ALE M3-M5-M7-M8 DeskPhones

Administrator Guide

Alcatel·Lucent Enterprise

Legal Notice

This document is created by ALE China Co. Ltd. (hereinafter referred to as "ALE China"). Anyone who accesses and uses this document shall agree to comply with the following clauses. If you do not agree to comply with these clauses, please do not use this document. ALE China reserves the right to update, correct and modify the following clauses at any time without notice, and these updates will also be binding on you.

Trademark Notice

The Alcatel-Lucent name and logo are trademarks of Nokia used under license by ALE China.

Copyright Notice

Disclaimer

While efforts were made to verify the completeness and accuracy of the information contained in this documentation, this document is provided “as is”. To get more accurate content concerning Cross Compatibilities, Product Limits, Software Policy and Feature Lists, please refer to the accurate documents published on the Business Partner Web Site.

In the interest of continued product development, ALE China reserves the right to make improvements to this documentation and the products it describes at any time, without notice or obligation.

The user shall be solely liable for any loss or damage (including direct, indirect, special or consequential loss or damage) arising from the use of the information contained herein for any reason whatsoever.

To the extent permitted by law, ALE China reserves the right of final interpretation.

This document is only authorized to be used under the purpose of performing the contract obligations under the relevant contract signed with ALE China and shall not be used for other purposes.

Contents

1. Introduction 7
2. Phone Network 8
2.1 IPv4 and IPv6 Network Settings 8
2.2 DHCP Options for IPv4 12
2.3 DHCP Options for IPv6 15
2.4 VLAN 15
2.5 Wi-Fi 17
2.6 Network Address Translation (NAT) 20
2.7 Internet Port and PC Port 20
2.8 OpenVPN 22
2.9 Quality of Service (QoS) 23
2.10 802.1x Authentication 24
2.11 TR-069 Device Management 25
3. Phone Provisioning 29
3.1 Web User Interface 29
3.2 Phone User Interface 31
3.3 Configuration Files 31
3.4 EDS (Easy Deployment Server) 32
3.5 Provisioning Methods 32
3.6 Auto Provisioning Process 32
3.7 Keeping User's Personalized Settings after Auto Provisioning 36
3.8 Supported Provisioning Server Discovery Methods 37
4. Firmware Upgrade 43
4.1 Firmware 43
4.2 Firmware Upgrade Configuration 43
4.3 Firmware Upgrade via USB disk 44
5. Security Features 45
5.1 User and Administrator Identification 45
5.2 Auto Logout 53
5.3 Phone Lock 53
5.4 Transport Layer Security (TLS) 54
5.5 Secure Real-Time Transport Protocol (SRTP) 57
5.6 SSH Activation 59
5.7 HTTPS Peer Verification 59
5.8 Encrypting and Decrypting Files 59
6. Directory 60
6.1 Local Directory 60
6.2 Lightweight Directory Access Protocol (LDAP) 62
6.3 External Directory 65
6.4 Directory Search Settings 68

6.5 Remote Phone Book 68
6.6 Contact Backup 69
6.7 Blacklist 70
6.8 Directory List for Directory/Dir Soft Key 70
6.9 Favorite Contacts 71
6.10 History List Display in Web UI 72
7. Audio Features 73
7.1 Dial Tone 73
7.2 Stutter Tone 73
7.3 Ring Tones 73
7.4 Distinctive Ring Tones 76
7.5 Ringer Device 79
7.6 Tones 79
7.7 Audio Codecs 81
7.8 Packetization Time (PTime) 82
7.9 Early Media 83
7.10 Acoustic Clarity Technology 83
7.11 DTMF 84
7.12 Voice Quality Monitoring (VQM) 85
7.13 Suppress DTMF Display 86
8. Multiple SIP Accounts 87
8.1 Account Registration 87
8.2 Server Redundancy 90
8.3 SIP Server Name Resolution 91
9. Call Log 93
9.1 Call Log Display 93
9.2 Call Log Configuration 93
10. Call Features 94
10.1 Dial Plan 94
10.2 Hotline 99
10.3 Recall 100
10.4 Speed Dial 100
10.5 Call Timeout 101
10.6 Auto Dial Out Timer 101
10.7 Anonymous Call 102
10.8 Anonymous Call Rejection 103
10.9 Call Number Filter 103
10.10 IP Address Call 104
10.11 Auto Answer 105
10.12 Call Waiting 105
10.13 Do Not Disturb (DND) 106

10.14 Call Forward 110
10.15 DND & FWD Synchronization 118
10.16 Multiple Call Appearances 119
10.17 Call Hold 119
10.18 Call Mute 122
10.19 Call Transfer 122
10.20 Conference 124
10.21 Keep Mute 125
10.22 Auto Redial 125
10.23 USB Recording 126
10.24 Confidential Dial 126
10.25 Multicast Paging 127
10.26 Action URL 130
10.27 Action URI 142
11. Phone Customization 147
11.1 Multiple Languages 147
11.2 Screen Saver 148
11.3 Backlight of LCD 149
11.4 Backlight of LED (Only for M8) 150
11.5 ECO Mode (Only for M8) 151
11.6 Time and Date 154
11.7 Key As Send 162
11.8 Bluetooth 162
11.9 Handset/Headset/Speakerphone Mode 163
11.10 Programmable Keys 164
11.11 Wallpaper 174
11.12 Call Display 175
11.13 Notification Pop-ups 175
11.14 IME Optimization 176
11.15 Search Source List in Dialing 176
11.16 Soft Key Layout 176
12. Advanced Features 188
12.1 Audio Hub 188
12.2 X-party Conference 191
12.3 Hot Desking 194
12.4 Intercom 196
12.5 Push-To-Talk 200
12.6 Voicemail 200
12.7 BLF 202
12.8 Call Pickup 204
12.19 Call Park & Retrieve 208

12.10 Shared Line Appearance (SLA) 211
12.11 Call Completion 212
12.12 Automatic Call Distribution (ACD) 212
12.13 Broadsoft Hoteling 214
13. Troubleshooting 218
13.1 Log Collection 218
13.2 Resetting Device to Factory Settings 223
13.3 One Key Reboot 224
13.4 Network Diagnostics 225
13.5 Packets Capture via PC port 225
13.6 Screen Capture 226

1. Introduction

The ALE M3-M5-M7-M8 DeskPhones Administrator Guide provides general guidance on setting up phone network, provisioning and managing phones.

This guide is not intended for end users, but for administrators with experience in networking who understand the basics of open SIP networks and VoIP endpoint environments.

As an administrator, you can do the following with this guide:

- Set up a VoIP network and provisioning server
- Provision the phone with features and settings
- Upgrade and maintain phones

This guide is applicable to the following ALE Myriad Series devices running firmware version R130.

- The ALE Myriad Series phones including ALE M3/M5/M7/M8

The example is shown as below:

Phone UI	Menu → Advanced Setting (default password: 123456) → Network → IP Stack → IP Stack

2. Phone Network

The ALE Myriad Series phones operate on an Ethernet local area network (LAN) or wireless network.

2.1 IPv4 and IPv6 Network Settings

The ALE Myriad Series phones support IPv4 addressing mode and IPv6 addressing mode.

After connecting to the wired network, the phones can obtain the IPv4 or IPv6 network settings from a Dynamic Host Configuration Protocol (DHCP) server if your network supports it. To make it easier to manage IP settings, we recommend you use automated DHCP which can eliminate repetitive manual data entry.

You can also configure IPv4 or IPv6 network settings manually.

Note: The ALE Myriad Series phones comply with the DHCPv4 specifications documented in RFC 2131, and DHCPv6 specifications documented in RFC 3315.

In DHCP mode, if the phone cannot get IP address, the IP address in status menu will be displayed as “0.0.0.0” and prompt “network unavailable” message.

2.1.1 IP Addressing Mode Configuration

The following table lists the parameter you can use to configure the IP addressing mode.

Parameter	**DeviceNetworkIpStackMode**	**config.xml**
Description	It configures the IP addressing mode.	
Permitted Values	IPv4 IPv6	
Default	IPv4	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → IP Stack → IP Stack	
Web UI	Network → IP Parameters → Internet Port → IP Stack Mode **Note:** Only the M8 phone supports IPv6 configuration in phone web.	

Note: If you change this parameter, the IP phone will reboot for the change to take effect.

2.1.2 IPv4 Configuration

The following table lists the parameters you can use to configure IPv4.

Parameter	**DeviceNetworkDhcpMode**	**config.xml**
Description	It configures the Internet port type for IPv4. **Note:** It works only if “DeviceNetworkIpStackMode” is set to IPv4.	
Permitted Values	Static Dynamic DynamicAlcatel	
Default	Dynamic	
Web UI	Network → IP parameters → DHCP Mode	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → IP Config → IPv4 Settings → IPv4 Mode	
Parameter	**DeviceNetworkIpAddress**	**config.xml**

Description	It configures the IPv4 address. **Note:** It works only if “DeviceNetworkIpStackMode” is set to IPv4, and "DeviceNetworkDhcpMode" is set to Static.	
Permitted Values	IPv4 Address	
Default	0.0.0.0	
Web UI	Network → IP parameters → IP Address	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → IP Config → IPv4 Settings → IP	
Parameter	**DeviceNetworkSubnetMask**	**config.xml**
Description	It configures the IPv4 subnet mask. **Note:** It works only if “DeviceNetworkIpStackMode” is set to IPv4, and "DeviceNetworkDhcpMode" is set to Static.	
Permitted Values	Subnet Mask	
Default	255.255.255.255	
Web UI	Network → IP parameters → Subnet Mask	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → IP Config → IPv4 Settings → S/net	
Parameter	**DeviceNetworkGateway**	**config.xml**
Description	It configures the IPv4 default gateway. **Note:** It works only if “DeviceNetworkIpStackMode” is set to IPv4, and "DeviceNetworkDhcpMode " is set to Static.	
Permitted Values	IPv4 Address	
Default	0.0.0.0	
Web UI	Network → IP parameters → Gateway	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → IP Config → IPv4 Settings → Gateway	
Parameter	**DmEnetcfgDns1**	**config.xml**
Description	It configures the primary IPv4 DNS server. **Note:** It works only if “DeviceNetworkIpStackMode” is set to IPv4, and "DeviceNetworkDhcpMode" is set to Static.	
Permitted Values	IPv4 Address	
Default	Blank	
Web UI	Network → IP parameters → DNS1	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → IP Config → IPv4 Settings → DNS1	
Parameter	**DmEnetcfgDns2**	**config.xml**

Description	It configures the secondary IPv4 DNS server. **Note:** It works only if “DeviceNetworkIpStackMode” is set to IPv4, and "DeviceNetworkDhcpMode " is set to Static.
Permitted Values	IPv4 Address
Default	Blank
Web UI	Network → IP parameters → DNS2
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → IP Config → IPv4 Settings → DNS2

Note: If you change this parameter, the IP phone will reboot for the change to take effect.

2.1.3 IPv6 Configuration

To configure the network settings on the phone for an IPv6 network, you can set up an IP address for the phone by using SLAAC (ICMPv6), DHCPv6 or by manually entering an IP address. Ensure that your network environment supports IPv6. Contact your ISP for more information.

When you enable both SLAAC and DHCPv6 on the phone, the server can specify the IP phone to obtain the IPv6 address and other network settings either from SLAAC or from DHCPv6. If the SLAAC server is not working, the IP phone will try to obtain the IPv6 address and other network settings via DHCPv6.

The following table lists the parameters you can use to configure IPv6.

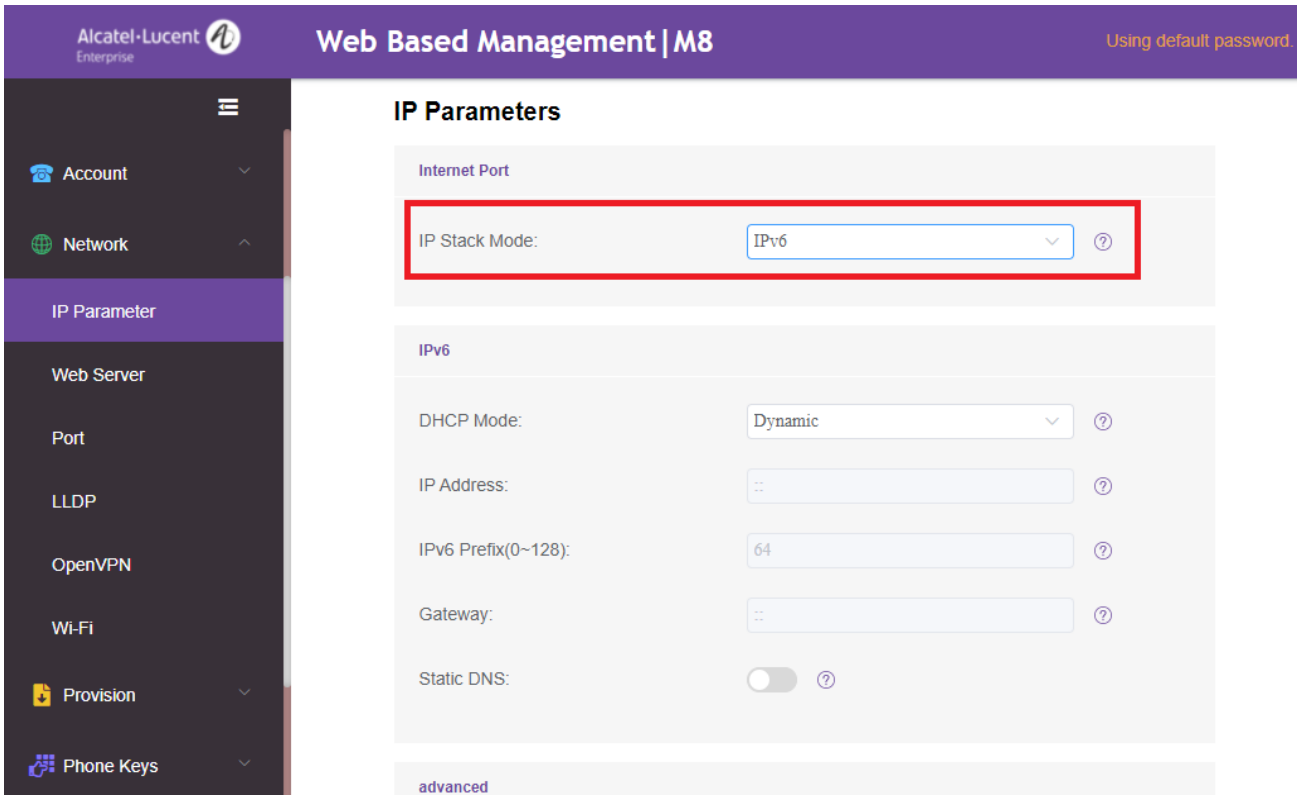
Parameter	**DeviceNetworkIpv6DhcpMode**	**config.xml**
Description	It configures the Internet port type for IPv6. **Note:** It works only if “DeviceNetworkIpStackMode” is set to IPv6.	
Permitted Values	Static Dynamic	
Default	Dynamic	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → IP Config → IPv6 Settings → IPv6 Mode	
Web UI	Network → IP Parameters → IPv6 → DHCP Mode **Note:** Only the M8 phone supports the IPv6 configuration in phone web.	
Parameter	**DeviceNetworkIpv6Address**	**config.xml**
Description	It configures the IPv6 address. **Note:** It works only if “DeviceNetworkIpStackMode” is set to IPv6, and "DeviceNetworkIpv6DhcpMode " is set to Static.	
Permitted Values	IPv6 Address	
Default	::	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → IP Config → IPv6 Settings → IP	
Web UI	Network → IP Parameters → IPv6 → IP Address **Note:** Only the M8 phone supports the IPv6 configuration in phone web.	
Parameter	**DeviceNetworkIpv6PrefixLen**	**config.xml**

Description	It configures the IPv6 prefix. **Note:** It works only if “DeviceNetworkIpStackMode” is set to IPv6, and "DeviceNetworkIpv6DhcpMode " is set to Static.	
Permitted Values	Integer from 0 to 128	
Default	64	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → IP Config → IPv6 Settings → Prefix6	
Web UI	Network → IP Parameters → IPv6 → IPv6 Prefix (0~128) **Note:** Only the M8 phone supports the IPv6 configuration in phone web.	
Parameter	**DeviceNetworkIpv6Gateway**	**config.xml**
Description	It configures the IPv6 default gateway. **Note:** It works only if “DeviceNetworkIpStackMode” is set to IPv6, and "DeviceNetworkIpv6DhcpMode" is set to Static.	
Permitted Values	IPv6 Address	
Default	::	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → IP Config → IPv4 Settings → Router	
Web UI	Network → IP Parameters → IPv6 → Gateway **Note:** Only the M8 phone supports the IPv6 configuration in phone web.	
Parameter	**DeviceNetworkIpv6Dns1**	**config.xml**
Description	It configures the primary IPv6 DNS server. **Note:** It works only if “DeviceNetworkIpStackMode” is set to IPv6, and "DeviceNetworkIpv6DhcpMode" is set to Static.	
Permitted Values	IPv6 Address	
Default	::	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → IP Config → IPv6 Settings → DNS1	
Web UI	Network → IP Parameters → IPv6 → DNS1 **Note:** Only the M8 phone supports the IPv6 configuration in phone web.	
Parameter	**DeviceNetworkIpv6Dns2**	**config.xml**
Description	It configures the secondary IPv6 DNS server. **Note:** It works only if “DeviceNetworkIpStackMode” is set to IPv6, and "DeviceNetworkIpv6DhcpMode" is set to Static.	
Permitted Values	IPv6 Address	
Default	Blank	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → IP Config → IPv6 Settings → DNS2	

Web UI	Network → IP Parameters → IPv6 → DNS2 **Note:** Only the M8 phone supports the IPv6 configuration in phone web.

Note: If you change this parameter, the IP phone will reboot for the change to take effect.

The M8 phone supports IPv6 configuration in phone web.



2.2 DHCP Options for IPv4

The IP phone can obtain IPv4-related parameters in an IPv4 network via DHCP option.

Note: For more information about DHCP options, refer to RFC 2131 or RFC 2132.

2.2.1 Supported DHCP Options for IPv4

The following table lists common DHCP options for IPv4 supported by the ALE Myriad Series phones.

Parameters	DHCP Option
Provision URL	Option 66
Provision URL	Option 67
Provision URL	Option 43 → Option 66
Provision URL	Option 43 → Option 67
DNS server	Option 6
Hostname	Option 12
Domain name	Option 15
SNTP Server	Option 42
802.1Q VLAN ID.	Option 132
802.1p LAYER 2 Priority	Option 133

Timezone	Option 100

2.2.2 DHCP Option 66/Option 67/Option 43 with Sub-Option 66/67

The usage scenarios for DHCP options 66 and 67 are listed below for reference:

Option 66	Option 67	Option 43		Result
		Option 66	Option 67	
http(s)://172.24.190.159		no data		http(s)://172.24.190.159/
http(s)://172.24.190.159	/provisioning			http(s)://172.24.190.159/provisioning
http(s)://172.24.190.159	http(s)://172.24.190.160			http(s)://172.24.190.159/
172.24.190.159	172.24.190.160			https://172.24.190.159/
172.24.190.159	http(s)://172.24.190.160			http(s)://172.24.190.160
	/provisioning Or 172.24.190.160			https://provisioning Or https://172.24.190.160
	http://172.24.190.160			http://172.24.190.160
any data		http://172.24.190.161		http://172.24.190.161
		http://172.24.190.161	/provisioning	http://172.24.190.161/provisioning
		http://172.24.190.161	http://172.24.190.162	http://172.24.190.161
		172.24.190.161	172.24.190.162	https://172.24.190.161
		172.24.190.161	http://172.24.190.162	http://172.24.190.162
			/provisioning	https://provisioning
			http://172.24.190.162	http://172.24.190.162

Note: If the user configures a relative path with only IP address or domain name for DHCP option 66/67, the default https protocol will be added to the provisioning URL.

2.2.3 DHCP Option 42

The ALE Myriad Series phones support using the NTP server address provided by DHCP.

DHCP option 42 is used to specify a list of NTP servers available to the client by IP address.

The following table lists the parameters you can use to configure DHCP option 42 for NTP server address.

Parameter	SettingSntpServer	config.xml
Description	It configures the primary NTP server.	
Permitted Values	IPv4 Address	
Default	0.pool.ntp.org	
Web UI	Setting → Time & Date → SNTP Address	
Parameter	SettingSntpServer2	config.xml
Description	It configures the secondary NTP server.	
Permitted Values	IPv4 Address	
Default	time.nist.gov	
Web UI	Setting → Time & Date → SNTP Secondary Address	

2.2.4 DHCP Option 12

You can specify a hostname for the phone when using DHCP. The DHCP client uses option 12 to send a predefined hostname to the DHCP registration server. The name may or may not be qualified with the local domain name (based on RFC 2132). See RFC 1035 for character phone restrictions.

2.2.5 DHCP Option 132

The ALE Myriad Series phones support configuring DHCP option 132 to define 802.1Q VLAN ID.

2.2.6 DHCP Option 133

The ALE Myriad Series phones support configuring DHCP option 133 to define 802.1p LAYER 2 priority for SIP/RTP.

2.2.7 DHCP Option 100

The IP phones support configuring DHCP option 100 to define time zone.

The format of the POSIX specifier is <name><offset><dst name><dst offset><dstrule>

- <name> is the name of the timezone when not in daylight savings (e.g., GMT, PST, NZST)
- <offset> is the offset added to the local time to get UTC, specified as [+|-]hh[:mm[:ss]] (eg 0, 8, -12)
- <dst name> is the name of the timezone when in daylight savings (eg BST, PDT, NZDT)
- <dst offset> is the offset added to the local time to get UTC during daylight savings, similarly specified as [+|-]hh[:mm[:ss]]

Examples:

- London: GMT0BST1,M3.5.0/1:00:00,M10.5.0/2:00:00
- Los Angeles: PST8PDT,M3.2.0/2:00:00,M11.1.0/2:00:00
- New Zealand: NZST-12NZDT,M9.5.0/2:00:00,M4.1.0/3:00:00

2.2.8 VCI Definition

You can define the VCI by the parameter below in the configuration file:

Parameter	DeviceNetworkVciValue	config.xml
Description	It configures the phone VCI information.	

Permitted Value	TEXT
Default	aledevice

2.3 DHCP Options for IPv6

The IP phone can obtain IPv6-related parameters in an IPv6 network via DHCP option.

Parameters	DHCP Option	Description
Provision URL	Option 59	One provisioning URL address or FQDN
Provision URL	Option 17	Full path provisioning URL
DNS server	Option 23	
Hostname	Option 39	
Domain name	Option 24	
SNTP server	Option 31	

2.3.1 DHCP Option 17 and Option 59

During the startup, the phone will automatically detect Option 17 or Option 59 for obtaining the provisioning server address. The priority of obtaining the provisioning server address is as follows: option 17→ option 59.

2.4 VLAN

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

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

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

2.4.1 LLDP Configuration

LLDP (Linker Layer Discovery Protocol) is a vendor-neutral link layer protocol, which allows IP phones to receive and/or transmit device-related information from/to directly connected devices on the network that are also using the protocol, and store the information about other devices.

When LLDP feature is enabled on IP phones, the IP phones periodically advertise their own information to the directly connected LLDP-enabled switch. The IP phones can also receive LLDP packets from the connected switch. When the application type is “voice”, the IP phones decide whether to update the VLAN configurations obtained from the LLDP packets. When the VLAN configurations on the IP phones are different from the ones sent by the switch, the IP phones perform an update and reboot. This allows the IP phones to plug into any switch, obtain their VLAN IDs, and then start communications with the call control.

The following table lists the parameters you can use to configure LLDP.

Parameter	**DeviceNetworkLldpVlanEnable**	**config.xml**

Description	It enables or disables the LLDP (Linker Layer Discovery Protocol) feature on the IP phone.
Permitted Values	true - enable false - disable
Default	true
Web UI	Network → LLDP → VLAN Acquirement
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → LLDP → VLAN Acquirement

2.4.2 Manual VLAN Configuration

VLAN is disabled on IP phones by default. You can configure VLAN for the Internet port and PC port manually. Before configuring VLAN on the IP phone, you need to obtain the VLAN ID from your network administrator.

The following table lists the parameters you can use to configure VLAN manually.

