable RTCP. Defining the parameter as "0" disables the feature, while "1" enables the feature. RTCP is enabled (i.e. "1") by default.

Enabling/Disabling RTCP Functionality

Use the following procedure to manually enable/disable RTCP functionality:

CONFIGURATION FILES

For the specific parameters you can set in the configuration files, see Appendix A, the section, “RTP, Codec, DTMF Global Settings” on page 136.

CONFIGURABLE SIP NO RTP PACKET TIMEOUT PERIOD

The "**sip no rtp timeout**" parameter allows Administrators the ability to define a timeout period (in seconds) whereby if no RTP packets (i.e. audio stream) are received in the defined amount of time, the phone will send a BYE request, thus releasing the call and returning the home/idle screen.

Note: This parameter is disabled by default.

Configuring the SIP No RTP Packet Timeout Period

Use the following procedure to configure the SIP No RTP packet timeout period:

CONFIGURATION FILES

For the specific parameters you can set in the configuration files, see Appendix A, the section, "RTP, Codec, DTMF Global Settings" on page 136.

OPTION TO PARSE OR IGNORE REFER EVENT IDS

The configuration parameter "**sip ignore refer event id**" has been allows Administrators the ability to set whether or not event IDs (i.e. Event: refer:id=xxxxx) in REFER NOTIFY event headers received by the phone should be ignored. Configuring the phones to ignore event IDs may fix call transfer issues caused by event IDs not matching REFER CSeq numbers.

Note: In previous firmware release, the phones were incorrectly hard-coded to ignore event IDs in REFER NOTIFY event headers. This has been corrected, and in Releases including and above 4.0.0 SP1, the default behavior is to parse and check for valid event IDs. Administrators should explicitly enable the "**sip ignore refer event id**" (i.e. define the parameter as "1") if call transfer errors occur due to event IDs not matching REFER CSeq numbers.

Configuring REFER Event ID Handling

Use the following procedure to configure how the phone handles REFER event IDs:

CONFIGURATION FILES

For the specific parameters you can set in the configuration files, see Appendix A, the section, "Advanced SIP Settings" on page 116.

REMOTE REBOOTING AND DYNAMIC RELOADING OF THE CONFIGURATION FILES

Upon a check sync NOTIFY message with a "reboot" parameter defined, the phone will (depending on the "reboot" parameter definition) either immediately reboot the phone or reload all the settings in the configuration files without rebooting.

Note: Feature availability is dependent on the call manager. The check sync NOTIFY message from the call manager must contain a defined "reboot" parameter.

Feature behavior is as follows:

- If a check sync NOTIFY containing the parameter "reboot=true" is received by the phone, the phone will automatically reboot itself.

- If a check sync NOTIFY containing the parameter "reboot=false" is received by the phone, the phone will reload the configuration files without rebooting. Any dynamic parameters in the configuration files (i.e. those that do not require a reboot for changes to be applied) will be synchronized accordingly.

MICLOUD TELEPO MUSIC ON HOLD SUPPORT

MiCloud Telepo "music on hold" functionality is supported on the 6800 and 6900 Series SIP phones. "Music on hold" is a feature whereby calls placed on hold are provided with an audio stream (often music) that is played back to the held party for the duration of the hold.

Note: The feature is applicable to the 6800 and 6900 Series SIP phones when used in conjunction with the MiCloud Telepo for Service Providers call manager.

Administrators can use the global "**sip moh server**" parameter or per line "**sip lineN moh server**" parameters to enable the music on hold feature. If a media server SIP address (excluding the domain name) is defined using the parameter, the phone will use the specified server to provide an audio stream to any held parties. The audio stream will be offered in all cases when a remote party is placed on hold (i.e. when placed on hold directly, when placed on hold while performing a transfer or conference, or when the local party switches lines).

Enabling Music on Hold Functionality

Use the following procedure to enable music on hold feature:

CONFIGURATION FILES

For the specific parameters you can set in the configuration files, see Appendix A, the section, “MiCloud Telepo Music on Hold Settings” on page 346.

UAC SESSION REFRESH SUPPORT

With certain networks, a Session Refresh is required to be performed by the User Agent Client (UAC). To accommodate this, a new configuration parameter “**sip force uac session refresh**” has been introduced. When the parameter is enabled and an incoming initial INVITE with a Session-Expires header with no refresher parameter is received, the Session-Expires header and the refresher=uac parameter are added to the 200 OK response as per the following format:

```
Session-Expires: n;refresher=uac
```

The value "n" above corresponds to the session timer value (either defined in the "**sip session timer**" parameter or provided by the server). The parameter is disabled by default.

Notes:

1. The "**sip session timer**" configuration parameter must be configured to enable UAC Session Refresh feature functionality.
2. When the "**sip force uac session refresh**" parameter is enabled:
   - If a phone processes an incoming initial INVITE with a Session-Expires header set but without the refresher parameter, the refresher=uac parameter is added in the 200 OK response instead of the default refresher=uas. This ensures the call initiator performs the refresh.
   - If a phone processes an incoming initial INVITE with a Session-Expires header set and the refresher parameter set to "uas" (i.e. refresher=uas), the phone will follow the directive received in the INVITE.
   - If a phone initiates an outbound call, the outgoing INVITE will only include the Session-Expires header.

Enabling UAC Session Refresh Support

Use the following procedure to enable UAC session refresh support:

CONFIGURATION FILES

For the specific parameters you can set in the configuration files, see Appendix A, the section, "UAC Session Refresh Settings" on page 348.

CONFIGURABLE SRTP ROLLOVER COUNTER (ROC) RESET BEHAVIOR

In a Secure Real-time Transport Protocol (SRTP) environment, when a re-INVITE is sent but there is no change to the media Synchronization Source (SSRC) identifier, as per RFC3711 the phone must not reset its Rollover Counter (ROC) to zero. Certain call managers do not adhere to RFC3711 and with these call managers one-way audio may be observed after a re-INVITE is sent (e.g. in a call hold/unhold scenario).

To allow interoperability with these call managers that do not adhere to RFC3711 ROC processing, the "srtp loose roc" parameter has been introduced. By default (i.e. when the parameter is not defined or if the parameter is defined as "0") the phone strictly adheres to RFC3711 and does not reset the ROC to zero after a re-INVITE. Enabling this parameter (i.e. by defining the parameter as "1") the phone loosely adheres to RFC3711 and resets the ROC to zero after a re-INVITE.

Configuring ROC Reset Behavior

Use the following procedure to configure the ROC reset behavior:

CONFIGURATION FILES

For the specific parameters you can set in the configuration files, see Appendix A, the section, “ROC Reset Behavior Settings” on page 348.

SRTP AES_256_CM ENCRYPTION SUPPORT

SRTP AES_256_CM encryption is supported on the 6867i, 6869i, 6873i, 6920, 6930, 6940,and 6970 Series SIP phones which offers capability with current AES 128 implementation from the application level.

Note: srtp aes256 AKA AES_256_CM_HMAC_SHA1_80 is not supported on 6863i, 6865i, 6905 and 6910 models.

A new configuration parameter “**srtp aes256”** is introduced to enable the SRTP AES_256_CM support. Administrators can enable this functionality by defining the “**srtp aes256**” parameter as “**1**” in the configuration files. By default, this feature is disabled.

Note: The configuration parameter is not dynamic. Reboot the phone to reflect the parameter update.

Enable or Disable SRTP AES_256_CM Support Using the Configuration Files

CONFIGURATION FILES

For the specific parameters you can set in the configuration files, see Appendix A, the section, “SRTP AES_256_CM Encryption Settings” on page A-348.

Note: The configuration parameter is to be only used by servers that support SRTP AES_256_CM.

On the SIP phones, the RTP encryption should be set as SRTP Preferred.

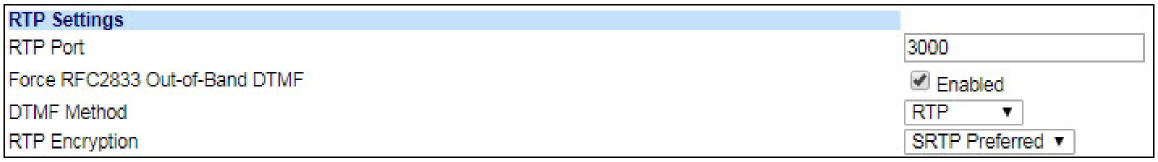
Enable SRTP Preferred Option Using Mitel Web UI

Use the following procedure to enable the RTP encryption to SRTP Preferred on the phone using Mitel Web UI:

MITEL WEB UI

1. Click on **Advanced Settings > Global SIP**

2. In the **RTP Encryption** field under **RTP Settings**, select **SRTP Preferred** from the drop down list.



3. Click **Save Settings**.

Chapter 7

ENCRYPTED FILES ON THE IP PHONE

ABOUT THIS CHAPTER

This chapter provides information about encryption on the IP phones and provides methods an administrator can use to store encrypted files to a server.

TOPICS

This chapter covers the following topics:

ENCRYPTED FILES ON THE IP PHONE

An encryption feature for the IP phone allows Service Providers the capability of storing encrypted files on their server to protect against unauthorized access and tampering of sensitive information (i.e. user accounts, login passwords, registration information). Service Providers also have the capability of locking a phone to use a specific server-provided configuration only.

CONFIGURATION FILE ENCRYPTION METHOD

Only a System Administrator can encrypt the configurations files for an IP Phone. System Administrators use a password distribution scheme to manually pre-configure or automatically configure the phones to use the encrypted configuration with a unique key.

From a Microsoft Windows command line, the System Administrator uses an Mitel-supplied configuration file encryption tool called "*anacrypt.exe*" to encrypt the *<mac>.tuz* file.

Note: Mitel also supplies encryption tools to support Linux platforms (*anacrypt.linux*) if required.

This tool processes the plain text *<mac>.cfg, <model>.cfg,* and *startup.cfg* files and creates triple-DES encrypted versions called *<mac>.tuz, <model>.tuz,* and *startup.tuz.*

Note: In releases previous to 4.0.0 SP1, the "startup.tuz" file was named "aastra.tuz". Apart from the file names, the "startup.tuz" file acts as an identical replacement for the "aastra.tuz" file. Releases including and above 4.0.0 SP1 support both the "startup.tuz" and "aastra.tuz" files, but if the "startup.tuz" file is available, the phone will disregard the "aastra.tuz" file (if available). The "aastra.tuz" file will be used if the "startup.tuz" file is unavailable and will continue to be supported going forward to ensure backwards compatibility with existing customer deployments.

Encryption is performed using a secret password that is chosen by the administrator.

The encryption tool is also used to create an additional encrypted tag file called *security.tuz*, which controls the decryption process on the IP phones. If *security.tuz* is present on the TFTP/FTP/HTTP server, the IP phones download it and use it locally to decrypt the configuration information from the *startup.tuz* and *<mac>.tuz* files. Because only the encrypted versions of the configuration files need to be stored on the server, no plain-text configuration or passwords are sent across the network, thereby ensuring security of the configuration data.

To make changes to the configuration files, the System Administrator must save the original files.

Note: If the use of encrypted configuration files is enabled (via *security.tuz* or pre-provisioned on the IP phone) the *startup.cfg, <model>.cfg,* and *<mac>.cfg* files are ignored, and only the encrypted equivalent files *startup.tuz, <model>.tuz,* and *<mac>.tuz* are read.

The security feature described above prevents unauthorized parties from **reading** or **writing** the contents of the *<MAC>.tuz* file. It also provides the following:

- Prevents users from using the *<MAC>.tuz* file that does not match the user's phone MAC address.

- Renders the <*MAC*>*.tuz* file invalid if the user renames the file.
- Works with IP phone releases prior to Release 2.2.
- Provides compatibility between the previous encryption routine and the new decryption routine.

PROCEDURE TO ENCRYPT CONFIGURATION FILES

To encrypt the IP phone configuration files (using a Microsoft Windows OS):

1. Obtain the anacrypt encryption tool (anacrypt.exe) from your Mitel representative.
2. Open a command line window application (i.e. DOS window).
3. At the prompt, enter ***anacrypt.exe*** and press <Return>.
4. Enter a command utilizing the details provided in the help screen.

```
C:\> anacrypt.exe -h

Provides encryption of the configuration files used for the
family of Mitel SIP phones.

Copyright (c) 2005-2014, Mitel Networks Corporation.

Usage:

anacrypt {infile.cfg|-d <dir>} [-p password] [-m] [-i] [-v] [-h]
```

ANACRYPT SWITCH	DESCRIPTION
{infile.cfg | -d <dir>}	Specifies that all .cfg files in <dir> should be encrypted.
[-p password]	Specify password used to generate keys.
-m	Generate MAC.tuz files that are phone specific. This switch generates files that are only usable for phones with firmware version 2.2.0 and above.
-v1	Specifies the version of encryption that the anacrypt tool uses. Use version 1 encryption (i.e. -v1) to generate files that are readable by all model phones.
-v2	(Default) Specifies the version of encryption that the anacrypt tool uses. Use version 2 encryption (i.e. -v2) to generate files that are readable by phones with firmware 2.2.0 and above.
-v3	(Enhanced security version) Specifies the version of encryption that the anacrypt tool uses. Use version 3 encryption (i.e. -v3) to generate files that are readable by phones with firmware 3.3.1 and above.
-i	Generate security.tuz file.
-h	Show the help screen.

Notes:

1. Configuration files that are encrypted using v3 encryption can only be decoded by phones on Release 3.3.1 (and above).Customers with v3-encrypted configuration files will lose the ability to decode the files (and in turn will lose all previously configured settings) if they downgrade their phones to any firmware release prior to 3.3.1.
2. An incorrect password produces garbage. For site-specific keyfile security.cfg the plaintext must match the password.

EXAMPLES

The following examples illustrate the use of the anacrypt.exe file.

Example 1

Generating a security.tuz file with password 1234abcd:

For firmware version 3.3.1 (enhanced security):

```
C:\>anacrypt -i -p 1234abcd -v3
```

For firmware version 2.2.0 and above:

```
C:\>anacrypt -i -p 1234abcd
```

or

```
C:\>anacrypt -i -p 1234abcd -v2
```

For any firmware version:

```
C:\>anacrypt -i -p 1234abcd -v1
```

Example 2

Encrypting a single startup.cfg file with password 1234abcd (for firmware version 3.3.1 and above):

```
C:\>anacrypt startup.cfg -p 1234abcd -v3
```

Example 3

Encrypting a <mac>.cfg file with password 1234abcd (for firmware version 3.3.1 and above):

```
C:\>anacrypt 00085d000000.cfg -p 1234abcd -v3
```

Example 4

Encrypting a <mac>.cfg file with password 1234abcd using MAC encryption (for firmware version 3.3.1 and above):

```
C:\>anacrypt 00085d000000.cfg -m -p 1234abcd -v3
```

Example 5

Encrypting all cfg files in C:\data with password 1234abcd using MAC encryption and generating a security.tuz file at the same time (for firmware version 3.3.1 and above):

```
C:\>anacrypt -d C:\data -p 1234abcd -m -i -v3
```

Example 6

Encrypting all cfg files in C:\data with password 1234abcd and generating a security.tuz file at the same time (for firmware version 3.3.1 and above):

```
C:\>anacrypt -d C:\data -p 1234abcd -i -v3
```

VENDOR CONFIGURATION FILE ENCRYPTION

Some vendors can have specific methods to encrypt files on their configuration servers. For each phone, the configuration server can generate a random hex string (encryption key) that is used to encrypt the phone's MAC-specific configuration file.

The encryption key is placed in a plain text MAC-specific configuration file that the server downloads to the phone. After the phone receives the file, it updates the encryption key.

Note: The phone will not reboot automatically after updating the configuration encryption key. Upon the next reboot, the phone will download the encrypted MAC-specific configuration file from configuration server (provided that the unencrypted MAC-specific file is not present on the configuration server)

This method of encryption does not affect the implementation of the Mitel method of file encryption.

Note: The *startup.cfg* file is not encrypted with this feature.

You can set the phone-specific encryption key using the configuration files only.

For more information about configuration file encryption, contact Mitel Technical Support.

CONFIGURING VENDOR CONFIGURATION FILE ENCRYPTION

Use the following procedure to configure vendor configuration file encryption on the IP Phones.

CONFIGURATION FILES

For specific parameters you can set in the configuration files for automatic update, see Appendix A, the section, "Configuration Encryption Setting" on page A-326.

Chapter 8

UPGRADING THE FIRMWARE

ABOUT THIS CHAPTER

This chapter provides information about upgrading the IP phone firmware.

TOPICS

This chapter covers the following topics:

UPGRADING THE FIRMWARE

The IP phones support the protocols, TFTP, FTP, HTTP or HTTPS to download configuration files and upgrade firmware to the phones from a configuration server.

The configuration server should be ready and able to accept connections. For information on configuration server requirements, see Chapter 1, the section, "Configuration Server Requirement" **on** page 1-38**.**

You can download the firmware stored on the configuration server in one of four ways:

- Using the "**Firmware Update**" page in the Mitel Web UI at the location ***Advanced Settings-firmware Update***.
- Using the IP Phone UI or the Mitel Web UI to restart the phone. The phone automatically looks for firmware updates and configuration files during the boot process.
- Setting an **Auto-Resync** feature to automatically update the firmware, configuration files, or both at a specific time in a 24-hour period). (Feature can be enabled using the configuration files or the Mitel Web UI).
- Using the **Manual Software Upgrade** from the **Voice Services** menu after Factory Default of the IP Phone.

USING THE "FIRMWARE UPDATE" PAGE IN THE MITEL WEB UI

You can use the Mitel Web UI to manually force a firmware update from the configuration server to a phone in your network by selecting ***Advanced Settings->Firmware Update***. You can configure the phone to perform the update using any of the protocols that the phone supports: TFTP, FTP, HTTP, or HTTPS.

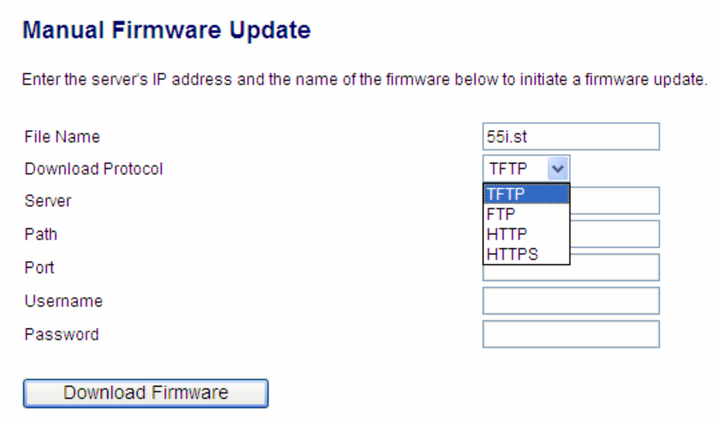
WARNING: DO NOT RESET OR TURN OFF THE PHONE UNTIL THE DOWNLOAD IS COMPLETE.

Note: This procedure downloads an updated <*phone model.st*> file as well as any other firmware files that were updated, to your phone.

Use the following procedure to manually update the firmware on your phone from the specified configuration server.

MITEL WEB UI

1. Click on **Advanced Settings->Firmware Update.**



2. In the "**File Name**" field, enter the firmware file name (*<phone model>.st*) that you want to download to your IP phone. For example, *6867i.st (for a 6867i phone)*.

   Note: This file name must match the actual name of the firmware file residing on your configuration server.

   The phones use the following naming convention for the ***.st*** files. See the following table.

IP PHONE MODEL	ASSOCIATED FIRMWARE
6863i	6863i.st
6865i	6865i.st
6867i	6867i.st
6869i	6869i.st
6873i	6873i.st
6905	6905.st
6910	6910.st
6920	6920.st
6930	6930.st
6940	6940.st
6970	6970.st

3. In the "**Download Protocol**" field, select the protocol from the list to use for downloading the new firmware. Valid values are:
   - TFTP
   - FTP
   - HTTP

- HTTPS

4. In the "**Server**" field, enter the IP address in dotted decimal format, of the TFTP configuration server, or the domain name of the FTP, HTTP, or HTTPS configuration servers (dependent on the protocol you selected in step 3.) For example: 432.221.45.6.
5. In the "**Path**" field, enter the path location on the protocol server for where the new firmware resides. For example, C:\mitel\configserver\firmwareupgrade.
6. In the "**Port**" field, enter the port number of the protocol server. For example, 80 (for HTTP) or 443 (for HTTPS).

   Note: This field is not applicable to the TFTP and FTP protocols.

7. (FTP only) In the "**Username**" field, enter the username that is used for authentication when the FTP server is accessed.
8. (FTP only) In the "**Password**" field, enter the password that is used for authentication when the FTP server is accessed.
9. Click **Download Firmware**.
   This starts the upgrade process. If the upgrade is successful the following message displays on the screen: "Firmware Upgrade Successful".

USING THE "VOICE SERVICES" MENU AFTER FACTORY DEFAULT ON THE IP PHONE UI

Note: Applicable to the 6905, 6910, 6920, 6930, 6940, and 6970 IP Phones only.

After factory default of the 6900 series SIP phone, a Voice Services screen auto-prompts on the IP Phone. You can use the Telephone UI to manually force a firmware update from the configuration server to a phone in your network by selecting **Voice Services** > **Manual Software Upgrade**. You can configure the phone to perform the update using any of the protocols that the phone supports: TFTP, FTP, HTTP, or HTTPS.

WARNING: DO NOT RESET OR TURN OFF THE PHONE UNTIL THE DOWNLOAD IS COMPLETE.

Note: This procedure downloads an updated <*phone model.st*> file as well as any other firmware files that were updated, to your phone.

Use the following procedure to manually update the firmware on your phone from the specified configuration server using the IP Phone UI

IP PHONE UI

1. Navigate to the **Voice Services** > **Manual Software Upgrade.**
2. In the "**Download Protocol**" field, select the protocol from the list to use for downloading the new firmware. Valid values are:
   - TFTP
   - FTP
   - HTTP
   - HTTPS
3. In the "**Server**" field, enter the IP address in dotted decimal format, of the TFTP configuration server, or the domain name of the FTP, HTTP, or HTTPS configuration servers (dependent on the protocol you selected in step 3.) For example: 432.221.45.6.
4. In the "**Path**" field, enter the path location on the protocol server for where the new firmware resides. For example, C:\mitel\configserver\firmwareupgrade.
5. In the "**Port**" field, enter the port number of the protocol server. For example, 80 (for HTTP) or 443 (for HTTPS).

   Note: This field is not applicable to the TFTP and FTP protocols.

6. (FTP only) In the "**Username**" field, enter the username that is used for authentication when the FTP server is accessed.
7. (FTP only) In the "**Password**" field, enter the password that is used for authentication when the FTP server is accessed.
8. Click **Download Firmware**.
   This starts the upgrade process. If the upgrade is successful the following message displays on the screen: "Firmware Upgrade Successful".

USING THE RESTART FEATURE

Restarting the phone forces the phone to check for both firmware and configuration files stored on the configuration server.

WARNING:DO NOT RESET OR TURN OFF THE PHONE UNTIL THE DOWNLOAD IS COMPLETE.

RESTARTING THE PHONE USING THE IP PHONE UI

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Restart Phone**.
3. Press **#** to confirm.

> **Note:** To cancel the Restart, press the key.

For the 6867i/6869i/6920/6930:

1. Press or on the phone to enter the Options List.
2. Select **Restart**. The following prompt displays:
   "Restart phone?"
3. Select **Yes** to restart the phone
   or
   Select **No** to go back to the Options Screen.

For the 6873i/6940/6970:

1. Press , or the **Settings** softkey on the phone to enter the Options List.
2. Tap the **Restart** icon. The following prompt displays:
   "Restart phone?"

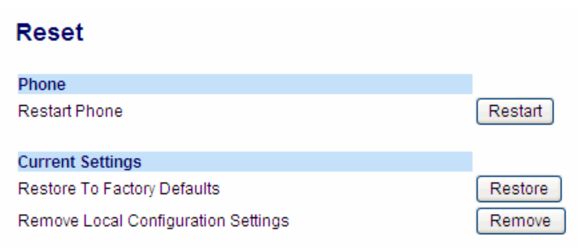
> **Note:** If required, swipe left on the screen to navigate to the second page of options.

3. Tap **Yes** to restart the phone
   or
   Tap **No** to go back to the Options Screen.

RESTARTING THE PHONE USING THE MITEL WEB UI

MITEL WEB UI

1. Click on **Operation->Reset->Phone.**



Click **Restart** to restart the phone.

USING THE AUTO-RESYNC FEATURE

The auto-resync feature on the IP phones allows an administrator to enable the phone to be updated automatically once a day at a specific time in a 24-hour period if the files on the server have changed. This feature works with TFTP, FTP, HTTP, and HTTPS servers. An administrator can enable this feature using the Mitel Web UI or using the configuration files (startup.cfg, <model>.cfg, and <mac>.cfg).

Notes:

1. The automatic update feature works with both encrypted and plain text configuration files.
2. If the IP phones fails to get the automatic updates during the scheduled time of the day, the updates are pushed during the next scheduled auto-resync interval.

An Administrator can enable Auto-Resync using the configuration files or the Mitel Web UI. In the configuration files you set the following parameters:

- **auto resync mode** - Determines whether the configuration server automatically updates the phone's configuration files only, the firmware only, both the firmware and configuration files, or disables automatic updates. This parameter works with TFTP, FTP, HTTP, and HTTPS servers.
- **auto resync time** - Sets the time of day in a 24-hour period for the IP phone to be automatically updated. This parameter works with TFTP, FTP, HTTP and HTTPS servers.
- **auto resync max delay** - Specifies the maximum time, in minutes, the phone waits past the scheduled time before starting a checksync.
- **auto resync days -** Specifies the amount of days that the phone waits between checksync operations.

In the Mitel Web UI, you can set the following parameters at the path *Advanced Settings->Configuration Server->Auto-Resync*:

- Mode
- Time (24 hours)
- Maximum Delay
- Days

Setting the "**auto resync max delay**" (Maximum Delay) and "auto resync days" (Days) parameters can greatly reduce the load placed on the configuration server when downloading configurations.

RELOADING OF DIRECTORY FILES DURING AN AUTO-RESYNC

During an auto-resync, the IP phones have the ability to initiate a comparison of its local directory files with those located on the configuration server and automatically update the local directory files if changes are detected

If the auto-resync mode is set to" Configuration Files (1)" or "Both (3)", either through the IP phone's Web UI or configuration files, when the phone reaches the configured auto-resync date/time, the phone will perform a comparison on the directory files and trigger a reboot if differences are found.

If the auto-resync mode is set to “None (0)” or “Firmware Info (2)” and the phone reaches the configured auto-resync date/time, the directory files will not be checked.

Note: Irrespective of the auto-resync feature, if the phone receives a check-sync NOTIFY, the directory file comparison will be performed and the applicable files will be automatically updated as required.

ENABLING AUTO-RESYNC USING THE CONFIGURATION FILES

Use the following procedure to configure automatic updates of the IP phone firmware, configuration files, or both.

CONFIGURATION FILES

For specific parameters you can set in the configuration files for automatic update, see Appendix A, the section, “Configuration Server Settings” on page A-33.

Notes:

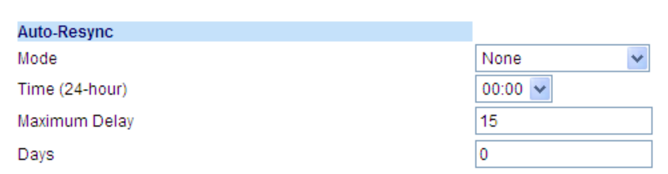
1. If a user is accessing the Mitel Web UI, they are not informed of an auto-reboot.
2. Any changes made using the Mitel Web UI or the IP phone UI are not overwritten by an auto-resync update. Auto-resync affects the configuration files only. However, the settings in the Mitel Web UI take precedence over the IP phone UI and the configuration files.
3. If the IP phone is in use (not idle) at the time of the resync check, the reboot occurs when the phone becomes idle.
4. The resync time is based on the local time of the IP phone.
5. The automatic update feature works with both encrypted and plain text configuration files.

ENABLING AUTO-RESYNC USING THE MITEL WEB UI

Use the following procedure to enable auto-resync for the phones in your network.

MITEL WEB UI

1. Click on **Advanced Settings->Configuration Server->Auto-Resync.**



2. In the “**Mode**” field, select the auto-resync mode you want to use to automatically update the phone.
   Valid values are:
   - **None** Disable auto-resync
   - **Configuration Files** Updates the configuration files on the IP phone automatically at the specified time if the files on the server have changed.
   - **Firmware** Updates the firmware on the IP phone automatically at the specified time if the files on the server have changed.

- **Both** Updates the configuration files and firmware automatically at the specified time if the files on the server have changed.

> **Notes:**
> 1. If a user is accessing the Mitel Web UI, they are not informed of an auto-reboot.
> 2. Any changes made using the Mitel Web UI or the IP phone UI are not overwritten by an auto-resync update. Auto-resync affects the configuration files only. However, the settings in the Mitel Web UI take precedence over the IP phone UI and the configuration files.
> 3. The resync time is based on the local time of the IP phone.
> 4. If the IP phone is in use (not idle) at the time of the resync check, the reboot occurs when the phone becomes idle.

3. In the “**Time (24-hour)**” field, select the time that you want the update to take place. Valid values are 00:00 to 23:30 (in 30 minute increments).

> **Notes:**
> 1. The resync time is based on the local time of the IP phone.
> 2. The value of 00:00 is 12:00 A.M.
> 3. When selecting a value for this parameter in the Mitel Web UI, the values are in 30-minute increments only.

4. In the “**Maximum Delay**” field, specify the maximum time, in minutes, the phone waits past the scheduled time before starting a checksync. The range is 0 to 1439. Default is 15.
5. In the “**Days**” field, specify the amount of days that the phone waits between checksync operations.
The range is 0 to 364. Default is 0.

> **Note:** A value of 0 causes the phone to checksync every time the clock reads the proper time. A value of 1 forces the phone to wait 24 hours prior to doing the first checksync.

6. Click **Save Settings** to save your settings.

> **Notes:**
> 1. These changes are not dynamic.
> 2. You must restart your IP phone for the changes to take affect.

7. Click on **Operation->Reset**.
8. In the "**Restart Phone**" field click **Restart** to restart the IP phone and apply the update. The update performs automatically at the time you designated.

6900 MINET TO SIP CONVERSION

By factory default, the 6900 series IP phones have the MiNet firmware pre-installed. All 6900 phones will need to be upgraded to SIP R5.0 to become interoperable with Mitel’s SIP-based solutions.

SIP UPGRADE OPTIONS FOR PHONES WITH MINET FIRMWARE PRIOR TO 01.01.00.152

Use the following methods to upgrade IP phones pre MiNet firmware 01.01.00.152 to SIP firmware.

Method 1: use static settings for a TFTP server

1. Place the SIP firmware files on the TFTP Server (ensure that no MiNet files are present).
2. Press the Gear button to go into Settings on the 6900 IP phone.
3. Select Advanced Settings (default password is 73738).
4. Select Network and Static Settings.
5. Enter the IP address of the TFTP server (ensure your IP phone has an IP address assigned)
6. Select Restart through the Settings App.
7. The IP phone will attempt to download MiNet firmware from the TFTP server. When not found, it will subsequently download the SIP firmware.
8. Once the 6900 phone is upgraded to the SIP build, optionally remove the files from the TFTP directory.

Method 2: use DHCP option 43

1. Place the SIP firmware files on the TFTP Server. Alternatively, an FTP Server can be used (ensure that no MiNet files are present).
2. Configure DHCP option 43 parameter sw_tftp tag for location of the firmware files (e.g. id:ipphone.mitel.com; tftp://10.30.102.91/firmwarefilesDIR; ftp://test:Aastra123@10.30.102.91/5.0.0.143).
3. Power up the phone.
4. The phone will attempt to download MiNet firmware from the TFTP/FTP server (not found), and will subsequently download the SIP firmware. Note that the config file will not download.
5. Reboot the phone – it will follow existing SIP procedures for configuration and firmware upgrades.

Note: For Mitel 6900 series REV B phones, the minimum supported SIP firmware version is 5.0.0.2036 (R5.0SP2).

Method 3: use DHCP option 66

1. Place the SIP firmware files on the TFTP Server. Alternatively, an FTP Server can be used (ensure that no MiNet files are present).
2. Configure DHCP option 66 with TFTP server URL (e.g. tftp://10.30.102.91/firmwarefiles-DIR; ftp://test:Aastra123@10.30.102.91/5.0.0.143).
3. Power up the phone.
4. The phone will attempt to download MiNet firmware from the TFTP/FTP server (not found). It will subsequently download the SIP firmware. Note that the config file will not be downloaded.

5. Reboot the phone – it will follow existing SIP procedures for configuration and firmware upgrades.

Method 4: use RCS

1. SIP 6.0 firmware will be available at RCS at GA time.
2. Add the MAC address for the phone to RCS.
3. Configure RCS to use SIP 6.0 firmware for the phone's MAC.
4. Power up the phone.
5. The phone will contact RCS and if its MAC is found on RCS it will download the firmware.
6. Reboot the phone – it will follow existing SIP procedures for configuration and firmware upgrades.

6900 SIP TO MINET CONVERSION

In Release 5.0.0, it is possible to roll back 6900 Series phone models from SIP to MiNet. This release supports SIP to MiNet conversion through the following methods:

- DHCP options
- Firmware Download Server configured through TUI or configuration file
- Manual firmware update through Web UI

Note: Using these conversion methods, 6900 SIP Series phones search for SIP firmware files (69xx.st) and if not found, search for MiNet firmware.

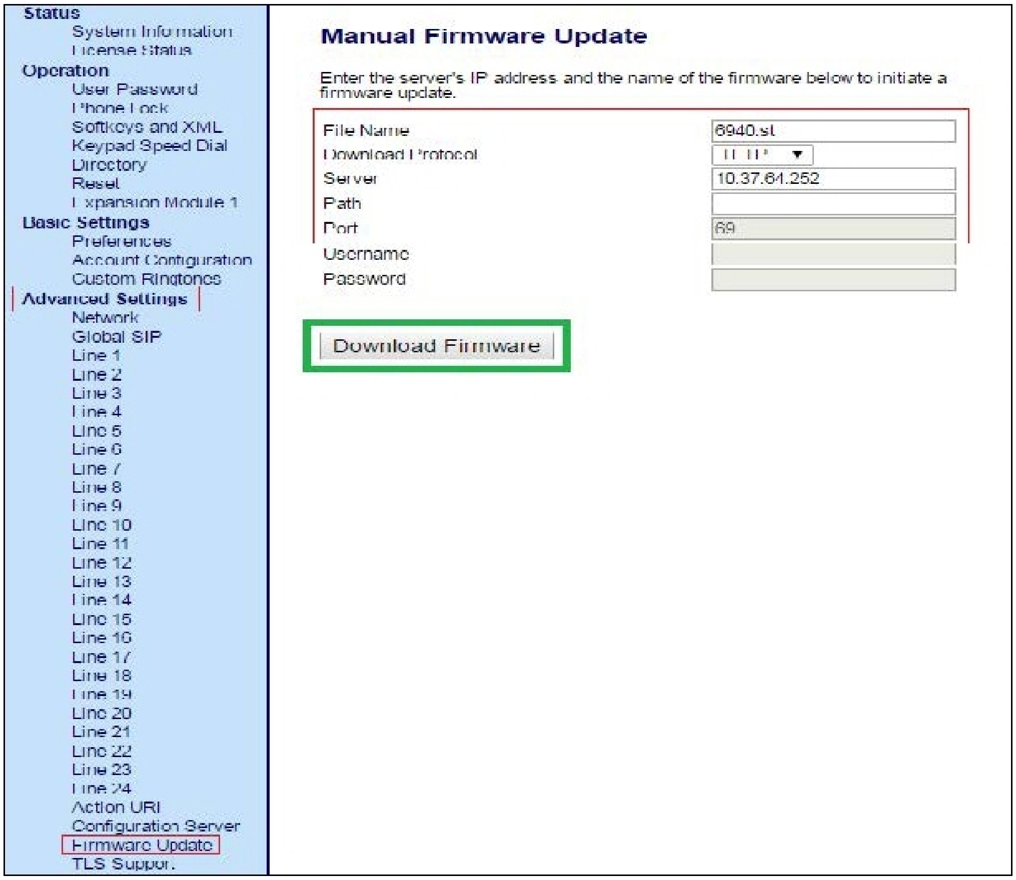
PROCEDURE FOR SIP TO MINET CONVERSION

The SIP image has a key to encrypt the MiNet image header and supports decryption of the MiNet image.

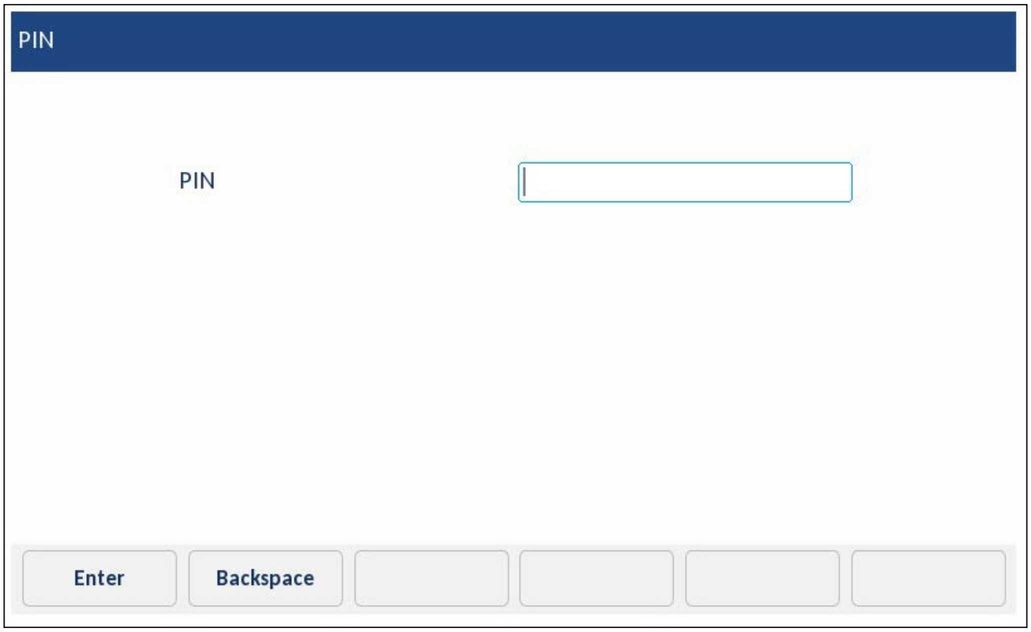
Following is the procedure for 6900 series SIP to MiNet conversion:

1. Copy and save the MiNet (MINET_69XX-enc.st) on TFTP server directory for each 6900 series phone model.
2. From the SIP phone's Web UI, navigate to **Advanced Settings/Firmware Update** form and enter respectively: Filename as MINET_69XX-enc.st, Download Protocol as TFTP and the TFTP server IP address information (add path and port if required) and press **Download Firmware**.

Note: During TFTP download of a MiNet firmware file exceeding 32M, ensure to set the lease expiry time of the DHCP server to at least 30 mins to prevent possible download failure.



3. The phone TUI updates with “**Checking For Firmware**”.
4. After the firmware has been uploaded, the phone will restart in MiNet mode.
5. Once the phone boots up in MiNet mode, enter the PIN to log in or register the phone as required by the TUI screen message.
6. If the phone was not previously configured, enter minimal static settings such as the **Call Server IP Address**.
7. Press the **Option** key, select the **Advanced** softkey, and enter admin login credentials.
8. Navigate to **Network Settings** and enter the **Call Server IP Address** and click **Save**.
9. Navigate to the TUI screen and enter the respective PIN request to log in or register a specific user: ***XXXX.


PIN
PIN
Enter
Backspace

Chapter 9

TROUBLESHOOTING

ABOUT THIS CHAPTER

This chapter describes tasks that a system administrator can perform on the IP phones for troubleshooting purposes. It also includes answers to questions you may have while using the IP phones.

TOPICS

This chapter covers the following topics:

TROUBLESHOOTING

This section describes tasks that a system administrator can perform on the IP phones for troubleshooting purposes. Using the Mitel Web UI, a system administrator can:

- Assign an IP address and IP port to which log information will be transmitted
- Filter the logs according to severity
- Save the current local configuration file to a specified location
- Save the current server configuration file to a specified location
- Save the current user configuration file to a specified location (if logged on using the Visitor Desk Phone feature).
- Save the current user_local configuration file to a specified location (if logged on using the Visitor Desk Phone feature).
- Show task and stack status (including “Free Memory” and “Maximum Memory Block Size”)

Mitel Technical Support can then use the information gathered to perform troubleshooting tasks.

LOG SETTINGS

Using the configuration files or the Mitel Web UI, you can specify the location where log information will be stored for troubleshooting purposes.

In the configuration files, you use the following parameters to configure log settings:

- **log server ip** - The IP address of the log server to which log information will be transmitted.
- **log server port** - The IP port of the log server.

In the Mitel Web UI, you use the following parameters to configure log settings:

- **Log IP** -The IP address of the log server to which log information will be transmitted
- **Log Port** - The IP port of the log server.

Note: You can disable the above by clearing the Log IP address field.

REFERENCES

For more information about the log setting configuration parameters, see , the section, “Troubleshooting Parameters” on page 350.

For information about configuring the log settings using the Mitel Web UI, see “Performing Troubleshooting Tasks” on page 9-8.

MODULE/DEBUG LEVEL SETTINGS

The Mitel IP phones provide blog module support that allows enhanced severity filtering of log calls sent as blog output.

The blog, as used on the IP phones, is a an online debugging tool that can be frequently updated and intended for technical support analysis. Blogs are defined by their format: a series of entries posted to a single page in reverse-chronological order. The IP Phone blogs are separated into modules which allow you to log specific information for analyzing.

Note: Enabling the syslog module and configuring debug levels should only be used for support purposes. Mitel recommends Administrators leave the debug level at its default for normal production use. Enabling all the debug levels on the phone will impact performance and normal operation of the phone.

The following table identifies the blog modules you can set.

MITEL WEB UI PARAMETERS	CONFIGURATION FILE PARAMETERS
LINMGR (Line Manager information)	log module linemgr
AUDIOMGR (Audio Manager information)	log module audiomgr
UI (User Interface (UI) related)	log module user interface
MISC (Miscellaneous)	log module misc
SIP (Call control SIP stack)	log module sip
DIS (Display drivers)	log module dis
DSTORE (Delayed storage)	log module dstore
EPT (Endpoint module)	log module ept
IND (Indicator module)	log module ind
KBD (Keyboard module)	log module kbd
NET (Network module)	log module net
PROVIS (Provisioning module)	log module provis
RTPT (Realtime Transport module)	log module rtpt
SND (Sound module)	log module snd
PROF (Profiler module)	log module prof
XML (Extension Markup Language)	log module xml
LLDP (Link Layer Discovery Protocol)	log module lldp

SETTING VALUES FOR THE MODULE/DEBUG LEVELS

There are 14 debug levels for the modules. Each debug level has a value you can use to turn individual levels ON and OFF. The following table identifies these debug levels and their values.

DEBUG LEVEL	VALUE
Fatal Error	1
Error	3
Warning	7
Initialization	15
Functions Entry Exit	31
Info	63
User1	127
User2	255
User3	511
User4	1023
User5	2047
User6	4095
User7	8191 (default)
User8	16383 or 65535

The following table identifies the default logging values for the configuration file parameters.

CONFIGURATION FILE PARAMETERS	DEFAULT VALUE
log module sip	1
log module dis	1
log module dstore	1
log module ept	1
log module ind	1
log module kbd	1
log module net	1
log module rtpt	1
log module snd	1
log module prof	1
log module xml	1
log module lldp	1
log module linemgr	1
log module audiomgr	1
log module user interface	1
log module misc	1

CONFIGURATION FILE PARAMETERS	DEFAULT VALUE
log module provis	1

Notes:

When the log issue parameter is disabled (default value), logging levels for all modules will be default to 1 unless set differently in the configuration files.

When the log issue parameter is enabled, the IP phone sets the logging level to 8191 for the following modules:

- log module linemgr: 8191
- log module audiomgr: 8191
- log module user interface: 8191
- log module misc: 8191
- log module sip: 8191(When registered with MiCloud Connect or MiVoice Connect)
- log module provis: 8191

For details, see on page A-355.

Example 1

To turn two or more debug levels on at the same time, you add the value associated with each level. For example,

Fatal Errors + Errors + Warnings = 1 + 2 + 4 = **7**

```
log module linemgr: 7
log module user interface: 7
log module sip: 7
```

In the above example, fatal errors, general errors, and warnings are logged for the line manager, user interface, and SIP call control modules.

Example 2

Functions and Info = 16 + 32 = **48**

```
log module dis: 48
log module net: 48
log module audiomgr: 48
```

In the above example, functions and general information are logged for the display drivers, network, and sound modules.

Example 3

```
log module rtpt: 0
log module ind: 65535
```

In the above example, all debug levels are OFF for the Real Time Transport module. All debug levels are ON for the indicator module.

You can set the Module/Debug Levels using the configuration files or the Mitel Web UI.

References

For more information about the debug level configuration parameters, see , the section, “Troubleshooting Parameters” on page 350.

For information about configuring the log settings using the Mitel Web UI, see “Performing Troubleshooting Tasks” on page 9-8.

SUPPORT INFORMATION

You can save the local and/or server configuration files of the IP phone to the location specified in the "Log Settings" section.

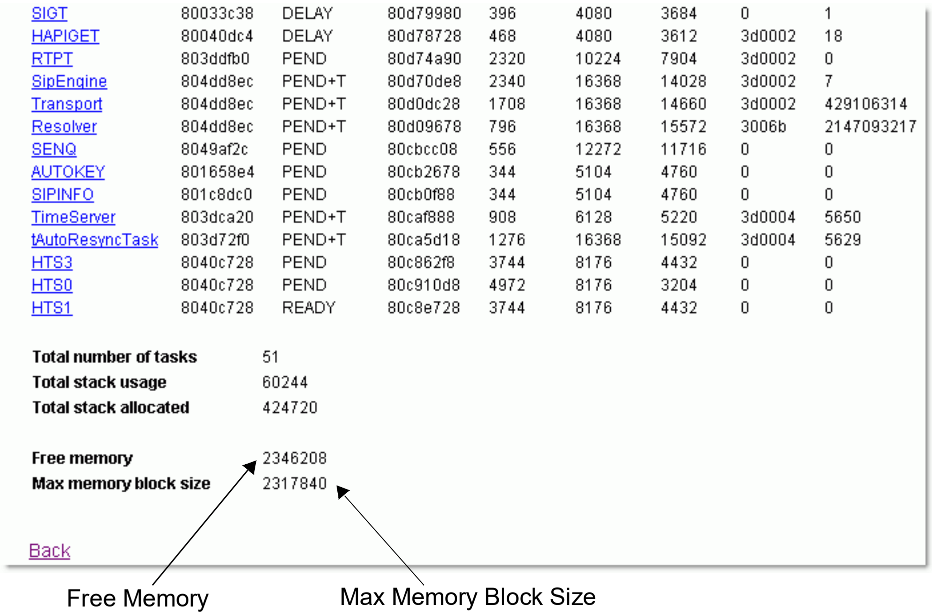
Performing this task allows Mitel Technical Support to view the current configuration of the IP phone and troubleshoot as necessary.

In the “Support Information” section, you can:

- Get local.cfg
- Get server.cfg
- Get <user>.cfg (if logged on using the Visitor Desk Phone feature; see "Visitor Desk Phone Support," on page 102 for details)
- Get <user>_local.cfg (if logged on using the Visitor Desk Phone feature; see "Visitor Desk Phone Support," on page 102 for details)
- Get Log Files
- Show Task and Stack Status

Mitel Technical Support uses this support information for troubleshooting the IP phone when required.

Using the Mitel Web UI and selecting “**Show Task and Stack Status**” displays the tasks and stack status on the IP phone. This screen also displays the **Free Memory** and the **Max Block Free Memory** currently on the phone as shown in the following illustration. This information is for troubleshooting purposes only.



SIGT	80033c38	DELAY	80d79980	396	4080	3684	0	1
HAPIGET	80040dc4	DELAY	80d78728	468	4080	3612	3d0002	18
RTPT	803ddfb0	PEND	80d74a90	2320	10224	7904	3d0002	0
SipEngine	804dd8ec	PEND+T	80d70de8	2340	16368	14028	3d0002	7
Transport	804dd8ec	PEND+T	80d0dc28	1708	16368	14660	3d0002	429106314
Resolver	804dd8ec	PEND+T	80d09678	796	16368	15572	3006b	2147093217
SENQ	8049af2c	PEND	80cbcc08	556	12272	11716	0	0
AUTOKEY	801658e4	PEND	80cb2678	344	5104	4760	0	0
SIPINFO	801c8dc0	PEND	80cb0f88	344	5104	4760	0	0
TimeServer	803dca20	PEND+T	80caf888	908	6128	5220	3d0004	5650
tAutoResyncTask	803d72f0	PEND+T	80ca5d18	1276	16368	15092	3d0004	5629
HTS3	8040c728	PEND	80c862f8	3744	8176	4432	0	0
HTS0	8040c728	PEND	80c910d8	4972	8176	3204	0	0
HTS1	8040c728	READY	80c8e728	3744	8176	4432	0	0

Total number of tasks	51
Total stack usage	60244
Total stack allocated	424720

Free memory	2346208
Max memory block size	2317840

Back

PERFORMING TROUBLESHOOTING TASKS

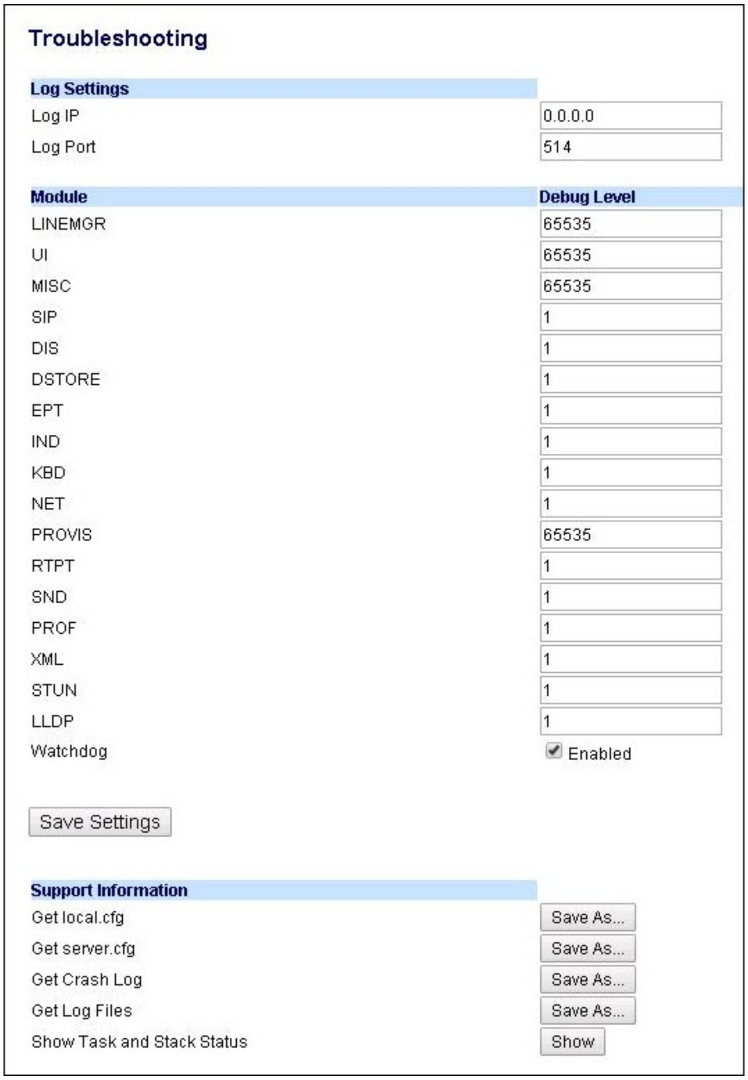
Use the following procedures to perform troubleshooting on the IP phone via the configuration files or the Mitel Web UI.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see , the section, "Log Settings" on page A-350.

MITEL WEB UI

1. Click on **Advanced Settings->Troubleshooting**.



To set log settings:

2. In the "**Log IP**" field, enter the IP address of the log server (i.e. the server to which log information will be transmitted).

3. In the "**Log Port**" field, enter the port number associated with the IP address specified in the "Log IP" field. This port passes the information from the IP phone to the IP address location.

4. Click **Save Settings** to save your settings.

5. Click on **Operation->Reset**.

6. In the "**Restart Phone**" field click **Restart** to restart the IP phone.

To set blog modules:

7. Select the applicable module.
8. Enter a debug level value in the "**Debug Level**" field for a module. Valid values are:

DEBUG LEVEL	VALUE
Fatal Errors	1
Errors	2
Warnings	4
Init	8
Functions	16
Info	32
All debug levels OFF	0
All Debug Levels ON	65535

The value of "**0**" turns all debug levels OFF for a module. The value of "**65535**" turns all debug levels ON for a module.
To turn two or more debug levels on at the same time, you add the value associated with each level. For example, Fatal Errors + Errors + Warnings = 1 + 2 + 4 = **7**

log module linemgr: 7
log module user interface: 7
log module sip: 7

In the above example, fatal errors, general errors, and warnings are logged for the line manager, user interface, and SIP call control modules.

9. Click **Save Settings** to save your settings.
10. Click on **Operation->Reset**.
11. In the "**Restart Phone**" field click **Restart** to restart the IP phone.

To perform support tasks:

12. To store the local configuration file to the specified location, click on **Save As** in the "**Get local.cfg**" field.
13. To store the server configuration file to the specified location, click on **Save As** in the "**Get server.cfg**" field.
14. To retrieve phone logs (syslogs) from the SIP phone, click on **Save As** in the "**Get Log Files**" field.
15. To display task and stack status information, as well as Free Memory and Maximum Block Free Memory on the phone, click on **Show** in the "**Show Task and Stack Status**" field.

Note: The local and server configuration file information and the task and stack status information is for use by Mitel Technical Support for troubleshooting purposes.

Reference

For information that describes solutions to most common problems using the IP phones, see the next section, "Troubleshooting Solutions" on page 9-23.

WATCHDOG TASK FEATURE

The IP Phones include a troubleshooting feature called the "**WatchDog**" that monitors the status of the phone's tasks and provides the ability to get stack traces from the last time the phone failed. When the phone detects a failure (i.e. a crash), it automatically reboots. You can view a WatchDog crash file using the Mitel Web UI at the path, *Advanced Settings->Troubleshooting*. You can enable/disable the WatchDog task using the configuration files or the Mitel Web UI.

ENABLING/DISABLING WATCHDOG

Use the following procedure to enable/disable the WatchDog.

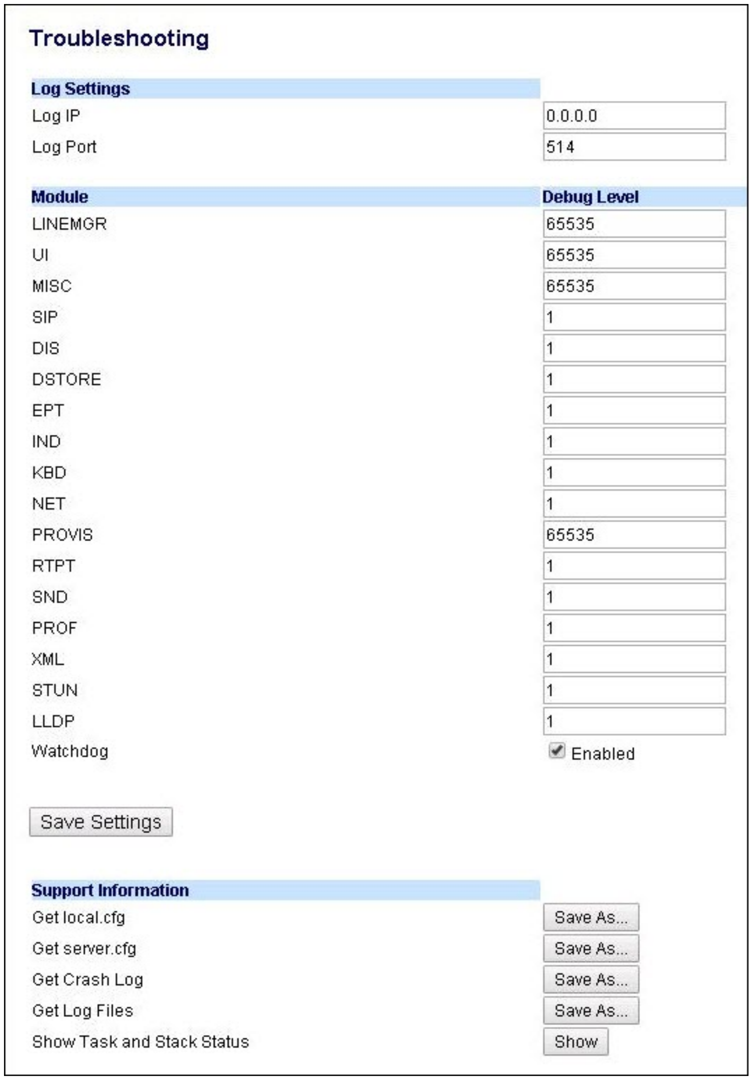
CONFIGURATION FILES

For specific parameters you can set in the configuration files, see , the section, "WatchDog Settings" on page A-352.

Use the following procedure to enable/disable the WatchDog task for the IP Phones using the Mitel Web UI. You can also view the “Crash Log” generated by the WatchDog task using the Mitel Web UI.

MITEL WEB UI

1. Click on **Advanced Settings->Troubleshooting.**



Enable/Disable WatchDog Task

2. The “**WatchDog**” field is enabled by default. To disable the WatchDog task, click in the “Enabled” box to clear the check mark.

3. Click **Save Settings** to save your changes.

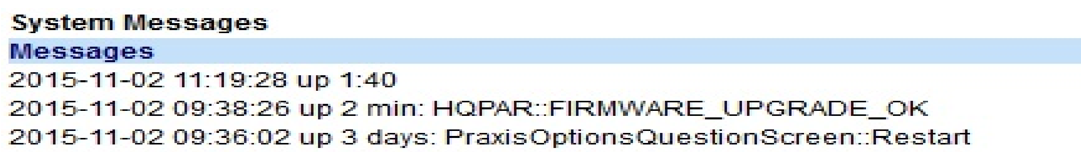
View the Crash Log

4. To view a crash log, in the “**Get a Crash Log**” field, click the **SAVE AS** button. You can open the file immediately, or you can save the Crash Log to your PC.

SYSTEM MESSAGES DISPLAY

When the phone reboots, information regarding the reboot is added to the reboot.log file and can also be viewed in the *Advanced Settings->Troubleshooting->System Messages* menu through the phone's Web UI.

The image below is an example of the information System Messages section of the Web UI upon reboot. This same information is logged in the reboot.log file.



The first line of the log details the current date, time, and up time, and the subsequent lines encompass the reboot information (up to nine lines sorted from newest event to oldest). The reboot information encompasses the date and time of the reboot (2015-11-02 09:35:02), the up time (up 3 days), and the reboot code/cause of the reboot (PraxisOptionsRestartScreen::Restart).

The following table lists the reboot codes that are supported in this release and a description of what the codes mean:

REBOOT CODE	DESCRIPTION
WEBUI::Restart	Reboot prompted by pressing the **Restart** button in the **Operation > Reset > Phone** menu of the Web UI or by changing the network configuration settings through the Web UI.
AutoResync::ForceResync	Reboot triggered by an external event (primarily when a reboot is prompted by the processing of a NOTIFY message with a resync request).
AutoResync::TimeForResync	Reboot prompted due to scheduled auto resync time (when the scheduled time arrives, the phone will check with the configuration server and if any changes are detected, the phone will reboot).
MAINTASK::8021X	Reboot prompted due to 802.1x configuration changes.
HQPAR::FIRMWARE_UPGRADE_OK	Reboot prompted by the detection of new firmware during boot up.
HQPARS::CFG_ENCRYPTION_KEY	Reboot prompted by the detection of vendor configuration file encryption key changes during boot up.
TR69::rebootHandler	Reboot prompted by a restart initiated through TR-069.
TR69::FACTORYRESET	Reboot prompted by a factory reset initiated through TR-069.

REBOOT CODE	DESCRIPTION
HttpDigestLoginAppPraxis::AppActionRestarting (6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970) or HttpDigestLoginAppText::LOGIN_RESTARTING (6863i, 6865i, 6905, and 6910)	Reboot prompted by the detection of correct HTTP Digest login credentials.
OPTION::RESET (6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970) or ResetConfigAction::performAction (6863i, 6865i, 6905, and 6910)	Reboot prompted by erasing the local settings of the phone through the Options menu of the phone’s native UI.
OPTION::FACTORYDEFAULT (6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970) or FactoryDefaultAction::performAction (6863i, 6865i, 6905, and 6910)	Reboot prompted by a factory default of the phone through the Options menu of the phone’s native UI.
PraxisOptionsQuestionScreen::Restart (6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970) or TUI::mreset (6863i, 6865i, 6905, and 6910	Reboot prompted by the manual restarting of the phone through the Options menu of the phone’s native UI.
XMLCommand: Reset	Reboot prompted by the processing of a Reset XML command.
XMLCommand: FastReboot	Reboot prompted by the processing of a FastReboot XML command.
XMLCommand: ClearLocal	Reboot prompted by the processing of a ClearLocal XML command.
PHONEAPP::DHCP_NEW	Reboot prompted by the IP address of the phone dynamically changing via DHCP. **Note:** In this scenario, reboot information is not logged in the syslog, but is displayed on the Error Messages section of the Troubleshooting menu of the phone’s Web UI.
RCS::UpdateFirmware	Reboot prompted by a firmware update initiated by the Redirection and Configuration Service (RCS). **Note:** In this scenario, reboot information is not logged in the syslog, but is displayed on the Error Messages section of the Troubleshooting menu of the phone’s Web UI.
FirmwardUpgradePage::SetPage	Reboot prompted by manually updating the firmware through the **Advanced Settings > Firmware Update** menu of the Web UI.

ERROR MESSAGES DISPLAY

An Administrator can view generated error messages that may have occurred during startup or reboot of the IP Phones. The IP Phone UI has a selection on the Phone Status page called, "**Error Messages**" at the location, *Options->Phone Status->Error Messages* (6863i, 6865i, 6905, and 6910) or *Options->Status->Error Messages* (6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970). The Mitel Web UI also allows you to view these error messages at the location *Advanced Settings->Troubleshooting->Error Messages*. These options allow you to view error messages generated by modules during startup only (not after registration has completed). You can use this information for troubleshooting purposes or for reporting the errors to the Administrator.

The IP Phone stores and displays up to 10 error messages (any extra error messages beyond 10 are discarded). The time and date of each error message also displays. After a reboot, the previous error messages are discarded and, if applicable, new error messages display. If there are no error messages during startup or after a reboot, the message, "*No Error Messages*" displays on the screen. Error messages display in the language currently set on the phone.

The following table identifies the possible error messages that may display.

POSSIBLE ERROR MESSAGE	DESCRIPTION
Bad Certificate	A Transport Layer Security (TLS) certificate is not valid. The invalid certificate can be any of the following: • root and intermediate certificate • local certificate • private key filename • trusted certificate
802.1x Startup Failed	The Extensible Authentication Protocol TLS (EAP-TLS) certificates and/or the EAP-MD5 information has failed on the phone.
LLDP Startup Failed	Link Layer Discovery Protocol (LLDP) failed during startup of the phone.
HTTP Connection Manager Init Failed	The Hypertext Transfer Protocol (HTTP) connection manager initialization failed while updating the configuration on the phone.
Failed to Config Line Manager	The configuration of the Line Manager module on the phone has failed.

VIEWING THE ERROR MESSAGES USING THE IP PHONE UI

Use the following procedure to view the error messages, if any, that generated during startup.

IP PHONE UI

1. Press the **Options** key on the phone to enter the Options List.
2. Select **Phone Status** (6863i/6865i/6905/6910) or **Status** (6867i/6869i/6873i/6920/6930/6940/6970).
3. Select **Error Messages**.
4. If error messages display, use the ▲ and ▼ or navigation keys (or swipe on the 6873i, 6940, and 6970) to view the messages. If no error message exist, the message, "*No Error Messages*" displays on the screen.
5. When done viewing, press **Back or Cancel** to exit the Error Messages screen.