Parameter	**DeviceNetworkLanVlanEnable**	**config.xml**
Description	It enables or disables the VLAN for the Internet port.	
Permitted Values	true - enable false - disable	
Default	false	
Web UI	Network → IP Parameters → LAN VLAN	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → IP Config → Vlan → Vlan Config → Use VLAN	
Parameter	**DeviceNetworkLanVlanNumber**	**config.xml**
Description	It configures the VLAN ID for the Internet port. **Note:** It works only if “DeviceNetworkLanVlanEnable” is set to true.	
Permitted Values	Integer from 0 to 4095	
Default	4095	
Web UI	Network → IP Parameters → LAN VLAN Number	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → IP Config → Vlan → Vlan Config → ID	
Parameter	**DeviceNetworkPcVlanEnable**	**config.xml**
Description	It enables or disables the VLAN for the PC port.	
Permitted Values	true - enable false - disable	
Default	false	
Web UI	Network → IP Parameters → PC VLAN	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → IP Config → Vlan → Data Vlan Config → Use VLAN	

Parameter	DeviceNetworkPcVlanNumber	config.xml
Description	It configures the VLAN ID for the PC port. **Note:** It works only if “DeviceNetworkPcVlanEnable” is set to true.	
Permitted Values	Integer from 0 to 4094	
Default	0	
Web UI	Network → IP Parameters → PC VLAN Number	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → IP Config → Vlan → Data Vlan Config → ID	

2.4.3 DHCP VLAN

The ALE Myriad Series phones support VLAN discovery via DHCP. The predefined Option 43→ Option 58 is used to supply the VLAN ID by default. And Option 58 has higher priority than Option 132.

2.5 Wi-Fi

Wi-Fi feature enables you to connect the phones to the organization’s wireless network. The wireless network is more convenient and cost-effective than the wired network. Wi-Fi feature is applicable to the ALE Myriad Series phones.

When the Wi-Fi feature is enabled, the IP phone will automatically scan the available wireless networks. All the available wireless networks will display in scanning list on the phone screen.

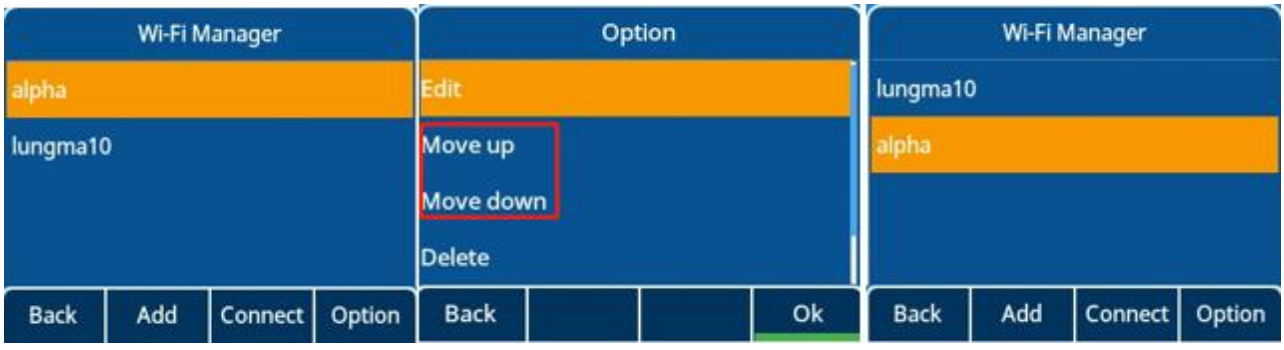
You can store up to 5 frequently used wireless networks on your phone.

You can configure for the ALE Myriad Series phones: Basic Setting → Wi-Fi → Wi-Fi Manager (phone user interface).

Note: To use Wi-Fi feature on the ALE Myriad Series phones M3/M5/M7, make sure the Wi-Fi USB dongle is properly connected to the USB port on the phone. The Wi-Fi USB dongle should be purchased separately.

For M8, Wi-Fi is built-in. Wi-Fi USB dongle which is connected to the phone USB port is not supported for M8.

The M3/M5/M7/M8 phones support storing up to 5 frequently used wireless networks on your phone and specifying the priority for them. You can configure the priority of AP by pressing the “Move up” or “Move down” button as indicated in the following screenshots.



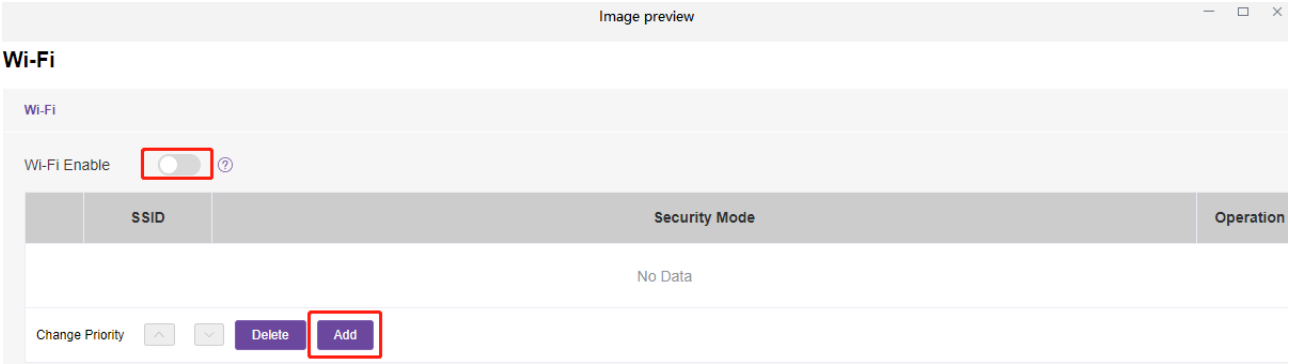
The phones also provide the Wi-Fi status showing the information of currently connected Wi-Fi.

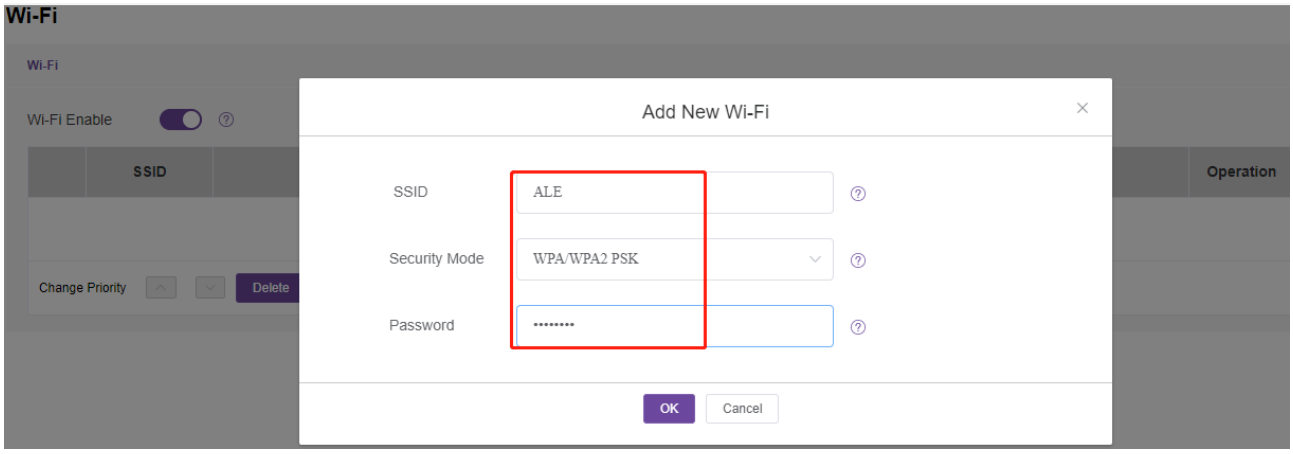
The following table lists the parameters you can use to configure Wi-Fi.

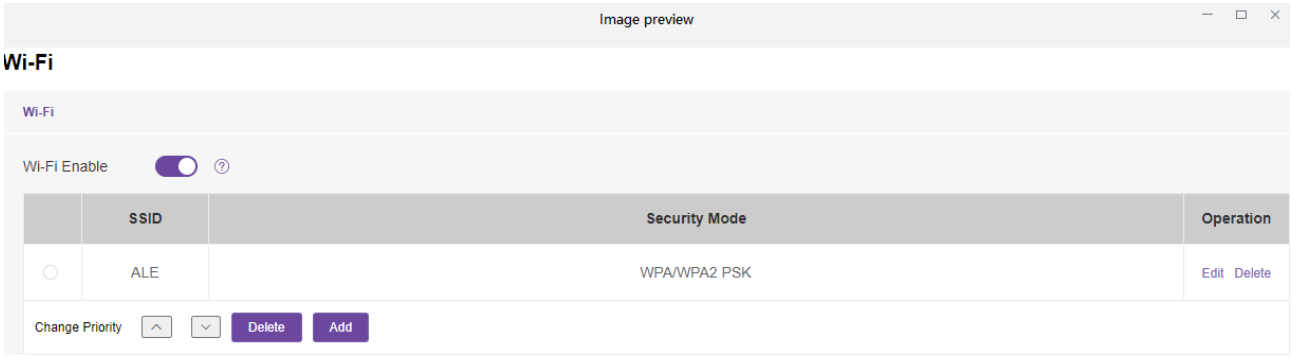
Parameter	**DeviceWifiFunctionEnable**	**config.xml**
Description	It enables or disables the Wi-Fi feature.	
Permitted Values	false - disabled true – enable	
Default	true	
Parameter	**DeviceWifiEnable**	**config.xml**
Description	It activates or deactivates the Wi-Fi mode.	
Permitted Values	false - disabled true - enable	
Default	true **Note**: For the M8 phone, the default value is false.	
Phone UI	Basic Setting → Wi-Fi → Enable WiFi	
Web UI	Network → Wi-Fi	
Parameter	**DeviceNetworkRedundancyMode**	**config.xml**
Description	It configures preferentially network type.	
Permitted Values	0 - Wi-Fi only 1 - Wi-Fi preferentially 2 - Wired preferentially	
Default	1 **Note**: For the M8 phone, the default value is 2.	
Parameter	**DeviceWifi[1-5]Ssid**	**config.xml**
Description	It configures the AP SSIDs.	
Permitted Values	Strings	
Default	Blank	
Phone UI	Basic Setting → Wi-Fi → Wi-Fi Manager	

Web UI	Network → Wi-Fi	
Parameter	**DeviceWifi[1-5]AuthMode**	**config.xml**
Description	It configures the authentication method of AP.	
Permitted Values	0 - NONE 1 - WPA/WPA2 PSK 2 - WEP	
Default	0	
Phone UI	Basic Setting → Wi-Fi → Wi-Fi Manager	
Web UI	Network → Wi-Fi	
Parameter	**DeviceWifi[1-5]Password**	**config.xml**
Description	If “WPA/WPA2 PSK” is chosen, this will be used. The length should be >=8 and <=63. If “WEP” is chosen, this will be used. This should be 5 ASCII for WEP64 and 13 ASCII for WEP128.	
Permitted Values	password	
Default	empty	
Phone UI	Basic Setting → Wi-Fi → Wi-Fi Manager	
Web UI	Network → Wi-Fi	
Parameter	**DeviceWifi[1-5]Priority**	**config.xml**
Description	It configures the priority for the wireless network for the IP phone. 5 is the highest priority, and 1 is the lowest priority.	
Permitted Values	1 - 1 2 - 2 3 - 3 4 - 4 5 - 5	
Default	1	
Phone UI	Basic Setting → Wi-Fi → Wi-Fi Manager	
Web UI	Network → Wi-Fi	

The M8 phone supports configuring the Wi-Fi feature on phone WBM (Network → Wi-Fi).







2.6 Network Address Translation (NAT)

Network Address Translation (NAT) is a function that allows multiple devices to share the same public routable IP address to establish connections over the Internet. NAT is present in many broadband access devices to translate public and private IP address.

The ALE Myriad Series phones can work with Rport type of NAT.

2.6.1 Rport Configuration

The ALE Myriad Series phones support Rport described in RFC 3581. It allows a client to request that the server sends the response back to the source port from which the request came.

Rport feature needs support from SIP server.

The following table lists the parameter you can use to configure Rport.

Parameter	**AccountXRportEnable**	**config.xml**
Description	It enables or disables the NAT Rport feature. **Note:** X means account ID and it can be number 1~8 for M3/M5/M7, 1-20 for M8.	
Permitted Values	false - disable true - enable	
Default	false	
Web UI	Account → Advanced → Rport	

2.7 Internet Port and PC Port

The ALE Myriad Series phones support two Ethernet ports: Internet port and PC port. You can enable or disable the PC port on the IP phones.

2.7.1 Supported Transmission Methods

Three methods of configuration transmission for IP phone Internet port and PC port:

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

Auto-negotiate is configured for both Internet port and PC port on the IP phone by default.

2.7.2 Internet Port and PC Port Configuration

The following table lists the parameters you can use to configure Internet port and PC port.

Parameter	**DeviceNetworkLanAutoEnable**	**config.xml**
Description	It configures the transmission method for Internet port.	
Permitted Values	false - disable true - enable	
Default	true	
Web UI	Network → Port → LAN Auto	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → Ethernet → LAN → Auto	
Parameter	**DeviceNetworkLanSpeed**	**config.xml**
Description	It configures the transmission method for Internet port. **Note:** It works only if “DeviceNetworkLanAutoEnable” is set to false.	
Permitted Values	10 100	
Default	1000	
Web UI	Network → Port → LAN Speed	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → Ethernet → LAN → LAN speed	
Parameter	**DeviceNetworkLanDuplexType**	**config.xml**
Description	It configures the transmission method for Internet port. **Note:** It works only if “DeviceNetworkLanAutoEnable” is set to false.	
Permitted Values	Half full	
Default	half	
Web UI	Network → Port → Lan Duplex	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → Ethernet → LAN → LAN duplex	
Parameter	**DeviceNetworkPcAutoEnable**	**config.xml**
Description	It configures the transmission method for PC port.	
Permitted Values	false - disable true - enable	

Default	true	
Web UI	Network → Port → PC Auto	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → Ethernet → PC → Auto	
Parameter	**DeviceNetworkPcSpeed**	**config.xml**
Description	It configures the transmission method for PC port. **Note:** It works only if "DeviceNetworkPcAutoEnable" is set to false.	
Permitted Values	10 100	
Default	-	
Web UI	Network → Port → PC Speed	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → Ethernet → PC → PC speed	
Parameter	**DeviceNetworkPcDuplexType**	**config.xml**
Description	It configures the transmission method for PC port. **Note:** It works only if "DeviceNetworkPcAutoEnable" is set to false.	
Permitted Values	Half Full	
Default	-	
Web UI	Network → Port → PC Duplex	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → Ethernet → PC → PC duplex	

2.8 OpenVPN

The ALE Myriad Series phones use OpenVPN to achieve VPN feature. After you configure VPN feature on the IP phone, the IP phone will act as a VPN client and use the certificates to authenticate with the VPN server.

2.8.1 OpenVPN Related Files

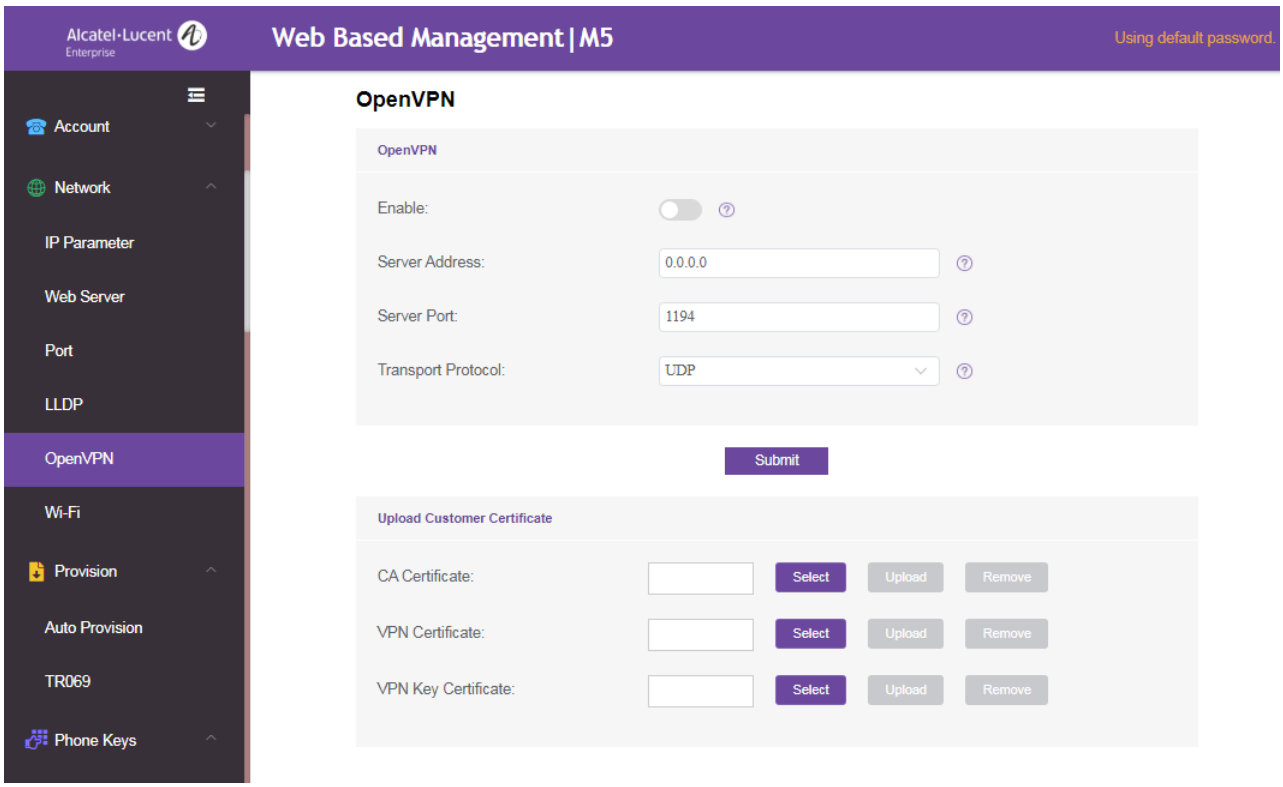
The OpenVPN-related files include certificates (ca.crt and client.crt), key (client.key) and the configuration file (vpn.cnf) of the OpenVPN client.

The following table lists the unified directories of the OpenVPN certificates and key in the configuration file (vpn.cnf) for the ALE Myriad Series phones:

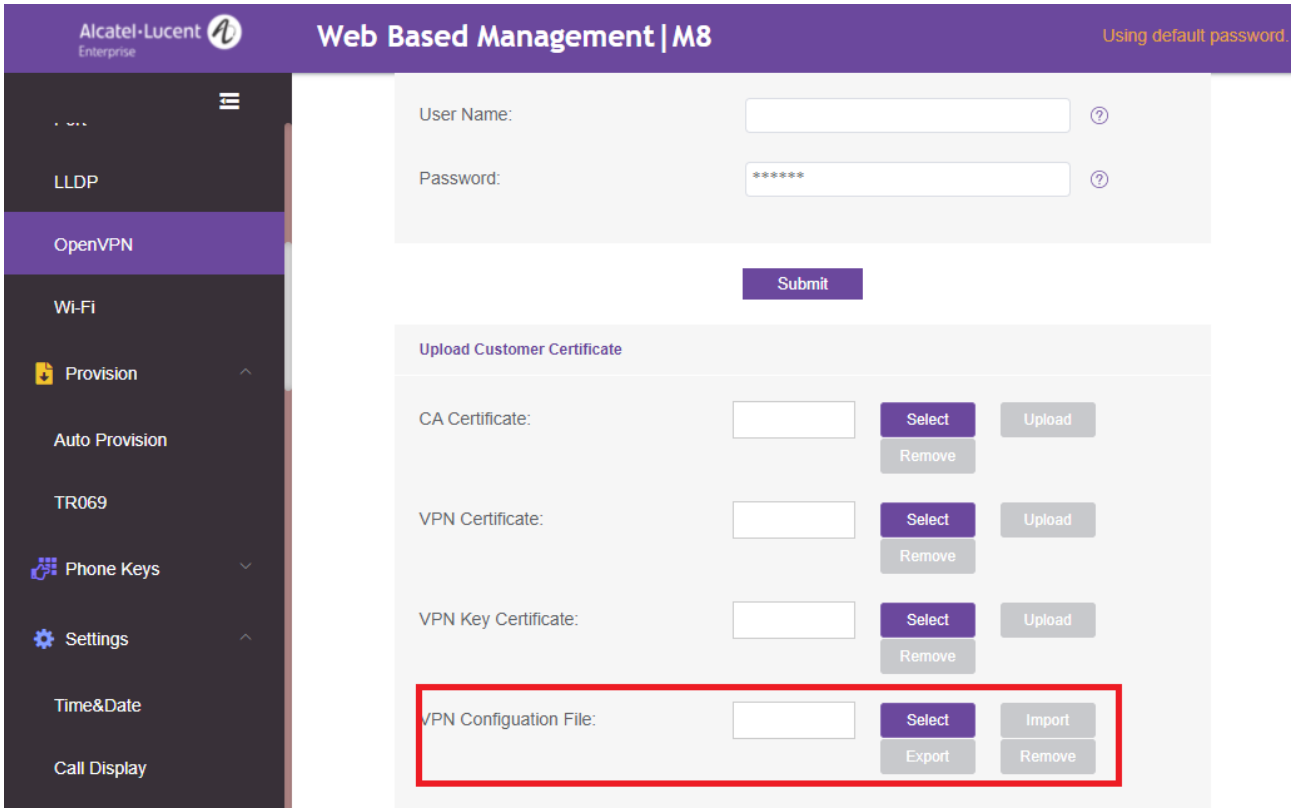
OpenVPN Files	Description	Unified Directories
ca.crt	CA certificate	/config/cert/openvpn/ ca.crt
client.crt	Client certificate	/config/cert/openvpn/client.crt
client.key	Private key of the client	/config/cert/openvpn/client.key

2.8.2 OpenVPN Configuration

You can configure the OpenVPN feature via the Web UI path: Network → OpenVPN for the ALE Myriad Series phones.



The M8 phone supports uploading the OpenVPN configuration file in phone web.



2.9 Quality of Service (QoS)

VoIP is extremely bandwidth- and delay-sensitive. QoS is a major issue in VoIP implementations regarding how to guarantee that packet traffic is not delayed or dropped due to interference from other lower priority traffic. VoIP can guarantee high-quality QoS only if the voice and the SIP packets are given priority over other kinds of network traffic. IP phones support the 802.1P/DiffServ model of QoS.

Voice QoS

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

SIP QoS

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

DSCPs for voice and SIP packets can be specified respectively.

2.9.1 Voice and SIP QoS Configuration

The following table lists the parameters you can use to configure voice QoS and SIP QoS.

Parameter	**Setting8021pPriority**	**config.xml**
Description	It configures audio 802.1p priority.	
Permitted Values	[0-7]	
Default	5	
Web UI	Setting → Audio → 802.1P Priority	
Parameter	**SettingAudiodiffserv**	**config.xml**
Description	It configures audio TOS/Diffserv.	
Permitted Values	[0-63]	
Default	46	
Parameter	**Setting8021pUserPriority**	**config.xml**
Description	It configures 802.1P User Priority for SIP messages.	
Permitted Values	[0-7]	
Default	5	
Parameter	**SIPDscp**	**config.xml**
Description	It configures TOS/Diffserv for SIP messages.	
Permitted Values	[0-63]	
Default	40	

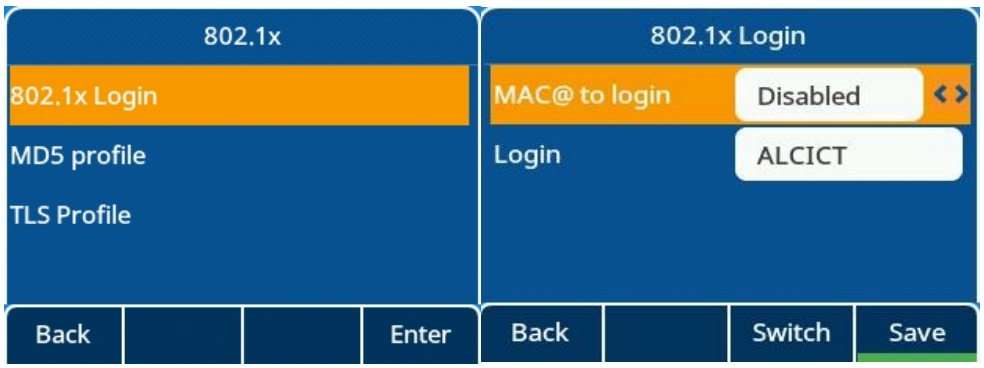
2.10 802.1x Authentication

The ALE Myriad Series phones support the following protocols for 802.1X authentication:

- EAP-MD5
- EAP-TLS (requires Device and CA certificates, requires no password)

You can configure the 802.1x feature via Phone UI path:

Menu → Advanced Setting (default password: 123456) → Network → 802.1x



2.11 TR-069 Device Management

TR-069 is a technical specification defined by the Broadband Forum, which defines a mechanism that encompasses secure auto-configuration of a CPE (Customer-Premises Equipment), and incorporates other CPE management functions into a common framework. TR-069 uses common transport mechanisms (HTTP and HTTPS) for communication between CPE and ACS (Auto Configuration Servers). The HTTP(S) messages contain XML-RPC methods defined in the standard for configuration and management of the CPE.