Viewing the Error Messages Using the Mitel Web UI

Use the following procedure to view the error messages, if any, that generated during startup.

MITEL WEB UI

1. Click on **Advanced Settings->Troubleshooting->Error Messages.**

Error Messages

Date/Time	Error Messages
	No Error Messages

2. Scroll down to the "**Error Messages**" section to view the error messages that may have generated during startup or reboot of the IP Phone.

WARNING MESSAGE DISPLAY

Previously when a phone fails to download from the first configuration server as listed in the Fully Qualified Domain Name (FQDN) server list, it attempts to download from the other servers from the list. If the phone successfully downloads from the alternate server, it would display an Error message on the idle screen. This Error message is now classified as a Warning message and is not displayed to the end user on the idle screen.

Administrators will see the warning message along with other error messages in the Web UI (**Advanced Settings -> Troubleshooting -> Error Messages**) or on the Phone UI (**Options Key -> Phone Status -> Error Messages**).

CONFIGURATION AND CRASH FILE RETRIEVAL

In addition to using the Troubleshooting page in the Mitel Web UI, an Administrator can also use three new configuration parameters in the configuration files to enable/disable the uploading of support information to a pre-defined server. These parameters are:

- **upload system info server** - Specifies the server for which the phone sends the system and crash files.
- **upload system info manual option** - Enables and disables the ability to manually upload support information from the IP Phone UI and Mitel Web UI.
- **upload system info on crash** - Enables and disables the watchdog to automatically reboot the phone and send a crash file to the pre-defined server.

When this feature is enabled (configuration files only), support files can be automatically or manually generated and uploaded when the server detects a phone failure. An Administrator or User can manually send the files when required using the IP Phone UI or the Mitel Web UI. Each time the files are generated and uploaded, a new timestamp on the file name is created so that existing files are not overwritten on the server. File names are generated in the format ***MAC ID_Date_Time_server.cfg, MAC ID_Date_Time_local.cfg, MAC ID_Date_Time_crash.gz, MAC ID_Date_Time_summary.log,*** *and* ***MAC ID_Date_Time_reboot.log.***

Notes:

1. The phone performs the generation and sending of Support Information in the background. This feature does not affect the use or operation of the phone.

2. During a startup or reboot of the phone, an upload of Support Information is automatically generated and sent to the pre-defined server.

3. This feature supports the TFTP, FTP, HTTP, and HTTPS protocols.

The following table identifies the methods you can use to retrieve support information from the phone to the pre-defined server when the above configuration parameters are enabled.

METHOD FOR RETRIEVING SUPPORT INFO	DESCRIPTION
Configuration Files (automatic retrieval)	1. Enter "**upload system info server**" parameter in the configuration files and specify the server for which the phone sends the system crash information 2. Enter "**upload system info on crash: 1**" to enable the phone to automatically send system crash information to the pre-defined server each time the watchdog reboots.
IP Phone UI (manual retrieval)	1. On the phone, navigate to ***Options->Status->Upload System Info***. 2. Press "**Select**" or "**Enter**". The system information is immediately sent to the pre-defined server and the message "*Files Sent*" displays.
Mitel Web UI (manual retrieval)	1. On the Mitel Web UI, navigate to ***Status->System Information->Support Information***. 2. Press <**Upload**>. The system information is immediately sent to the pre-defined server and the message "*Files Sent*" displays.

When this feature is enabled, the phone sends the following support information files to the server:

- **Server.cfg** - File in the format ***MAC ID_Date_Time_server.cfg*** that contains configuration information from the startup.cfg, the <model>.cfg, and the <mac>.cfg files. The MAC address, date, and time are specified in the file name to identify the phone sending the information, and the date and time the file was generated and sent to the server.
(for example, **00093D435522_2010-02-25_1141am_server.cfg**)
- **Local.cfg** - File in the format ***MAC ID_Date_Time_local.cfg*** that contains information of locally modified values made using the Mitel Web UI and/or the IP Phone UI. The MAC address, date, and time are specified in the file name to identify the phone sending the information, and the date and time the file was generated and sent to the server.
(for example, **00043D199345_2010-02-26_1030am_local.cfg**)
- **Crash.gz** - (only generated if an error or crash occurs on the phone) File in the format ***MAC ID_Date_Time_crash.gz*** that contains information about a current phone error/crash causing a reboot of the phone. The MAC address, date, and time are specified in the file name to identify the phone sending the information, and the date and time the crash occurred. The crash file is compressed as in gzip format.
(for example, **00033D000111_2010-02-27_0204pm_crash.gz**)
- **summary.log** - File in the format ***MAC ID_Date_Time*_summary.log** that contains details of the last 10 error messages generated by the phone's modules during startup.
- **reboot.log** - File in the format ***MAC ID_Date_Timer_reboot*.log** that contains information regarding the latest phone reboots.

CONFIGURING CRASH FILE RETRIEVAL USING THE CONFIGURATION FILES

Use the following procedure to configure crash file retrieval from the phone to a server.

CONFIGURATION FILES

For specific parameters you can set in the configuration files, see , the section, "Crash File Retrieval" on page A-354.

GENERATING AND SENDING SUPPORT INFORMATION FROM THE IP PHONE UI

Use the following procedure to generate and send Support Information files to the server.

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Phone Status**.

3. Select **Upload System Info** and press **<Enter>.** The phone immediately generates the applicable Support Information files (server.cfg, local. cfg, and/or crash.gz) and sends the files to the pre-defined server. The message "*Files Sent*" displays.

For the 6867i/6869i/6920/6930:

1. Press [⚙] or [⚙] on the phone to enter the Options List.
2. Select **Status**.
3. Press the **Sys Info** softkey. The following prompt displays:
   "Upload System Info Files?"
4. Select **Yes.** The phone immediately generates the applicable Support Information files (server.cfg, local. cfg, and/or crash.gz) and sends the files to the pre-defined server. The message "*Files Sent*" displays.

For the 6873i/6940/6970:

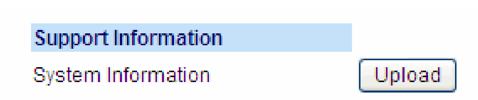
1. Press [⚙], [⚙] or the **Settings** softkey on the phone to enter the Options List.
2. Tap the **Status** icon.
3. Tap the **Sys Info** softkey. The following prompt displays:
   "Upload System Info Files?"
4. Tap **Yes.** The phone immediately generates the applicable Support Information files (server.cfg, local. cfg, and/or crash.gz) and sends the files to the pre-defined server. The message "*Files Sent*" displays.

GENERATING AND SENDING SUPPORT INFORMATION FROM THE MITEL WEB UI

Use the following procedure to generate and send Support Information files to the server.

MITEL WEB UI

1. Click on **Status->System Information-> Support Information.**



2. Press <**Upload**>. The phone immediately generates the applicable Support Information files (server.cfg, local. cfg, and/or crash.gz) and sends the files to the pre-defined server. The message "*Files Sent*" displays.

LIMITATIONS

- If sending the Support Information files to a folder on the server, then write privileges must be allowed for that folder.
- If the Administrator password and username are configured in the Server.cfg file, a User can retrieve that information after the Server.cfg file is loaded to the server.

- TFTP does not report transmission failure if the destination server is down. In this case, the Support Information files are not sent.

TCPDUMP NETWORK PACKET CAPTURE SUPPORT

Tcpdump network packet capture functionality is natively available on the phones. By navigating to the Advanced Settings > Capture page on the phone's Web UI, Administrators can configure/perform the following:

- **Port:** The port, ports, or range of ports from where the phone should capture traffic.
- **Timeout:** The amount of time (in hours) the capture should extend until. The range is from 1 to 168 (7 days) and the default is 24 (1 day). The capture will automatically stop when the timeout is met.
- **Get capture file:** Allows you to save the capture file to the desired directory.
- **Start/Stop:** Allows you to start/stop the tcpdump capture.

Notes:

1. Tcpdump capture functionality in this release supports phone side capture and storage for troubleshooting issues that are of a consistent and reproducible nature. For larger or long duration capture, Administrators are recommended to capture on the network side using a hub or switch with port mirroring.
2. If attempting to capture packet data relating to an issue, Mitel recommends Administrators perform multiple captures of the issue (if possible) to ensure the respective packet data is collected.
3. The type of packets captured (TCP or UDP) is dependent on the transport protocol configured on the phone.
4. Tcpdump packet data is not captured during the reboot process and the feature is automatically disabled upon reboot. Administrators must re-enable the feature after a reboot to resume Tcpdump capture functionality.
5. To change the **Port** or **Timeout** settings, do the following:
    1. Stop and save the current capture.
    2. Modify the **Port** or **Timeout** settings.
    3. Start and Stop the capture.
    4. Save the capture.

DUMPING/RETRIEVING CAPTURES ON PHONE'S FLASH VS. USB DRIVE INTERACTION

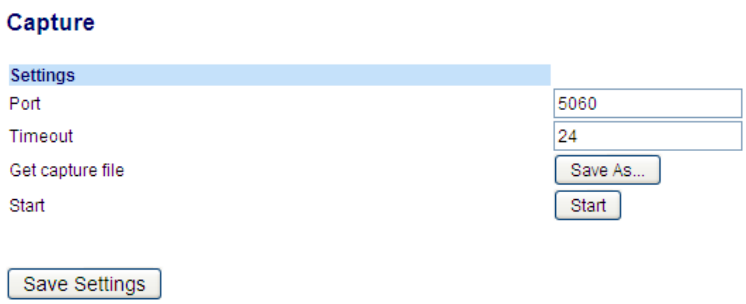
1. **Dumping data**
   The phone starts saving data to the flash memory of the phone if an external USB device is not attached to the phone while starting the capture. However, this behavior continues even after you connect a USB device to the phone during the capture. If the administrator wants to save the capture to a USB device, the capture must start when the USB device is connected to the phone.
2. **Retrieving capture**
   As an Administrator, you can retrieve the saved data from the flash memory by removing the USB device from the phone and clicking Save As.

CONFIGURING/ENABLING TCPDUMP CAPTURE FUNCTIONALITY USING THE MITEL WEB UI

Use the following procedure to configure/enable Tcpdump capture functionality using the Web UI:

MITEL WEB UI

1. Click on **Advanced Settings > Capture.**



2. In the **Port** field, enter the port or ports from where the phone should capture traffic (e.g. 5000:6000;7000).

   Notes:

   1. The default is 5060.
   2. Use a colon (i.e. ":") or hyphen (i.e. "-") to set a range. For example, 5000:6000 or 5000-6000 will capture traffic from ports 5000 through to 6000.
   3. Use a semi-colon (i.e. ";") to add individual ports. For example, 5000;6000;7000 will capture traffic from ports 5000, 6000, and 7000.
   4. Ranges and individual ports can be combined. For example, 5000:7000;8000 will capture traffic from ports 5000 through to 7000 as well as capture traffic from port 8000.
   5. Packets on port 23 (Telnet) will not be captured.

3. In the **Timeout** field, enter the amount of time (in hours) the capture should extend until (e.g. 48).

   Notes:

   1. The default is 24 hours.
   2. The range is from 1 hour to 168 hours (7 days).

4. Click **Save Settings.**
5. Click on **Advanced Settings > Capture.**
6. Click **Start** to begin the capture.

   Note: At any time, navigate back to **Advanced Settings > Capture** and click **Stop** to end the capture manually. Otherwise, the capture will end automatically when the timeout has been reached.

7. When the capture has ended, navigate back to **Advanced Settings > Capture** and click the Get capture file -- **Save As...** button to save the tcpdump.pcap file.

TROUBLESHOOTING SOLUTIONS

DESCRIPTION

This section describes solutions to some most common problems that can occur while using the IP phones.

WHY DOES MY PHONE DISPLAY “APPLICATION MISSING”?

If you have experienced networking issues while the phone was downloading the application from the TFTP server, it is possible that the phone can no longer retrieve the required firmware file. In the event that the phone is no longer able to communicate with the TFTP server in its attempt to re-download the firmware and the phone cannot locate the application locally, the message "Application missing" displays.

The phone also displays the following: “Recovery web-client at: <*IP Address*>”. The IP Address displayed is the IP address of the phone. If the phone is unable to receive an IP from the DHCP server or has lost its record of its static IP, the phone auto-assigns itself the default IP 192.168.0.50.

To recover the firmware for your phone in this circumstance, please perform the following:

1. Launch your web browser on your computer.

> **Note:** Your computer needs to be on the same network as your IP Phone.

2. In the URL, type: “**http://<*IP Address*>**” (where IP Address is the IP Address displayed on the phone). Your browser launches the **Mitel IP Phone Firmware Recovery** page.
3. Call Customer Support and request a <*phone model*>*.st* file.
4. Copy the file to your TFTP server.
5. Enter the <*phone model*>*.st* file that is ready for download.
6. Enter the IP address or qualified domain name of the TFTP server.
7. Press the Download Firmware button.

Please ensure that the TFTP server is running and accessible on the network. If the firmware file is correctly located on the running TFTP server, the phone will locate the file and reload the application onto the phone.

WHY DOES MY PHONE DISPLAY THE “NO SERVICE” MESSAGE?

The phone displays the “**No Service**” message if it is not able to successfully register with the Registrar. If the Registrar is up and running the SIP settings may not have not been set up correctly.

The Registrar server could be set to 0.0.0.0. A global value of 0.0.0.0 disables registration. However, the phone is still active and you can dial using username@ip address of the phone. The phone displays "**No Service**".

If the Registrar IP address is set to 0.0.0.0 for a per-line basis (i.e. line 1, line 2, etc.), then the register request is not sent, the "**No Service**" message does not display, and the message waiting indicator (MWI) does not come on.

Check that the "**Registrar Server**" IP address in the Mitel Web UI at **Advanced Settings->Global SIP** is correct. Check the "**sip registrar ip**" parameter in the configuration files is correct.

WHY DOES MY PHONE DISPLAY "BAD ENCRYPTED CONFIG"?

The IP phone displays "Bad Encrypted Config" because encrypted configuration files are enabled but the decryption process has failed. Specific cases where decryption fails are:

REASON

The site-specific password in *security.tuz* does not match the password used to encrypt the *<mac>.tuz* or *startup.tuz* files.

FIX

Encrypt the *.cfg* files to *.tuz* using the correct password, or replace the *security.tuz* with the correct encrypted file.

REASON

Neither of the *<mac>.tuz* and *startup.tuz* files are present on the configuration server (TFTP/FTP/HTTP).

FIX

Create the encrypted files using *anacrypt.exe* and copy them to the configuration server.

REASON

The encrypted *<mac>.tuz* or *startup.tuz* file is encrypted using a different version of *anacrypt.exe* than the phone firmware.

FIX

Run "*anacrypt.exe -v*" and confirm that the correct version is reported, compared to the phone firmware version.

WHY IS MY PHONE NOT RECEIVING THE TFTP IP ADDRESS FROM THE DHCP SERVER?

For DHCP to automatically populate the IP address or qualified domain name for the TFTP server, your DHCP server must support Option 66. Option 66 is responsible for forwarding the TFTP server IP address or domain name to the phone automatically. If your DHCP server does not support Option 66, you must manually enter the IP address or qualified domain name for the TFTP server into your IP phone configuration.

Additionally, the phone may not be receiving the TFTP IP address if there are other DHCP servers within the same broadcast domain providing different Option 66 (TFTP server) settings. See “DHCP” on page 4 for more information on option precedence.

For procedures on configuring the TFTP server using the IP phone UI and the Mitel Web UI, see Chapter 4, the section, “Configuring the Configuration Server Protocol” on page 4-104.

For specific protocol parameters you can set in the configuration files, see Appendix A, the section, “Configuration Server Settings” on page 33.

HOW DO I RESTART THE IP PHONE?

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Restart Phone**.
3. Press **#** to confirm.

Note: To cancel the Restart, press the key.

For the 6867i/6869i/6920/6930:

1. Press or on the phone to enter the Options List.
2. Select **Restart**. The following prompt displays:
   "Restart phone?"
3. Select **Yes** to restart the phone
   or
   Select **No** to go back to the Options Screen.

For the 6873i/6940/6970:

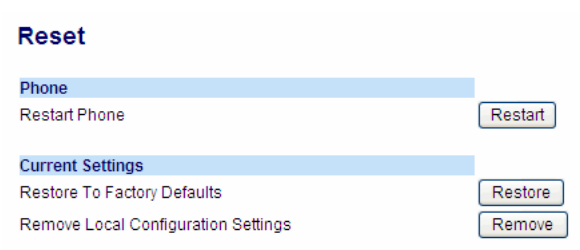
1. Press , or the **Settings** softkey on the phone to enter the Options List.
2. Tap the **Restart** icon. The following prompt displays:
   "Restart phone?"

Note: If required, swipe left on the screen to navigate to the second page of options.

3. Select **Yes** to restart the phone
   or
   Select **No** to go back to the Options Screen.

MITEL WEB UI

1. Click on **Operation->Reset->Phone.**



2. Click **Restart** to restart the phone.

HOW DO I SET THE IP PHONE TO FACTORY DEFAULT?

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Administrator Menu** and enter your Administrator Password (default is **22222**).
3. Select **Factory Default.**
4. The "*Restore Defaults?*" prompt displays.
   Press **#** to confirm.

For the 6867i/6869i/6920/6930:

1. Press or on the phone to enter the Options List.
2. Press the Advanced softkey and enter your Administrator password using the keypad keys. (Default is **22222**).
3. Select **Reset**.
4. With **Factory Default** highlighted, press the **Select** softkey.
   The "*Factory Default?*" prompt displays.
5. Select **Yes** to factory default the phone.
   The phone immediately sets the phone to factory defaults and automatically restarts the phone.

For the 6873i/6940/6970:

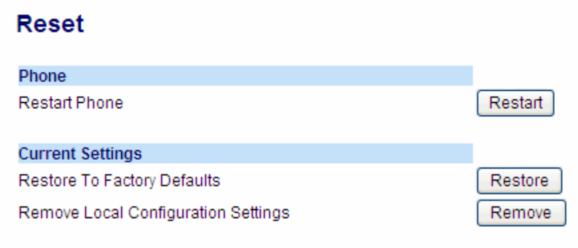
1. Press , or the **Settings** softkey on the phone to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password and press the blue Enter key. Default is "**22222**".
4. Tap the **Reset** icon.

   Note: If required, swipe left on the screen to navigate to the second page of options.

5. With **Factory Default** highlighted, press the **Select** softkey.
   The "*Factory Default?*" prompt displays.
6. Select **Yes** to factory default the phone.
   The phone immediately sets the phone to factory defaults and automatically restarts the phone.

MITEL WEB UI

1. Click on **Operation->Reset->Current Settings.**



2. In the "**Restore to Factory Defaults**" field, click **Restore**.
   This restores all factory defaults, and removes any saved configuration and directory list files.

HOW DO I ERASE THE PHONE'S LOCAL CONFIGURATION?

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **Administrator Menu** and enter your Administrator Password (default is **22222**).
3. Select **Erase Local Config.**
4. The "*Erase local config?*" prompt displays.
   Press **#** to confirm.

For the 6867i/6869i/6920/6930:

1. Press or on the phone to enter the Options List.
2. Press the Advanced softkey and enter your Administrator password using the keypad keys. (Default is **22222**).
3. Select **Reset**.
4. Select **Erase Local Config**.
5. With **Erase Local Config** highlighted, press the **Select** softkey.
   The "*Erase Local Configuration?*" prompt displays.
6. Select **Yes** to erase the local configuration.
   The phone immediately erases the local configuration and automatically restarts the phone.

For the 6873i/6940/6970:

1. Press , or the **Settings** softkey on the phone to enter the Options List.
2. Tap the **Advanced** softkey.
3. Enter the Administrator password and press the blue Enter key. Default is "**22222**".

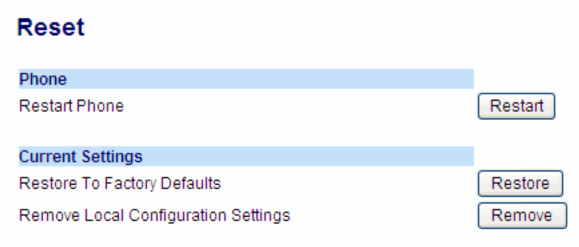
4. Tap the **Reset** icon.

> **Note:** If required, swipe left on the screen to navigate to the second page of options.

5. Tap **Erase Local Config**.
6. With **Erase Local Config** highlighted, tap the **Select** softkey.
   The "*Erase Local Configuration?*" prompt displays.
7. Select **Yes** to erase the local configuration.
   The phone immediately erases the local configuration and automatically restarts the phone.

MITEL WEB UI

1. Click on **Operation->Reset->Current Settings.**



2. In the "**Remove Local Configuration Settings**" field, click **Remove**.
   This removes the last customized configuration settings made on the phone.

HOW TO RESET A USER'S PASSWORD?

IP PHONE UI

For the 6863i/6865i/6905/6910:

1. Press or on the phone to enter the Options List.
2. Select **User Password**.
3. Enter the current user password.
4. Press **Enter**.
5. Enter the new user password.

> **Note:** The IP phones support alphanumeric password with the supported characters.

6. Press **Enter**.
7. Re-enter the new user password.
8. Press **Enter**.
   A message, "Password Changed" displays on the screen.

For the 6867i/6869i/6920/6930:

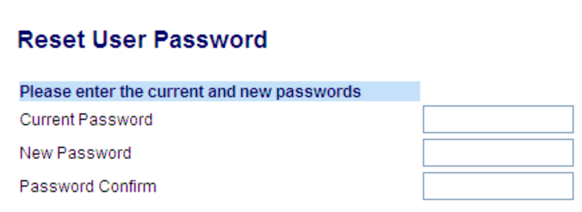
1. Press or on the phone to enter the Options List.
2. Select **Lock > Password.**
3. Enter the current password in the **<Current Password>** field.
4. Press the down navigation key and enter the new password in the **<New Password>** field.
5. Press the down navigation key and enter the new password again in the **<Re-enter Password>** field.
6. Press the **Save** softkey.
   A message, "***Password Changed***" displays on the screen.

For the 6873i/6940/6970:

1. Press , or the **Settings** softkey on the phone to enter the Options List.
2. Tap the **Lock** icon.
3. Tap the **Password** icon.
4. Enter the current password in the **<Current Password>** field.
5. Enter the new password in the **<New Password>** field.
6. Enter the new password again in the **<Re-enter Password>** field.
7. Tap the **Save** softkey.
   A message, "***Password Changed***" displays on the screen.

MITEL WEB UI

1. Click on **Operation->User Password**.



2. In the "**Current Password**" field, enter the current user password.
3. In the "**New Password**" field, enter the new user password.
4. In the "**Confirm Password**" field, enter the new user password again.
5. Click **Save Settings** to save your changes.

HOW DO I LOCK AND UNLOCK THE PHONE?

6863I/6865I/6905/6910:

IP PHONE UI

Lock the phone:

1. Press or on the phone to enter the Options List.
2. Select **Phone Lock.**
   The prompt, "*Lock the phone*?" displays.
3. Press **Lock** to lock the phone.

Unlock the phone:

1. Press on the phone to enter the Options List.
   The prompt, "*To unlock the phone...Password:*"
2. Enter the user or administrator password and press **Enter**.
   The phone unlocks.

6867I/6869I/6920/6930:

IP PHONE UI

Lock the phone:

1. Press or on the phone to enter the Options List.
2. Select **Lock > Phone Lock.**
   The prompt, "*Lock the phone*?" displays.
3. Select **Yes** to lock the phone.

Unlock the phone:

1. Press or on the phone to enter the Options List.
   An "Enter Unlock Password" prompt displays.
2. Enter the user or administrator password and press **Enter**. Default is "**22222**".
   A prompt "Unlock the Phone?" displays.
3. Select **Yes** to unlock the phone.

6873I/6940/6970:

IP PHONE UI

Lock the phone:

1. Press , or the **Settings** softkey on the phone to enter the Options List.
2. Tap the **Lock** icon.

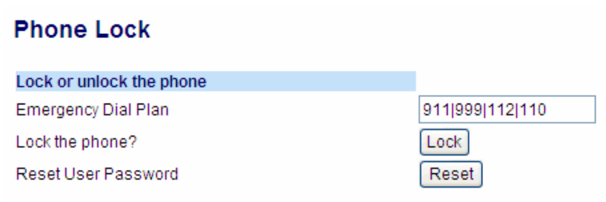
3. Tap the **Phone Lock** icon.
   The prompt, "*Lock the phone*?" displays.
4. Select **Yes** to lock the phone.

Unlock the phone:

1. Press or on the phone to enter the Options List.
   An "Enter Unlock Password" prompt displays.
2. Enter the user or administrator password and press **Enter**. Default is "**22222**".
   A prompt "Unlock the Phone?" displays.
3. Tap **Yes** to unlock the phone.

MITEL WEB UI

1. Click on **Operation->Phone Lock**.



Lock the phone:

2. In the "**Lock the Phone?**" field, click **Lock**.
   The phone locks dynamically and displays the following message:
   "*Phone is locked*".

Unlock the phone:

3. Click on **Operation->Phone Lock**.
4. In the "**Unlock the Phone?**" field, click **Unlock**.
   The phone unlocks dynamically and displays the following message:
   "*Phone is unlocked*".

Appendix A

CONFIGURATION PARAMETERS

ABOUT THIS APPENDIX

This appendix describes the parameters you can set in the configuration files for the IP phones. The configuration files include startup.cfg, <model>.cfg, and <mac.cfg>.

TOPICS

This appendix covers the following topics:

SETTING PARAMETERS IN CONFIGURATION FILES

You can set specific configuration parameters in the configuration files for configuring you IP phone. The *startup.cfg, <model>.cfg,* and *<mac>.cfg* files are stored on the server. The *startup.cfg* file stores global IP phone configuration settings.

Note: In releases previous to 4.0.0 SP1, the "startup.cfg" file was named "aastra.cfg". Apart from the file names, the "startup.cfg" file acts as an identical replacement for the "aastra.cfg" file. Releases including and above 4.0.0 SP1 support both the "startup.cfg" and "aastra.cfg" files, but if the "startup.cfg" file is available, the phone will disregard the "aastra.cfg" file (if available). The "aastra.cfg" file will be used if the "startup.cfg" file is unavailable and will continue to be supported going forward to ensure backwards compatibility with existing customer deployments.

The *<model>.cfg* file contains model specific information. The *<mac>.cfg* file stores configuration settings specific to the IP phone with that MAC address. When you restart the IP phone, these files are downloaded to the phone.

If you make changes to the phone configuration, the changes are stored in a local configuration on the phone (not on the server).

Configuration changes made to the *<model>.cfg* file override the configuration settings in the *startup.cfg* file. Configuration changes made to the *<mac>.cfg* file override the configuration settings in the *<model>.cfg* and *startup.cfg* files.

Note: Configuration parameters that you enter in the configuration files are NOT case sensitive.

- ***G722 overload point setting in aastra.cfg***

  Note: When the default overload point of G722 is set at -3dbm0. You can set the overload point at the level as specified by the following standard:

  - Add the command line "**g722 9dbm0: 1**" to the aastra.cfg file.
  - The phone is reset to update the configuration to ensure the location of configuration server that is set through the phone web interface to the same location where the aastra.cfg is.
  - Ensure that the formal load with all audio improvements measure the same levels as 4.1.0.2038.
  - Check the configuration is set to the correct overload point as default value in the load and overload becomes 0 on each upgrade that you make.

Reference

For information about configuration file precedence, see Chapter 1, the section, “Configuration File Precedence” on page 1-43.

This section includes the following types of configurable parameters:

- Operational, Basic, and Advanced Parameters on page A-10.
- Mapping Key Settings on page A-240.
- Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters on page A-248.
- Advanced Operational Parameters on page A-312.
- Troubleshooting Parameters on page A-350.

OPERATIONAL, BASIC, AND ADVANCED PARAMETERS

The following sections provide the configuration parameters you can configure on the IP phone. Each parameter table includes the name of the parameter, a description, the format, default value, range, and example. The table also provides in which configuration file the parameter can be defined (startup.cfg, <model>.cfg, <mac>.cfg).

ENHANCED CONFIGURATION FILE DOWNLOAD

PARAMETER – *config files mandatory download*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Multiple files can be specified separated by comma. If mandatory files are specified then this feature will be enabled, or else, it will be disabled.
FORMAT	String
DEFAULT VALUE	Blank
RANGE	NA
EXAMPLE	config files mandatory download: "startup.cfg, mac.cfg, model.cfg" (Only three files are considered mandatory - startup, model and mac. The file extensions “cfg, tuz, tuz2” are allowed, in any order and is case insensitive.

PARAMETER – *config files number of reattempt*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the number of reattempts to download the configuration file after an unsuccessful download.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 (no reattempt) -1 (infinite reattempt) Other integers (number of reattempts)
EXAMPLE	config files number of reattempt: -1

PARAMETER – *config files max delay*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the delay between each reattempt. It is dynamic in nature and value is random seconds not greater than the configured value.
FORMAT	Integer
DEFAULT VALUE	15 seconds
RANGE	Max value is 86400 seconds
EXAMPLE	config files max delay: 20

PARAMETER – *config files skip key enabled*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not to display the ’skip’ softkey during a reattempt to download the configuration file.
FORMAT	Boolean
DEFAULT VALUE	1

RANGE	0 (skip softkey is not displayed during reattempt) 1 (skip softkey is displayed during reattempt)
EXAMPLE	config files skip key enabled: 1

SIMPLIFIED IP PHONE UI OPTIONS MENU

PARAMETER – *options simple menu*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to enable a simplified options menu or enable the full menu on the IP Phone UI. **WARNING: WHEN USING THE SIMPLIFIED MENU, YOU CANNOT CHANGE THE NETWORK SETTINGS FROM THE IP PHONE UI. IF THE NETWORK SETTINGS BECOME MISCONFIGURED, YOU MUST USE THE MITEL WEB UI TO CONFIGURE THE NETWORK SETTINGS OR FACTORY DEFAULT THE PHONE THROUGH THE WEB UI AND THEN USE THE PHONE UI'S FULL OPTIONS MENU TO RECOVER THE NETWORKS SETTING.**
FORMAT	Boolean
DEFAULT VALUE	0 (full options menu)
RANGE	0 (full options menu) 1 (simplified options menu)
EXAMPLE	options simple menu: 1

NETWORK SETTINGS

PARAMETER – *dhcp*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables DHCP. Enabling DHCP populates the required network information. The DHCP server serves the network information that the IP phone requires. If the IP phone is unable to get any required information, then you must enter it manually. DHCP populates the following network information: IP Address, Subnet Mask, Gateway, Domain Name System (DNS) servers, TFTP, HTTP, HTTP Port, HTTPS, HTTPS Port, and FTP servers, and Timer servers. **Note:** For DHCP to automatically populate the IP address or qualified domain name for the TFTP server, your DHCP server must support Option 66.
FORMAT	Integer
DEFAULT VALUE	1 (enabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	dhcp: 1

PARAMETER – *ip*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This parameter assigns a static IP address to the IP phone device. **Note:** For DHCP to automatically populate this parameter, your DHCP server must support Option 66.
FORMAT	IP address
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	ip: 192.168.0.25

PARAMETER – *subnet mask*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Subnet mask defines the IP address range local to the IP phone. **Note:** For DHCP to automatically populate this parameter, your DHCP server must support Option 66.
FORMAT	IP address
DEFAULT VALUE	255.255.255.0
RANGE	N/A
EXAMPLE	subnet mask: 255.255.255.224

PARAMETER – *default gateway*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The IP address of the network's gateway or default router IP address. **Note:** For DHCP to automatically populate this parameter, your DHCP server must support Option 66.
FORMAT	IP address
DEFAULT VALUE	1.0.0.1
RANGE	N/A
EXAMPLE	default gateway: 192.168.0.1

PARAMETER – *dns1*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Primary DNS server IP address. For any of the IP address settings on the IP phone a domain name value can be entered instead of an IP address. With the help of the DNS servers the domain names for such parameters can then be resolved to their corresponding IP addresses. **Note:** For DHCP to automatically populate this parameter, your DHCP server must support Option 66.
FORMAT	IP address
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	dns1: 192.168.0.5

PARAMETER – *dns2*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	A service that translates domain names into IP addresses. To assign static DNS addresses, disable DHCP. **Note:** For DHCP to automatically populate this parameter, your DHCP server must support Option 66.
FORMAT	IP address
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	dns2: 192.168.0.6

PARAMETER – *ethernet port 0*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The send (TX) and receive (RX) method to use on Ethernet port 0 to transmit and receive data over the LAN.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 - Auto Negotiate 1 - Full Duplex, 10Mbps 2 - Full Duplex, 100Mbps 3 - Full Duplex, 1000Mbps (applicable for the 6865i, 6867i, 6869i, and 6873i IP phones only) 4 - Half Duplex, 10Mbps 5 - Half Duplex, 100Mbps 6 - Half Duplex, 1000Mbps (applicable for the 6865i, 6867i, 6869i, and 6873i IP phones only)
EXAMPLE	ethernet port 0: 4

PARAMETER – *ethernet port 1*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The send (TX) and receive (RX) method to use on Ethernet port 1 to transmit and receive data over the LAN.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 - Auto Negotiate 1 - Full Duplex, 10Mbps 2 - Full Duplex, 100Mbps 3 - Full Duplex, 1000Mbps (applicable for 6865i, 6867i, 6869i, and 6873i IP phones only) 4 - Half Duplex, 10Mbps 5 - Half Duplex, 100Mbps 6 - Half Duplex, 1000Mbps (applicable for the 6865i, 6867i, 6869i, and 6873i IP phones only)
EXAMPLE	ethernet port 1: 2

PARAMETER – *ethernet port mirroring*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows to enable or disable port mirroring on IP phones. When enabled, the LAN and PC ports are set to promiscuous mode which allows sniffing all packets from phone boot up onwards.
FORMAT	Boolean
DEFAULT VALUE	0 (disable)
RANGE	0 (disable) 1 (enable)
EXAMPLE	ethernet port mirroring: 0

PARAMETER – *pc port passthru enabled*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the PC port.
FORMAT	Integer
DEFAULT VALUE	1 (enable)
RANGE	0 (disable) 1 (enable)
EXAMPLE	pc port passthru enabled: 1

DHCP OPTION SETTINGS

OPTION 12

PARAMETER – *hostname*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the hostname DHCP Option 12 that the phone sends with the DHCP Request packet. **Note:** If you change this parameter, you must restart your phone for the change to take affect.
FORMAT	String
DEFAULT VALUE	[<model><MAC IP Address>]
RANGE	Up to 64 alpha-numeric characters **Note:** The value for this parameter can also be a fully qualified domain name.
EXAMPLE	hostname: mitel4

OPTION 60

PARAMETER – *dhcp opt60 extended vendor class*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether to send a DHCP Option 60 value consisting of the identifier value only, or an extended DHCP Option 60 value consisting of the identifier, firmware version, and bootrom version. If the latter, the syntax is as follows: “Identifier Value + Firmware Version + BootRom Version”
FORMAT	Integer
DEFAULT VALUE	0 (Disabled)
RANGE	0-1 0 (Disabled - Sends only the identifier value) 1 (Enabled - Sends the identifier value, firmware version, and bootrom version)
EXAMPLE	dhcp opt60 extended vendor class identifier: 1

OPTION 77

PARAMETER – *dhcp userclass*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the User Class DHCP Option 77 that the phone sends to the configuration server with the DHCP Request packet. **Note:** If you specify a value for this parameter, you must restart your phone for the change to take affect. Any change in its value during start-up results in an automatic reboot.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	Up to 8 alpha-numeric characters
EXAMPLE	dhcp userclass: admin

OPTION 120

PARAMETER – *use dhcp option 120*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables support for DHCP Option 120 on the IP phones. DHCP Option 120 allows SIP clients to locate a local SIP server (i.e. outbound proxy server) that can be used for all outbound SIP requests.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0-1 0 (disabled) 1 (enabled)
EXAMPLE	use dhcp option 120: 1

OPTIONS 159 AND 160 - DHCP OPTION OVERRIDE

PARAMETER – *dhcp config option override*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The value specified for this parameter overrides the precedence order for determining a configuration server. **Note:** You must restart the IP Phone for this parameter to take affect.
FORMAT	Integer
DEFAULT VALUE	0 (Any - no override - uses normal precedence order of 43, 160, 159, 66)
RANGE	-1 (Disabled - ignores all DHCP configuration options (43, 66, 159, 160) 0 (Any) 43 66 159 160
EXAMPLE	dhcp config option override: 66

OPTIONS 132 - TRANSFER VLAN ID ASSIGNMENT USING DHCP

PARAMETER – *dhcp option 132 vlan id enabled*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables the phone to transport the VLAN ID parameter in the DHCP protocol. When the phone receives the VLAN ID from the DHCP and the value is different from the one used by the phone to trigger the DHCP request, the phone reboots and then sends a new DHCP request in the new VLAN. The phone will remember the VLAN ID obtained by DHCP options so that on a reboot, the phone will send a DHCP request using the correct VLAN.
FORMAT	Integer
DEFAULT VALUE	1 (enabled)
RANGE	0-1 0 (disabled) 1 (enabled)
EXAMPLE	dhcp option 132 vlan id enabled: 0

PASSWORD SETTINGS

PARAMETER – *admin password*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to set a new administrator password for the IP phone. **Note:** The IP phones support alphanumeric password with the supported characters.
FORMAT	String
DEFAULT VALUE	22222
RANGE	Up to 15 alpha-numeric characters
EXAMPLE	admin password: Mitel@123

PARAMETER – *user password*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to set a new user password for the IP phone. **Note:** The IP phones support alphanumeric password with the supported characters.
FORMAT	String
DEFAULT VALUE	Default value is an empty string "" (left blank)
RANGE	Up to 15 alpha-numeric characters
EXAMPLE	user password: Mitel*123

PARAMETER – *options password enabled*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables password protection of the Options key on the IP phone. If enabled, upon pressing the Options key, a user has to enter a password at the IP phone UI. If the password is entered correctly, the user is allowed to gain access to the Options Menu and no more password prompts display for other password protected screens. If the user fails to enter the correct password in three attempts, access to the Options Menu is denied and the IP phone returns to the idle screen. **Note:** The password to enter is the administrator password configured for that phone.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (false; not password protected) 1 (true; password protected)
EXAMPLE	options password enabled: 1

ENHANCED E911 LOCATION REPORTING FOR IP ENDPOINTS (RAY BAUM)

PARAMETER – *held enable*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	• If enabled, contact location server to retrieve location information. SIP INVITE message contains location information content if call is a emergency call or call matches held geolocation dial plan • If disabled, the phone does not contact location server to retrieve location information. SIP INVITE message does not contain location information content
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	*held enable:* 0

PARAMETER – *held server1 url*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies which Location Information Server (LIS) to use as primary
FORMAT	String (up to 256 characters)
DEFAULT VALUE	N/A

RANGE	N/A
EXAMPLE	held server1 url: https://lis1.mitelcloud.com

PARAMETER – *held server1 auth type*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies how authentication to LIS is done. The types of authentication are: • basic • cert • devicecert
FORMAT	String
DEFAULT VALUE	basic
RANGE	N/A
EXAMPLE	held server1 auth type: basic

PARAMETER – *held server1 username*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Required if authentication type is basic. If authentication type is cert or devicecert, it is null.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	held server1 username: abcd

PARAMETER – *held server1 password*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Required if authentication type is basic. If authentication type is cert or devicecert, it is null.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	held server1 password: 1234

PARAMETER – *held server1 certificate*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg

DESCRIPTION	• If authentication type is basic, this parameter is null. • If authentication type is cert, this parameter is concatenated cert/key string. • If authentication type is devicecert, this parameter is null. The client certificate will read from existing config parameter "sips micloud connect device certificate"
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	held server1 certificate: -----BEGIN CERTIFICATE-----\nABCD\n-----END CERTIFICATE-----

PARAMETER – *held server1 key*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	If authentication type is cert, this parameter is key string.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	held server1 key: -----BEGIN RSA PRIVATE KEY-----\nABCD\n-----END RSA PRIVATE KEY-----

PARAMETER – *held server2 url*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies which LIS server to use as secondary
FORMAT	String (up to 256 characters)
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	held server2 url: https://lis1.mitelcloud.com

PARAMETER – *held server2 auth type*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies how authentication to LIS is done. The types of authentication are: • basic • cert • devicecert
FORMAT	String
DEFAULT VALUE	basic

RANGE	N/A
EXAMPLE	held server2 auth type: basic

PARAMETER – *held server2 username*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Required if authentication type is basic. If authentication type is cert or devicecert, it is null.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	held server2 username: abcd

PARAMETER – *held server2 password*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Required if authentication type is basic. If authentication type is cert or devicecert, it is null.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	held server2 password: 1234

PARAMETER – *held server2 certificate*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	• If authentication type is basic, this parameter is null. • If authentication type is cert, this parameter is concatenated cert/key string. • If authentication type is devicecert, this parameter is null. The client certificate will read from existing config parameter "sips micloud connect device certificate"
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	held server2 certificate: -----BEGIN CERTIFICATE-----\nABCD\n-----END CERTIFICATE-----

PARAMETER – *held server2 key*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg

DESCRIPTION	If authentication type is cert, this parameter is key string.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	held server2 key: -----BEGIN RSA PRIVATE KEY-----\nABCD\n-----END RSA PRIVATE KEY-----

PARAMETER – *held location identifier name*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LIS Vendor specific identity name key required. Possible values are: • companyID • networkZoneId
FORMAT	String
DEFAULT VALUE	companyID
RANGE	N/A
EXAMPLE	held location identifier name: companyID

PARAMETER – *held location identifier value*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the value of the identity
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	held location identifier value: 32E23023-27C1-4FF1-BC47-28B4D7A03F8E

PARAMETER – *held location type*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LIS request type. The possible values are: • any • civic • locationURI
FORMAT	String
DEFAULT VALUE	any
RANGE	N/A
EXAMPLE	held location type: any

PARAMETER – *held location type exact*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	• If enabled, the phone will set "exact" attribute to true when the "locationType" element is included in a location request message to indicate to the LIS that the contents of the "locationType" parameter must be strictly followed • If disabled, the phone will set "exact" attribute to false when the "locationType" element is included in a location request message to indicate to the LIS that the contents of the "locationType" parameter may not be strictly followed, which allows the LIS the option of returning something beyond what is specified, such as a set of Location URIs when only a civic location was requested
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	held location type exact: 0

PARAMETER – *held max response time*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the requestTime parameter on the locationRequest, if provided.
FORMAT	Integer
DEFAULT VALUE	10
RANGE	N/A
EXAMPLE	held max response time: 10

PARAMETER – *held refresh time*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies how often to refresh location from the HELD request if a locationResponse expiry time is not provided. This differs from the RFC.
FORMAT	Integer
DEFAULT VALUE	3600
RANGE	3600 - 86400 seconds
EXAMPLE	held refresh time: 3600

PARAMETER – *held retry timer*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies how long to wait until next retry, if no response is received from the LIS. **Note:** There is a random time offset added while retrying to contact LIS. This is done to avoid all the phones retrying to connect to LIS server at the same time and to avoid overloading the server.
FORMAT	Integer
DEFAULT VALUE	60
RANGE	60 - 300 seconds
EXAMPLE	held retry timer: 60

PARAMETER – *held lldp bssid format standard*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	• If enabled, tells devices to report LLDP/BSSID information using RFC7105 • If disabled, tells devices to report LLDP/BSSID information using Polycom format used by intrado/redsky
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	held lldp bssid format standard: 0

PARAMETER – *held sip header geolocation routing enable*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	• If enabled, include Geolocation-Routing header on emergency calls and calls that match the locationTx.additional-pattern • If disabled, do not include Geolocation-Routing header on emergency calls and calls that match the locationTx.additional-pattern
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	held sip header geolocation routing enable: 0

PARAMETER – *held sip header priority enable*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	• If enabled, include "Priority: emergency” • If disabled, do not include "Priority: emergency”
FORMAT	Boolean
DEFAULT VALUE	1
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	held sip header priority enable: 1

PARAMETER – *held nai enable*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	• If enabled, the NAI is included as a device identity in the location request sent to the LIS • If disabled, the NAI is excluded as a device identity in the location request sent to the LIS
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	held nai enable: 0

PARAMETER – *held loc info report status enable*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	• If enabled, reports location information status to PBX • If disabled, does not report location information status to PBX
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	held loc info report status enable: 0

PARAMETER – *teleworker loc enable*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg

DESCRIPTION	Enables/disables teleworker location update feature. **Note:** For MiVoice Connect TeleWorker integration only, Default will be changed to 1.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	teleworker loc enable: 0

PARAMETER – *teleworker loc update prompt enable*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables/disables the prompt on UI screen if the location has changed. **Note:** For MiVoice Connect TeleWorker integration only, Default will be changed to 1.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	teleworker loc update prompt enable: 0

PARAMETER – *teleworker loc update notify enable*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables notification to be sent to the Call Manager if location is changed. If "teleworker loc update prompt enable " parameter is enabled, status of update prompt display and user action will also be provided. By disabling the feature no notification message is sent to the call manager if the location is changed. **Note:** For MiVoice Connect TeleWorker integration only, Default will be changed to 1.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	teleworker loc update notify enable: 0

EMERGENCY DIAL PLAN SETTINGS

PARAMETER – *emergency dial plan*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to specify an emergency number to use on your IP phone so a caller can contact emergency services in the local area when required. The default emergency numbers on the IP phones is 911, 999, 112, and 110. 911 - A United States emergency number. 999 - A United Kingdom emergency number. 112 - An international emergency telephone number for **GSM mobile phone** networks. In all European Union countries it is also the emergency telephone number for both mobile and fixed-line telephones. 110 - A police and/or fire emergency number in Asia, Europe, Middle East, and South America. Dial plan (characters) — Length (bytes) 911 — 14 4xx — 18 x+#|xx+* — 35 911|999|112|110|450 — 54 911|112|011XX+#|101XX+#|1[2-3]XXXXXXXXX|[4-5]XXXXXXXXX|[6-7]XXXXXXXXXX,3|[8-9]XXXXXXXXXXX,2|XX+*|XX+#|*XXX+#|#XX+#|4xx,2 — 325 **Note:** Contact your local phone service provider for available emergency numbers in your area.
FORMAT	Integer
DEFAULT VALUE	911|999|112|110
RANGE	Up to 512 characters
EXAMPLE	emergency dial plan: 911|999

EMERGENCY CALL BEHAVIOR SETTINGS

PARAMETER – *emergency call connection hold enabled*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	If enabled, this parameter changes the behavior of the IP phones when an emergency call (i.e. a call made to an emergency number matching one of the values defined in the “emergency dial plan” parameter) is placed. The IP phones will ensure that the voice/audio path and other resources associated with the emergency call are continually active and any functions that could reduce the “continuous reachability” of the caller are disabled. Additionally, the only way the call can be terminated is if the emergency services agent ends the call.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0-1 0 (disabled) 1 (enabled)
EXAMPLE	emergency call connection hold enabled: 1

USER DIAL PLAN SETTING

PARAMETER – *sip user parameter dial plan*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The dial plan that the network uses to distinguish between a real PSTN number and a number that looks like a PSTN number but is actually on an IP network. **Note:** You can configure the “sip user parameter dial plan” parameter on a global basis only. If it is misconfigured, then the parameter is ignored. Entering no value disables this feature.
FORMAT	Alpha-numeric characters
DEFAULT VALUE	Blank
RANGE	Up to 512 characters (more than 512 characters disables this parameter).
EXAMPLE	sip user parameter dial plan: 6xx | 8xxxx |9xxxxxxx

MITEL WEB UI SETTINGS

PARAMETER – *web interface enabled*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the Mitel Web UI interface for a single IP phone when this parameter is entered in the *<mac>.cfg* file. Enables or disables the Mitel Web UI interface for all phones when this parameter is placed in the *startup.cfg* file.
FORMAT	Integer
DEFAULT VALUE	1 (admin/user enabled)
RANGE	0 (admin/user disabled) 1 (admin/user enabled) 2 (only admin enabled)
EXAMPLE	web interface enabled: 1

PARAMETER – *web interface blacklist duration*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the maximum amount of time, in seconds, that the IP of the phone’s Web UI attacker will remain on the blacklist.
FORMAT	Integer
DEFAULT VALUE	3600 (1 hour)
RANGE	0 - 9999999 (seconds) **Note:** A value “0” will disable the blacklist feature.
EXAMPLE	web interface blacklist duration: 600

PARAMETER – *web interface http port*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the HTTP port for the Web UI server
FORMAT	String
DEFAULT VALUE	default_http_port:80
RANGE	10000 to 11000
EXAMPLE	web interface http port: 10001

PARAMETER – *web interface https port*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the HTTPS port for the Web UI server
FORMAT	String
DEFAULT VALUE	default_https_port:443
RANGE	10000 to 11000

EXAMPLE	web interface https port: 10101

SECURE WEB SERVICE SETTINGS

PARAMETER – *secure web service*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables/disables TCP ports 80, 443, and 49249 for web services on the phone. **Note:** Closing ports 80, 443, and 49249 does not have an effect on the HTTP/HTTPs client service on the phone.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (Disabled - Ports 80, 443, and 49249 open) 1 (Enabled - Ports 80, 443, and 49249 closed)
EXAMPLES	secure web service: 1

CONFIGURATION SERVER SETTINGS

PARAMETER – *download protocol*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Protocol to use for downloading new versions of software to the IP phone.
FORMAT	Text
DEFAULT VALUE	TFTP
RANGE	TFTP FTP HTTP HTTPS
EXAMPLE	download protocol: HTTPS

PARAMETER – *tftp server*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The TFTP server's IP address. If DHCP is enabled and the DHCP server provides the information, this field is automatically populated. Use this parameter to change the IP address or domain name of the TFTP server. This will become effective after this configuration file has been downloaded into the phone. **Note:** For DHCP to automatically populate this parameter, your DHCP server must support Option 66.
FORMAT	IP address or qualified domain name
DEFAULT VALUE	0.0.0.0

RANGE	N/A
EXAMPLE	tftp server: 192.168.0.130

PARAMETER – *tftp path*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the path name for which the configuration files reside on the TFTP server for downloading to the IP Phone. **Note:** Enter the path name in the form *folderX\folderX\folderX*. For example, ***ipphone\6867i\configfiles***.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	Up to 256 alphanumeric characters
EXAMPLE	tftp path: configs\tftp

PARAMETER – *alternate tftp server*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The alternate TFTP server's IP address or qualified domain name. This will become effective after this configuration file has been downloaded into the phone.
FORMAT	IP address or qualified domain name
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	alternate tftp server: 192.168.0.132

PARAMETER – *alternate tftp path*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies a path name for which the configuration files reside on an alternate TFTP server for downloading to the IP Phone. **Note:** Enter the path name in the form *folderX\folderX\folderX*. For example, ***ipphone\6867i\configfiles***.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	Up to 256 alphanumeric characters
EXAMPLE	alternate tftp path: configs\alternate

PARAMETER – *use alternate tftp*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the alternate TFTP server. Valid values are "0" disabled and "1" enabled.
FORMAT	N/A
DEFAULT VALUE	0
RANGE	0 or 1
EXAMPLE	use alternate tftp: 1

PARAMETER – *ftp server*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The FTP server's IP address or network host name. This will become effective after this configuration file has been downloaded into the phone. **Optional**: You can also assign a username and password for access to the FTP server. See the following parameters for setting username and password. **Note:** For DHCP to automatically populate this parameter, your DHCP server must support Option 66.
FORMAT	IP address or fully qualified Domain Name
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	ftp server: 192.168.0.131

PARAMETER – *ftp path*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies a path name for which the configuration files reside on an FTP server for downloading to the IP Phone. **Note:** Enter the path name in the form *folderX\folderX\folderX*. For example, ***ipphone\6867i\configfiles***.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	Up to 256 alphanumeric characters
EXAMPLE	ftp path: configs\ftp

PARAMETER – *ftp username*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The username to enter for accessing the FTP server. This will become effective after this configuration file has been downloaded into the phone. **Note:** The IP Phones support usernames containing dots (".").
FORMAT	Text
DEFAULT VALUE	N/A
RANGE	Up to 63 alphanumeric characters
EXAMPLE	ftp username: 6867imitel

PARAMETER – *ftp password*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The password to enter for accessing the FTP server. This will become effective after this configuration file has been downloaded into the phone.
FORMAT	Text
DEFAULT VALUE	N/A
RANGE	Up to 63 alphanumeric characters
EXAMPLE	ftp password: 1234

PARAMETER – *http server*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The HTTP server's IP address. This will become effective after this configuration file has been downloaded into the phone. **Optional**: You can also assign an HTTP relative path to the HTTP server. See the next parameter (**http path**). **Note:** For DHCP to automatically populate this parameter, your DHCP server must support Option 66.
FORMAT	IP address or fully qualified Domain Name
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	http server: 192.168.0.132

PARAMETER – *http path*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The HTTP path name to enter. If the IP phone's configuration and firmware files are located in a sub-directory beneath the server's HTTP root directory, the relative path to that sub-directory should be entered in this field.
FORMAT	dir/dir/dir
DEFAULT VALUE	N/A
RANGE	Up to 256 alphanumeric characters
EXAMPLE	http path: ipphones/6867i

PARAMETER – *http port*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the HTTP port that the server uses to load the configuration to the phone over HTTP. **Note:** For DHCP to automatically populate this parameter, your DHCP server must support Option 66.
FORMAT	Integer
DEFAULT VALUE	80
RANGE	1 through 65535
EXAMPLE	http port: 1025

PARAMETER – *https server*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The HTTPS server's IP address. This will become effective after this configuration file has been downloaded into the phone. **Optional**: You can also assign an HTTPS relative path to the HTTPS server. See the next parameter (**https path**). **Note:** For DHCP to automatically populate this parameter, your DHCP server must support Option 66.
FORMAT	IP address or Fully Qualified Domain Name
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	https server: 192.168.0.143

PARAMETER – *https path*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The HTTPS path name to enter. If the IP phone's configuration and firmware files are located in a sub-directory beneath the server's HTTPS root directory, the relative path to that sub-directory should be entered in this field.
FORMAT	dir/dir/dir
DEFAULT VALUE	N/A
RANGE	Up to 256 alphanumeric characters
EXAMPLE	https path: ipphones/6869i

PARAMETER – *https port*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the HTTPS port that the server uses to load the configuration to the phone over HTTPS. **Note:** For DHCP to automatically populate this parameter, your DHCP server must support Option 66.
FORMAT	Integer
DEFAULT VALUE	443
RANGE	1 through 65535
EXAMPLE	https port: 1025

PARAMETER – *auto resync mode*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Determines whether the configuration server automatically updates the configuration files only, the firmware only, both the firmware and configuration files, or disables automatic updates. This parameter works with TFTP, FTP, HTTP and HTTPS servers. Valid values are: • **None (0)** - Disable auto-resync • **Configuration Files (1)** - Updates the configuration files on the IP phone automatically at the specified time if the files on the server have changed. • **Firmware (2)** - Updates the firmware on the IP phone automatically at the specified time if the files on the server have changed. • **Both (3)** - Updates the configuration files and firmware automatically at the specified time if the files on the server have changed. **Notes:** • If a user is accessing the Mitel Web UI, they are not informed of an auto-reboot. • Any changes made using the Mitel Web UI or the IP phone UI are not overwritten by an auto-resync update. Auto-resync affects the configuration files only. However, the settings in the Mitel Web UI take precedence over the IP phone UI and the configuration files. • The resync time is based on the local time of the IP phone. • If the IP phone is in use (not idle) at the time of the resync check, the reboot occurs when the phone becomes idle. • The automatic update feature works with both encrypted and plain text configuration files.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 (none) 1 (configuration files only) 2 (firmware only) 3 (configuration files and firmware)
EXAMPLE	auto resync mode: 1

PARAMETER – *auto resync time*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Sets the time of day in a 24-hour period for the IP phone to be automatically updated. This parameter works with TFTP, FTP, HTTP and HTTPS servers. **Notes:** • The resync time is based on the local time of the IP phone. • The value of 00:00 is 12:00 A.M. • When selecting a value for this parameter in the Mitel Web UI, the values are in 30-minute increments only. • When entering a value for this parameter using the configuration files, the value can be entered using minute values from 00 to 59 (for example, the auto resync time can be entered as 02:56). • Auto-Resync adds as a default 15 minutes of random time to the configured time. For example, if the auto resync time parameter is set to 02:00, the event takes place any time between 02:00 and 02:15. This max delay can be configured using the "**auto resync max delay**" parameter below. • When the language on the phone is set to French or Spanish, you must enter the time in the format "00h00" (configuration files only).
FORMAT	hh:mm 00h00 (for French and Spanish configuration files)
DEFAULT VALUE	00:00
RANGE	hh = 00 to 23 mm = 00 to 59
EXAMPLE	auto resync time: 03:24

PARAMETER – *auto resync max delay*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the maximum time, in minutes, the phone waits past the scheduled time before starting a checksync.
FORMAT	Integer
DEFAULT VALUE	15
RANGE	0-1439
EXAMPLE	auto resync max delay: 20

PARAMETER – *auto resync days*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the amount of days that the phone waits between checksync operations. **Note:** A value of 0 causes the phone to checksync every time the clock reads the proper time. A value of 1 forces the phone to wait 24 hours prior to doing the first checksync.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0-364
EXAMPLE	auto resync days: 1

IPV6 SUPPORT ON 6800/6900 SERIES SIP PHONES

PARAMETER – *ipv6*	CONFIGURATION FILES startup.cfg, <mac>.cfg
DESCRIPTION	IPv6 enable
FORMAT	Number
DEFAULT VALUE	0
RANGE	0-1
EXAMPLE	ipv6:1

PARAMETER – *dhcp6*	CONFIGURATION FILES startup.cfg, <mac>.cfg
DESCRIPTION	IPv6 mode
FORMAT	Number
DEFAULT VALUE	1
RANGE	0-2 0: manual 1: DHCPv6 2: Autoconfig
EXAMPLE	dhcp6:1

PARAMETER – *ip6*	CONFIGURATION FILES startup.cfg, <mac>.cfg
DESCRIPTION	IPv6 address required for all IPv6 supported features, namely webserver, image download, SIP and file download and so on.

FORMAT	String
DEFAULT VALUE	"::0"
RANGE	-
EXAMPLE	ip6: 2001: f586:1dc4:35e4::198

PARAMETER – *prefix length*	**CONFIGURATION FILES** startup.cfg, <mac>.cfg
DESCRIPTION	IPv6 prefix length
FORMAT	Number
DEFAULT VALUE	64
RANGE	0-128
EXAMPLE	prefix length: 64

PARAMETER – *ipv6 gateway*	**CONFIGURATION FILES** startup.cfg, <mac>.cfg
DESCRIPTION	IPv6 gateway
FORMAT	String
DEFAULT VALUE	"::0"
RANGE	-
EXAMPLE	ipv6 gateway: 2001:f586:1dc4:35e4::1

PARAMETER – *ipv6 dns1*	**CONFIGURATION FILES** startup.cfg, <mac>.cfg
DESCRIPTION	IPv6 DNS1
FORMAT	String
DEFAULT VALUE	"::0"
RANGE	-
EXAMPLE	ipv6 dns1: 2001:f586:1dc4:35e4::12

PARAMETER – *ipv6 dns2*	**CONFIGURATION FILES** startup.cfg, <mac>.cfg
DESCRIPTION	IPv6 DNS2
FORMAT	String

DEFAULT VALUE	"::0"
RANGE	-
EXAMPLE	ipv6 dns2: 2001:f586:1dc4:35e4::12

MULTIPLE CONFIGURATION SERVER SETTINGS

PARAMETER – *firmware server*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies either a full or partial URL of a server (other than the original configuration server) from which the phones in the network get their firmware. **Note:** The default method for the update of firmware to the phones is from the original configuration server. The Administrator must specify a correct server URL for the phones to get their firmware information from that server. If the URL is incorrect, no firmware download occurs to the phones from the specified server.
FORMAT	String (up to 256 characters) **FTP** "ftp://username:password@0.0.0.0:port/path" **TFTP** "tftp://0.0.0.0:port/path" **HTTP** "http://0.0.0.0:port/path" **HTTPS** "https://0.0.0.0:port/path" Partial URL "/path"
DEFAULT VALUE	Blank
RANGE	N/A
EXAMPLE	firmware server: Leaving this parameter blank downloads all configuration and firmware files from the original configuration server. firmware server: tftp://10.30.102.158/test1 The above example uses TFTP to download all firmware files that exist in the "test1" directory on the specified server, to the phones. firmware server: /path The above example uses the configuration server that is linked to the partial path to load the firmware.

ADDITIONAL INFORMATION

The CSV directory files, language packs, TLS certificate files, 802.1x certificate files, and HTTPS files can also be downloaded to the phone from a server other than the configuration server. For each of these types of files, you can specify a URL (server IP address) from which the phone gets these files. You can use existing parameters on the phone to specify the URL.

For more information about this feature, refer to Chapter 1, the section, "CSV Directory Files, Language Packs, TLS Certificates, 802.1x Certificates, HTTPS Files and Multiple Configuration Servers" on page 1-45.

For information on configuring the directory, language pack, TLS certificates, 802.1x certificates, and HTTPS parameters, see the applicable parameters in this Appendix.