2.11.1 RPC Methods

The following table provides a description of RPC methods supported by IP phones.

RPC Method	Description
GetRPCMethods	Used for discovering supported methods by CPE.
PhoneParameterValues	Used for modifying the value of one or more CPE parameters.
GetParameterValues	Used for obtaining the value of one or more CPE parameters.
etParameterNames	Used for discovering the parameters accessible on a specific CPE.
GetParameterAttributes	Used for reading the attributes associated with one or more CPE parameters.
PhoneParameterAttributes	Used for modifying attributes associated with one or more CPE parameters.
Reboot	Used for rebooting CPE.
Download	Used for downloading a file from the server. Supported file types: • Firmware Image • Configuration File
Upload	Used for uploading a file to the server. Supported file types:

	• Configuration File • Log File
ScheduleInform	Used for requesting the CPE to schedule information.
FactoryReset	Used for resetting to factory.
TransferComplete	This method informs the ACS of the completion (either successful or unsuccessful) of a file transfer initiated by an earlier Download or Upload method call.
AddObject	Use for adding a new instance of an object defined on the CPE.
DeleteObject	Use for removing a specific instance of an object.

2.11.2 TR069 Configuration

The following table lists the parameters you can use to configure TR069.

Parameter	**DeviceTr069Enable**	**config.xml**
Description	It enables or disables the TR069 feature.	
Permitted Values	false - disable true - enable	
Default	true	
Web UI	Provision → TR069 → Enable TR069	
Parameter	**DeviceTr069ThirdPartyAcsUrl**	**config.xml**
Description	It configures third party ACS server URL.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Provision → TR069 → ACS URL	
Parameter	**DeviceTr069AcsUsername**	**config.xml**
Description	It configures ACS account username.	
Permitted Values	String within 128 characters	
Default	easycwmp	
Web UI	Provision → TR069 → ACS Username	
Parameter	**DeviceTr069AcsPwd**	**config.xml**
Description	It configures ACS account password.	
Permitted Values	String within 64 characters	
Default	easycwmp	
Web UI	Provision → TR069 → ACS Password	
Parameter	**DeviceTr069AcsPeriodicEnable**	**config.xml**
Description	It enables ACS Periodic informing.	

Permitted Values	true - enable false - disable	
Default	false	
Web UI	Provision → TR069 → ACS Periodic Enable	
Parameter	**DeviceTr069AcsPeriodicInterval**	**config.xml**
Description	It configures ACS Periodic Interval inform timer.	
Permitted Values	Integer	
Default	1000	
Web UI	Provision → TR069 → ACS Periodic Interval	
Parameter	**DeviceTr069AcsConnectionUsername**	**config.xml**
Description	It configures client account username.	
Permitted Values	String within 128 characters	
Default	easycwmp	
Web UI	Provision → TR069 → ACS Connection Username	
Parameter	**DeviceTr069AcsConnectionPwd**	**config.xml**
Description	It configures client account password.	
Permitted Values	String within 64 characters	
Default	easycwmp	
Web UI	Provision → TR069 → ACS Connection Password	
Parameter	**DeviceTr069StunEnable**	**config.xml**
Description	It enables https STUN function.	
Permitted Values	true - enable false - disable	
Default	true	
Web UI	Provision → STUN → STUN Enable	
Parameter	**DeviceTr069StunServerAddress**	**config.xml**
Description	It configures STUN server address.	
Permitted Values	IP address or domain name	
Default	stun.l.google.com	
Web UI	Provision → STUN → STUN Server Address	
Parameter	**DeviceTr069StunServerPort**	**config.xml**
Description	It configures STUN server port.	

Permitted Values	Integer from 1024 to 65535
Default	19302
Web UI	Provision → STUN → STUN Server Port

3. Phone Provisioning

This chapter provides basic instructions for setting up your IP phones with a provisioning server.

The M3/M5/M7/M8 phones support the download of configuration files and binary files using TFTP, HTTP and HTTPS protocols.

3.1 Web User Interface

You can configure IP phones via web user interface, a web-based interface that is especially useful for remote configuration.

Because features and configurations vary by phone models and firmware versions, options available on each page of the web user interface can vary as well. Note that the features configured via web user interface are limited. Therefore, you can use the web user interface in conjunction with a central provisioning method and phone user interface.

When configuring IP phones via web user interface, you are required to enter a user name and password for access.

The default username/password is admin/123456.

3.1.1 Accessing the Web User Interface

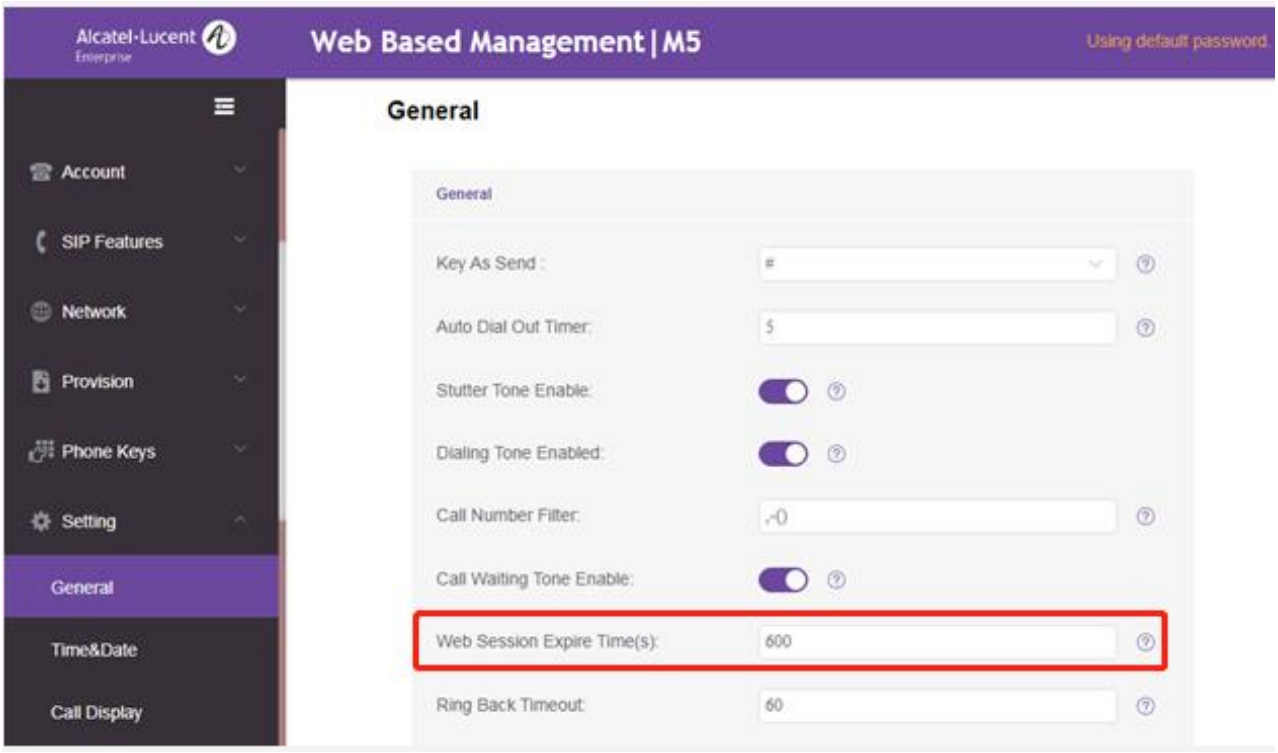
Procedures:

- Step 1: Find the ALE Myriad Series phone's IP address. Press the OK key when the phone is idle.
- Step 2: Enter the IP address in the address bar of a web browser on your PC.
  For example, for IPv4: https://192.168.0.10; for IPv6: https://[2005:1:1:1:215:65ff:fe64:6e0a]
- Step 3: Enter the user name and password.
- Step 4: Click Login.

3.1.2 Navigating the Web User Interface

When you log into the web user interface successfully, the phone status is displayed on the first page of the web user interface. You can click the navigation bar to customize or click Log Out to log out of the web user interface.

The following shows an example of navigating to Setting → General:



3.1.3 Web Server Type Configuration

The ALE Myriad Series phones support both HTTP and HTTPS protocols when accessing the web user interface. You can configure the web server type. Web server type determines the protocol used for accessing the web user interface. If you disable access to web user interface using the HTTP/HTTPS protocol, both you and the user cannot access the web user interface.

The following table lists the parameters you can use to configure web server type.

Parameter	**DeviceNetworkHttpEnable**	**config.xml**
Description	It enables or disables the http protocol to access the web interface.	
Permitted Values	false - disable true - enable	
Default	true	
Web UI	Network → Web Server	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network →Web Server	
Parameter	**DeviceNetworkHttpPort**	**config.xml**
Description	It configures the http port to access the web interface.	
Permitted Values	1~65535	
Default	80	
Web UI	Network → Web Server	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → Web Server	
Parameter	**DeviceNetworkHttpsEnable**	**config.xml**
Description	It enables or disables the https protocol to access the web interface.	

Permitted Values	false - disable true - enable	
Default	true	
Web UI	Network → Web Server	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → Web Server	
Parameter	**DeviceNetworkHttpsPort**	**config.xml**
Description	It configures the http port to access the web interface.	
Permitted Values	1~65535	
Default	443	
Web UI	Network → Web Server	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → Web Server	
Parameter	**DeviceNetworkHttpsDefaultEnable**	**config.xml**
Description	It enables or disables access to the web user interface of the IP phone using the HTTPS protocol by default.	
Permitted Values	false - disable true - enable	
Default	true	

3.2 Phone User Interface

Phone user interface makes configurations available to users and administrators; but the Advanced/Advanced Settings option is only available to administrators and requires an administrator password (default: 123456).

3.3 Configuration Files

The ALE Myriad Series phones support three configuration template files: Common config file, MAC-Oriented config file and Device config file.

3.3.1 Common Config File

Common CFG file, named config.xml, contains parameters that affect the basic features of the IP phone, such as SettingLanguage and volume. It will be effective for all IP phones. The common Config file has a fixed name for each phone model.

3.3.2 MAC-Oriented Config File

MAC-Oriented CFG file is named after the MAC address of the IP phone. For example, if the MAC address of an IP phone is 3C28A6200088, the name of MAC-Oriented CFG file is config. 3C28A6200088.xml.

It contains parameters unique to a specific phone, such as account registration. It will only be effective for a MAC-specific IP phone.

3.3.3 Device Config File

Device Config file is named after the device model of the IP phone. For example, if the device model of an IP phone is M7, the name of Device CFG file is config.M7.xml.

It contains common parameters that affect the same model IP phones. The Device CFG file has a fixed name for each phone model.

3.4 EDS (Easy Deployment Server)

EDS (Easy Deployment Server) is a server which provides the information for ALE SIP devices to connect to the provisioning server. It is a redirect provisioning server and has a web-based interface for the user to manage such information. Please find the EDS user manual by accessing https://aledevice.com for more information.

3.5 Provisioning Methods

The ALE Myriad Series phones provide two ways to provision your phones:

- Manual Provisioning: provisioning via the local phone user interface or web user interface.
- Central Provisioning: provisioning through configuration files stored in a central provisioning server.

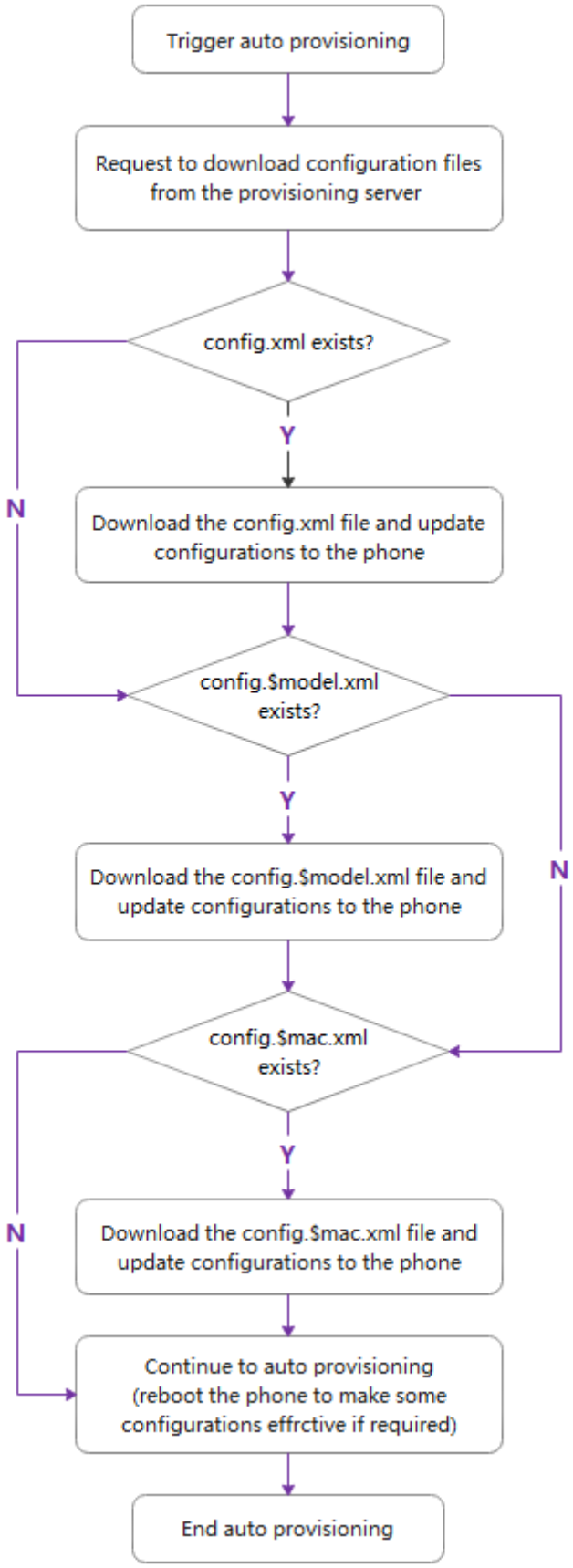
Key factor for choosing which method is used depends on how many phones need to be deployed and what features and settings need to be configured. Manual provisioning on the web or phone user interface does not contain all the phone settings available for the centralized method. You can use the web user interface method in conjunction with a central provisioning method and phone user interface method. We recommend using centralized provisioning as your primary provisioning method when provisioning multiple phones.

3.6 Auto Provisioning Process

3.6.1 Auto Provisioning Process

The auto provisioning process will be executed after finishing the initialization. After the phone boots up, it will request configuration files through the acquired URL in sequence. The sequence of auto provisioning execution is DHCP → PNP → Local → EDS → RDDS. At any of the five steps, once the phone can download the configuration files successfully, the phone will exit auto provisioning process.

Note: If the phone downloads a configuration file in wrong format during the auto provisioning process, parsing fails, and the phone will continue auto provisioning process.



Flow Chart

3.6.2 Relative Path of Configuration File

The following table lists the parameters which you can use for configuring the customized configuration file.

Parameter	DeviceProvisionFileFirst	config.xml
Description	It configures the first requested configuration file.	
Permitted Values	String within 511 characters	
Default	config.xml	
Parameter	DeviceProvisionFileSecond	config. xml
Description	It configures the second requested configuration file.	
Permitted Values	String within 511 characters	
Default	config.$model.xml	
Parameter	DeviceProvisionFileThird	config.xml
Description	It configures the third requested configuration file.	
Permitted Values	String within 511 characters	
Default	config.$mac.xml	

When the phone is performing the auto provisioning process via a relative URL, the phone will request the following three default configuration files in turn.

- config.xml
- config.$model.xml
- config.$mac.xml

If you want to customize the configuration file, you can create some new files by making a copy and renaming the configuration template file, then save the configuration file and place it on the provisioning server. The IP phone will request the customized file.

For example, set the **DeviceProvisionFileFirst** to 1.xml, set the **DeviceProvisionFileSecond** to 2.xml, and set the **DeviceProvisionFileThird** to 3.xml, the phone will request the following three configuration files in turn.

- 1.xml
- 2.xml
- 3.xml

Note: The ALE Myriad Series phones only support the xml format config file.

3.6.3 Timeout Mechanisms

In the process of auto provisioning, there are two kinds of timeout mechanisms for some abnormal scenarios. It provides a clearer definition of some behaviors of the phone when there are network issues and can also improve the efficiency of the auto provisioning process.

The following table lists the parameters you can use to configure the settings of timeout in auto provisioning process.

Parameter	DeviceNetworkConnectExpiredTime	config.xml

Description	It configures the timeout interval (in seconds) to transfer a file for HTTP/HTTPS connection. **Note:** When the HTTP/HTTPS connection cannot be successfully established within the configured time, the phone will exit the current auto provisioning process and perform the next one.	
Permitted Values	Integer from 1 to 20	
Default	10	
Parameter	**DeviceProvisionAttemptExpiredTime**	**config.xml**
Description	It configures the timeout interval (in seconds) to transfer a file via auto provisioning. **Note:** When the phone cannot complete the downloading of configuration file within the configured time, it will exist the current auto provisioning process and execute the next one.	
Permitted Values	Integer from 1 to 300	
Default	20	

3.6.4 Multistage Request Mechanism

To deal with the issue (e.g. the phone may loop indefinitely to perform the auto provisioning process) caused by the parameter **DeviceProvisionServerUrl** in the configuration file, a new parameter **DeviceProvisionImmediateUpdateTimes** has been added.

When the parameter **DeviceProvisionImmediateUpdateTimes** is set to default value :0, the phone, after getting the configuration file, will not execute the auto provisioning process for the acquired URL, but will save the new URL to replace the old one.

When the parameter **DeviceProvisionImmediateUpdateTimes** is not default value 0 but value 2, after getting the configuration file which includes auto provisioning url1 (file1), the phone will request the auto provisioning url1 to download file1 which includes auto provisioning url2 (file2). After the phone requests the auto provisioning url2 to download the file2 which includes auto provisioning url3 (file3) successfully, the phone will finally request the auto provisioning url3 to download the file3 which includes auto provisioning url4 (file4). At this time, the auto provisioning request reached 3 (n+1) times, so the phone will exit the auto provisioning process and save the auto provisioning url4 to replace auto provisioning url3.

During the whole multistage request process, if the new acquired URL is the same as one of the records in the list, for example, URL 2 is same as URL1, the device will exit the auto provisioning process directly after getting the file2.

The following table lists the parameter you can use to configure the settings for multistage request mechanism.

Parameter	**DeviceProvisionImmediateUpdateTimes**	**config.xml**
Description	It configures the times of auto provisioning the phone executes if the phone gets the new auto provisioning URL.	
Permitted Values	Integer from 0 to 20	
Default	0	

3.6.5 Restoring Default Value

The Myriad phones support restoring the parameters to default values via auto provisioning. When you want to restore several parameters to default values, you do not need to factory reset the phone. Instead, you just need to modify the parameters in the configuration file as following format:

Original:

<setting id="FeatureDndEnable" **value="true"** />

Change:

<setting id="FeatureDndEnable" **define="default"** />

After the phone downloads the configuration file, the parameter of FeatureDndEnable will be changed to default value.

3.7 Keeping User's Personalized Settings after Auto Provisioning

Generally, the system administrators deploy phones in batches and timely maintain company phones via auto provisioning, however, there are some users would like to keep personalized settings after auto provisioning.

The following table lists the parameters you can configure to keep user's personalized settings.

Parameter	**DeviceProvisionUserConfigProtectEnable**	**config.xml**
Description	It enables or disables the IP phone to keep user's personalized settings after auto provisioning. If enabled, the <MAC>-local.xml file will be generated automatically and personalized settings configured via the web or phone user interface will be kept after auto provisioning.	
Permitted Values	false - disable true - enable	
Default	false	
Parameter	**DeviceProvisionUserConfigSyncEnable**	**config.xml**
Description	It enables or disables the IP phone to upload the <MAC>-local.xml file to the server each time the file is updated, and to download the <MAC>-local.xml file from the server during auto provisioning. **Note:** It works only if "DeviceProvisionUserConfigProtectEnable" is set to true (Enabled). The upload/download path is configured by the parameter "DeviceProvisionUserConfigSyncPath".	
Permitted Values	false - disable true - enable	
Default	false	
Parameter	**DeviceProvisionUserConfigSyncPath**	**config.xml**
Description	It configures the URL for uploading/downloading the <MAC>-local.xml file. **Note:** It works only if "DeviceProvisionUserConfigSyncEnable" is set to true (Enabled).	
Permitted Values	URL within 511 characters	
Default	Blank	

Parameter	DeviceProvisionUserConfigUploadMethod	config.xml
Description	It configures the way the IP phone uploads the <MAC>-local.xml file to the server (for HTTP/HTTPS server only).	
Permitted Values	0 - PUT 1 - POST	
Default	1	

3.8 Supported Provisioning Server Discovery Methods

After the phone has established network connection, a provisioning server address should be obtained for configuration settings.

The IP phone supports the following methods to discover the provisioning server address:

PnP: PnP feature allows IP phones to discover the provisioning server address by broadcasting the PnP SUBSCRIBE message during startup.

DHCP: DHCP option can be used to provide the address or URL of the provisioning server to IP phones. When the IP phone requests an IP address using the DHCP protocol, the response may contain option 66 (for IPv4)/option 59 (for IPv6) or the custom option (if configured) that contains the provisioning server address.

Static: You can manually configure the server address via phone user interface or web user interface.

3.8.1 PnP Provisioning Configuration

The following table lists the parameter you can use to configure PnP provisioning.

Parameter	DeviceProvisionPnPEnable	config.xml
Description	It enables or disable PNP function.	
Permitted Values	false - disable true - enable	
Default	true	
Web UI	Provision → Auto Provision	

3.8.2 DHCP Provisioning Configuration

You can choose IPv4 or IPv6 custom DHCP option according to your network environment. The IPv4 or IPv6 custom DHCP option must be in accordance with the one defined in the DHCP server.

The following table lists the parameters you can use to configure DHCP provisioning.