RPORT SETTING

PARAMETER – *sip rport*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to enable (1) or disable (0) the use of Rport on the IP phone. "Rport" in RFC 3581, allows a client to request that the server send the response back to the source IP address **and** the port from which the request came. **Note:** Configuring the Rport parameter is recommended for clients behind a firewall.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (disable) 1 (enable)
EXAMPLE	sip rport: 1

LOCAL SIP UDP/TCP PORT SETTING

PARAMETER – *sip local port*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the local source port (UDP/TCP) from which the phone sends SIP messages.
FORMAT	Numeric
DEFAULT VALUE	5060
RANGE	Greater than 1024 and less than 65535 **Notes:** • It is recommended that you avoid the conflict RTP port range in case of a UDP transport. • By default, the IP phones use symmetric UDP signaling for outgoing UDP SIP messages. When symmetric UDP is enabled, the IP phone generates and listens for UDP messages using port 5060.If symmetric UDP signaling is disabled, the phone sends from random ports but it listens on the configured SIP local port.
EXAMPLE	sip local port: 5060

LOCAL SIP TLS PORT

PARAMETER – *sip local tls port*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the local source port (SIPS/TLS) from which the phone sends SIP messages.
FORMAT	Numeric
DEFAULT VALUE	5061
RANGE	Greater than 1024 and less than 65535. **Notes:** • It is recommended that you avoid the conflict with any TCP ports being used. For example: WebUI HTTP server on 80/tcp and HTTPS on 443/tcp. • By default, the IP phones use symmetric TLS signaling for outgoing TLS SIP messages. When symmetric TLS is enabled, the IP phone uses port 5061 as the persistent TLS connection source port. When symmetric TLS signaling is disabled, the IP phone chooses a random persistent TLS connection source port from the TCP range (i.e. 49152...65535) for TLS messages after each reboot regardless of whether the parameter “sip outbound support” is enabled or disabled.
EXAMPLE	sip local tls port: 5061

SIP KEEP ALIVE SUPPORT

PARAMETER – *sip keepalive timer*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This value is how many seconds to wait before sending a SIP UDP keep alive packet to the configured SIP servers. A zero value disables this feature. **Note:** This is only for UDP transport protocol.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	Any positive integer
EXAMPLE	sip keepalive timer: 6

HTTPS CLIENT AND SERVER SETTINGS

PARAMETER – *https client method*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Defines the security method that the client advertises to the server during the Secure Socket Layer (SSL) handshake. Available options are: • **TLS 1.0** - The phone will attempt to communicate using TLS 1.0 only. • **TLS 1.1** - The phone will attempt to communicate using TLS 1.1 only. • **TLS 1.2** - The phone will attempt to communicate using TLS 1.2 only. • **TLS Preferred** - The phone will negotiate with the highest possible TLS version during the handshake. **Note:** This implementation has changed, see Chapter 4, "HTTPS Client/Server Configuration" on page 4-36.
FORMAT	Alphanumeric characters
DEFAULT VALUE	TLS Preferred
RANGE	TLS 1.0 TLS 1.1 TLS 1.2 TLS Preferred
EXAMPLE	https client method: TLS 1.2

PARAMETER – *https redirect http get*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows or disallows redirection from the HTTP server to the HTTPS server.
FORMAT	Boolean
DEFAULT VALUE	1 (enables redirection)
RANGE	0 (disables redirection) 1 (enables redirection)
EXAMPLE	https redirect http get: 0

PARAMETER – *https block http post xml*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the blocking of XML scripts from HTTP POSTs. Some client applications use HTTP POSTs to transfer XML scripts. The phones's HTTP server accepts these POSTs even if server redirection is enabled, effectively bypassing the secure connection. When this parameter is enabled (blocking is enabled), receipt of an HTTP POST containing an XML parameter header results in the following response: "403 Forbidden". This forces the client to direct the POSTs to the HTTPS server through use of the "https://" URL.
FORMAT	Boolean
DEFAULT VALUE	0 (disables blocking of XML HTTP POSTs)
RANGE	0 (disables blocking of XML HTTP POSTs) 1 (enables blocking of XML HTTP POSTs)
EXAMPLE	https block http post xml: 1

HTTPS SERVER CERTIFICATE VALIDATION SETTINGS

PARAMETER – *https validate certificates*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the HTTPS validation of certificates on the phone. When this parameter is set to 1, the HTTPS client performs validation on SSL certificates before accepting them. **Note:** Defining this parameter as "0" (disabled) significantly reduces security for the provisioning process to encryption only. Validation of the chain-of-trust (i.e. the originator of the files) will not be performed if this feature is disabled. Therefore, disabling HTTPS validation of certificates is only recommended for troubleshooting purposes or when self-signed certificates are in use.
FORMAT	Boolean
DEFAULT VALUE	1 (enabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	https validate certificates: 0

PARAMETER – *https validate hostname*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the HTTPS validation of hostnames on the phone.
FORMAT	Boolean
DEFAULT VALUE	1 (enabled)

RANGE	0 (disabled) 1 (enabled)
EXAMPLE	https validate hostname: 0

PARAMETER – *https user certificates*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies a file name for a .PEM file located on the configuration server. This file contains the User-provided certificates in PEM format. These certificates are used to validate peer certificates. **Note:** To install a user-provided certificate through a configuration server using the HTTPS protocol, you must temporarily disable the "**https validate certificates**". After the certificate is installed and you can re-enable the "**https validate certificates**" parameter. You can use this parameter in three ways: • To download no certificates • To download a certificate from the original configuration server • To download a certificate from another specified server To download a specific file, the string value MUST HAVE A FILENAME at the end of the string. For example: https user certificates: ftp://admin:admin!@1.2.3.4:50/path/phonesHTTPSUserCert.pem where "path" is the directory and "phonesHTTPSUserCert.pem" is the filename. If you do not specify a filename, the download fails. See examples for each below.
FORMAT	Alphanumeric string in the format <filename.pem>
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	The following example downloads no HTTPS user certificate file: https user certificates: The following example downloads the HTTPS user certificate file from the original configuration server. https user certificates: phonesHTTPSUserCert.pem The following example uses FTP to download the firmware file "phonesHTTPSUserCert.pem" (HTTPS user certificate file) from the "path" directory on server 1.2.3.4 using port 50: https user certificates:ftp://admin:admin!@1.2.3.4:50/path/phonesHTTPSUserCert.pem

VIRTUAL LOCAL AREA NETWORK (VLAN) SETTINGS

GLOBAL PARAMETERS

PARAMETER – *tagging enabled*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables VLAN on the IP phones. This is a global setting.
FORMAT	Boolean
DEFAULT VALUE	0 (false)
RANGE	0 (false) 1 (true)
EXAMPLE	tagging enabled: 1

PARAMETER – *priority non-ip*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the priority value for non-IP packets. This is a global setting.
FORMAT	Integer
DEFAULT VALUE	5
RANGE	0 to 7
EXAMPLE	priority non-ip: 7

LAN PORT (ETHERNET PORT 0) PARAMETERS

PARAMETER – *vlan id*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg

DESCRIPTION	Allows you to configure a VLAN ID that associates with the physical Ethernet Port 0 (LAN port).
	• When "vlan id" = 4095 and "vlan id port 1" = any ID from 1 to 4094,
	  • The phone allows tagged frames from the PC port (with a VLAN ID) to be untagged before being forwarded to the LAN port.
	  • The phone allows untagged frames from the LAN port (without a VLAN ID) to be tagged with the configured VLAN ID before being forwarded to the PC port.
	
	Example:
	You enable tagging on the phone port as normal but set the "vlan id" to 4095 and the "vlan id port 1" to any ID from 1 to 4094. The following example sets the PC port to be on VLAN 3 but the LAN port is configured as untagged:
	
	tagging enabled: 1
	vlan id: 4095
	vlan id port 1: 3
	
	• When "vlan id" = any ID from 1 to 4094 and "vlan id port 1" = 4095,
	  • The phone allows untagged frames from the LAN port (containing a VLAN ID) to be forwarded to the PC port.
	  • The phone untags the frames in the configured VLAN ID and forwards them to the PC port (without a VLAN ID).
	  • The phone tags the untagged frames from the PC port with the configured VLAN ID and forwards them to the network.
	
	Example:
	You enable tagging on the phone port as normal but set the "vlan id port 1" to 4095 and the "vlan id " to any ID from 1 to 4094. The following example sets the LAN port to be on VLAN 3 but the PC port is configured as untagged:
	
	tagging enabled: 1
	vlan id: 3
	vlan id port 1: 4095

FORMAT	Integer
DEFAULT VALUE	1
RANGE	1 to 4095
EXAMPLE	vlan id: 300

PARAMETER – *tos priority map*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This parameter is based on the Type of Service (ToS), Differentiated Services Code Point (DSCP) setting for SIP (tos sip parameter), RTP (tos rtp parameter) and RTCP (tos rtcp parameter). It is the mapping between the DSCP value and the VLAN priority value for SIP, RTP, and RTCP packets. You enter the tos priority map value as follows: (DSCP_1,Priority_1)(DSCP_2,Priority_2).....(DSCP_64,Priority_64) where the DSCP value range is 0-63 and the priority range is 0-7. Mappings not enclosed in parentheses and separated with a comma, or with values outside the ranges, are ignored.
FORMAT	Integer
DEFAULT VALUE	3 (based on the default ToS DSCP SIP setting of 26) 5 (based on the default ToS DSCP RTP setting of 46) 5 (based on the default ToS DSCP RTCP setting of 46)
RANGE	0 to 63 (for DSCP) 0 to 7 (for SIP, RTP, and RTCP priorities)
EXAMPLE	tos priority map: (26,7)

The following table identifies the default DSCP-to-priority mapping structure.

DSCP RANGE	DSCP PRIORITY
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

PC PORT (ETHERNET PORT 1) PARAMETERS

PARAMETER – *vlan id port 1*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg

DESCRIPTION	Allows you to configure a VLAN ID that associates with the physical Ethernet Port 1 (PC port).
	• When “vlan id” = any ID from 1 to 4094 and “vlan id port 1” = 4095,
	  • The phone allows untagged frames from the LAN port (with a VLAN ID) to be forwarded to the PC port.
	  • The phone untags the frames in the configured VLAN ID and forwards them to the PC port (without a VLAN ID).
	  • The phone tags the untagged frames from the PC port with the configured VLAN ID and forwards them to the network.
	
	Example:
	You enable tagging on the phone port as normal but set the “vlan id port 1” to 4095 and the “vlan id ” to any ID from 1 to 4094. The following example sets the LAN port to be on VLAN 3 but the PC port is configured as untagged:
	
	tagging enabled: 1
	vlan id: 3
	vlan id port 1: 4095
	• When "vlan id" = 4095 and “vlan id port 1” = any ID from 1 to 4094,
	  • The phone allows tagged frames from the PC port (with a VLAN ID) to be untagged before being forwarded to the LAN port.
	  • The phone allows untagged frames from the LAN port (without a VLAN ID) to be tagged with the configured VLAN ID before being forwarded to the PC port.
	
	Example:
	You enable tagging on the phone port as normal but set the “vlan id” to 4095 and the “vlan id port 1” to any ID from 1 to 4094. The following example sets the PC port to be on VLAN 3 but the LAN port is configured as untagged:
	
	tagging enabled: 1
	vlan id: 4095
	vlan id port 1: 3

FORMAT	Integer
DEFAULT VALUE	4095
RANGE	1 to 4095
EXAMPLE	vlan id port 1: 3

PARAMETER – *qos eth port 1 priority*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg

DESCRIPTION	Specifies the priority value used for passing VLAN packets through to a PC via Port 1.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 to 7
EXAMPLE	qos eth port 1 priority: 3

RTCP SUMMARY REPORTS

GLOBAL PARAMETERS

PARAMETER – *sip rtcp summary reports*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not to send of RTCP summary reports. You must restart the phone after setting a value for this parameter.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (disabled - OFF) 1 (enabled - ON)
EXAMPLE	sip rtcp summary reports: 1

PARAMETER – *sip rtcp summary report collector*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the hostname server for which to send (collect) the RTCP summary reports. You must restart the phone after setting a value for this parameter.
FORMAT	<username>@<server> **Note:** Hostname/server string must not exceed 128 characters in length.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	sip rtcp summary report collector: collector@example.org

PARAMETER – *sip rtcp summary report collector port*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the port address of the hostname server receiving the RTCP summary reports. You must restart the phone after setting a value for this parameter.
FORMAT	Integer

DEFAULT VALUE	0
RANGE	0 to 65536
EXAMPLE	sip rtcp summary report collector port: 5060

LINE PARAMETERS

PARAMETER – *sip lineN rtcp summary reports* (where N = line number)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables/disables the specified line number on the phone for which to send the RTCP summary reports. **Note:** You must restart the phone after setting a value for this parameter.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sip line1 rtcp summary reports: 1

PARAMETER – *sip lineN rtcp summary report collector* (where N = line number)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Per-line parameter specifying the hostname of the server receiving the RTCP summary reports. **Note:** You must restart the phone after setting a value for this parameter.
FORMAT	<username>@<server> **Note:** Hostname/server string must not exceed 128 characters in length.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	sip line1 rtcp summary report collector: collector@example.org

PARAMETER – *sip lineN rtcp summary report collector port* (where N = line number)	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Per-line parameter specifying the port address of the server receiving the RTCP summary reports. **Note:** You must restart the phone after setting a value for this parameter.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 to 65536
EXAMPLE	sip line1 rtcp summary report collector port: 5060

TYPE OF SERVICE (TOS)/DSCP SETTINGS

PARAMETER – *tos sip*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The Differentiated Services Code Point (DSCP) for SIP packets.
FORMAT	Integer
DEFAULT VALUE	26
RANGE	0-63
EXAMPLE	tos sip: 3

PARAMETER – *tos rtp*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The Differentiated Services Code Point (DSCP) for RTP packets.
FORMAT	Integer
DEFAULT VALUE	46
RANGE	0-63
EXAMPLE	tos rtp: 2

PARAMETER – *tos rtcp*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The Differentiated Services Code Point (DSCP) for RTCP packets.
FORMAT	Integer
DEFAULT VALUE	46
RANGE	0-63
EXAMPLE	tos rtcp: 3

TIME AND DATE SETTINGS

PARAMETER – *time format*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This parameter changes the time to 12 hour or 24 hour format. Use “0” for the 12 hour format and “1” for the 24 hour format.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 (12 hr format)) 1 (24 hr format)
EXAMPLE	time format: 0

PARAMETER – *date format*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This parameter allows the user to change the date to various formats.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 (WWW MMM DD) (default) 1 (DD-MMM-YY) 2 (YYYY-MM-DD) 3 (DD/MM/YYYY) 4 (DD/MM/YY) 5 (DD-MM-YY) 6 (MM/DD/YY) 7 (MMM DD) 8 (DD MMM YYYY) 9 (WWW DD MMM) 10 (DD MMM) 11 (DD.MM.YYYY)
EXAMPLE	date format: 7

PARAMETER – *dst config*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables/disables the use of daylight savings time.
FORMAT	Integer
DEFAULT VALUE	3
RANGE	0 - OFF 1 - 30 min summertime 2 - 1 hr summertime 3 - automatic
EXAMPLE	dst config: 0

TIME ZONE NAME

PARAMETER – *time zone name*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Assigns a time zone name to the time server. The **Custom** option allows you to customize additional time zone parameters. The **DP-Dhcp** option allows you to enable and disable a DHCP Option 2 value for the phone to use as an offset from Coordinated Universal Time (UTC). If this parameter is enabled, the phone derives the time and date from UTC and the time offset offered by the DHCP server. **Notes:** • Assigning the name "**Custom**" (with initial cap) in the configuration files, allows you to create a custom time zone using the additional parameters in the section "Custom Time Zone and DST Settings" on page A-67. • When DHCP Option 2 is enabled on the phone, the phone still uses the custom timezone configuration settings to control daylight savings time. • The default behavior for the phone is to use the NTP server from Option 42 (or current configuration setting) and the current timezone settings.
FORMAT	Text
DEFAULT VALUE	US-Eastern **Note:** If the time zone name parameter is set to a value other than Dhcp, then DHCP Option 2 is disabled.
RANGE	See "Time Zone Name/Time Zone Code Table" on page A-61 for specific time zone names. **Custom** (allows you to create a customized time zone). **DP-Dhcp** (allows you to enable and disable a DHCP Option 2 value for the phone to use as an offset from Coordinated Universal Time (UTC))
EXAMPLE	time zone name: US-Central time zone name: Custom time zone name: DP-Dhcp

TIME ZONE NAME/TIME ZONE CODE TABLE

TIME ZONE NAME	TIME ZONE CODE
AD-Andorra	CET
AE-Dubai	GST
AG-Antigua	AST
AI-Anguilla	AST
AL-Tirane	CET
AN-Curacao	AST
AR-Buenos Aires	ART
AR-Saudi Arabia	ART
AS-Pago Pago	BST
AT-Vienna	CET
AU-Lord Howe	LHS
AU-Tasmania	EST
AU-Melbourne	EST
AU-Sydney	EST
AU-Broken Hill	CST
AU-Brisbane	EST
AU-Lindeman	EST
AU-Adelaide	CST
AU-Darwin	CST
AU-Perth	WST
AW-Aruba	AST
AZ-Baku	AZT

TIME ZONE NAME	TIME ZONE CODE
BA-Sarajevo	EET
BB-Barbados	AST
BE-Brussels	CET
BG-Sofia	EET
BM-Bermuda	AST
BO-La Paz	BOT
BR-Noronha	FNT
BR-Belem	BRT
BR-Fortaleza	BRT
BR-Recife	BRT
BR-Araguaina	BRS
BR-Maceio	BRT
BR-Sao Paulo	BRS
BR-Cuiaba	AMS
BR-Porto Velho	AMT
BR-Boa Vista	AMT
BR-Manaus	AMT
BR-Eirunepe	ACT
BR-Rio Branco	ACT
BS-Nassau	EST
BY-Minsk	EET
BZ-Belize	CST
CA-Newfoundland	NST
CA-Atlantic	AST
CA-Eastern	EST
CA-Saskatchewan	EST
CA-Central	CST
CA-Mountain	MST
CA-Pacific	PST
CA-Yukon	PST
CH-Zurich	CET
CK-Rarotonga	CKS
CL-Santiago	CLS
CL-Easter	EAS
CN-Beijing	CST
CO-Bogota	COS
CR-Costa Rica	CST
CU-Havana	CST
CY-Nicosia	EES
CZ-Prague	CET

TIME ZONE NAME	TIME ZONE CODE
DE-Berlin	CET
DK-Copenhagen	CET
DM-Dominica	AST
DO-Santo Domingo	AST
Dhcp	DP
EE-Tallinn	EET
ES-Madrid	CET
ES-Canary	WET
FI-Helsinki	EET
FJ-Fiji	NZT
FK-Stanley	FKS
FO-Faeroe	WET
FR-Paris	CET
GB-London	GMT
GB-Belfast	GMT
GD-Grenada	AST
GE-Tbilisi	GET
GF-Cayenne	GFT
GI-Gibraltar	CET
GP-Guadeloupe	AST
GR-Athens	EET
GS-South Georgia	GST
GT-Guatemala	CST
GU-Guam	CST
GY-Guyana	GYT
HK-Hong Kong	HKS
HN-Tegucigalpa	CST
HR-Zagreb	CET
HT-Port-au-Prince	EST
HU-Budapest	CET
IE-Dublin	GMT
IN-Kolkata	IST
IS-Reykjavik	GMT
IT-Rome	CET
JM-Jamaica	EST
JP-Tokyo	JST
KY-Cayman	EST
LC-St Lucia	AST
LI-Vaduz	CET
LT-Vilnius	EET
LU-Luxembourg	CET
LV-Riga	EET

TIME ZONE NAME	TIME ZONE CODE
MC-Monaco	CET
MD-Chisinau	EET
MK-Skopje	CET
MQ-Martinique	AST
MS-Montserrat	AST
MT-Malta	CET
MU-Mauritius	MUT
MX-Mexico City	CST
MX-Cancun	CST
MX-Merida	CST
MX-Monterrey	CST
MX-Mazatlan	MST
MX-Chihuahua	MST
MX-Hermosillo	MST
MX-Tijuana	PST
NI-Managua	CST
NL-Amsterdam	CET
NO-Oslo	CET
NR-Nauru	NRT
NU-Niue	NUT
NZ-Auckland	NZS
NZ-Chatham	CHA
OM-Muscat	GST
PA-Panama	EST
PE-Lima	PES
PL-Warsaw	CET
PR-Puerto Rico	AST
PT-Lisbon	WET
PT-Madeira	WET
PT-Azores	AZO
PY-Asuncion	PYS

TIME ZONE NAME	TIME ZONE CODE
RO-Bucharest	EET
RU-Kaliningrad	EET
RU-Moscow	MSK
RU-Samara	SAM
RU-Yekaterinburg	YEK
RU-Omsk	OMS
RU-Novosibirsk	NOV
RU-Krasnoyarsk	KRA
RU-Irkutsk	IRK
RU-Yakutsk	YAK
RU-Vladivostok	VLA
RU-Sakhalin	SAK
RU-Magadan	MAG
RU-Kamchatka	PET
RU-Anadyr	ANA
SA-Saudi Arabia	AST
SE-Stockholm	CET
SG-Singapore	SGT
SI-Ljubljana	CET
SK-Bratislava	CET
SM-San Marino	CET
SR-Paramaribo	SRT
SV-El Salvador	CST
TR-Istanbul	EET
TT-Port of Spain	AST
TW-Taipei	CST
UA-Kiev	EET
US-Eastern	EST
US-Central	CST
US-Mountain	MST
US-Pacific	PST
US-Alaska	AKS
US-Aleutian	HAS
US-Hawaii	HST
UY-Montevideo	UYS
VA-Vatican	CET
VE-Caracas	VET
YU-Belgrade	CET

TIME SERVER SETTINGS

PARAMETER – *time server disabled*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the time server. This parameter affects the **time server1**, **time server2**, and **time server3** parameters. Setting this parameter to **0** allows the use of the configured Time Server(s). Setting this parameter to **1** prevents the use of the configured Time Server(s).
FORMAT	Integer
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	time server disabled: 0

PARAMETER – *time server1*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The primary time server's IP address or qualified domain name. If the time server is enabled, the value for time server1 will be used to request the time. **Note:** For DHCP to automatically populate this parameter, your DHCP server must support Option 42.
FORMAT	IP address or qualified domain name
DEFAULT VALUE	1.mitel.pool.ntp.org
RANGE	N/A
EXAMPLE	time server1: 192.168.0.5

PARAMETER – *time server2*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The secondary time server's IP address or qualified domain name. If the time server is enabled, and the primary time server is not configured or cannot be accessed the value for time server2 will be used to request the time. For DHCP to automatically populate this parameter, your DHCP server must support Option 42.
FORMAT	IP address or qualified domain name
DEFAULT VALUE	2.mitel.pool.ntp.org
RANGE	N/A
EXAMPLE	time server2: 192.168.0.5

PARAMETER – *time server3*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The tertiary time server's IP address or qualified domain name. If the time server is enabled, and the primary and secondary time servers are not configured or cannot be accessed the value for time server3 will be used to request the time. For DHCP to automatically populate this parameter, your DHCP server must support Option 42.
FORMAT	IP address or qualified domain name
DEFAULT VALUE	3.mitel.pool.ntp.org
RANGE	N/A
EXAMPLE	time server3: 192.168.0.5

CUSTOM TIME ZONE AND DST SETTINGS

Note: To use the parameters in this section, the "**time zone name**" parameter must be set to "**Custom**". See page A-60 for more information.

PARAMETER – *time zone minutes*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The number of minutes the timezone is offset from UTC (Coordinated Universal Time). This can be positive (West of the Prime Meridian) or negative (East of the Prim Meridian). Eastern Standard Time (EST) has a value of 300 which is the default.
FORMAT	Integer
DEFAULT VALUE	300

RANGE	Any positive or negative Integers: 720 (GMT minus 12 hours) 660 (GMT minus 11 hours) 600 (GMT minus 10 hours) 540 (GMT minus 9 hours - Alaska Standard Time North America) 480 (GMT minus 8 hours - Pacific Standard Time North America) 420 (GMT minus 7 hours - Mountain Standard Time North America) 360 (GMT minus 6 hours - Central Standard Time North America) 300 (GMT minus 5 hours - Eastern Standard Time North America) 270 (GMT minus 4.5 hours - Venezuela) 240 (GMT minus 4 hours) 210 (GMT minus 3.5 hours - Newfoundland Standard Time North America) 180 (GMT minus 3 hours) 150 (GMT minus 2.5 hours - Newfoundland daylight time) 120 (GMT minus 2 hours) 60 (GMT minus 1 hour) 0 (GMT = 0 hours - Greenwich Mean Time) -60 (GMT + 1 hour - Central European Time) -120 (GMT + 2 hours - Eastern European Time Europe) -180 (GMT + 3 hours) -210 (GMT + 3.5 hours) -240 (GMT + 4 hours) -270 (GMT + 4.5 hours) -300 (GMT + 5 hours) -330 (GMT + 5.5 hours) -345 (GMT + 5.75 hours) -360 (GMT + 6 hours) -390 (GMT + 6.5 hours) -420 (GMT + 7 hours - Christmas Island Time Australia) -480 (GMT + 8 hours - Australian Western Standard Time) -540 (GMT + 9 hours) -570 (GMT + 9.5 hours - Australian Central Standard Time) -600 (GMT + 10 hours - Australian Eastern Standard Time) -660 (GMT + 11 hours) -720 (GMT + 12 hours) -780 (GMT + 13 hours)
EXAMPLE	time zone minutes: 300

PARAMETER – *dst minutes*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The number of minutes to add during Daylight Saving Time. Valid values are a positive integer between 0 to 60.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	0-60
EXAMPLE	dst minutes: 60

PARAMETER – *dst start relative date*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies how to interpret the start day, month, and week parameters - absolute (0) or relative (1).
FORMAT	Boolean
DEFAULT VALUE	N/A
RANGE	0 (absolute) 1 (relative)
EXAMPLE	dst start relative date: 1

PARAMETER – *dst end relative date*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies how to interpret the end day, month, and week parameters - absolute (0) or relative (1).
FORMAT	Boolean
DEFAULT VALUE	N/A
RANGE	0 (absolute) 1 (relative)
EXAMPLE	dst end relative date: 1

Absolute Time

PARAMETER – *dst start month*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The month that DST starts. Valid values are 1 to 12 (January to December).
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	1 (January) 2 (February) 3 (March) 4 (April) 5 (May) 6 (June) 7 (July) 8 (August) 9 (September) 10 (October) 11 (November) 12 (December)
EXAMPLE	dst start month: 7

PARAMETER – *dst end month*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The month that DST ends. Valid values are 1 to 12 (January to December).
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	1 (January) 2 (February) 3 (March) 4 (April) 5 (May) 6 (June) 7 (July) 8 (August) 9 (September) 10 (October) 11 (November) 12 (December)
EXAMPLE	dst end month: 6

PARAMETER – *dst start day*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The day of the month that DST starts. Valid values are 1 to 31.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	1-31
EXAMPLE	dst start day: 1

PARAMETER – *dst end day*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The day of the month that DST ends. Valid values are 1 to 31.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	1-31
EXAMPLE	dst end day: 31

PARAMETER – *dst start hour*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The hour that DST starts. Valid values are an integer from 0 (midnight) to 23.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	0 (midnight) to 23
EXAMPLE	dst start hour: 0

PARAMETER – *dst end hour*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The hour that DST ends. Valid values are an integer from 0 (midnight) to 23.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	0 (midnight) to 23
EXAMPLE	dst end hour: 23

Relative Time

PARAMETER – *dst start month*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The month that DST starts. Valid values are 1 to 12 (January to December).
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	1 (January) 2 (February) 3 (March) 4 (April) 5 (May) 6 (June) 7 (July) 8 (August) 9 (September) 10 (October) 11 (November) 12 (December)
EXAMPLE	dst start month: 6

PARAMETER – *dst end month*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The month that DST ends. Valid values are 1 to 12 (January to December).
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	1 (January) 2 (February) 3 (March) 4 (April) 5 (May) 6 (June) 7 (July) 8 (August) 9 (September) 10 (October) 11 (November) 12 (December)
EXAMPLE	dst end month: 12

PARAMETER – *dst start week*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The week in the specified month in which DST starts. Valid value is a positive or negative integer from 1 to 5.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	1 = first full week of month -1 = last occurrence "dst start day" in the month 2 = second full week of month -2 = second last occurrence "dst start day" in the month 3 = third full week of month -3 = third last occurrence "dst start day" in the month 4 = fourth full week of month -4 = fourth last occurrence "dst start day" in the month 5 = fifth full week of month -5 = fifth last occurrence "dst start day" in the month
EXAMPLE	dst start week: 1

PARAMETER – *dst end week*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The week in the specified month in which DST ends. Valid value is a positive or negative integer from 1 to 5.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	1 = first full week of month -1 = last occurrence "dst end day" in the month 2 = second full week of month -2 = second last occurrence "dst end day" in the month 3 = third full week of month -3 = third last occurrence "dst end day" in the month 4 = fourth full week of month -4 = fourth last occurrence "dst end day" in the month 5 = fifth full week of month -5 = fifth last occurrence "dst end day" in the month
EXAMPLE	dst end week: 5

PARAMETER – *dst start day*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The day of the specified week in the specified month that DST starts on. Valid values are an integer from 1 to 7.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	1 (Sunday) 2 (Monday) 3 (Tuesday) 4 (Wednesday) 5 (Thursday) 6 (Friday) 7 (Saturday)
EXAMPLE	dst start day: 1

PARAMETER – *dst end day*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The day of the specified week in the specified month that DST ends on. Valid values are an integer from 1 to 7.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	1 (Sunday) 2 (Monday) 3 (Tuesday) 4 (Wednesday) 5 (Thursday) 6 (Friday) 7 (Saturday)
EXAMPLE	dst end day: 7

PARAMETER – *dst start hour*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The hour that DST starts. Valid values are an integer from 0 (midnight) to 23.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	0 (midnight) to 23
EXAMPLE	dst start hour: 0

PARAMETER – *dst end hour*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The hour that DST ends. Valid values are an integer from 0 (midnight) to 23.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	0 (midnight) to 23
EXAMPLE	dst end hour: 23

BACKLIGHT MODE SETTINGS

Note: Backlight mode **off** is applicable to the 6865i and 6910 IP phones only.

PARAMETER – *backlight mode*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to turn the backlight on the LCD, Off (always off) or Auto. The “Auto” setting sets the phone to turn off the backlight after a period of inactivity. You can set the amount of time before the backlight goes off using the “Backlight on Time” option (“bl on time” parameter).
FORMAT	Integer
DEFAULT VALUE	1 (Auto)
RANGE	**0** (Off - Turns the backlight off constant) - applicable on 6865i and 6910 IP Phones only. **1** (Auto - Turns the backlight off after a period of inactivity.) **Note:** In the IP Phone UI of 6865i and 6910, the options for this parameter are "Off" and "Auto" only.
EXAMPLE	backlight mode: 0

PARAMETER – *bl on time*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to set the amount of time, in seconds, that the backlight stays ON before turning OFF because of inactivity. **Note:** For the 6865i and 6910, the backlight mode must be set to "Auto" before this parameter can take effect.
FORMAT	Integer
DEFAULT VALUE	600 seconds (equals 10 minutes)
RANGE	1-36000 seconds

EXAMPLE	bl on time: 15

BRIGHTNESS LEVEL SETTINGS

Note: Applicable to the 6865i, 6867i, 6869i, 6873i, 6910, 6920, 6930, 6940, and 6970 IP Phones only.

PARAMETER – *brightness level*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the brightness level when the phone is active, brightness level is applicable on 6865i and 6910 as well unless "backlight mode" is 0.
FORMAT	Integer
DEFAULT VALUE	3
RANGE	1-5
EXAMPLE	brightness level: 5

PARAMETER – *inactivity brightness level*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the brightness level when the phone is inactive.
FORMAT	Integer
DEFAULT VALUE	1
RANGE	0-4 (where “0” represents screen going complete black on 6867i, 6869i, 6873i, 6920, 6930, 6940 and 6970. For 6865i and 6910 backlight will be turned off)
EXAMPLE	inactivity brightness level: 0

BACKGROUND IMAGE ON IDLE SCREEN

Note: Applicable to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones only.

PARAMETER – *background image*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the location of the background image for the idle screen on the SIP IP phones. Requirements are as follows: • 320x240 pixels (6867i/ 6920) • 480x272 pixels (6869i/ 6930) • 800x480 pixels (6873i/ 6940/ 6970) • 24 or 32-bit color depth • 1MB maximum file size • Both JPG and PNG files are supported (JPG strongly recommended due to smaller file size and faster loading time) • There should be no frame around the image
FORMAT	String (up to 256 characters)
DEFAULT VALUE	NA
RANGE	tftp://server/image.png ftp://server/image.jpg http://server/image.png https://server/image/jpg
EXAMPLE	background image: http://10.30.100.233/pics/image.png

HOME/IDLE SCREEN SETTINGS

Note: Applicable to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones only.

PARAMETER – *idle screen mode*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Used to switch between the two Home/Idle screen modes. The primary screen mode provides users with a larger date and time and displays the Screen Name (“**sip screen name**”) parameter beside the line number in the top status bar. The secondary screen mode displays both the Screen Name and Screen Name 2 (“**sip screen name 2**”) parameters above the smaller, repositioned date and time.
FORMAT	Boolean
DEFAULT VALUE	0 (primary screen mode)
RANGE	0-1 0 (primary screen mode) 1 (secondary screen mode)
EXAMPLE	idle screen mode: 1

PARAMETER – *idle screen font color*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the font color of the date, time, and status message text on the home/idle screen of the SIP IP phones.
FORMAT	String
DEFAULT VALUE	blue
RANGE	blue white black
EXAMPLE	idle screen font color: white

SCREEN SAVER SETTINGS

Note: Applicable to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones only.

PARAMETER – *screen save time*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the amount of time (in seconds) the phone must be idle before the SIP IP phone's screen saver initiates. **Note:** From Release 6.1.0, IP phones will not support the complete disabling of the screen saver.
FORMAT	Integer
DEFAULT VALUE	1800 (seconds)
RANGE	1 - 14400
EXAMPLE	screen save time: 240

BACKGROUND IMAGE ON SCREEN SAVER

PARAMETER – *screen saver background image*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the location and file name of the background image for the screen saver on 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 phones. Requirements are as follows: • 320x240 pixels (6867i/ 6920) • 480x272 pixels (6869i/ 6930) • 800x480 pixels (6873i/ 6940/ 6970) • 24 or 32-bit color depth • 1MB maximum file size • Both JPG and PNG files are supported (JPG strongly recommended due to smaller file size and faster loading time) • There should be no frame around the image
FORMAT	String (up to 256 characters)
DEFAULT VALUE	N/A
RANGE	tftp://server/image.jpg ftp://server/image.jpg http://server/image.jpg https://server/image.jpg
EXAMPLE	screen saver background image: http://192.168.0.22/pics/image.jpg

PARAMETER – *screen saver refresh timer*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the interval (in minutes) when the screen saver background image is refreshed.
FORMAT	Integer
DEFAULT VALUE	1 (every 1 min screen saver background image will be refreshed)
RANGE	1 to 1440 minutes
EXAMPLES	screen saver refresh timer: 5

USE COLOR AVATAR

PARAMETER – *use color avatars*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to enable or disable the color avatar/placeholders on the phone.
FORMAT	Boolean
DEFAULT VALUE	1 (Enabled)

RANGE	0 - 1 0 (Disabled) 1 (Enabled)
EXAMPLES	use color avatars: 1

PICTURE ID FEATURE

Note: Applicable to the 6867i, 6869i, 6873i, 6920, 6930, 6940, and 6970 IP Phones only.

PARAMETER – *image server uri*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to specify the server URI where pictures are stored for display to the phone during incoming and outgoing calls, and in the Directory, Received Callers List, and Outgoing Redial List entries. The pictures are dynamically retrieved from the centralized server for each call and then locally cached in the phone to reduce network traffic. If there is no picture on the central server for the dialed number and/or Caller Id number, and Directory, Received Callers List, and/or Outgoing Redial List entry, the generic blue figure image is shown. Pictures must be in ".png" format and 150 pixels wide x 150 pixels tall. For the 6867i/6869i/6873i, the png can be 24-bit or 32-bit. The filenames for pictures must be stored using the phone number as the filename (for example, 9995551234.png). **Notes:** • Entering no value for this parameter disables this feature. • The "image server uri" parameter supports TFTP, FTP, HTTP, and HTTPS. • The resolution specification for Picture IDs in releases previous to Release 4.3.0 SP1 was 150x200 pixels. Picture IDs in this resolution can still be used, but will not be optimally displayed on-screen due to the UI redesign implemented in Release 4.3.0 SP1. To align with the new UI implemented in Release 4.3.0 SP1, ensure the resolution of your Picture IDs are 150x150 pixels.
FORMAT	Server URI String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	image server uri: tftp://192.168.1.100

IDLE SCREEN ERROR MESSAGES SUPPRESSION

PARAMETER – *idle screen error messages suppression*	CONFIGURATION FILES startup.cfg, aastra.cfg, <model>.cfg <mac>.cfg
DESCRIPTION	Enable or disable idle screen error messages suppression. When idle screen error messages suppression is enabled the IP phone will suppress the error message on the idle screen. This parameter is bitwise, it means only the 3 least significant bit are used, but any value can be configured. 1: suppress 802.1x error 2: suppress TR-069 error 4: suppress https cert error As a result "idle screen error messages suppression: 3" will suppress 802.1x and TR-069 error message on idle screen. **Note:** The *idle screen error messages suppression* parameter can be configured using the configuration file only.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	NA
EXAMPLE	idle screen error messages suppression: 0

DHSG SETTINGS

Note: Applicable to the 6865i, 6867i, 6869i, 6920, and 6930 IP Phones only.

PARAMETER – *dhsg*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables and disables the DHSG headset support on the phone. **Note:** The phones that support DHSG are the 6865i, 6867i, and 6869i. For more information about installing a DHSG headset on your phone, see your *IP Phone-Specific Installation Guide*.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (disable - DHSG support is OFF) 1 (enable - DHSG support is ON)
EXAMPLE	dhsg: 1

LIVE DIALPAD SETTINGS

PARAMETER – *live dialpad*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg

DESCRIPTION	Turns the "Live Dialpad" feature ON or OFF. With live dial pad ON, the IP phone automatically dials out and turns ON Handsfree mode as soon as a dial pad key or softkey is pressed. With live dial pad OFF, if you dial a number while the phone is on-hook, lifting the receiver or pressing the Speaker/Headset key initiates a call to that number.
FORMAT	Boolean
DEFAULT VALUE	0 (Disabled)
RANGE	0 - 1 0 (Disabled) 1 (Enabled)
EXAMPLE	live dialpad: 1

LIVE KEYBOARD SETTINGS

PARAMETER – *live keyboard*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not an alphabetic character key press on a K680i keyboard attached to an idle 6867i or 6869i SIP phone should launch the Directory search function.
FORMAT	Boolean
DEFAULT VALUE	0 (Disabled)
RANGE	0 - 1 0 (Disabled) 1 (Enabled)
EXAMPLE	live keyboard: 1

PARAMETER – *keyboard script*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the URI to be called when an alphabetic key on a K680i keyboard attached to a 6867i or 6869i SIP phone is pressed. If this parameter is not defined or left blank, the phone's native Directory search function will be launched. **Note:** The Live Keyboard feature must be enabled to use this feature.
FORMAT	Alphanumeric characters
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	keyboard script: http://192.168.0.20/keyboardscript.xml

SIP LOCAL DIAL PLAN SETTINGS

PARAMETER –
sip dial plan

CONFIGURATION FILES
startup.cfg, <model>.cfg, <mac>.cfg

DESCRIPTION

A dial plan describes the number and pattern of digits that a user dials to reach a particular telephone number. The SIP local dial plan is as follows:

<table>
<tr><th>Symbol</th><th>Description</th></tr>
<tr><td>0, 1, 2, 3, 4, 5, 6, 7, 8, 9</td><td>Digit symbol</td></tr>
<tr><td>X</td><td>Match any digit symbol (wildcard)</td></tr>
<tr><td>*, #, .</td><td>Other keypad symbol; # can terminate a dial string</td></tr>
<tr><td>|</td><td>Expression inclusive OR</td></tr>
<tr><td>+</td><td>• 0 or more of the preceding digit symbol or [] expression.
• The dial plan must not end with +.
• The dial plan must be suffixed with "#", if the sip dial plan terminator is disabled or it must be suffixed with "^", if the sip dial plan terminator is enabled.</td></tr>
<tr><td>[]</td><td>Symbol inclusive OR</td></tr>
<tr><td>-</td><td>Used only with [], represent a range of acceptable symbols; For example, [2-8]</td></tr>
<tr><td>“,” (open/close quotes)</td><td>In the configuration files, enter the sip dial plan value using quotes.</td></tr>
<tr><td>.;.</td><td>Used when a secondary dial tone is required on the phone. (For example, “9;xxxxxx”, when a user has to dial “9” to get and outside line and needs a secondary dial tone presented.</td></tr>
</table>

You can configure prefix dialling by adding a prepend digit to the dial string. For example, if you add a prepend map of “[2-9]XXXXXXXXX,91”, the IP phone adds the digits “91” to any 10-digit number beginning with any digit from 2 to 9 that is dialed out. Other examples of prepend mappings are:

1X+#,9 (Prepends 9 to any digit string beginning with “1” and terminating with “#”.)

6XXX,579 (Prepends “579” to any 4-digit string starting with “6”.)

[4-6]XXXXXX,78 (Prepends “78” to any 7-digit string starting with “4”, “5”, or “6”.

FORMAT
Alphanumeric characters

DEFAULT VALUE
X+#|XX+*

RANGE	Up to 512 alphanumeric characters. If a User enters a dial plan longer than 512 characters, or a parsing error occurs, the phone uses the default dial plan of “x+#|xx+*”. If this is the case, the Administrator cannot change the dial plan from the configuration files. The dial plan must be changed from the Mitel Web UI.
EXAMPLE	sip dial plan: "X+#|XXX+*"

PARAMETER – *sip dial plan terminator*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not pressing the hash/pound (i.e. "#") key, while performing an outgoing call on an open line, should be sent as %23 to the proxy in the dial string or if the key should be used as a dial plan terminator (i.e. dials out the call immediately). When enabled, the hash/pound key does not act as a dial plan terminator and is instead sent as %23 to the proxy in the dial string. When disabled (default), the hash/pound key acts as a dial plan terminator.
FORMAT	Boolean
DEFAULT VALUE	0 (Disabled)
RANGE	0 (Disabled - # used as a dial plan terminator) 1 (Enabled - # sent as %23 in dial string)
EXAMPLE	sip dial plan terminator: 1

PARAMETER – *sip digit timeout*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Represents the time, in seconds, between consecutive key presses on the IP phone. The default for this parameter is 4 seconds. If you press a key on the phone and wait 4 seconds before pressing the next key, the key times out and cancels the digit selection. You must press consecutive keys before the timeout occurs.
FORMAT	Integer
DEFAULT VALUE	4
RANGE	N/A
EXAMPLE	sip digit timeout: 6

SIP OUTBOUND SUPPORT

PARAMETER – *sip outbound support*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables and disables whether or not the phone uses Draft 15 (draft-ietf-sip-outbound-15) support for SIP outbound packets. A SIP User Agent (UA) behind a firewall, reuses an existing connection (usually the REGISTER outbound connection) for the inbound request if the proxy supports it. The UA uses keep-alive packets to monitor the connection status. **Notes:** • If the Global SIP parameter “Persistent TLS” is set on the phone, then only one TLS persistent connection can be established since the phone uses the local port 5061 for connection. If the Global SIP parameter “TLS” is set on the phone, more than one connection can be setup since the phone uses a random local port for connection. • This parameter must be enabled for this feature to start keep-alive for a particular transport.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sip outbound support: 1

CONTACT HEADER MATCHING

PARAMETER – *sip contact matching*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the method for which the phone uses to match the Contact header in a SIP registration packet.
FORMAT	Integer
DEFAULT VALUE	2 (matching username only)
RANGE	0(default) URI matching of username, domain name, phone IP and port, and transport 1matching of phone IP only 2matching of username only 3matching of phone IP and username only
EXAMPLE	sip contact matching: 1

SIP BASIC, GLOBAL SETTINGS

SIP GLOBAL AUTHENTICATION SETTINGS

PARAMETER – *sip screen name*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Used to display text on the screen of the phone. You may want to set this parameter to display the user's name of the phone.
FORMAT	Text
DEFAULT VALUE	N/A
RANGE	Up to 20 alphanumeric characters
EXAMPLE	sip screen name: Joe Smith

PARAMETER – *sip screen name 2*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Used to display text on a second line on the screen of the phone. **Notes:** • If other status messages display on the phone, such as "Network Disconnected", the Screen Name 2 value does not display. • Symbol characters are allowed (such as "#"). • If the text is longer than the display width, than the display truncates the text to fit the display.
FORMAT	Alphanumeric characters.
DEFAULT VALUE	N/A
RANGE	Up to 20 alphanumeric characters.
EXAMPLE	sip screen name 2: Lab Phone

PARAMETER – *sip user name*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Used in the name field of the *SIP URI* for the IP phone and for registering the IP phone at the registrar. **Note:** The IP Phones support Usernames containing dots (".").
FORMAT	Text
DEFAULT VALUE	N/A
RANGE	Up to 20 alphanumeric characters
EXAMPLE	sip user name: 1010

PARAMETER – *sip display name*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Used in the display name field of the *From* SIP header field. Some IP PBX systems use this as the caller's ID and some may overwrite this with the string that is set at the PBX system.
FORMAT	Text
DEFAULT VALUE	N/A
RANGE	Up to 20 alphanumeric characters
EXAMPLE	sip display name: Joe Smith

PARAMETER – *sip auth name*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Used in the username field of the Authorization header field of the *SIP REGISTER* request.
FORMAT	Text
DEFAULT VALUE	N/A
RANGE	Up to 20 alphanumeric characters
EXAMPLE	sip auth name: 5553456

PARAMETER – *sip password*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Password used to register the IP phone with the SIP proxy.
FORMAT	Text
DEFAULT VALUE	N/A
RANGE	Up to 20 alphanumeric characters
EXAMPLE	sip password: 12345

PARAMETER – *mask sip password*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables the enhanced security feature whereby a user's SIP account password is hidden/masked in the server.cfg and local.cfg files (downloaded from the IP phone's Web UI troubleshooting page for debug purposes).
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0-1 0 (disabled) 1 (enabled)
EXAMPLE	mask sip password: 1

PARAMETER – *sip bla number*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to assign a phone number that is shared across all IP phones.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	sip bla number: 1010

PARAMETER – *sip mode*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to configure the mode of the line. Applicable values are: • **Generic** - Normal line • **BroadSoft SCA** - Shared Call/Line Appearances (SCA) line for BroadWorks network (call activity can go to more than one phone) • **BLA** - Bridged Line Appearance (BLA) line.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	Valid values are: 0 - Generic 1 - BroadSoft SCA 2 - (reserved) 3 - BLA
EXAMPLE	sip mode: 2

CALL WAITING SETTINGS

PARAMETER – *call waiting*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to enable or disable Call Waiting on the IP phone. If you enable call waiting (default), the user has the option of accepting a second call while currently on the first call. If you disable call waiting, and a user is currently on a call, a second incoming call is automatically rejected by the phone with a busy message. If you disable call waiting on the phone, and the user is on a call, any further incoming calls will receive busy unless “Call Forward Busy” or “Call Forward No Answer and Busy” is configured on the phone. It will then forward the call according to the rule configured. The phone can only: • transfer the currently active call or • accept transferred calls if there is no active calls. If call waiting is disabled: • intercom calls are treated as regular incoming calls and are rejected. • pre-dialing with live dial pad disabled still accepts incoming calls. • the Missed Calls List does not get updated with details of calls. • the Blind Transfer feature on the phone may not work if two calls are made to the phone at one time.
FORMAT	Boolean
DEFAULT VALUE	1 (enabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	call waiting: 0

PARAMETER – call waiting tone	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enable or disables the playing of a call waiting tone when a caller is on an active call and a new call comes into the phone. **Note:** The Call Waiting Tone feature works only if the Call Waiting parameter is enabled.
FORMAT	Boolean
DEFAULT VALUE	1 (enabled)
RANGE	0 (disable) 1 (enabled)
EXAMPLE	call waiting tone: 0

PARAMETER – *call waiting tone period*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the time period, in seconds, that the call waiting tone is audible on an active call when another call comes in. When enabled, the call waiting tone plays at regular intervals for the amount of time set for this parameter. For example, if set to “30” the call waiting tone plays every 30 seconds. When set to “0”, the call waiting tone is audible only once on the active call.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0-4294967295
EXAMPLE	call waiting tone period: 30

SIP GLOBAL NETWORK SETTINGS

PARAMETER – *sip proxy ip*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The IP address of the SIP proxy server for which the IP phone uses to send all SIP requests. A SIP proxy is a server that initiates and forwards requests generated by the IP phone to the targeted user.
FORMAT	IP address or fully qualified Domain Name
DEFAULT VALUE	0.0.0.0
RANGE	Not applicable
EXAMPLE	sip proxy ip: 192.168.0.101

PARAMETER – *sip proxy port*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The proxy server's port number.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	N/A
EXAMPLE	sip proxy port: 5060

PARAMETER – *sip backup proxy ip*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The IP address of the backup SIP proxy server for which the IP phone uses when the primary SIP proxy is unavailable.
FORMAT	IP address or fully qualified Domain Name
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	sip backup proxy ip: 192.168.0.102

PARAMETER – *sip backup proxy port*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The backup proxy's port number.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	N/A
EXAMPLE	sip backup proxy port: 5060

PARAMETER – *sip outbound proxy*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This is the address of the outbound proxy server. All SIP messages originating from the phone are sent to this server. For example, if you have a Session Border Controller in your network, then you would normally set its address here.
FORMAT	IP Address or fully qualified Domain Name
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	sip outbound proxy: 10.42.23.13

PARAMETER – *sip outbound proxy port*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The proxy port on the proxy server to which the IP phone sends all SIP messages.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	N/A
EXAMPLE	sip outbound proxy port: 5060

PARAMETER – *sip registrar ip*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The address of the registrar for which the IP phone uses to send *REGISTER* requests. A SIP registrar is a server that maintains the location information of the IP phone. A global value of 0.0.0.0 disables registration. However, the phone is still active and you can dial using username@ip address of the phone. If the Registrar IP address is set to 0.0.0.0 for a per-line basis (i.e, line 1, line 2, etc.), then the register request is not sent, the "No Service" message does not display, and the message waiting indicator (MWI) does not come on.
FORMAT	IP address or fully qualified Domain Name
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	sip registrar ip: 192.168.0.101

PARAMETER – *sip registrar port*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The registrar's port number.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	N/A
EXAMPLE	sip registrar port: 5060

PARAMETER – *sip backup registrar ip*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The address of the backup registrar (typically, the backup SIP proxy) for which the IP phone uses to send *REGISTER* requests if the primary registrar is unavailable. A global value of 0.0.0.0 disables backup registration. However, the phone is still active and you can dial using username@ip address of the phone. If the backup registrar IP address is set to 0.0.0.0 for a per-line basis (i.e, line 1, line 2, etc.), then the backup register request is not sent, the "No Service" message does not display, and the message waiting indicator (MWI) does not come on.
FORMAT	IP address or fully qualified Domain Name
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	sip backup registrar ip: 192.168.0.102

PARAMETER – *sip backup registrar port*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The backup registrar's (typically the backup SIP proxy) port number.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	N/A
EXAMPLE	sip backup registrar port: 5060

PARAMETER – *sip registration period*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The requested registration period, in seconds, from the registrar.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 - 2147483647
EXAMPLE	sip registration period: 3600

BACKUP OUTBOUND PROXY (GLOBAL SETTINGS)

PARAMETER – *sip backup outbound proxy*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The IP address or domain name of the backup outbound SIP proxy server for which the IP phone uses when the primary SIP proxy is unavailable. Use this parameter to configure the sip backup outbound proxy on a global basis.
FORMAT	IP address or fully qualified Domain Name
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	sip backup outbound proxy: drax.us.mitel.com

PARAMETER – *sip backup outbound proxy port*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The backup outbound proxy port on the backup outbound proxy server to which the IP phone sends all SIP messages. Use this parameter to configure the sip backup outbound proxy port on a global basis.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 - 65535
EXAMPLE	sip backup outbound proxy port: 5060

SIP BASIC, PER-LINE SETTINGS

The following parameters are SIP per-line settings. The value of "*N*" is 1 - 24 or 1-2 depending on your model phone.

SIP PER-LINE AUTHENTICATION SETTINGS

PARAMETER – *sip lineN screen name* (where N = line number)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Used to display text on the screen of the phone. You may want to set this parameter to display the phone user's name.
FORMAT	Text
DEFAULT VALUE	N/A
RANGE	Up to 20 alphanumeric characters
EXAMPLE	sip line1 screen name: Joe Smith

PARAMETER – *sip lineN screen name 2* (where N = line number)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Used to display text on a second line on the screen of the phone. **Notes:** • If other status messages display on the phone, such as “Network Disconnected”, the Screen Name 2 value does not display. • Characters are allowed (such as “#”). • If the text is longer than the display width, than the display truncates the text to fit the display.
FORMAT	Alphanumeric characters
DEFAULT VALUE	N/A
RANGE	Up to 20 alphanumeric characters
EXAMPLE	sip line1 screen name 2: Lab Phone

PARAMETER – *sip lineN user name* (where N = line number)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Used in the name field of the *SIP URI* for the IP phone and for registering the IP phone at the registrar. When configuring per-line BLA on an ININ server, the username must be incremented as shown in the example for the "sip lineN bla number" parameter on page A-101. **Note:** The IP Phones support Usernames containing dots (“.”).
FORMAT	Text
DEFAULT VALUE	N/A
RANGE	Up to 20 alphanumeric characters
EXAMPLE	sip line1 user name: 1010

PARAMETER – *sip lineN display name* (where N = line number)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Used in the display name field of the *From* SIP header field. Some IP PBX systems use this as the caller’s ID and some may overwrite this with the string that is set at the PBX system.
FORMAT	Text
DEFAULT VALUE	N/A
RANGE	Up to 20 alphanumeric characters
EXAMPLE	sip line1 display name: Joe Smith

PARAMETER – *sip lineN auth name* (where N = line number)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Used in the username field of the Authorization header field of the *SIP REGISTER* request.
FORMAT	Text
DEFAULT VALUE	N/A
RANGE	Up to 20 alphanumeric characters
EXAMPLE	sip line1 auth name: 5553456

PARAMETER – *sip lineN password* (where N = line number)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The password that will be used to register at the registrar.
FORMAT	Text
DEFAULT VALUE	N/A
RANGE	Up to 20 alphanumeric characters
EXAMPLE	sip line1 password: 12345

PARAMETER – sip lineN bla number (where N = line number)	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to assign a phone number that is shared on specific lines on the IP phone. For Sylantro Server: When configuring the BLA feature on a Sylantro server, the value set for the **sip lineN bla number** parameter shall be the same value set for the **sip lineN user name** parameter for all the phones in the group. For example, if sip lineN user name is 1010, you would configure BLA on a per-line basis for the Sylantro server as follows: sip line1 user name: 1010 (# for all the phones) sip line1 bla number: 1010 For ININ Server: When configuring the BLA feature on an ININ server, the value set for the **sip lineN bla number** parameter shall be the same value set for the **sip lineN user name** parameter without the incremented digit added to the phone #. For example, if the sip lineN user name for the first phone is 10101, and the sip lineN user name for the second phone is 10102, etc. you would configure BLA on a per-line basis for the ININ server as follows: sip line1 user name: 10101 (# for phone 1 with) sip line1 bla number: 1010 (appearance of phone 3) sip line1 user name: 10102(# for phone 2 with) sip line1 bla number: 1010 (appearance of phone 3) sip line1 user name: 1010(# for phone 3) sip line1 bla number: 1010 **Note:** The original phone number which has the bridged line appearance on other phones, will have the "sip lineN user name" parameter the same as the "sip lineN bla number" (1010 in the above example on Phone 3).
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	Sylantro Server: sip line1 bla number: 1010 ININ Server: sip line 1 bla number: 1010

PARAMETER – *sip lineN mode* (where N = line number)	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to configure the mode of the line. Applicable values are: • **Generic** - Normal line • **BroadSoft SCA** - Shared Call/Line Appearances (SCA) line for BroadWorks network (call activity can go to more than one phone) • **BLA** - Bridged Line Appearance (BLA) line.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	Valid values are: 0 - Generic 1 - BroadSoft SCA 2 - (Reserved) 3 - BLA
EXAMPLE	sip line1 mode: 2

HASH PASSWORD SETTING FOR SIP AUTHENTICATION

PARAMETER – *sip lineN hash*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Password supported for SIP authentication in hashed format
FORMAT	Text
DEFAULT VALUE	N/A
RANGE	Alphanumeric characters
EXAMPLE	sip lineN hash: *************

SIP PER-LINE CALL WAITING SETTING

PARAMETER – *sip lineN call waiting* (where N = line number)	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to enable or disable Call Waiting on the IP phone on a per line basis. If you enable call waiting (default), the user has the option of accepting a second call while currently on the first call. If you disable call waiting, and a user is currently on a call, a second incoming call is automatically rejected by the phone with a busy message. If you disable call waiting on the phone, and the user is on a call, any further incoming calls will receive busy unless "Call Forward Busy" or "Call Forward No Answer and Busy" is configured on the phone. It will then forward the call according to the rule configured. The phone can only: • transfer the currently active call or • accept transferred calls if there is no active calls. If call waiting is disabled: • intercom calls are treated as regular incoming calls and are rejected. • pre-dialing with live dial pad disabled still accepts incoming calls. • the Missed Calls List does not get updated with details of calls. • the Blind Transfer feature on the phone may not work if two calls are made to the phone at one time.
FORMAT	Boolean
DEFAULT VALUE	Global
RANGE	Global 0 (disabled) 1 (enabled)
EXAMPLE	sip line1 call waiting: 0 sip line2 call waiting: 1 sip line3 call waiting: 0

SIP PER-LINE NETWORK SETTINGS

PARAMETER – *sip lineN proxy ip* (where N = line number)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The IP address of the SIP proxy server for which the IP phone uses to send all SIP requests. A SIP proxy is a server that initiates and forwards requests generated by the IP phone to the targeted user.
FORMAT	IP address or fully qualified Domain Name
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	sip line1 proxy ip: 192.168.0.101

PARAMETER – *sip lineN proxy port* (where N = line number)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The proxy server's port number
FORMAT	Integer
DEFAULT VALUE	0
RANGE	N/A
EXAMPLE	sip line1 proxy port: 5060

PARAMETER – *sip lineN backup proxy ip* (where N = line number)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The IP address of the backup SIP proxy server for which the IP phone uses when the primary SIP proxy is unavailable.
FORMAT	IP address or fully qualified Domain Name
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	sip line1 backup proxy ip: 192.168.0.102

PARAMETER – *sip lineN backup proxy port* (where N = line number)	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The backup proxy's port number.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	N/A
EXAMPLE	sip line1 backup proxy port: 5060

PARAMETER – *sip lineN outbound proxy* (where N = line number)	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This is the address of the outbound proxy server. All SIP messages originating from the phone are sent to this server. For example, if you have a Session Border Controller in your network, then you would normally set its address here.
FORMAT	IP Address or fully qualified Domain Name
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	sip line1 outbound proxy: 10.42.23.13

PARAMETER – *sip lineN outbound proxy port* (where N = line number)	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The proxy port on the proxy server to which the IP phone sends all SIP messages.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	N/A
EXAMPLE	sip line1 outbound proxy port: 5060

PARAMETER – *sip lineN registrar ip* (where N = line number)	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The address of the registrar for which the IP phone uses to send *REGISTER* requests. A SIP registrar is a server that maintains the location information of the IP phone. A global value of 0.0.0.0 disables registration. However, the phone is still active and you can dial using username@ip address of the phone. If the Registrar IP address is set to 0.0.0.0 for a per-line basis (i.e, line 1, line 2, etc.), then the register request is not sent, the "No Service" message does not display, and the message waiting indicator (MWI) does not come on.
FORMAT	IP address or fully qualified Domain Name
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	sip line1 registrar ip: 192.168.0.101

PARAMETER – *sip lineN registrar port* (where N = line number)	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The registrar's port number
FORMAT	Integer
DEFAULT VALUE	0
RANGE	N/A
EXAMPLE	sip line1 registrar port: 5060

PARAMETER – *sip lineN backup registrar ip* (where N = line number)	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The address of the backup registrar (typically, the backup SIP proxy) for which the IP phone uses to send *REGISTER* requests if the primary registrar is unavailable. A global value of 0.0.0.0 disables backup registration. However, the phone is still active and you can dial using username@ip address of the phone. If the backup registrar IP address is set to 0.0.0.0 for a per-line basis (i.e, line 1, line 2, etc.), then the backup register request is not sent, the "No Service" message does not display, and the message waiting indicator (MWI) does not come on.
FORMAT	IP address or fully qualified Domain Name
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	sip line1 backup registrar ip: 192.168.0.102

PARAMETER – *sip lineN backup registrar port* (where N = line number)	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The backup registrar's (typically the backup SIP proxy) port number.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	N/A
EXAMPLE	sip line1 backup registrar port: 5060

PARAMETER – *sip lineN registration period* (where N = line number)	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The requested registration period, in seconds, from the registrar.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 to 2147483647
EXAMPLE	sip line1 registration period: 3600

BACKUP OUTBOUND PROXY (PER-LINE SETTINGS)

PARAMETER – *sip lineN backup outbound proxy* (where N = line number)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The IP address or domain name of the backup outbound SIP proxy server for which the IP phone uses when the primary SIP proxy is unavailable. Use this parameter to configure the sip backup outbound proxy on a per-line basis.
FORMAT	IP address or fully qualified Domain Name
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	sip line1 backup outbound proxy: drax.us.mitel.com

PARAMETER – *sip lineN backup outbound proxy port* (where N = line number)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The backup outbound proxy port on the backup outbound proxy server to which the IP phone sends all SIP messages. Use this parameter to configure the sip backup outbound proxy port on a per-line basis.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 - 65535
EXAMPLE	sip line1 backup outbound proxy port: 5060

BLA SUPPORT FOR MWI

PARAMETER – *sip mwi for bla account*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables a BLA configured line to send an MWI SUBSCRIBE message for the BLA account. **Notes:** • If you change the setting on this parameter, you must reboot the phone for it to take affect. • Both the “sip explicit mwi subscription” and “sip mwi for bla account” parameters must be enabled in order for the MWI subscription for BLA to occur. • The MWI re-subscription for the BLA account uses the value set for the "sip explicit mwi subscription period" parameter to re-subscribe. • Whether or not the "sip mwi for bla account" parameter is enabled, the priority for displaying MWI does not change.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sip mwi for bla account: 1

SHARED CALL APPEARANCE (SCA) CALL BRIDGING

GLOBAL SETTING

PARAMETER – *sip sca bridging*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables/disables SCA bridging on the phone-side on a global basis. **Note:** You must restart the phone after setting a value for this parameter.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sip sca bridging: 1

PER-LINE SETTING

PARAMETER – *sip lineN sca bridging* (where N = line number)	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables/disables SCA bridging on the phone-side on a per-account basis using a specific SCA-configured line. **Note:** You must restart the phone after setting a value for this parameter.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sip line1 sca bridging: 1

CENTRALIZED CONFERENCING SETTINGS

GLOBAL SETTING

PARAMETER – *sip centralized conf*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg

DESCRIPTION	Globally enables or disables SIP centralized conferencing for an IP phone as follows:
	• To disable centralized conferencing, leave this field empty (blank).
	• To enable SIP centralized conferencing, then do one of the following actions:
	  • If you have specified a proxy server/registrar server, then to reach the media server via the proxy server, set this field to one of the following:
	
	conf (Sylantro server), or
	Conference (BroadSoft server)
	
	By setting this field to **conf**, you specify conf@<proxy_server _address>: <proxy_port>. For example, if the proxy server address is 206.229.26.60 and the proxy port used is 10060, then by setting this parameter to **conf**, you are specifying the following: conf@206.229.26.60:10060
	  • To reach the media server using a different address/port than that specified by the proxy, set this field to the following:
	
	conf@<media_server _address>: <media_port>

FORMAT	String
DEFAULT VALUE	Blank
RANGE	N/A
EXAMPLE	sip centralized conf: conf

PER-LINE SETTING

PARAMETER – *sip lineN centralized conf* (where N = line number)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg

DESCRIPTION	Enable or disable per-line SIP centralized conferencing for an IP phone as follows:
	• To disable centralized conferencing, leave this field empty (blank).
	• To enable SIP centralized conferencing, then do one of the following actions:
	  • If you have specified a proxy server/registrar server, then to reach the media server via the proxy server, set this field to one of the following:
	
	conf (Sylantro server), or
	Conference (BroadSoft server)
	
	By setting this field to **conf**, you specify conf@<proxy_server _address>: <proxy_port>. For example, if the proxy server address is 206.229.26.60 and the proxy port used is 10060, then by setting this parameter to **conf**, you are specifying the following: conf@206.229.26.60:10060
	  • To reach the media server using a different address/port than that specified by the proxy, set this field to the following:
	
	conf@<media_server _address>: <media_port>

FORMAT	String
DEFAULT VALUE	Blank
RANGE	N/A
EXAMPLE	sip line3 centralized conf: conf

CUSTOM AD-HOC CONFERENCE

PARAMETER – *custom adhoc conference*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables/disables the phone to interoperate with Genband Call Manager for ad-hoc conference.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	custom adhoc conference: 1

SIP JOIN FEATURE FOR 3-WAY CONFERENCE

PARAMETER – *sip join support*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the phone to allow a conference to be set up with a join header as described in RFC 3911.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sip join support: 1

CONFERENCE/TRANSFER IN LIVE DIAL MODE

PARAMETER – *confxfer live dial*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables/disables support for live dial mode when initiating a conference call or transfer.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	**0** - Pre-dial mode: When a user initiates a conference call or transfer, they do not hear a dial tone before dialing begins. The phone does not automatically dial out the number until the user presses the “Conf” or “Xfer” key. **1** - Live dial mode with dial plan matching: When a user initiates a conference call or transfer, they hear a dial tone before dialing begins. The phone automatically dials out if the number matches the local dial plan or if it reaches the set digit timeout. **2** - Live dial mode without dial plan matching: When a user initiates a conference call or transfer, they hear a dial tone before dialing begins. The phone does not match the number to the local dial plan and automatically dials out only if it reaches the set digit timeout (or if the number matches a number defined in the emergency dial plan).
EXAMPLE	confxfer live dial: 2

HTTP/HTTPS AUTHENTICATION SUPPORT FOR BROADSOFT CMS

PARAMETER – *http digest username*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the username to use for HTTP/HTTPS digest authentication. The server uses this username for authentication purposes when loading configuration to the phone over HTTP/HTTPS. This parameter initiates a “Username/Password” screen after pressing the **Log In** softkey. **Notes:** • The Username field accepts special characters, such as, @, #, %, =, _, etc. You can also specify domain names (i.e. user@domain). • You must reboot the phone after setting the HTTP/HTTPS digest authentication parameters.
FORMAT	String
DEFAULT VALUE	aastra
RANGE	Up to 40 alphanumeric characters
EXAMPLE	http digest username: myusername

PARAMETER – *http digest password*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the password to use for HTTP/HTTPS digest authentication. The server uses this password for authentication purposes when loading configuration to the phone over HTTP/HTTPS. This parameter initiates a "Username/Password" screen after pressing the **Log In** softkey. **Notes:** • The Password field accepts special characters, such as, @, #, %, =, _, etc. • You must reboot the phone after setting the HTTP/HTTPS digest authentication parameters.
FORMAT	String
DEFAULT VALUE	aastra
RANGE	Up to 20 alphanumeric characters
EXAMPLE	http digest password: mypassword

PARAMETER – *http digest force login*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables and disables the display of a LOGIN key on the phone's idle screen. **Note:** After the server has authenticated the phone, this parameter must be set to "**0**" in order for the server to send the default profile to the phone.
FORMAT	Boolean
DEFAULT VALUE	0 (disable)
RANGE	0 (disable) 1 (enable)
EXAMPLE	http digest force login: 1

PARAMETER – *http digest domain enable*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables and disables the domain checkbox for authentication based on either username and password only or with username, password and domain.
FORMAT	Boolean
DEFAULT VALUE	0 (disable)

RANGE	0 (disable) - authentication based on Username and Password. 1 (enable) - authentication based on Username, Password and Domain
EXAMPLE	http digest domain enable: 1

PARAMETER – *http digest domain*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the domain for HTTP/HTTPS digest authentication.
FORMAT	String
DEFAULT VALUE	Blank
RANGE	N/A
EXAMPLE	http digest domain: @8280001.com

PERSONAL MODE SETTINGS

Note: The parameter "**personal mode**" is applicable to the 6970 IP Phone only.

PARAMETER – *personal mode*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to disable the Hotdesk Logout Pop-up, which prompts the user to log out or stay logged in after the call ends.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	**0** (disabled) **1** (enabled)
EXAMPLE	personal mode: 0

ADVANCED SIP SETTINGS

PARAMETER – *sip explicit mwi subscription*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	If the IP phone has a message waiting subscription with the Service Provider, a Message Waiting Indicator (MWI) (LED or display icon) tells the user there is a message on the IP Phone. You can enable and disable MWI by setting this parameter to the following: "**0**" to disable "**1**" to enable
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (disable) 1 (enable)
EXAMPLE	sip explicit mwi subscription: 1

PARAMETER – *sip explicit mwi subscription period*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The requested duration, in seconds, before the MWI subscription times out. The phone re-subscribes to MWI before the subscription period ends.
FORMAT	Integer
DEFAULT VALUE	86400
RANGE	30 - 2147483647
EXAMPLE	sip explicit mwi subscription period: 30

PARAMETER – *sip send mac*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Adds an "Aastra-Mac:" header to the SIP REGISTER messages sent from the phone to the call server, where the value is the MAC address of the phone.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sip send mac: 1

PARAMETER – *sip send line*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Adds an "Aastra-Line:" header to the SIP REGISTER messages sent from the phone to the call server, where the value is the line number that is being registered.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sip send line: 1

PARAMETER – *sip session timer*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The time, in seconds, that the IP phone uses to send periodic re-*INVITE* requests to keep a session alive. The proxy uses these re-*INVITE* requests to maintain the status' of the connected sessions. See RFC4028 for details. The minimum session timer is 90.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0, 90 +
EXAMPLE	sip session timer: 90

PARAMETER – *sip T1 timer*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This timer is a SIP transaction layer timer defined in RFC 3261. Timer 1 is an estimate, in milliseconds, of the round-trip time (RTT).
FORMAT	Integer
DEFAULT VALUE	500
RANGE	N/A
EXAMPLE	sip T1 timer: 600

PARAMETER – *sip T2 timer*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
Description	This timer is a SIP transaction layer timer defined in RFC 3261. Timer 2 represents the amount of time, in milliseconds, a non-INVITE server transaction takes to respond to a request.
FORMAT	Integer
Default Value	0
Range	N/A
Example	sip T2 timer: 8

PARAMETER – *sip transaction timer*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The amount of time, in milliseconds that the phone allows the callserver (registrar/proxy) to respond to SIP messages that it sends. If the phone does not receive a response in the amount of time designated for this parameter, the phone assumes the message has timed out.
FORMAT	Integer
DEFAULT VALUE	4000
RANGE	4000 to 64000
EXAMPLE	sip transaction timer: 6000

PARAMETER – *sip transport protocol*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The protocol that the IP phone uses to send out SIP messages. **Notes:** • If you set the value of this parameter to 4 (TLS), the phone checks to see if the "**sips persistent tls**" is enabled. If it is enabled, the phone uses Persistent TLS on the connection. If "**sips persistent tls**" is disabled, then the phone uses TLS on the connection. If TLS is used, you must specify the Root and Intermediate Certificates, the Local Certificate, the Private Key, and the Trusted Certificates. • If the phone uses Persistent TLS, you MUST specify the Trusted Certificates; the Root and Intermediate Certificates, the Local Certificate, and the Private Key are optional. • This parameter implies keep-alive mechanism. For more information about Persistent TLS, see "Transport Layer Security (TLS) Settings" on page A-124.
FORMAT	Integer
DEFAULT VALUE	1 (UDP)
RANGE	Valid values are: 0 - User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) 1 - UDP 2 - TCP 4 - Transport Layer Security (TLS)
EXAMPLE	sip transport protocol: 4

PARAMETER – *sip registration retry timer*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the time, in seconds, that the phone waits between registration attempts when a registration is rejected by the registrar.
FORMAT	Integer
Default Value	1800 (30 minutes)
Range	30-1800
Example	sip registration retry timer: 30

PARAMETER – *sip registration timeout retry timer*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the length of time, in seconds, that the phone waits until it re-attempts to register after a REGISTER message times out. If this parameter is set lower than 30 seconds, the phone uses a minimum timer of 30 seconds.
FORMAT	Integer
DEFAULT VALUE	120
RANGE	30 - 2147483647
EXAMPLE	sip registration timeout retry timer: 150

PARAMETER – *sip registration renewal timer*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The threshold value, in seconds, prior to expiration, that the phone renews registrations. The phone will automatically send registration renewals half-way through the registration period, unless half-way is more than the threshold value. For example, if the threshold value is set to 60 seconds and if the registration period is 600 seconds, the renewal REGISTER message will be sent 60 seconds prior to the expiration, as half-way (600/2) > 60. If the registration period was 100 seconds, then the renewal would be sent at the half-way point as (100/2) < 60.
FORMAT	Integer
DEFAULT VALUE	15
RANGE	0 - 2147483647 **Note:** The value set for this parameter should be between 0 and the value set for the registration period.
EXAMPLE	sip registration renewal timer: 10

PARAMETER – *sip subscription timeout retry timer*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Applicable for all event packages, this parameter controls how long the phone delays then retries a subscription when a SUBSCRIBE request is responded with a 408 (timeout) or 503 (service unavailable) error code. **Note:** If set to 0 or an invalid value is set, the parameter will not take effect.
FORMAT	Seconds
DEFAULT VALUE	0
RANGE	1-3600
EXAMPLE	sip subscription timeout retry timer: 60

PARAMETER – *sip subscription failed retry timer*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Applicable for all event packages, this parameter controls how long the phone delays then retries a subscription when a SUBSCRIBE request is responded with error codes other than 408 (timeout) or 503 (service unavailable). **Note:** If set to 0 or an invalid value is set, the parameter will not take effect.
FORMAT	Seconds
DEFAULT VALUE	0
RANGE	1-3600
EXAMPLE	sip subscription failed retry timer: 30

PARAMETER – *sip blf subscription period*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The requested duration, in seconds, before the BLF subscription times out. The 6865i, 6867i, 6869i, and 6873i IP phones re-subscribe to the BLF subscription service before the defined subscription period ends. **Note:** This parameter is not applicable to BLF/List subscriptions.
FORMAT	Integer
DEFAULT VALUE	3600
RANGE	120 - 2147483647
EXAMPLE	sip blf subscription period: 2000

PARAMETER – *sip acd subscription period*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the time period, in seconds, that the IP phone re-subscribes the Automatic Call Distribution (ACD) subscription service after a software/firmware upgrade or after a reboot of the 6865i, 6867i, 6869i, and 6873i IP phone.
FORMAT	Integer
DEFAULT VALUE	3600
RANGE	120 - 2147483647
EXAMPLE	sip acd subscription period: 2000

PARAMETER – *sip bla subscription period*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the amount of time, in seconds, that the phone waits to receive a BLA subscribe message from the server. If you specify zero (0), the phone uses the value specified for the BLA expiration in the subscribe message received from the server. If no value is specified, the phone uses the default value of 300 seconds.
FORMAT	Integer
DEFAULT VALUE	300
RANGE	0-3700 **Note:** When set to zero (0), the phone uses BLA expiry value specified in subscribe message.
EXAMPLE	sip bla subscription period: 0

PARAMETER – *sip ignore refer event id*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not event IDs (i.e. Event: refer:id=xxxxx) in REFER NOTIFY event headers received by the phone should be ignored.
FORMAT	Boolean
DEFAULT VALUE	0 (Disabled)
RANGE	0 (Disabled - Check for valid event ID) 1 (Enabled - Ignore event ID)
EXAMPLE	sip ignore refer event id: 1

AS-FEATURE-EVENT SUBSCRIPTION SETTINGS

PARAMETER – *sip lineN as-feature-event subscription* (where N = line number)	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the specified line with the BroadSoft's server-side DND, CFWD, or ACD features.
FORMAT	Boolean
DEFAULT VALUE	0 (disable)
RANGE	0 (disable) 1 (enable)
EXAMPLE	sip line1 as-feature-event subscription: 1

PARAMETER – *sip as-feature-event subscription period*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the amount of time, in seconds, between re-subscribing. If the phone does not re-subscribe in the time specified for this parameter, it loses subscription.
FORMAT	Integer
DEFAULT VALUE	3600
RANGE	5 - 2147483647
EXAMPLE	sip as-feature-event subscription period: 600

TRANSPORT LAYER SECURITY (TLS) SETTINGS

To configure TLS, you must enter the "**sip transport protocol**" parameter with a value of "**4**" (TLS). See the "sip transport protocol" description on page A-119.

Also enter the following parameters in the configuration files to configure TLS:

PARAMETER – *sips persistent tls*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the use of Persistent Transport Layer Security (TLS). Persistent TLS sets up the connection to the server once and re-uses that connection for all calls from the phone. The setup connection for Persistent TLS is established during the registration of the phone. If the phones are set to use Persistent TLS, and a call is made from the phone, this call and all subsequent calls use the same authenticated connection. This significantly reduces the delay time when placing a call. **Notes:** • There can be only one persistent TLS connection created per phone. • If you configure the phone to use Persistent TLS, you must also specify the **Trusted Certificate** file to use. The Root and Intermediate Certificates, Local Certificate, and Private Key files are optional.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sips persistent tls: 1

PARAMETER – *sip persistent tls keep alive*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
Description	When enabled, the configured value indicates frequency (in seconds) that phone will send the keep alive messages.
FORMAT	Integer
Default Value	0
Range	0 (Disabled) 15-3600 **Note**: The real time interval will vary between 80% and 100% of the configured value.
Example	sip persistent tls keep alive: 60

PARAMETER – *sip send sips over tls*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows administrators the ability to manually configure the IP phones to use either the SIP or SIPS URI scheme when TLS or persistent TLS is enabled
FORMAT	Integer
DEFAULT VALUE	1 (Enabled)
RANGE	0-1 0 (Disabled - Use SIP URI scheme) 1 (Enabled - Use SIPS URI scheme)
EXAMPLE	sip send sips over tls: 0

PARAMETER – *sips root and intermediate certificates*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to specify the SIP Root and Intermediate Certificate files to use when the phone uses the TLS transport protocol to setup a call. The Root and Intermediate Certificate files contain one root certificate and zero or more intermediate certificates which must be placed in order of certificate signing with root certificate being the first in the file. If the local certificate is signed by some well known certificate authority, then that authority provides the user with the Root and Intermediate Certificate files (most likely just CA root certificate). This parameter is required when configuring TLS (optional for Persistent TLS.) You can use this parameter in three ways: • To download no certificates • To download a certificate from the original configuration server • To download a certificate from another specified server To download a specific file, the string value MUST HAVE A FILENAME at the end of the string. For example: sips root and intermediate certificates: ftp://admin:admin!@1.2.3.4:50/path/phonesRootCert.pem where “path” is the directory and “phonesRootCert.pem” is the filename. If you do not specify a filename, the download fails. See examples for each below. **Note:** The certificate files must use the format “.pem”. To create custom certificate files to use on your IP phone, contact Mitel Technical Support.
FORMAT	<filename>.pem
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	The following example downloads no root and intermediate certificate file: sips root and intermediate certificates: The following example downloads the root and intermediate certificate file from the original configuration server. sips root and intermediate certificates: phonesRootCert.pem The following example uses FTP to download the firmware file “phonesRootCert.pem” (root and intermediate certificate file) from the “path” directory on server 1.2.3.4 using port 50. sips root and intermediate certificates: ftp://admin:admin!@1.2.3.4:50/path/phonesRootCert.pem

PARAMETER – *sips local certificate*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to specify the Local Certificate file to use when the phone uses the TLS transport protocol to setup a call. This parameter is required when configuring TLS (optional for Persistent TLS.) You can use this parameter in three ways: • To download no certificates • To download a certificate from the original configuration server • To download a certificate from another specified server To download a specific file, the string value MUST HAVE A FILENAME at the end of the string. For example: sips local certificate:ftp://admin:admin!@1.2.3.4:50/path/phonesLocalCert.pem where “path” is the directory and “phonesLocalCert.pem” is the filename. If you do not specify a filename, the download fails. See examples for each below. **Note:** The certificate file must use the format “.pem”. To create specific certificate files to use on your IP phone, contact Mitel Technical Support.
FORMAT	<filename>.pem
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	The following example downloads no local certificate file: sips local certificate: The following example downloads the local certificate file from the original configuration server. sips local certificate: phonesLocalCert.pem The following example uses FTP to download the firmware file “phonesLocalCert.pem” (local certificate file) from the “path” directory on server 1.2.3.4 using port 50: sips local certificate: ftp://admin:admin!@1.2.3.4:50/path/phonesLocalCert.pem

PARAMETER – *sips private key*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to specify a Private Key file to use when the phone uses the TLS transport protocol to setup a call. This parameter is required when configuring TLS (optional for Persistent TLS.) You can use this parameter in three ways: • To download no private key • To download a private key from the original configuration server • To download a private key from another specified server To download a specific file, the string value MUST HAVE A FILENAME at the end of the string. For example: sips private key: ftp://admin:admin!@1.2.3.4:50/path/phonesPrivatekey.pem where “path” is the directory and “phonesPrivateKey.pem” is the filename. If you do not specify a filename, the download fails. See examples for each below. **Note:** The key file must use the format “.pem”. To create specific private key files to use on your IP phone, contact Mitel Technical Support.
FORMAT	<filename>.pem
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	The following example downloads no private key file: sips private key: The following example downloads the private key file from the original configuration server. sips private key: phonesPrivateKey.pem The following example uses FTP to download the firmware file “phonesPrivateKey.pem” (private key file) from the “path” directory on server 1.2.3.4 using port 50: sips private key: ftp://admin:admin!@1.2.3.4:50/path/phonesPrivateKey.pem

PARAMETER – *sips trusted certificates*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to specify the Trusted Certificate files to use when the phone uses the TLS transport protocol to setup a call. The Trusted Certificate files define a list of trusted certificates. The phone's trusted list must contain the CA root certificates for all the servers it is connecting to. For example, if the phone is connecting to server A which has a certificate signed by CA1, and server B that has a certificate signed by CA2, the phone must have CA1 root certificate and CA2 root certificate in its Trusted Certificate file. This parameter is required when configuring TLS or Persistent TLS. You can use this parameter in three ways: • To download no certificates • To download a certificate from the original configuration server • To download a certificate from another specified server To download a specific file, the string value MUST HAVE A FILENAME at the end of the string. For example: sips trusted certificates: ftp://admin:admin!@1.2.3.4:50/path/phonesTrustedCert.pem where "path" is the directory and "phonesTrustedCert.pem" is the filename. If you do not specify a filename, the download fails. See examples for each below. **Note:** The certificate files must use the format ".pem". To create custom certificate files to use on your IP phone, contact Mitel Technical Support.
FORMAT	<file name>.pem
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	The following example downloads no trusted certificate file: sips trusted certificates: The following example downloads the trusted certificate file from the original configuration server. sips trusted certificates: phonesTrustedCert.pem The following example uses FTP to download the firmware file "phonesTrustedCert.pem" (trusted certificate file) from the "path" directory on server 1.2.3.4 using port 50: sips trusted certificates: ftp://admin:admin!@1.2.3.4:50/path/phonesTrustedCert.pem

PARAMETER – *sips strict cert cn validation*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	If enabled, specifies that the phone validates CNs from the server certificates by comparing them with the configured SIP peer name. If disabled, specifies that the phone validates the CNs by wildcard comparison.

FORMAT	Boolean
DEFAULT VALUE	1 (Enabled)
RANGE	0-1 0 (Disabled - Wildcards Allowed) 1 (Enabled - Identical Matching)
EXAMPLE	sips strict cert cn validation: 0

802.1X SUPPORT SETTINGS

Use the following parameters to configure the 802.1x Protocol on your phone using the configuration files.

For EAP-MD5 use:

- eap type
- identity
- md5 password
- pc port passthrough enabled

For EAP-TLS use:

- eap type
- identity
- 802.1x root and intermediate certificates
  (use 1 root and 0 or more intermediate certificates)
- 802.1x local certificate
  (use 1 local certificate)

Notes:

1. The 802.1x local certificate configuration file must have only one client certificate for the phone.

2. If a certificate bundle or multiple certificates are found in the configuration file, the first certificate from the bundle is read and loaded to the phone.

- 802.1x private key
  (1 private key that corresponds to local certificate)
- 802.1x trusted certificates
  (0 or more trusted certificates)
- 802.1x mutual authentication
  (Enables or disables mutual authentication for EAP-TLS for 802.1x setup)
- pc port passthrough enabled

PARAMETER – *pc port passthru enabled*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the PC port.
FORMAT	Integer
DEFAULT VALUE	1 (enable)
RANGE	0 (disable) 1 (enable)
EXAMPLE	pc port passthru enabled: 1

PARAMETER – *eap type*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the type of authentication to use on the IP Phone.
FORMAT	Integer
DEFAULT VALUE	0 (disable)
RANGE	0 (disable) 1 (MD5) 2 (TLS)
EXAMPLE	eap type: 1

PARAMETER – *identity*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the identity or username used for authenticating the phone. **Note:** The value you enter for this parameter also displays in the Mitel Web UI at the path ->802.1x Support->General->Identity.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	identity: phone1

PARAMETER – *md5 password*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the password used for the MD5 authentication of the phone. **Note:** The value you enter for this parameter also displays in the Mitel Web UI at the path Advanced Settings-> 802.1x Support->EAP-MD5 Settings->MD5 Password. The password displays as “*******”.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	md5 password: password1

PARAMETER – *802.1x root and intermediate certificates*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the file name that contains the root and intermediate certificates related to the local certificate. You can use this parameter in three ways: • To download no certificates • To download a certificate from the original configuration server • To download a certificate from another specified server To download a specific file, the string value MUST HAVE A FILENAME at the end of the string. For example: 802.1x root and intermediate certificates:ftp://admin:admin!@1.2.3.4:50/path/phones802RootCert.pem where “path” is the directory and “phones802RootCert.pem” is the filename. If you do not specify a filename, the download fails. See examples for each below.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	The following example downloads no 802.1x root and intermediate certificate file: 802.1x root and intermediate certificates: The following example downloads the 802.1x root and intermediate certificate file from the original configuration server. 802.1x root and intermediate certificates: phones802RootCert.pem The following example uses FTP to download the firmware file “phones802RootCert.pem” (802.1x root and intermediate certificate file) from the “path” directory on server 1.2.3.4 using port 50: 802.1x root and intermediate certificates:ftp://admin:admin!@1.2.3.4:50/path/phones802RootCert.pem

PARAMETER – *802.1x local certificate*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the file name that contains the local certificate. You can use this parameter in three ways: • To download no certificates • To download a certificate from the original configuration server • To download a certificate from another specified server To download a specific file, the string value MUST HAVE A FILENAME at the end of the string. For example: 802.1x local certificate:ftp://admin:admin!@1.2.3.4:50/path/phones802LocalCert.pem where “path” is the directory and “phones802LocalCert.pem” is the filename. If you do not specify a filename, the download fails. See examples for each below.
FORMAT	String
Default Value	N/A
Range	N/A
Example	The following example downloads no local certificate file: 802.1x local certificate: The following example downloads the local certificate file from the original configuration server. 802.1x local certificate: phones802LocalCert.pem The following example uses FTP to download the firmware file “phones802LocalCert.pem” (802.1x local certificate file) from the “path” directory on server 1.2.3.4 using port 50: 802.1x local certificate:ftp://admin:admin!@1.2.3.4:50/path/phones802LocalCert.pem

PARAMETER – *802.1x private key*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the file name that contains the private key.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	802.1x private key: filename.pem

PARAMETER – *802.1x trusted certificates*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the file name that contains the trusted certificates. You can use this parameter in three ways: • To download no certificates • To download a certificate from the original configuration server • To download a certificate from another specified server To download a specific file, the string value MUST HAVE A FILENAME at the end of the string. For example: 802.1x trusted certificates:ftp://admin:admin!@1.2.3.4:50/path/phones802TrustedCert.pem where "path" is the directory and "phones802TrustedCert.pem" is the filename. If you do not specify a filename, the download fails. See examples for each below.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	The following example downloads no 802.1x trusted certificate file: 802.1x trusted certificates: The following example downloads the 802.1x trusted certificate file from the original configuration server. 802.1x trusted certificates: phones802TrustedCert.pem The following example uses FTP to download the firmware file "phones802TrustedCert.pem" (802.1x trusted certificate file) from the "path" directory on server 1.2.3.4 using port 50: 802.1x trusted certificates:ftp://admin:admin!@1.2.3.4:50/path/phones802TrustedCert.pem

PARAMETER – *802.1x mutual authentication*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables mutual authentication for EAP-TLS for 802.1x set up.
FORMAT	boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	802.1x mutual authentication: 0

RTP, CODEC, DTMF GLOBAL SETTINGS

GLOBAL SETTINGS

PARAMETER – *sip rtp port*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Indicates the port through which the RTP packets are sent. This value must specify the beginning of the RTP port range on the gateway or router. **Note:** The SIP RTP port is used to send audio streams; port 5012 is used to record the streams. The RTP port is used for sending DTMF tones and for the audio stream. Your network administrator may close some ports for security reasons. You may want to use this parameter to send RTP data using a different port. **Note:** The phones support decoding and playing out DTMF tones sent in SIP INFO requests. The following DTMF tones are supported: • Support signals 0-9, #, * • Support durations up to 5 seconds
FORMAT	Integer
DEFAULT VALUE	3000
RANGE	N/A
EXAMPLE	sip rtp port: 3000

PARAMETER – *rtp symmetric port*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	By default the phones support symmetrical RTP port handling (i.e. the phone will only play an RTP stream if it comes from a "source" port that is the same as the "listening" port negotiated by the call manager. By disabling this parameter, administrators can configure the phones to support asymmetrical RTP port handling. If disabled, the phone will accept an RTP stream coming from a different "source" port and send RTP traffic to the caller at the "listening" port.
FORMAT	Boolean
DEFAULT VALUE	1 (Enabled)
RANGE	0 - 1 0 (Disabled) 1 (Enabled)
EXAMPLE	rtp symmetric port: 0

PARAMETER – *rtcp enable*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables Real-Time Transport Control Protocol (RTCP) functionality.
FORMAT	Boolean
DEFAULT VALUE	1 (Enabled)
RANGE	0 - 1 0 (Disabled) 1 (Enabled)
EXAMPLE	rtcp enable: 0

PARAMETER – *sip no rtp timeout*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the timeout period (in seconds) whereby if no audio stream (i.e. RTP packets) is received in the defined amount of time, the phone will send a BYE request, thus releasing the call and returning the home/idle screen.
FORMAT	Integer
DEFAULT VALUE	0 (Disabled)
RANGE	0 - 2147483647 (seconds)
EXAMPLE	sip no rtp timeout: 240

PARAMETER – *sip use basic codecs*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables basic codecs (G.711 u-Law, G.711 a-Law, G.729). Enabling this parameter allows the IP phone to use the basic Codecs when sending/receiving RTP packets.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 - Disable 1 - Enable
EXAMPLE	sip use basic codecs: 1

PARAMETER – *sip amr codec payload format*	**CONFIGURATION FILES** startup.cfg, <model>.cfg <mac>.cfg
DESCRIPTION	Specifies the payload format for the AMR/AMR-WB codec.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0-2 0 (Enable bandwidth efficient mode per RFC, no octet-aligned header is in the INVITE SDP [default]). 1 (Enable octet-aligned mode and add octet-align:1 in SDP, negotiate mode for incoming calls). 2 (Disable octet-aligned mode and add octet-align:0 in SDP, negotiate mode for incoming calls).
EXAMPLE	sip amr codec payload format: 1

PARAMETER – *sip amr codec mode set*	**CONFIGURATION FILES** startup.cfg, <model>.cfg <mac>.cfg
DESCRIPTION	Specifies the list of mode sets supported and also the preferred mode to use if multiple modes are supported by both sides.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0-7 0 (4.75 kbps) 1 (5.15 kbps) 2 (5.90 kbps) 3 (6.70 kbps) 4 (7.40 kbps) 5 (7.95 kbps) 6 (10.2 kbps) 7 (12.2 kbps)
EXAMPLE	sip amr codec mode set: 2,1,0,3,4

PARAMETER – sip amr wb codec mode set	**CONFIGURATION FILES** startup.cfg, <model>.cfg <mac>.cfg
DESCRIPTION	Specifies the list of mode sets supported and also the preferred mode to use if multiple modes are supported by both sides.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0-8 0 (6.60 kbps) 1 (8.85 kbps) 2 (12.65 kbps) 3 (14.25 kbps) 4 (15.85 kbps) 5 (18.25 kbps) 6 (19.85 kbps) 7 (23.05 kbps) 8 (23.85 kbps)
EXAMPLE	sip amr wb codec mode set: 2,1,0

PARAMETER – *sip out-of-band dtmf*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables out-of-band DTMF. Enabling this parameter forces the IP phone to use out-of-band DTMF according to RFC2833. **Note:** See "Out-of-Band DTMF and DTMF Method on page 4-94" for DTMF behavior information when this parameter is used in conjunction with the "sip dtmf method" parameter.
FORMAT	Boolean
DEFAULT VALUE	1
RANGE	0 - Disable 1 - Enable
EXAMPLE	sip out-of-band dtmf: 0

PARAMETER – *sip customized codec*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies a customized codec preference list which allows you to select the preferred codecs for this IP phone. You can enter up to 10 codec preferences.
FORMAT	Comma-separated list of semicolon-separated values
DEFAULT VALUE	N/A
RANGE	Valid values for the syntax are: **payload**: Configuration Files — Web UI 0 - G711u/8000 — G.711u (8K) 8 - G711a/8000 — G.711a (8K) 9 - G722/8000 — G.722 18 - G729/8000 — G.729 96 - G726-40/8000 — G.726-40 97 - G726-24/8000 — G.726-24 98 - G726-16/8000 — G.726-16 110 - G711u/16000 — G711u (16K) 111 - G711a/16000 — G711a (16K) 112 - L16/8000 — L16 (8K) 113 - L16/16000 — L16 (16K) 115 - G726-32/8000 — G.726-32 118 - AMR — AMR (Licensed feature) 119 - AMR-WB G.722.2 — AMR-WB (Licensed feature) 121 - G.722.1 — G.722.1 Leave blank for all codecs — All (Codec 1 only) Basic (Codec 1 only) None (Codecs 2 through 10 only) **ptime** (in milliseconds) 5, 10, 15, 20........90 **silsupp** on, off **Note:** Enabling or disabling silence suppression (**sil supp**) enables/disables it for all codecs in the customized list. When mismatch occurs in the configured silsupp parameter, the first one specified in the parameter value will be used. **Note:**
EXAMPLE	sip customized codec: payload=18;ptime=10;silsupp=on,payload=0;ptime=10;silsupp=on

PARAMETER – *sip dtmf method*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Sets the Dual-tone multifrequency (DTMF) method to use on the IP phone. **Note:** See “Out-of-Band DTMF and DTMF Method” on page 4-94 for DTMF behavior information when this parameter is used in conjunction with the “sip out-of-band dtmf” parameter.
FORMAT	Integer
DEFAULT VALUE	0 (RTP)
RANGE	0 (RTP) 1 (SIP INFO) 2 (BOTH)
EXAMPLE	sip dtmf method: 1

PARAMETER – *sip srtp mode*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This parameter determines if SRTP is enabled on this IP phone, as follows: • If set to 0, then disable SRTP. • If set to 1 then SRTP calls are preferred. • If set to 2, then SRTP calls only are generated/accepted. • If set to 3, then SRTP and RTP calls are generated/accepted
FORMAT	Integer
DEFAULT VALUE	0 (SRTP Disabled)
RANGE	0 (SRTP Disabled) 1 (SRTP Preferred) 2 (SRTP Only) 3 (SRTP and RTP)
EXAMPLE	sip srtp mode: 1

PARAMETER – *sip silence suppression*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Silence suppression is enabled by default on the IP phones. The phone negotiates whether or not to use silence suppression. Disabling this feature forces the phone to ignore any negotiated value.
FORMAT	Boolean
DEFAULT VALUE	1 (enabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sip silence suppression: 0

PARAMETER – *sip remove silence suppression offer*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not the silence suppression attribute should be included in the Session Description Protocol (SDP) offer. If enabled, the silence suppression attribute will be removed from the SDP offer. If disabled, the attribute will not be removed from the SDP offer. **Note:** If the value of this parameter has changed, a reboot will be required for the change to take effect.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sip remove silence suppression offer: 1

PER-LINE SETTINGS

PARAMETER – *sip lineN dtmf method* (where N = line number)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Sets the Dual-tone multifrequency (DTMF) method to use on the IP phone for a specific line.
FORMAT	Integer
DEFAULT VALUE	0 (RTP)
RANGE	0 (RTP) 1 (SIP INFO) 2 (BOTH)
EXAMPLE	sip line1 dtmf method: 1

PARAMETER – *sip lineN srtp mode* (where N = line number)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This parameter determines if SRTP is enabled on this line, as follows: • If set to -1, then use the global setting for this line. (This is the default setting.) • If set to 0, then disable SRTP. • If set to 1 then SRTP calls are preferred. • If set to 2, then SRTP calls only are generated/accepted.
FORMAT	Integer
DEFAULT VALUE	0 (disabled)
RANGE	-1 0 1 2
EXAMPLE	sip line1 srtp mode: 1

AUTODIAL SETTINGS

Global Settings

PARAMETER – *sip autodial number*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Globally specifies the SIP phone number that the IP phone autodials when the handset is lifted from the phone cradle. An empty (blank) value disables autodial on the phone.
FORMAT	Integer
DEFAULT VALUE	Blank
RANGE	Any valid SIP number
EXAMPLE	sip autodial number: 8500

PARAMETER – *sip autodial timeout*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Globally specifies the time, in seconds, that the phone waits to dial a pre-configured number after the handset is lifted from the IP phone cradle. If this parameter is set to 0 (hotline), the phone immediately dials a pre-configured number when you lift the handset. If this parameter is set to a value greater than 0, the phone waits the specified number of seconds before dialing the pre-configured number (warmline) when you lift the handset. Default is 0 (hotline).
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0-120
EXAMPLE	sip autodial timeout: 30

PER-LINE SETTINGS

PARAMETER – *sip lineN autodial number* (where N = line number)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	On a per-line basis, this parameter specifies the SIP phone number that the IP phone autodials when the handset is lifted from the phone cradle. Valid values can be: • -1 (Default): The phone uses the global autodial setting for this line. • Blank (Empty field): Disables autodial on this line. • Valid SIP Number: Dials the SIP number specified for this line.
FORMAT	Integer
DEFAULT VALUE	-1
RANGE	Any valid SIP number.
EXAMPLE	sip line1 autodial number: 8500

PARAMETER – *sip lineN autodial timeout* (where N = line number)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	On a per-line basis, this parameter specifies the time, in seconds, that the phone waits to dial a pre-configured number after the handset is lifted from the IP phone cradle. If this parameter is set to 0 (hotline), the phone immediately dials a pre-configured number when you lift the handset. If this parameter is set to a value greater than 0, the phone waits the specified number of seconds before dialing the pre-configured number (warmline) when you lift the handset. Default is 0 (hotline).
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0-120
EXAMPLE	sip line1 autodial timeout: 30

VOICEMAIL SETTINGS

PARAMETER –	CONFIGURATION FILES
sip lineN vmail (where N = line number)	startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Use this parameter in the *<mac>.cfg* file to configure the phone to dial a specific number to access an existing voicemail account on a Service Provider's server. The user then follows the voicemail instructions for listening to voicemails. **Note:** The phone must have a registered voicemail account from a server for this feature to be enabled. When no registered voicemail accounts are registered to the phone, the display shows "List Empty". The phone displays up to 99 voicemails for an account even if the number of voicemails exceeds the limit. Registered account numbers/URIs that exceed the length of the screen, either with or without the voicemail icon and the message count, are truncated with an ellipse character at the end of the number/URI string.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	0-99
EXAMPLE	sip line1 vmail: *97 **Note:** In the above example, the user would dial *97 to access the voicemail account.

PARAMETER –	CONFIGURATION FILES
sip vmail	startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the phone number of the voicemail system connected to the sip account. This parameter specifies the phone number you dial from your phone to retrieve your voicemail. Configuring this parameter allows you to call the voicemail system directly from the "voicemail" application via the IP Phone UI under the "Services" menu of the IP Phone.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	sip vmail: 5553435

SCA VOICEMAIL INDICATOR SETTINGS

PARAMETER – *voice mail indicator*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Controls which visual indicators are displayed on the IP phone when voicemail messages are pending on SCA-configured lines. Applicable to the 6867i, 6869i, and 6873i model IP phones (as well as expansion modules).
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0-2 0: Do no display any visual indicators. 1: Display a gray circle for the 6867i/6869i/6873i and the number of pending messages inside the circle and illuminate the softkey's LED. 2: Display only a gray circle for the 6867i/6869i/6873i (no indication of the number of pending messages) and illuminate the softkey's LED.
EXAMPLE	voice mail indicator: 1

ENHANCED DIRECTORY SETTINGS

CSV DIRECTORY SETTINGS

PARAMETER – *directory 1*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The name of the first CSV-based directory list file that you can download from the configuration server. You can use this parameter in three ways: • To download no directory • To download a directory from the original configuration server • To download a directory from another specified server To download a specific file, the string value MUST HAVE A FILENAME at the end of the string. For example: • directory 1: tftp://10.30.102.158/path/companylist.csv where “path” is the directory and “companylist.csv” is the filename. If you do not specify a filename, the download fails. See examples for each below.
FORMAT	Alphanumeric characters
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	Example The following example downloads no directory: • directory 1: The following example downloads a company directory from the original configuration server: • directory 1: companylist.csv The following example downloads a company directory file from the specified server in the “path” directory: • directory 1: tftp://192.168.0.55/path/companylist.csv

PARAMETER – *directory 2*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The name of the second CSV-based directory list file that you can download from the configuration server. You can use this parameter in three ways: • To download no directory • To download a directory from the original configuration server • To download a directory from another specified server To download a specific file, the string value MUST HAVE A FILENAME at the end of the string. For example: • directory 2: tftp://10.30.102.158/path/companylist.csv where “path” is the directory and “companylist.csv” is the filename. If you do not specify a filename, the download fails. See examples for each below.
FORMAT	Alphanumeric characters
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	Example The following example downloads no directory: • directory 2: The following example downloads a company directory from the original configuration server: • directory 2: companylist.csv The following example downloads a company directory file from the specified server in the “path” directory: • directory 2: tftp://192.168.0.55/path/companylist.csv

PARAMETER – *directory 1 name*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the folder name of the directory defined in the “directory 1” parameter.
FORMAT	Alphanumeric characters
DEFAULT VALUE	Corporate
RANGE	N/A
EXAMPLE	directory 1 name: Office

PARAMETER – *directory 2 name*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the folder name of the directory defined in the “directory 2” parameter.
FORMAT	Alphanumeric characters
DEFAULT VALUE	Personal
RANGE	N/A
EXAMPLE	directory 2 name: Friends

PARAMETER – directory 1 enabled	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not the directory defined in the “directory 1” parameter should be enabled to be accessed on the phone.
FORMAT	Boolean
DEFAULT VALUE	1 (Enabled)
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	directory 1 enabled: 1

PARAMETER – *directory 2 enabled*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not the directory defined in the “directory 2” parameter should be enabled to be accessed on the phone.
FORMAT	Boolean
DEFAULT VALUE	1 (Enabled)
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	directory 2 enabled: 1

EXCHANGE DIRECTORY SETTINGS

PARAMETER – *exchange server*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the user’s Microsoft Exchange server IP address or Fully Qualified Domain Name (FQDN).
FORMAT	IP address or FQDN
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	exchange server: mail.acme.com

PARAMETER – *exchange use ssl*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether SSL (Secure Sockets Layer) should be enabled or disabled.
FORMAT	Boolean
DEFAULT VALUE	1 (Enabled)
RANGE	0 -1 0 (Disabled) 1 (Enabled)
EXAMPLE	exchange use ssl: 1

PARAMETER – *exchange path*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Configures a custom Exchange Web Services (EWS) path on the Exchange server hosting the EWS managed API. By default the path is "ews/exchange.asmx" on a typical Microsoft Exchange installation.
FORMAT	String
DEFAULT VALUE	ews/exchange.asmx
RANGE	N/A
EXAMPLE	exchange path: custom_ews/exchange.asmx

PARAMETER – *exchange user name*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the user's Microsoft Exchange user name.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	exchange user name: jdoe

PARAMETER – *exchange contacts enabled*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not the Microsoft Exchange directory should be enabled to be accessed on the phone.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	exchange contacts enabled: 1

PARAMETER – *exchange contacts name*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the folder name of the Microsoft Exchange directory when enabled.
FORMAT	Alphanumeric characters
DEFAULT VALUE	Exchange Contacts
RANGE	N/A
EXAMPLE	exchange contacts name: MS Exchange

PARAMETER – *exchange contacts resync time*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Sets the time of day in a 24-hour period for the IP phone to update the Microsoft Exchange directory. This parameter works with TFTP, FTP, HTTP and HTTPS servers. **Notes:** • The resync time is based on the local time of the IP phone. • The value of 00:00 is 12:00 A.M. • When entering a value for this parameter using the configuration files, the value can be entered using minute values from 00 to 59 (for example, the auto resync time can be entered as 02:56). • Resync adds up to 15 minutes random time to the configured time. For example, if the resync time parameter is set to 02:00, the event takes place any time between 02:00 and 02:15. • When the language on the phone is set to French or Spanish, you must enter the time in the format "00h00" (configuration files only).
FORMAT	hh:mm 00h00 (for French and Spanish configuration files)
DEFAULT VALUE	02:00
RANGE	hh = 00 to 23 mm = 00 to 59
EXAMPLE	exchange contacts resync time: 03:24

PARAMETER – *exchange contacts resync days*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the amount of days that the phone waits between Microsoft Exchange directory resync operations. **Note:** A value of 0 causes the phone to checksync every time the clock reads the proper time. A value of 1 forces the phone to wait 24 hours prior to doing the first checksync.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0-364
EXAMPLE	exchange contacts resync days: 1

PARAMETER – *exchange contacts resync max delay*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the maximum time, in minutes, the phone waits past the scheduled time before starting a Microsoft Exchange directory checksync.
FORMAT	Integer
DEFAULT VALUE	30
RANGE	0-1439
EXAMPLE	exchange contacts resync max delay: 20

BROADSOFT XSI DIRECTORY SETTINGS

PARAMETER – *xsi ip*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the Xsi Enterprise Directory credentials (if applicable) and IP address or Fully Qualified Domain Name (FQDN) of the Xsi server in the following syntax: server or username:password@server **Note:** Xsi credentials defined through the "**xsi ip**" parameter are only applicable to the Xsi Enterprise Directory feature and not applicable to user-related Xsi features such as Speed Dial 8, Basic Call Logs, Hide Number, and other Xsi directories. Credentials for the user-related Xsi features require encryption and therefore must be entered through the phone's Options List > Credentials menu.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLES	xsi ip: xsp.xsi.broadworks.net or xsi ip: johndoe:mitel123@xsp.xsi.broadworks.net

PARAMETER – *xsi protocol*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the protocol (either HTTP or HTTPs) used for communicating with the Xsi server.
FORMAT	String
DEFAULT VALUE	http
RANGE	http https
EXAMPLE	xsi protocol: https

PARAMETER – *xsi port*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the port used for communicating with the Xsi server.
FORMAT	Integer
DEFAULT VALUE	80 (when protocol used is HTTP) 443 (when protocol used is HTTPs)
RANGE	Any valid port
EXAMPLE	xsi port: 8080

PARAMETER – *xsi user name*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the user name used for authentication of the Xsi account.
FORMAT	<username>@<server>
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	xsi user name: xsi@xsi.broadworks.net

PARAMETER – *xsi personal contacts enabled*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not the BroadSoft Xsi Personal Contacts directory should be enabled to be accessed on the phone.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	xsi personal contacts enabled: 1

PARAMETER – xsi enterprise directory enabled	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not the BroadSoft Xsi Enterprise Directory should be enabled to be accessed on the phone.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	xsi enterprise directory enabled: 1

PARAMETER – *xsi enterprise common directory enabled*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not the BroadSoft Xsi Enterprise Common Directory should be enabled to be accessed on the phone.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	xsi enterprise common directory enabled: 1

PARAMETER – *xsi group directory enabled*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not the BroadSoft Xsi Group Directory should be enabled to be accessed on the phone.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	xsi group directory enabled: 1

PARAMETER – *xsi group common directory enabled*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not the BroadSoft Xsi Group Common Directory should be enabled to be accessed on the phone.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	xsi group common directory enabled: 1

PARAMETER – *xsi personal contacts name*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the folder name of the BroadSoft Xsi Personal Contacts when enabled.
FORMAT	Alphanumeric characters
DEFAULT VALUE	Personal Contacts
RANGE	N/A
EXAMPLE	xsi personal contacts name: Xsi Personal

PARAMETER – *xsi enterprise directory name*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the folder name of the BroadSoft Xsi Enterprise Directory when enabled.
FORMAT	Alphanumeric characters
DEFAULT VALUE	Enterprise Directory
RANGE	N/A
EXAMPLE	xsi enterprise directory name: Xsi Enterprise

PARAMETER – *xsi enterprise common directory name*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the folder name of the BroadSoft Xsi Enterprise Common Directory when enabled.
FORMAT	Alphanumeric characters
DEFAULT VALUE	Enterprise Common Directory
RANGE	N/A
EXAMPLE	xsi enterprise common directory name: Xsi Ent. Common

PARAMETER – *xsi group directory name*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the folder name of the BroadSoft Xsi Group Directory when enabled.
FORMAT	Alphanumeric characters
DEFAULT VALUE	Group Directory
RANGE	N/A
EXAMPLE	xsi group directory name: Xsi Group

PARAMETER – *xsi group common directory name*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the folder name of the BroadSoft Xsi Group Common Directory when enabled.
FORMAT	Alphanumeric characters
DEFAULT VALUE	Group Common Directory
RANGE	N/A
EXAMPLE	xsi group common directory name: Xsi Group Common

PARAMETER – *xsi resync time*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Sets the time of day in a 24-hour period for the IP phone to update the BroadSoft Xsi directories. This parameter works with TFTP, FTP, HTTP and HTTPS servers. **Notes:** • The resync time is based on the local time of the IP phone. • The value of 00:00 is 12:00 A.M. • When entering a value for this parameter using the configuration files, the value can be entered using minute values from 00 to 59 (for example, the auto resync time can be entered as 02:56). • Resync adds up to 15 minutes random time to the configured time. For example, if the resync time parameter is set to 02:00, the event takes place any time between 02:00 and 02:15. • When the language on the phone is set to French or Spanish, you must enter the time in the format "00h00" (configuration files only).
FORMAT	hh:mm 00h00 (for French and Spanish configuration files)
DEFAULT VALUE	02:30
RANGE	hh = 00 to 23 mm = 00 to 59
EXAMPLE	xsi resync time: 03:24

PARAMETER – *xsi resync days*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the amount of days that the phone waits between BroadSoft Xsi directory resync operations. **Note:** A value of 0 causes the phone to checksync every time the clock reads the proper time. A value of 1 forces the phone to wait 24 hours prior to doing the first checksync.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0-364
EXAMPLE	xsi resync days: 1

PARAMETER – *xsi resync max delay*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the maximum time, in minutes, the phone waits past the scheduled time before starting a BroadSoft Xsi directory checksync.
FORMAT	Integer

DEFAULT VALUE	30
RANGE	0-1439
EXAMPLE	xsi resync max delay: 20

BASIC LDAP SETTINGS

PARAMETER – *ldap enabled*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not the LDAP Directory should be enabled to be accessed on the phone.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	ldap enabled: 1

PARAMETER – *ldap name*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the folder name of the LDAP Directory when enabled.
FORMAT	Alphanumeric characters
DEFAULT VALUE	LDAP
RANGE	N/A
EXAMPLE	ldap name: Mitel

PARAMETER – *ldap server*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg

DESCRIPTION	Specifies the LDAP server hostname or IP address. This parameter handles multiple values, in the format "username:password@ldapserver:port", where: • username for authentication (optional, if not provided anonymous connection or user inputted username will be used) • password for authentication (optional, if not provided no password or user inputted password will be used) • ldapserver is the IP address or name of the LDAP server (mandatory) By default, a Fully Qualified Domain Name (FQDN) of the LDAPS server is required to enable secure LDAP connection using LDAP over port 636 and with STARTTLS. • port is the LDAP interface port (optional, default is 389) For secure LDAP connection, LDAPS over port 636 is used to connect to the Active Directory and LDAPS with STARTTLS uses port 389. For LDAPS connection, scheme (ldaps://) is mandatory in the format username:password@scheme://ldapserver:port The scheme (ldap://) is optional for non-secure LDAP and LDAPS with STARTTLS.
FORMAT	String (hostname or IP address)
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap server: ldap.company.com (no authentication and using default port 389) ldap server: user:password@ldap.company.com:3268 (authentication and using port 3268) ldap server: CN=admin01,OU=toronto,DC=mitel,DC=com:1234@abc.mitel.com:389 ldap server: CN=admin01,OU=toronto,DC=mitel,DC=com:1234@ldap://abc.mitel.com:389 ldap server: CN=admin01,OU=toronto,DC=mitel,DC=com:1234@ldaps://abc.mitel.com:636

PARAMETER – *ldap user name*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the user's LDAP user name.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap user name: jdoe

PARAMETER – *ldap base dn*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP server base DN. It is the description of the top level of the directory tree. Usually if a company domain is “company.com”, the base DN (distinguished name) must be entered under the form “dc=company, dc=com”.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap base dn: dc=acme, dc=com (for acme.com)

PARAMETER – *ldap resync time*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Sets the time of day in a 24-hour period for the IP phone to update the LDAP directory. This parameter works with TFTP, FTP, HTTP and HTTPS servers. **Notes:** • The resync time is based on the local time of the IP phone. • The value of 00:00 is 12:00 A.M. • When entering a value for this parameter using the configuration files, the value can be entered using minute values from 00 to 59 (for example, the auto resync time can be entered as 02:56). • Resync adds up to 15 minutes random time to the configured time. For example, if the resync time parameter is set to 02:00, the event takes place any time between 02:00 and 02:15. • When the language on the phone is set to French or Spanish, you must enter the time in the format "00h00" (configuration files only).
FORMAT	hh:mm 00h00 (for French and Spanish configuration files)
DEFAULT VALUE	02:00
RANGE	hh = 00 to 23 mm = 00 to 59
EXAMPLE	ldap resync time: 03:24

PARAMETER – *ldap resync days*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the amount of days that the phone waits between LDAP directory resync operations. **Note:** A value of 0 causes the phone to checksync every time the clock reads the proper time. A value of 1 forces the phone to wait 24 hours prior to doing the first checksync.

FORMAT	Integer
DEFAULT VALUE	0
RANGE	0-364
EXAMPLE	ldap resync days: 1

PARAMETER – *ldap resync max delay*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the maximum time, in minutes, the phone waits past the scheduled time before starting an LDAP directory checksync.
FORMAT	Integer
DEFAULT VALUE	30
RANGE	0-1439
EXAMPLE	ldap resync max delay: 20

PARAMETER – *ldaps trusted certificates*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the path of the certificate file on the configuration server.
FORMAT	String
DEFAULT VALUE	NA
RANGE	NA
EXAMPLE	ldaps trusted certificates: cacert.pem

PARAMETER – *ldap starttls*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This parameter activates LDAP with STARTTLS to enable secure LDAP connection to Active Directory.
FORMAT	Integer
DEFAULT VALUE	1
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	ldap starttls: 1

PARAMETER – *ldap mtls*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables access to LDAP Server via mTLS (mutual Transport Layer Security).
FORMAT	Boolean
DEFAULT VALUE	0

RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	*ldap mtls*: 1

ADVANCED LDAP SETTINGS

PARAMETER – *ldap cn attribute*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Used when both the first and last name of a record are empty
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap cn attribute: display

PARAMETER – *ldap dn attribute*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Used to perform the search request for the detailed view of an LDAP contact.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap dn attribute: customDN

PARAMETER – *ldap search filter*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Used to set search filters. This parameter format must follow RFC 4515, for example (sn=%). This parameter must include a '%' character at the place where it will be replaced by a*, b*, etc...
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap search filter: (&(sn=%)(number=*))

PARAMETER – *ldap search scope*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Used to set the search scope. A "base" search is performed only on the baseDN, a "onelevel" search is performed on the baseDN and the first sublevel, and a "subtree" search is performed on the whole tree under the base DN.
FORMAT	String list base/onelevel/subtree
DEFAULT VALUE	N/A
RANGE	base/onelevel/subtree
EXAMPLE	ldap search scope: onelevel

PARAMETER – *ldap search timeout*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Used to set the request timeout for LDAP requests.
FORMAT	Integer, seconds
DEFAULT VALUE	20
RANGE	1 to 120
EXAMPLE	ldap search timeout: 30

PARAMETER – *ldap network timeout*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Used to set the network timeout for LDAP requests.
FORMAT	Integer, seconds
DEFAULT VALUE	20
RANGE	1 to 120
EXAMPLE	ldap network timeout: 50

PARAMETER – *ldap use ISO-8859-1 encoding*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not the LDAP directory the phone is configured to use ISO-8859-1 or UTF-8 encoding. If the LDAP directory utilizes ISO-8859-1 encoding and the parameter is set to “1”, the phone will transcode any characters using diacritical marks from the ISO-8859-1 character set to the equivalent UTF-8 characters, correcting any character encoding issues. **Note:** This parameter is ignored if the LDAP directory is a Microsoft Active Directory.
FORMAT	Boolean
DEFAULT VALUE	0 (False)
RANGE	0 - 1 0 = False (LDAP directory uses UTF-8 encoding) 1 = True (LDAP directory uses ISO-8859-1 encoding)
EXAMPLE	ldap use ISO-8859-1 encoding: 1

PARAMETER – *ldap first name attribute list*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP first name (e.g. John) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A

EXAMPLE	ldap first name attribute list: fname, uname

PARAMETER – *ldap last name attribute list*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP last name (e.g. Doe) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap last name attribute list: name, lname

PARAMETER – *ldap company attribute list*	**CONFIGURATION FILES** astra.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP company name (e.g. Mitel) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap company attribute list: organization, bname

PARAMETER – *ldap job title attribute list*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP job title (e.g. Vice President) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap job title attribute list: jtitle, title

PARAMETER – *ldap business street attribute list*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP business street (e.g. Snow Blvd.) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap business street attribute list: waddress, baddress

PARAMETER – *ldap business city attribute list*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP business city (e.g. Concord) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap business city attribute list: wcity, bcity

PARAMETER – *ldap business state attribute list*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP business state (e.g. Ontario) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap business state attribute list: wstate, bstate

PARAMETER – *ldap business postal code attribute list*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP business postal code (e.g. L4K 4N9) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap business postal code attribute list: bcode, wcode

PARAMETER – *ldap business country attribute list*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP business country (e.g. Canada) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap business country attribute list: bcountry, wcountry

PARAMETER – *ldap home street attribute list*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP home street (e.g. Internet Blvd.) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap home street attribute list: hstreet, pstreet

PARAMETER – *ldap home city attribute list*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP home city (e.g. Frisco) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap home city attribute list: hcity, pcity

PARAMETER – *ldap home state attribute list*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP home state (e.g. Texas) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap home state attribute list: hstate, pstate

PARAMETER – *ldap home postal code attribute list*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP home postal code (e.g. 75034) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap home postal code attribute list: hcode, pcode

PARAMETER – *ldap home country attribute list*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP home country (e.g. U.S.A) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap home country attribute list: hcountry, pcountry

PARAMETER – *ldap business phone 1 attribute list*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP business phone 1 (e.g. 1-905-760-4200) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap business phone 1 attribute list: wphone1, bphone1

PARAMETER – *ldap business phone 2 attribute list*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP business phone 2 (e.g. 1-905-760-4201) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap business phone 2 attribute list: wphone2, bphone2

PARAMETER – *ldap home phone 1 attribute list*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP home phone 1 (e.g. 1-416-468-3266) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap home phone 1 attribute list: hphone1, pphone1

PARAMETER – *ldap home phone 2 attribute list*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP home phone 2 (e.g. 1-416-468-3267) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap home phone 2 attribute list: hphone2, pphone2

PARAMETER – *ldap mobile phone attribute list*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP mobile phone (e.g. 1-416-468-3268) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap mobile phone attribute list: cell, mobile

PARAMETER – *ldap other phone attribute list*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP other phone (e.g. 1-416-468-3269) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap other phone attribute list: otherphone, mphone

PARAMETER – *ldap business fax attribute list*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP business fax (e.g. 1-905-760-4233) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap business fax attribute list: fax, bfax

PARAMETER – *ldap email 1 attribute list*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP email 1 (e.g. john.doe@mitel.com) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap email 1 attribute list: email1, mail1

PARAMETER – *ldap email 2 attribute list*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP email 2(e.g. john.d@mitel.com) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap email 2 attribute list: email2, mail2

PARAMETER – *ldap email 3 attribute list*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the LDAP email 3 (e.g. j.doe@mitel.com) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
FORMAT	String, list of attribute names separated by a comma.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	ldap email 3 attribute list: email3, mail3

ASYNCHRONOUS LDAP DIRECTORY LOOKUP MODE SUPPORT

PARAMETER – *ldap downloaded*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the LDAP mode between cached and lookup. When defined as "**0**", LDAP directories are not cached on the phone (i.e. LDAP directories are available using the lookup method). When defined as "**1**" (default), LDAP directories are cached on phone.
FORMAT	Boolean
DEFAULT VALUE	1 (Enabled)
RANGE	0 - 1 0 (Disabled) 1 (Enabled)
EXAMPLE	ldap downloaded: 0

PARAMETER – *ldap lookup filter*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Represents the custom LDAP query sent for an LDAP lookup. This parameter allows the query to be aligned to the LDAP server data scheme. **Note:** This parameter is ignored if the LDAP server is Exchange.
FORMAT	String Must include at least one character "%" which will be replaced by the lookup string in the request sent to the server.
DEFAULT VALUE	(|(givenName=%)(sn=%)(company=%))
RANGE	N/A
EXAMPLE	ldap lookup filter: (|(givenName=%)(sn=%))

Note: The Mitel 6863i and 6865i SIP IP phone models do not support Asynchronous LDAP directory lookup mode.

GENERAL DIRECTORY SETTINGS

PARAMETER – *directory disabled*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the local as well as all externally-sourced directories on the IP phone. If this parameter is set to 0, users can access the Directory List via the IP phone UI. If this parameter is set to 1, the Directory List does not display on the IP phone and the Directory key is disabled.
FORMAT	Boolean
DEFAULT VALUE	0 (false)

RANGE	0 - 1 0 (False) 1 (True)
EXAMPLE	directory disabled: 1

PARAMETER – *directory display name order*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the order in which a directory contact's name is displayed on screen.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 - 1 0 (First Last) 1 (Last, First)
EXAMPLE	directory display name order: 1

PARAMETER – *directory sort preference*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the order in which the phone should sort directory contacts when displayed on screen.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 - 1 0 (By First Name) 1 (By Last Name)
EXAMPLE	directory sort preference: 1

DIRECTORY SEARCH DYNAMIC THRESHOLD

PARAMETER – *directory search dynamic threshold*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the threshold value where the contact search is no longer dynamic (for the 6867i, 6869i, and 6873i). If any enabled Directory source holds more entries than the configured value, the user must manually press the Search softkey in order to trigger the search.
FORMAT	Integer
DEFAULT VALUE	5000
RANGE	0 - 1000000
EXAMPLE	directory search dynamic threshold: 1000

DIRECTORY LOOSE NUMBER MATCHING

PARAMETER – *directory digits match*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies how many digits of an incoming call's phone number the phone will take into consideration when performing a directory lookup.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 - 10 **Notes:** 1. When defined as 0, the default behaviour is to match the incoming call's number with the directory entry's number, after both of them were stripped from the country code, the national prefix or the trunk prefix. 2. If the incoming call's phone number is greater than or equal to the defined value and the respective last digits of the phone number match those of a directory entry, the phone will display the directory entry's name on screen. 3. If the incoming call's phone number is less than the defined value, the phone will not perform a directory lookup and will display the information provided in the SIP header.
EXAMPLE	directory digits match: 9

CUSTOMIZABLE DIRECTORY LIST KEY

PARAMETER – *directory script*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to specify a specific URI for accessing the Directory List after pressing the Directory List key. When this parameter is set, it overrides the standard function of the Directory List key.
FORMAT	Alphanumeric characters
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	directory script: http://10.50.100.234/test.xml

MISSED/RECEIVED CALLERS LIST SETTINGS

PARAMETER – *callers list disabled*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the Missed/Received Callers List. If this parameter is set to 0, the Missed/Received Callers List can be accessed by all users. If this parameter is set to 1, the IP phone does not save any caller information to the Missed/Received Callers List.
FORMAT	Boolean
DEFAULT VALUE	0 (false)
RANGE	0 (false), 1 (true)
EXAMPLE	callers list disabled: 1

CUSTOMIZABLE RECEIVED CALLERS LIST AND SERVICES KEY

PARAMETER – *services script*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to specify a specific URI for accessing services after pressing the Services key. When this parameter is set, it overrides the standard function of the Services key.
FORMAT	Alphanumeric characters
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	services script: http://10.50.100.234/test.xml

PARAMETER – *callers list script*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to specify a specific URI for accessing the Received Callers List after pressing the Received Callers List key. When this parameter is set, it overrides the standard function of the Received Callers List key.
FORMAT	Alphanumeric characters
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	callers list script: http://10.50.100.234/test.xml

CALL FORWARD SETTINGS

PARAMETER – *call forward disabled*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the ability to configure Call Forwarding. If this parameter is set to 0, a user and administrator can configure Call Forwarding via the Mitel Web UI and the IP Phone UI using the "Call Forward" options. If this parameter is set to 1, all "Call Forward" options are removed from the Mitel Web UI and the IP Phone UI, preventing the ability to configure Call Forwarding.
FORMAT	Boolean
DEFAULT VALUE	0 (false)
RANGE	0 (false), 1 (true)
EXAMPLE	call forward disabled: 1

CALL FORWARD KEY MODE SETTINGS

PARAMETER – *call forward key mode*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Sets the mode for how the phone uses “call forwarding” (CFWD) • **account** The account mode allows you to configure CFWD on a per account basis. Pressing a configured CFWD key applies to the account in focus. • **phone** The Phone mode allows you to set the same CFWD configuration for all accounts (**All**, **Busy**, and/or **No Answer**). When you configure the initial account, the phone applies the configuration to all other accounts. (In the Mitel Web UI, only the account you configured is enabled. All other accounts are grayed out but set to the same configuration.) Using the Mitel Web UI, if you make changes to that initial account, the changes apply to all accounts on the phone. • **custom** The Custom mode allows you to configure CFWD for a specific account or all accounts. You can configure a specific mode (**All**, **Busy**, and/or **No Answer**) for each account independently or all accounts. On the 6863i and 6865i, you can set all accounts to **ALL On** or **ALL Off**. On the 6867i, 6869i, and 6873i you can set all accounts to **All On**, **All Off**, or copy the configuration for the account in focus to all other accounts using a **CopytoAll** softkey. **Notes:** • If there is no CFWD key configured on the phone or it is removed, you can still set the CFWD modes via the IP Phone UI at the path *Options->Call Forward.* • If there is only one account configured on the phone, then the mode setting is ignored and the phone behaves as if the mode was set to “Phone”. • When configuring a CFWD mode (All, Busy, No Answer) for an account, you must configure a CFWD number for that mode in order for the mode to be enabled.
FORMAT	Integer
DEFAULT VALUE	0 (account)
RANGE	0 (account) 1 (phone) 2 (custom)
EXAMPLE	call forward key mode: 2

Example:

The following is an example of configuring the CFWD key mode in the configuration files:

```
call forward key mode: 2
softkey1 type: callforward
softkey1 states: idle connected incoming outgoing busy
```

In the above example, softkey 1 is configured for CFWD on line 1 (account 1) with a "**custom**" configuration. Pressing softkey 1 displays CFWD screens for which you can customize on the phone.

PIN SUPPRESSION

PARAMETER – *pin suppression dial plan*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows a pattern based configuration of the PIN suppression.
FORMAT	Alphanumeric characters

Symbol	Description
0, 1, 2, 3, 4, 5, 6, 7, 8, 9	Digit symbol
X	Match any digit symbol (wildcard)
*, #, .	Other keypad symbol; # can terminate a dial string
|	Expression inclusive OR
+	• 0 or more of the preceding digit symbol or [] expression • The dial plan must not end with +. • The dial plan must be suffixed with "#", if the SIP dial plan terminator is disabled or it must be suffixed with "^", if the SIP dial plan terminator is enabled.
[]	Symbol inclusive OR
-	Used only with [], represent a range of acceptable symbols; For example, [2-8]
"," (open/close quotes)	n the configuration files, enter the SIP dial plan value using quotes.
( )	Controls the masking of the pin. In the configuration files, enter the pin inside the brackets ().