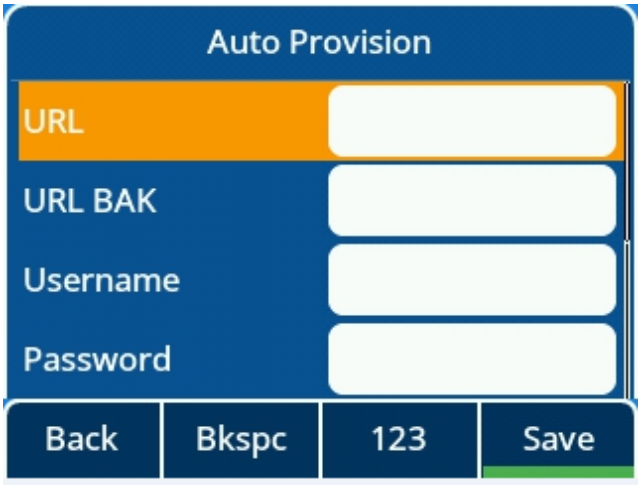
Parameter	DeviceProvisionDHCPEnable	config.xml
Description	It enables or disable DHCP option for acquiring auto provisioning server URL.	
Permitted Values	false - disable true - enable	
Default	true	
Web UI	Provision → Auto Provision	

Parameter	DeviceProvisionDHCPCustomOption	config.xml
Description	It configures the IPv4 custom DHCP option for requesting provisioning server address.	
Permitted Values	Integer from 128-254 Multiple options are separated by ";".	
Default	Blank	
Web UI	Provision → Auto Provision	
Parameter	DeviceProvisionDHCPCustomOptionIPv6	config.xml
Description	It configures the IPv6 custom DHCP option for requesting provisioning server address.	
Permitted Values	Integer from 135-65535, except 143 Multiple options are separated by ";".	
Default	Blank	
Web UI	Provision → Auto Provision	

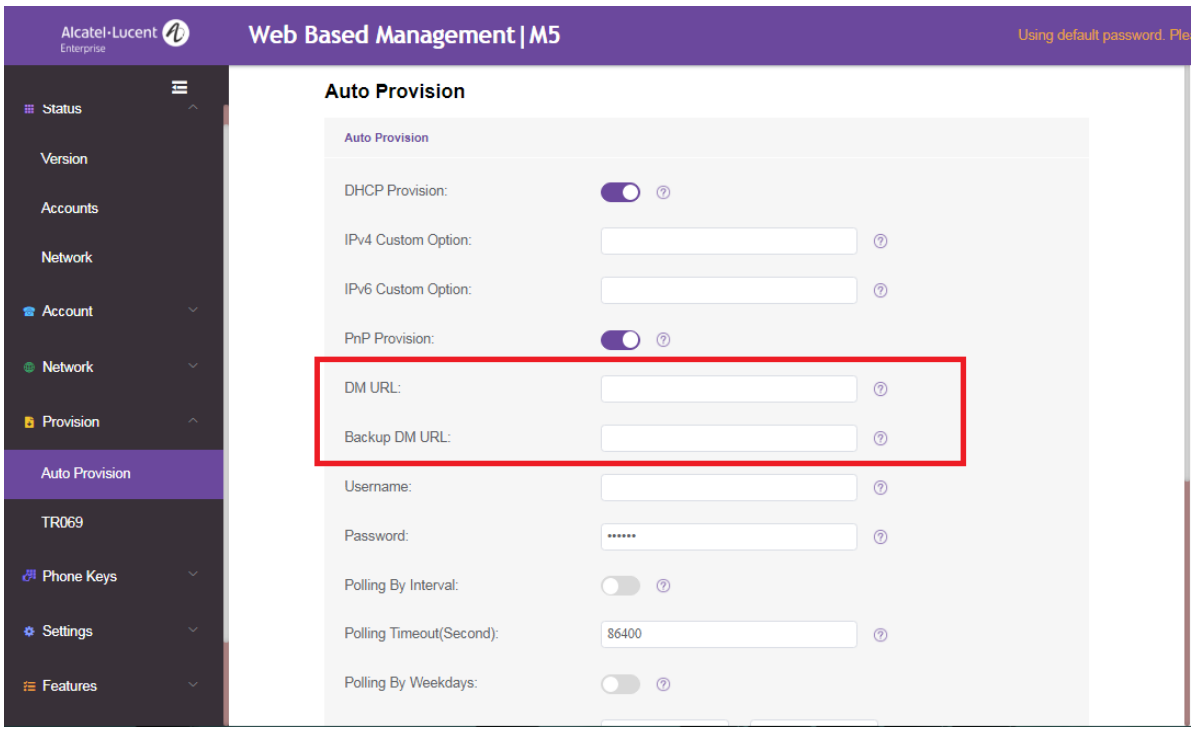
3.8.3 Static Provisioning Configuration

Users can manually configure the server address via phone user interface or web user interface.

- Configure the auto provisioning URL on phone user interface by path: Menu → Advanced Setting (default password: 123456) → Auto Provision



- Configure the auto provisioning URL via the Web UI path: Provision → Auto Provision



- Configure the auto provisioning URL by parameters.

The following table lists the parameters you can use to configure Static provisioning.

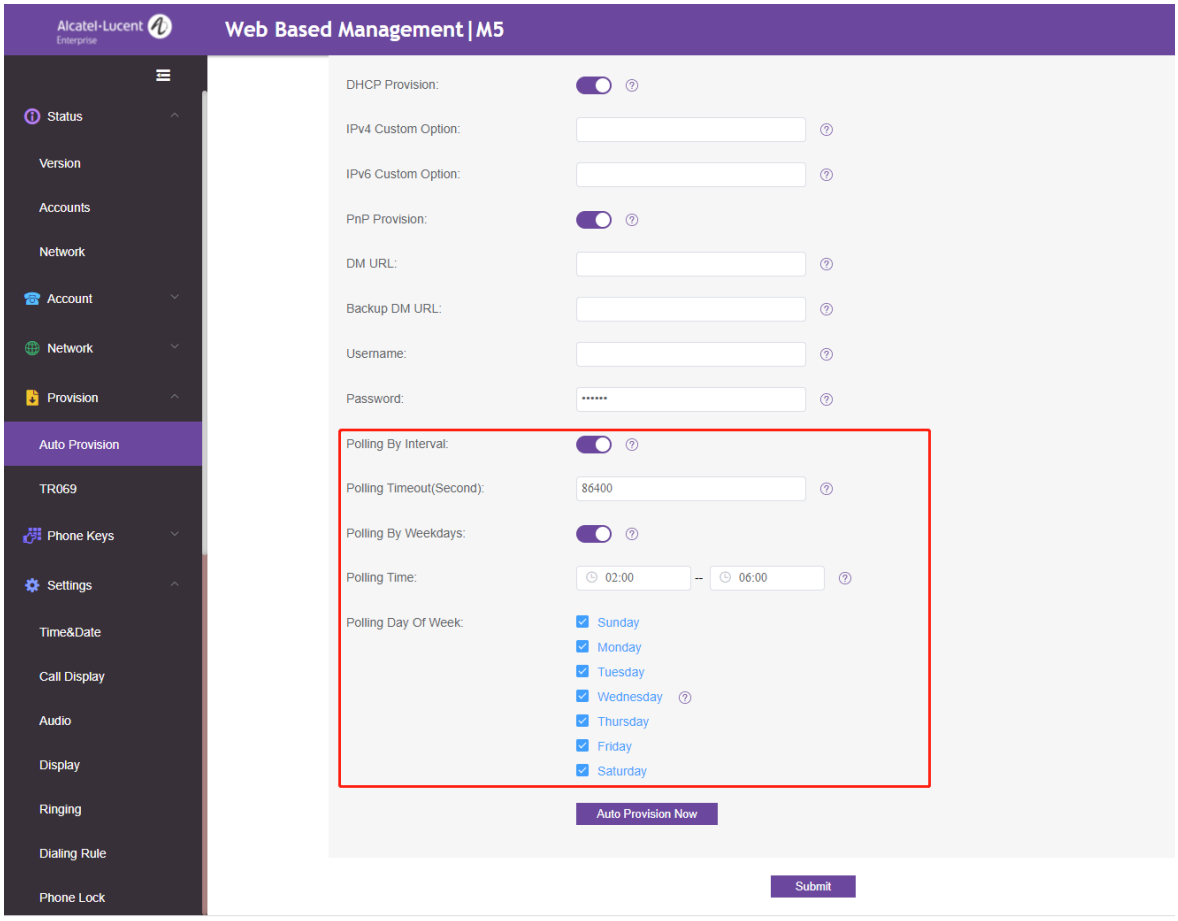
Parameter	**DeviceProvisionServerUrl**	**config.xml**
Description	It configures the DM URL.	
Permitted Values	Strings	
Default	Blank	
Web UI	Provision → Auto Provision	
Phone UI	Menu → Advanced Setting (default password: 123456) → Auto Provision	
Parameter	**DeviceProvisionBackupServerUrl**	**config.xml**
Description	It configures the DM backup URL.	
Permitted Values	Strings	
Default	Blank	
Web UI	Provision → Auto Provision	
Phone UI	Menu → Advanced Setting (default password: 123456) → Auto Provision	
Parameter	**DeviceProvisionServerUsername**	**config.xml**
Description	It configures the username used for http authentication.	
Permitted Values	Strings	
Default	Blank	
Web UI	Provision → Auto Provision	
Phone UI	Menu → Advanced Setting (default password: 123456) → Auto Provision	

Parameter	DeviceProvisionServerPassword	config.xml
Description	It configures the password used for http authentication.	
Permitted Values	Strings	
Default	Blank	
Web UI	Provision → Auto Provision	
Phone UI	Menu → Advanced Setting (default password: 123456) → Auto Provision	

3.8.4 Provisioning Polling Configuration

Users can configure the polling time so that the phone can download the configuration file periodically once the time reached. Furthermore, the IP phone also allow users to define the phone downloading the configuration files weekly.

- Configure the polling time via the Web UI path: Provision → Auto Provision. The default value of interval time is 86400 seconds.



- Configure the auto provisioning polling settings by parameters.

The following table lists the parameters you can use to configure polling mechanism.

Parameter	DeviceProvisionPollingByIntervalEnable	config.xml
Description	It enables or disables configuration file polling periodly.	
Permitted Values	false - disable true - enable	

Default	false	
Web UI	Provision → Auto Provision	
Parameter	**DeviceProvisionPollingInterval**	**config.xml**
Description	It configures update process polling period. The unit is second.	
Permitted Values	Numeric [60 – 86400]	
Default	86400	
Web UI	Provision → Auto Provision	
Parameter	**DeviceProvisionPollingByWeekdaysEnable**	**config.xml**
Description	It enables or disables polling weekly.	
Permitted Values	false - disable true - enable	
Default	false	
Phone UI	Menu → Advanced Setting (default password: 123456) → Auto Provision	
Parameter	**DeviceProvisionPollingBeginTime**	**config.xml**
Description	It configures polling begin time.	
Permitted Values	Time from 00:00 to 23:59	
Default	02:00	
Web UI	Provision → Auto Provision	
Parameter	**DeviceProvisionPollingEndTime**	**config.xml**
Description	It configures polling end time.	
Permitted Values	Time from 00:00 to 23:59	
Default	06:00	
Web UI	Provision → Auto Provision	
Parameter	**DeviceProvisionPollingDayofWeek**	**config.xml**
Description	It configures polling day of week. **Note:** It works only if the value of “DeviceProvisionPollingByWeekdaysEnable” is true.	
Permitted Values	0,1,2,3,4,5,6 or a combination of these digits 0 - Sunday 1 - Monday 2 - Tuesday 3 - Wednesday 4 - Thursday 5 - Friday 6 - Saturday	
Default	0123456	

Web UI	Provision → Auto Provision

4. Firmware Upgrade

There are three methods of firmware upgrade:

- Manually, from the local system for a single phone via web user interface.
- Automatically, from the provisioning server for a batch of phones.
- USB upgrade

4.1 Firmware

You can download the latest firmware online: https://www.aledevice.com/site/download

The M3/M5/M7/M8 DeskPhones share the same firmware. There are two files including in the package. bin9000N is used for bootloader module upgrading. sip9000N is used for SIP module upgrading.

Generally, the two files should be uploaded to the phone at the same time for upgrading.

4.2 Firmware Upgrade Configuration

4.2.1 Firmware Upgrade from Provisioning Server with Configuration File

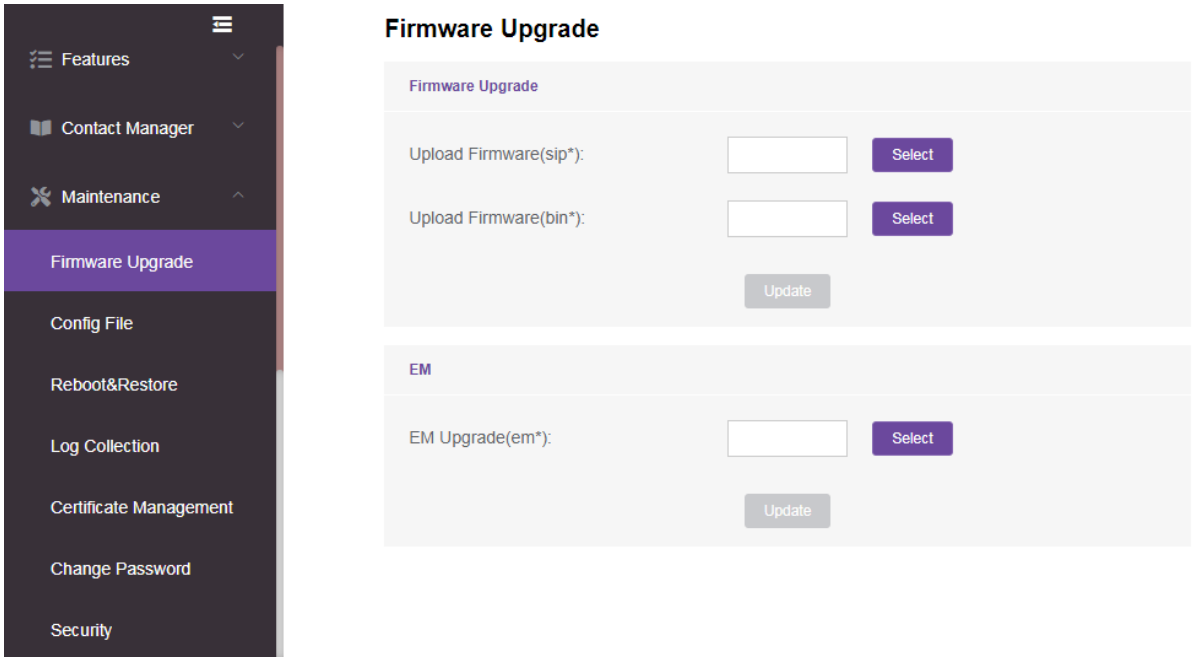
The following table lists the parameter you can use to upgrade firmware.

Parameter	DeviceFirmwareUpgradeUrl	config.xml
Description	It configures the access URL of the firmware file.	
Permitted Values	URL within 511 characters	
Default	Blank	

4.2.2 Firmware Upgrade via Web User Interface

Before upgrading firmware, you need to know the following:

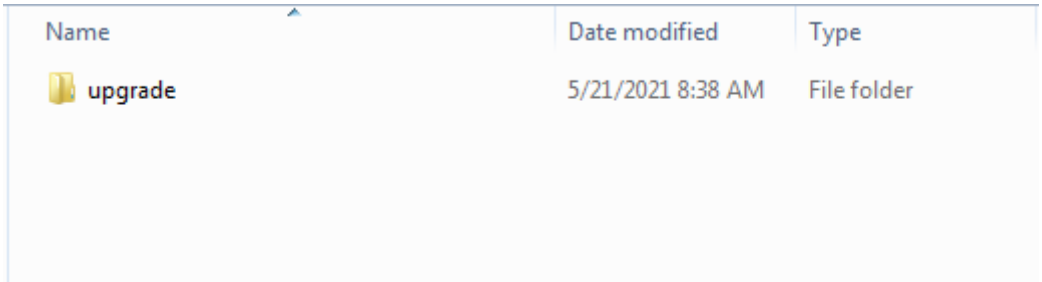
- Do not close and refresh the browser when the IP phone is upgrading firmware.
- Do not unplug the network cables and power cables when the IP phone is upgrading firmware.



4.3 Firmware Upgrade via USB disk

Procedures:

- Step 1: Prepare a USB disk in FAT32 format.
- Step 2: Create a folder and name it “upgrade”.
- Step 3: Put the firmware binary files into upgrade folder.



- Step 4: Plug USB disk into the phone’s USB port when the phone is powered off.
- Step 5: Power on the phone.
- Step 6: During step 1 of initialization process, pressing “4”+”7”+”8”+”*” keys at the same time. Release all keys until all the LEDs are lighting on.
- Step 7: Phone will reboot and start upgrading process.

5. Security Features

This chapter provides information about configuring the security features of the phone.

5.1 User and Administrator Identification

By default, some menu options are protected by different privilege levels: user and administrator. You can also customize the access permission for the web user interface and phone user interface.

The ALE Myriad Series phones support access levels of admin, var and user.

When logging into the web user interface or accessing advanced settings on the phone, as an administrator, you need an administrator password, then you will be able to access various menu options. The default username and password for administrator is “admin/123456”. The default username and password for user is “user/user”. Both “administrator” and “user” can log into the web user interface, and administrator will see all the user options. The default username and password for the user is “user”.

For security reasons, you’d better change the default user or administrator password. Since advanced menu options are strictly used by the administrator, users can configure them only if they have administrator privileges.

5.1.1 User and Administrator Identification Configuration

The following table lists the parameters you can use to configure the user and administrator identification.

Parameter	**DeviceSecurityUserName**	**config.xml**
Description	It configures the user name of the user.	
Permitted Values	String within 32 characters	
Default	user	
Parameter	**DeviceSecurityVarName**	**config.xml**
Description	It configures the user name of the var.	
Permitted Values	String within 32 characters	
Default	var	
Parameter	**DeviceSecurityAdminName**	**config.xml**
Description	It configures the user name of the admin.	
Permitted Values	String within 32 characters	
Default	admin	
Parameter	**DeviceSecurityUserPwd**	**config.xml**
Description	It configures the password of the user	
Permitted Values	String of 3 to 32 characters	
Default	user	
Parameter	**DeviceSecurityVarPwd**	**config.xml**
Description	It configures the password of the var	

Permitted Values	String of 3 to 32 characters	
Default	var	
Parameter	**DeviceSecurityAdminPwd**	**config.xml**
Description	It configures the password of the admin.	
Permitted Values	String of 4 to 32 characters	
Default	Blank	
Web UI	Maintenance → Change Password	
Phone UI	Menu → Advanced Setting (default password: 123456) → Change Password	

5.1.2 User Access Level Configuration

The following table lists the parameters you can use to configure the user access level.

Parameter	**DeviceUserAccessPermissionEnable**	**config.xml**
Description	It enables or disables the 3-level access permissions (admin, var, user).	
Permitted Values	false - disable true - enable	
Default	false	
Parameter	**DeviceUserAccessPermissionUrl**	**config.xml**
Description	It configures the access URL of the file, which defines 3-level access permissions.	
Permitted Values	URL within 512 characters	
Default	Blank	
Parameter	**DeviceDefaultAccessLevel**	**config.xml**
Description	It configures the default access level to access the phone user interface. **Note:** It works only if “DeviceUserAccessPermissionEnable” is set to true (Enabled).	
Permitted Values	0 - user 1 - var 2 - admin	
Default	0	

5.1.3 Access Permissions Specification

Access permissions of all configuration items available on phones’ web user interface and phone user interface can be defined in a fixed UserAccessPermission.xml file.

Each configuration item in the file is formatted as:
ItemName = X1X2

The valid values of X1, X2 include 0, 1, 2 and 3.

X1 is used for specifying the access level. The access levels: 2 = admin, 1 = var, 0 = user, 3 = none.

X2 is used for defining the access permission. 2 means the configuration item is read-only for X1 and higher access levels, the highest is always writable. 1 means the configuration item is read- only for X1 access level

and writable for higher access levels. 0 means the configuration item is writable for X1 and higher access levels. 3 means the configuration item is read-only for X1 and higher access levels.

The following table lists the possible values of X1X2 and the configuration results with different access levels: (W: writable; R: read only; N: hidden)

Value	admin	var	user
0	WR	WR	WR
1	WR	WR	N
2	WR	N	N
3	N	N	N
00	WR	WR	WR
01	WR	WR	R
02	WR	R	R
03	R	R	R
10	WR	WR	N
11	WR	WR	N
12	WR	R	N
13	R	R	N
20	WR	N	N
21	WR	N	N
22	WR	N	N
23	R	N	N
30/31/32/33	N	N	N

Note: The phone user interface currently does not support read-only (R), only writable-read (WR) or hidden (N).

Customizing UserAccessPermission.xml

You can contact you interface person of Alcatel-Lucent Enterprise for the template file

“UserAccessPermission.xml”.

Web User Interface

The following parameters show the configuration for the web user interface in the UserAccessPermission.xml file for reference.

Note: If you change the web user interface permission parameters, the IP phone will reboot to make the changes took effect.

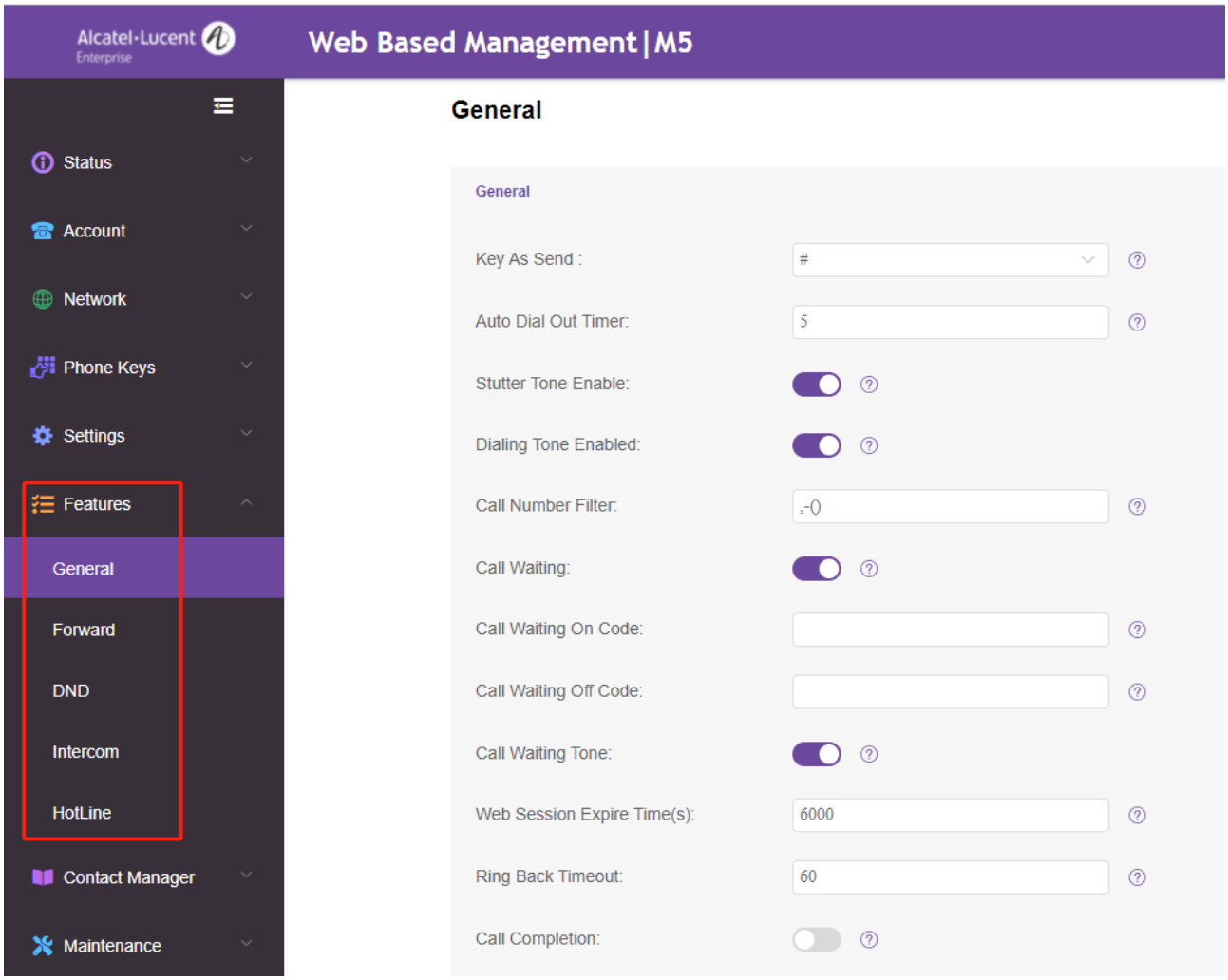
Example: Configuration items in the UserAccessPermission.xml for navigation bar settings of the Features for web user interface:

```
<?xml version="1.0" encoding="UTF-8" ?>
<settings>
        <setting id="WBMFeatureGeneral" value="0" override="true"/>
        <setting id="WBMFeatureForward" value="0" override="true"/>
```