DEFAULT VALUE	NA
RANGE	Up to 512 alphanumeric characters
EXAMPLE	pin suppression dial plan: "*11*(x+)*(x+)#"

LLDP-MED AND ELIN SETTINGS

PARAMETER – *lldp*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) on the IP Phone.
FORMAT	Boolean
DEFAULT VALUE	1 (enabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	lldp: 0

PARAMETER – *lldp interval*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The amount of time, in seconds, between the transmission of LLDP Data Unit (LLDPDU) packets. The value of zero (0) disables this parameter.
FORMAT	Integer
DEFAULT VALUE	30
RANGE	0 - 2147483647
EXAMPLE	lldp interval: 60

PARAMETER – *use lldp elin*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the use of an Emergency Location Identification Number (ELIN) received from LLDP as a caller ID for emergency numbers. Additional functionality to add an "elin=number" value to the From header is also available.
FORMAT	Integer
DEFAULT VALUE	1 (enabled)
RANGE	0 (disabled) 1 (enabled) 2 (enabled and will add an "elin=number" value to the From header indicating the call is an emergency call)
EXAMPLE	use lldp elin: 0

PARAMETER – *lldp startinterval*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Mitel IP Phones have a 32 second time-out interval for listening to LLDP-MED responses when the phone is booting up. If LLDP-MED responses are received after this initial listening period, the phone will ignore the response. This "lldp startinterval" parameter can be used to configure the time-out interval. This parameter is only valid during the phone bootup process.
FORMAT	Integer
DEFAULT VALUE	32 (seconds)
RANGE	0- 65535 (seconds)
EXAMPLE	lldp startinterval: 7

PARAMETER – *lldp optional inventory management tlv*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Implements either all of the LLDP-MED Inventory Management TLV sets or none of the sets.
FORMAT	Integer
DEFAULT VALUE	1 (send all LLDP-MED Inventory Management TLV sets)
RANGE	0-1 0 (do not send any LLDP-MED Inventory Management TLV sets) 1 (send all LLDP-MED Inventory Management TLV sets)
EXAMPLE	lldp optional inventory management tlv: 0

MISSED CALLS INDICATOR SETTINGS

PARAMETER – *missed calls indicator disabled*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the Missed Calls Indicator. If the "missed calls indicator disabled" parameter is set to 0, the indicator increments as unanswered calls come into the IP phone. If the "missed calls indicator disabled" parameter is set to 1, the indicator is disabled and will NOT increment as unanswered calls come into the IP phone.
FORMAT	Boolean
DEFAULT VALUE	0 (false)
RANGE	0 (false), 1 (true)
EXAMPLE	missed calls indicator disabled: 1

PARAMETER – *sip lineN missed calls enabled* (where N = line number)	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether missed calls on the defined line should increment the missed calls indicator on the phone's home/idle screen.
FORMAT	Boolean
DEFAULT VALUE	1
RANGE	0 - 1 0 (Disabled) 1 (Enabled)
EXAMPLE	sip line1 missed calls enabled: 1 sip line2 missed calls enabled: 0 sip line3 missed calls enabled: 1

XML SETTINGS

PARAMETER – *xml get timeout*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to specify a timeout value, in seconds, that the phone waits for the far side to return a response after accepting the HTTP GET connection. If the far side accepts the GET connection but never returns a response, it blocks the phone until it is rebooted. If you enter a value greater than 0 for this parameter, the phone times out and will not be blocked.
FORMAT	Integer
DEFAULT VALUE	0 (never timeout)
RANGE	0 to 2147483647 seconds
EXAMPLE	xml get timeout: 20

PARAMETER – *xml application URI*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This is the XML application you are loading into the IP phone configuration.
FORMAT	HTTP server path or fully qualified Domain Name
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	xml application URI: http://172.16.96.63/mitel/internet.php

PARAMETER – *xml application title*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This parameter allows you to rename the XML application in the IP phone UI (Services->4. Custom Feature). By default, when you load an XML application to the IP phone, the XML application title is called "Custom Feature". The "xml application title" parameter allows you to change that title. For example, if you are loading a traffic report XML application, you could change this parameter title to "Traffic Reports", and that title will display in the IP phone UI as Services->4. Traffic Reports.
FORMAT	Alphanumeric characters
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	xml application title: Traffic Reports

PARAMETER – *xml application post list*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The HTTP server that is pushing XML applications to the IP phone.
FORMAT	IP address in dotted decimal format and/or Domain name address
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	xml application post list: 10.50.10.53, dhcp10-53.ana.mitel.com

PARAMETER – *xml beep notification*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables a BEEP notification on the phone when a status message object (AastraIPPhoneStatus) containing a “beep” attribute arrives to the phone. Changes to this parameter are applied immediately.
FORMAT	Boolean
DEFAULT VALUE	1 (ON)
RANGE	0 (OFF)No beep is audible even if the beep attribute is present in the XML object. 1 (ON)The phone beeps when an XML object with the “beep” attribute arrives to the phone.
EXAMPLE	xml beep notification: 0

PARAMETER – *xml status scroll delay*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the length of time, in seconds, that each XML status message displays on the phone. **Note:** Changes to this parameter are applied immediately.
FORMAT	Integer
DEFAULT VALUE	5
RANGE	1 to 25
EXAMPLE	xml status scroll delay: 3

ACTION URI SETTINGS

PARAMETER – *action uri startup*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the URI for which the phone executes a GET on when a startup event occurs. This parameter can use any of the following variables: $$DISPLAYNAME$$ $$SIPUSERNAME$$ $$SIPAUTHNAME$$ $$PROXYURL$$ $$LINESTATE$$ $$LOCALIP$$ $$REGISTRATIONSTATE$$ $$REGISTRATIONCODE$$
FORMAT	Fully qualified URI
DEFAULT VALUE	N/A
RANGE	Up to 128 ASCII characters
EXAMPLE	action uri startup: http://10.50.10.140/startup

PARAMETER – *action uri registered*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the URI for which the phone executes a GET on when a successful registration event occurs. This parameter can use the following variables: $$SIPUSERNAME$$ $$SIPAUTHNAME$$ $$PROXYURL$$ $$LINESTATE$$ $$LOCALIP$$ **Note:** The "**action uri registered**" parameter executes on the first successful registration of each unique line configured on the phone.
FORMAT	Fully qualified URI
DEFAULT VALUE	N/A
RANGE	Up to 128 ASCII characters
EXAMPLE	action uri registered: http://10.50.10.14/registered.php?auth name=$$SIPAUTHNAME$$

PARAMETER – *action uri registration event*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the URI that the phone executes a GET on, when a registration event change occurs. This parameter uses the following variables to determine the state of the event: $$REGISTRATIONSTATE$$ $$REGISTRATIONCODE$$ **Note:** If defined, this action URI is also called upon at startup if the SIP registrar IP has not been configured (i.e. the IP is 0.0.0.0). **Note:** This action URI is not called when the same event is repeated (for example, a timeout occurs again when registration is already in a timeout state.)
FORMAT	String
DEFAULT VALUE	N/A
RANGE	Any valid URI
EXAMPLE	action uri registration event: http://10.30.100.39/PHPtests/actionuri.php?action=RegEvt&regstat e=$$REGISTRATIONSTATE$$&regcode=$$REGISTRATIONCOD E$$

PARAMETER – *action uri incoming*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the URI for which the phone executes a GET on when an incoming call event occurs. This parameter can use the following variables: $$REMOTENUMBER$$ $$DISPLAYNAME$$ $$SIPUSERNAME$$ $$INCOMINGNAME$ $$LINESTATE$$ $$CALLDURATION$$ $$CALLDIRECTION$$ $$LOCALIP$$ $$LINEINDEX$$
FORMAT	Fully qualified URI
DEFAULT VALUE	N/A
RANGE	Up to 128 ASCII characters
EXAMPLE	action uri incoming: http://10.50.10.140/incoming.php?number=$$REMOTENUMBER$$

PARAMETER – *action uri outgoing*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the URI for which the phone executes a GET on when an outgoing call event occurs. This parameter can use the following variables: $$REMOTENUMBER$$ $$SIPUSERNAME$$ $$LINESTATE$$ $$LOCALIP$$ $$LINEINDEX$$
FORMAT	Fully qualified URI
DEFAULT VALUE	N/A
RANGE	Up to 128 ASCII characters
EXAMPLE	action uri outgoing: http://10.50.10.140/outgoing.php?number=$$REMOTENUMBER$$

PARAMETER – *action uri offhook*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the URI for which the phone executes a GET on when an offhook event occurs. This parameter can use the following variables: $$LINESTATE$$ $$LOCALIP$$
FORMAT	Fully qualified URI
DEFAULT VALUE	N/A
RANGE	Up to 128 ASCII characters
EXAMPLE	action uri offhook: http://10.50.10.140/offhook

PARAMETER – *action uri onhook*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the URI for which the phone executes a GET on when an onhook event occurs. This parameter can use the following variables: $$LOCALIP$$ $$CALLDURATION$$ $$CALLDIRECTION$$ $$LINESTATE$$ **Note:** The “LocalIP”, “CallDuration”, and “CallDirection” variables allow for enhanced information in call records and billing applications.
FORMAT	Fully qualified URI
DEFAULT VALUE	N/A
RANGE	Up to 128 ASCII characters
EXAMPLE	action uri onhook: http://10.50.10.140/onhook

PARAMETER – *action uri connected*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the URI that the phone executes a GET on, when a call is connected. This parameter uses the following variables to determine the state of the line: $$REMOTENUMBER$$ $$DISPLAYNAME$$ $$SIPUSERNAME$$ $$SIPAUTHNAME$$ $$INCOMINGNAME$ $$PROXYURL$$ $$LINESTATE$$ $$CALLDIRECTION$$ $$LOCALIP$$ $$DISPLAYNAME$$ $$CALLDURATION$$ $$REGISTRATIONSTATE$$ $$REGISTRATIONCODE$$
FORMAT	String
DEFAULT VALUE	N/A
RANGE	Any valid URI
EXAMPLE	action uri connected: http://fargo.ana.mitel.com/connected.xml?state=$$LINESTATE$$

PARAMETER – *action uri disconnected*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the URI that the phone executes a GET on, when it transitions from the incoming, outgoing, calling, or connected state into the idle state. This parameter uses the following variables to determine the state of the line: $$LINESTATE$$ $$LOCALIP$$
FORMAT	String
DEFAULT VALUE	N/A
RANGE	Any valid URI
EXAMPLE	action uri disconnected: http://fargo.ana.mitel.com/disconnected.xml?state=$$LINESTATE$$

PARAMETER – *action uri blf*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the URI for which the phone executes a GET on when an BLF/List or BLF/Xfer key is pressed. This parameter can use the following variables: $$BLFNO$$ $$BLFSTATE$$ $$BLFTRANSFER$$ **Note:** The "blf key mode" parameter must be defined as "2" to use this feature.
FORMAT	Fully qualified URI
DEFAULT VALUE	N/A
RANGE	Up to 128 ASCII characters
EXAMPLE	action uri blf: http://192.168.0.50/blf.php?BLFNo=$$BLFNO$$

XML SIP NOTIFY SETTINGS

PARAMETER – *sip xml notify event*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the phone to accept or reject an aastra-xml SIP NOTIFY message. **Note:** To ensure the SIP NOTIFY is coming from a trusted source, it is recommended that you enable the Whitelist feature (**Whitelist Proxy** parameter) on the IP phone. If enabled, and the phone receives a SIP NOTIFY from a server that is NOT on the whitelist (i.e. untrusted server), the phone rejects the message.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 - disabled 1 - enabled
EXAMPLE	sip xml notify event: 1

PARAMETER – *action uri xml sip notify*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the URI to be called when an empty XML SIP NOTIFY is received by the phone. This parameter can use the following variable: $$LOCALIP$$ **Note:** The **sip xml notify event** parameter must be enabled.

FORMAT	HTTP(s) server path or Fully Qualified Domain Name
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	action uri xml sip notify: http://myserver.com/myappli.xml

POLLING ACTION URI SETTINGS

PARAMETER – *action uri poll*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the URI to be called every "action uri poll interval" seconds.
FORMAT	HTTP(s) server path or Fully Qualified Domain Name
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	action uri poll: http://myserver.com/myappli.xml

PARAMETER – *action uri poll interval*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the interval, in seconds, between calls from the phone to the "action uri poll".
FORMAT	Integer
DEFAULT VALUE	0 (disabled)
RANGE	N/A
EXAMPLE	action uri poll interval: 60

RING TONE AND TONE SET GLOBAL SETTINGS

PARAMETER – *ring tone*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Globally sets the type of ring tone on the IP phone. Ring tone can be set to one of 15 pre-defined rings (excluding silence) or one of 8 custom ringtones.
FORMAT	Integer
DEFAULT VALUE	0 (Tone 1)
RANGE2	Configuration Files 0 (Tone 1) 1 (Tone 2) 2 (Tone 3) 3 (Tone 4) 4 (Tone 5) 5 (Silent) 6 (Tone 7) 7 (Tone 8) 8 (Tone 9) 9 (Tone 10) 10 (Tone 11) 11 (Tone 12) 12 (Tone 13) 13 (Tone 14) 14 (Tone 15) 15 (Tone 16) 20 Velocity 21 Skyline 22 Rise 23 Daybreak 24 After Hours 25 Open Road 26 Pronto 27 Voyage 28 Bloom 29 Move 100 (Custom Ring Tone 1) 101 (Custom Ring Tone 2) 102 (Custom Ring Tone 3) 103 (Custom Ring Tone 4) 104 (Custom Ring Tone 5) 105 (Custom Ring Tone 6) 106 (Custom Ring Tone 7) 107 (Custom Ring Tone 8)
EXAMPLE	ring tone: 3

PARAMETER – *tone set*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Globally sets a tone set for a specific country.
FORMAT	Text
DEFAULT VALUE	US
RANGE	Australia Brazil Canada Europe (generic tones) France Germany Italy Italy2 Malaysia Mexico Russia Slovakia United Kingdom (UK) US
EXAMPLE	tone set: Germany

RING TONE PER-LINE SETTINGS

PARAMETER –	CONFIGURATION FILES
lineN ring tone (where N = line number)	startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Sets the type of ring tone on the IP phone on a per-line basis. Ring tone can be one of 15 pre-defined rings (excluding silence) or one of 8 custom ringtones.
FORMAT	Integer
DEFAULT VALUE	-1 (Global)
RANGE	-1 (Global) 0 (Tone 1) 1 (Tone 2) 2 (Tone 3) 3 (Tone 4) 4 (Tone 5) 5 (Silent) 6 (Tone 7) 7 (Tone 8) 8 (Tone 9) 9 (Tone 10) 10 (Tone 11) 11 (Tone 12) 12 (Tone 13) 13 (Tone 14) 14 (Tone 15) 15 (Tone 16) 20 Velocity 21 Skyline 22 Rise 23 Daybreak 24 After Hours 25 Open Road 26 Pronto 27 Voyage 28 Bloom 29 Move 100 (Custom Ring Tone 1) 101 (Custom Ring Tone 2) 102 (Custom Ring Tone 3) 103 (Custom Ring Tone 4) 104 (Custom Ring Tone 5) 106 (Custom Ring Tone 6) 107 (Custom Ring Tone 7)
EXAMPLE	line1 ring tone: 3

RINGING/RING BACK TIMEOUT PERIOD SETTINGS

PARAMETER – *ringback timeout*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the timeout period (in seconds) before the phone terminates the call. For outgoing calls, the originating phone will send a SIP CANCEL to stop the ringing at the destination phone after the timeout expires. For incoming calls, the terminating phone will send a SIP 486 Busy Here to stop the ringback at the originating phone after the timeout expires.
FORMAT	Integer
DEFAULT VALUE	300
RANGE	0 - 86400 (seconds)
EXAMPLE	ringback timeout: 600

CUSTOM RING TONE SETTINGS

For information on how to set a custom ring tone using the configuration files, see “Ring Tone and Tone Set Global Settings” on page A-195 or “Ring Tone Per-Line Settings” on page A-197.

PARAMETER – *custom ringtone N* (where N = 1 to 8)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the location and filename of the custom ringtone to be installed on the phone.
FORMAT	String (up to 256 characters) FTP “ftp://[username]:[password]@[server]:[port]/[path]/[filename.wav]” TFTP “tftp://[server]:[port]/[path]/[filename.wav]” HTTP “http://[server]:[port]/[path]/[filename.wav]” HTTPS “https://[server]:[port]/[path]/[filename.wav]”
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	custom ringtone 1: beep.wav

PARAMETER – *ringtone webui lock*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies if the Custom Ringtones menu (for ringtone installation) should be available in both User and Administrator Web UIs, available in the Administrator Web UI only, or unavailable in both User and Administrator Web UIs.
FORMAT	Integer
DEFAULT VALUE	0 (Disabled - Custom Ringtones menu available in both Web UIs)
RANGE	0 - 2 0 (Disabled - Available in both Administrator and User Web UIs) 1 (Available in Administrator Web UI, unavailable in User Web UI) 2 (Unavailable in both Administrator and User Web UIs).
EXAMPLE	ringtone webui lock: 2

RING TONE VIA SPEAKER DURING ACTIVE CALLS SETTINGS

PARAMETER – *ring audibly enable*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables/disables the feature whereby the ring tone of an incoming call is played through the IP phone's speaker if a user is on an active call. **Notes:** • Feature compatibility is dependent on the IP phone model (see Ring Tone via Speaker During Active Calls on page 5-142 for more information). • This feature is not supported when utilizing the headset audio mode. • With this feature enabled and when the phone's speaker is playing the incoming call's ring tone, call-waiting tones will not be played.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0-1 0 (disabled) 1 (enabled)
EXAMPLE	ring audibly enable: 1

NO SERVICE CONGESTION TONE SETTINGS

PARAMETER – *no service congestion tone*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	If enabled, the congestion tone will replace the conventional dial tone when the handset is off hook, a headset is employed, or the speakerphone is engaged. The congestion tone is played on a per line basis whereby only the specific lines that are without service are affected.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0-1 0 (disabled) 1 (enabled)
EXAMPLE	no service congestion tone: 1

STATUS CODE ON IGNORING INCOMING CALLS

PARAMETER – *sip ignore status code*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the status code that is sent in the response to the server when a user ignores an incoming call.
FORMAT	Integer
DEFAULT VALUE	486
RANGE	Valid SIP final negative response code (Refer to RFC3261)
EXAMPLE	sip ignore status code: 486

SWITCH FOCUS TO RINGING LINE

PARAMETER – *switch focus to ringing line*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not the UI focus is switched to a ringing line while the phone is in the connected state.
FORMAT	Boolean
DEFAULT VALUE	1 (enable)
RANGE	0 (disable) 1 (enable)
EXAMPLE	switch focus to ringing line: 1

CALL HOLD REMINDER SETTINGS

PARAMETER – *call hold reminder*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the reminder ring splash timer to start as soon as you put a call on hold (even when no other calls are active on the phone). When enabled, the phone initiates a reminder ring splash periodically for the single call on hold. When disabled, no reminder ring splash is audible.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (disable) 1 (enable)
EXAMPLE	call hold reminder: 1

PARAMETER – *call hold reminder during active calls*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the ability for the phone to initiate a continuous reminder tone on the active call when another call is on hold. For example, when the call on Line 1 is on hold, and the User answers a call on Line 2 and stays on that line, a reminder tone is played in the active audio path on Line 2 to remind the User that there is still a call on hold on Line 1. When this feature is disabled, a ring splash is heard when the active call hangs up and there is still a call on hold.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (disable) 1 (enable)
EXAMPLE	call hold reminder during active calls: 1

PARAMETER – *call hold reminder timer*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the time delay, in seconds, that a ring splash is heard on an active call when another call was placed on hold. For example, if a call comes into Line 1, and then a call comes into Line 2 and you answer Line 2, Line 1 is automatically placed on hold. While on the active Line 2, after 7 seconds, a ring splash audio sounds on the line reminding you that the call on Line 1 is still on hold. This timer begins to increment after Line 2 is answered. **Notes:** • This parameter is used with the “call hold reminder frequency” parameter. • You must enable this “call hold reminder timer” parameter for it to work. • A value of “0” disables the call hold reminder feature.
FORMAT	Integer
DEFAULT VALUE	7
RANGE	0-4294967295 seconds
EXAMPLE	call hold reminder timer: 10

PARAMETER – *call hold reminder frequency*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the time interval, in seconds, between each ring splash sound on the active line. For example, if a call comes into Line 1, and then a call comes into Line 2 and you answer Line 2, Line 1 is automatically placed on hold. While on the active Line 2, after 7 seconds, a ring splash audio sounds on the line reminding you that the call on Line 1 is still on hold (determined by the “call hold reminder timer” parameter), and then the ring splash is heard again after 60 seconds (determined by this parameter). **Notes:** • You must enable the “call hold reminder” and/or “call hold reminder during active calls” parameter(s), and the “call hold reminder timer” parameter, for this parameter to work. • A value of “0” prevents additional rings.
FORMAT	Integer
DEFAULT VALUE	60
RANGE	0-4294967295
EXAMPLE	call hold reminder frequency: 50

PREFERRED LINE AND PREFERRED LINE TIMEOUT

PARAMETER – *preferred line*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the preferred line to switch focus to when incoming or outgoing calls end on the phone.
FORMAT	Integer
DEFAULT VALUE	1
RANGE	0 (none - disables the preferred line focus feature) 1-2 (6863i) 1-24 (6865i/6867i/6869i/6873i)
EXAMPLE	preferred line: 2

PARAMETER – *preferred line timeout*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the time, in seconds, that the phone switches back to the preferred line after a call (incoming or outgoing) ends on the phone, or after a duration of inactivity on an active line.
FORMAT	Integer
DEFAULT VALUE	0 (the phone returns the line to the preferred line immediately)
RANGE	0-999
EXAMPLE	preferred line timeout: 30

GOODBYE KEY CANCELS INCOMING CALL

PARAMETER – *goodbye cancels incoming call*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enable or disables the behavior of the Goodbye Key on the IP phone. When you enable this parameter (1 = enable), the Goodbye key rejects the incoming call. When you disable this parameter (0 = disable), the Goodbye key hangs up the active call. For the 6867i, 6869i, and 6873i: If you enable this parameter, and the phone receives another call when an active call is already present, the phone displays “**answer**” and “**ignore**”. You can press the required softkey as applicable. For the 6863i and 6865i If you disable this parameter, and the phone receives another call when an active call is already present, the “**ignore**” option displays in the LCD window. The phone will ignore the incoming call if you press the **DOWN** arrow navigation key. The phone will hang up on the active call if you press the Goodbye key. **Note:** After enabling or disabling this feature, it takes affect on the phone immediately.
FORMAT	Boolean
DEFAULT VALUE	1 (true)
RANGE	0 (false) 1 (true)
EXAMPLE	goodbye cancels incoming call: 0

STUTTERED DIAL TONE SETTING

PARAMETER – *stutter disabled*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enable or disables the playing of a stuttered dial tone when there is a message waiting on the IP phone.
FORMAT	Boolean
DEFAULT VALUE	0 (false)
RANGE	0 (false) 1 (true)
EXAMPLE	stutter disabled: 1

MESSAGE WAITING INDICATOR SETTINGS

PARAMETER – *mwi led line*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to enable the Message Waiting Indicator (MWI) on a single line or on all lines on the phone. For example, if you set this parameter to 3, the LED illuminates if a voicemail is pending on line 3. If you set this parameter to 0, the LED illuminates if a voicemail is pending on any line on the phone. **Note:** To enable MWI for all lines in the configuration files, set this parameter to zero (0). The enable MWI for all lines in the Mitel Web UI, select “All” in the “Message Waiting Indicator Line” field.
FORMAT	Integer
DEFAULT VALUE	0 (all lines)
RANGE	0-2 (6863i) 0-24 (6865i/6867i/6869i/6873i)
EXAMPLE	mwi led line: 3

MESSAGE WAITING INDICATOR REQUEST URI SETTING

PARAMETER – *sip linex mwi request uri*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the URI to use when specifying which proxy server **Notes:** • Quotes (“) must be used to enclose the value when specifying it with this parameter. • Sip Explicit MWI Subscription must be enabled to use this feature.
FORMAT	“sip:user@host:port”
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	sip line1 mwi request uri: “sip:1020@10.50.224.53”

DND UI SETTINGS

Note: Applicable to the 6863i IP Phone only.

PARAMETER – *dnd ui*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether the DND option should be listed and available in the 6863i IP phone's Services menu for users to select. The DND option is available by default. Defining this parameter as "0" will remove the DND option from the Services menu.
FORMAT	Boolean
DEFAULT VALUE	1 (True)
RANGE	0 (False) 1 (True)
EXAMPLE	dnd ui: 0

DND KEY MODE SETTINGS

PARAMETER – *dnd key mode*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Sets the mode for how the phone uses "do not disturb" (DND): • **account** - Sets DND for a specific account. DND key toggles the account in focus on the IP Phone UI, to ON or OFF. • **phone** - Sets DND ON for all accounts on the phone. DND key toggles all accounts on the phone to ON or OFF. • **custom -** Sets the phone to display custom screens after pressing the DND key, that list the account(s) on the phone. The user can select a specific account for DND, turn DND ON for all accounts, or turn DND OFF for all accounts. **Notes:** • If there is only one account configured on the phone, then the mode setting is ignored and the phone behaves as if the mode was set to "Phone". • You must configure a DND key on the phone to use this feature. To configure a DND key, see "Softkey/Programmable Key/Keypad Key/Expansion Module Key/Hard Key Parameters" on page A-248.
FORMAT	Integer
DEFAULT VALUE	1 (phone)
RANGE	0 (account) 1 (phone) 2 (custom)
EXAMPLE	dnd key mode: 2

The following is an example of configuring the mode for DND in the configuration files:

```
dnd key mode: 2
softkey1 type: dnd
softkey1 states: idle connected incoming outgoing busy
```

In the above example, softkey 1 is configured for DND for line 1 only, with a "**custom**" configuration. Pressing softkey 1 displays DND screens for which you can customize on the phone.

PRIORITY ALERT SETTINGS

PARAMETER – *priority alerting enabled*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables and disables distinctive ringing on the IP phone for incoming calls and call-waiting calls.
FORMAT	Boolean
DEFAULT VALUE	1 (true)
RANGE	0 (false) 1 (true)
EXAMPLE	priority alerting enabled: 0

FOR SYLANTRO SERVER ONLY

PARAMETER – *alert auto call distribution*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	When an "alert-acd" keyword appears in the header of the INVITE request, the configured Bellcore ring tone is applied to the IP phone.
FORMAT	Integer
DEFAULT VALUE	0 Normal ringing
RANGE	0 Normal ringing (default) 1 Bellcore-dr2 2 Bellcore-dr3 3 Bellcore-dr4 4 Bellcore-dr5 5 Silent
EXAMPLE	alert auto call distribution: 2

PARAMETER – *alert community 1*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	When an "alert-community-1" keyword appears in the header of the INVITE request, the configured Bellcore ring tone is applied to the IP phone.
FORMAT	Integer
DEFAULT VALUE	0 Normal ringing
RANGE	0 Normal ringing (default) 1 Bellcore-dr2 2 Bellcore-dr3 3 Bellcore-dr4 4 Bellcore-dr5 5 Silent
EXAMPLE	alert community 1: 3

PARAMETER – *alert community 2*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	When an "alert-community-2" keyword appears in the header of the INVITE request, the configured Bellcore ring tone is applied to the IP phone.
FORMAT	Integer
DEFAULT VALUE	0 Normal ringing
RANGE	0 Normal ringing (default) 1 Bellcore-dr2 2 Bellcore-dr3 3 Bellcore-dr4 4 Bellcore-dr5 5 Silent
EXAMPLE	alert community 2: 4

PARAMETER – *alert community 3*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	When an "alert-community-3" keyword appears in the header of the INVITE request, the configured Bellcore ring tone is applied to the IP phone.
FORMAT	Integer
DEFAULT VALUE	0 Normal ringing
RANGE	0 Normal ringing (default) 1 Bellcore-dr2 2 Bellcore-dr3 3 Bellcore-dr4 4 Bellcore-dr5 5 Silent
EXAMPLE	alert community 3: 1

PARAMETER – *alert community 4*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	When an "alert-community-4" keyword appears in the header of the INVITE request, the configured Bellcore ring tone is applied to the IP phone.
FORMAT	Integer
DEFAULT VALUE	0 Normal ringing
RANGE	0 Normal ringing (default) 1 Bellcore-dr2 2 Bellcore-dr3 3 Bellcore-dr4 4 Bellcore-dr5 5 Silent
EXAMPLE	alert community 4: 2

PARAMETER – *alert external*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	When an "alert-external" keyword appears in the header of the INVITE request, the configured Bellcore ring tone is applied to the IP phone.
FORMAT	Integer
DEFAULT VALUE	0 Normal ringing
RANGE	0 Normal ringing (default) 1 Bellcore-dr2 2 Bellcore-dr3 3 Bellcore-dr4 4 Bellcore-dr5 5 Silent
EXAMPLE	alert external: 4

PARAMETER – *alert emergency*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	When an "alert-emergency" keyword appears in the header of the INVITE request, the configured Bellcore ring tone is applied to the IP phone.
FORMAT	Integer
DEFAULT VALUE	0 Normal ringing
RANGE	0 Normal ringing (default) 1 Bellcore-dr2 2 Bellcore-dr3 3 Bellcore-dr4 4 Bellcore-dr5 5 Silent
EXAMPLE	alert emergency: 4

PARAMETER – *alert group*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	When an "alert-group" keyword appears in the header of the INVITE request, the configured Bellcore ring tone is applied to the IP phone.
FORMAT	Integer
DEFAULT VALUE	0 Normal ringing
RANGE	0 Normal ringing (default) 1 Bellcore-dr2 2 Bellcore-dr3 3 Bellcore-dr4 4 Bellcore-dr5 5 Silent
EXAMPLE	alert group: 4

PARAMETER – *alert internal*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	When an "alert-internal" keyword appears in the header of the INVITE request, the configured Bellcore ring tone is applied to the IP phone.
FORMAT	Integer
DEFAULT VALUE	0 Normal ringing
RANGE	0 Normal ringing (default) 1 Bellcore-dr2 2 Bellcore-dr3 3 Bellcore-dr4 4 Bellcore-dr5 5 Silent
EXAMPLE	alert internal: 4

PARAMETER – *alert priority*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	When an "alert-priority" keyword appears in the header of the INVITE request, the configured Bellcore ring tone is applied to the IP phone.
FORMAT	Integer
DEFAULT VALUE	0 Normal ringing
RANGE	0 Normal ringing (default) 1 Bellcore-dr2 2 Bellcore-dr3 3 Bellcore-dr4 4 Bellcore-dr5 5 Silent
EXAMPLE	alert priority: 4

BELLCORE CADENCE SETTINGS

PARAMETER – *bellcore cadence dr2*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Sets the cadence for Bellcore-dr2. **Note:** You can define up to 8 cadence rings. The value of -1 indicates “do not repeat”.
FORMAT	Integer
DEFAULT VALUE	800,400, 800,4000
RANGE	N/A
EXAMPLE	bellcore cadence dr2: 800, 400, 800, 4000

PARAMETER – *bellcore cadence dr3*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Sets the cadence for Bellcore-dr3. **Note:** You can define up to 8 cadence rings. The value of -1 indicates “do not repeat”.
FORMAT	Integer
DEFAULT VALUE	400,200,400,200,800,4000
RANGE	N/A
EXAMPLE	bellcore cadence dr3: 400,200,400,200,800,4000

PARAMETER – *bellcore cadence dr4*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Sets the cadence for Bellcore-dr4. **Note:** You can define up to 8 cadence rings. The value of -1 indicates “do not repeat”.
FORMAT	Integer
DEFAULT VALUE	300,200,1000,200,300,4000
RANGE	N/A
EXAMPLE	bellcore cadence dr4: 300,200,1000,200,300,300,200,4000

PARAMETER – *bellcore cadence dr5*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Sets the cadence for Bellcore-dr5. **Note:** You can define up to 8 cadence rings. The value of -1 indicates “do not repeat”.
FORMAT	Integer
DEFAULT VALUE	500,-1
RANGE	N/A
EXAMPLE	bellcore cadence dr5: 500,-1

SIP DIVERSION DISPLAY

GLOBAL SETTING

PARAMETER – *sip diversion display*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	If enabled, when an outgoing call is being diverted to another destination the phone displays the Caller ID of the new destination and the reason for the call diversion. Similarly, for incoming diverted calls, the Caller ID of the original call destination displays. If disabled, the reason for the call diversion on outgoing diverted calls, and the Caller ID of the original call destination on incoming diverted calls is not displayed. **Notes:** • This is a global parameter. • You must restart the phone after setting a value for this parameter.
FORMAT	Boolean
DEFAULT VALUE	1
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sip diversion display: 0

PER-LINE SETTING

PARAMETER – *sip lineN diversion display* (where N = line number)	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	If enabled, when an outgoing call is being diverted to another destination the phone displays the Caller ID of the new destination and the reason for the call diversion. Similarly, for incoming diverted calls, the Caller ID of the original call destination displays. If disabled, the reason for the call diversion on outgoing diverted calls, and the Caller ID of the original call destination on incoming diverted calls is not displayed. **Notes:** • This parameter is used to configure a specific line. • You must restart the phone after setting a value for this parameter.
FORMAT	Boolean
DEFAULT VALUE	1
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sip line1 diversion display: 0

DISPLAY OF CALL DESTINATION FOR INCOMING CALLS

PARAMETER – *show call destination name*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enable/disables the display of the call destination name to the LCD on the phone during incoming calls.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	show call destination name: 1

DISPLAY NAME CUSTOMIZATION SETTINGS

PARAMETER – *directory lookup suppression pattern*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows a pattern-based configuration whereby if the configured pattern is found in the From header display name of an incoming call, the phone bypasses the local directory lookup and shows the display name as intended by the call manager (i.e. as specified in the From header). Patterns that can be defined include: • “-->x+” • “==>x+” • “@@@x+” • “aaax+” **Notes:** • Use | to specify multiple OR combined patterns. • Quotation marks must be used when defining the pattern.
FORMAT	String
DEFAULT VALUE	NA
RANGE	NA
EXAMPLE	directory lookup suppression pattern: “-->x+|==>x+|aaax+”

LANGUAGE SETTINGS

PARAMETER – *language*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The language you want to display for the IP Phone UI. Valid values for all phones are: • 0 (English) default • 1-4 The values 1-4 are dependent on the "**Language N**" parameter. For example, if "language 1: lang_fr.txt", then "language: 1" would set the IP phone UI language to French. **Note:** All languages may not be available for selection. The available languages are dependent on the language packs currently loaded to the IP phone. For more information about loading language packs, see "Loading Language Packs" on page 5-62.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 to 4 (all phones)
EXAMPLE	language: 1

PARAMETER – *web language*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The language you want to display for the Mitel Web UI. Valid values for all phones are: • 0 (English) default • 1-4 The values 1-4 are dependent on the "**Language N**" parameter. For example, if "language 1: lang_fr.txt", then "language: 1" would set the webpage language to French. **Note:** All languages may not be available for selection. The available languages are dependent on the language packs currently loaded to the IP phone. For more information about loading language packs, see "Loading Language Packs" on page 5-62.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 to 4
EXAMPLE	web language: 1

PARAMETER – *input language*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to specify the language to use for inputs on the IP Phone. Entering a language value for this parameter allows users to enter text and characters in the IP Phone UI and in XML applications via the keypad on the phone (or for the 6873i on-screen keyboard), in the language(s) specified.
FORMAT	Text
DEFAULT VALUE	English
RANGE	Valid values are: • English • French • Français • German • Deutsch • Greek (6867i, 6869i, and 6873i only) • ελληνικά (6867i, 6869i, and 6873i only) • Italian • Italiano • Spanish • Español • Portuguese • Português • Russian • Русский • Nordic
EXAMPLE	input language: French

LANGUAGE PACK SETTINGS

PARAMETER – *language N* Where "N" can be 1, 2, 3, or 4	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The language pack you want to load to the IP phone. Valid values are: • lang_ca.txt (Catalan) • lang_ca_va.txt (Valencian) • lang_cs.txt (Czech - UTF-8) • lang_cs_op.txt (Czech - ASCII) • lang_cy.txt (Welsh) • lang_de.txt (German) • lang_da.txt (Danish) • lang_el.txt (Greek - 6867i, 6869i, and 6873i only) • lang_es.txt (Spanish) • lang_es_mx.txt (Mexican Spanish) • lang_eu.txt (Euskera) • lang_fi.txt (Finnish) • lang_fr.txt (French) • lang_fr_ca.txt (Canadian French) • lang_gl.txt (Galego) • lang_hu.txt (Hungarian) • lang_it.txt (Italian) • lang_nl.txt (Dutch) • lang_nl_nl.txt (Dutch - Netherlands) • lang_no.txt (Norwegian) • lang_pl.txt (Polish - ASCII) • lang_pl_pl.txt (Polish - UTF-8) • lang_pt.txt (Portuguese) • lang_pt_br.txt (Brazilian Portuguese) • lang_ro.txt (Romanian) • lang_ru.txt (Russian) • lang_sk.txt (Slovak - UTF-8) • lang_sk_op.txt (Slovak - ASCII) • lang_sv.txt (Swedish) • lang_tr.txt (Turkish)

You can use this parameter in three ways:

- To download no language packs
- To download a language pack(s) from the original configuration server
- To download a language pack(s) from another specified server

Notes:

- The languages packs you load are dependent on available language packs from the configuration server. For more information about loading language packs, see “Loading Language Packs” on page 5-62.
- You must reboot the phone to load a language pack.
- To download a specific file, the string value MUST HAVE A FILENAME at the end of the string. For example:

  language 1:ftp://admin:admin!@1.2.3.4:50/path/lang_de.txt
  where “path” is the directory and “lang_de.txt” is the filename. If you do not specify a filename, the download fails.

See examples for each below.

FORMAT	lang_<ISO 639>_<ISO 3166>.txt or lang_<ISO 639>.txt **Note:** For valid values for <ISO 639> and <ISO 3166>, see “Language Codes (from Standard ISO 639)” on page A-220 and “Country Codes (from Standard ISO 3166)” on page A-221.
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	The following example downloads no language pack file: • language 1: The following example downloads the German language pack to the phones from the original configuration server: • language 1: lang_de.txt The following example uses FTP to download the firmware file “lang_de.txt” (German language pack) from the “path” directory on server 1.2.3.4 using port 50: • language 1:ftp://admin:admin!@1.2.3.4:50/path/lang_de.txt

The following table identifies the language code to use for the IP phone language packs.

LANGUAGE CODES (FROM STANDARD ISO 639)

LANGUAGE	LANGUAGE CODE
English	en
Czech (UTF-8)	cs
Czech (ASCII)	cs_op
Catalan	ct
Valencian*	ct_va
Welsh	cy
German	de
Danish	da
Greek	el
Spanish	es
Mexican Spanish	es_mx
Euskera	eu
Finnish	fi
French	fr
Canadian French	fr_ca
Galego	gl
Hungarian	hu
Italian	it
Dutch	nl
Dutch (Netherlands)	nl_nl
Norwegian	no
Polish (ASCII)	pl
Polish (UTF-8)	pl_pl
Portuguese	pt
Portuguese Brazilian	pt_br
Romanian	ro
Russian	ru
Slovak (UTF-8)	sk
Slovak (ASCII)	sk_op
Swedish	sv
Turkish	tr

The following table identifies the country codes to use for the IP phone language packs. Not all country code are applicable.

COUNTRY CODES (FROM STANDARD ISO 3166)

COUNTRY	COUNTRY CODE
AFGHANISTAN	AF
ÅLAND ISLANDS	AX
ALBANIA	AL
ALGERIA	DZ
AMERICAN SAMOA	AS
ANDORRA	AD
ANGOLA	AO
ANGUILLA	AI
ANTARCTICA	AQ
ANTIGUA AND BARBUDA	AG
ARGENTINA	AR
ARMENIA	AM
ARUBA	AW
AUSTRALIA	AU
AUSTRIA	AT
AZERBAIJAN	AZ
BAHAMAS	BS
BAHRAIN	BH
BANGLADESH	BD
BARBADOS	BB
BELARUS	BY
BELGIUM	BE
BELIZE	BZ
BENIN	BJ
BERMUDA	BM
BHUTAN	BT
BOLIVIA	BO
BOSNIA AND HERZEGOVINA	BA
BOTSWANA	BW
BOUVET ISLAND	BV
BRAZIL	BR
BRITISH INDIAN OCEAN TERRITORY	IO
BRUNEI DARUSSALAM	BN
BULGARIA	BG
BURKINA FASO	BF
BURUNDI	BI

COUNTRY	COUNTRY CODE
CAMBODIA	KH
CAMEROON	CM
CANADA	CA
CAPE VERDE	CV
CAYMAN ISLANDS	KY
CENTRAL AFRICAN REPUBLIC	CF
CHAD	TD
CHILE	CL
CHINA	CN
CHRISTMAS ISLAND	CX
COCOS (KEELING) ISLANDS	CC
COLOMBIA	CO
COMOROS	KM
CONGO	CG
CONGO, THE DEMOCRATIC REPUBLIC OF THE	CD
COOK ISLANDS	CK
COSTA RICA	CR
CÔTE D'IVOIRE	CI
CROATIA	HR
CUBA	CU
CYPRUS	CY
CZECH REPUBLIC	CZ
DENMARK	DK
Dhcp (see Chapter 4, the section, "DHCP Time Offset (Option 2) Support" on page 5-24)	DP DJ
DJIBOUTI	DM
DOMINICA	DO
DOMINICAN REPUBLIC	
ECUADOR	EC
EGYPT	EG
EL SALVADOR	SV
EQUATORIAL GUINEA	GQ
ERITREA	ER
ESTONIA	EE
ETHIOPIA	ET
FALKLAND ISLANDS (MALVINAS)	FK
FAROE ISLANDS	FO
FIJI	FJ
FINLAND	FI
FRANCE	FR
FRENCH GUIANA	GF
FRENCH POLYNESIA	PF
FRENCH SOUTHERN TERRITORIES	TF

COUNTRY	COUNTRY CODE
GABON	GA
GAMBIA	GM
GEORGIA	GE
GERMANY	DE
GHANA	GH
GIBRALTAR	GI
GREECE	GR
GREENLAND	GL
GRENADA	GD
GUADELOUPE	GP
GUAM	GU
GUATEMALA	GT
GUERNSEY	GG
GUINEA	GN
GUINEA-BISSAU	GW
GUYANA	GY
HAITI	HT
HEARD ISLAND AND MCDONALD ISLANDS	HM
HOLY SEE (VATICAN CITY STATE)	VA
HONDURAS	HN
HONG KONG	HK
HUNGARY	HU
ICELAND	IS
INDIA	IN
INDONESIA	ID
IRAN, ISLAMIC REPUBLIC OF	IR
IRAQ	IQ
IRELAND	IE
ISLE OF MAN	IM
ISRAEL	IL
ITALY	IT
JAMAICA	JM
JAPAN	JP
JERSEY	JE
JORDAN	JO
KAZAKHSTAN	KZ
KENYA	KE
KIRIBATI	KI
KOREA, DEMOCRATIC PEOPLE'S REPUBLIC OF	KP
KOREA, REPUBLIC OF	KR
KUWAIT	KW
KYRGYZSTAN	KG

COUNTRY	COUNTRY CODE
LAO PEOPLE'S DEMOCRATIC REPUBLIC	LA
LATVIA	LV
LEBANON	LB
LESOTHO	LS
LIBERIA	LR
LIBYAN ARAB JAMAHIRIYA	LY
LIECHTENSTEIN	LI
LITHUANIA	LT
LUXEMBOURG	LU
MACAO	MO
MACEDONIA, THE FORMER YUGOSLAV REPUBLIC OF	MK
MADAGASCAR	MG
MALAWI	MW
MALAYSIA	MY
MALDIVES	MV
MALI	ML
MALTA	MT
MARSHALL ISLANDS	MH
MARTINIQUE	MQ
MAURITANIA	MR
MAURITIUS	MU
MAYOTTE	YT
MEXICO	MX
MICRONESIA, FEDERATED STATES OF	FM
MOLDOVA, REPUBLIC OF	MD
MONACO	MC
MONGOLIA	MN
MONTENEGRO	ME
MONTSERRAT	MS
MOROCCO	MA
MOZAMBIQUE	MZ
MYANMAR	MM

COUNTRY	COUNTRY CODE
NAMIBIA	NA
NAURU	NR
NEPAL	NP
NETHERLANDS	NL
NETHERLANDS ANTILLES	AN
NEW CALEDONIA	NC
NEW ZEALAND	NZ
NICARAGUA	NI
NIGER	NE
NIGERIA	NG
NIUE	NU
NORFOLK ISLAND	NF
NORTHERN MARIANA ISLANDS	MP
NORWAY	NO
OMAN	OM
PAKISTAN	PK
PALAU	PW
PALESTINIAN TERRITORY, OCCUPIED	PS
PANAMA	PA
PAPUA NEW GUINEA	PG
PARAGUAY	PY
PERU	PE
PHILIPPINES	PH
PITCAIRN	PN
POLAND	PL
PORTUGAL	PT
PUERTO RICO	PR
QATAR	QA
RÉUNION	RE
ROMANIA	RO
RUSSIAN FEDERATION	RU
RWANDA	RW

COUNTRY	COUNTRY CODE
SAINT HELENA	SH
SAINT KITTS AND NEVIS	KN
SAINT LUCIA	LC
SAINT PIERRE AND MIQUELON	PM
SAINT VINCENT AND THE GRENADINES	VC
SAMOA	WS
SAN MARINO	SM
SAO TOME AND PRINCIPE	ST
SAUDI ARABIA	SA
SENEGAL	SN
SERBIA	RS
SEYCHELLES	SC
SIERRA LEONE	SL
SINGAPORE	SG
SLOVAKIA	SK
SLOVENIA	SI
SOLOMON ISLANDS	SB
SOMALIA	SO
SOUTH AFRICA	ZA
SOUTH GEORGIA AND THE SOUTH SANDWICH ISLANDS	GS
SPAIN	ES
SRI LANKA	LK
SUDAN	SD
SURINAME	SR
SVALBARD AND JAN MAYEN	SJ
SWAZILAND	SZ
SWEDEN	SE
SWITZERLAND	CH
SYRIAN ARAB REPUBLIC	SY
TAIWAN, PROVINCE OF CHINA	TW
TAJIKISTAN	TJ
TANZANIA, UNITED REPUBLIC OF	TZ
THAILAND	TH
TIMOR-LESTE	TL
TOGO	TG
TOKELAU	TK
TONGA	TO
TRINIDAD AND TOBAGO	TT
TUNISIA	TN
TURKEY	TR
TURKMENISTAN	TM
TURKS AND CAICOS ISLANDS	TC
TUVALU	TV

COUNTRY	COUNTRY CODE
UGANDA	UG
UKRAINE	TA
UNITED ARAB EMIRATES	AE
UNITED KINGDOM	GB
UNITED STATES	US
UNITED STATES MINOR OUTLYING ISLANDS	TM
URUGUAY	UY
UZBEKISTAN	UZ
VANUATU	VU
Vatican City State	see HOLY SEE
VENEZUELA	VE
VIET NAM	VN
VIRGIN ISLANDS, BRITISH	VG
VIRGIN ISLANDS, U.S.	VI
WALLIS AND FUTUNA	WF
WESTERN SAHARA	EH
YEMEN	YE
Zaire	see CONGO, THE DEMOCRATIC REPUBLIC OF THE
ZAMBIA	ZM
ZIMBABWE	ZW

SUPPRESS DTMF PLAYBACK SETTING

PARAMETER – *suppress dtmf playback*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables and disables suppression of DTMF playback when a number is dialed from the softkeys or programmable keys. When you disable the suppression of DTMF playback and you press a softkey or programmable key, the IP phone dials the stored number and displays each digit as dialed in the LCD window. When you enable the suppression of DTMF playback, the IP phone dials the stored number and displays the entire number immediately in the LCD window, allowing the call to be dialed faster.
FORMAT	Boolean
DEFAULT VALUE	1 (enabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	suppress dtmf playback: 0

DISPLAY DTMF DIGITS SETTING

PARAMETER – *display dtmf digits*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables and disables the display of DTMF digits when dialing on the IP phone. DTMF is the signal sent from the phone to the network that you generate when you press the phone’s touch keys. This is also known as “touchtone” dialing. Each key you press on your phone generates two tones of specific frequencies. One tone is generated from a high-frequency group of tones and the other from a low frequency group. If enabled, this parameter displays the digits on the IP phone display if you are dialing from the keypad, or from a softkey or programmable key. This parameter is disabled by default (no digits display when dialing).
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	display dtmf digits: 1

FILTER OUT INCOMING DTMF EVENTS

PARAMETER – *suppress incoming dtmf playback*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Suppress playback of both SIP INFO and RFC2833 DTMF tones.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0-1 0 (Disabled) 1 (Enabled)
EXAMPLE	suppress incoming dtmf playback:1

MUTE DTMF PLAYBACK SETTINGS

PARAMETER – *mute dtmf playback*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	A feature on the IP phones allows administrators to enable or disable the mute of local DTMF playback tone when the phone is in **Dialing** or **Offhook** state.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0-1 0 (Disabled) 1 (Enabled)
EXAMPLE	mute dtmf playback: 1

INTERCOM, AUTO-ANSWER, AND BARGE IN SETTINGS

OUTGOING INTERCOM SETTINGS

PARAMETER – *sip intercom type*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Determines whether the IP phone or the server is responsible for notifying the recipient that an Intercom call is being placed.
FORMAT	Integer
DEFAULT VALUE	3 - Off
RANGE	1 - Phone-Side 2 - Server-Side 3 - Off
EXAMPLE	sip intercom type: 1

PARAMETER – *sip intercom prefix code*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The prefix to add to the phone number for server-side outgoing Intercom calls. This parameter is required for all server-side Intercom calls. **Note:** The example below shows *96 for the prefix code which is used for Sylantro servers.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	sip intercom prefix code: *96

PARAMETER – *sip intercom line*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the line for which the IP phone uses the configuration from, when making the Intercom call. The IP phone uses the first available line for physically making the call but uses the configuration from the line you set for this parameter. **Note:** The "*sip intercom type*" parameter must be set with the **Server-Side** option to enable the "*sip intercom line*" parameter.
FORMAT	Integer
DEFAULT VALUE	1
RANGE	0-2 (6863i) 0-24 (6865i/6867i/6869i/6873i)
EXAMPLE	sip intercom line: 1

INCOMING INTERCOM SETTINGS

PARAMETER – *sip allow auto answer*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the IP phone to allow automatic answering for an Intercom call. If auto-answer is enabled on the IP phone, the phone plays a tone to alert the user before answering the intercom call. If auto-answer is disabled, the phone treats the incoming intercom call as a normal call.
FORMAT	Boolean
DEFAULT VALUE	1 (true)
RANGE	0 (false - do not allow auto-answer) 1 (true - allow auto-answer)
EXAMPLE	sip allow auto answer: 0

PARAMETER – *sip intercom mute mic*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the microphone on the IP phone for Intercom calls made by the originating caller.
FORMAT	Integer
DEFAULT VALUE	1 (true)
RANGE	0 (false - microphone is not muted) 1 (true - microphone is muted)
EXAMPLE	sip intercom mute mic: 1

PARAMETER – *sip intercom warning tone*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables a warning tone to play when the phone receives an incoming intercom call on an active line.
FORMAT	Integer
DEFAULT VALUE	1 (true)
RANGE	0 (false - warning tone will not play) 1 (true - warning tone will play)
EXAMPLE	sip intercom warning tone: 0

PARAMETER – sip intercom allow barge in	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enable or disables how the phone handles incoming intercom calls while the phone is on an active call as well as how the phone handles multicast paging calls while the phone is in a dialing state. When you enable this parameter, an incoming intercom call takes precedence over any active call, by placing the active call on hold and automatically answering the intercom call. Also when enabled, for multicast pages during a dialing state, the phone will automatically switch focus to the multicast page screen. When you disable this parameter and there is an active call, the phone treats an incoming intercom call like a normal call and plays the call warning tone. Also when disabled, for multicast pages during a dialing state, the phone will keep its focus on the dialing screen.
FORMAT	Boolean
DEFAULT VALUE	1 (Enabled)
RANGE	0 - 1 0 (Disabled) 1 (Enabled)
EXAMPLE	sip intercom allow barge in: 0

AUDIO SWITCHING SUPPORT FOR INTERCOM CALLS

PARAMETER – *action uri answericom*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the URI, for which the phone executes a GET on when user switches one way audio intercom to two way audio intercom by pressing the "AnswerIcom" softkey or the scroll down key.
FORMAT	String
DEFAULT VALUE	" "
RANGE	Same as other action uri.
EXAMPLE	action uri answericom: http://http-server-ip/aastraSipTerm.xml?requestType=answericom

ENABLE MICROPHONE DURING EARLY MEDIA

PARAMETER – *sip early media mute mic*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the microphone while in early media.
FORMAT	Boolean
DEFAULT VALUE	1 (disabled)
RANGE	0-1 0 (enables mic during early media) 1 (disables mic during early media)
EXAMPLE	sip early media mute mic: 0

CODEC NEGOTIATION BEHAVIOR

PARAMETER – *sip single codec reply in sdp*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether the phone should reply to and SDP Offer (with several codecs defined in the media stream) with an SDP Answer containing all the codecs present in the Offer (as per RFC 3264) or with an SDP Answer containing just one preferred codec (as per 3GPP TS 24.229).
FORMAT	Boolean
DEFAULT VALUE	0 (Disabled)
RANGE	0-1 0 (Disabled - RFC 3264) 1 (Enabled - 3GPP TS 24.229)
EXAMPLE	sip single codec reply in sdp: 1

GROUP PAGING RTP SETTINGS

PARAMETER – *paging group listening*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the multicast address(es) and the port(s) on which the phone listens for incoming multicast RTP packets. **Note:** If this field is blank, Paging listening capability is disabled on the phone.
FORMAT	IP Address in dotted decimal format/Port #
DEFAULT VALUE	N/A
RANGE	The valid port range is from 1 to 65535.
EXAMPLE	paging group listening: 224.0.0.2:10000,239.0.1.20:15000

Example: The following is an example of configuring RTP streaming for Paging applications using the configuration files:

```
paging group listening: 224.0.0.2:10000,239.0.1.20:15000
softkey1 type: paging
softkey1 label: group 1
softkey1 value: 224.0.0.2:10000
```

AUDIO TRANSMIT AND RECEIVE GAIN ADJUSTMENTS

PARAMETER – *headset sidetone gain*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Disables the sidetone on the analog headset of the phone.
FORMAT	Integer
DEFAULT VALUE	-2000
RANGE	-1000 db will disable the sidetone on the analog headset of the phone. Any value other than -1000 will be ignored, and will have no impact. This implies that by default this parameter will have no impact as default value is -2000.
EXAMPLE	headset sidetone gain: -1000

PARAMETER – *handset sidetone gain*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Disables the sidetone on the analog handset of the phone.
FORMAT	Integer
DEFAULT VALUE	-2000

RANGE	-1000 db will disable the sidetone on the analog handset of the phone. Any value other than -1000 will be ignored, and will have no impact. This implies that by default this parameter will have no impact as default value is -2000.
EXAMPLE	handset sidetone gain: -1000

PARAMETER – *audio mode*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to configure how the "handsfree" button on the IP phone operates.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	**0.** Speaker - This is the default setting. Calls can be made or received using the handset or handsfree speakerphone. In handset audio mode, pressing the handsfree button on the phone switches to handsfree speakerphone. In Speaker audio mode, lift the handset to switch to the handset. **1**. Headset - Choose this setting if you want to make or receive all calls using a handset or headset. For the 6865i, 6867i, 6869i, and 6873i, calls can be switched from the handset to headset by pressing the handsfree button on the phone. To switch from the headset to the handset, lift the handset. **2**. Speaker/Headset - Incoming calls are sent to the handsfree speakerphone first when the handsfree button is pressed. By pressing the handsfree button again, you can switch back and forth between the handsfree speakerphone and the headset. For the 6865i, 6867i, 6869i, and 6873i lifting the handset at any time switches back to the handset from either the handsfree speakerphone or the headset. **3**. Headset/Speaker - Incoming calls are sent to the headset first when the handsfree button is pressed. By pressing the handsfree button again, you can switch back and forth between the headset and the handsfree speakerphone. For the 6865i, 6867i, 6869i, and 6873i lifting the handset at any time switches back to the handset from either the headset or the handsfree speakerphone.
EXAMPLE	audio mode: 2

AUDIO MODE VOLUME

PARAMETER – *ringer volume*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the ringer volume level
FORMAT	Integer
DEFAULT VALUE	5
RANGE	0-9
EXAMPLE	ringer volume: 1

PARAMETER – *handset volume*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the handset volume level
FORMAT	Integer
DEFAULT VALUE	4
RANGE	0-9
EXAMPLE	handset volume: 1

PARAMETER – *speaker volume*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the speaker volume level
FORMAT	Integer
DEFAULT VALUE	4
RANGE	0-9
EXAMPLE	speaker volume: 1

PARAMETER – *headset volume*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the headset volume level
FORMAT	Integer
DEFAULT VALUE	4
RANGE	0-9
EXAMPLE	headset volume: 1

DISABLE USER LOGIN TO MITEL WEB UI

PARAMETER – *web interface enabled*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not to disable the web user interface
FORMAT	Integer

DEFAULT VALUE	1 (admin/user enabled)
RANGE	0 (admin/user disabled) 1 (admin/user enabled) 2 (only admin enabled)
EXAMPLE	web interface enabled: 0

MINIMUM RINGER VOLUME

PARAMETER – *ringer volume minimum*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the minimum ringer volume level
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0-9
EXAMPLE	ringer volume minimum: 1

TERMINATED CALLS INDICATOR

PARAMETER – *far end disconnect timer*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not the phone displays an indication of a terminated call. If set to 0, this feature is disabled and the phone does not display the “Call Terminated” screen. If you specify a value for this parameter other than “0”, the “Call Terminated” screen displays for the configured time interval. The audible busy tone also plays for the configured time interval specified.
FORMAT	Integer
DEFAULT VALUE	0 (disabled)
RANGE	0 to 86400 seconds
EXAMPLE	far end disconnect timer: 5

DIRECTED CALL PICKUP (BLF OR XML CALL INTERCEPTION) SETTINGS

PARAMETER – *directed call pickup*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the use of "directed call pickup" feature.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	directed call pickup: 1

PARAMETER – *enhanced directed call pickup*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables the enhanced BLF directed call pickup feature. If defined as "1", pressing a softkey corresponding to a ringing BLF will not pick up the call immediately but will instead display the remote caller's information first, allowing the user to review who is calling. When using the MiCloud Telepo platform, the parameter must be defined as "3". In this mode, pressing a BLF key when the monitored extension is ringing will cause the phone use the dialog information sent in the NOTIFY message to form the INVITE request (the dialog information will be detailed in the "Replaces" header of the INVITE). **Notes:** • Feature availability is dependent on your call manager. • Applicable to the 6865i, 6867i, 6869i, 6873i IP phones only.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 - 3 0 (disabled) 1 (two-stage BLF for non-ALU call managers) 2 (reserved) 3 (directed call pickup for MiCloud Telepo)
EXAMPLE	enhanced directed call pickup: 3

PARAMETER – *directed call pickup prefix*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to enter a specific prefix string (depending on what is available on your server), that the phone automatically dials when dialing the Directed Call Pickup number. For example, for BroadSoft servers, you can enter a value of ***98** for the "**directed call pickup prefix**". For Asterisk servers, you can enter a value of ***76**. For sipXecs proxy servers, you can enter a value of ***78**. When the phone performs the Directed Call Pickup after pressing a BLF or BLF/List softkey, the phone prepends the *98 value to the designated extension of the BLF or BLF/List softkey when dialing out. **Notes:** • The default method for the phone to use is Directed Call Pickup over BLF if the server provides applicable information. If the Directed Call Pickup over BLF information is missing in the messages to the server, the Directed Call Pickup by Prefix method is used if a value for the prefix code exists in the configuration. • You can define only one prefix, which will be applicable to all BLF- or BLF/List-monitored extensions. • The phone that picks up displays the prefix code + the extension number (for example, *981234 where prefix key = *98, extension = 1234). • Symbol characters are allowed (for example "*").
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	directed call pickup prefix: *98

ACD AUTO-AVAILABLE TIMER SETTINGS

Note: Applicable to the 6865i, 6867i, 6869i, and 6873i IP Phones only.

PARAMETER – *acd auto available*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the use of the ACD Auto-Available Timer.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	acd auto available: 1

PARAMETER – *acd auto available timer*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the length of time, in seconds, before the IP phone status switches back to “available.”
FORMAT	Integer
DEFAULT VALUE	60 (seconds)
RANGE	0 to 120 (seconds)
EXAMPLE	acd auto available timer: 60

MAPPING KEY SETTINGS

This section provides the hard key settings you can use to enable and disable the Redial, Conf, and Xfer keys on the IP phone.

PARAMETER – *redial disabled*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the Redial key on the IP phone. If this parameter is set to 0, the key is active and can be pressed by the user. If this parameter is set to 1, pressing the Redial key is ignored, and the dialed number is not saved to the "Outgoing Redial List".
FORMAT	Boolean
DEFAULT VALUE	0 (false)
RANGE	0 (false), 1 (true)
EXAMPLE	redial disabled: 1

PARAMETER – *conference disabled*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the Conf key on the IP phone. If this parameter is set to 0, the key is active and can be pressed by the user. If this parameter is set to 1, pressing the Conf key is ignored.
FORMAT	Boolean
DEFAULT VALUE	0 (false)
RANGE	0 (false), 1 (true)
EXAMPLE	conference disabled: 1

PARAMETER – *call transfer disabled*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the Xfer key on the IP phone. If this parameter is set to 0, the key is active and can be pressed by the user. If this parameter is set to 1, pressing the Xfer key is ignored.
FORMAT	Boolean
DEFAULT VALUE	0 (false)
RANGE	0 (false), 1 (true)
EXAMPLE	call transfer disabled: 1

PARAMETER – *map redial key to*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Sets the **Redial** key as a Speeddial key if a value is entered for this parameter. If you leave this parameter blank, the **Redial** key returns to its original functionality.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	map redial key to: 5551234

PARAMETER – *map conf key to*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Sets the **Conf** key as a Speeddial key if a value is entered for this parameter. If you leave this parameter blank, the **Conf** key returns to its original functionality.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	map conf key to: 5551267

SEND DTMF FOR REMAPPING CONFERENCE OR REDIAL KEY

PARAMETER – *map redial as dtmf*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows the phone to send the stored number as DTMF using the phone configured DTMF method when the “Redial” key is pressed.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0-1 0 (Disabled) 1 (Enabled)
EXAMPLE	map redial as dtmf:1

PARAMETER – *map conf as dtmf*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows the phone to send the stored number as DTMF using the phone configured DTMF method when the “Conf” key is pressed.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0-1 0 (Disabled) 1 (Enabled)
EXAMPLE	map conf as dtmf: 1

PARK AND PICKUP SETTINGS

PARAMETER – *sip park pickup config* (global) sip lineN park pickup config (per line)	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the code to enter before entering the extension for where you want to park an incoming call. The applicable value is dependent on the type of server in the network: Server/Park & Pickup Values* **Asterisk** 70;70;asterisk **Sylantro** *98;*99;sylantro **BroadWorks** *68;*88;broadworks ININ PBX callpark;pickup;inin *Leave “value” fields blank to disable the park and pickup feature. For BroadSoft BroadWorks the following syntax is applicable: <park_code>,<park_dial_code>;<pickup_code>, <pickup_dial_code>;broadworks **Note:** Pauses can be introduced in the park and pick up dial codes by adding commas. Each comma amounts to approximate 500ms.
FORMAT	Alphanumeric characters
DEFAULT VALUE	<Blank>
RANGE	See applicable values in table above.
EXAMPLE	sip lineN park pickup config: *68;*88;broadworks or sip park pickup config: *68,,,,,,42;*88,,,,,,42;broadworks

PARAMETER – *sprecode*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the code to enter before entering the extension for where you want to park an incoming call. The applicable value is dependent on the type of server in the network: Server/Park Values** **Asterisk** 70 **Sylantro** *98 **BroadWorks** *68 ININ PBX callpark **Leave “value” fields blank to disable the static park and pickup feature.
FORMAT	Alphanumeric characters
DEFAULT VALUE	<Blank>
RANGE	See applicable values in table above.
EXAMPLE	sprecode: *68

PARAMETER – *pickupsprecode*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the code to enter before entering the extension for where you want to pickup a parked call. The applicable value is dependent on the type of server in the network: Server/Pickup Values** **Asterisk** 70 **Sylantro** *99 **BroadWorks** *88 **ININ PBX** pickup **Leave “value” fields blank to disable the static park and pickup feature.
FORMAT	Alphanumeric characters
DEFAULT VALUE	<Blank>
RANGE	See applicable values in table above.
EXAMPLE	pickupsprecode: *88

LINE LABELING WITH CALLER ID

PARAMETER – *line show caller id*	**CONFIGURATION FILES** startup.cfg, <mac>.cfg
DESCRIPTION	Enable or disable the caller ID display on the line and mobile softkeys.
FORMAT	Boolean
DEFAULT VALUE	1 (enabled) for 6900, 0 (disabled) for 6800
RANGE	0-1 0 - disable 1 - enable
EXAMPLE	line show caller id:1

SELF-AVATAR DISPLAY ON IDLE SCREEN

PARAMETER – *idle screen avatar*	**CONFIGURATION FILES** startup.cfg, <mac>.cfg
DESCRIPTION	Enable or disable the self-picture ID display attached to the focused line.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0-1 0 - disable 1 - enable
EXAMPLE	idle screen avatar: 1

PICTURE REFRESH TIMEOUT

PARAMETER – *picture refresh timeout*	**CONFIGURATION FILES** startup.cfg, <mac>.cfg
DESCRIPTION	Indicates the timeout in hours for a downloaded picture.
FORMAT	Integer
DEFAULT VALUE	0 (no timeout)
RANGE	0- 672
EXAMPLE	picture refresh timeout: 24 (deletes downloaded images after 24 hours to be downloaded again)

MOBILE CONTACTS SYNC

PARAMETER – *mobile contacts enabled*	**CONFIGURATION FILES** startup.cfg, <mac>.cfg
DESCRIPTION	Enable or disable the mobile contacts import.
FORMAT	Boolean
DEFAULT VALUE	1
RANGE	0-1 0 - disable 1 - enable
EXAMPLE	mobile contacts enabled: 1 (to enable mobile contacts)

PARAMETER – *mobile contacts name*	**CONFIGURATION FILES** startup.cfg, <mac>.cfg
DESCRIPTION	Override the default folder name “Mobile Contacts” to provide a customized name to the mobile contacts folder.
FORMAT	String
DEFAULT VALUE	Empty
RANGE	Not applicable
EXAMPLE	mobile contacts name: iphone (to name the mobile directory folder “iphone”)

PHONE AUTO-LOCK AND UNLOCK ON MOBILE PROXIMITY

PARAMETER – *proximity lock*	**CONFIGURATION FILES** startup.cfg, <mac>.cfg
DESCRIPTION	Enable or disable phone automatic lock on proximity detection.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0-1 0 - disable 1 - enable
EXAMPLE	proximity lock: 1 (to enable the feature)

PARAMETER – *proximity lock delay*	**CONFIGURATION FILES** startup.cfg, <mac>.cfg
DESCRIPTION	When proximity lock is enabled, delay after proximity event detection before locking the phone.
FORMAT	Integer
DEFAULT VALUE	0 (no delay)
RANGE	0 to 1440 minutes

EXAMPLE	proximity lock delay: 5 (wait for 5 minutes before phone lock)

PARAMETER – *proximity unlock*	**CONFIGURATION FILES** startup.cfg, <mac>.cfg
DESCRIPTION	Enable or disable phone automatic unlock on proximity detection.
FORMAT	Boolean
DEFAULT VALUE	0 0 - disable 1 - enable
RANGE	Not applicable
EXAMPLE	proximity unlock: 1 (to enable the feature)

PARAMETER – *proximity unlock delay*	**CONFIGURATION FILES** startup.cfg, <mac>.cfg
DESCRIPTION	When proximity unlock is enabled, delay after proximity event detection before unlocking the phone.
FORMAT	Integer
DEFAULT VALUE	0 (no delay)
RANGE	0 to 1440 minutes
EXAMPLE	proximity unlock delay: 5 (wait for 5 minutes before phone unlock)

SOFTKEY/PROGRAMMABLE KEY/KEYPAD KEY/EXPANSION MODULE KEY/HARD KEY PARAMETERS

This section provides the softkey, programmable key, keypad key, and expansion module key parameters you can configure on the IP phones. The following table provides the number of keys you can configure for each model phone and expansion module, and the number of lines available for each type of phone.