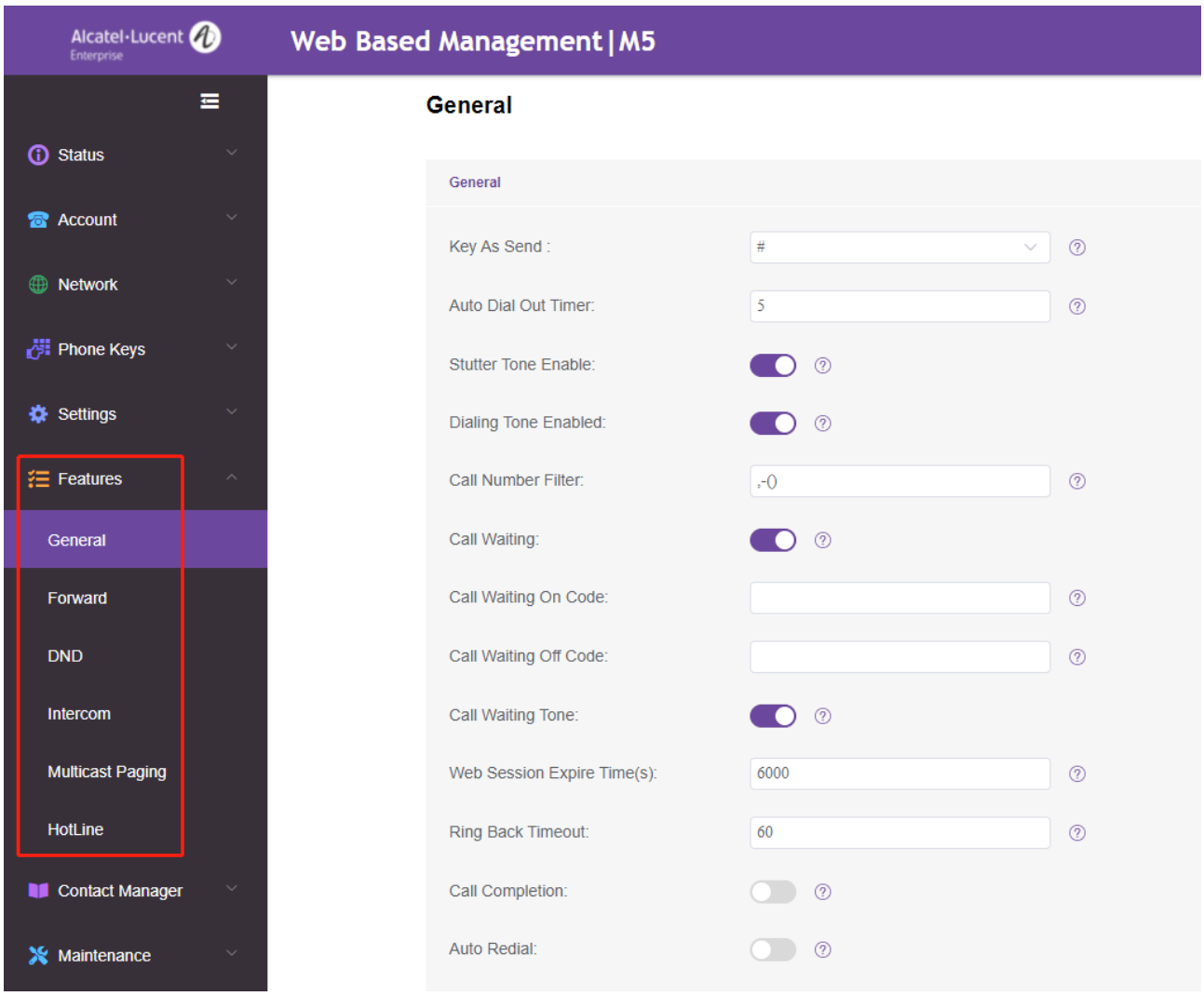
```
        <setting id="WBMFeatureDnd" value="0" override="true"/>
        <setting id="WBMFeatureIntercom" value="0" override="true"/>
        <setting id="WBMFeatureMulticast" value="1" override="true"/>
        <setting id="WBMFeatureHotLine" value="1" override="true"/>
        <setting id="WBMFeatureTransfer" value="1" override="true"/>
        <setting id="WBMFeatureAcd" value="2" override="true"/>
        <setting id="WBMFeatureSip" value="2" override="true"/>
        <setting id="WBMFeatureRemoteControl" value="2" override="true"/>
        <setting id="WBMFeatureActionUrl" value="2" override="true"/>
</settings>
```

Based on the above configuration of access level:

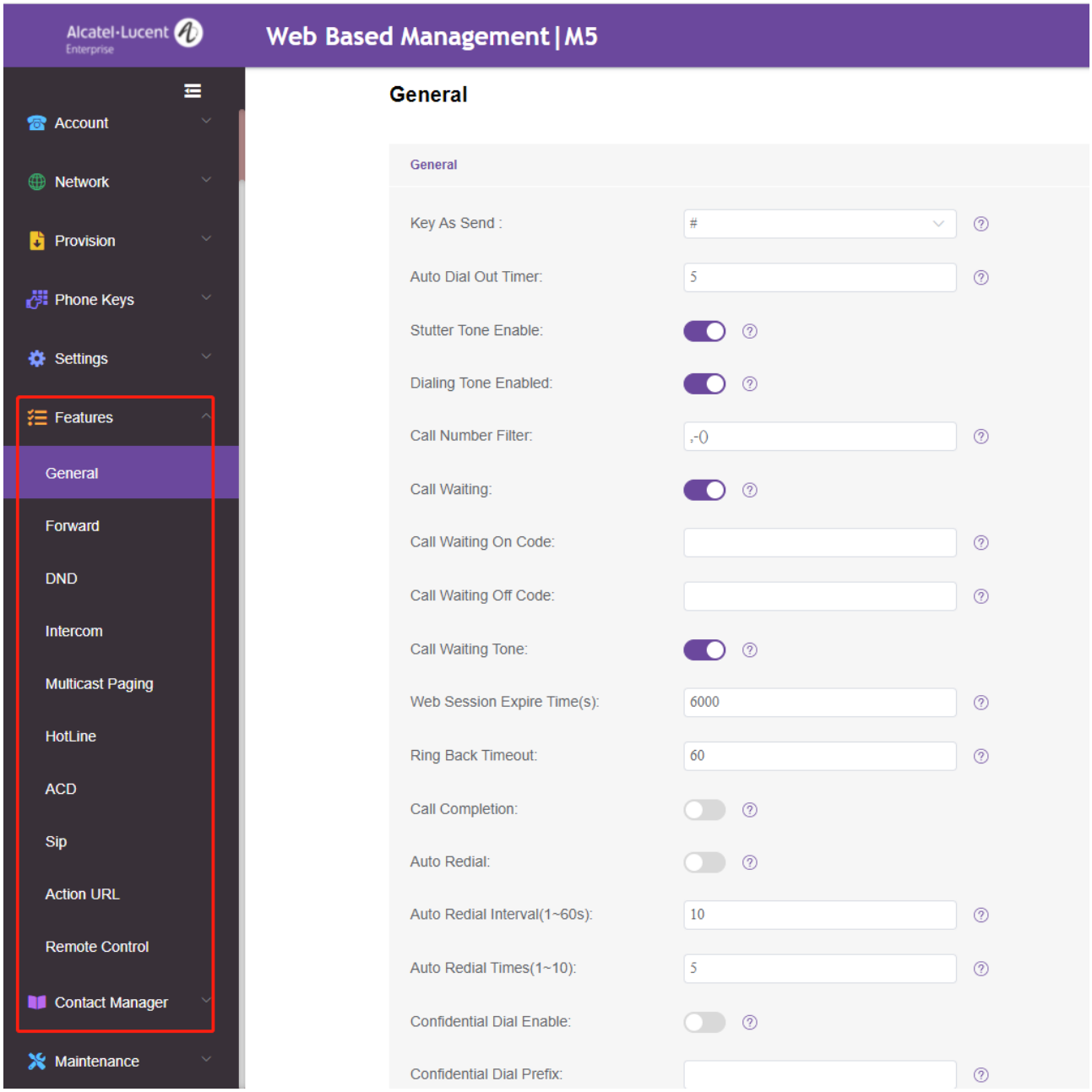
When logging in the web user interface with user access level, the web user interface will be displayed as follows:



When logging in the web user interface with var access level, the web user interface will be displayed as follows:



When logging in the web user interface with admin access level, the web user interface will be displayed as follows:



Phone User Interface

The following shows configuration parameters for the phone user interface in the UserAccessPermission.xml file for reference.

Note: The phone user interface currently does not support read-only (R), only writable-read (WR) or hidden (N).

Example: Configuration items in the UserAccessPermission.xml for call forward menu and its submenu settings for phone user interface:

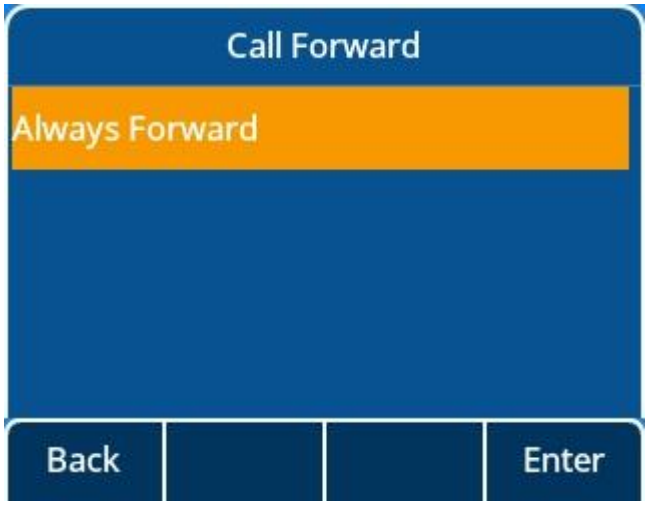
```
<?xml version="1.0" encoding="UTF-8" ?>
<settings>
        <setting id="MMIFeatureForward" value="0" override="true"/>
        <setting id="MMIFeatureAlwaysForward" value="0" override="true"/>
        <setting id="MMIFeatureBusyForward" value="1" override="true"/>
        <setting id="MMIFeatureNoAnswerForward" value="2" override="true"/>
```

</settings>

According to the above configuration of access level:

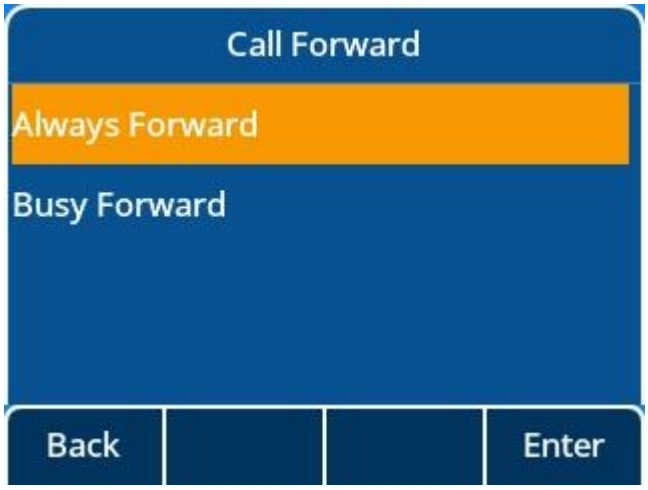
When logging in the phone user interface with user access level, the access permission of each submenu is displayed as follows:

Busy forward submenu and no answer forward submenu are hidden for user access level.



When logging in the phone user interface with var access level, the access permission of each submenu is displayed as follows:

No answer forward submenu is hidden for var access level.



When logging in the phone user interface with admin access level, the access permission of each submenu is displayed as follows:

5.1.4 Logging in the Web/Phone User Interface with Different Access Levels

When the user access level is enabled, you can log in the web/phone user interface with different access levels.

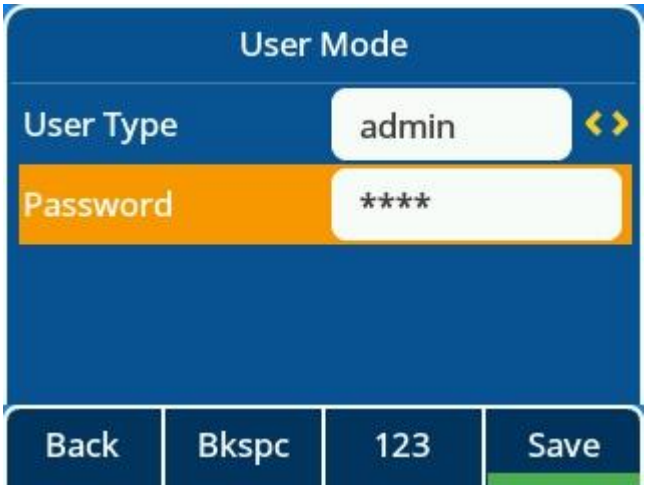
To login in the web user interface with different access levels:

1. Enter the IP address in the address bar of the web browser on your PC and then press the **Enter** key.
2. Enter the user name (admin/var/user) and password (admin/var/user) in the login page.
3. Click **Login** to log in.

When logging in with different access levels, you will have corresponding permissions of the web user interface.

To login in the phone user interface with different access levels:

1. Press Menu → User Mode
2. Press the left or right navigation button, or the **Switch** soft key to select the desired access level in the User Type field.
3. Enter the password in the Password field.

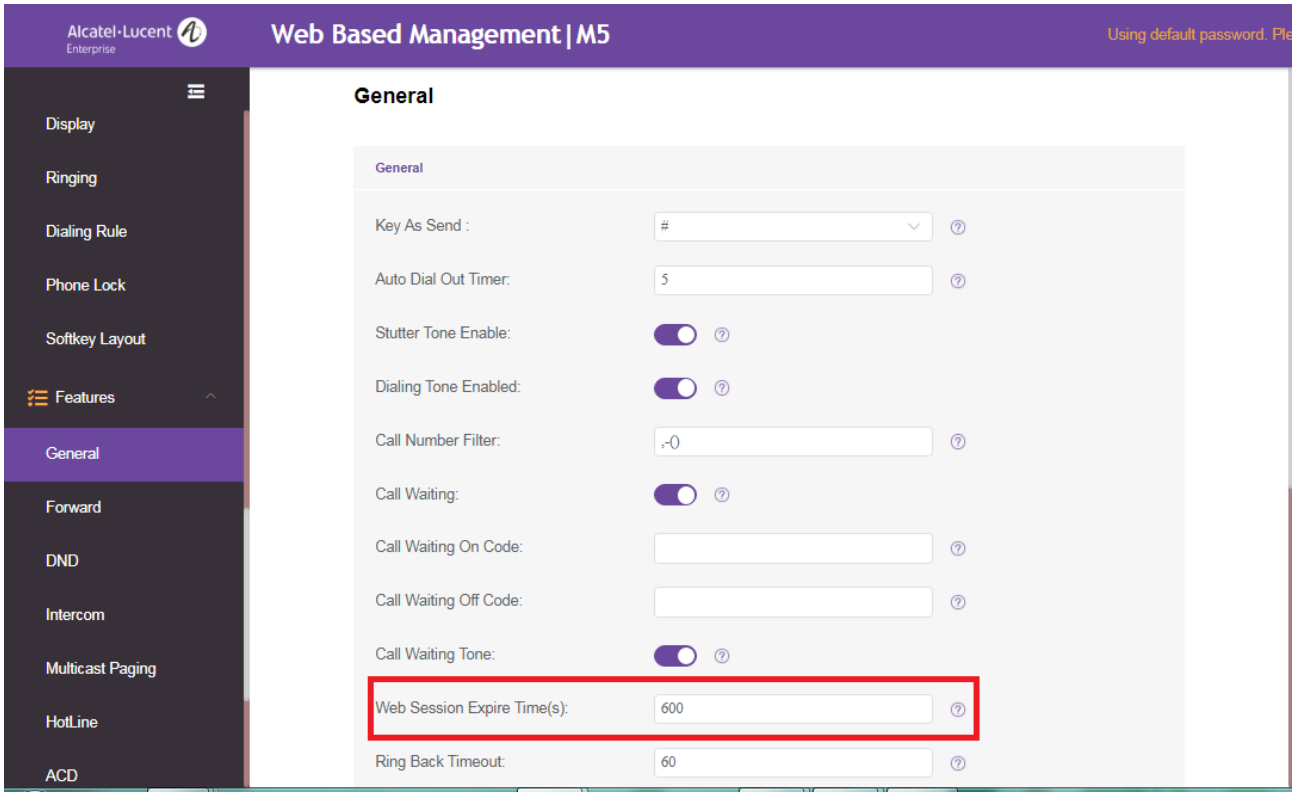


4. Press the Save soft key to accept the change.

You will have corresponding permissions of the phone user interface when logging in with different access levels.

5.2 Auto Logout

Auto logout time (default 5 minutes) defines the time interval of logging out the web user interface automatically when you do not perform any action on web user interface. Once logged out, you must re-enter username and password for web access authentication, and then log in again.



5.3 Phone Lock

You can lock the IP phone to prevent it from unauthorized use. Once the IP phone is locked, you must enter the password to unlock it. The default password is “0000”.

You can set waiting time interval for locking the phone automatically.

Note: Once the phone is locked, the user can input the password “0000” to unlock the phone.

But if the default password is changed and lost, the user can reset the parameter “SettingPhoneUnlockPwd” in the configuration file over auto provisioning.

5.3.1 Operation Behaviors on Locked Phone

When the phone is locked, you can only initiate an emergency call.

The following table lists the parameter you can use to configure the emergency number.

Parameter	**SettingEmergencyNumber**	**config.xml**
Description	It configures the emergency phone numbers when screen is locked.	
Permitted Values	Numeric	
Default	112,911,110	
Web UI	Setting → Phone Lock → Emergency Call	

5.3.2 Phone Lock Configuration

The following table lists the parameters you can use to configure the phone lock.

Parameter	SettingPhoneAutoLockEnable	config.xml
Description	It enables or disables the phone lock feature.	
Permitted Values	false - disable true - enable	
Default	false	
Web UI	Setting → Phone Lock → Automatic Lock	
Phone UI	Menu → Basic Setting → Phone Lock	
Parameter	SettingPhoneAutoLockTimeout	config.xml
Description	It configures screen saver timeout.	
Permitted Values	Numeric [60,18000]	
Default	300	
Web UI	Setting → Phone Lock → Automatic Lock Time	
Phone UI	Basic Setting → Display → Screen Saver → Wait Time	
Parameter	SettingPhoneUnlockPwd	config.xml
Description	It configures screen lock password.	
Permitted Values	Integer	
Default	0000	
Web UI	Setting → Phone Lock → Unlock Password	

5.4 Transport Layer Security (TLS)

TLS is a commonly used protocol for providing communications privacy and managing the message transmission security, allowing IP phones to communicate with other remote parties and connect to the HTTPS URL for provisioning in a way that is designed to prevent eavesdropping and tampering.

The ALE Myriad Series phones support TLS versions 1.0, 1.1 and 1.2. When TLS is enabled for an account, the SIP message of this account will be encrypted.

5.4.1 Supported Cipher Suites

A cipher suite is a named combination of authentication, encryption, and message authentication code (MAC) algorithms used to negotiate the security settings for network connection using the TLS/SSL network protocol.

The ALE Myriad Series phones support the following cipher suites:

- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA
- AES256-SHA
- EDH-RSA-DES-CBC3-SHA
- EDH-DSS-DES-CBC3-SHA
- DES-CBC3-SHA
- DES-CBC3-MD5
- DHE-RSA-AES128-SHA
- DHE-DSS-AES128-SHA

- AES128-SHA
- RC2-CBC-MD5
- IDEA-CBC-SHA
- DHE-DSS-RC4-SHA
- RC4-SHA
- RC4-MD5
- RC4-64-MD5
- EXP1024-DHE-DSS-DES-CBC-SHA
- EXP1024-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-DSS-DES-CBC-SHA
- DES-CBC-SHA
- DES-CBC-MD5
- EXP1024-DHE-DSS-RC4-SHA
- EXP1024-RC4-SHA
- EXP1024-RC4-MD5
- EXP-EDH-RSA-DES-CBC-SHA
- EXP-EDH-DSS-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP-RC2-CBC-MD5
- EXP-RC4-MD5
- ECDHE

5.4.2 Supported Trusted and Server Certificates

The IP phone can serve as a TLS client or a TLS server. The phone supports the dual-authentication method. These are also known as CA and device certificates.

The TLS requires the following security certificates to perform the TLS handshake:

- Trusted Certificate: When the IP phone requests a TLS connection with a server, the IP phone should verify the certificate sent by the server to decide whether it is trusted based on the trusted certificates list. The IP phone has 58 built-in trusted certificates. You can upload 10 custom certificates at most. The format of the trusted certificate files must be *.pem,*.cer,*.crt and *.der and the maximum file size is 5MB.
- Server Certificate: When clients request a TLS connection with the IP phone, the IP phone sends the server certificate to the clients for authentication. The IP phone has two types of built-in server certificates: a unique server certificate and a custom server certificate. You can only upload one server certificate to the IP phone. The old server certificate will be overridden by the new one. The format of the server certificate files must be *.p12 and *.pfx and the maximum file size is 5MB.
- A unique server certificate: It is unique to an IP phone (based on the MAC address) and issued by the ALE Certificate Authority (CA).
- A custom server certificate: Users can upload the custom certificate for authentication.

The IP phone can authenticate the server certificate based on the trusted certificates list. The trusted certificates list and the server certificates list contain the default and custom certificates.

Common Name Validation feature enables the IP phone to mandatorily validate the common name of the certificate sent by the connecting server. The Security verification rules are compliant with RFC 2818.

The ALE Myriad Series phones trust the following CAs by default:

- entrust_g2_ca.pem
- CybertrustPublicSureServerSVCA.pem
- SFSRootCAG2.pem

- GeoTrust_Primary_CA_G2_ECC.pem
- AddTrustExternalCARoot.pem
- comodosslca.pem
- DigiCertHighAssuranceEVRootCA.pem
- GeoTrust_Global_CA.pem
- thawte_Primary_Root_CA.pem
- DSTRootCAX3.pem
- DigiCert_Global_Root_CA.pem
- letsencryptauthorityx2.pem
- isrgrootx1.pem
- SVRSecureG3.pem
- GeoTrust_Primary_CA.pem
- Root_R2.pem
- sfroot_g2.pem
- TCTrustCenterClass3CAII.pem
- Root_R1.pem
- TCTrustCenterClass4CAII.pem
- DigiCertGlobalRootG2.pem
- Thawte_Personal_Freemail_CA.pem
- BaltimoreCyberTrustRoot.pem
- entrust_ev_ca.pem
- Thawte_Server_CA.pem
- AmazonRootCA2.pem
- DigiCertTrustedRootG4.pem
- VeriSign_Class_3_Public_Primary_Certification_Authority_G4.pem
- DigiCertAssuredIDRootG3.pem
- DigiCert_SHA2_Secure_Server_CA.pem
- StartComCertificationAuthorityG2.pem
- GeoTrust_Universal_CA2.pem
- AmazonRootCA3.pem
- comodorsadomainvalidationsecureserverca.pem
- Thawte_Premium_Server_CA.pem
- DigiCertAssuredIDRootG2.pem
- TCTrustCenterClass2CAII.pem
- GeoTrust_Universal_CA.pem
- StartComCertificationAuthority.pem
- entrust_2048_ca.pem
- DigiCertAssuredIDRootCA.pem
- VeriSign_Class_3_Public_Primary_Certification_Authority_G5.pem
- letsencryptauthorityx1.pem
- thawte_Primary_Root_CA_G3_SHA256.pem
- VeriSign_Class_4_Public_Primary_Certification_Authority_G3.pem
- VeriSign_Universal_Root_Certification_Authority.pem
- thawte_Primary_Root_CA_G2_ECC.pem
- VeriSign_Class_3_Public_Primary_Certification_Authority_G3.pem
- TCTrustCenterUniversalCAI.pem
- AmazonRootCA1.pem
- comodorsacertificationauthority.pem
- VeriSign_Class_2_Public_Primary_Certification_Authority_G3.pem
- DigiCertGlobalRootG3.pem

- AmazonRootCA4.pem
- Geotrust_PCA_G3_Root.pem
- VerizonPublicSureServerCAG14_SHA2.pem
- VeriSign_Class_1_Public_Primary_Certification_Authority_G3.pem
- EquifaxSecureGlobaleBusinessCA1.pem

Note: ALE endeavors to maintain a built-in list of the most commonly used CA Certificates. If you are using a certificate from a commercial Certificate Authority, which is not in the list above, you can send a request to ALE technical support team, and ALE will evaluate if this certificate could be added into later firmware release. At this point, you can also upload your specific CA certificate into your phone.