Note: 9 keypad keys are available to be configured as press-and-hold speeddials on all IP phone models.

IP PHONE MODEL	SOFTKEYS	EXPANSION MODULE KEYS	PROGRAMMABLE KEYS	LINES AVAILABLE
6863i	-	N/A	3	2
6865i	-	16 to 48* (Model M680i) 84 to 252** (Model (M685i)	8	24
6867i	6 top (maximum of 20 functions) 4 bottom (maximum of 18 functions)	16 to 48* (Model M680i) 84 to 252** (Model (M685i)	-	24
6869i	12 top (maximum of 44 functions) 5 bottom (maximum of 24 functions)	16 to 48* (Model M680i) 84 to 252** (Model (M685i)	-	24
6873i	12 top (maximum of 48 functions) 6 bottom (maximum of 30 functions)	16 to 48* (Model M680i) 84 to 252** (Model (M685i)	-	24

*The M680i expansion module consists of 16 softkeys. You can have up to 3 expansion modules on an IP phone totalling 48 softkeys. Valid for 6865i, 6867i, 6869i, and 6873i phones.
**The M685i expansion module consists of 3 pages of 28 softkeys (for a total of 84). You can have up to 3 expansion modules on an IP phone totalling 252 softkeys. Valid for 6865i, 6867i, 6869i, and 6873i phones.

Note: When entering definitions for softkeys, the “#” sign must be enclosed in quotes.

SOFTKEY SETTINGS

The value of "*N*" for the following parameters is dependent on the number of softkeys available on the 6867i, 6869i, and 6873i models. See the table above for applicable values. Available softkey types are dependent on the IP phone model. Please refer to the respective model's User Guide for the model's available softkey types.

Note: Applicable to the 6867i, 6869i, and 6873i IP Phone only.

PARAMETER – *softkeyN type*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The type of softkey to configure. Valid types are: • **none** - Indicates key is disabled. • **speeddial** - Indicates key is configured for speeddial use. Speeddial is applicable to the M680i and M685i also. You can configure a key to speeddial a specific number by pressing that key. Optionally, you can also configure a Speeddial key to dial prefix numbers. With this option, the prefix numbers automatically dial when you press the key, and the phone waits for you to enter the remaining numbers to dial out. **Note**: When there is an active call, the Speeddial keys send DTMF digits through the active voice path. To dial out, you have to first put the active call on hold and then press the Speeddial key. • **dnd** - Indicates key is configured for do not disturb on the phone. This option is "**Do Not Disturb**" in the Mitel Web UI). You must also set the DND key mode (see "DND Key Mode" on page 5-109 and "DND Key Mode Settings" on page A-206 for details). • **xml** - Indicates the key is configured to accept an XML application for accessing customized XML services. You can also specify an XML key URL for this option. • **flash** - Indicates the key is set to generate a flash event when it is pressed. The IP phone generates flash events only when a call is connected and there is an active RTP stream (for example, when the call is not on hold). • **spre** - Indicates the key is configured to automatically activate specific services offered by the server. For example, if the spre value of *82 is configured, then by pressing the key, *82 automatically activates a service provided by the server. • **park** - Indicates the key is configured to park incoming calls when pressed. • **pickup** - Indicates the key is configured to pick up parked calls when pressed. • **lcr** - Indicates the key is configured for "last call return" when pressed. • **callforward** - Indicates the key is configured for accessing the Call Forward features on the phone. A Call Forwarding Mode must be enabled to use this key. "Account" mode is the default. • **speeddialxfer** - Indicates the key is configured to transfer calls AND configured for speeddialing to a specific number.

	• **speeddialconf** - Indicates the key is configured to be used as a Speeddial key AND as a Conference key. • **directory** - Indicates the key is configured to access the Directory List. • **filter** - Indicates the key is configured to activate/deactivate Executive Call Filtering. • **callers** - Indicates the key is configured to access the Received Callers List. • **redial** - Indicates the key is configured to access the Outgoing Redial List. • **conf** - Indicates the key is configured as a Conference key. • **xfer**- Indicates the key is configured as a Transfer key for transferring calls. • **icom** - Indicates the key is configured to be used as the Intercom key. • **phonelock** - Indicates the key is configured to be used to lock/unlock the phone. • **paging** - Indicates the key is configured for Group Paging on the phone. Pressing this key automatically sends a Real Time Transport Protocol (RTP) stream to pre-configured multicast address(es) without involving SIP signaling. • **hotdesklogin** - Indicates the key is configured to be used as a login key when utilizing the Visitor Desk Phone hotdesk feature. • **discreetringing** - Indicates the key is configured to toggle Discreet Ringing on/off. • **callhistory -** Indicates the key is configured as a Call History key, which allow users the ability to directly access the list of all calls in the Call History. • **callcenter -** Indicates the key is configured for Xsi call center functionality. • **contacts -** Indicates the key is configured for Contact List functionality when interoperability with XMPP UC-ONE services is enabled. • **empty** - Indicates the key is configured to force a blank entry on the IP phone display for a specific key. The softkeys are added in order after any hardcoded keys have been added. If a particular softkey is not defined, it is ignored.
FORMAT	Text
DEFAULT VALUE	none

RANGE	none speeddial dnd ("Do Not Disturb" in the Mitel Web UI) xml flash spre park pickup lcr callforward speeddialxfer speeddialconf directory filter callers (“Callers List” in Mitel Web UI) redial conf xfer icom phonelock paging hotdesklogin discreetringing callhistory callcenter contacts empty
EXAMPLE	softkey1 type: directory softkey2 type: speeddial softkey3 type: lcr softkey4 type: xml

PARAMETER – *softkeyN label*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The text label that displays on the IP phone for the softkey. The “**softkeyN label**” parameter can be set for the following softkey types only: • speeddial • xml • flash • spre • park • pickup • speeddialxfer • speeddialconf • directory • filter • callers • redial • conf • xfer • icom • paging • hotdesklogin • callhistory • callcenter • contacts **Note:** If the *softkeyN type* parameter is set to "**flash**", and no label value is entered for the *softkeyN label* parameter, the label of "**Flash**" is used.
FORMAT	Text
DEFAULT VALUE	N/A
RANGE	Varies
EXAMPLE	softkey1 label: "jane" softkey2 label: “info” softkey3 label: flash softkey4 label: “johnsmith”

PARAMETER – *softkeyN value*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This is the value you assign to the softkey. The "**softkeyN value**" parameter can be set for the following softkey types only: • speeddial (you can enter a speeddial number for this field; optionally, you can also enter a prefix for the speeddial value to allow the phone to dial the prefix after you press the Speeddial key; you then enter the rest of the number from the keypad on the phone). • spre • xml • park • pickup • speeddialxfer • speeddialconf • redial • filter • icom • paging • callcenter • For speeddial the value is the phone number, extension, or prefix number to enter for the softkey. • For blf the value is the extension you want to monitor. • For spre the value is dependent on services offered by server. • For park and pickup valid values, see Chapter 5, the section, "Park/Pickup Call Server Configuration Values" on page 5-247. • For xml you can specify a URI to use for this XML softkey. The variables you can use with the XML softkey URI are: •$$SIPUSERNAME$$ •$$SIPAUTHNAME$$ •$$PROXYURL$$ •$$LINESTATE$$ •$$LOCALIP$$ •$$REMOTENUMBER$$ •$$DISPLAYNAME$$ •$$SIPUSERNAME$$ •$$INCOMINGNAME$$ •$$CALLDURATION$$ •$$CALLDIRECTION$$ • For icom, the value is the predefined intercom call number. • For paging the value is the ip and port (the port range is from 1 to 65535). • For callcenter, the value for the key must be identical to the call center ID value configured for the specific user in the BroadSoft BroadWorks call manager software.

FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	softkey1 value: 9 softkey2 value: 411 softkey4 value: http://10.50.10.140 script.pl?name=$$SIPUSERNAME$$ softkey5 value: 123456+ (example of a speeddial prefix)

PARAMETER – *softkeyN line*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This is the line associated with the softkey you are configuring. The number of applicable lines available is dependent on the specific IP phone model. The "**softkeyN line**" parameter can be set for the following softkey types only: • speeddial • list • lcr • speeddialxfer • speeddialconf • redial • filter
FORMAT	Integer
DEFAULT VALUE	1
RANGE	1-24
EXAMPLE	softkey1 line: 1 softkey2 line: 5

PARAMETER – *softkeyN states*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Displays the status of the phone when a softkey is pressed. You can enter multiple values (**idle, connected, incoming, outgoing, busy**) for the "softkeyN state" parameter. You must associate the softkeyN state parameter with a specific softkey. In the following example, the softkeyN states parameter is associated with softkey 12: softkey12 type: speeddial softkey12 label: voicemail softkey12 value *89 softkey12 states: outgoing **Note:** The IP phone idle screen condenses the softkeys. So in the previous example, softkey 12 will appear in position 1 if no other softkeys are set. A softkey type of "empty" does not display on the idle screen at all.
FORMAT	Text
DEFAULT VALUE	For softkey type none, flash, phonelock, paging: All states disabled For softkey types dnd, speeddial, xml, lcr, callforward, speeddialxfer, speeddialconf, directory, filter, callers, redial, conf, xfer, icom, empty: idle, connected, incoming, outgoing, busy For softkey type flash: All states disabled For softkey type park, spre: connected For softkey type pickup: idle, outgoing
RANGE	Valid values are: **idle**: The phone is not being used. **connected:** The line currently being displayed is in an active call (or the call is on hold) **incoming**: The phone is ringing. **outgoing**: The user is dialing a number, or the far-end is ringing. **busy:** The current line is busy because the line is in use or the line is set as “Do Not Disturb”. **Note:** For softkey type, Pickup, values can be: just idle, just outgoing, or idle outgoing.
EXAMPLE	softkey1 states: idle incoming outgoing softkey2 states: connected

CONFIGURABLE POSITIONING OF PROGRAMMED SOFTKEYS

Note: Applicable to the 6867i, 6869i, and 6873i IP Phone only.

PARAMETER – *collapsed softkey screen*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the 6867i/6869i/6873i from collapsing the softkeys to remove blank keys. When enabled, the phone will remove all the softkeys defined as “None” and display the programmed softkeys in consecutive order. When disabled, the softkey will retain its programmed position. This parameter applies to both top and bottom softkeys.
FORMAT	Integer
DEFAULT VALUE	1 (Enabled)
RANGE	0-1 0 (Disabled) 1 (Enabled)
EXAMPLE	collapsed softkey screen: 0

PARAMETER *collapsed softkey screen offset top*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Defines the offset for locking or collapsing the top softkeys. If the "**collapsed softkey screen**" parameter is enabled, the phone will lock the respective top softkeys (from top softkey 1 to the value defined) and collapse the rest of the top softkeys. If the "**collapsed softkey screen**" parameter is disabled, the phone will collapse the respective top softkeys (from top softkey 1 to the value defined) and lock the rest of the top softkeys.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	• 1 - 19 (6867i) • 1 - 43 (6869i) • 1 - 47 (6873i)
EXAMPLES	collapsed softkey screen offset top: 4

PARAMETER	CONFIGURATION FILES
collapsed softkey screen offset bottom	startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Defines the offset for locking or collapsing the bottom softkeys. If the "**collapsed softkey screen**" parameter is enabled, the phone will lock the respective bottom softkeys (from bottom softkey 1 to the value defined) and collapse the rest of the bottom softkeys. If the "**collapsed softkey screen**" parameter is disabled, the phone will collapse the respective bottom softkeys (from bottom softkey 1 to the value defined) and lock the rest of the bottom softkeys.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	• 1 - 17 (6867i) • 1 - 23 (6869i/6873i)
EXAMPLES	collapsed softkey screen offset bottom: 2

SHIFTING OF SOFTKEY POSITIONS FOR BUSY STATES

Note: Applicable to the 6867i, 6869i, and 6873i IP Phone only.

PARAMETER –	CONFIGURATION FILES
collapsed context user softkey screen	startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	When enabled, user configured softkeys on the applicable phones will collapse and fill in any unused softkeys starting on the first page of softkeys during the following states: • outgoing • ringing • connected • hold
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0-1 0 (Disabled) 1 (Enabled)
EXAMPLE	collapsed context user softkey screen:1

OPTION TO REMOVE THE "MORE" SOFTKEY WHEN NOT REQUIRED

Note: Applicable to the 6867i, 6869i, and 6873i IP Phone only.

PARAMETER – *collapsed more softkey screen*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Controls how softkeys are displayed on the 6867i, 6869i, and 6873i IP phones' screens when the number of softkeys configured matches the exact number of softkey buttons on the phone. By default, when a total of six top softkeys and four bottom softkeys are configured for the 6867i IP phone, the screen displays five top softkeys, four bottom softkeys and "More" options to access the remaining softkeys. When this parameter is enabled, the "More" softkeys are removed allowing the phones to display all configured top and bottom softkeys on one screen. The same behavior is applied to the 6869i when 12 top softkeys or 5 bottom softkeys are configured. The same behavior is applied to the 6873i when 12 top softkeys or 6 bottom softkeys are configured.
FORMAT	Integer
DEFAULT VALUE	0 (Disabled)
RANGE	0-1 0 (Disabled) 1 (Enabled)
EXAMPLE	collapsed more softkey screen: 1

PROGRAMMABLE KEY SETTINGS

Note: Applicable to the 6863i and 6865i IP phones only. Available functions vary by IP phone model.

The value of "N" for the following parameters is dependent on the number of programmable keys available on the 6863i and 6865i phone models. See the table on page A-248 for the applicable values. Available programmable key types are dependent on the IP phone model. Please refer to the respective model's User Guide for the model's available programmable key types.

PARAMETER – *prgkeyN type*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The type of programmable key to configure. Valid types are: • **none** - Indicates key is disabled. • **line** - Indicates key is configured for line use. • **speeddial** - Indicates key is configured for speeddial use. Speeddial is applicable to the M680 and M685i also. You can configure a key to speeddial a specific number by pressing that key. Optionally, you can also configure a Speeddial key to dial prefix numbers. With this option, the prefix numbers automatically dial when you press the key, and the phone waits for you to enter the remaining numbers to dial out. **Note**: When there is an active call, the Speeddial keys send DTMF digits through the active voice path. To dial out, you have to first put the active call on hold and then press the Speeddial key. • **dnd** - Indicates key is configured for do not disturb on the phone. This option is "**Do Not Disturb**" in the Mitel Web UI). You must also set the DND key mode (see "DND Key Mode" on page 5-109 and "DND Key Mode Settings" on page A-206 for details). • **blf** - Indicates key is configured for Busy Lamp Field (BLF) use. User can dial out on a BLF configured key. You can configure a maximum of 50 BLFs shared between the phone and any attached expansion modules. • **list** - Indicates key is configured for BLF/List use. (This option is BLF/List in the Mitel Web UI). User can dial out on a BLF/List configured key. You can also use the "**BLF List URI**" parameter to specify a URI for the phone to access for the BLF/List. • **acd** - (for Sylantro/BroadWorks servers only) Indicates the key is configured for Auto Call Distribution (called "**Auto Call Distribution**" in the Mitel Web UI). The ACD feature allows the Sylantro/BroadWorks server to distribute calls from a queue to registered IP phone users (agents). • **xml** - Indicates the key is configured to accept an XML application for accessing customized XML services. You can also specify an XML key URL for this option. • **flash** - Indicates the key is set to generate a flash event when it is pressed. The IP phone generates flash events only when a call is connected and there is an active RTP stream (for example, when the call is not on hold).

- **spre** - Indicates the key is configured to automatically activate specific services offered by the server. For example, if the spre value of *82 is configured, then by pressing the key, *82 automatically activates a service provided by the server.
- **park** - Indicates the key is configured to park incoming calls when pressed.
- **pickup** - Indicates the key is configured to pick up parked calls when pressed.
- **lcr** - Indicates the key is configured for “last call return” when pressed.
- **callforward** - Indicates the key is configured for accessing the Call Forward features on the phone. A Call Forwarding Mode must be enabled to use this key. “Account” mode is the default.
- **blfxfer** - Indicates the key is configured to transfer calls AND configured for BLF on a single key.
- **speeddialxfer** - Indicates the key is configured to transfer calls AND configured for speeddialing to a specific number.
- **speeddialconf** - Indicates the key is configured to be used as a Speeddial key AND as a Conference key.
- **speeddialmwi** - Indicates the key is configured to be used as a Speeddial key for a voicemail account.
- **directory** - Indicates the key is configured to access the Directory List.
- **filter** - Indicates the key is configured to activate/deactivate Executive Call Filtering.
- **callers** - Indicates the key is configured to access the Received Callers List.
- **redial** - Indicates the key is configured to access the Outgoing Redial List.
- **conf** - Indicates the key is configured as a Conference key.
- **xfer**- Indicates the key is configured as a Transfer key for transferring calls.
- **icom** - Indicates the key is configured to be used as the Intercom key.
- **services** - Indicates the key is configured to be used as the Services key.
- **phonelock** - Indicates the key is configured to be used to lock/unlock the phone.
- **paging** - Indicates the key is configured for Group Paging on the phone. Pressing this key automatically sends a Real Time Transport Protocol (RTP) stream to pre-configured multicast address(es) without involving SIP signaling.
- **save** - Indicates key is configured for save functionality.
- **delete** - Indicates key is configured for delete functionality.
- **hotdesklogin** - Indicates the key is configured to be used as a login key when utilizing the Visitor Desk Phone hotdesk feature.
- **discreetringing** - Indicates the key is configured to toggle Discreet Ringing on/off.

	• **callcenter -** Indicates the key is configured for Xsi call center functionality. • **empty** - Indicates the key is configured to force a blank entry on the IP phone display for a specific key.
FORMAT	Text
DEFAULT VALUE	N/A
RANGE	none line speeddial dnd ("Do Not Disturb" in the Mitel Web UI) blf list (“BLF/List” in the Mitel Web UI) acd (“Auto Call Distribution” in the Mitel Web UI) xml flash spre park pickup lcr callforward blfxfer speeddialxfer speeddialconf speeddialmwi directory filter callers (“Callers List” in Mitel Web UI) redial conf xfer icom services phonelock paging save delete hotdesklogin discreetringing callcenter empty
EXAMPLE	prgkey3 type: speeddial

PARAMETER – *prgkeyN value*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This is the value you assign to the programmable key. The “**prgkeyN value**” parameter can be set for the following softkey types only: • speeddial (you can enter a speeddial number for this field; optionally, you can also enter a prefix for the speeddial value to allow the phone to dial the prefix after you press the speeddial programmable key; you then enter the rest of the number from the keypad on the phone). • line • blf • spre • xml • park • pickup • blfxfer • speeddialxfer • speeddialconf • speeddialmwi • redial • filter • icom • paging • callcenter **Notes:** • For speeddial the value is the phone number, extension, or prefix number to enter for the softkey. • For line the value is optional; for example L4. • For blf the value is the extension you want to monitor. • For list the value is the target’s resource URI and (optional) extension number. Only use for manual placement of BLF/List keys. • For spre the value is dependent on services offered by server. • For park and pickup valid values, see Chapter 5, the section, “Park/Pickup Call Server Configuration Values” on page 5-247.

	• For xml you can specify a URI to use for this XML softkey. The variables you can use with the XML softkey URI are: •$$SIPUSERNAME$$ •$$SIPAUTHNAME$$ •$$PROXYURL$$ •$$LINESTATE$$ •$$LOCALIP$$ •$$REMOTENUMBER$$ •$$DISPLAYNAME$$ •$$SIPUSERNAME$$ •$$INCOMINGNAME$$ •$$CALLDURATION$$ •$$CALLDIRECTION$$ • For icom, the value is the predefined intercom call number. • For paging the value is the ip and port (the port range is from 1 to 65535). • For callcenter, the value for the key must be identical to the call center ID value configured for the specific user in the BroadSoft BroadWorks call manager software.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	prgkey3 value: 411 prgkey4 value: 123456+ (example of a speeddial prefix)

PARAMETER – *prgkeyN line*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This is the line associated with the programmable key you are configuring. The “**prgkeyN line**” parameter can be set for the following softkey types only: • speeddial • blf • list • acd • lcr • blfxfer • speeddialxfer • speeddialconf • speeddialmwi • redial • filter
FORMAT	Integer
DEFAULT VALUE	1
RANGE	1-2 (6863i) 1-24 (6865i)
EXAMPLE	prgkey3 line: 1 prgkey4 line: 5

TOP SOFTKEY SETTINGS

Note: Applicable to the 6867i, 6869i, and 6873i IP Phones only.

PARAMETER – *topsoftkeyN type*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The type of softkey to configure. Valid types are: • **none** - Indicates key is disabled. • **line** - Indicates key is configured for line use. • **speeddial** - Indicates key is configured for speeddial use. Speeddial is applicable to the M680i and M685i also. You can configure a key to speeddial a specific number by pressing that key. Optionally, you can also configure a Speeddial key to dial prefix numbers. With this option, the prefix numbers automatically dial when you press the key, and the phone waits for you to enter the remaining numbers to dial out. **Note**: When there is an active call, the Speeddial keys send DTMF digits through the active voice path. To dial out, you have to first put the active call on hold and then press the Speeddial key. • **dnd** - Indicates key is configured for do not disturb on the phone. This option is "**Do Not Disturb**" in the Mitel Web UI). You must also set the DND key mode (see "DND Key Mode" on page 5-109 and "DND Key Mode Settings" on page A-206 for details). • **blf** - Indicates key is configured for Busy Lamp Field (BLF) use. User can dial out on a BLF configured key. You can configure a maximum of 50 BLFs shared between the phone and any attached expansion modules. • **list** - Indicates key is configured for BLF/List use. (This option is BLF/List in the Mitel Web UI). User can dial out on a BLF/List configured key. You can also use the **"BLF List URI"** parameter to specify a URI for the phone to access for the BLF/List. • **acd** - (for Sylantro/BroadWorks servers only) Indicates the key is configured for Auto Call Distribution (called "**Auto Call Distribution**" in the Mitel Web UI). The ACD feature allows the Sylantro/BroadWorks server to distribute calls from a queue to registered IP phone users (agents). • **xml** - Indicates the key is configured to accept an XML application for accessing customized XML services. You can also specify an XML key URL for this option. • **flash** - Indicates the key is set to generate a flash event when it is pressed. The IP phone generates flash events only when a call is connected and there is an active RTP stream (for example, when the call is not on hold). • **spre** - Indicates the key is configured to automatically activate specific services offered by the server. For example, if the spre value of *82 is configured, then by pressing the key, *82 automatically activates a service provided by the server.

- **park** - Indicates the key is configured to park incoming calls when pressed.
- **pickup** - Indicates the key is configured to pick up parked calls when pressed.
- **lcr** - Indicates the key is configured for “last call return” when pressed.
- **callforward** - Indicates the key is configured for accessing the Call Forward features on the phone. A Call Forwarding Mode must be enabled to use this key. “Account” mode is the default.
- **blfxfer** - Indicates the key is configured to transfer calls AND configured for BLF on a single key.
- **speeddialxfer** - Indicates the key is configured to transfer calls AND configured for speeddialing to a specific number.
- **speeddialconf** - Indicates the key is configured to be used as a Speeddial key AND as a Conference key.
- **speeddialmwi** - Indicates the key is configured to be used as a Speeddial key for a voicemail account.
- **directory** - Indicates the key is configured to access the Directory List.
- **filter** - Indicates the key is configured to activate/deactivate Executive Call Filtering.
- **callers** - Indicates the key is configured to access the Received Callers List.
- **redial** - Indicates the key is configured to access the Outgoing Redial List.
- **conf** - Indicates the key is configured as a Conference key.
- **xfer**- Indicates the key is configured as a Transfer key for transferring calls.
- **icom** - Indicates the key is configured to be used as the Intercom key.
- **services** - Indicates the key is configured to be used as the Services key.
- **phonelock** - Indicates the key is configured to be used to lock/unlock the phone.
- **paging** - Indicates the key is configured for Group Paging on the phone. Pressing this key automatically sends a Real Time Transport Protocol (RTP) stream to pre-configured multicast address(es) without involving SIP signaling.
- **hotdesklogin** - Indicates the key is configured to be used as a login key when utilizing the Visitor Desk Phone hotdesk feature.
- **discreetringing** - Indicates the key is configured to toggle Discreet Ringing on/off.
- **callhistory** - Indicates the key is configured as a Call History key, which allow users the ability to directly access the list of all calls in the Call History.
- **callcenter -** Indicates the key is configured for Xsi call center functionality.
- **mystatus -** Indicates the key is configured for My Status functionality when interoperability with XMPP UC-ONE services is enabled.
- **contacts -** Indicates the key is configured for Contact List functionality when interoperability with XMPP UC-ONE services is enabled.

	• **favorite -** Indicates the key is configured for favorite contacts functionality when interoperability with XMPP UC-ONE services is enabled. • **empty** - Indicates the key is configured to force a blank entry on the IP phone display for a specific key. • The softkeys are added in order (from softkey1 to softkey20) after any hardcoded keys have been added. If a particular softkey is not defined, it is ignored.
FORMAT	Text
DEFAULT VALUE	none
RANGE	• none • line • speeddial • dnd • blf • list ("BLF/List" in the Mitel Web UI) • acd (“Auto Call Distribution” in the Mitel Web UI) • xml • flash • spre • callforward • park • pickup • blfxfer • speeddialxfer • speeddialconf • speeddialmwi • lcr • directory • filter • callers (“Callers List” in Mitel Web UI) • redial • conf • xfer • icom • services • phonelock • paging • hotdesklogin • discreetringing • callhistory • callcenter • mystatus

	• contacts • favorite • empty
EXAMPLE	topsoftkey1 type: line topsoftkey2 type: speeddial topsoftkey3 type: lcr topsoftkey4 type: xml

PARAMETER – *topsoftkeyN label*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The text label that displays on the IP phone for the softkey. The "**topsoftkeyN label**" parameter can be set for the following softkey types only: • line • speeddial • blf • acd • xml • flash • spre • park • pickup • blfxfer • speeddialxfer • speeddialconf • speeddialmwi • directory • filter • callers • redial • conf • xfer • icom • services • paging • hotdesklogin • callhistory • callcenter • contacts **Note:** If the *topsoftkeyN type* parameter is set to "**flash**", and no label value is entered for the top*softkeyN label* parameter, the label of "**Flash**" is used.
FORMAT	Text
DEFAULT VALUE	N/A
RANGE	Varies
EXAMPLE	topsoftkey1 label: "Line 9" topsoftkey2 label: "info" topsoftkey4 label: "johnsmith"

PARAMETER – *topsoftkeyN value*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg

DESCRIPTION

This is the value you assign to the softkey.

The "**topsoftkeyN value**" parameter can be set for the following softkey types only:

- speeddial (you can enter a speeddial number for this field; optionally, you can also enter a prefix for the speeddial value to allow the phone to dial the prefix after you press the Speeddial key; you then enter the rest of the number from the keypad on the phone).
- line
- blf
- spre
- xml
- park
- pickup
- blfxfer
- speeddialxfer
- speeddialconf
- speeddialmwi
- redial
- paging
- icom
- filter
- callcenter

Notes:

- For speeddial the value is the phone number, extension, or prefix number to enter for the softkey.
- For line the value is optional; for example L4.
- For blf the value is the extension you want to monitor.
- For list the value is the target's resource URI and (optional) extension number. Only use for manual placement of BLF/List keys.
- For spre the value is dependent on services offered by server.
- For park and pickup valid values, see Chapter 5, the section, "Park/Pickup Call Server Configuration Values" on page 5-247.

- For xml you can specify a URI to use for this XML softkey. The variables you can use with the XML softkey URI are:
  •$$SIPUSERNAME$$
  •$$SIPAUTHNAME$$
  •$$PROXYURL$$
  •$$LINESTATE$$
  •$$LOCALIP$$
  •$$REMOTENUMBER$$
  •$$DISPLAYNAME$$
  •$$SIPUSERNAME$$
  •$$INCOMINGNAME$$
  •$$CALLDURATION$$
  •$$CALLDIRECTION$$
- For icom, the value is the predefined intercom call number.
- For paging the value is the ip and port (the port range is from 1 to 65535).
- For callcenter, the value for the key must be identical to the call center ID value configured for the specific user in the BroadSoft BroadWorks call manager software.

FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	topsoftkey1 value: 9 topsoftkey2 value: 411 topsoftkey4 value: http://10.50.10.140 script.pl?name=$$SIPUSERNAME$$ topsoftkey5 value: 12345+ (example of a speeddial prefix)

PARAMETER – *topsoftkeyN line*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This is the line associated with the softkey you are configuring. The number of applicable lines available is dependent on the specific IP phone model. The “**topsoftkeyN line**” parameter can be set for the following softkey types only: • speeddial • blf • list • acd • lcr • blfxfer • speeddialxfer • speeddialconf • speeddialmwi • redial • filter
FORMAT	Integer
DEFAULT VALUE	1
RANGE	1-24
EXAMPLE	topsoftkey1 line: 1 topsoftkey2 line: 5

PRESS-AND-HOLD SPEEDDIAL KEYPAD KEY SETTINGS

PARAMETER – *pnhkeypadN value* (where N corresponds to the keypad keys 1-9)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The speeddial number that is dialed out when you press and hold the corresponding keypad key.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	pnhkeypad7 value: 5557605123

PARAMETER – *pnhkeypadN line* (where N corresponds to the keypad keys 1-9)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The line associated with the press and hold speeddial number configured on the keypad key.
FORMAT	Integer
DEFAULT VALUE	1
RANGE	1-2 (6863i) 1-24 (6865i/6867i/6869i/6873i)
EXAMPLE	pnhkeypad7 line: 2

EXPANSION MODULE KEY SETTINGS FOR M680I AND M685I

PARAMETER – *expmodX keyN type*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The type of softkey to configure. Valid types are: • **none** - Indicates key is disabled. • **line** - Indicates key is configured for line use. • **speeddial** - Indicates key is configured for speeddial use. You can configure a key to speeddial a specific number by pressing that key. Optionally, you can also configure a Speeddial key to dial prefix numbers. With this option, the prefix numbers automatically dial when you press the key, and the phone waits for you to enter the remaining numbers to dial out. **Note**: When there is an active call, the Speeddial keys send DTMF digits through the active voice path. To dial out, you have to first put the active call on hold and then press the Speeddial key. • **dnd** - Indicates key is configured for do not disturb on the phone. This option is "**Do Not Disturb**" in the Mitel Web UI). You must also set the DND key mode (see "DND Key Mode" on page 5-109 and "DND Key Mode Settings" on page A-206 for details). • **blf** - Indicates key is configured for Busy Lamp Field (BLF) use. User can dial out on a BLF configured key. You can configure a maximum of 50 BLFs shared between the phone and any attached expansion modules. • **list** - Indicates key is configured for BLF/List use. (This option is BLF/List in the Mitel Web UI). User can dial out on a BLF/List configured key. You can also use the **"BLF List URI"** parameter to specify a URI for the phone to access for the BLF/List. • **acd** - (for Sylantro/BroadWorks servers only) Indicates the key is configured for Auto Call Distribution (called "**Auto Call Distribution**" in the Mitel Web UI). The ACD feature allows the Sylantro/BroadWorks server to distribute calls from a queue to registered IP phone users (agents). • **xml** - Indicates the key is configured to accept an XML application for accessing customized XML services. You can also specify an XML key URL for this option. • **flash** - Indicates the key is set to generate a flash event when it is pressed. The IP phone generates flash events only when a call is connected and there is an active RTP stream (for example, when the call is not on hold). • **spre** - Indicates the key is configured to automatically activate specific services offered by the server. For example, if the spre value of *82 is configured, then by pressing the key, *82 automatically activates a service provided by the server. • **park** - Indicates the key is configured to park incoming calls when pressed. • **pickup** - Indicates the key is configured to pick up parked calls when pressed. • **lcr** - Indicates the key is configured for "last call return" when pressed.

	• **callforward** - Indicates the key is configured for accessing the Call Forward features on the phone. A Call Forwarding Mode must be enabled to use this key. “Account” mode is the default. • **blfxfer** - Indicates the key is configured to transfer calls AND configured for BLF on a single key. • **speeddialxfer** - Indicates the key is configured to transfer calls AND configured for speeddialing to a specific number. • **speeddialconf** - Indicates the key is configured to be used as a Speeddial key AND as a Conference key. • **speeddialmwi** - Indicates the key is configured to be used as a Speeddial key for a voicemail account. • **directory** - Indicates the key is set for accessing the Directory List. • **filter** - Indicates the key is configured to activate/deactivate Executive Call Filtering. • **callers** - Indicates the key is configured to access the Received Callers List. • **redial** - Indicates the key is configured to access the Outgoing Redial List. • **conf** - Indicates the key is configured as a Conference key. • **xfer**- Indicates the key is configured as a Transfer key for transferring calls. • **icom** - Indicates the key is configured to be used as the Intercom key. • **services** - Indicates the key is set to be used as the Services key. • **phonelock** - Indicates the key is set to be used to lock/unlock the phone. • **paging** - Indicates the key is set for Group Paging on the phone. Pressing this key automatically sends a Real Time Transport Protocol (RTP) stream to pre-configured multicast address(es) without involving SIP signaling. • **save** - Indicates key is configured for save functionality. • **delete** - Indicates key is configured for delete functionality. • **hotdesklogin** - Indicates the key is configured to be used as a login key when utilizing the Visitor Desk Phone hotdesk feature. • **discreetringing** - Indicates the key is configured to toggle Discreet Ringing on/off. • **callhistory** - Indicates the key is configured as a Call History key, which allow users the ability to directly access the list of all calls in the Call History. • **callcenter -** Indicates the key is configured for Xsi call center functionality. • **empty** - Indicates the key is configured to force a blank entry on the IP phone display for a specific key.
FORMAT	Text
DEFAULT VALUE	None

Range	• none • line • speeddial • dnd • blf • list ("BLF/List" in the Mitel Web UI) • acd (“Auto call distribution” in the Mitel Web UI) • xml • flash • spre • park • pickup • lcr • callforward • blfxfer • speeddialxfer • speeddialconf • speeddialmwi • directory • filter • callers (“Callers List” in Mitel Web UI) • redial • conf • xfer • icom • services • phonelock • paging • save • delete • hotdesklogin • discreetringing • callhistory • callcenter • empty
Example	expmod1 key1 type: line expmod1 key2 type: speeddial expmod1 key3 type: blf expmod1 key4 type: list

PARAMETER – *expmodX keyN label*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The text label that displays on the softkey for the Expansion Module. The “**expmodX keyN label**” parameter can be set for the following softkey types only: • line • speeddial • blf • acd • xml • flash • spre • park • pickup • blfxfer • speeddialxfer • speeddialconf • speeddialmw5i • directory • filter • callers • redial • conf • xfer • icom • services • paging • hotdesklogin • callhistory • callcenter **Note:** If the *expmodXkeyN type* parameter is set to "**flash**", and no label value is entered for the *expmodXkeyN label* parameter, the label of "**Flash**" is used.
FORMAT	Text
DEFAULT VALUE	N/A
RANGE	Varies
EXAMPLE	expmod1 key1 label: “Line 9” expmod2 key1 label: “info” expmod3 key1 label: “johnsmith”

PARAMETER – *expmodX keyN value*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The text label that displays on the IP phone for the softkey on the Expansion Module.

The "**expmodX keyN value**" parameter can be set for the following softkey types only:

- speeddial (you can enter a speeddial number for this field; optionally, you can also enter a prefix for the speeddial value to allow the phone to dial the prefix after you press the Speeddial key; you then enter the rest of the number from the keypad on the phone).
- line
- blf
- spre
- xml
- park
- pickup
- blfxfer
- speeddialxfer
- speeddialconf
- speeddialmwi
- redial
- filter
- icom
- paging
- callcenter

Notes:

- For speeddial the value is the phone number, extension, or prefix number to enter for the softkey.
- For line the value is optional; for example L4.
- For blf the value is the extension you want to monitor.
- For list the value is the target's resource URI and (optional) extension number. Only use for manual placement of BLF/List keys.
- For spre the value is dependent on services offered by server.
- For park and pickup valid values, see Chapter 5, the section, "Park/Pickup Call Server Configuration Values" on page 5-247.

	• For xml you can specify a URI to use for this XML softkey. The variables you can use with the XML softkey URI are: •$$SIPUSERNAME$$ •$$SIPAUTHNAME$$ •$$PROXYURL$$ •$$LINESTATE$$ •$$LOCALIP$$ •$$REMOTENUMBER$$ •$$DISPLAYNAME$$ •$$SIPUSERNAME$$ •$$INCOMINGNAME$$ •$$CALLDURATION$$ •$$CALLDIRECTION$$ • For icom, the value is the predefined intercom call number. • For paging the value is the ip and port (the port range is from 1 to 65535). • For callcenter, the value for the key must be identical to the call center ID value configured for the specific user in the BroadSoft BroadWorks call manager software.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	expmod1 key1 value: 9 expmod1 key2 value: 411 expmod1 key3 value: 123456+ (example of a speeddial prefix)

PARAMETER – *expmodX keyN line*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This is the line associated with the softkey you are configuring on the Expansion Module. The number of applicable lines available is dependent on the specific IP phone model. The “**expmodX keyN line**” parameter can be set for the following softkey types only: • speeddial • blf • list • acd • lcr • blfxfer • speeddialxfer • speeddialconf • speeddialmwi • redial • filter
FORMAT	Integer
DEFAULT VALUE	1
RANGE	1-24
EXAMPLE	expmod1 key1 line: 1 expmod1 key2 line: 5

HARD KEY SETTINGS

PARAMETER – *hardkeyN type*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The type of key to which you would like to change the hard key. Valid types include: • **none** - Indicates no setting for the key. • **line** - Indicates the key is configured for line use. • **speeddial** - Indicates the key is configured for speeddial use. You can configure a key to speeddial a specific number by pressing that key. Optionally, you can also configure a Speeddial key to dial prefix numbers. With this option, the prefix numbers automatically dial when you press the key, and the phone waits for you to enter the remaining numbers to dial. **Note**: When there is an active call, the Speeddial keys send DTMF digits through the active voice path. To dial out, you have to first put the active call on hold and then press the Speeddial key. • **dnd** - Indicates the key is configured for Do Not Disturb on the phone. • **blf** - Indicates the key is configured for Busy Lamp Field (BLF) use. • **list** - Indicates the key is configured for BLF/List use. • **acd** - (for Sylantro/BroadWorks servers only) Indicates the key is configured for Auto Call Distribution (called “**Auto Call Distribution**” in the Mitel Web UI). The ACD feature allows the Sylantro/BroadWorks server to distribute calls from a queue to registered IP phone users (agents). • **xml** - Indicates the key is configured to accept an XML application for accessing customized XML services. You can also specify an XML softkey URL for this option. • **flash** - Indicates the key is set to generate a flash event when it is pressed. The IP phone generates flash events only when a call is connected and there is an active RTP stream (for example, when the call is not on hold). • **spre** - Indicates the key is configured to automatically activate specific services offered by the server. For example, if the spre value of *82 is configured, then by pressing the softkey, *82 automatically activates a service provided by the server. • **park** - Indicates the key is configured to park incoming calls when pressed. • **pickup** - Indicates the key is configured to pick up parked calls when pressed. • **lcr** - Indicates the key is configured for the Last Call Return function when pressed. • **callforward** - Indicates the key is configured for accessing the Call Forward features on the phone. A Call Forwarding Mode must be enabled to use this key. “Account” mode is the default. • **blfxfer** - Indicates the key is configured to transfer calls AND configured for BLF on a single key.

	• **speeddialxfer** - Indicates the key is configured to transfer calls AND configured for speeddialing to a specific number. • **speeddialconf** - Indicates the key is configured to be used as a Speeddial key AND as a Conference key. • **speeddialmwi** - Indicates the key is configured to be used as a Speeddial key for a voicemail account. • **directory** - Indicates the key is configured to access the Directory List. • **filter** - Indicates the key is configured to activate/deactivate Executive Call Filtering. • **services** - Indicates the key is set to be used as the Services key. • **callers** - Indicates key is configured to access the Received Callers List. • **redial** - Indicates key is configured to access the Outgoing Redial List. • **conf** - Indicates the key is configured as a Conference key. • **xfer**- Indicates the key is configured as a Transfer key for transferring calls. • **icom** - Indicates the key is set to be used as the Intercom key. • **phonelock** - Indicates the key is set to be used to lock/unlock the phone. • **paging** - Indicates the key is set for Group Paging on the phone. Pressing this key automatically sends a Real Time Transport Protocol (RTP) stream to pre-configured multicast address(es) without involving SIP signaling. • **hotdesklogin** - Indicates the key is configured to be used as a login key when utilizing the Visitor Desk Phone hotdesk feature. • **discreetringing** - Indicates the key is configured to toggle Discreet Ringing on/off. • **callhistory** - Indicates the key is configured as a Call History key, which allow users the ability to directly access the list of all calls in the Call History. • **callcenter -** Indicates the key is configured for Xsi call center functionality.
FORMAT	Text
DEFAULT VALUE	N/A

RANGE	• none • line • speeddial • dnd • blf • list ("BLF/List" in the Mitel Web UI) • acd (“Auto call distribution” in the Mitel Web UI) • xml • flash • spre • park • pickup • lcr • callforward • blfxfer • speeddialxfer • speeddialconf • speeddialmwi • directory • filter • callers (“Callers List” in Mitel Web UI) • redial • conf • xfer • icom • services • phonelock • paging • hotdesklogin • discreetringing • callhistory • callcenter
EXAMPLE	hardkey1 type: speeddial

PARAMETER – *hardkeyN value*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The value you would like to assign to the hard key you are configuring. The “hardkeyN value” parameter can be set for the following key types only: • speeddial (you can enter a speeddial number for this field; optionally, you can also enter a prefix for the speeddial value to allow the phone to dial the prefix after you press the Speeddial key; you then enter the rest of the number from the keypad on the phone). • line • blf • spre • xml • park • pickup • blfxfer • speeddialxfer • speeddialconf • speeddialmwi • redial • filter • paging • callcenter **Notes:** • For speeddial the value is the phone number, extension, or prefix number to enter for the key. • For line the value is optional; for example L4. • For blf the value is the extension you want to monitor. • For spre the value is dependent on services offered by server. • For xml you can specify a URI to use for this XML key. The variables you can use with the XML softkey URI are: •$$SIPUSERNAME$$ •$$SIPAUTHNAME$$ •$$PROXYURL$$ •$$LINESTATE$$ •$$LOCALIP$$ •$$REMOTENUMBER$$ •$$DISPLAYNAME$$ •$$SIPUSERNAME$$ •$$INCOMINGNAME$$ •$$CALLDURATION$$ •$$CALLDIRECTION$

	• For paging the value is the ip and port (the port range is from 1 to 65535). • For callcenter, the value for the key must be identical to the call center ID value configured for the specific user in the BroadSoft BroadWorks call manager software.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	hardkey1 value: 123456+ (example of a speeddial prefix)

PARAMETER – *hardkeyN line*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The line associated with the hard key you are configuring. The “hardkeyN line” parameter can be set for the following key types only: • speeddial • blf • list • acd • lcr • blfxfer • speeddialxfer • speeddialconf • speeddialmwi • redial • filter
FORMAT	Integer
DEFAULT VALUE	N (where N = line number)
RANGE	1-2 (6863i) 1-24 (6865i, 6867i, 6869i, and 6873i)
EXAMPLE	hardkey1 line: 9

CUSTOMIZING THE KEY TYPE LIST

Softkeys, Programmable Keys, Expansion Module Keys

PARAMETER – *softkey selection list*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to specify which key types to display and the order in which to display them in the "**Type**" list for softkeys, programmable keys, and/or expansion module keys when configuring the keys in the Mitel Web UI. If no value is specified for this "**softkey selection list**" parameter, the key "**Type**" list displays ALL of the key types by default in the Mitel Web UI. **Notes:** • Any key types configured that do not apply to the phone's environment are ignored. • The SAVE and DELETE keys appear by default as Keys 5 and 6 on the 6865i unless specifically changed by your Administrator. • An Administrator must use the English value when configuring the key types in the configuration files. • Any key type already configured on a phone displays in that key's "Type" list, in addition to the values specified for this parameter. • After configuring specific key types for a phone, the key types in the Mitel Web UI display the same for both the User and Administrator Web interfaces for that phone.
FORMAT	Alpha Characters in a comma separated list

DEFAULT VALUE	• none	• filter
	• line	• callers
	• speeddial	• redial
	• dnd	• conf
	• blf	• xfer
	• list	• icom
	• acd	• services
	• xml	• phonelock
	• flash	• paging
	• spre	• save
	• park	• delete
	• pickup	• hotdesklogin
	• lcr	• discreetringing
	• callforward	• callhistory
	• blfxfer	• mystatus
	• speeddialxfer	• contacts
	• speeddialconf	• favorite
	• speeddialmwi	• empty
	• directory	
RANGE	Any of the key types in the “Default Value” field above.	
EXAMPLE	softkey selection list: blf, speeddial, line, xml	

LOCKING KEYS

PARAMETER – *softkeyN locked*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Locks the specified softkey on the 6867i, 6869i, or 6873i IP phone. When enabled, the phone locks the key with the provisioned local settings and prevents users from changing or configuring the key. **Note:** If no settings are configured locally but the “softkeyN type” is defined in a configuration file, the phone will lock the key with the key type defined in the configuration file along with any values associated with the additional “softkeyN” parameters (i.e. “softkeyN label”, “softkeyN value”, “softkeyN line”, “softkeyN states”).
FORMAT	Boolean
DEFAULT VALUE	0 (disable)
RANGE	0 (disable) 1 (enable)
EXAMPLE	softkey1 locked: 1

PARAMETER – *topsoftkeyN locked*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Locks the specified top softkey on the 6867i, 6869i, or 6873i IP phone. When enabled, the phone locks the key with the provisioned local settings and prevents users from changing or configuring the key. **Note:** If no settings are configured locally but the “topsoftkeyN type” is defined in a configuration file, the phone will lock the key with the key type defined in the configuration file along with any values associated with the additional “topsoftkeyN” parameters (i.e. “topsoftkeyN label”, “topsoftkeyN value”, “topsoftkeyN line”).
FORMAT	Boolean
DEFAULT VALUE	0 (disable)
RANGE	0 (disable) 1 (enable)
EXAMPLE	topsoftkey1 locked: 1

PARAMETER – *prgkeyN locked*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Locks the specified programmable key on the 6863i or 6865i IP phone. When enabled, the phone locks the key with the provisioned local settings and prevents users from changing or configuring the key. **Note:** If no settings are configured locally but the “prgkeyN type” is defined in a configuration file, the phone will lock the key with the key type defined in the configuration file along with any values associated with the additional “prgkeyN” parameters (i.e. “prgkeyN value”, “prgkeyN line”).
FORMAT	Boolean
DEFAULT VALUE	0 (disable)
RANGE	0 (disable) 1 (enable)
EXAMPLE	prgkey1 locked: 1

PARAMETER – *expmodX keyN locked*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Locks the specified softkey on the Expansion Module attached to the IP phone. When enabled, the phone locks the key with the provisioned local settings and prevents users from changing or configuring the key. **Note:** If no settings are configured locally but the “expmodX keyN type” is defined in a configuration file, the phone will lock the key with the key type defined in the configuration file along with any values associated with the additional “expmodX keyN” parameters (i.e. “expmodX keyN label” [M685i only], “expmodX keyN value”, “expmodX keyN line”).
FORMAT	Boolean
DEFAULT VALUE	0 (disable)
RANGE	0 (disable) 1 (enable)
EXAMPLE	expmod1 key4 locked: 1

PARAMETER – *pnhkeypadN locked*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Locks the specified keypad key on the IP phones. When enabled, the phone locks the key with the provisioned local settings and prevents users from changing or configuring the key. **Note:** If no settings are configured locally but the “pnhkeypadN type” is defined in a configuration file, the phone will lock the key with the key type defined in the configuration file along with any values associated with the additional “pnhkeypadN” parameters (i.e. “pnhkeypadN value” and “pnhkeypadN line”).
FORMAT	Integer
DEFAULT VALUE	0 (Disabled)
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	pnhkeypad1 locked: 1

PARAMETER – *hardkeyN locked*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Locks the specified hard key on the IP phones. When enabled, the phone locks the key with the provisioned local settings and prevents users from changing or configuring the key. **Note:** If no settings are configured locally but the “hardkeyN type” is defined in a configuration file, the phone will lock the key with the key type defined in the configuration file along with any values associated with the additional “hardkeyN” parameters (i.e. “hardkeyN value” and “hardkeyN line”).
FORMAT	Integer
DEFAULT VALUE	0 (Disabled)
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	hardkey1 locked: 1

LOCKING THE SAVE AND DELETE KEYS

Note: Applicable to the 6865i IP Phone only.

PARAMETER – *prgkey5 locked*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to lock or unlock the **Save** key on the 6865i IP Phone. When the **Save** key is unlocked, a User can change the function of the key using the Mitel Web UI. An Administrator can change the function of the key using the Mitel Web UI or the configuration files. **Note:** Changing the function from the **Save** key to another function without assigning another **Save** key removes the ability to save items on the IP phone.
FORMAT	Boolean
DEFAULT VALUE	1 (lock)
RANGE	0 (unlock) 1 (lock)
EXAMPLE	prgkey5 locked: 0

PARAMETER – *prgkey6 locked*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to lock or unlock the **Delete** key on the 6865i IP Phone. When the **Delete** key is unlocked, a User can change the function of the key using the Mitel Web UI. An Administrator can change the function of the key using the Mitel Web UI or the configuration files. **Note:** Changing the function from the **Delete** key to another function without assigning another **Delete** key removes the ability to delete items on the IP phone.
FORMAT	Boolean
DEFAULT VALUE	1 (lock)
RANGE	0 (unlock) 1 (lock)
EXAMPLE	prgkey6 locked: 0

ENABLING/DISABLING PHONE LOCK

PARAMETER – *phone lock*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to lock and unlock the IP phone. If this parameter is enabled, the IP phone is locked.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) - phone is unlocked 1 (enabled) - phone is locked
EXAMPLE	phone lock: 1

ENABLING/DISABLING ABILITY TO ADD/EDIT SPEEDDIAL KEYS

PARAMETER – *speeddial edit*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to enable or disable the ability to add a Speeddial key or edit a Speeddial key. The default is enabled (Yes) allowing you to create and edit Speeddial keys on the phone using the Press-and-hold feature, softkeys, programmable keys, expansion module keys and key pad, Speeddial menu in the IP Phone UI, and the SAVE TO key. If this parameter is set to disabled (No), it blocks the user from using any of the features on the phone to create or edit a Speeddial key.
FORMAT	Boolean
DEFAULT VALUE	1 (Enabled)
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	speeddial edit: 0

BLF LIST URI SETTINGS

Note: Applicable to the 6865i, 6867i, 6869i, and 6873i IP Phones only.

PARAMETER – *list uri*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the URI that the phone uses to access the BLF list on the BroadSoft server when the BLF list key is pressed. When you specify a URI for this parameter, the phone uses the Internet to access the BLF list on the BroadSoft server.
FORMAT	HTTP server path or Fully Qualified Domain Name
DEFAULT VALUE	N/A
RANGE	N/A

EXAMPLE	list uri: sip:9@192.168.104.13

BLF PAGE SWITCH

Note: Applicable to the 6867i and 6869i IP Phones only. This feature is currently not supported on the 6873i IP phone.

PARAMETER – *blf activity page switch*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables the phone to automatically switch the screen focus to an expansion module or softkey page that has BLF activity. **Note:** This feature is not applicable to BLF/List keys.
FORMAT	Integer
DEFAULT VALUE	0 (disabled)
RANGE	0-3 0 (disabled) 1 (switch page if monitored extension transitions to ringing [fast flashing] state) 2 (switch page if monitored extension transitions to either ringing [fast flashing] or hold [slow flashing] state) 3 (switch page if monitored extension transitions to either ringing or hold state OR from idle [off] state to “in call” [solid] state)
EXAMPLE	blf activity page switch: 1

CONFIGURABLE DISPLAY MODES FOR BLF AND BLF/LIST SOFTKEY LABELS

Note: Applicable to the 6867i, 6869i, and 6873i IP Phones only.

PARAMETER – *blf display label to max*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies how the phone should display BLF and BLF/List softkey labels. In the primary (default) display mode, when a label exceeds the maximum characters the respective phone’s screen can display, the phone adds an ellipsis (i.e. “...”) at the end of the label indicating the label has been automatically truncated. In the secondary display mode, the phone does not automatically truncate the label and simply displays as many characters as the area reserved for the label allows.
FORMAT	Boolean
DEFAULT VALUE	0 (Primary Display Mode)
RANGE	0 - 1 0 (Primary Display Mode) 1 (Secondary Display Mode)
EXAMPLE	blf display label to max: 1

CONFIGURABLE DISPLAY FOR BLANK BLF/LIST AND XMPP PRESENCE-RELATED FAVORITE SOFTKEYS

Note: Applicable to the 6867i, 6869i, 6873i IP Phones only.

PARAMETER – *keys noname hidden*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	If this parameter is set to “0” (disabled) then a series of question marks will be displayed on the screen indicating blank BLF/List and/or Favorite softkeys. **Note:** For BLF/List softkeys, symbols can be configured as defined by the “keys noname symbol” parameter described below. If this parameter is set to “1” (enabled) then the series of question marks will be hidden and nothing will be shown on the screen beside the affected softkeys.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0-1 0 (disabled) 1 (enabled)
EXAMPLE	keys noname hidden: 1

PARAMETER – *keys noname symbol*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	By default, when softkeys are configured as BLF/List keys on the phone but there are not enough members in the BLF/List on the BroadSoft server side, then a series of question marks (i.e. “? ???”) are displayed on screen beside some of the softkeys. The question marks can be replaced with a different symbol/character by defining this parameter. **Note:** Applicable to BLF/List keys only.
FORMAT	Any character placed within quotation marks
DEFAULT VALUE	“?”
RANGE	Any character (can be left empty as well)
EXAMPLE	keys noname symbol: “e”

CONFIGURABLE BLF AND BLF/LIST KEY BEHAVIOR WHEN IN AN ACTIVE CALL

Note: Applicable to the 6865i, 6867i, 6869i, and 6873i IP Phones only.

PARAMETER – *blf key mode*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the behavior when a BLF, BLF/List, or BLF/Xfer key is pressed during an active call. If the parameter is defined as "0" (default), upon a BLF or BLF/List key press, the BLF or BLF/List number will be sent as DTMF tones in the active call. If defined as "1", upon a BLF or BLF/List key press, the active call will be placed on hold and the phone will place a call to the BLF or BLF/List number using the next available line. If defined as "2", upon a BLF or BLF/Xfer key press, an HTTP GET will be triggered on the URI defined in the "action uri blf" parameter. **Note:** If defined as "2", a valid URI must be defined for the "action uri blf" parameter. If a valid URI is not defined, the key mode behavior will revert to the default value (DTMF in active call).
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 - 2 0 (DTMF in active call) 1 (Active call placed on hold and BLF or BLF/List number dialed out using the next available line) 2 (HTTP GET triggered on the URI defined in the "action uri blf" parameter)
EXAMPLE	blf key mode: 2

RING SPLASH SETTINGS

Note: Applicable to the 6865i, 6867i, 6869i, and 6873i IP Phones only.

PARAMETER – *play a ring splash*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the playing of a short ring splash when there is an incoming call on a BLF-monitored extension.
FORMAT	Integer
DEFAULT VALUE	0 (Disabled)
RANGE	0 - 2 0 (Disabled) 1 (Enabled for idle state only) 2 (Enabled for idle state and active call state) **Note:** Playing a BLF ring splash while in an active call state (i.e. defining the parameter as “2”) is only available to the 6865i, 6867i, 6869i, and 6873i IP phones.
EXAMPLE	play a ring splash: 2

PARAMETER – *prgkeyN ring splash*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	When a key is configured for BLF or BLF/List functionality, this parameter controls the ring splash alert pattern per key. The following alerting patterns are available: • **0**: Silence (ring splash off). • **1**: Normal (same as current BLF ring splash). • **2**: Normal delayed (After a delay of [x] seconds, the ring signal that is the same as the current BLF ring splash is played [use the “ring splash delay” parameter to define the delay]). • **3**: Periodic (similar to the normal ring signal that is used by the phone itself. The actual ring melody is based on the current melody set for the line to which the BLF or BLF/List key is associated). • **4**: Periodic delayed (same as Periodic but after a delay of [x] seconds, the ring signal that is used by the phone is played [use the “ring splash delay” parameter to define the delay]). • **5**: Low volume (same as the current BLF ring splash but at a lower level to be less intrusive). • **6**: Low volume delayed (after a delay of [x] seconds, the ring signal that is the same as the current BLF ring splash is played at a lower level [use the “ring splash delay” parameter to define the delay]). • **7**: The behavior is determined by the global parameter “play a ring splash”. •If “play a ring splash” is defined as 0 then the feature is disabled. •If “play a ring splash” is defined as 1 then the behavior is the same as Normal. •If “play a ring splash” is defined as 2 then the behavior is the same as Normal but the ring splash plays when idle and also during the active call state. • **8**: In call delayed (same as Normal delayed but ring splash plays when idle and also during the active call state [use the “ring splash delay” parameter to define the delay]). • **9**: In call periodic (same as Periodic but ring splash plays when idle and also during the active call state [use the “ring splash frequency” parameter to define the ring splash frequency interval for the active call state]). • **10**: In call periodic delayed (same as Periodic delayed but ring splash plays when idle and also during the active call state [use the “ring splash delay” parameter to define the delay for the active and idle call state and the “ring splash frequency” parameter to define the ring splash frequency interval for the active call state]).

	• **11**: In call low volume (same as Low volume but ring splash plays when idle and also during the active call state). • **12**: In call low volume delayed (same as Low volume delayed but ring splash plays when idle and also during the active call state [use the “ring splash delay” parameter to define the delay]). **Notes:** • Ring tones are based on the current ring tone set configured on the IP phone. • Ring splashes will not be played if a custom ring tone is selected.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	0 (Silence) 1 (Normal) 2 (Normal delayed) 3 (Periodic) 4 (Periodic delayed) 5 (Low volume) 6 (Low volume delayed) 7 (The behavior is determined by the global parameter “play a ring splash”. • If “play a ring splash” is defined as 0 then the feature is disabled. • If “play a ring splash” is defined as 1 then the behavior is the same as Normal. • If “play a ring splash” is defined as 2 then the behavior is the same as Normal but the ring splash plays when idle and also during the active call state). 8 (In call delayed) 9 (In call periodic) 10 (In call periodic delayed) 11 (In call low volume) 12 (In call low volume delayed)
EXAMPLE	prgkey1 ring splash: 1

PARAMETER – *softkeyN ring splash*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	When a key is configured for BLF or BLF/List functionality, this parameter controls the ring splash alert pattern per key. The following alerting patterns are available: • **0**: Silence (ring splash off). • **1**: Normal (same as current BLF ring splash). • **2**: Normal delayed (After a delay of [x] seconds, the ring signal that is the same as the current BLF ring splash is played [use the “ring splash delay” parameter to define the delay]). • **3**: Periodic (similar to the normal ring signal that is used by the phone itself. The actual ring melody is based on the current melody set for the line to which the BLF or BLF/List key is associated. • **4**: Periodic delayed (same as Periodic but after a delay of [x] seconds, the ring signal that is used by the phone is played [use the “ring splash delay” parameter to define the delay]). • **5**: Low volume (same as the current BLF ring splash but at a lower level to be less intrusive). • **6**: Low volume delayed (after a delay of [x] seconds, the ring signal that is the same as the current BLF ring splash is played at a lower level [use the “ring splash delay” parameter to define the delay]). • **7**: The behavior is determined by the global parameter “play a ring splash”. •If “play a ring splash” is defined as 0 then the feature is disabled. •If “play a ring splash” is defined as 1 then the behavior is the same as Normal. •If “play a ring splash” is defined as 2 then the behavior is the same as Normal but the ring splash plays when idle and also during the active call state. • **8**: In call delayed (same as Normal delayed but ring splash plays when idle and also during the active call state [use the “ring splash delay” parameter to define the delay]). • **9**: In call periodic (same as Periodic but ring splash plays when idle and also during the active call state [use the “ring splash frequency” parameter to define the ring splash frequency interval for the active call state]). • **10**: In call periodic delayed (same as Periodic delayed but ring splash plays when idle and also during the active call state [use the “ring splash delay” parameter to define the delay for the active and idle call state and the “ring splash frequency” parameter to define the ring splash frequency interval for the active call state]).