5.4.3 TLS Configuration

The following table lists the parameters you can use to configure TLS.

Parameter	**AccountXServer1Transport**	**config.xml**
Description	It configures the type of transport protocol.	
Permitted Values	0 - UDP 1 - TCP 2 - TLS 3 - DNS-NAPTR. If no server port is given, the IP phone performs the DNS NAPTR and SRV queries for the service type and port.	
Default	0	
Web UI	Account → Basic → Transport Mode	
Parameter	**SIPTlsVersion**	**config.xml**
Description	It configures the TLS version the IP phone uses to authenticate with the server.	
Permitted Values	0 - All 1 - TLS1.0 2 - TLS1.2	
Default	0	
Parameter	**SIPTlsPeerVerify**	**config.xml**
Description	It enables or disables the peer verify for sip server.	
Permitted Values	false - disable true - enable	
Default	false	
Web UI	SIP Features → General → SIPs Peer Verify	
Parameter	**SIPCertificateUrl**	**config.xml**
Description	It configures the URL to download SIP server certificate.	
Default	Blank	
Web UI	Maintenance → Certificate Management → Upload Customer Certificate	

5.5 Secure Real-Time Transport Protocol (SRTP)

Secure Real-Time Transport Protocol (SRTP) encrypts the audio streams during VoIP phone calls to avoid interception and eavesdropping. The parties participating in the call must enable SRTP feature

simultaneously. When this feature is enabled on both phones, the type of encryption to use for the session is negotiated between the IP phones. This negotiation process is compliant with RFC 4568.

When you place a call on the enabled SRTP phone, the IP phone sends an INVITE message with the RTP/RTCP encryption algorithm to the destination phone. As described in RFC 3711, RTP/RTCP streams may be encrypted using an AES (Advanced Encryption Standard) algorithm.

Example of the RTP encryption algorithm carried in the SDP of the INVITE message:

```
m=audio 6000 RTP/SAVP 0 8 18 9 101
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:NzFlNTUwZDk2OGVlOTc3YzNkYTkwZWVkMTM1YWFj
a=crypto:2 AES_CM_128_HMAC_SHA1_32
inline:NzkyM2FjNzQ2ZDgxYjg0MzQwMGVmMGUxMzdmNWFm
a=crypto:3 F8_128_HMAC_SHA1_80 inline:NDliMWIzZGE1ZTAwZjA5ZGFhNjQ5YmEANTMzYzA0
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:9 G722/8000
a=fmtp:101 0-15
a=rtpmap:101 telephone-event/8000
a=ptime:20
a=sendrecv
```

The callee receives the INVITE message with the RTP encryption algorithm, and then answers the call by responding with a 200 OK message which carries the negotiated RTP encryption algorithm.

Example of the RTP encryption algorithm carried in the SDP of the 200 OK message:

```
m=audio 6000 RTP/SAVP 0 101
a=rtpmap: 0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:NGY4OGViMDYzZjQzYTNiOTNkOWRiYzRlMjM0Yzcz
a=sendrecv
a=ptime:20
a=fmtp:101 0-15
```

When SIP-TLS/SRTP is enabled on both IP phones, RTP streams will be encrypted, and a lock icon appears on the LCD screen of each IP phone after successful negotiation.

The following table lists the parameters you can use to configure the SRTP.

Parameter	**SIPGroup1SrtpWorkingMode**	**config.xml**
Description	It configures whether to use voice encryption service.	
Permitted Values	0 - None 1 - Best effort 2 - Strict 3 - 0SRTP	
Default	0	

Web UI	Account → Advanced → SRTP Working Mode

5.6 SSH Activation

It is possible to open a secure remote connection through SSH to access the phone for Further operation test and debug purposes. SSH Connection is disable by default.

The following table lists the parameters you can use to configure the SSH session.

Parameter	**DeviceSecuritySshEnable**	**config.xml**
Description	It enables or disable the SSH session.	
Permitted Values	false - disable true - enable	
Default	false	
Web UI	Maintenance → Security → SSH Activation	

5.7 HTTPS Peer Verification

When the phone downloads the common configuration file from the provisioning server, the IP phone can enable or disable the authentication of the server certificate based on the trusted certificates list.

The following table lists the parameters you can use to configure the HTTPS peer verification.

Parameter	**DeviceSecurityHttpsPeerVerifyEnable**	**config.xml**
Description	It enables or disable HTTPS peer verification.	
Permitted Values	0 - NO 1 - YES	
Default	1	
Web UI	Maintenance → Certificate Management → HTTPS Peer Verify	

5.8 Encrypting and Decrypting Files

Myriad IP phones support downloading encrypted config.xml/config.xml file(s) from http/https server. To encrypt/decrypt files, you may have to configure an AES key.

The following table lists the parameters you can use to configure the encryption and decryption.

Parameter	**DeviceSecurityEncryptionAesKey**	**config.xml**
Description	It configures the plaintext AES key for encrypting/decrypting the config/config.xml file.	
Permitted Values	string	
Default	Blank	
Phone UI	Menu → Advanced Setting (default password: 123456) → Auto Provision → AES Key	

6. Directory

The ALE Myriad Series phones provide several types of phone directories.

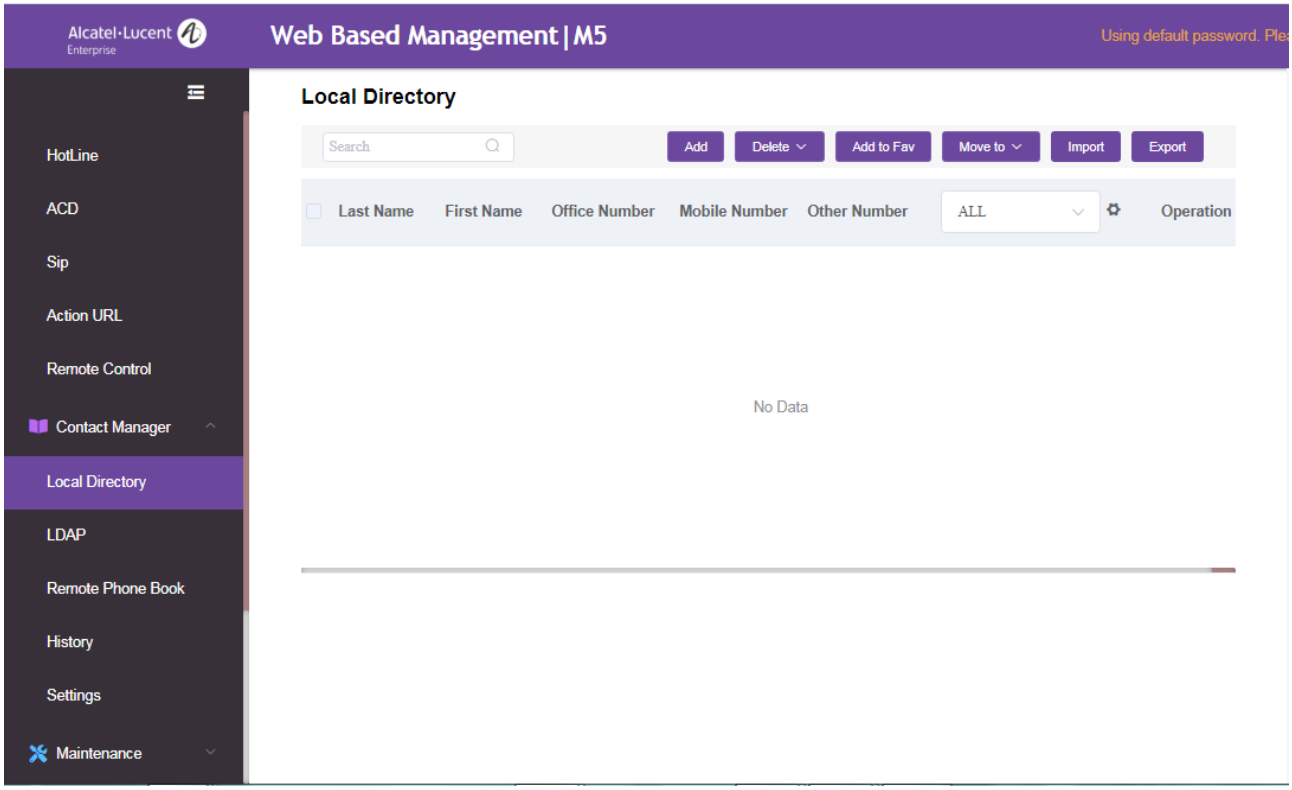
6.1 Local Directory

The ALE Myriad Series phones maintain a local directory that you can use to store contacts. The local directory can store up to 1000 contacts and 50 groups.

Contacts and groups can be added manually or imported in batch with a contact file. The ALE Myriad Series phones support *.xml format contact files.

6.1.1 Local Contact File Customization

You can download local contact template from the phone Web UI.



6.1.1.1 Local Contact File Elements and Attributes

The following table lists the elements and attributes you can use to add groups or contacts in the local contact file. We recommend you do not edit these elements and attributes.

Elements	Attributes	Description
Group	display_name	Specify the group name. For example: All Contacts, Blacklist or Friend
Contact	display_name	Specify the office number
	mobile_number	Specify the mobile number
	other_number	Specify the other number
	line	Specify a registered line for this contact for calling. Valid Values: 1~15/1~8; The ALE Myriad Series phones support 8 accounts.

	group_id_name	Specify which group the contact adds to. Built-in group: All Contacts, External Directory (supported by only M7) Custom group: XXX (for example, Friend)
	default_photo	Built-in avatar: Resource: avatar name

6.1.1.2 Customizing Local Contact File

Procedures:

1. Download a contact template from Web UI.
2. Open the contact template.
3. Add a group by adding <GroupName>Fn</GroupName> to the configuration file. Each starts on a new line.

For example:

```
<Contact>
        <FirstName>Thierry </FirstName>
        <LastName>Agbo</LastName>
        <Account>1</Account>
        <GroupName>All Contacts</GroupName>
        <AvatarSmall>avatar_small_default</AvatarSmall>
        <AvatarBig>avatar_large_default</AvatarBig>
        <OfficeNumber>8566</OfficeNumber>
        <MobileNumber></MobileNumber>
        <OtherNumber></OtherNumber>
        <HomeNumber></HomeNumber>
        <Favorite>False</Favorite>
    </Contact>
<Groups>
    <Group>
      <GroupName>Manager</GroupName>
    </Group>
  </Groups>
```

4. Save the changes and upload this file to the phone Web UI or place this file to the provisioning server.

6.1.2 Local Contact File Upload

On the ALE Myriad Series phones, you can upload multiple contacts by a contact file at the same time.

The following table lists the parameters you can use to upload the local contact files and resource.

Parameter	LocalContactUploadUrl	config.xml

Description	It configures the access URL of the local contact file (*.xml).
Permitted Values	URL within 511 characters
Default	Blank

6.1.3 Add Contacts Using a Contact File

The following example shows the configuration for customizing a local contact file.

Customize the contact file “contact.xml” and place the contact file “contact.xml” to the provisioning server http://192.168.10.25 .

Example:

<setting id="LocalContactUploadUrl" value="http://192.168.10.25/directory.xml" override="true"/>

During auto provisioning, the IP phone connects to the provisioning server “192.168.10.25” and downloads the local contact file “directory.xml”. You can view the contacts on the phone and specify the avatar for a contact.

The following images show the added contact Lily wang with the corresponding avatar displayed on the phone screen:

6.2 Lightweight Directory Access Protocol (LDAP)

LDAP is an application protocol for accessing and maintaining information services for the distributed directory over an IP network. You can configure the IP phones to interface with a corporate directory server that supports LDAP version 2 or 3. The following LDAP servers are supported:

- Microsoft Active Directory
- Sun ONE Directory Server
- Open LDAP Directory Server
- Microsoft Active Directory Application Mode (ADAM)

6.2.1 LDAP Attributes

The following table lists the most common attributes used to configure the LDAP lookup on IP phones.

Abbreviation	Name	Description
gn	givenName	First name
cn	commonName	LDAP attribute is made up from given name joined to surname.
sn	surname	Last name or family name
dn	distinguishedName	Unique identifier for each entry
dc	dc	Domain component
-	company	Office phone number
-	telephoneNumber	Company or organization name
mobile	mobilephoneNumber	Mobile or cellular phone number

ipPhone	IPphoneNumber	Home phone number

6.2.2 LDAP Configuration

The following table lists the parameters you can use to configure LDAP.

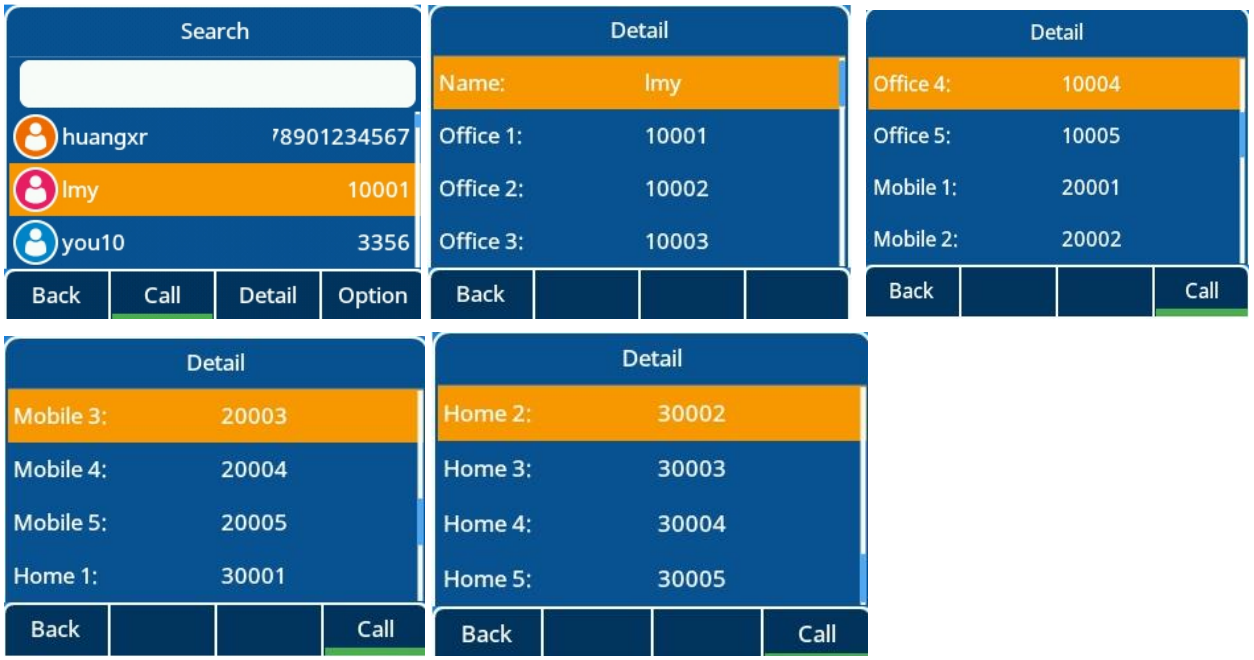
Parameter	**LdapEnable**	**config.xml**
Description	It enables or disables the LDAP feature on the IP phone.	
Permitted Values	false - disable true - enable	
Default	false	
Web UI	Contact Manager → LDAP → LDAP Enable	
Parameter	**LdapServerUrl**	**config.xml**
Description	It configures the LDAP Server URL.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Contact Manager → LDAP → LDAP Server URL	
Parameter	**LdapSearchBase**	**config.xml**
Description	It configures the LDAP base DN used for searching.	
Permitted Values	String within 99 characters	
Default	o=Alcatel,o=directoryRoot	
Web UI	Contact Manager → LDAP → LDAP Search Base	
Parameter	**LdapFieldsMapping**	**config.xml**
Description	It configures LDAP Fields Mapping.	
Default	{"firstname":"givenname", "name":"sn", "officephone":"telephonenumber"}	
Permitted Values	String within 99 characters	
Web UI	Contact Manager → LDAP → LDAP Fields Mapping	
Parameter	**LdapFilter**	**config.xml**
Description	It configures LDAP searching rules.	
Permitted Values	String within 99 characters	
Default	(|(givenName=*%1*)(sn=*%1*))	
Web UI	Contact Manager → LDAP → LDAP Filter	
Parameter	**LdapUserName**	**config.xml**

Description	This login is used in conjunction with the password, if the LDAP server requires authentication.	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	Contact Manager → LDAP → LDAP User Name	
Parameter	**LdapPassword**	**config.xml**
Description	This password is used in conjunction with the LDAP login, if the LDAP server requires authentication.	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	Contact Manager → LDAP → LDAP Password	
Parameter	**LdapSearchTimeout**	**config.xml**
Description	It configures the LDAP search timeout.	
Permitted Values	NUMERIC[1,30]	
Default	5	
Web UI	Contact Manager → LDAP → LDAP Search Timeout(1-30s)	
Parameter	**LdapConnectionTimeout**	**config.xml**
Description	It configures the LDAP connection timeout.	
Permitted Values	NUMERIC[1,30]	
Default	3	
Web UI	Contact Manager → LDAP → LDAP Connection Timeout(1-30s)	
Parameter	**LdapMaxHits**	**config.xml**
Description	It configures the maximum matched number of LDAP query.	
Permitted Values	NUMERIC [1,1000]	
Default	50	
Web UI	Contact Manager → LDAP → LDAP Max Hits(1-1000)	
Parameter	**LdapCallQueryEnable**	**config.xml**
Description	It enables or disables LDAP query during call.	
Permitted Values	false - disable true - enable	
Default	false	
Web UI	Contact Manager → LDAP → LDAP Call Query Enable	

6.2.3 LDAP Number

LDAP feature has been optimized and the optimization is aimed at adding softkeys “Detail” and “Option” in phone MMI and displaying up to 15 numbers for each contact on the server. There are three types of number attributes for each contact, i.e. Office number, Mobile number and Home number. For each attribute, MMI can display up to 5 numbers.

The image below shows the display of a LDAP number which has multiple numbers for each attribute.



When adding a contact from LDAP to Local contacts, Blacklists or Favorites, the number can be added to office, mobile or other options. Press Switch or Left/Right key on the “Add to xxx” page to select numbers.

6.3 External Directory

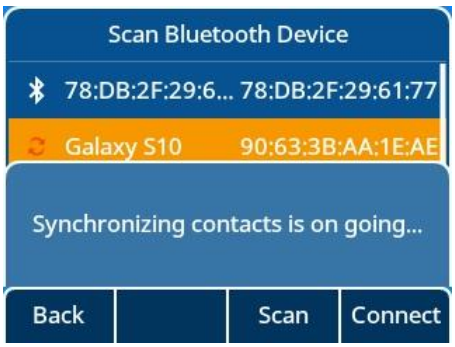
After a cellphone is paired with a desktop phone via Bluetooth, for the M7 phone, the contacts in cellphone will be synchronized to desktop phone automatically. For the M8 phone, users could choose synchronizing of contacts or not. In addition, manual synchronizing of contacts is also supported after a cellphone has been paired. After synchronizing contacts automatically or manually, all the contacts from the cellphone are grouped into a special group named “External Directory”.

This feature is supported by the M7/M8 phones.

During pairing with cellphone process, the M7 phone screens will be displayed as follows:

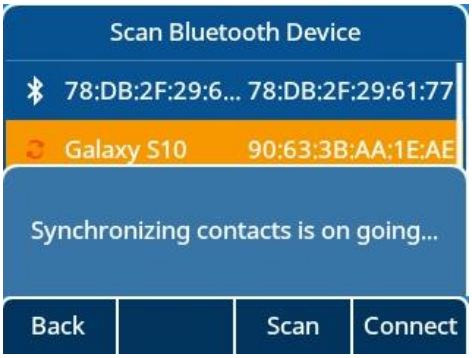
1. When the deskphone is pairing a cellphone, the cellphone will prompt you whether to enable contact synchronization rights. If agreed, the desktop phone will synchronize contacts automatically. If not, the phone won’t synchronize contacts after being paired.

   - Synchronizing automatically



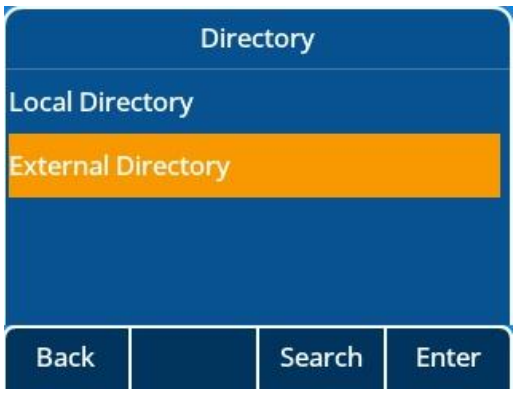
- Synchronizing manually

2. Synchronizing is ongoing.

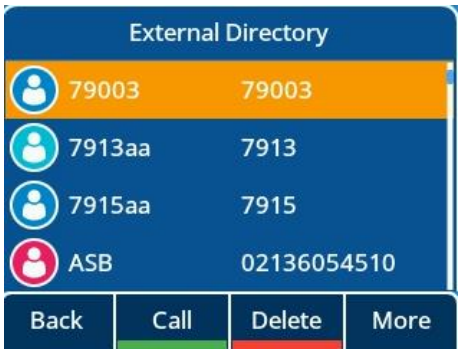


3. Synchronizing is done.

4. Special directory group “External Directory” for cellphone.



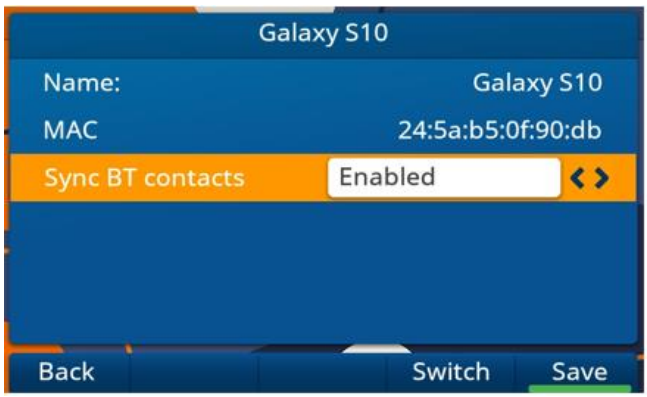
5. Contacts display in group “External Directory”.



During pairing with cellphone process, the M8 phone could accept or reject synchronizing of contacts.

For M8, after pairing process, user can go into the below phone UI to enable or disable synchronizing BT contacts, select the paired cellphone, press detail, and then enable/disable sync BT contacts.

Menu → Basic Setting → Bluetooth → Paired Bluetooth Device



6.4 Directory Search Settings

The feature is implemented as follows:

- If the first character is digit, the IP phone will search whether phoneNumber1/phoneNumber2/phoneNumber3/firstName/lastName contain/start with the entered character(s).
- If the first character is not digit, the IP phone will search whether firstName/lastName contain/start with the entered character(s).

The following table lists the parameters you can use to configure directory search settings.

Parameter	**SettingDirectorySearchType**	**config.xml**
Description	It configures the search type when searching the contact in Local Directory or Remote Phone Book.	
Permitted Values	0 - contains 1 - startwith	
Default	0	

6.5 Remote Phone Book

The remote phone book is a centrally maintained phone book, stored on the remote server. Users only need to configure the access URL of the remote phone book. The IP phone can establish a connection with the remote server and download the phone book, and then display the remote phone book entries on the phone. The ALE Myriad Series IP phones support up to 6 remote phone book groups.

The following table lists the parameters you can use to configure remote phone book.

Parameter	**RemotePhoneBookEnable**	**config.xml**
Description	It configures whether to enable or disable the remote phone book feature.	
Permitted Values	false - disable true - enable	
Default	false	
Web UI	Contact Manager → Remote Phone Book → RemotePB Enable	
Parameter	**RemotePhoneBookForceUpdateMode**	**config.xml**
Description	It configures whether to enable or disable the forced update mode.	
Permitted Values	0 - disable the forced update mode 1 - enable the forced update mode	
Default	0	
Parameter	**RemotePhoneBookPeriodUpdateEnable**	**config.xml**
Description	It configures whether to enable or disable the periodic update mode.	
Permitted Values	false - disable true - enable	
Default	false	
Web UI	Contact Manager → Remote Phone Book → Periodically Update Enable	

Parameter	**RemotePhoneBookInterval**	**config.xml**
Description	It configures the update interval.	
Permitted Values	Numeric [60 – 3600]	
Default	3600	
Web UI	Contact Manager → Remote Phone Book → Periodically Update Interval (Seconds)	
Parameter	**RemotePhoneBookXGroupName**	**config.xml**
Description	It configures the name of the specific group remote phone book. If set, it is displayed on MMI. X can be 1~6.	
Permitted Values	Strings	
Default	Blank	
Phone UI	Directory → Remote Directory	
Web UI	Contact Manager → Remote Phone Book → Display Name	
Parameter	**RemotePhoneBookXUrl**	**config.xml**
Description	It configures the download address of the specific group of remote phone book. X can be 1~6.	
Permitted Values	Strings	
Default	Blank	
Web UI	Contact Manager → Remote Phone Book → Remote Phone Book URL	
Parameter	**RemotePhoneBookXAuthName**	**config.xml**
Description	It configures the authenticated account of remote phone book. X can be 1~6.	
Permitted Values	Strings	
Default	Blank	
Parameter	**RemotePhoneBookXAuthPwd**	**config.xml**
Description	It configures the authentication password of remote phone book. X can be 1~6.	
Permitted Values	Strings	
Default	Blank	

6.6 Contact Backup

The IP phone will automatically upload contact file at regular intervals to the provisioning server or a specific server. If the contact file exists on the server, it will be overwritten. The IP phone will request to download the contact.<MAC>.file according to its MAC address from the server during auto provisioning.

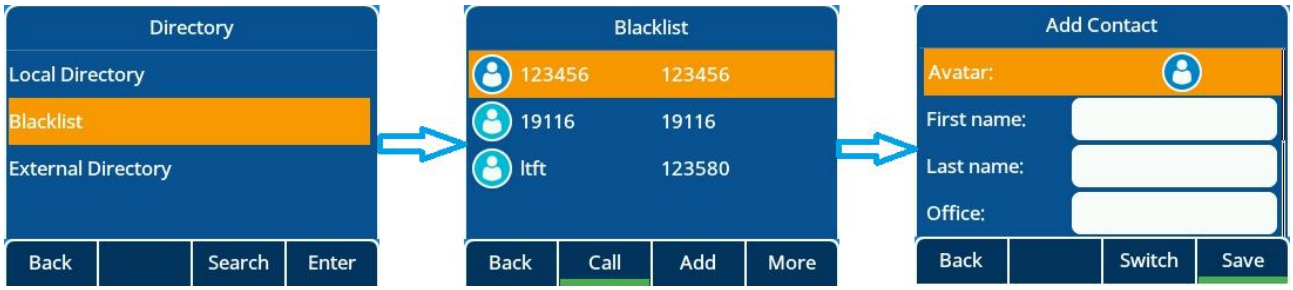
The following table lists the parameters you can use to back up the local contacts.

Parameter	DeviceBackupUploadTime	config.xml
Description	It configures the interval time between uploading a backup file.	
Permitted Values	Numeric [60 - 3600]	
Default	3600	
Parameter	DeviceBackupUrl	config.xml
Description	It configures the URL which is used to upload and download the backup file.	
Permitted Values	Strings	
Default	Blank	
Parameter	DeviceBackupUploadMethod	config.xml
Description	It configures the way to upload files (post/put).	
Permitted Values	0 - put 1 - post	
Default	0	
Parameter	DeviceContactBackupEnable	config.xml
Description	It configures whether to enable or disable contactBackup.	
Permitted Values	false - disable true - enable	
Default	false	

6.7 Blacklist

When the user never wants to receive calls from somebody, the phone number can be added into the blacklist of directory. Then all calls from this phone number which is included in the blacklist will be refused automatically.

On the phone, go to the directory via path: Menu → Directory → Blacklist, and then press “Add” key to add one contact in Blacklist.



6.8 Directory List for Directory/Dir Soft Key

Users can access frequently used directory lists by pressing the Directory/Dir soft key when the IP phone is idle. The lists include Local Directory by default.

You can add the desired lists to directory list using a config file (config.xml) or the Web UI.

The following table lists the parameters you can use to configure directory list.

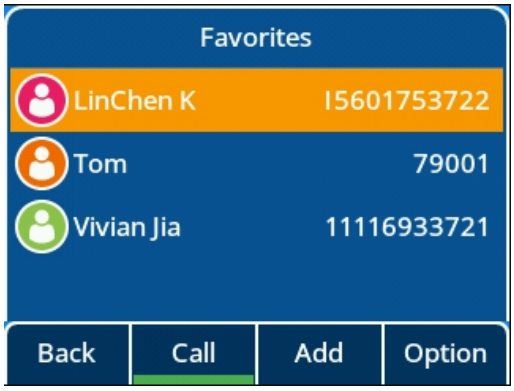
Parameter	DirectoryList	config.xml
Description	It configures directory list display contents by pressing the Directory/Dir softkey. If RemotePhoneBookEnable is false, Remote Phone Book will not be displayed. If LdapEnable is false, LDAP will not be displayed. If SettingBluetoothEnable is false, External Directory will not be displayed. Example: DirectoryList = 0;1;2, RemotePhoneBookEnable = true, LdapEnable = true. Local Directory, Remote Phone Book and LDAP will be displayed when pressing the Directory/Dir soft key.	
Permitted Values	0 - Local Directory 1 - Remote Phone Book 2 - LDAP 3 - Blacklist 4 - Favorites 5 - External Directory 6 - Network Contacts	
Default	0	
Web UI	Contact Manager → Settings → Directory List	

6.9 Favorite Contacts

User can mark local contacts as favorite contacts when this feature enabled. The favorite contacts will be stored in the Favorites directory and the phone will automatically assign Speed Dial keys for these favorite contacts.

The following images show three favorite contacts:

In the Favorites directory:



On the idle screen:

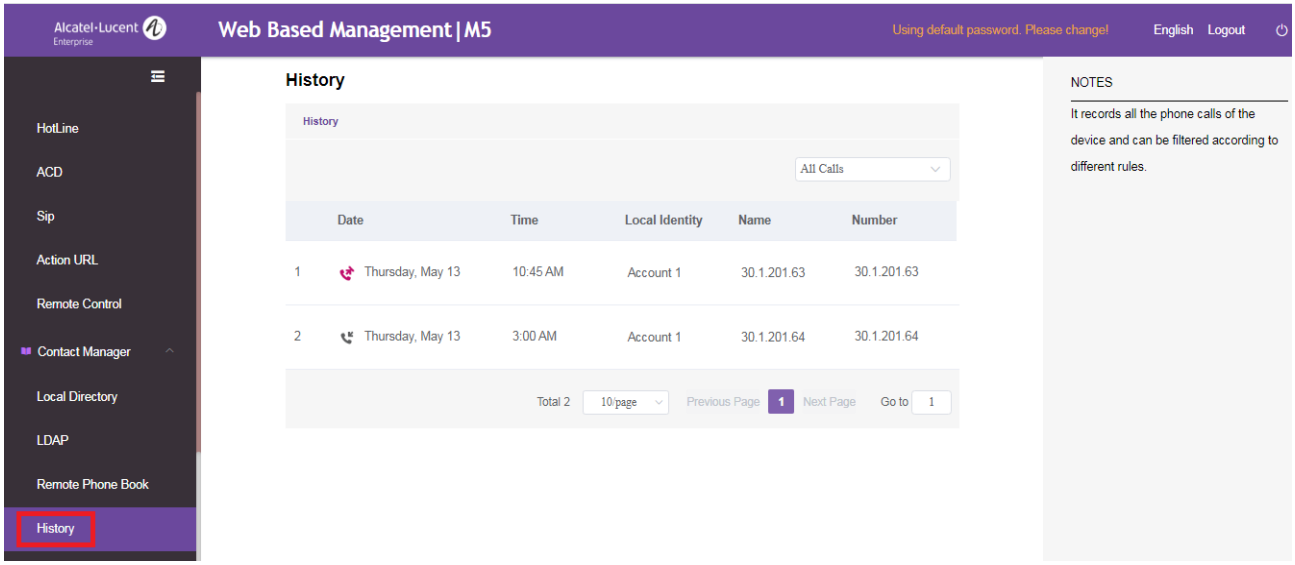
6.9.1 Favorites Configuration

The following table lists the parameters you can use to configure the favorites.

Parameter	DirectoryFavoriteMode	config.xml
Description	It enables or disables generating speed dial key for favorite contact automatically.	
Permitted Values	0 - Not generate speed dial key for favorite contact automatically 1 - Generate speed dial key for favorite contact automatically	
Default	0	

6.10 History List Display in Web UI

On the Web UI the user can check the call history of the phone via path: Contact Manager→History.



7. Audio Features

This chapter describes the audio sound quality features and options you can configure for the IP phone.

7.1 Dial Tone

You can configure whether to enable or disable the dialing tone.

7.1.1 Dialing Tone Configuration

The following table lists the parameters you can use to enable or disable the dialing tone.

Parameter	**FeatureDialingToneEnable**	**config.xml**
Description	It enables or disables the dialing tone.	
Permitted Values	false - disable true - enable	
Default	true	
Web UI	Features → General → Dialing Tone Enable	

7.2 Stutter Tone

The phone can play a specific dial tone when it has new/unreaded voice messages received.

Parameter	**SettingStutterEnable**	**config.xml**
Description	It enables or disables the stutter tone.	
Permitted Values	false - disable true - enable	
Default	true	
Web UI	Features → General → Stutter Tone Enable	

7.3 Ring Tones

Ring tones are used to play for internal/external incoming calls. You can select a built-in ring tone for the phone system or specific account registration. To set the custom ring tones, you need to upload the custom ring tones to the IP phone in advance.

You can also specify a period of time after which the IP phone will stop ringing if the call is not answered.

7.3.1 Custom Ringtone Limit

Phone Model	Format	Single File Size	Note
M3/M5/M7	Wav, zip	Wav file 200kb, zip file 1.2M	

7.3.2 Ringtone Configuration

The following table lists the parameters you can use to configure ringtone.

Parameter	**SettingRingInternal**	**config.xml**
Description	It configures internal call ring melody.	
Permitted Values	String (within 511 Characters)	

Default	Cold River	
Web UI	Setting → Ringing → Internal Melody	
Phone UI	Basic Setting → Sound → Ringing → Int Melody	
Parameter	**SettingRingExternal**	**config.xml**
Description	It configures external call ring melody.	
Permitted Values	String (within 511 Characters)	
Default	Cold River	
Web UI	Setting → Ringing → External Melody	
Phone UI	Basic Setting → Sound → Ringing → Ext Melody	
Parameter	**SettingRingProgressive**	**config.xml**
Description	It configures ring progressive (only 0, 2 supported).	
Permitted Values	0 - NoProgressive 1 - NormalProgressive	
Default	0	
Web UI	Setting → Ringing → Progressive Ringing	
Phone UI	Basic Setting → Sound → Ringing → Ring mode → Progressive Ringing	
Parameter	**SettingRingSilentEnable**	**config.xml**
Description	It enables or disables ring silent mode.	
Permitted Values	false - disable true - enable	
Default	false	
Web UI	Setting → Ringing → Silent Mode	
Phone UI	Basic Setting → Sound → Ringing → Ring mode → Silent mode	
Parameter	**SettingRingBeep**	**config.xml**
Description	It configures ring beep (only support 0, 1, 3).	
Permitted Values	0 - BeepNone 1 - BeepSingle 2 - BeepDouble 3 - BeepTriple	
Default	0	
Web UI	Setting → Ringing → Beeps Before Ringing	
Phone UI	Basic Setting → Sound → Ringing → Beep	
Parameter	**SettingRingtoneUploadUrl**	**config.xml**
Description	It configures the URL that phone can download the custom ringtone.	

Permitted Values	String (within 511 Characters)	
Default	Blank	
Web UI	Settings → Ringing → Custom Melody	
Parameter	**SettingRingtoneDelete**	**config.xml**
Description	It configures the name of the custom ringtone that to be deleted.	
Permitted Values	/all - delete all customized ringtones Text – delete specific ringtone	
Default	Blank	
Web UI	Settings → Ringing → Custom Melody	

7.3.3 Custom Ringtone

This feature allows users to upload and delete the custom ringtone(s) to the phone. Users can upload and delete customized ringtone(s) through the config file or Web UI for the phone.

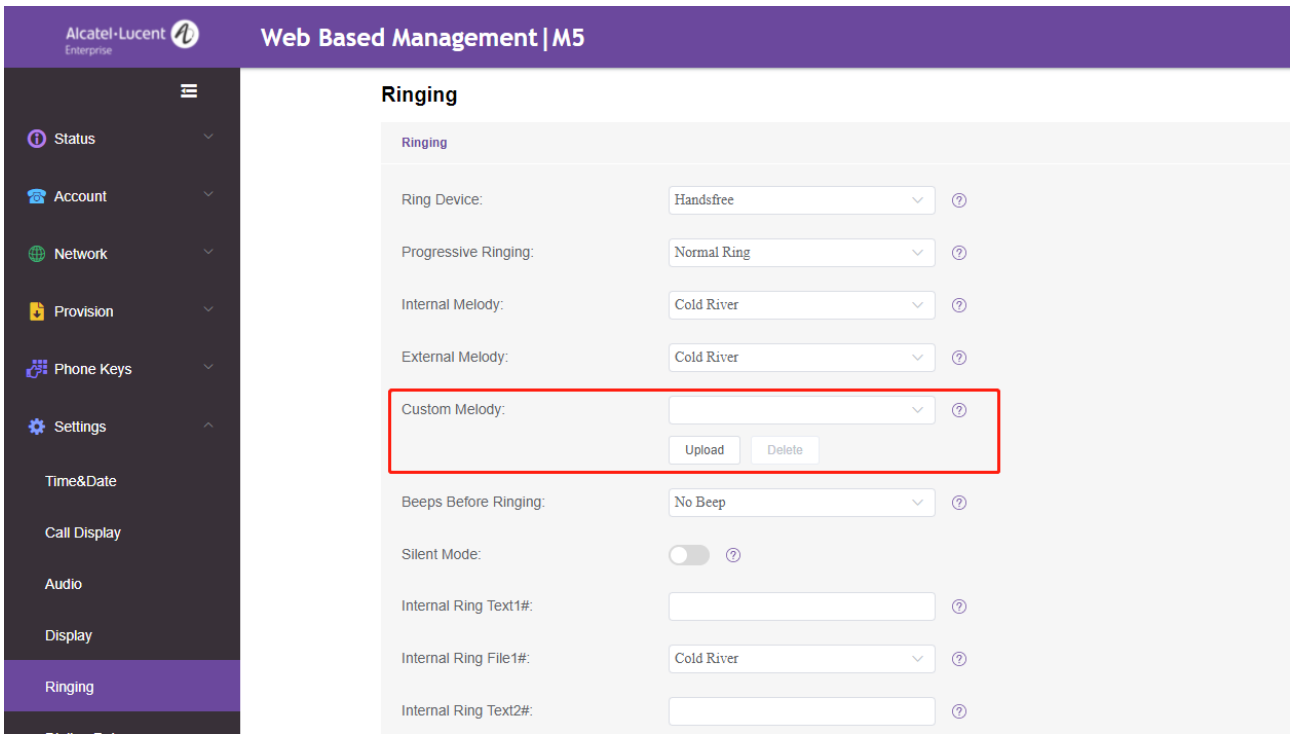
- Upload/Delete custom ringtone(s) by config file
  <setting id="SettingRingtoneUploadUrl " value="http://x.x.x.x/xxx.wav" override="true"/>
  <setting id="SettingRingtoneDelete" value="" override="true"/>

When uploading ringtone(s) by config file, .wav and .zip file can be supported. To upload a .wav ring file, the file size should be less than 200kb, and the upper limit is 5 ringtones. The zip file should not exceed 1.2M, and the phone will ignore the file when the size is more than 1.2M. If there are more than 5 ringtones, the phone will only save the first 5 ringtones.

When deleting a ringtone by config file you can either enter the ringtone name to delete the customized ringtone from the phone or enter “/all” to delete all customized ringtones.

- Upload/Delete custom ringtone(s) through WEB

Login in the phone web interface, go to Settings → Ringing → Custom Melody:



Buttons “Upload” and “Delete” can be used to upload or delete ringtone(s), only wav file is supported on WBM, and the upper limit is also 5 ringtones.

7.4 Distinctive Ring Tones

The feature of distinctive ring tones allows certain incoming calls to trigger IP phones to play distinctive ring tones. The IP phone inspects the INVITE request for an "Alert-Info" header when receiving an incoming call. If the INVITE request contains an "Alert-Info" header, the IP phone strips out the URL or keyword parameter and maps it to the appropriate ring tone.

7.4.1 Supported Alert-Info Headers Format

The Desktop phone supports four types of alert-info message header fields: Bellcore-drN, ringtone-N (or MyMelodyN), and info=info text; x-line-id=0.

Note: If the Alert-Info header contains multiple types of keywords, the IP phone will process the keywords in the following order: <urn:alert:tone:internal/external> >> ringtone/ MyMelody >> Bellcore-dr >> info=.

When desktop phone receives an INVITE message with Alert-info (Alert-info: internal/external), the phone will play a preset ringtone.

The following table lists the parameters you can use to configure the ringtone.

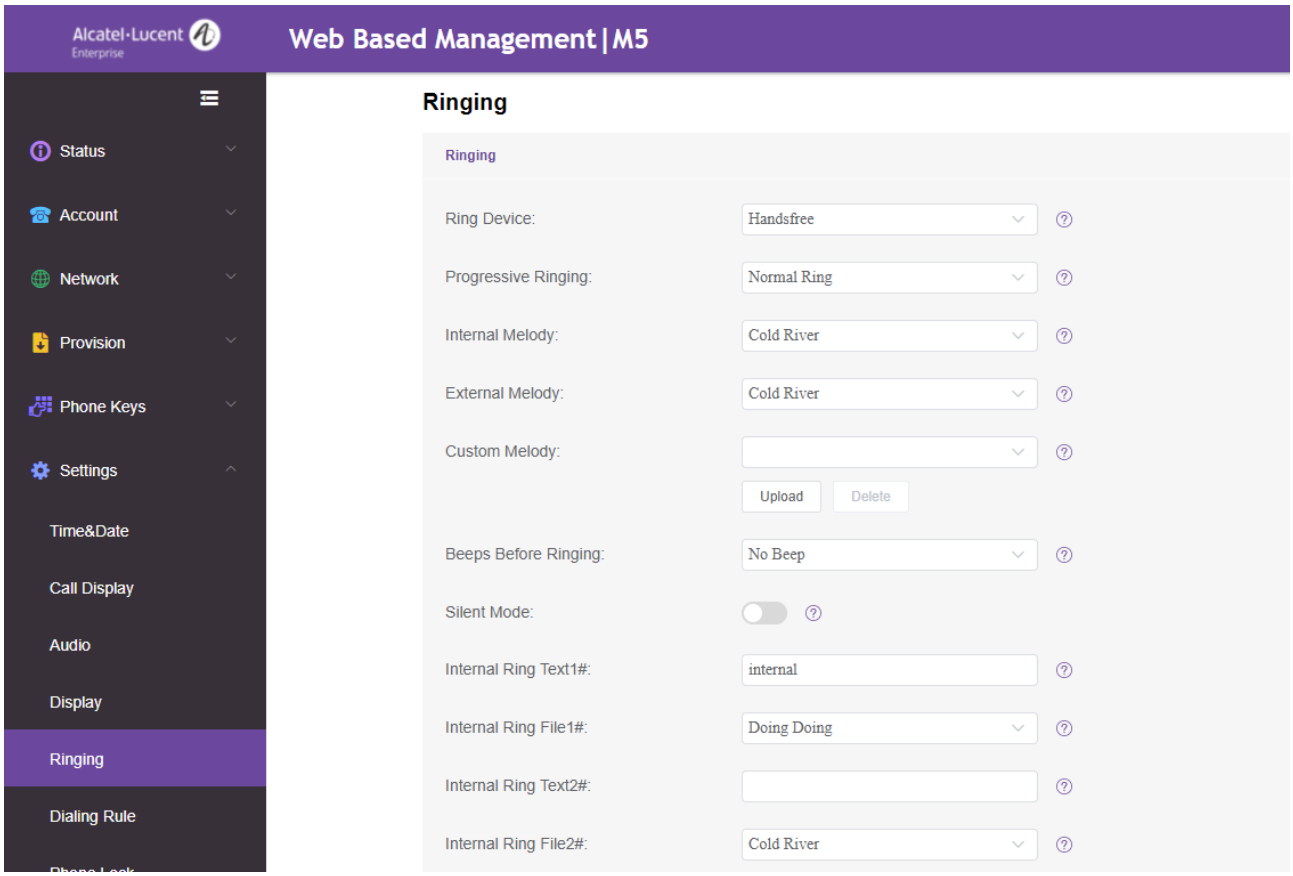
Parameter	**SettingRingerTextX**	**config.xml**
Description	It configures internal ringer text X. The X can be 1-10.	
Permitted Values	Strings	
Default	Blank	
Web UI	Setting → Ringing → Internal Ring TextX	
Parameter	**SettingRingerFileX**	**config.xml**
Description	It configures internal call ring melody X. The X can be 1-10.	
Permitted Values	Cold river Disco Neture Street dance Xylofun Sunrise Doing Doing Baby piano Transatlantic Moon Light Submarine Classic Jazzy Party Zen Orchid	
Default	Blank	

Web UI	Setting → Ringing → Internal Ring FileX

You can configure the distinctive ring tones via the phone's Web UI.

Configuration as shown below:

When receiving an INVITE Message with Alert-info (Alert-Info: <http://127.0.0.1>; info=internal), the phone will play the "Doing Doing" ringtone.



7.4.1.1 Alert-Info: Bellcore-drN

When the Alter-Info header contains the keyword "Bellcore-drN", the IP phone will play the desired ring tone.

The following table identifies the corresponding ring tone:

Value of N	Ring Tone (features.alert_info_tone = 1)	Ring Tone (features.alert_info_tone = 0)
0	Bellcore-dr0	ring00
1	Bellcore-dr1	ring01
2	Bellcore-dr2	ring02
3	Bellcore-dr3	ring03
4	Bellcore-dr4	ring04
5	Bellcore-dr5	ring05
6	Bellcore-dr6	ring06
7	Bellcore-dr7	ring07
8	Bellcore-dr8	ring08

9	Bellcore-dr9	ring09
10	Bellcore-dr10	ring10
11	Bellcore-dr11	ring11
12	Bellcore-dr12	ring12
13	Bellcore-dr13	ring13
14	Bellcore-dr14	ring14
N<1 or N>15		ring00

Examples:

```
Alert-Info: test/Bellcore-dr1
Alert-Info: Bellcore-dr1
Alert-Info: Bellcore-dr1;x-line-id=1
```

7.4.1.2 Alert-Info: Ringtone

When the Alter-Info header contains the keyword “ringtone-N/ringtone-RingN” or “MyMolodyN/MyMelodyRingN”, the IP phone will play the corresponding local ring tone (RingN.wav), or play the first local ring tone (Ring1.wav) in about 10 seconds if “N” is greater than 15 or less than 1.

Examples:

```
Alert-Info: ringtone-2
Alert-Info: ringtone-Ring2.wav
Alert-Info: ringtone-2;x-line-id=1
Alert-Info: MyMelody2
Alert-Info: MyMelodyRing2.wav
Alert-Info: MyMelody2;x-line-id=1
```

The following table identifies the corresponding local ring tone:

Value of N	Ring Tone
0	ring00
1	ring01
2	ring02
3	ring03
4	ring04
5	ring05
6	ring06
7	ring07
8	ring08
9	ring09
10	ring10
11	ring11

12	ring12
13	ring13
14	ring14
N<1 or N>15	ring00

7.4.1.3 Alert-Info: info=info text; x-line-id=0

When the Alert-Info header contains an info text, the IP phone will map the text with the Internal Ringer Text preconfigured on the IP phone, and then play the ring tone associated with the Internal Ringer Text (the ring tone can be configured by the parameter). If no internal ringer text maps, the IP phone will play the preconfigured local ring tone in about 10 seconds.