	• **11**: In call low volume (same as Low volume but ring splash plays when idle and also during the active call state). • **12**: In call low volume delayed (same as Low volume delayed but ring splash plays when idle and also during the active call state [use the “ring splash delay” parameter to define the delay]). **Notes:** • Ring tones are based on the current ring tone set configured on the IP phone. • Ring splashes will not be played if a custom ring tone is selected.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	0 (Silence) 1 (Normal) 2 (Normal delayed) 3 (Periodic) 4 (Periodic delayed) 5 (Low volume) 6 (Low volume delayed) 7 (The behavior is determined by the global parameter “play a ring splash”. • If “play a ring splash” is defined as 0 then the feature is disabled. • If “play a ring splash” is defined as 1 then the behavior is the same as Normal. • If “play a ring splash” is defined as 2 then the behavior is the same as Normal but the ring splash plays when idle and also during the active call state). 8 (In call delayed) 9 (In call periodic) 10 (In call periodic delayed) 11 (In call low volume) 12 (In call low volume delayed)
EXAMPLE	softkey1 ring splash: 1

PARAMETER – *topsoftkeyN ring splash*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	When a key is configured for BLF or BLF/List functionality, this parameter controls the ring splash alert pattern per key. The following alerting patterns are available: • **0**: Silence (ring splash off). • **1**: Normal (same as current BLF ring splash). • **2**: Normal delayed (After a delay of [x] seconds, the ring signal that is the same as the current BLF ring splash is played [use the “ring splash delay” parameter to define the delay]). • **3**: Periodic (similar to the normal ring signal that is used by the phone itself. The actual ring melody is based on the current melody set for the line to which the BLF or BLF/List key is associated. • **4**: Periodic delayed (same as Periodic but after a delay of [x] seconds, the ring signal that is used by the phone is played [use the “ring splash delay” parameter to define the delay]). • **5**: Low volume (same as the current BLF ring splash but at a lower level to be less intrusive). • **6**: Low volume delayed (after a delay of [x] seconds, the ring signal that is the same as the current BLF ring splash is played at a lower level [use the “ring splash delay” parameter to define the delay]). • **7**: The behavior is determined by the global parameter “play a ring splash”. •If “play a ring splash” is defined as 0 then the feature is disabled. •If “play a ring splash” is defined as 1 then the behavior is the same as Normal. •If “play a ring splash” is defined as 2 then the behavior is the same as Normal but the ring splash plays when idle and also during the active call state. • **8**: In call delayed (same as Normal delayed but ring splash plays when idle and also during the active call state [use the “ring splash delay” parameter to define the delay]). • **9**: In call periodic (same as Periodic but ring splash plays when idle and also during the active call state [use the “ring splash frequency” parameter to define the ring splash frequency interval for the active call state]). • **10**: In call periodic delayed (same as Periodic delayed but ring splash plays when idle and also during the active call state [use the “ring splash delay” parameter to define the delay for the active and idle call state and the “ring splash frequency” parameter to define the ring splash frequency interval for the active call state]).

	• **11**: In call low volume (same as Low volume but ring splash plays when idle and also during the active call state). • **12**: In call low volume delayed (same as Low volume delayed but ring splash plays when idle and also during the active call state [use the “ring splash delay” parameter to define the delay]). **Notes:** • Ring tones are based on the current ring tone set configured on the IP phone. • Ring splashes will not be played if a custom ring tone is selected.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	0 (Silence) 1 (Normal) 2 (Normal delayed) 3 (Periodic) 4 (Periodic delayed) 5 (Low volume) 6 (Low volume delayed) 7 (The behavior is determined by the global parameter “play a ring splash”. • If “play a ring splash” is defined as 0 then the feature is disabled. • If “play a ring splash” is defined as 1 then the behavior is the same as Normal. • If “play a ring splash” is defined as 2 then the behavior is the same as Normal but the ring splash plays when idle and also during the active call state). 8 (In call delayed) 9 (In call periodic) 10 (In call periodic delayed) 11 (In call low volume) 12 (In call low volume delayed)
EXAMPLE	topsoftkey1 ring splash: 1

PARAMETER – *expmodX KeyN ring splash*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
	When a key is configured for BLF or BLF/List functionality, this parameter controls the ring splash alert pattern per key. The following alerting patterns are available: • **0**: Silence (ring splash off). • **1**: Normal (same as current BLF ring splash). • **2**: Normal delayed (After a delay of [x] seconds, the ring signal that is the same as the current BLF ring splash is played [use the “ring splash delay” parameter to define the delay]). • **3**: Periodic (similar to the normal ring signal that is used by the phone itself. The actual ring melody is based on the current melody set for the line to which the BLF or BLF/List key is associated). • **4**: Periodic delayed (same as Periodic but after a delay of [x] seconds, the ring signal that is used by the phone is played [use the “ring splash delay” parameter to define the delay]). • **5**: Low volume (same as the current BLF ring splash but at a lower level to be less intrusive). • **6**: Low volume delayed (after a delay of [x] seconds, the ring signal that is the same as the current BLF ring splash is played at a lower level [use the “ring splash delay” parameter to define the delay]). • **7**: The behavior is determined by the global parameter “play a ring splash”. •If “play a ring splash” is defined as 0 then the feature is disabled. •If “play a ring splash” is defined as 1 then the behavior is the same as Normal. •If “play a ring splash” is defined as 2 then the behavior is the same as Normal but the ring splash plays when idle and also during the active call state. • **8**: In call delayed (same as Normal delayed but ring splash plays when idle and also during the active call state [use the “ring splash delay” parameter to define the delay]). • **9**: In call periodic (same as Periodic but ring splash plays when idle and also during the active call state [use the “ring splash frequency” parameter to define the ring splash frequency interval for the active call state]). • **10**: In call periodic delayed (same as Periodic delayed but ring splash plays when idle and also during the active call state [use the “ring splash delay” parameter to define the delay for the active and idle call state and the “ring splash frequency” parameter to define the ring splash frequency interval for the active call state]).

	• **11**: In call low volume (same as Low volume but ring splash plays when idle and also during the active call state). • **12**: In call low volume delayed (same as Low volume delayed but ring splash plays when idle and also during the active call state [use the "ring splash delay" parameter to define the delay]). **Notes:** • Ring tones are based on the current ring tone set configured on the IP phone. • Ring splashes will not be played if a custom ring tone is selected.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	0 (Silence) 1 (Normal) 2 (Normal delayed) 3 (Periodic) 4 (Periodic delayed) 5 (Low volume) 6 (Low volume delayed) 7 (The behavior is determined by the global parameter "play a ring splash". • If "play a ring splash" is defined as 0 then the feature is disabled. • If "play a ring splash" is defined as 1 then the behavior is the same as Normal. • If "play a ring splash" is defined as 2 then the behavior is the same as Normal but the ring splash plays when idle and also during the active call state). 8 (In call delayed) 9 (In call periodic) 10 (In call periodic delayed) 11 (In call low volume) 12 (In call low volume delayed)
EXAMPLE	expmod1 key1 ring splash: 1

PARAMETER – *hardkeyN ring splash*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	(6865i, 6867i, 6869i, and 6873i only) When a key is configured for BLF or BLF/List functionality, this parameter controls the ring splash alert pattern per key. The following alerting patterns are available: • **0**: Silence (ring splash off). • **1**: Normal (same as current BLF ring splash). • **2**: Normal delayed (After a delay of [x] seconds, the ring signal that is the same as the current BLF ring splash is played [use the “ring splash delay” parameter to define the delay]). • **3**: Periodic (similar to the normal ring signal that is used by the phone itself. The actual ring melody is based on the current melody set for the line to which the BLF or BLF/List key is associated). • **4**: Periodic delayed (same as Periodic but after a delay of [x] seconds, the ring signal that is used by the phone is played [use the “ring splash delay” parameter to define the delay]). • **5**: Low volume (same as the current BLF ring splash but at a lower level to be less intrusive). • **6**: Low volume delayed (after a delay of [x] seconds, the ring signal that is the same as the current BLF ring splash is played at a lower level [use the “ring splash delay” parameter to define the delay]). • **7**: The behavior is determined by the global parameter “play a ring splash”. •If “play a ring splash” is defined as 0 then the feature is disabled. •If “play a ring splash” is defined as 1 then the behavior is the same as Normal. •If “play a ring splash” is defined as 2 then the behavior is the same as Normal but the ring splash plays when idle and also during the active call state. • **8**: In call delayed (same as Normal delayed but ring splash plays when idle and also during the active call state [use the “ring splash delay” parameter to define the delay]). • **9**: In call periodic (same as Periodic but ring splash plays when idle and also during the active call state [use the “ring splash frequency” parameter to define the ring splash frequency interval for the active call state]). • **10**: In call periodic delayed (same as Periodic delayed but ring splash plays when idle and also during the active call state [use the “ring splash delay” parameter to define the delay for the active and idle call state and the “ring splash frequency” parameter to define the ring splash frequency interval for the active call state]).

FORMAT	• **11**: In call low volume (same as Low volume but ring splash plays when idle and also during the active call state). • **12**: In call low volume delayed (same as Low volume delayed but ring splash plays when idle and also during the active call state [use the “ring splash delay” parameter to define the delay]). **Notes:** • Ring tones are based on the current ring tone set configured on the IP phone. • Ring splashes will not be played if a custom ring tone is selected.
DEFAULT VALUE	Integer
RANGE	N/A
EXAMPLE	0 (Silence) 1 (Normal) 2 (Normal delayed) 3 (Periodic) 4 (Periodic delayed) 5 (Low volume) 6 (Low volume delayed) 7 (The behavior is determined by the global parameter “play a ring splash”. • If “play a ring splash” is defined as 0 then the feature is disabled. • If “play a ring splash” is defined as 1 then the behavior is the same as Normal. • If “play a ring splash” is defined as 2 then the behavior is the same as Normal but the ring splash plays when idle and also during the active call state). 8 (In call delayed) 9 (In call periodic) 10 (In call periodic delayed) 11 (In call low volume) 12 (In call low volume delayed)
Example	hardkey1 ring splash: 1

PARAMETER – *ring splash delay*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Indicates the delay (in seconds) between the target ringing and the ring splash played when the "...keyN ring splash" parameter is set to a "delayed" alerting pattern. **Note:** If defined as "0", the ring splash is played immediately.
FORMAT	Numeric
DEFAULT VALUE	7 (seconds)
RANGE	NA
EXAMPLE	ring splash delay: 10

PARAMETER – *ring splash volume*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Indicates the volume of the ring splash from 1 (loudest) to 9 (softest) when the "...keyN ring splash" parameter is set to a "low volume" alerting pattern.
FORMAT	Numeric
DEFAULT VALUE	5
RANGE	1-9
EXAMPLE	ring splash volume: 2

PARAMETER – *ring splash frequency*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Indicates the frequency interval (in seconds) when the "...keyN ring splash" parameter is set to a "in call periodic" alerting pattern. **Note:** If defined as "0", the ring splash alerting pattern is treated as Normal or Normal - delayed. This parameter is not applicable when the phone is in an idle state.
FORMAT	Numeric
DEFAULT VALUE	4 (seconds)
RANGE	N/A
EXAMPLE	ring splash frequency: 8

DISCREET RINGING SETTINGS

PARAMETER – *discreet ringing*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not the discreet ringing feature should be enabled. When enabled, during incoming calls, all applicable visual indicators (LED for the corresponding Line key, Message Waiting Indicator [MWI], etc...) will behave normally, but the ring tone will be played only once.
FORMAT	Boolean
DEFAULT VALUE	0 (Disabled)
RANGE	0 - 1 0 (Disabled) 1 (Enabled)
EXAMPLE	discreet ringing: 1

DROP SOFTKEY SETTINGS

Note: Applicable to the 6867i, 6869i, and 6873i IP Phones only.

PARAMETER – *drop context softkey*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows administrators the ability to manually configure whether or not the Drop softkey is displayed on screen. If the parameter is disabled, the Drop softkey will not be displayed in any active call screens (e.g. single point-to-point call, attended transfer and conference scenarios, conference calls, paging calls, and so on).
FORMAT	Boolean
DEFAULT VALUE	1
RANGE	0 - 1 0 (Disabled - **Drop** softkey removed) 1 (Enabled - **Drop** softkey displayed)
EXAMPLE	drop context softkey: 0

CUSTOMIZING M685I/M695 EXPANSION MODULE COLUMN DISPLAY

EXPANSION MODULE 1 THROUGH 3

PARAMETER – *expmodXpageNleft*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to specify a customized heading for the M685i expansion module, in the left column of a specific page. You can specify the following options for this parameter: Expansion Module 1 expmod1page1left (Expansion Module 1, Page 1, left column) expmod1page2left (Expansion Module 1, Page 2, left column) expmod1page3left (Expansion Module 1, Page 3, left column) Expansion Module 2 expmod2page1left (Expansion Module 2, Page 1, left column) expmod2page2left (Expansion Module 2, Page 2, left column) expmod2page3left (Expansion Module 2, Page 3, left column) Expansion Module 3 expmod3page1left (Expansion Module 3, Page 1, left column) expmod3page2left (Expansion Module 3, Page 2, left column) expmod3page3left (Expansion Module 3, Page 3, left column)
FORMAT	Text String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	expmod1page1left: Personnel Ext

PARAMETER – *expmodXpageNright*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to specify a customized heading for the M685i expansion module, in the right column of a specific page. You can specify the following options for this parameter: Expansion Module 1 expmod1page1right (Expansion Module 1, Page 1, right column) expmod1page2right (Expansion Module 1, Page 2, right column) expmod1page3right (Expansion Module 1, Page 3, right column) Expansion Module 2 expmod2page1right (Expansion Module 2, Page 1, right column) expmod2page2right (Expansion Module 2, Page 2, right column) expmod2page3right (Expansion Module 2, Page 3, right column) Expansion Module 3 expmod3page1right (Expansion Module 3, Page 1, right column) expmod3page2right (Expansion Module 3, Page 2, right column) expmod3page3right (Expansion Module 3, Page 3, right column)
FORMAT	Text String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	expmod1page1right: Operations Ext

ADVANCED OPERATIONAL PARAMETERS

The following parameters in this section allow the system administrator to set advanced operational features on the IP phones.

UACSTA SETTINGS

PARAMETER – *csta*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables/disables uaCSTA support on the phones. uaCSTA refers to the mechanism of transporting CSTA XML messages over a SIP session allowing for compatibility with SIP phone user agents.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 - 1 0 (Disabled) 1 (Enabled)
EXAMPLE	csta: 1

PARAMETER – *csta proxy*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The IP address or FQDN of the CSTA proxy server. The CSTA proxy a server that initiates and forwards requests generated by the SIP phone to the targeted user using CSTA XML messages.
FORMAT	IP address or FQDN
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	csta proxy: 192.1680.0.120

PARAMETER – *csta port*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the CSTA proxy server’s port number.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	N/A
EXAMPLE	csta port: 5060

PARAMETER – *csta password*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Password used to authenticate the phone with the CSTA proxy server.
FORMAT	Text
DEFAULT VALUE	N/A
RANGE	Up to 20 alphanumeric characters
EXAMPLE	csta password: 12345

BLIND TRANSFER SETTING

PARAMETER – *sip cancel after blind transfer*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Forces the phone to use the Blind Transfer method available in software prior to release 1.4. This method sends the CANCEL message after the REFER message when blind transferring a call.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sip cancel after blind transfer: 1

SEMI-ATTENDED TRANSFER SETTINGS

PARAMETER – *sip refer-to with replaces*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Flag for controlling the mode of a semi-attended transfer.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sip refer-to with replaces: 1

PARAMETER – *sip refer-to from contact*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	When enabled, the phone will check the user name from the contact header received in 180 response and: • if the contact header has user name, blind transfer the call to the user name or • if there is no contact header found or the contact header has no user name, put the remote address of the original INVITE to the Refer-To header.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sip refer-to from contact: 1

UPDATE CALLER ID SETTING

PARAMETER – *sip update callerid*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the updating of the Caller ID information during a call.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sip update callerid: 1

SIP UNREGISTER ON BOOT

PARAMETER – *sip unregister on boot*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables unregister on boot or reboot functionality on SIP phones.
FORMAT	Boolean
DEFAULT VALUE	0 (Disabled)
RANGE	0 - 1 0 (Disabled) 1 (Enabled)
EXAMPLE	sip unregister on boot: 1

BOOT SEQUENCE RECOVERY MODE SETTINGS

PARAMETER – *force web recovery mode disabled*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the forcing web recovery mode feature. If this parameter is set to "**1**", you cannot force web recovery. If this parameter is set to "**0**", press **1** and **#** keys during boot up when the logo displays to force the web recovery mode.
FORMAT	Boolean
DEFAULT VALUE	0 (false)
RANGE	0 (false) 1 (true)
EXAMPLE	force web recovery mode disabled: 1

PARAMETER – *max boot count*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the number of faulty boots that occur before the phone is forced into Web recovery mode.
FORMAT	Integer
DEFAULT VALUE	10
RANGE	0 to 32767 Zero (0) disables the max boot count feature.
EXAMPLE	max boot count: 0

BLACKLIST DURATION SETTING

PARAMETER – *sip blacklist duration*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the length of time, in seconds, that a failed server remains on the server blacklist. The IP phone avoids sending a SIP message to a failed server (if another server is available) for this amount of time. **Note:** The value of "**0**" disables the blacklist feature.
FORMAT	Integer
DEFAULT VALUE	300 (5 minutes)
RANGE	0 to 9999999
EXAMPLE	sip blacklist duration: 600

WHITELIST PROXY SETTING

PARAMETER – *sip whitelist*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This parameter enables/disables the whitelist proxy feature, as follows: • Set to 0 to disable the feature. • Set to 1 to enable the feature. When this feature is enabled, an IP phone accepts call requests from a trusted proxy server *only*. The IP phone rejects any call requests from an untrusted proxy server.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sip whitelist: 1

IPWHITELIST SETTING

PARAMETER – *ip whitelist*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	This parameter allows configuration of iptables to limit the number of incoming IP packets into the IP Phone. This helps in protecting your phone from a DoS attack.
FORMAT	ip address
DEFAULT VALUE	0.0.0.0
RANGE	100 IP addresses
EXAMPLE	ip whitelist: 1.1.1.1, 2.2.2.2

XML KEY REDIRECTION SETTINGS (FOR REDIAL, XFER, CONF, ICOM, VOICEMAIL)

PARAMETER – *redial script*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies a redial script for the phone to use. When this parameter is set, pressing the Redial key GETs the specified URI from the server to use in performing the redial action.
FORMAT	String
DEFAULT VALUE	empty
RANGE	Any valid URI
EXAMPLE	redial script: http://bluevelvet.ana.mitel.com/redial.php

PARAMETER – *xfer script*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies an Xfer script for the phone to use. When this parameter is set, pressing the Xfer key GETs the specified URI from the server instead of starting the transfer action.
FORMAT	String
DEFAULT VALUE	empty
RANGE	Any valid URI
EXAMPLE	xfer script: http://bluevelvet.ana.mitel.com/xfer.php

PARAMETER – *conf script*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies an Conf script for the phone to use. When this parameter is set, pressing the Conf key GETs the specified URI from the server to use in performing the conference action.
FORMAT	String
DEFAULT VALUE	empty
RANGE	Any valid URI
EXAMPLE	conf script: http://bluevelvet.ana.mitel.com/conf.php

PARAMETER – *icom script*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies an Icom script for the phone to use. When this parameter is set, pressing the Icom key GETs the specified URI from the server to use in performing the Intercom action.
FORMAT	String

DEFAULT VALUE	empty
RANGE	Any valid URI
EXAMPLE	icom script: http://bluevelvet.ana.mitel.com/icom.php

PARAMETER – *voicemail script*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies a Voicemail script for the phone to use. When this parameter is set, selecting the voicemail option from the Services Menu GETs the specified URI from the server instead of starting the Voicemail application.
FORMAT	String
DEFAULT VALUE	empty
RANGE	Any valid URI
EXAMPLE	voicemail script: http://bluevelvet.ana.mitel.com/voicemail.php

OPTIONS KEY REDIRECTION SETTING

PARAMETER – options script	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies an Options script for the phone to use. When this parameter is set, pressing the Options Key GETs the specified URI from the server. **Note:** Pressing and holding the Options key displays the local Options Menu on the phone.
FORMAT	String
DEFAULT VALUE	empty
RANGE	Any valid URI
EXAMPLE	options script: http://fargo.ana.mitel.com/options.xml

OFF-HOOK AND XML APPLICATION INTERACTION SETTING

PARAMETER – auto offhook	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies whether or not the phone is prevented from entering the off-hook/dialing state, if the handset is off-hook for more than 2 seconds, and the call ends.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled - phone is prevented from entering the off-hook dialing state) 1 (enabled - allows phone to enter the off-hook dialing state)
EXAMPLE	auto offhook: 1

XML OVERRIDE FOR A LOCKED PHONE SETTING

PARAMETER – *xml lock override*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the method to use for overriding a locked phone when XML applications are sent to the phone. There are three settings for this parameter: • **0 -** Phone prevents XML POSTs and XML GETs from being received or sent. • **1** - Phone allows XML POSTs; however, XML GETs by pressing the XML keys (softkeys/programmable keys/extension module keys) are not allowed. • **2** - Phone allows XML POSTs to the phone as well as XML GETs to/from the phone by pressing the XML keys (softkeys/programmable keys/extension module keys).
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 to 2
EXAMPLE	xml lock override: 1

SYMMETRIC UDP SIGNALING SETTING

PARAMETER – *sip symmetric udp signaling*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to enable or disable the phone to use port 5060 to send SIP UDP messages. The value “**1**” (which is the default) enables the phone to use port 5060. The value “**0**” (zero) disables the phone from using port 5060 and allows the phone to choose a random port to send SIP UDP messages. **Note:** This parameter should be disabled according to M5T.
FORMAT	Boolean
DEFAULT VALUE	1 (enabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sip symmetric udp signaling: 0

SYMMETRIC TLS SIGNALING SETTING

PARAMETER – *sips symmetric tls signaling*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to enable or disable the phone to use port 5061 as the persistent TLS connection source port. The valid values are - • 0 - disables the phone from using port 5061 and allows the phone to choose a random persistent TLS connection source port from the TCP range (i.e. 49152...65535) regardless of whether the parameter “sip outbound support” is enabled or disabled. • 1 - enables the phone to use port 5061, by default. • 2 - phone uses a random new port for reconnecting to the server over persistent TLS and forces close connection. • 3 - phone uses a random new port for reconnecting to the server over persistent TLS but does not force a close connection.
FORMAT	Integer
DEFAULT VALUE	1 (enabled)
RANGE	0 (disabled) 1 (enabled) 2 (new random port with forced close connection) 3 (new random port without forced close connection)
EXAMPLE	sips symmetric tls signaling: 0

USER-AGENT SETTING

PARAMETER – *sip user-agent*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows you to enable or disable the addition of the User-Agent and Server SIP headers in the SIP stack. The value of “0” prevents the UserAgent and Server SIP header from being added to the SIP stack. The value of “1” allows these headers to be added.
FORMAT	Boolean
DEFAULT VALUE	1 (true)
RANGE	0 (false) 1 (true)
EXAMPLE	sip user-agent: 0

GRUU AND SIP.INSTANCE SUPPORT

PARAMETER – *sip gruu*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg

DESCRIPTION	Enables or disables Globally Routable User-Agent URI (GRUU) support on the IP Phone according to draft-ietf-sip-gruu-15. If this parameter is disabled, parsing of inbound GRUU's for transfer are still enabled.
FORMAT	Boolean
DEFAULT VALUE	1 (enabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sip gruu: 0

DNS QUERY SETTING

PARAMETER – *sip dns query type*	CONFIGURATION FILES startup.cfg, <mac>.cfg
DESCRIPTION	Specifies the Domain Name Service (DNS) query method to use when the IP Phones issue requests for DNS records using one of three methods: “A” only, SRV & A, and NAPTR & SRV & A.
FORMAT	Integer
DEFAULT VALUE	1 (SRV & A)
RANGE	0**: A only** - The phone issues requests for “**A**” (Host IP Address) records from the DNS server to get the IP address, and uses the default port number of 5060. 1: **SRV & A** - The phone issues requests for “**SRV**” (Service Location Record) records from the DNS server to get the port number. Most often, the IP address is included in the response from the DNS server to avoid extra queries. If there is no IP address returned in the response, the phones send out the request for “**A**” records from the DNS server to find the IP address. 2: **NAPTR & SRV & A** - First, the phone sends "**NAPTR**" (Naming Authority Pointer) lookup to get the “**SRV**” pointer and service type. For example, if Global SIP transport protocol on the phone is “UDP”, and Proxy server on the phone is “test.mitel.com”, then: • If the **NAPTR** record is returned empty, the phone will use the default value “_sip._udp.test.mitel.com" for the “**SRV**” lookup. • If the **NAPTR** record is returned "test.mitel.com SIP+D2U .... _sip._udp.abc.mitel.com", the phone will use “_sip._udp.abc.mitel.com" for the “**SRV**” lookup. • If the **NAPTR** record is returned "test.mitel.com SIP+D2T .... _sip._tcp.test.mitel.com", where the service type TCP mismatches the phone configured transport protocol “UDP”, the phone will ignore this value and use the default value “_sip._udp.test.mitel.com" for the “**SRV**” lookup. **Note:** The phone does not use the service type sent by the **NAPTR** response to switch its transport protocol, nor does it use the **NAPTR** response to determine whether to use a secure or insecure communication path**.** The phone will always use a global sip protocol that is configured on the phone via configuration files or web user interface. After performing **NAPTR**, the phone sends “**SRV**” lookup to get the IP address and port number. If there is no IP address in the “**SRV**” response, then it sends out an “**A**” lookup to get it. **Note:** On the phone side, if you configure the phone with a Fully-Qualified Domain Name (FQDN) proxy and specified port, the phone always sends “**A only**” lookups to find the Host IP Address of the proxy.
EXAMPLE	sip dns query type: 2

IGNORE OUT OF ORDER SIP REQUESTS

PARAMETER – *sip accept out of order requests*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables a workaround for non-compliant SIP devices (for example, Asterisk) which do not increment the CSeq numbers in SIP requests sent to the phone.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	sip accept out of order requests: 1

OPTIONAL "ALLOW" AND "ALLOW-EVENT" HEADERS

PARAMETER – *sip notify opt headers*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables and disables whether or not the "Allow" and Allow-Events" optional headers are included in the SIP NOTIFY messages sent from the phone to the server.
FORMAT	Boolean
DEFAULT VALUE	1
RANGE	0 (disabled - optional headers are removed from the SIP NOTIFY message) 1 (enabled - no change; optional headers are included in SIP NOTIFY message)
EXAMPLE	sip notify opt headers: 0

P-ASSERTED IDENTITY (PAI)

PARAMETER – *sip pai*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables whether PAI information is displayed on the phone and specifies which URI field ("sip" or "tel") the phone should use when displaying the PAI URI information
FORMAT	Integer
DEFAULT VALUE	1
RANGE	0 - 4 0 - Disabled: PAI information is ignored. 1 - Use sip URI only: (Default) The phone will use the URI information contained in the "sip" URI field (if available) and ignore the information contained in the "tel" URI field (if available). 2 - sip URI preferred: The phone will use the URI information contained in the "sip" URI field. If the "sip" URI field is unavailable, the phone will use the URI information contained in the "tel" URI field. 3 - Use tel URI only: The phone will use the URI information contained in the "tel" URI field (if available) and ignore the information contained in the "sip" URI field (if available). 4 - tel URI preferred: The phone will use the URI information contained in the "tel" URI field. If the "tel" URI field is unavailable, the phone will use the URI information contained in the "sip" URI field. **Note:** The default value (i.e. "1") will be enforced if this parameter is defined with any unsupported value.
EXAMPLE	sip pai: 3

ROUTE HEADER IN SIP PACKET

PARAMETER – *sip remove route*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables and disables the addition of the Route header in a SIP packet. Enable this parameter for outbound proxies that do not support Route headers. **Note:** When enabled this will break all support for SIP routing, so if some other device in the network attempts to add itself to the route it will fail.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 (disable - adds the Route header to the packet) 1 (enable - removes the Route header from the packet)
EXAMPLE	sip remove route: 1

COMPACT SIP HEADER

PARAMETER – *sip compact headers*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the IP phones to use compact SIP headers in the SIP packets sent from the phone.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled- uses long SIP header format)
RANGE	0 (disabled- uses long SIP header format) 1 (enabled- uses short (compact) SIP header format)
EXAMPLE	sip compact headers: 1

REJECTION OF INV OR BYE

PARAMETER – *sip enforce require hdr*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables and disables the rejection of an INV or BYE with a “420 Bad Extension” if the INV or BYE contains an unsupported value in the REQUIRE header.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 (disable) 1 (enable)
EXAMPLE	sip enforce require hdr: 1

CONFIGURATION ENCRYPTION SETTING

PARAMETER – *config encryption key*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the phone-specific encryption key that the configuration server uses to encrypt in a MAC-specific configuration file.
FORMAT	String
DEFAULT VALUE	Not applicable
RANGE	String length of 4 to 32 alphanumeric characters
EXAMPLE	config encryption key: 123abcd

DNS HOST FILE

PARAMETER – *sip dns host file*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The UNIX-format host file on the configuration server. The phone(s) download this file to perform DNS lookups on the local network instead of the service provider's public network. **Note:** If using a text file on a PC to enter this value, you must enter a carriage return (CR) after entering the host file name.
FORMAT	UNIX format using Carriage Return (CR) or Carriage Return + Line Feed (CRLF) to terminate each line
DEFAULT VALUE	N/A
RANGE	File name allows Alpha-numeric characters
EXAMPLE	sip dns host file: hostfile.txt

DNS SERVER QUERY

PARAMETER – *sip dns srvX name* **Note:** The "X" indicate a record number with values from 1 to 4.	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The fully qualified URI of the DNS SRV record
FORMAT	Fully qualified URI including service prefix
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	sip dns srv1 name: _sip._udp.example.com

PARAMETER – *sip dns srvX priority* **Note:** The "X" indicate a server number with values from 1 to 4.	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The priority level assigned to this DNS server. After this parameter is downloaded from the configuration server to the phone, the phone uses the DNS server with the lowest numbered priority first to perform DNS lookups.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 to 65535
EXAMPLE	sip dns srv1 priority: 10

PARAMETER – *sip dns srv1 weight*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The weight level assigned to this server. If a service has multiple SRV records with the same priority value, the phones use the weight field to determine which host to use. The weight value is relevant only in relation to other weight values for the service, and only among records with the same priority value.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 to 65535
EXAMPLE	sip dns srv1 weight: 60

PARAMETER – *sip dns srvX port* **Note:** The “X” indicate a server number with values from 1 to 4.	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The port number on the target host.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	0 to 65535
EXAMPLE	sip dns srv1 port: 5060

PARAMETER – *sip dns srvX target* **Note:** The “X” indicate a server number with values from 1 to 4.	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	The host name of the target.
FORMAT	Host name or fully qualified domain name
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	sip dns srv1 target: bigbox.example.com

DNS-SRV HANDLING FOR DIFFERENT 5XX ERROR CONDITIONS

SERVICE UNAVAILABLE STATUS CODES

PARAMETER – *sip service unavailable status codes*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Configure service unavailable status codes on the SIP phone.
FORMAT	Integer
DEFAULT VALUE	N/A
RANGE	300 - 699
EXAMPLE	sip service unavailable status codes: 500, 501, 502, 503, 504, 505, 513

SERVICE UNAVAILABLE RESPONSE FAILOVER RULE

PARAMETER – *sip service unavailable failover rule*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Configure service unavailable response failover rule on the SIP phones.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 - 1 0 (failover only if the service unavailable response is the first response received) 1 (failover when the service unavailable response is received and no response other than 100 trying responses were received for the SIP request)
EXAMPLE	sip service unavailable failover rule: 0

DNS SRV FAILOVER MODE

PARAMETER – *sip srv failover enabled*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Configure DNS SRV failover mode on the SIP phones.
FORMAT	Integer
DEFAULT VALUE	0 (Disabled)
RANGE	0 - 2 0 (DNS SRV failover is disabled) 1 (DNS SRV failover is enabled, current behavior) 2 (DNS SRV failover following registration, new behavior)
EXAMPLE	sip srv failover enabled: 2

DNS MAXIMUM CACHE TTL SETTINGS

PARAMETER – *sip dns cache negative max ttl*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the DNS maximum cache TTL for negative responses.
FORMAT	Integer
DEFAULT VALUE	-1 (5 minutes)
RANGE	0 - 2147483647 (seconds) (0 = Disabled)
EXAMPLE	sip dns cache negative max ttl: 3600

PARAMETER – *sip dns cache positive max ttl*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the DNS maximum cache TTL for positive responses.
FORMAT	Integer
DEFAULT VALUE	-1 (5 minutes)
RANGE	0 - 2147483647 (seconds) (0 = Disabled)
EXAMPLE	sip dns cache positive max ttl: 3600

REUSE OF EXPIRED DNS RECORD SETTINGS

PARAMETER – *sip dns use cached expired response*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies if expired DNS records are to be reused in case of DNS server errors.
FORMAT	Boolean
DEFAULT VALUE	0 (Disabled)
RANGE	0 (Do not reuse expired DNS records, in case DNS server errors occur) 1 (Reuse expired DNS records, in case DNS server errors occur)
EXAMPLE	sip dns use cached expired response: 1

SIP SERVICES/RTCP SUMMARY REPORTS TRANSPORT PROTOCOL SETTINGS

SIP SERVICES

PARAMETER – *sip services transport protocol*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the transport protocol used for SIP services.
FORMAT	Numeric
DEFAULT VALUE	-1 (Invalid)
RANGE	-1 (Invalid) 0 (TCP/UDP) 1 (UDP) 2 (TCP) 3 (Not used) 4 (Persistent TLS or TLS)
EXAMPLE	sip services transport protocol: 1

PARAMETER – *sip services port*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the port used for SIP services.
FORMAT	Numeric
DEFAULT VALUE	5060
RANGE	Greater than 1024 and less than 65535
EXAMPLE	sip services port: 7300

RTCP SUMMARY REPORTS

PARAMETER – *sip rtcp summary reports transport protocol*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the transport protocol used for sending RTCP summary reports. This parameter takes effect when at least one line has RTCP summary reports enabled. **Note:** The parameter "sip symmetric udp signaling" is effective when the transport protocol for RTCP summary reports is set to UDP.
FORMAT	Numeric
DEFAULT VALUE	1 (UDP)
RANGE	0 (TCP/UDP) 1 (UDP) 2 (TCP)
EXAMPLE	sip rtcp summary reports transport protocol: 2

ALPHANUMERIC INPUT ORDER FOR USERNAME PROMPTS

Note: Applicable to the 6863i and 6865i IP Phones only.

PARAMETER – *username alphanumeric input order*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	When enabled, this parameter changes the default behavior of the keypad input order during username and password prompts from uppercase letters > digit > lowercase letters to digit > uppercase letters > lowercase letters. For example, when pressing “2” on the keypad during a username prompt with this parameter disabled (default) each key press will successively enter the letter/digit A, B, C, 2, a, b, c. When enabled, each key press will successively enter 2, A, B, C, a, b, c.
FORMAT	Integer
DEFAULT VALUE	1 (Digit first)
RANGE	0-1 0 (Uppercase letters first) 1 (Digit first)
EXAMPLE	username alphanumeric input order: 0

ACTIVE VOIP RECORDING SETTINGS

WARNING: WHEN A RECORDING SESSION IS IN PROGRESS, THE RESPECTIVE IP PHONES DISPLAY A RECORDING ICON ON SCREEN. THE RECORDING ICON IS DISPLAYED ON THE IP PHONES TO INDICATE THE RECORDING SESSION IS ACTIVE AND THAT A DUPLICATE COPY OF THE RTP/SRTP STREAM IS TO BE SENT FROM THE PHONE TO THE RECORDING SERVER. THE OVERALL RECORDING AND ITS QUALITY IS DEPENDENT ON THE RECORDING SERVER AND THE NETWORK.

PARAMETER – *recorder addressN* (N is a number from 1 to 6)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies a trusted IP address (maximum of six) corresponding to the voice recording system. The IP phone will check and respond to SIP messages coming from these IP addresses on the port defined by the “sip services port” parameter. **Note:** If all of the “recorder addressN” parameters are left undefined, the active IP voice recording feature is disabled.
FORMAT	IP Address
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	recorder address1: 192.168.1.20 recorder address2: 192.168.1.21 recorder address3: 192.168.1.22 recorder address4: 192.168.1.23 recorder address5: 192.168.1.24 recorder address6: 192.168.1.25

PARAMETER – *recording destinationN* (N is a number from 1 to 6)	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies trusted IP addresses (maximum of six) corresponding to the destination where the RTP/SRTP packets should be sent. The IP phone will check to see if the destination IP addresses are trusted before sending the duplicated RTP/SRTP packets. **Note:** If all of these parameters are left undefined, no authentication checks will be performed.
FORMAT	IP Address
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	recording destination1: 192.168.1.30 recording destination2: 192.168.1.31 recording destination3: 192.168.1.32 recording destination4: 192.168.1.33 recording destination5: 192.168.1.34 recording destination6: 192.168.1.35

PARAMETER – *recording periodic beep*	CONFIGURATION FILES startup.cfg, <mac>.cfg
DESCRIPTION	Specifies how often (in seconds) the periodic beep tone (notifying users that their call is being recorded) should be played.
FORMAT	Integer
DEFAULT VALUE	15 (seconds)
RANGE	0 (Disabled) 15 30 45 60
EXAMPLE	recording periodic beep: 30

PARAMETER – *recording beep direction*	CONFIGURATION FILES startup.cfg, <mac>.cfg
DESCRIPTION	Specifies where the periodic beep tone (notifying users that their call is being recorded) should be played.
FORMAT	Integer
DEFAULT VALUE	1 (Network)
RANGE	0-2 0 (Local) 1 (Network) 2 (Both Local and Network)
EXAMPLE	recording beep direction: 2

XSI FEATURE SETTINGS

PARAMETER – *xsi allow sip authentication*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables Xsi SIP authentication. When Xsi SIP authentication is enabled, the phone sends the configured BroadWorks Xsi user name ("**sip xsi user name**" parameter) along with the SIP authentication user name ("**sip auth name**" parameter) and password ("**sip password**" parameter) to authenticate the Xsi interface. This allows users to authenticate without having to manually enter their login credentials.
FORMAT	Boolean
DEFAULT VALUE	0
RANGE	0 - 1 0 (Disabled) 1 (Enabled)
EXAMPLE	xsi allow sip authentication: 1

PARAMETER – *sip xsi user name*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Global parameter that specifies the user name used for authentication of the Xsi account when using Xsi SIP authentication. The user name must match the value specified in the "**sip auth name**" parameter.
FORMAT	<sip auth name>@<server>
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	sip xsi user name: 5553456@xsi.broadworks.net

PARAMETER – sip lineN xsi user name (where N = line number)	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Per-line parameter that specifies the user name used for authentication of the Xsi account when using Xsi SIP authentication. The user name must match the value specified in the "**sip lineN auth name**" parameter.
FORMAT	<sip lineN auth name>@<server>
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	sip line1 xsi user name: 5553456@xsi.broadworks.net sip line2 xsi user name: 5551234@xsi.broadworks.net

PARAMETER – *xsi user name*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the user name used for normal authentication (not SIP authentication) of the Xsi account.
FORMAT	<username>@<server>
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	xsi user name: xsi@xsi.broadworks.net

PARAMETER – *xsi ip*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the Xsi Enterprise Directory credentials (if applicable) and IP address or Fully Qualified Domain Name (FQDN) of the Xsi server in the following syntax: server or username:password@server **Note:** Xsi credentials defined through the "**xsi ip**" parameter are only applicable to the Xsi Enterprise Directory feature and not applicable to user-related Xsi features such as Speed Dial 8, Basic Call Logs, and Personal Directory Contacts. Credentials for the user-related Xsi features require encryption and therefore must be entered through the phone's Options List > Credentials menu.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLES	xsi ip: xsp.xsi.broadworks.net or xsi ip: johndoe:mitel123@xsp.xsi.broadworks.net

PARAMETER – *xsi protocol*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the protocol (either HTTP or HTTPs) used for communicating with the Xsi server.
FORMAT	String
DEFAULT VALUE	http
RANGE	http https
EXAMPLE	xsi protocol: https

PARAMETER – *xsi port*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the port used for communicating with the Xsi server.
FORMAT	Integer
DEFAULT VALUE	80 (when protocol used is HTTP) 443 (when protocol used is HTTPs)
RANGE	Any valid port
EXAMPLE	xsi port: 8080

PARAMETER – *xsi speeddial8 enabled*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables Xsi Speed Dial 8 functionality.
FORMAT	Boolean
DEFAULT VALUE	0 (Disabled)
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	xsi speeddial8 enabled: 1

PARAMETER – *xsi calllogs enabled*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables Xsi Basic Call Log functionality.
FORMAT	Boolean
DEFAULT VALUE	0 (Disabled)
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	xsi calllogs enabled: 1

PARAMETER – *xsi hide number enabled*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables Xsi Hide Number functionality.
FORMAT	Boolean
DEFAULT VALUE	0 (Disabled)
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	xsi hide number enabled: 1

PARAMETER – *xsi call center*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables Xsi join/unjoin call center functionality.
FORMAT	Boolean
DEFAULT VALUE	0 (Disabled)
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	xsi call center: 1

PARAMETER – *xsi remote office*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables Xsi Remote Office functionality.
FORMAT	Boolean
DEFAULT VALUE	0 (Disabled)
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	xsi remote office: 1

PARAMETER – *xsi simultaneous ring personal*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables Xsi Simultaneous Ring Personal functionality.
FORMAT	Boolean
DEFAULT VALUE	0 (Disabled)
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	xsi simultaneous ring personal: 1

PARAMETER – *xsi broadworks anywhere*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables Xsi BroadWorks Anywhere functionality.
FORMAT	Boolean
DEFAULT VALUE	0 (Disabled)
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	xsi broadworks anywhere: 1

PARAMETER – *xsi broadworks anywhere locations*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the number of BroadWorks Anywhere locations that can be viewed and edited through the phone's native UI.
FORMAT	Integer
DEFAULT VALUE	10
RANGE	1 - 25
EXAMPLE	xsi broadworks anywhere locations: 25

SETTINGS FOR RE-BRANDING BROADSOFT-RELATED FEATURE UI STRINGS

PARAMETER *broadsoft branding*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows service providers the ability to replace BroadSoft-related feature strings (e.g. "BroadSoft SCA", "BSFT Call Settings, "BroadWorks Anywhere") in the UI with their own custom branding names.
FORMAT	String in the following format: "<full name>;<short name>;<platform name>" **Note**: To ensure the applicable UI strings are not truncated on the 6863i and 6865i, it is recommended to limit the character length of the short name value to four when the screen language is configured as English. Maximum character lengths may vary when a different screen language is configured.
DEFAULT VALUE	"BroadSoft;BSFT;BroadWorks"
RANGE	N/A
EXAMPLES	broadsoft branding: "Mitel;MTL;MiVoice" broadsoft branding: ";MTL;" broadsoft branding: ";MTL;MiVoice" broadsoft branding: ";;"

UC-ONE INTEROPERABILITY SETTINGS

PARAMETER – *instant messaging and presence*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables interoperability with XMPP-based BroadSoft UC-ONE presence services.
FORMAT	Boolean
DEFAULT VALUE	0 (Disabled)
RANGE	0 (Disabled) 1 (Enabled)
EXAMPLE	instant messaging and presence: 1

PARAMETER – *imp user name*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the user name used for authentication of the XMPP BroadSoft UC-ONE presence account.
FORMAT	<username>@<server>
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	imp user name: johnsmith@imp.broadsoft.com

PARAMETER – *imp password*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the password used for authentication of the XMPP BroadSoft UC-ONE presence account.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	imp password: Mitel2016

PARAMETER – *imp ip*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the IP used for communicating with the XMPP UC-ONE presence server.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	imp ip: imp.broadsoft.com

PARAMETER – *imp port*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the port used for communicating with the XMPP UC-ONE presence server.
FORMAT	Integer
DEFAULT VALUE	5222
RANGE	Any valid port
EXAMPLE	imp port: 5221

BROADSOFT BROADWORKS EXECUTIVE AND ASSITANT SERVICES SETTINGS

Note: Applicable to the 6865i, 6867i, 6869i, and 6873i SIP phones only.

PARAMETER – *sip execassist filter call prefix*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the prefix of the Alerting Custom Calling Line ID name configured for Executives. For an incoming call, the phone will treat the call as a filtered call if the prefix is found in the front of the display name of the FROM header of the INVITE. The prefix from the display name of the FROM header or PAI header will be stripped before it is displayed on the phone's screen. For example, if the From header sent by the BroadWorks call manager SIP INVITE message is: From:"[F] Filtrage -> Dupont, Francois"<sip:5551234567@as.aastra.com;user=phone> then the IP phone displays the calling name as "Filtrage -> Dupont, Francois" since the "[F]" prefix is removed.
FORMAT	String (in quotations)
DEFAULT VALUE	"[F]"
RANGE	N/A
EXAMPLE	sip execassist filter call prefix: "[F]"

PARAMETER – *sip execassist fac call push*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the Feature Access Code (FAC) for the BroadSoft Executive- Assistant Call Push feature.
FORMAT	String (in quotations)
DEFAULT VALUE	"#63"
RANGE	N/A
EXAMPLE	sip execassist fac call push: "#63"

PARAMETER – *sip execassist fac initiate call*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the Feature Access Code (FAC) for the BroadSoft Executive- Assistant Initiate Call feature.
FORMAT	String (in quotations)
DEFAULT VALUE	"#64"
RANGE	N/A
EXAMPLE	sip execassist fac initiate call: "#64"

VISITOR DESK PHONE SETTINGS

Note: For VDP functionality, the phone must be configured to accept XML SIP NOTIFY messages. See “XML SIP Notify Settings” on page A-193 for more information.

PARAMETER – *user config url*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the configuration server URL where the <user>.cfg is located when utilizing the Visitor Desk Phone (VDP) feature.
FORMAT	String (up to 256 characters) FTP - “ftp://server:port/path” TFTP - “tftp://server:port/path” HTTP - “http://server:port/path” HTTPS - “https://server:port/path”
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	user config url: http://100.200.50.79/vdp

PARAMETER – *backup user config url*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	When defined, a secondary server can be configured with the phone to download and upload the user config in the event of failure of the primary server.
FORMAT	String
DEFAULT VALUE	N/A
RANGE	maximum length 256 characters
EXAMPLE	backup user config url: http://example.com/vdp

PARAMETER *hot desk high security*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables a higher security level on the phone when using the VDP feature. When enabled, the phone will require a password to log out and will require users to re-enter their login credentials when phone is restarted.
FORMAT	Integer
DEFAULT VALUE	1 (Enabled)
RANGE	0-1 0 (Disabled) 1 (Enabled)
EXAMPLES	hot desk high security: 0

PARAMETER – *user config upload*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the time period (in seconds) between “<user>_local.cfg” saves (while the user is logged in).
FORMAT	Integer
DEFAULT VALUE	3600 (1 hour)
RANGE	5 – 9999999 **Note:** A value “0” will disable this feature.
EXAMPLE	user config upload: 600

PARAMETER – *user config upload delta*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Used in conjunction with the “user config upload” parameter, this parameter is utilized to help distribute the file transfers to the config ration server in a more even manner (i.e. so that the server does not get bombarded by file transfer requests all at the same time). After the initial save, the “<user>_local.cfg” is saved at a random time period between the values defined in the “user config upload” parameter and this “user config upload delta” parameter. This parameter specifies the upper limit of the extra random time (in seconds) added to the time defined in the “user config upload” parameter.
FORMAT	Integer
DEFAULT VALUE	60 (1 minute)
RANGE	0 – 9999999 **Note:** A value “0” will disable this feature.
EXAMPLE	user config upload delta: 120

PARAMETER – *user config upload control*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Controls when the" <user>_local.cfg" will be uploaded/saved.
FORMAT	Integer
DEFAULT VALUE	1
RANGE	0 – 2 **0** (Every time the "user config upload" time period expires and at every logout regardless of if the <user>_local.cfg has changed or not). **1** (When the "user config upload" time period expires but only if the <user>_local.cfg has changed, and at every logout regardless of if the <user>_local.cfg has changed or not). **2** (Only if the <user>_local.cfg has changed. Checked when the "user config upload" time period expires and at logout).
EXAMPLE	user config upload control: 2

MICLOUD TELEPO MUSIC ON HOLD SETTINGS

PARAMETER *sip moh server*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	(Global parameter) Specifies the media server SIP address providing the audio stream for music on hold functionality. If defined, the phone will use the specified server to provide an audio stream to any held parties globally. The audio stream will be offered in all cases when a remote party is placed on hold (i.e. when placed on hold directly, when placed on hold while performing a transfer or conference, or when the local party switches lines).
FORMAT	String (SIP address excluding the domain name)
DEFAULT VALUE	Empty
RANGE	N/A
EXAMPLES	sip moh server: musiconhold

PARAMETER	CONFIGURATION FILES
sip lineN moh server (where N = line number)	startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	(Per-line parameter) Specifies the media server SIP address providing the audio stream for music on hold functionality. If defined, the phone will use the specified server to provide an audio stream to any held parties on the specific line. The audio stream will be offered in all cases when a remote party is placed on hold (i.e. when placed on hold directly, when placed on hold while performing a transfer or conference, or when the local party switches lines).
FORMAT	String (SIP address excluding the domain name)
DEFAULT VALUE	Empty
RANGE	N/A
EXAMPLES	sip line2 moh server: musiconhold

UAC SESSION REFRESH SETTINGS

PARAMETER – *sip force uac session refresh*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
Description	Used when Session Refresh is required to be performed by the UAC. When enabled, if an INVITE with a Session-Expires header with no refresher parameter is received, the Session-Expires header and refresher=uac parameter are added to the 200 OK response. This ensures the refresh is performed by the call initiator. **Note:** The "**sip session timer**" configuration parameter must be configured to enable UAC Session Refresh feature functionality.
FORMAT	Boolean
Default Value	0 (Disabled)
Range	0 - 1 0 (Disabled) 1 (Enabled)
Example	sip force uac session refresh: 1

ROC RESET BEHAVIOR SETTINGS

PARAMETER – *srtp loose roc*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
Description	Enables or disables a Rollover Counter (ROC) reset in scenarios where a re-INVITE is sent but the media Synchronization Source (SSRC) identifier value is left unchanged.
FORMAT	Boolean
Default Value	0 (Disabled)
Range	0 - 1 0 (Disabled - Strict adherence to RFC3711. Does not reset ROC after a re-INVITE). 1 (Enabled - Loose adherence to RFC3711. Resets ROC after a re-INVITE).
Example	srtp loose roc: 1

SRTP AES_256_CM ENCRYPTION SETTINGS

PARAMETER – *srtp aes256*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables or disables the SRTP AES_256_CM support on the SIP phones.
FORMAT	Boolean
DEFAULT VALUE	0 (Disabled)
RANGE	0 - 1 0 (Disabled) 1 (Enabled)

EXAMPLE	srtp aes256: 1

TROUBLESHOOTING PARAMETERS

The following parameters in this section allow the system administrator to set logging and support settings for troubleshooting purposes.

Note: Enabling the syslog module and configuring debug levels should only be used for support purposes. Mitel recommends Administrators leave the debug level at its default for normal production use. Enabling all the debug levels on the phone will impact performance and normal operation of the phone.

LOG SETTINGS

PARAMETER – *log server ip*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the IP address of the log server to which log information will be transmitted.
FORMAT	IP address
DEFAULT VALUE	0.0.0.0
RANGE	N/A
EXAMPLE	log server ip: 192.168.3.2

PARAMETER – *log server port*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the IP port of the log server. This is the IP port that transmits information from the IP phone to the IP address location.
FORMAT	Integer
DEFAULT VALUE	0
RANGE	Any valid IP port
EXAMPLE	log server port: 2

PARAMETER – *log module <module name>*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Allows enhanced severity filtering of log calls sent as blog output. The blog, as used on the IP phones, is a an online debugging tool that can be frequently updated and intended for technical support analysis. Blogs are defined by their format: a series of entries posted to a single page in reverse-chronological order. The IP Phone blogs are separated into modules which allow you to log specific information for analyzing: Module Name (configuration files) • linemgr (line manager information) • audiomgr (audio manager information) • user interface • misc (miscellaneous) • sip (call control SIP stack) • dis (display driver) • dstore (delayed storage) • ept (endpoint) • ind (indicator) • kbd (keyboard) • net (network) • provis (provisioning) • rtpt (Real Time Transport) • snd (sound) • prof (profiler) • xml (Extension Markup Language) • lldp (Link Layer Discovery Protocol) **Note:** When the log issue parameter is disabled (default value), logging levels for all modules will be default to 1 unless set differently in the configuration files. When the log issue parameter is enabled, the IP phone sets the logging level to 8191 for the following four modules: • log module linemgr: 8191 • log module audiomgr: 8191 • log module user interface: 8191 • log module misc: 8191 • log module sip: 8191(When registered with MiCloud Connect or MiVoice Connect) • log module provis: 8191 For details, see on page A-355.
FORMAT	Integer
DEFAULT VALUE	1 (Fatal Errors)

RANGE

DEBUG LEVEL	VALUE
Fatal Errors	1
Errors	2
Warnings	4
Init	8
Functions	16
Info	32
All debug levels OFF	0
All Debug Levels ON	65535

EXAMPLE

Enter a debug level value in the "**Debug Level**" field for a module.

Example 1

To turn two or more debug levels on at the same time, you add the value associated with each level. For example,

Fatal Errors + Errors + Warnings = 1 + 2 + 4 = 7

log module linemgr: 7

log module user interface: 7

log module sip: 7

In the above example, fatal errors, general errors, and warnings are logged for the line manager, user interface, and SIP call control modules.

Example 2

Functions and Info = 16 + 32 = 48

log module dis: 48

log module net: 48

log module snd: 48

In the above example, functions and general information are logged for the display drivers, network, and sound modules.

Example 3

log module rtpt: 0

log module ind: 65535

In the above example, all debug levels are OFF for the Real Time Transport module. All debug levels are ON for the indicator module.

You can set the Module/Debug Levels using the configuration files or the Mitel Web UI.

WATCHDOG SETTINGS

PARAMETER – *watchdog enable*	CONFIGURATION FILES startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables/disables the use of the WatchDog task for the IP Phones.

FORMAT	Boolean
DEFAULT VALUE	1 (enabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	watchdog enable: 0

CRASH FILE RETRIEVAL

PARAMETER – *upload system info server*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Specifies the server for which the phone sends the system and crash files (server.cfg, local.cfg, and crash.gz).
FORMAT	IP address or qualified domain name. Supported protocols are TFTP, FTP, HTTP, and HTTPS. Example: tftp://0.0.0.0:port/path ftp://username:password@0.0.0.0:port/path http://0.0.0.0:port/path https://0.0.0.0:port/path
DEFAULT VALUE	N/A
RANGE	N/A
EXAMPLE	upload system info server: tftp://132.432.0.43:69/sysinfo

PARAMETER – *upload system info manual option*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables and disables the ability to manually upload support information from the IP Phone UI and Mitel Web UI. IP Phone UI: *Options->Phone Status->Upload System Info* Mitel Web UI: *Status->System Information->Support Information* When this parameter is enabled, an "**Upload System Info**" option displays on the IP Phone UI AND an <**Upload**> button displays on the System Information page in the Mitel Web UI.
FORMAT	Boolean
DEFAULT VALUE	1 (enabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	upload system info manual option: 1

PARAMETER – *upload system info on crash*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enables and disables the watchdog to automatically reboot the phone and send a crash file to the pre-defined server.
FORMAT	Boolean
DEFAULT VALUE	0 (disabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	upload system info on crash: 1

DIAGNOSTICS

PARAMETER – *diagnostics*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Enabled and disables the display of Log Issue key and Diagnostic menu in User/Admin settings.
FORMAT	Boolean
DEFAULT VALUE	1 (enabled)
RANGE	0 (disabled) 1 (enabled)
EXAMPLE	diagnostics: 0

PARAMETER – *cloud diagnostic server*	**CONFIGURATION FILES** startup.cfg, <model>.cfg, <mac>.cfg
DESCRIPTION	Defines the server and path where the phone uploads logs and Capture Trace. Supports TFTP, HTTP, HTTPS and FTP. If no protocol specified, uses FTP with anonymous credentials
FORMAT	IP address
DEFAULT VALUE	Empty
RANGE	NA
EXAMPLE	cloud diagnostic server: 10.30.108.7 cloud diagnostic server: ftp://test:pin@10.30.108.7

Appendix B

CONFIGURING THE IP PHONE AT THE ASTERISK IP PBX

ABOUT THIS APPENDIX

This appendix describes how to setup a user's 6800 series phone with an extension to make and receive calls using the Asterisk as the PBX.

TOPICS

This appendix covers the following topics:

IP PHONE AT THE ASTERISK IP PBX

The following configuration illustrates how to create a user with an extension to make and receive calls using the Asterisk as the PBX. This configuration is defined in the *sip.conf* file present along with the other configuration files that are created when Asterisk is installed. Usually, the configuration files can be found at the */etc/asterisk* directory.

```
;This is used in the “extensions.conf” file to identify this
;physical phone when issuing Dial commands.
[phone1]

;The type to use for the 6867i is “friend”.
;”Peer” is used when the Asterisk is contacting a proxy,
;”user” is used for phones that can only make calls
;and “friend” acts as both a peer and a user.
type=friend

;If your host has an entry in your DNS then you just enter the
;machines name in the host= field.
host=dynamic

defaultip=192.168.1.1   ;default IP address that the phone is
                        ;configured to

;The password that phone1 will use to register with this PBX
secret=1234

dtmfmode=rfc2833;Choices are inband, rfc2833, or info
mailbox=1000  ;Mailbox for message waiting indicator

;If a phone is not in a valid context you will not be
;able to use it. In this example' sip' is used. You can use
;whatever you like, but make sure they are the same, you will
;need to make an entry in your extensions.conf file (which we
;will get to later)

context=sip

callerid="Phone 1" <1234>
```

After this is defined in the “sip.conf” file, some information has to be entered in the “extensions.conf” file present in the same directory as the “sip.conf” file. The following definition in the file under the [sip]section/context completes defining the extension for the 6867i phone:

exten -> 1234,1,Dial(SIP/phone1,20)

This definition completes configuring the 6867i phone at the IP PBX system.

To verify whether the extension has been successfully registered at the IP PBX system, enter the Asterisk console and reload Asterisk. Use the command “sip show peers” at the console. This will display the extensions that are registered at the IP PBX system.

NAME/USERNAME	HOSTMASK	MASK	PORT	STATUS
phone1/phone1	192.168.1.1	(D)255.255.255.255	5060	Unmonitored

This completes the basic set-up for the 6867i phone with 1234 extension at the Asterisk IP PBX system. Refer to Asterisk documentation for set-up on extended or advanced features such as voicemail and call forwarding, etc.

Appendix C

SAMPLE CONFIGURATION FILES

ABOUT THIS APPENDIX

This appendix provides sample configuration files for the 6869i, 6865i, and 6920 IP phones. Sample 6867i and 6873i configuration files can be derived from the 6869i sample. Sample 6863i configuration files can be derived from the 6865i sample. Sample 6930, 6940, and 6970 configuration files can be derived from the 6920 sample.

TOPICS

This appendix covers the following topics:

SAMPLE CONFIGURATION FILES

This section consists of the sample configuration files necessary to configure the IP phones. The general format is similar to configuration files used by several Unix-based programs. Any text following a number sign (#) on a line is considered to be a comment, unless the # is contained within double-quotes. Currently, Boolean fields use 0 for false and 1 for true.

6869I SAMPLE CONFIGURATION FILE

```
# Sample Configuration File
# ===========================

# Phone Model: 6869i

# Notes:
#
# The general format used here is similar to configuration files
# used by several UNIX-based programs. Any text following a number
# sign (#) is considered to be a comment, unless the number sign is
# contained within double-quotes ("#") where it is considered to be
# a pound. For Boolean fields, 0 = false, 1 = true.

# Comments:
#
# This file contains sample configurations for the "startup.cfg", <model>.cfg, or
# "<mac>.cfg" file. The settings included here are examples only.
# You should change/comment the values to suit your requirements.
#
# Not all possible parameters are shown, refer to the admin guide for
# the full list of supported parameters, their defaults and valid
# ranges.
#
# The Mitel 6800 Series IP phones will download 2
# configuration files from the TFTP server while restarting, the
# "startup.cfg" file, the "<model>.cfg" file, and the "<mac>.cfg" file. These three configuration
# files can be used to configure all of the settings of the phone with
# the exception of assigning a static IP address to a phone and line
# settings, which should only be set in the "<mac>.cfg" file.
#
# The "startup.cfg" file configures the settings server wide, the "<model>.cfg" file contains model
# specific information (for example, "6869i.cfg"), while the "<mac>.cfg" file configures only the
# phone with the MAC address for which the file is named (for example, "00085d0304f4.cfg"). The
# settings in the "startup.cfg" file will be overridden by settings in the <model>.cfg file, and
# settings in the "<mac>.cfg" file override both settings in the "<model>.cfg" and the
# "startup.cfg" files.
#-------------------------------------------------------------------
```

```
# DHCP Setting
# ==============

#dhcp: 1 # DHCP enabled.

# DHCP:
# 0 = false, means DHCP is disabled.
# 1 = true, means DHCP is enabled.
#
# Notes:
#
#  DHCP is normally set from the Options list on the phone or
#  the web interface
#
#  If DHCP is disabled, the following network settings will
#  have to be configured manually either through the configuration
#  files, the Options List in the phone, or the Web Client: IP
#  Address (of the phone), Subnet Mask, Gateway, DNS, and TFTP
#  Server.
#--------------------------------------------------------------------


# Network Settings
## = = = = = = = =

# Notes: If DHCP is enabled, you do not need to set these network
# settings. Although depending on you DHCP server configuration you
# may still have to set the dns address.

#ip:     # This value is unique to each phone on a server
         # and should be set in the "<mac>.cfg" file if
         # setting this manually.

#subnet mask:
#default gateway:
#dns1:
#dns2:


# Time Server Settings
## =====================

#time server disabled: 1  # Time server disabled.
#time server1:            # Enable time server and enter at
#time server2:            # least one time server IP address or
#time server3: # qualified domain name

# Time Server Disabled:
#   0 = false, means the time server is not disabled.
#   1 = true, means the time server is disabled.
```

```
# Additional Network Settings
# =============================

#sip rtp port: 3000     # Eg. RTP packets are sent to port 3000.


#-------------------------------------------------------------------


# Configuration Server Settings
## = = = = = = = = = = = = = = =

# Notes: This section defines which server the phone retrieves new
# firmware images and configuration files from.  Three protocols are
# supported TFTP, FTP and HTTP

download protocol: TFTP   # valid values are TFTP, FTP and HTTP

## TFTP server settings
tftp server: 192.168.0.130
#alternate tftp server:
#use alternate tftp server: 1         # If your DHCP server assigns
                                        # a TFTP server address which
 # you do not use, you can use
                                        # the alternate tftp server.

## FTP server settings
#ftp server: 192.168.0.131   # can be IP or FQDN
#ftp username: mitel
#ftp password: 6869imitel
```

```
## HTTP server settings (for http://bogus.mitel.com/firmware/)
#http server: bogus.mitel.com   # can be IP or FQDN
#http path: firmware


#--------------------------------------------------------------------


# Dial Plan Settings
# =====================
#
# Notes:
#
#  As you dial a number on the phone, the phone will initiate a call
#  when one of the following conditions are meet:
#
#   (1) The entered number is an exact match in the dial plan
#   (2) The "#" symbol has been pressed
#   (3) A timeout occurs
#
#  The dial plan is a regular expression that supports the following
#  syntax:
#
#    0,1,2,3,4,5,6,7,8,9,*,#  : matches the keypad symbols
#    x                        : matches any digit (0...9)
#    +                        : matches 0 or more repetitions of the
#                             : previous expression
#    []                       : matches any number inside the brackets
#                             : can be used with a "-" to represent a
#                             : range
#    ()                       : expression grouping
#    |                        : either or
#
#
#  If the dialled number doesn't match the dial plan then the call
#  is rejected.

sip digit timeout: 3        # set the inter-digit timeout in seconds

# Example dial plans
sip dial plan: "x+#|xx+*"   # this is the default dial string, note
                            # that is must be quoted since it contains
                            # a '#' character


#sip dial plan: [01]xxx|[2-8]xxxx|91xxxxxxxxxx
                            # accept any 4 digit number beginning
                            # with a 0 or 1, any 5 digit number
                            # beginning with a number between 2 and 8
                            # (inclusive) or a 12 digit number
                            # beginning with 91


#sip dial plan terminator: 1   # enable sending of the "#" symbol to
                               # to the proxy in the dial string

#------------------------------------------------------------------
```

```
# General SIP Settings
# = = = = = = = = = = = =

#sip session timer: 90      # enable support of RFC4028, the default
                            # value of 0 disables this functionality

#sip transport protocol: 0  # use UDP (1), TCP (2) or both (0) for sip
                            # messaging

#sip use basic codecs: 1    # limit codecs to G711 and G729
#sip out-of-band dtmf: 0    # turn off support for RFC2833 (on by
                            # default)



# Global SIP User Settings
# ==========================
#
# Notes:
#   These settings are used as the default configuration for the hard
#   key lines on the phone. That is:
#
#     L1 to L2 on the 6800 Series IP phones
#
#   These can be over-ridden on a per-line basis using the per-line
#   settings.
#
#   See the Admin Guide for a detailed explanation of how this works

sip screen name: Joe Smith     # the name display on the phone's screen
sip user name: 4256            # the phone number
sip display name: Joseph Smith # the caller name sent out when making
                               # a call.
sip vmail: *78                 # the number to reach voicemail on

sip auth name: jsmith          # account used to authenticate user
sip password: 12345            # password for authentication account

sip mode: 0                    # line type:
                               #   0 - generic,
                               #   1 - BroadSoft SCA line
                               #   2 - Reserved

sip proxy ip: proxy.mitel.com # IP address or FQDN of proxy
sip proxy port: 5060           # port used for SIP messages on the
                               # proxy. Set to 0 to enable SRV
                               # lookups

sip registrar ip: mitel.com   # IP address or FQDN of registrar
sip registrar port: 0          # as proxy port, but for the registrar
sip registration period: 3600 # registration period in seconds
```

```
# Per-line SIP Settings
# =====================

# configure line 3 as the support BroadSoft SCA line
#   - the proxy and registrar settings are taken from the global
#     settings above

sip line3 screen name: Support
sip line3 user name: 4000
sip line3 display name: Mitel Support
sip line3 auth name: support
sip line3 password: 54321
sip line3 mode: 1
sip line3 vmail: *78


# configure line 5 (a soft key line) as an ordinary line
# of a test server

sip line5 screen name: Test 1
sip line5 user name: 5551001
sip line5 display name: Test 1
sip line5 auth name: 5551001
sip line5 password: 5551001
sip line5 mode: 0
sip line5 proxy ip: 10.50.10.102
sip line5 proxy port: 5060
sip line5 registrar ip: 10.50.10.102
sip line5 registrar port: 5060
sip line5 registration period: 60


#-------------------------------------------------------------------

# Softkey Settings
#

# Softkeys can be set either server wide or unique to each phone.
# Setting softkeys as line/call appearances should be done in the
# "<mac>.cfg" file, since these are unique to each phone.

# Notes:
#
#  There are a maximum of 44 top softkeys that can be configured on the
#  6869i IP phone. These can be set up through either of the 2
#  configuration files, depending on whether this is to be server wide
#  ("startup.cfg"), or model specific ("<model>.cfg), or phone specific ("<mac>.cfg"). Each softkey
#  needs to be numbered from 1 - 44, for example "topsoftkey12 type:
#  speeddial". Top softkeys can be set up as speeddials or as additional
#  call/line appearances and have a type, label and value associated
#  with it as seen here in the default top softkey settings.
```

```
#  TOPSOFTKEY TYPES: "line", "speeddial", "blf", "list", "dnd"
#  TOPSOFTKEY LABEL: Alpha numeric name for the softkey. The maximum
#                    number of characters for this value is 10 for
#                    speeddials and dnd, 9 chars for lines, blf
#  TOPSOFTKEY VALUE: If softkey type is a speeddial, any DTMFs (from
#                    0 - 9, *, "#") or a comma (,) for 500ms pause and
#                    'E' for On-hook can be set for the value.
#                    If softkey type is blf it is the extension you want
#                    to monitor.
#  TOPSOFTKEY LINE:  This is line associated with the softkey. For line
#                    softkeys the value must be between 3 and 24 (1 - 2
#                    are already hardcoded as the L1 and L2 hard
#                    key line/call appearances)

# Speed Dials
topsoftkey1 type: speeddial
topsoftkey1 label: "Ext Pickup"
topsoftkey1 value: *8
topsoftkey2 type: speeddial
topsoftkey2 label: "Call Return"
topsoftkey2 value: *69

# DND Key
topsoftkey4 type: dnd
topsoftkey4 label: DND

# Line appearance
topsoftkey6 type: line
topsoftkey6 label: Test 1
topsoftkey6 line: 5

# blf
topsoftkey8 type: blf
topsoftkey8 label: Jane Doe
topsoftkey8 value: 4559
topsoftkey8 line: 1

# list
topsoftkey11 type: list
topsoftkey12 type: list
```

6865I SAMPLE CONFIGURATION FILE

```
# Sample Configuration File
#= = = = = = = = = = = = = = = = = = = = = =

# Phone Model: 6865i

# Notes:
#
# The general format used here is similar to configuration files
# used by several UNIX-based programs. Any text following a number
# sign (#) is considered to be a comment, unless the number sign is
# contained within double-quotes ("#") where it is considered to be
# a pound. For Boolean fields, 0 = false, 1 = true.

# Comments:
#
# This file contains sample configurations for the "startup.cfg", "<model>.cfg, or
# "<mac>.cfg" file. The settings included here are examples only.
# You should change/comment the values to suit your requirements.
#
# Not all possible parameters are shown, refer to the admin guide
# for the full list of supported parameters, their defaults and
# valid ranges.
#
# The Mitel 6800 Series IP phones will download 2
# configuration files from the TFTP server while restarting, the
# "startup.cfg" file, the "<model>.cfg" file and the "<mac>.cfg" file. These three
# configuration files can be used to configure all of the settings
# of the phone with the exception of assigning a static IP address
# to a phone and line settings, which should only be set in the "<mac>.cfg" file.
#
# The "startup.cfg" file configures the settings server wide, the "<model.cfg" file contains model
# specific information (for example, "6865i.cfg"), while the "<mac>.cfg" file configures only the
# phone with the MAC address for which the file is named (for example, "00085d0304f4.cfg"). The
# settings in the "startup.cfg" file will be overridden by settings that also appear in the
# "<model>.cfg" file. Settings in the "<mac>.cfg" file override setting that appear in the
# "startup.cfg" and "<model>.cfg files.
#-----------------------------------------------------------------
```

```
# DHCP Setting
# =============

#dhcp: 1 # DHCP enabled.

# DHCP:
#0 = false, means DHCP is disabled.
#1 = true, means DHCP is enabled.
#
# Notes:
#
#  DHCP is normally set from the Options list on the phone or
#  the web interface
#
#  If DHCP is disabled, the following network settings will
#  have to be configured manually either through the configuration
#  files, the Options List in the phone, or the Web Client: IP
#  Address (of the phone), Subnet Mask, Gateway, DNS, and TFTP
#  Server.
#-----------------------------------------------------------------


# Network Settings
# = = = = = = = = =

# Notes: If DHCP is enabled, you do not need to set these network
# settings. Although depending on you DHCP server configuration
# you may still have to set the dns address.



#ip:     # This value is unique to each phone on a server
         # and should be set in the "<mac>.cfg" file if
         # setting this manually.

#subnet mask:
#default gateway:
#dns1:
#dns2:


# Time Server Settings
# ====================

#time server disabled: 1  # Time server disabled.
#time server1:            # Enable time server and enter at
#time server2:            # least one time server IP address or
#time server3:# qualified domain name.

# Time Server Disabled:
#   0 = false, means the time server is not disabled.
#   1 = true, means the time server is disabled.
```

```
# Additional Network Settings
# ============================

#sip rtp port: 3000     # Eg. RTP packets are sent to port 3000.

#-----------------------------------------------------------------

# Configuration Server Settings
# = = = = = = = = = = = = = = =

# Notes: This section defines which server the phone retrieves new
# firmware images and configuration files from. Three protocols
# are supported TFTP, FTP and HTTP

download protocol: TFTP   # valid values are TFTP, FTP and HTTP

## TFTP server settings
tftp server: 192.168.0.130
#alternate tftp server:
#use alternate tftp server: 1 # If your DHCP server assigns
# a TFTP server address which
# you do not use, you can use
# the alternate tftp server.

## FTP server settings
#ftp server: 192.168.0.131   # can be IP or FQDN
#ftp username: mitel
#ftp password: 6865imitel


## HTTP server settings (for http://bogus.mitel.com/firmware/)
#http server: bogus.mitel.com   # can be IP or FQDN
#http path: firmware


#----------------------------------------------------------------


# Dial Plan Settings
# ====================
#
# Notes:
#
#  As you dial a number on the phone, the phone will initiate a call
#  when one of the following conditions are meet:
#
#   (1) The entered number is an exact match in the dial plan
#   (2) The "#" symbol has been pressed
#   (3) A timeout occurs
#
#  The dial plan is a regular expression that supports the following:
#  syntax:
#
#    0,1,2,3,4,5,6,7,8,9,*,#  : matches the keypad symbols
#    x                        : matches any digit (0...9)
#    +                        : matches 0 or more repetitions of the
#                             :  previous expression
#    []                       : matches any number inside the brackets
```

```
#                              :  can be used with a "-" to represent a
#                              :  range
#    ()                        : expression grouping
#    |                         : either or
#
#
#  If the dialled number doesn't match the dial plan then the call
#  is rejected.

sip digit timeout: 3        # set the inter-digit timeout in seconds

# Example dial plans
sip dial plan: "x+#|xx+*"   # this is the default dial string, note
                            # that is must be quoted since it contains
                            # a '#' character


#sip dial plan: [01]xxx|[2-8]xxxx|91xxxxxxxxxx
                            # accept any 4 digit number beginning
                            # with a 0 or 1, any 5 digit number
                            # beginning with a number between 2 and 8
                            # (inclusive) or a 12 digit number
                            # beginning with 91


#sip dial plan terminator: 1   # enable sending of the "#" symbol to
                               # to the proxy in the dial string

#-----------------------------------------------------------------
```

```
# General SIP Settings
# ======================

#sip session timer: 90      # enable support of RFC4028, the default
                            # value of 0 disables this functionality

#sip transport protocol: 0  # use UDP (1), TCP (2) or both (0) for
                            # sip messaging

#sip use basic codecs: 1    # limit codecs to G711 and G729
#sip out-of-band dtmf: 0    # turn off support for RFC2833 (on by
                            # default)



# Global SIP User Settings
# ==========================
#
# Notes:
#   These settings are used as the default configuration for the
#   hard key lines on the phone. That is:
#
#     L1 to L2 on the 6800 Series IP phones
#
#   These can be over-ridden on a per-line basis using the per-line
#   settings.
#
#   See the Admin Guide for a detailed explanation of how this works

sip screen name: Joe Smith # the name display on the phone's screen
sip user name: 4256 # the phone number
sip display name: Joseph Smith # the caller name sent out when making
# a call.
sip vmail: *78 # the number to reach voicemail on

sip auth name: jsmith # account used to authenticate user
sip password: 12345            # password for authentication account

sip mode: 0                    # line type:
                               #   0 - generic,
                               #   1 - BroadSoft SCA line
                               #   2 - Reserved

sip proxy ip: proxy.mitel.com # IP address or FQDN of proxy
sip proxy port: 5060           # port used for SIP messages on the
                               # proxy.  Set to 0 to enable SRV
                               # lookups

sip registrar ip: mitel.com   # IP address or FQDN of registrar
sip registrar port: 0          # as proxy port, but for the registrar
sip registration period: 3600  # registration period in seconds
```

```
# Per-line SIP Settings
# ======================

# configure line 3 as the support BroadSoft SCA line
#   - the proxy and registrar settings are taken from the global
#     settings above

sip line3 screen name: Support
sip line3 user name: 4000
sip line3 display name: Mitel Support
sip line3 auth name: support
sip line3 password: 54321
sip line3 mode: 1
sip line3 vmail: *78


# configure line 5 (a soft key line) as an ordinary line
# of a test server

sip line5 screen name: Test 1
sip line5 user name: 5551001
sip line5 display name: Test 1
sip line5 auth name: 5551001
sip line5 password: 5551001
sip line5 mode: 0
sip line5 proxy ip: 10.50.10.102
sip line5 proxy port: 5060
sip line5 registrar ip: 10.50.10.102
sip line5 registrar port: 5060
sip line5 registration period: 60


#------------------------------------------------------------------

# Programmable Key Settings
# ==========================

# Programmable keys can be set either server wide or unique to each phone.
# Setting programmable keys as line/call appearances should be done
# in the "<mac>.cfg" file, since these are unique to each phone.

# Notes:
#
#  There are a maximum of 8 programmable keys that can be configured
#  on the 6865i IP phone. These can be
#  set up through either of the 2 configuration files, depending on
#  whether this is to be server wide ("startup.cfg"), or model specific ("<model>.cfg"), or phone
#  specific ("<mac>.cfg").  Each prgkey needs to be numbered from
# 1 - 8, for example "prgkey2 type:
# speeddial". Programmable keys can be set up as speeddials or as
# additional call/line appearances or as feature keys and have a
# type, value and line associated with it as seen here in the
# default programmable settings.
```

```
#  PRGKEY TYPES:  "line", "speeddial", "blf", "list", "dnd"
#  PRGKEY VALUE:  If prgkey type is a speeddial, any DTMFs (from
#                 0 - 9, *, "#") or a comma (,) for 500ms pause and
#                 'E' for On-hook can be set for the value.
#                 If prgkey type is blf it is the extension you want
#                 to monitor.
#  PRGKEY LINE:   This is line associated with the prgkey.  For line
#                 prgkeys the value must be between 3 and 24 (1 - 2
#                 are already hardcoded as the L1 and L2 hard
#                 key line/call appearances).

# Speed Dials
prgkey1 type: speeddial
prgkey1 value: *8
prgkey2 type: speeddial
prgkey2 value: *69

# DND Key
prgkey3 type: dnd

# Line appearance
prgkey4 type: line
prgkey4 line: 5

# blf
prgkey5 type: blf
prgkey5 value: 4559
prgkey5 line: 1

# list
prgkey6 type: list
prgkey7 type: list
```

6920 SAMPLE CONFIGURATION FILE

```
# Sample Configuration File
# ===========================

# Phone Model: 6920

# Notes:
#
# The general format used here is similar to configuration files
# used by several UNIX-based programs. Any text following a number
# sign (#) is considered to be a comment, unless the number sign is
# contained within double-quotes ("#") where it is considered to be
# a pound. For Boolean fields, 0 = false, 1 = true.

# Comments:
#
# This file contains sample configurations for the "startup.cfg", <model>.cfg, or
# "<mac>.cfg" file. The settings included here are examples only.
# You should change/comment the values to suit your requirements.
#
# Not all possible parameters are shown, refer to the admin guide for
# the full list of supported parameters, their defaults and valid
# ranges.
#
# The Mitel 6900 Series IP phones will download 2
# configuration files from the TFTP server while restarting, the
# "startup.cfg" file, the "<model>.cfg" file, and the "<mac>.cfg" file. These three configuration
# files can be used to configure all of the settings of the phone with
# the exception of assigning a static IP address to a phone and line
# settings, which should only be set in the "<mac>.cfg" file.
#
# The "startup.cfg" file configures the settings server wide, the "<model>.cfg" file contains model
# specific information (for example, "6869i.cfg"), while the "<mac>.cfg" file configures only the
# phone with the MAC address for which the file is named (for example, "00085d0304f4.cfg"). The
# settings in the "startup.cfg" file will be overridden by settings in the <model>.cfg file, and
# settings in the "<mac>.cfg" file override both settings in the "<model>.cfg" and the
# "startup.cfg" files.
#------------------------------------------------------------------
```

```
# DHCP Setting
# ==============

#dhcp: 1 # DHCP enabled.

# DHCP:
# 0 = false, means DHCP is disabled.
# 1 = true, means DHCP is enabled.
#
# Notes:
#
#  DHCP is normally set from the Options list on the phone or
#  the web interface
#
#  If DHCP is disabled, the following network settings will
#  have to be configured manually either through the configuration
#  files, the Options List in the phone, or the Web Client: IP
#  Address (of the phone), Subnet Mask, Gateway, DNS, and TFTP
#  Server.
#--------------------------------------------------------------------


# Network Settings
## = = = = = = = =

# Notes: If DHCP is enabled, you do not need to set these network
# settings. Although depending on you DHCP server configuration you
# may still have to set the dns address.

#ip:     # This value is unique to each phone on a server
         # and should be set in the "<mac>.cfg" file if
         # setting this manually.

#subnet mask:
#default gateway:
#dns1:
#dns2:


# Time Server Settings
## =====================

#time server disabled: 1  # Time server disabled.
#time server1:            # Enable time server and enter at
#time server2:            # least one time server IP address or
#time server3: # qualified domain name

# Time Server Disabled:
#   0 = false, means the time server is not disabled.
#   1 = true, means the time server is disabled.
```

```
# Additional Network Settings
# =============================

#sip rtp port: 3000     # Eg. RTP packets are sent to port 3000.


#-------------------------------------------------------------------


# Configuration Server Settings
## = = = = = = = = = = = = = = =

# Notes: This section defines which server the phone retrieves new
# firmware images and configuration files from.  Three protocols are
# supported TFTP, FTP and HTTP

download protocol: TFTP   # valid values are TFTP, FTP and HTTP

## TFTP server settings
tftp server: 192.168.0.130
#alternate tftp server:
#use alternate tftp server: 1         # If your DHCP server assigns
                                        # a TFTP server address which
 # you do not use, you can use
                                        # the alternate tftp server.

## FTP server settings
#ftp server: 192.168.0.131   # can be IP or FQDN
#ftp username: mitel
#ftp password: 6869imitel
```

```
## HTTP server settings (for http://bogus.mitel.com/firmware/)
#http server: bogus.mitel.com   # can be IP or FQDN
#http path: firmware


#--------------------------------------------------------------------


# Dial Plan Settings
# =====================
#
# Notes:
#
#  As you dial a number on the phone, the phone will initiate a call
#  when one of the following conditions are meet:
#
#   (1) The entered number is an exact match in the dial plan
#   (2) The "#" symbol has been pressed
#   (3) A timeout occurs
#
#  The dial plan is a regular expression that supports the following
#  syntax:
#
#    0,1,2,3,4,5,6,7,8,9,*,#  : matches the keypad symbols
#    x                        : matches any digit (0...9)
#    +                        : matches 0 or more repetitions of the
#                             : previous expression
#    []                       : matches any number inside the brackets
#                             : can be used with a "-" to represent a
#                             : range
#    ()                       : expression grouping
#    |                        : either or
#
#
#  If the dialled number doesn't match the dial plan then the call
#  is rejected.

sip digit timeout: 3        # set the inter-digit timeout in seconds

# Example dial plans
sip dial plan: "x+#|xx+*"   # this is the default dial string, note
                            # that is must be quoted since it contains
                            # a '#' character


#sip dial plan: [01]xxx|[2-8]xxxx|91xxxxxxxxxx
                            # accept any 4 digit number beginning
                            # with a 0 or 1, any 5 digit number
                            # beginning with a number between 2 and 8
                            # (inclusive) or a 12 digit number
                            # beginning with 91


#sip dial plan terminator: 1   # enable sending of the "#" symbol to
                               # to the proxy in the dial string

#-------------------------------------------------------------------
```

```
# General SIP Settings
# = = = = = = = = = = = =

#sip session timer: 90      # enable support of RFC4028, the default
                            # value of 0 disables this functionality

#sip transport protocol: 0  # use UDP (1), TCP (2) or both (0) for sip
                            # messaging

#sip use basic codecs: 1    # limit codecs to G711 and G729
#sip out-of-band dtmf: 0    # turn off support for RFC2833 (on by
                            # default)



# Global SIP User Settings
# ==========================
#
# Notes:
#   These settings are used as the default configuration for the hard
#   key lines on the phone. That is:
#
#     L1 to L2 on the 6900 Series IP phones
#
#   These can be over-ridden on a per-line basis using the per-line
#   settings.
#
#   See the Admin Guide for a detailed explanation of how this works

sip screen name: Joe Smith     # the name display on the phone's screen
sip user name: 4256            # the phone number
sip display name: Joseph Smith # the caller name sent out when making
                               # a call.
sip vmail: *78                 # the number to reach voicemail on

sip auth name: jsmith          # account used to authenticate user
sip password: 12345            # password for authentication account

sip mode: 0                    # line type:
                               #   0 - generic,
                               #   1 - BroadSoft SCA line
                               #   2 - Reserved

sip proxy ip: proxy.mitel.com # IP address or FQDN of proxy
sip proxy port: 5060           # port used for SIP messages on the
                               # proxy. Set to 0 to enable SRV
                               # lookups

sip registrar ip: mitel.com   # IP address or FQDN of registrar
sip registrar port: 0          # as proxy port, but for the registrar
sip registration period: 3600 # registration period in seconds
```

```
# Per-line SIP Settings
# ======================

# configure line 3 as the support BroadSoft SCA line
#   - the proxy and registrar settings are taken from the global
#     settings above

sip line3 screen name: Support
sip line3 user name: 4000
sip line3 display name: Mitel Support
sip line3 auth name: support
sip line3 password: 54321
sip line3 mode: 1
sip line3 vmail: *78


# configure line 5 (a soft key line) as an ordinary line
# of a test server

sip line5 screen name: Test 1
sip line5 user name: 5551001
sip line5 display name: Test 1
sip line5 auth name: 5551001
sip line5 password: 5551001
sip line5 mode: 0
sip line5 proxy ip: 10.50.10.102
sip line5 proxy port: 5060
sip line5 registrar ip: 10.50.10.102
sip line5 registrar port: 5060
sip line5 registration period: 60


#--------------------------------------------------------------------

# Softkey Settings
#

# Softkeys can be set either server wide or unique to each phone.
# Setting softkeys as line/call appearances should be done in the
# "<mac>.cfg" file, since these are unique to each phone.

# Notes:
#
#  There are a maximum of 44 top softkeys that can be configured on the
#  6920 IP phone. These can be set up through either of the 2
#  configuration files, depending on whether this is to be server wide
#  ("startup.cfg"), or model specific ("<model>.cfg), or phone specific ("<mac>.cfg"). Each softkey
#  needs to be numbered from 1 - 44, for example "topsoftkey12 type:
#  speeddial". Top softkeys can be set up as speeddials or as additional
#  call/line appearances and have a type, label and value associated
#  with it as seen here in the default top softkey settings.
```

```
#  TOPSOFTKEY TYPES: "line", "speeddial", "blf", "list", "dnd"
#  TOPSOFTKEY LABEL: Alpha numeric name for the softkey. The maximum
#                    number of characters for this value is 10 for
#                    speeddials and dnd, 9 chars for lines, blf
#  TOPSOFTKEY VALUE: If softkey type is a speeddial, any DTMFs (from
#                    0 - 9, *, "#") or a comma (,) for 500ms pause and
#                    'E' for On-hook can be set for the value.
#                    If softkey type is blf it is the extension you want
#                    to monitor.
#  TOPSOFTKEY LINE:  This is line associated with the softkey. For line
#                    softkeys the value must be between 3 and 24 (1 - 2
#                    are already hardcoded as the L1 and L2 hard
#                    key line/call appearances)

# Speed Dials
topsoftkey1 type: speeddial
topsoftkey1 label: "Ext Pickup"
topsoftkey1 value: *8
topsoftkey2 type: speeddial
topsoftkey2 label: "Call Return"
topsoftkey2 value: *69

# DND Key
topsoftkey4 type: dnd
topsoftkey4 label: DND

# Line appearance
topsoftkey6 type: line
topsoftkey6 label: Test 1
topsoftkey6 line: 5

# blf
topsoftkey8 type: blf
topsoftkey8 label: Jane Doe
topsoftkey8 value: 4559
topsoftkey8 line: 1

# list
topsoftkey11 type: list
topsoftkey12 type: list
```

Appendix D

SAMPLE BLF SOFTKEY SETTINGS

ABOUT THIS APPENDIX

This appendix provides sample BLF softkey settings for both the Asterisk server and the BroadSoft BroadWorks server.

TOPICS

This appendix covers the following topics:

SAMPLE BLF SOFTKEY SETTINGS

ASTERISK/SIPXECS BLF

The following are sample topsoftkey and programmable key configurations to enable Asterisk/sipXecs BLF support on Mitel IP phones.

SOFTKEY CONFIGURATION PARAMETERS FOR ASTERISK/SIPXECS BLF

```
topsoftkey1 type: blf
topsoftkey1 value: 9995551212
topsoftkey1 label: John
topsoftkey1 line: 1
```

PROGRAMMABLE KEY CONFIGURATION PARAMETERS FOR ASTERISK/SIPXECS BLF

```
prgkey1 type: blf
prgkey1 value: 9995551212
prgkey1 label: John
prgkey1 line: 1

prgkey7 type: blf
prgkey7 value: 9995551313
prgkey7 label: Jane
prgkey7 line: 1
```

BROADSOFT BROADWORKS BLF

The following are sample top softkey and programmable key configurations to enable BroadSoft BroadWorks Busy Lamp Field support on Mitel IP phones.

By default, BLF/List keys are automatically populated using the data from the BLF/List NOTIFY, but Administrators can manually configure the programmable key/softkey positioning of BLF/List targets on their phones. In addition to allowing users the ability to control the key placement of the BLF/List targets, this feature also ensures the order of targets does not shift due to lost or partially received BLF/List NOTIFY data packets.

Note: For BLF/List functionality, the "**list uri**" parameter or "**BLF List URI**" field located on the key configuration menu of the Web UI must be defined with the same BLF List URI defined on the BroadSoft BroadWorks Busy Lamp Field page for the respective account.

To bind a BLF/List target to a key, the key must be configured as a BLF/List key and the value must be defined with the target's resource URI using the following syntax:

```
sip:username@domain.com;ext=extension number
```

whereby the "username@domain.com" is identical to the resource URI of the BLF/List key configured on the call manager and the "extension number" (an optional value) corresponds to the target's extension number.

For example, if the resource URI of a BLF/List key is configured on the call manager as "jsmith@mitel.com", the value of the respective BLF/List key on the phone should be defined as:

```
sip:9@192.168.104.13
```

If an extension number is defined (e.g. `sip:jsmith@mitel.com;ext=5000`) it will be used, when the key is pressed, to dial out to the BLF/List target in scenarios where the corresponding key has not been updated with the BLF/List data. If the BLF/List key has been updated, the target URI is used to dial out when the key is pressed.

Note: If a resource URI is not defined for a key configured with BLF/List functionality, the key will be automatically populated using the first resource entry from the BLF/List NOTIFY data that has not already been populated (either manually or automatically).

In addition to configuring the BLF/List key value, the 6867i and 6869i SIP phones allow Administrators to define the BLF/List key's label. The defined label is displayed on the phone's screen up until the BLF/List key has been updated by the call manager. If a label is not defined, the label will be displayed as a series of question marks (i.e. ???) until it is updated with the appropriate data from the call manager.

SOFTKEY CONFIGURATION PARAMETERS FOR BROADSOFT BROADWORKS BLF

Note: One softkey must be defined of type “list” for EACH monitored user. So if there are two users being monitored, two top softkeys must be defined of type list.

```
topsoftkey1 type: list
topsoftkey1 label: John Smith
topsoftkey1 value: sip:5000@192.168.104.13;5000
topsoftkey1 line: 1

topsoftkey2 type: list
topsoftkey2 label: Martha Gold
topsoftkey2 value: sip:5001@192.168.104.13;5001
topsoftkey2 line: 1

list uri: sip:9@192.168.104.13
```

PROGRAMMABLE KEY CONFIGURATION PARAMETERS FOR BROADSOFT BROADWORKS BLF

Note: One prgkey must be defined of type “list” for each monitored user. So if there are two users being monitored, two prgkeys must be defined of type list.

```
prgkey5 type: list
prgkey5 value: sip:5000@192.168.104.13;5000
prgkey5 line: 1

prgkey6 type: list
prgkey6 value: sip:5001@192.168.104.13;5001
prgkey6 line: 1

list uri: sip:9@192.168.104.13
```

MIVOICE OFFICE 400 BLF LIST

The following are sample top softkey and programmable key configurations to enable MiVoice Office 400 Busy Lamp Field support on Mitel IP phones.

SOFTKEY CONFIGURATION PARAMETERS FOR MIVOICE OFFICE 400

Note: One softkey must be defined of type “list” for EACH monitored user. So if there are two users being monitored, two top softkeys must be defined of type list.

```
topsoftkey1 type: list
topsoftkey1 label: John Smith
topsoftkey1 value: sip:5000@192.168.104.13;5000
topsoftkey1 line: 1

topsoftkey2 type: list
topsoftkey2 label: Martha Gold
topsoftkey2 value: sip:5001@192.168.104.13;5001
topsoftkey2 line: 1

list uri: sip:9@192.168.104.13
```

PROGRAMMABLE KEY CONFIGURATION PARAMETERS FOR MIVOICE OFFICE 400

Note: One prgkey must be defined of type “list” for each monitored user. So if there are two users being monitored, two prgkeys must be defined of type list.

```
prgkey5 type: list
prgkey5 value: sip:5000@192.168.104.13;5000
prgkey5 line: 1

prgkey6 type: list
prgkey6 value: sip:5001@192.168.104.13;5001
prgkey6 line: 1

list uri: sip:9@192.168.104.13
```

Appendix E

SAMPLE MULTIPLE PROXY SERVER CONFIGURATION

ABOUT THIS APPENDIX

This appendix provides a sample multiple proxy server configuration.

TOPICS

This appendix covers the following topics:

MULTIPLE PROXY SERVER CONFIGURATION

Multiple proxy servers can be configured in the *startup.cfg* file, *<model>.cfg* file, or the *<mac>.cfg* file. In the example below, the default proxy setting is used if no specific setting is specified in the line configuration. Line2 and line3 are used for the global proxy configurations, while line1 and line4 use their own specific settings.

Note: The phones include support for a feature referenced in RFC3327, a SIP extension header called "PATH" for phones to discover intermediate proxies. This feature is always enabled on the phone.

```
#sip settings
sip proxy ip: #.#.#.#
sip proxy port: 5060
sip registrar ip: #.#.#.#
sip registrar port: 5060
sip registration period:3600

sip dial plan: "x+#""

#line info

# Fill in all necessary information below carefully. Populate all
# lines even if there is only one account

#line 1

sip line1 auth name:
sip line1 password:
sip line1 mode: 0
sip line1 user name:
sip line1 display name:
sip line1 screen name:
sip line1 proxy ip: &.&.&.&
sip line1 proxy port: 5060
sip line1 registrar ip: #.#.#.#
sip line1 registrar port: 5060
sip registration period:600

#line 2

sip line2 auth name:
sip line2 password:
sip line2 mode: 0
sip line2 user name:
sip line2 display name:
sip line2 screen name:
```

```
#line 3

sip line3 auth name:
sip line3 password:
sip line3 mode: 0
sip line3 user name:
sip line3 display name:
sip line3 screen name:

#line 4

sip line4 auth name:
sip line4 password:
sip line4 mode: 0
sip line4 user name:
sip line4 display name:
sip line4 screen name:
sip line4 proxy ip: %.%.%.%
sip line4 proxy port: 5060
sip line4 registrar ip: %.%.%.%
sip line4 registrar port: 5060
sip registration period:500
```

Appendix F

CERTIFICATE SUPPORT

ABOUT THIS APPENDIX

This appendix provides details on the certificates supported by the 6800/6900 Series SIP phones for this software release.

TOPICS

This appendix covers the following topics:

CERTIFICATES SUPPORTED IN THIS SOFTWARE RELEASE

The table below details the various certificates supported by the 6800/6900 Series SIP phones in this release:

CERTIFICATE COMMON NAME	PUBLIC KEY SIZE (BIT)	SIGNATURE ALGORITHM	VALIDITY EXPIRATION
AC Camerfirma SA Certificates			
Chambers of Commerce Root	RSA 2048 bits	SHA1WithRSA	2037 Sep 30
Chambers of Commerce Root - 2008	RSA 4096 bits	SHA1WithRSA	2038 Jul 31
Global Chambersign Root	RSA 2048 bits	SHA1WithRSA	2037 Sep 30
Global Chambersign Root - 2008	RSA 4096 bits	SHA1WithRSA	2038 Jul 31
Actalis Certificates			
Actalis Authentication Root CA	RSA 4096 bits	SHA256WithRSA	2030 Sep 22
Amazon Trust Services Certificates			
Amazon Root CA 1	RSA 2048 bits	SHA256WithRSA	2038 Jan 17
Amazon Root CA 2	RSA 4096 bits	SHA384WithRSA	2040 May 26
Amazon Root CA 3	EC secp256r1	ecdsaWithSHA256	2040 May 26
Amazon Root CA 4	EC secp384r1	ecdsaWithSHA384	2040 May 26
Starfield Services Root Certificate Authority - G2	RSA 2048 bits	SHA256WithRSA	2037 Dec 31
Asseco Data Systems S.A. Certificates			
Certum CA	RSA 2048 bits	SHA1WithRSA	2027 Jun 11
Certum Trusted Network CA	RSA 2048 bits	SHA1WithRSA	2029 Dec 31
Certum Trusted Network CA 2	RSA 4096 bits	SHA512WithRSA	2046 Oct 06
Atos Certificates			
Atos TrustedRoot 2011	RSA 2048 bits	SHA256WithRSA	2030 Dec 31
Autoridad de Certificacion Firmaprofesional Certificates			
Autoridad de Certificacion Firmaprofesional CIF A62634068	RSA 4096 bits	SHA1WithRSA	2030 Dec 31
Buypass Certificates			
Buypass Class 2 Root CA	RSA 4096 bits	SHA256WithRSA	2040 Oct 26
Buypass Class 3 Root CA	RSA 4096 bits	SHA256WithRSA	2040 Oct 26
certSIGN Certificates			
certSIGN ROOT CA	RSA 2048 bits	SHA1WithRSA	2031 Jul 04
China Financial Certification Authority (CFCA) Certificates			
CFCA EV ROOT	RSA 4096 bits	SHA256WithRSA	2029 Dec 31
Chunghwa Telecom Certificates			

CERTIFICATE COMMON NAME	PUBLIC KEY SIZE (BIT)	SIGNATURE ALGORITHM	VALIDITY EXPIRATION
Chunghwa Telecom Co., Ltd. - ePKI Root Certification Authority	RSA 4096 bits	SHA1WithRSA	2034 Dec 20
Consorci AOC Certificates			
EC-ACC	RSA 2048 bits	SHA1WithRSA	2031 Jan 07
Cybertrust Japan Certificates			
SecureSign RootCA11	RSA 2048 bits	SHA1WithRSA	2029 Apr 08
D-TRUST Certificates			
D-TRUST Root CA 3 2013	RSA 2048 bits	SHA256WithRSA	2028 Sep 20
D-TRUST Root Class 3 CA 2 2009	RSA 2048 bits	SHA256WithRSA	2029 Nov 05
D-TRUST Root Class 3 CA 2 EV 2009	RSA 2048 bits	SHA256WithRSA	2029 Nov 05
Certigna Certificates			
Certigna	RSA 2048 bits	SHA1WithRSA	2027 Jun 29
Certigna Root CA	RSA 4096 bits	SHA256WithRSA	2033 Oct 01
DigiCert Certificates			
Baltimore CyberTrust Root	RSA 2048 bits	SHA1WithRSA	2025 May 12
Cybertrust Global Root	RSA 2048 bits	SHA1WithRSA	2021 Dec 15
DigiCert Assured ID Root CA	RSA 2048 bits	SHA1WithRSA	2031 Nov 10
DigiCert Assured ID Root G2	RSA 2048 bits	SHA256WithRSA	2038 Jan 15
DigiCert Assured ID Root G3	EC secp384r1	ecdsaWithSHA384	2038 Jan 15
DigiCert Global Root CA	RSA 2048 bits	SHA1WithRSA	2031 Nov 10
DigiCert Global Root G2	RSA 2048 bits	SHA256WithRSA	2038 Jan 15
DigiCert Global Root G3	EC secp384r1	ecdsaWithSHA384	2038 Jan 15
DigiCert High Assurance EV Root CA	RSA 2048 bits	SHA1WithRSA	2031 Nov 10
DigiCert Trusted Root G4	RSA 4096 bits	SHA384WithRSA	2038 Jan 15
GeoTrust Global CA	RSA 2048 bits	SHA1WithRSA	2022 May 21
GeoTrust Primary Certification Authority	RSA 2048 bits	SHA1WithRSA	2036 Jul 16
GeoTrust Primary Certification Authority - G2	EC secp384r1	ecdsaWithSHA384	2038 Jan 18
GeoTrust Primary Certification Authority - G3	RSA 2048 bits	SHA256WithRSA	2037 Dec 01
GeoTrust Universal CA	RSA 4096 bits	SHA1WithRSA	2029 Mar 04
GeoTrust Universal CA 2	RSA 4096 bits	SHA1WithRSA	2029 Mar 04
Symantec Class 1 Public Primary Certification Authority - G4	EC secp384r1	ecdsaWithSHA384	2038 Jan 18

CERTIFICATE COMMON NAME	PUBLIC KEY SIZE (BIT)	SIGNATURE ALGORITHM	VALIDITY EXPIRATION
Symantec Class 1 Public Primary Certification Authority - G6	RSA 2048 bits	SHA256WithRSA	2037 Dec 01
Symantec Class 2 Public Primary Certification Authority - G4	EC secp384r1	ecdsaWithSHA384	2038 Jan 18
Symantec Class 2 Public Primary Certification Authority - G6	RSA 2048 bits	SHA256WithRSA	2037 Dec 01
thawte Primary Root CA	RSA 2048 bits	SHA1WithRSA	2036 Jul 16
thawte Primary Root CA - G2	EC secp384r1	ecdsaWithSHA384	2038 Jan 18
thawte Primary Root CA - G3	RSA 2048 bits	SHA256WithRSA	2037 Dec 01
VeriSign Class 1 Public Primary Certification Authority - G3	RSA 2048 bits	SHA1WithRSA	2036 Jul 16
VeriSign Class 2 Public Primary Certification Authority - G3	RSA 2048 bits	SHA1WithRSA	2036 Jul 16
VeriSign Class 3 Public Primary Certification Authority - G3	RSA 2048 bits	SHA1WithRSA	2036 Jul 16
VeriSign Class 3 Public Primary Certification Authority - G4	EC secp384r1	ecdsaWithSHA384	2038 Jan 18
VeriSign Class 3 Public Primary Certification Authority - G5	RSA 2048 bits	SHA1WithRSA	2036 Jul 16
VeriSign Universal Root Certification Authority	RSA 2048 bits	SHA256WithRSA	2037 Dec 01
Disig, a.s. Certificates			
CA Disig Root R2	RSA 4096 bits	SHA256WithRSA	2042 Jul 19
E-Tugra Certificates			
E-Tugra Certification Authority	RSA 4096 bits	SHA256WithRSA	2023 Mar 03
eMudhra Technologies Limited Certificates			
emSign ECC Root CA - C3	EC secp384r1	ecdsaWithSHA384	2043 Feb 18
emSign ECC Root CA - G3	EC secp384r1	ecdsaWithSHA384	2043 Feb 18
emSign Root CA - C1	RSA 2048 bits	SHA256WithRSA	2043 Feb 18
emSign Root CA - G1	RSA 2048 bits	SHA256WithRSA	2043 Feb 18
Entrust Certificates			
AffirmTrust Commercial	RSA 2048 bits	SHA256WithRSA	2030 Dec 31
AffirmTrust Networking	RSA 2048 bits	SHA1WithRSA	2030 Dec 31
AffirmTrust Premium	RSA 4096 bits	SHA384WithRSA	2040 Dec 31
AffirmTrust Premium ECC	EC secp384r1	ecdsaWithSHA384	2040 Dec 31
Entrust Root Certification Authority	RSA 2048 bits	SHA1WithRSA	2026 Nov 27
Entrust Root Certification Authority - EC1	EC secp384r1	ecdsaWithSHA384	2037 Dec 18

CERTIFICATE COMMON NAME	PUBLIC KEY SIZE (BIT)	SIGNATURE ALGORITHM	VALIDITY EXPIRATION
Entrust Root Certification Authority - G2	RSA 2048 bits	SHA256WithRSA	2030 Dec 07
Entrust Root Certification Authority - G4	RSA 4096 bits	SHA256WithRSA	2037 Dec 27
Entrust.net Certification Authority (2048)	RSA 2048 bits	SHA1WithRSA	2029 Jul 24
Global Digital Cybersecurity Authority Certificates			
GDCA TrustAUTH R5 ROOT	RSA 4096 bits	SHA256WithRSA	2040 Dec 31
GlobalSign Certificates			
GlobalSign	EC secp384r1	ecdsaWithSHA384	2038 Jan 19
GlobalSign	RSA 2048 bits	SHA256WithRSA	2029 Mar 18
GlobalSign	RSA 4096 bits	SHA384WithRSA	2034 Dec 10
GlobalSign Root CA	RSA 2048 bits	SHA1WithRSA	2028 Jan 28
GoDaddy Certificates			
Go Daddy Class 2 CA	RSA 2048 bits	SHA1WithRSA	2034 Jun 29
Go Daddy Root Certificate Authority - G2	RSA 2048 bits	SHA256WithRSA	2037 Dec 31
Starfield Class 2 CA	RSA 2048 bits	SHA1WithRSA	2034 Jun 29
Starfield Root Certificate Authority - G2	RSA 2048 bits	SHA256WithRSA	2037 Dec 31
Google Trust Services LLC (GTS) Certificates			
GlobalSign	EC secp256r1	ecdsaWithSHA256	2038 Jan 19
GlobalSign	RSA 2048 bits	SHA1WithRSA	2021 Dec 15
GTS Root R1	RSA 4096 bits	SHA384WithRSA	2036 Jun 22
GTS Root R2	RSA 4096 bits	SHA384WithRSA	2036 Jun 22
GTS Root R3	EC secp384r1	ecdsaWithSHA384	2036 Jun 22
GTS Root R4	EC secp384r1	ecdsaWithSHA384	2036 Jun 22
Government of Hong Kong (SAR) Certificates			
Hongkong Post Root CA 1	RSA 2048 bits	SHA1WithRSA	2023 May 15
Hongkong Post Root CA 3	RSA 4096 bits	SHA256WithRSA	2042 Jun 03
Government of Spain, ACCV Certificates			
ACCVRAIZ1	RSA 4096 bits	SHA1WithRSA	2030 Dec 31
Government of Spain, FNMT Certificates			
FNMT-RCM - SHA256	RSA 4096 bits	SHA256WithRSA	2030 Jan 01
Government of Taiwan, Government Root Certification Authority (GRCA) Certificates			
Government Root Certification Authority - Taiwan	RSA 4096 bits	SHA1WithRSA	2032 Dec 05
Government of The Netherlands, PKIoverheid (Logius) Certificates			

CERTIFICATE COMMON NAME	PUBLIC KEY SIZE (BIT)	SIGNATURE ALGORITHM	VALIDITY EXPIRATION
Staat der Nederlanden EV Root CA	RSA 4096 bits	SHA256WithRSA	2022 Dec 08
Staat der Nederlanden Root CA - G2	RSA 4096 bits	SHA256WithRSA	2020 Mar 25
Staat der Nederlanden Root CA - G3	RSA 4096 bits	SHA256WithRSA	2028 Nov 13
Government of Turkey, Kamu Sertifikasyon Merkezi (Kamu SM) Certificates			
TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1	RSA 2048 bits	SHA256WithRSA	2043 Oct 25
HARICA Certificates			
Hellenic Academic and Research Institutions ECC RootCA 2015	EC secp384r1	ecdsaWithSHA256	2040 Jun 30
Hellenic Academic and Research Institutions RootCA 2011	RSA 2048 bits	SHA1WithRSA	2031 Dec 01
Hellenic Academic and Research Institutions RootCA 2015	RSA 4096 bits	SHA256WithRSA	2040 Jun 30
IdenTrust Services, LLC Certificates			
DST Root CA X3	RSA 2048 bits	SHA1WithRSA	2021 Sep 30
IdenTrust Commercial Root CA 1	RSA 4096 bits	SHA256WithRSA	2034 Jan 16
IdenTrust Public Sector Root CA 1	RSA 4096 bits	SHA256WithRSA	2034 Jan 16
Internet Security Research Group (ISRG) Certificates			
ISRG Root X1	RSA 4096 bits	SHA256WithRSA	2035 Jun 04
Izenpe S.A. Certificates			
Izenpe.com	RSA 4096 bits	SHA256WithRSA	2037 Dec 13
Krajowa Izba Rozliczeniowa S.A. (KIR) Certificates			
SZAFIR ROOT CA2	RSA 2048 bits	SHA256WithRSA	2035 Oct 19
LuxTrust Certificates			
LuxTrust Global Root 2	RSA 4096 bits	SHA256WithRSA	2035 Mar 05
Microsec Ltd. Certificates			
Microsec e-Szigno Root CA 2009	RSA 2048 bits	SHA256WithRSA	2029 Dec 30
Mitel Certificates			
Mitel Networks Root CA	RSA 1024 bits	SHA1WithRSA	2029 Jun 11
Mitel Products Root CA	RSA 4096 bits	SHA256WithRSA	2045 May 27
NetLock Ltd. Certificates			
NetLock Arany (Class Gold) FÅ‘tanÃºsÃtvÃ¡ny	RSA 2048 bits	SHA256WithRSA	2028 Dec 06
OISTE Certificates			
OISTE WISeKey Global Root GA CA	RSA 2048 bits	SHA1WithRSA	2037 Dec 11

CERTIFICATE COMMON NAME	PUBLIC KEY SIZE (BIT)	SIGNATURE ALGORITHM	VALIDITY EXPIRATION
OISTE WISeKey Global Root GB CA	RSA 2048 bits	SHA256WithRSA	2039 Dec 01
OISTE WISeKey Global Root GC CA	EC secp384r1	ecdsaWithSHA384	2042 May 09
QuoVadis Certificates			
QuoVadis Root CA 1 G3	RSA 4096 bits	SHA256WithRSA	2042 Jan 12
QuoVadis Root CA 2	RSA 4096 bits	SHA1WithRSA	2031 Nov 24
QuoVadis Root CA 2 G3	RSA 4096 bits	SHA256WithRSA	2042 Jan 12
QuoVadis Root CA 3	RSA 4096 bits	SHA1WithRSA	2031 Nov 24
QuoVadis Root CA 3 G3	RSA 4096 bits	SHA256WithRSA	2042 Jan 12
QuoVadis Root Certification Authority	RSA 2048 bits	SHA1WithRSA	2021 Mar 17
SECOM Trust Systems CO., LTD. Certificates			
SECOM Trust.net - Security Communication RootCA1	RSA 2048 bits	SHA1WithRSA	2023 Sep 30
Security Communication RootCA2	RSA 2048 bits	SHA256WithRSA	2029 May 29
Sectigo Certificates			
AAA Certificate Services	RSA 2048 bits	SHA1WithRSA	2028 Dec 31
AddTrust Class 1 CA Root	RSA 2048 bits	SHA1WithRSA	2020 May 30
AddTrust External CA Root	RSA 2048 bits	SHA1WithRSA	2020 May 30
COMODO Certification Authority	RSA 2048 bits	SHA1WithRSA	2029 Dec 31
COMODO ECC Certification Authority	EC secp384r1	ecdsaWithSHA384	2038 Jan 18
COMODO RSA Certification Authority	RSA 4096 bits	SHA384WithRSA	2038 Jan 18
USERTrust ECC Certification Authority	EC secp384r1	ecdsaWithSHA384	2038 Jan 18
USERTrust RSA Certification Authority	RSA 4096 bits	SHA384WithRSA	2038 Jan 18
SecureTrust Certificates			
Secure Global CA	RSA 2048 bits	SHA1WithRSA	2029 Dec 31
SecureTrust CA	RSA 2048 bits	SHA1WithRSA	2029 Dec 31
XRamp Global Certification Authority	RSA 2048 bits	SHA1WithRSA	2035 Jan 01
Shanghai Electronic Certification Authority Co., Ltd. (SHECA) Certificates			
UCA Extended Validation Root	RSA 4096 bits	SHA256WithRSA	2038 Dec 31
UCA Global G2 Root	RSA 4096 bits	SHA256WithRSA	2040 Dec 31
SK ID Solutions AS Certificates			

CERTIFICATE COMMON NAME	PUBLIC KEY SIZE (BIT)	SIGNATURE ALGORITHM	VALIDITY EXPIRATION
EE Certification Centre Root CA	RSA 2048 bits	SHA1WithRSA	2030 Dec 17
SSL.com Certificates			
SSL.com EV Root Certification Authority ECC	EC secp384r1	ecdsaWithSHA256	2041 Feb 12
SSL.com EV Root Certification Authority RSA R2	RSA 4096 bits	SHA256WithRSA	2042 May 30
SSL.com Root Certification Authority ECC	EC secp384r1	ecdsaWithSHA256	2041 Feb 12
SSL.com Root Certification Authority RSA	RSA 4096 bits	SHA256WithRSA	2041 Feb 12
SwissSign AG Certificates			
SwissSign Gold CA - G2	RSA 4096 bits	SHA1WithRSA	2036 Oct 25
SwissSign Platinum CA - G2	RSA 4096 bits	SHA1WithRSA	2036 Oct 25
SwissSign Silver CA - G2	RSA 4096 bits	SHA1WithRSA	2036 Oct 25
T-Systems International GmbH (Deutsche Telekom) Certificates			
T-TeleSec GlobalRoot Class 2	RSA 2048 bits	SHA256WithRSA	2033 Oct 01
T-TeleSec GlobalRoot Class 3	RSA 2048 bits	SHA256WithRSA	2033 Oct 01
Taiwan-CA Inc. (TWCA) Certificates			
TWCA Global Root CA	RSA 4096 bits	SHA256WithRSA	2030 Dec 31
TWCA Root Certification Authority	RSA 2048 bits	SHA1WithRSA	2030 Dec 31
Telia Company (formerly TeliaSonera) Certificates			
Sonera Class2 CA	RSA 2048 bits	SHA1WithRSA	2021 Apr 06
TeliaSonera Root CA v1	RSA 4096 bits	SHA1WithRSA	2032 Oct 18
TrustCor Systems Certificates			
TrustCor ECA-1	RSA 2048 bits	SHA256WithRSA	2029 Dec 31
TrustCor RootCert CA-1	RSA 2048 bits	SHA256WithRSA	2029 Dec 31
TrustCor RootCert CA-2	RSA 4096 bits	SHA256WithRSA	2034 Dec 31
Trustis Certificates			
Trustis Limited - Trustis FPS Root CA	RSA 2048 bits	SHA1WithRSA	2024 Jan 21
Web.com Certificates			
Network Solutions Certificate Authority	RSA 2048 bits	SHA1WithRSA	2029 Dec 31

Note: The trust store on the SIP phone is used only for HTTPs connections and not for SIP-over-TLS.

Appendix G

WARRANTY

ABOUT THIS APPENDIX

This appendix provides details on warranty of the 6800/6900 Series SIP phones.

TOPICS

This appendix covers the following topics:

LIMITED WARRANTY

(Not applicable in Australia – see below for Limited Warranty in Australia)

Mitel warrants this product against defects and malfunctions in accordance with Mitel's authorized, written functional specification relating to such products during a one (1) year period from the date of original purchase ("Warranty Period"). If there is a defect or malfunction, Mitel shall, at its option, and as the exclusive remedy, either repair or replace the product at no charge, if returned within the Warranty Period. If replacement parts are used in making repairs, these parts may be refurbished, or may contain refurbished materials. If it is necessary to replace the product, it may be replaced with a refurbished product of the same design and color. If it should become necessary to repair or replace a defective or malfunctioning product under this warranty, the provisions of this warranty shall apply to the repaired or replaced product until the expiration of ninety (90) days from the date of pick up, or the date of shipment to you, of the repaired or replacement product, or until the end of the original Warranty Period, whichever is later. Proof of the original purchase date is to be provided with all products returned for warranty repairs.

EXCLUSIONS

Mitel does not warrant its products to be compatible with the equipment of any particular telephone company. This warranty does not extend to damage to products resulting from improper installation or operation, alteration, accident, neglect, abuse, misuse, fire or natural causes such as storms or floods, after the product is in your possession. Mitel will not accept liability for any damages and/or long distance charges, which result from unauthorized and/or unlawful use.

Mitel shall not be liable for any incidental or consequential damages, including, but not limited to, loss, damage or expense directly or indirectly arising from the customer's use of or inability to use this product, either separately or in combination with other equipment. This paragraph, however, shall not apply to consequential damages for injury to the person in the case of products used or bought for use primarily for personal, family or household purposes.

This warranty sets forth the entire liability and obligations of Mitel with respect to breach of warranty, and the warranties set forth or limited herein are the sole warranties and are in lieu of all other warranties, expressed or implied, including warranties or fitness for particular purpose and merchantability.

WARRANTY REPAIR SERVICES

Should the product fail during the Warranty Period;

- **In North America,** please call 1-800-574-1611 for further information.
- **Outside North America**, contact your sales representative for return instructions.

You will be responsible for shipping charges, if any. When you return this product for warranty service, you must present proof of purchase.

AFTER WARRANTY SERVICE

Mitel offers ongoing repair and support for this product. This service provides repair or replacement of your Mitel product, at Mitel's option, for a fixed charge. You are responsible for all shipping charges. For further information and shipping instructions:

- **In North America**, contact our service information number: 1-800-574-1611.
- **Outside North America**, contact your sales representative.

Note: Repairs to this product may be made only by the manufacturer and its authorized agents, or by others who are legally authorized. This restriction applies during and after the Warranty Period. Unauthorized repair will void the warranty.

LIMITED WARRANTY (AUSTRALIA ONLY)

The benefits under the Mitel Limited Warranty below are in addition to other rights and remedies to which you may be entitled under a law in relation to the products.

In addition to all rights and remedies to which you may be entitled under the *Competition and Consumer Act 2010* (Commonwealth) and any other relevant legislation, Mitel warrants this product against defects and malfunctions in accordance with Mitel's authorized, written functional specification relating to such products during a one (1) year period from the date of original purchase (“Warranty Period”). If there is a defect or malfunction, Mitel shall, at its option, and as the exclusive remedy under this limited warranty, either repair or replace the product at no charge, if returned within the Warranty Period.

REPAIR NOTICE

To the extent that the product contains user-generated data, you should be aware that repair of the goods may result in loss of the data. Goods presented for repair may be replaced by refurbished goods of the same type rather than being repaired. Refurbished parts may be used to repair the goods. If it is necessary to replace the product under this limited warranty, it may be replaced with a refurbished product of the same design and color.

If it should become necessary to repair or replace a defective or malfunctioning product under this warranty, the provisions of this warranty shall apply to the repaired or replaced product until the expiration of ninety (90) days from the date of pick up, or the date of shipment to you, of the repaired or replacement product, or until the end of the original Warranty Period, whichever is later. Proof of the original purchase date is to be provided with all products returned for warranty repairs.

EXCLUSIONS

Mitel does not warrant its products to be compatible with the equipment of any particular telephone company. This warranty does not extend to damage to products resulting from improper installation or operation, alteration, accident, neglect, abuse, misuse, fire or natural causes such as storms or floods, after the product is in your possession. Mitel will not accept liability for any damages and/or long distance charges, which result from unauthorized and/or unlawful use.

To the extent permitted by law, Mitel shall not be liable for any incidental damages, including, but not limited to, loss, damage or expense directly or indirectly arising from your use of or inability to use this product, either separately or in combination with other equipment. This paragraph, however, is not intended to have the effect of excluding, restricting or modifying the application of all or any of the provisions of Part 5-4 of Schedule 2 to the Competition and Consumer Act 2010 (**the ACL**), the exercise of a right conferred by such a provision or any liability of Mitel in relation to a failure to comply with a guarantee that applies under Division 1 of Part 3-2 of the ACL to a supply of goods or services.

This express warranty sets forth the entire liability and obligations of Mitel with respect to breach of this express warranty and is in lieu of all other express or implied warranties other than those conferred by a law whose application cannot be excluded, restricted or modified. Our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and for compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure.

WARRANTY REPAIR SERVICES

Procedure: Should the product fail during the Warranty Period and you wish to make a claim under this express warranty, please contact the Mitel authorized reseller who sold you this product (details as per the invoice) and present proof of purchase. You will be responsible for shipping charges, if any.

Manufacturer: Mitel Networks Corporation
745 Springvale Road
Mulgrave VIC 3170
ABN 16 140 787 195
Phone: +61 3 8562 2700

Limitation of Liability for Products not of a kind ordinarily acquired for personal, domestic or household use or consumption (e.g. goods/services ordinarily supplied for business-use)

1.1 To the extent permitted by law and subject to clause 1.2 below, the liability of Mitel to you for any non-compliance with a statutory guarantee or loss or damage arising out of or in connection with the supply of goods or services (whether for tort (including negligence), statute, custom, law or on any other basis) is limited to:

- **a.** in the case of services:
  - **i.** the resupply of the services; or
  - **ii.** the payment of the cost of resupply; and
- **b.** in the case of goods:
  - **i.** the replacement of the goods or the supply of equivalent goods; or
  - **ii.** the repair of the goods; or
  - **iii.** the payment of the cost of replacing the goods or of acquiring equivalent goods; or
  - **iv.**the payment of the cost of having the goods repaired.

1.2 Clause 1.1 is not intended to have the effect of excluding, restricting or modifying:

- **a.** the application of all or any of the provisions of Part 5-4 of Schedule 2 to the Competition and Consumer Act 2010 (**the ACL**); or
- **b.** the exercise of a right conferred by such a provision; or
- **c.** any liability of Mitel in relation to a failure to comply with a guarantee that applies under Division 1 of Part 3-2 of the ACL to a supply of goods or services.

AFTER WARRANTY SERVICE

Mitel offers ongoing repair and support for this product. If you are not otherwise entitled to a remedy for a failure to comply with a guarantee that cannot be excluded under the Australian Consumer Law, this service provides repair or replacement of your Mitel product, at Mitel's option, for a fixed charge. You are responsible for all shipping charges. For further information and shipping instructions contact:

Mitel Networks Corporation
745 Springvale Road

Mulgrave VIC 3170
ABN 16 140 787 195
Phone: +61 3 8562 2700

Note: Repairs to this product may be made only by the manufacturer and its authorized agents, or by others who are legally authorized. Unauthorized repair will void this express warranty.

Appendix H

LICENSE AGREEMENT

ABOUT THIS APPENDIX

This appendix provides details on the license agreement of the 6800/6900 Series SIP phones.

TOPICS

This appendix covers the following topics:

THIRD-PARTY COPYRIGHT COMPLIANCE

This product contains software provided under license to Mitel by one or more third parties. In addition to the Mitel SLA, use and distribution of this product is subject to the following license terms:

EXPAT XML PARSER

M5T SIP STACK - M5T

MD5 RSA

These notices must be retained in any copies of any part of this documentation and/or software.

OPENSSL

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OPENSSL LICENSE

*/

Original SSLeay License

*

* This package is an SSL implementation written

* by Eric Young (eay@cryptsoft.com).

* The implementation was written so as to conform with Netscapes SSL.

*

* This library is free for commercial and non-commercial use as long as

* the following conditions are aheared to. The following conditions

* apply to all code found in this distribution, be it the RC4, RSA,

* lhash, DES, etc., code; not just the SSL code. The SSL documentation

* included with this distribution is covered by the same copyright terms

* except that the holder is Tim Hudson (tjh@cryptsoft.com).

*

* Copyright remains Eric Young's, and as such any Copyright notices in

* the code are not to be removed.

* If this package is used in a product, Eric Young should be given attribution

* as the author of the parts of the library used.

* This can be in the form of a textual message at program startup or

* in documentation (online or textual) provided with the package.

* Redistribution and use in source and binary forms, with or without

* modification, are permitted provided that the following conditions

* are met:

* 1. Redistributions of source code must retain the copyright

*   notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright

*   notice, this list of conditions and the following disclaimer in the

LIBSRTP (SRTP) - CISCO

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Cisco Systems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION).

HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

WIND RIVER SYSTEMS - VXWORKS SOFTWARE

The VxWorks Run-Time software module is Copyright (c) WindRiver Systems Inc, all rights reserved. It is licensed for use, not sold. All use of this product and the VxWorks Run-Time module is subject to agreement with the following EULA terms

With respect to the Run-Time Module, Wind River and its licensors are third party beneficiaries of the End User License Agreement and that the provisions related to the Run-Time Module are made expressly for the benefit of, and are enforceable by, Wind River and its licensors.

Activities expressly prohibited: (i) copying the Run-Time Module, except for archive purposes consistent with the End User's archive procedures; (ii) transferring the Run-Time Module to a third party apart from the Target Application; (iii) modifying, decompiling, disassembling, reverse engineering or otherwise attempting to derive the Source Code of the Run-Time Module; (iv) exporting the Run-Time Module or underlying technology in contravention of applicable U.S. and foreign export laws and regulations; and (v) using the Run-Time Module other than in connection with operation of the Target Application.

Mitel and Wind River Systems: (i) Retain ownership of all copies of the Run-Time Module; (ii) expressly disclaim all implied warranties, including without limitation the implied warranties of merchantability, fitness for a particular purpose, title and non-infringement; (iii) exclude liability for any special, indirect, punitive, incidental and consequential damages; and (iv) require that any further distribution of the Run-Time Module be subject to the same restrictions set forth herein.

UPNP - INTEL

INTEL SOFTWARE LICENSE AGREEMENT (Final, Site License)

IMPORTANT - READ BEFORE COPYING, INSTALLING OR USING.

Do not use or load this software and any associated materials (collectively, the "Software") until you have carefully read the following terms and conditions. By loading or using the Software, you agree to the terms of this Agreement. If you do not wish to so agree, do not install or use the Software.

LICENSE. You may copy the Software onto your organization's computers for your organization's use, and you may make a reasonable number of back-up copies of the Software, subject to these conditions:

5. You may not copy, modify, rent, sell, distribute or transfer any part of the Software except as provided in this Agreement, and you agree to prevent unauthorized copying of the Software.
6. You may not reverse engineer, decompile, or disassemble the Software.
7. You may not sublicense the Software.
8. The Software may include portions offered on terms in addition to those set out here, as set out in a license accompanying those portions.

OWNERSHIP OF SOFTWARE AND COPYRIGHTS. Title to all copies of the Software remains with Intel or its suppliers. The Software is copyrighted and protected by the laws of the United States and other countries, and international treaty provisions. You may not remove any copyright notices from the Software. Intel may make changes to the Software, or to items referenced therein, at any time without notice, but is not obligated to support or update the Software. Except as otherwise expressly provided, Intel grants no express or implied right under Intel patents, copyrights, trademarks, or other intellectual property rights. You may transfer the Software only if the recipient agrees to be fully bound by these terms and if you retain no copies of the Software.

LIMITED MEDIA WARRANTY. If the Software has been delivered by Intel on physical media, Intel warrants the media to be free from material physical defects for a period of ninety days after delivery by Intel. If such a defect is found, return the media to Intel for replacement or alternate delivery of the Software as Intel may select.

EXCLUSION OF OTHER WARRANTIES. EXCEPT AS PROVIDED ABOVE, THE SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND INCLUDING WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE.

Intel does not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained within the Software.

LIMITATION OF LIABILITY. IN NO EVENT SHALL INTEL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, OR LOST INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF INTEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS PROHIBIT EXCLUSION OR LIMITATION OF LIABILITY FOR IMPLIED WARRANTIES OR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION. TERMINATION OF THIS AGREEMENT.

Intel may terminate this Agreement at any time if you violate its terms. Upon termination, you will immediately destroy the Software or return all copies of the Software to Intel.

APPLICABLE LAWS. Claims arising under this Agreement shall be governed by the laws of California, excluding its principles of conflict of laws and the United Nations Convention on Contracts for the Sale of Goods. You may not export the Software in violation of applicable export laws and regulations. Intel is not obligated under any other agreements unless they are in writing and signed by an authorized representative of Intel.

GOVERNMENT RESTRICTED RIGHTS. The Software is provided with "RESTRICTED RIGHTS."

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in FAR52.227-14 and DFAR252.227-7013 et seq. or its successor. Use of the Software by the Government constitutes acknowledgment of Intel's proprietary rights therein. Contractor or Manufacturer is Intel Corporation, 2200 Mission College Blvd., Santa Clara, CA 95052.