Example:

Alert-Info: info=family; x-line-id=0

7.4.1.4 Alert Info for Auto Answer

If the INVITE request contains the following type of strings, the IP phone will answer incoming calls automatically without playing the ring tone:

- Answer-Mode: Auto
- Alert-Info: info = alert-autoanswer
- Call-Info: answer-after = 0 (or Call-Info: Answer-After = 0)

7.5 Ringer Device

The IP phones support ringing from speaker or headset or both. You can configure which ringer device to be used when receiving an incoming call.

For example, if the ringer device is configured on speaker, the ring tone will be played through loud speaker.

If the ringer device is configured on headset or Headset & Speaker, the headset should be connected to the IP phone and the Headset mode also should be activated in advance.

The following table lists the parameters you can use to configure ringer device.

Parameter	**SettingRingDevice**	**config.xml**
Description	It configures Audio Ring Device.	
Permitted Values	0 - handsfree 1 - Headset 2 - handsfree_plus_Headset	
Default	0	
Web UI	Setting → Ringing → Ring Device	
Phone UI	Basic Setting → Sound → Ringing → Ring Device	

7.6 Tones

When receiving a message, the IP phone will play a warning tone. You can customize tones or select specialized tone phones (varying from country to country) to indicate different status of the IP phone.

7.6.1 Supported Country Tones

The default country tone is UK. Available list as follows:

- UK

- France
- Germany
- Italy
- Spain
- Dutch
- Portugal
- Canada
- US
- Hungary
- Czec
- Slovakia
- Slovenia
- Estonia
- Poland
- Lithuania
- Latvia
- Turkey
- Greece
- Russia
- China(Mainland)
- China(Hongkong)
- China(Taiwan)
- Thailand
- Korea
- Japan

7.6.2 Tones Configuration

The following table lists the parameters you can use to configure tones.

Parameter	**SettingCountryTone**	**config.xml**
Description	It configures country standard for call progress tone.	
Permitted Values	0 - UK 1 - France 2 - Germany 3 - Italy 4 - Spain 5 - Dutch 6 - Portugal 7 - Canada 8 - US 9 - Hungary 10 - Czec 11 - Slovakia 12 - Slovenia 13 - Estonia 14 - Poland 15 - Lithuania 16 - Latvia 17 - Turkey 18 - Greece	

	19 - Russia 20 - China(Mainland) 21 - China(Hongkong) 22 - China(Taiwan) 23 - Thailand 24 - Korea 25 - Japan
Default	0

7.7 Audio Codecs

Codec is an abbreviation of Compress-Decompress, capable of coding or decoding a digital data stream or signal by implementing an algorithm. The object of the algorithm is to represent the high-fidelity audio signal with a minimum number of bits while retaining the quality. This can effectively reduce the frame size and the bandwidth required for audio transmission.

The audio codec that the phone uses to establish a call should be supported by the SIP server. When placing a call, the IP phone will offer the enabled audio codec list to the server and then use the audio codec negotiated with the called party according to the priority.

7.7.1 Supported Audio Codecs

The following table summarizes the supported audio codecs on IP phones:

Codec	Algorithm	Reference	Bit Rate	Sample Rate	Packetization Time
G722	G722	RFC 3551	64 Kbps	16 Ksps	20ms
PCMA	PCMA G.711 a-law	RFC 3551	64 Kbps	16 Ksps	20ms
PCMU	G.711 u-law	RFC 3551	64 Kbps	16 Ksps	20ms
G729	G729	RFC 3551	8 Kbps	16 Ksps	20ms
iLBC_15_2kbps	iLBC	RFC 3952	15.2 Kbps	8 Ksps	20ms
iLBC_13_33kbps	iLBC	RFC 3952	13.33 Kbps	8 Ksps	30ms
opus	opus	RFC 6716	8-12 Kbps 28-40 Kbps 64-128 Kbps	8 Ksps 16 Ksps 48 Ksps	20ms

The Opus codec supports various audio bandwidths, defined as follows:

Abbreviation	Audio Bandwidth	Sample Rate (Effective)
NB (narrowband)	4 kHz	8 kHz
WB (wideband)	8 kHz	16 kHz
FB (fullband)	20 kHz	48 kHz

The following table lists the audio codecs supported by each phone model:

Phone Model	Supported Audio Codecs	Default Audio Codecs
Myriad Series	pcmu;pcma;g729AB;g722;iLBC;opus	pcmu;pcma;g729AB;g722;iLBC

7.7.2 Audio Codecs Configuration

The following table lists the parameters you can use to configure the audio codecs.

Note: X means account ID and it can be number 1~8 for M3/M5/M7, 1-20 for M8.

Parameter	**AccountXAudioCodec**	**config.xml**
Description	It configures the codec list which is supported by phone for accountX.	
Permitted Values	8 - pcma 0 - pcmu 9 - g722 18 - g729AB 98 - iLbc 125 - opus	
Default	0;8;18;9;98	
Web UI	Account → Codec → Audio Codec	
Parameter	**AccountXOpusBandwidth**	**config.xml**
Description	It configures OPUS bandwith for accountX.	
Permitted Values	0 - Narrow Band 1 - Wide Band 2 - Super Wide Band	
Default	1	
Web UI	Account → Codec → OPUS Bandwidth	
Parameter	**AccountXIlbcFrameMode**	**config.xml**
Description	It configures iLBC frame length for accountX.	
Permitted Values	20 - 20 30 - 30	
Default	30	
Web UI	Account → Codec → ILBC Frame Mode	

7.8 Packetization Time (PTime)

PTime is a measurement of the duration (in milliseconds) of the audio data in each RTP packet sent to the destination and defines how much network bandwidth is used for the RTP stream transfer. Before establishing a conversation, codec and ptime are negotiated through SIP signaling. The valid values of ptime range from 10 to 60, in increments of 10 milliseconds. The default ptime is 20ms.

7.8.1 Supported PTime of Audio Codec

The following table summarizes the valid values of PTime for each audio codec:

Codec	Packetization Time (Minimum)	Packetization Time (Maximum)
G722	10ms	40ms
PCMA	10ms	40ms
PCMU	10ms	40ms
G729	10ms	80ms
iLBC	20ms	30ms

iLBC_15_2kpbs	20ms, 40ms, 60ms	
iLBC_13_33kpbs	30ms, 60ms	
opus	10ms	20ms

7.8.2 PTime Configuration

The following table lists the parameter you can use to configure the PTime.

Note: X means account ID and it can be number 1~8 for M3/M5/M7, 1-20 for M8.

Parameter	**AccountXPtime**	**config.xml**
Description	It configures array of RTP packet interval (in ms) of 6 codecs (PCMU/PCMA/G729AB/G722/ILBC/OPUS) in sequence for certain account. X means account ID and can be 1~8 for M3/M5/M7.	
Permitted Values	10 20 30 40 50 60	
Default	20;20;20;20;20;20	
Web UI	Account → Codec → Ptime	

7.9 Early Media

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

7.10 Acoustic Clarity Technology

To optimize the audio quality of your network, the ALE Myriad Series phones support the acoustic clarity technology: Acoustic Echo Cancellation (AEC), Background Noise Suppression (BNS), Automatic Gain Control (AGC), Voice Activity Detection (VAD), Comfort Noise Generation (CNG) and jitter buffer.

7.10.1 Acoustic Echo Cancellation (AEC)

The ALE Myriad Series phones employ advanced AEC for hands-free operation. The AEC feature can remove the echo of the local loudspeaker from the local microphone without removing the near-end speech.

7.10.2 Noise Suppression

The impact noise in the room is picked-up, including paper rustling, coffee mugs, coughing, typing, and silverware striking plates. These noises, when transmitted to remote participants, can be very distracting. It is enabled on the ALE Myriad Series phones by default.

7.10.3 Background Noise Suppression (BNS)

Background noise suppression (BNS) is designed primarily for hands-free operation and reduces background noise to enhance communication in noisy environments.

7.10.4 Automatic Gain Control (AGC)

Automatic Gain Control (AGC) is applicable to the hands-free operation and is used to keep audio output at nearly a constant level by adjusting the gain of signals in some circumstances. This increases the effective user-phone radius and helps with the intelligibility of soft-talkers.

7.10.5 Voice Activity Detection (VAD)

VAD can avoid unnecessary coding or transmission of silence packets in VoIP applications, saving on computation and network bandwidth.

The following table lists the parameter you can use to configure VAD.

Note: X means account ID. It can be number 1~8 for M3/M5/M7, 1-20 for M8.

Parameter	**AccountXVad**	**config.xml**
Description	It enables or disables audio VAD for account.	
Permitted Values	false - disable true - enable	
Default	false	
Web UI	Account → Codec → VAD	

7.10.6 Comfort Noise Generation (CNG)

Comfort Noise Generation (CNG) is used to generate background noise for voice communications during periods of silence in a conversation.

7.10.7 Jitter Buffer

The ALE Myriad Series phones support fixed type of jitter buffers. A fixed jitter buffer with corresponding fixed delay to voice packets.

7.11 DTMF

DTMF (Dual Tone Multi-frequency) tone better known as touch tone. DTMF is the signal sent from the IP phone to the network, which is generated when pressing the IP phone's keypad during a call. Each key pressed on the IP phone generates one sinusoidal tone of two frequencies. One is generated from a high-frequency group and the other from a low-frequency group.

Five methods of transmitting DTMF digits on SIP calls:

- RFC 2833 - DTMF digits are transmitted by RTP Events compliant with RFC 2833. You can configure the payload type and sending times of the end RTP Event packet. The RTP Event packet contains 4 bytes. The 4 bytes are distributed over several fields denoted as Event, End bit, R-bit, Volume and Duration. If the End bit is set to 1, the packet contains the end of the DTMF event. You can configure the sending times of the end RTP Event packet.
- RFC 4733 - The RCF 4744 is optimized based on RFC 2833 framework, it specifically differs from RFC 2833 by removing the requirement that all compliant implementations support the DTMF events. Instead, compliant implementations taking part in out-of-band negotiations of media stream content indicate what events they support. it adds three new procedures to the RFC 2833 framework: subdivision of long events into segments, reporting of multiple events in a single packet, and the concept and reporting of state events.
- INBAND - DTMF digits are transmitted in the voice band. It uses the same codec as your voice and is audible to conversation partners.
- SIP INFO - DTMF digits are transmitted by SIP INFO messages. DTMF digits are transmitted by the SIP INFO messages when the voice stream is established after a successful SIP 200 OK-ACK

message sequence. The SIP INFO message can transmit DTMF digits in three ways: DTMF, DTMF-Relay and Telephone-Event.

- SIP INFO + RFC 2833

The following table lists the parameters for configuring the transmitting DTMF digit:

Note: X means account ID and it can be number 1~8 for M3/M5/M7, 1-20 for M8.

Parameter	**AccountXDtmfMode**	**config.xml**
Description	It configures the mode for server GroupX when sending DTMF.	
Permitted Values	0 - None 1 - InBand 2 - RFC2833 3 - RFC4733 4 - SIP_INFO 5 - SIP_INFO+RFC2833	
Default	2	
Web UI	Account → Advanced → DTMF Mode	
Parameter	**SettingDtmfDuration**	**config.xml**
Description	It configures the DTMF duration.	
Permitted Values	1 - 80ms 2 - 100ms 3 - 200ms 4 - 250ms	
Default	2	
Parameter	**SettingDtmfFeedbackEnable**	**config.xml**
Description	It enables or disables DTMF feedback.	
Permitted Values	false - disable true - enable	
Default	true	
Web UI	Setting → Audio → Enable DTMF Feedback	
Parameter	**SettingDtmfLevel**	**config.xml**
Description	It configures bias value of DTMF tone level.	
Permitted Values	[-6,6]	
Default	0	
Web UI	Setting → Audio → DTMF Level	

7.12 Voice Quality Monitoring (VQM)

Voice quality monitoring feature allows the IP phones to generate various quality metrics for listening quality and conversational quality. These metrics can be sent to a specific server in RTCP-XR packets. These metrics can also be sent in SIP PUBLISH messages to a central voice quality report collector.

7.12.1 RTCP-XR

The RTCP-XR mechanism, compliant with RFC 3611-RTP Control Extended Reports (RTCP XR), provides the metrics contained in RTCP-XR packets for monitoring the quality of calls. These metrics include network packet loss, delay metrics, analog metrics and voice quality metrics.

7.12.2 VQ-RTCPXR

The VQ-RTCPXR mechanism, compliant with RFC 6035, sends the service quality metric reports contained in SIP PUBLISH messages to the central report collector.

A wide range of performance metrics are generated in the following three ways:

- Based on current values, such as jitter, jitter buffer max and round-trip delay.
- Covers the time period from the beginning of the call until the report is sent, such as network packet loss.
- Computed using other metrics as input, such as listening Mean Opinion Score (MOS-LQ) and conversational Mean Opinion Score (MOS-CQ).

The following table lists the parameters you can use to configure the Central Report Collector.

Note: X means account ID. It can be number 1~8 for M3/M5/M7, and 1-20 for M8.

Parameter	**AccountXVoIPTicketsCollector**	**config.xml**
Description	The VoIP ticket collector name is used for publishing VoIP tickets. If Blank, no PUBLISH request will be sent at the end of each call. **Note:** X means account ID. It can be number 1~8 for M3/M5/M7, and 1-20 for M8..	
Permitted Values	String within 128 characters	
Default	Blank	
Web UI	Account → Advanced → SIP VoIP Tickets Collector	

7.13 Suppress DTMF Display

Suppress DTMF Display allows IP phones to suppress the display of DTMF digits during an active call. DTMF digits are displayed as “*” on the phone screen. Suppress DTMF Display delay defines whether to display the DTMF digits for a short period of time before displaying as “*”.

The following table lists the parameters you can configure to suppress DTMF display.

Parameter	**FeatureDtmfHideEnable**	**config.xml**
Description	It enables or disables the IP phone to suppress the display of DTMF digits during an active call.	
Permitted Values	false - disable true - enable	
Default	false	
Parameter	**FeatureDtmfHideDelay**	**config.xml**
Description	The DTMF number will be hidden after a few seconds.	
Permitted Values	[0,5]	
Default	1	

8. Multiple SIP Accounts

This chapter introduces how to configure the account settings and register to SIP server on the ALE Myriad Series phones.

8.1 Account Registration

Registering an account makes it easier for the IP phones to receive an incoming call or dial an outgoing call. The ALE Myriad Series phones support registering multiple accounts on a phone, each account requires an extension or phone number.

8.1.1 Supported Accounts

The ALE M3/M5/M7 DeskPhones support 8 accounts maximum, and M8 supports 20 accounts maximum.

8.1.2 SIP Accounts Registration Configuration

The following table lists the parameters you can use to register SIP accounts:

Note: X means account ID. It can be number 1~8 for M3/M5/M7, and 1-20 for M8.

Parameter	**AccountXEnable**	**config.xml**
Description	It enables or disables to certain account.	
Permitted Values	true- disable. false - enable	
Default	true	
Web UI	Account→Basic	
Parameter	**AccountXLabel**	**config.xml**
Description	It configures the label name.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Account → Basic → SIP Label Name	
Phone UI	Menu → Advanced Setting (default password: 123456) → Account → AccountX → Label Name	
Parameter	**AccountXDisplayName**	**config.xml**
Description	It configures the display name.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Account → Basic → Display Name	
Phone UI	Menu → Advanced Setting (default password: 123456) → Account → AccountX → Display name	
Parameter	**AccountXRegName**	**config.xml**

Description	It configures the register name.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Account → Basic → Register Name	
Phone UI	Menu → Advanced Setting (default password: 123456) → Account → AccountX → Register name	
Parameter	**AccountXPassword**	**config.xml**
Description	It configures the register password.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Account → Basic → Password	
Phone UI	Menu → Advanced Setting (default password: 123456) → Account → AccountX → Password	
Parameter	**AccountXUserName**	**config.xml**
Description	It configures the user name.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Account → Basic → User Name	
Phone UI	Menu → Advanced Setting (default password: 123456) → Account → AccountX → User name	
Parameter	**AccountXServer1Address**	**config.xml**
Description	It configures the IP address or domain name of the SIP server.	
Permitted Values	String within 256 characters	
Default	Blank	
Web UI	Account → Basic → Sip Server	
Phone UI	Menu → Advanced Setting (default password: 123456) → Account → AccountX → Sip server1	
Parameter	**AccountXServer1Port**	**config.xml**
Description	It configures the port of SIP server.	
Permitted Values	Integer from 0 to 65535	
Default	5060	

Web UI	Account → Basic → SIP Server Port	
Parameter	**AccountXOutboundProxy1Address**	**config.xml**
Description	It configures the IP address or domain name of the outbound proxy server.	
Permitted Values	String within 256 characters	
Default	Blank	
Web UI	Account → Basic → OutBound Proxy Address	
Phone UI	Menu → Advanced Setting (default password: 123456) → Account → AccountX → Outbound proxy1	
Parameter	**AccountXOutboundProxy1Port**	**config.xml**
Description	It configures the port of the outbound proxy server for accountX.	
Permitted Values	Integer from 0 to 65535	
Default	5060	
Web UI	Account → Basic → OutBound Proxy Port	
Parameter	**AccountXServer1Expire**	**config.xml**
Description	It configures the registration expiration time (in seconds) of SIP server for accountX.	
Permitted Values	Integer from 60 to *	
Default	3600	
Web UI	Account → Basic → Register Expire Time	

8.1.3 Registration Settings Configuration

The following table lists the parameters to configure the registration settings:

Note: X means account ID. It can be number 1~8 for M3/M5/M7, and 1-20 for M8.

Parameter	**AccountXSendUserPhoneEnable**	**config.xml**
Description	It enables or disables the IP phone to add “user=phone” to the SIP header of the INVITE message.	
Permitted Values	false - disable true - enable	
Default	false	
Web UI	Account → Advance → Send User=Phone	
Parameter	**AccountXServerType**	**config.xml**
Description	It configures the type of the SIP server.	

Permitted Values	0 - Default 1 - OXE 2 - OXO 6 - Broadsoft 10 - Metaswitch
Default	0
Web UI	Account → Advanced → Server Type

8.2 Server Redundancy

Server redundancy is often required in VoIP deployments to ensure continuity of phone service, for example, the call server offline for maintenance, the server crashes, or the connection between the IP phone and the server fails.

Two types of redundancy are possible. In some cases, a combination of the two may be deployed:

- **Failover**: In this mode, the full phone system functionality is preserved by having a second equivalent capability call server take over from the one that has gone down/off-line. After the IP phone fails to register to the primary server, it will send the register message to secondary server.
- **Fallback**: Compared with failover mode, fallback mode supports the policy of primary server first, which means IP phone always attempts to register to the primary server, it will return to the primary server once the primary server is available.

8.2.1 Registration Method of Failover/Fallback Mode with Outbound Proxy

Currently there is a binding relationship between SIP server and outbound proxy address. That means if you configure outbound proxy address1, the IP phone always sends SIP request message with server1 parameter to outbound proxy address1; when the outbound proxy address1 is not available, the phone will send SIP request message with server2 parameter to outbound proxy address2.

8.2.2 Failover/Fallback Mode Configuration

The following table lists the parameters you can use to configure failover/fallback server redundancy

Note: X means account ID. It can be number 1~8 for M3/M5/M7, and 1-20 for M8.

Parameter	**SIPFailOverEnable**	**config.xml**
Description	It configures the failover or fallback mode	
Permitted Values	true - failover false - fallback	
Default	true	
Web UI	Features → SIP → Account Server Failover Enable	
Parameter	**AccountXServer2Address**	**config.xml**
Description	It configures the IP address or domain name of the secondary server in which the account X is registered.	
Permitted Values	String within 256 characters	
Default	Blank	
Web UI	Account → Basic → Secondary SIP Server	

Phone UI	Menu → Advanced Setting (default password: 123456) → Account → AccountX → SIP Server2	
Parameter	**AccountXServer2Port**	**config.xml**
Description	It configures the port of secondary server in which the accountX use to register.	
Permitted Values	Integer from 0 to 65535	
Default	5060	
Web UI	Account → Basic → Secondary SIP Port	
Parameter	**AccountXServer2Expire**	**config.xml**
Description	It configures the registration expiration time (in seconds) of secondary server for accountX.	
Permitted Values	Integer from 60 to *	
Default	3600	
Web UI	Account → Basic → Secondary Register Expire Time	
Parameter	**AccountXOutboundProxy2Address**	**config.xml**
Description	It configures the IP address or domain name of the secondary outbound proxy server for accountX.	
Permitted Values	String within 256 characters	
Default	Blank	
Web UI	Account → Basic → Secondary Outbound Proxy Address	
Phone UI	Menu → Advanced Settings → Account → AccountX → Outbound Proxy2	
Parameter	**AccountXOutboundProxy2Port**	**config.xml**
Description	It configures the IP address or domain name of the secondary outbound proxy server for accountX.	
Permitted Values	Integer from 0 to 65535	
Default	5060	
Web UI	Account → Basic → Secondary Outbound Proxy Port	

8.3 SIP Server Name Resolution

If a domain name is configured for a server, the IP address associated with that domain name will be resolved through DNS as specified by RFC 3263. The DNS query involves NAPTR, SRV and A queries, which allow the IP phone to adapt to various deployment environments. The IP phone performs NAPTR query for the NAPTR pointer and transport protocol (UDP, TCP and TLS), the SRV query on the record returned from the NAPTR for the target domain name and the port number, and the A query for the IP addresses.

If an explicit port (except 0) is specified, A query will be performed only. If a server port is 0 and then the transport type is DNS-NAPTR, NAPTR and SRV queries will be tried before falling to A query. If no port is found through the DNS query, 5060 will be used.

The following table lists the parameters you can use to configure SIP server name resolution.

Note: X means account ID. It can be number 1~8 for M3/M5/M7, and 1-20 for M8.

Parameter	**AccountXServer1Transport**	**config.xml**
Description	It configures the type of transport protocol.	
Permitted Values	0 - UDP 1 - TCP 2 - TLS 3 - DNS NAPTR **Note:** If no server port is given, the IP phone performs the DNS NAPTR and SRV queries for the service type and port.	
Default	0	
Web UI	Account → Basic → Transport Mode	

9. Call Log

All call logs are divided into All Calls/Missed Calls/Placed Calls/Received Calls/Forwarded Calls.

The five types of call logs are displayed via five tabs in Local History page. Users can switch the tabs by pressing left/right keys.

9.1 Call Log Display

You can access the call history information via phone user interface by the History soft key on homepage.

9.2 Call Log Configuration

The following table lists the parameters for call log settings:

Parameter	CallHistorySave	config.xml
Description	It enables or disables the IP phone to save the call logs (for missed calls, placed calls, and received calls).	
Permitted Values	0 - Not save 1 - Save all	
Default	1	

10. Call Features

This chapter shows you how to configure call features for the ALE Myriad Series phones:

10.1 Dial Plan

Dial plan is a string of characters that governs the way how IP phones process the inputs received from the IP phone's keypads. You can use the regular expression to define the dial plan.

10.1.1 Dial Plan Defined by Dialing Rule

The ALE Myriad Series phones support user-defined dialing rules, the parameters you can configure such as Country code, Area code, External Prefix and so on. They defined what the number would eventually dial out.

The following table lists the parameters you can use to configure dialing rule.

Note: X means account ID and it can be number 1~8 for M3/M5/M7, and 1-20 for M8.

Parameter	**AccountXDialingRuleCountryCode**	**config.xml**
Description	It configures the country code for accountX.	
Permitted Values	ISO 3166 country code (Alpha-2)	
Default	Blank	
Web UI	Setting → Dialing Rule → Country Code	
Parameter	**AccountXDialingRuleAreaCode**	**config.xml**
Description	It configures the area code for accountX.	
Permitted Values	String within 16 characters	
Default	Blank	
Web UI	Setting → Dialing Rule → Area Code	
Parameter	**AccountXDialingRuleExternalPrefix**	**config.xml**
Description	It configures the external prefix for accountX.	
Permitted Values	String within 16 characters	
Default	Blank	
Web UI	Setting → Dialing Rule → External Prefix	
Parameter	**AccountXDialingRuleMinNumberLength**	**config.xml**
Description	It configures the minimum length of number for accountX.	
Permitted Values	Integer from 0 to 120	
Default	Blank	
Web UI	Setting → Dialing Rule → Min Number Len	
Parameter	**AccountXDialingRuleExternalPrefixExceptions**	**config.xml**

Description	It configures list of exceptions while adding the external prefix.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Setting → Dialing Rule → External Prefix Exception	
Parameter	**AccountXDialingRuleInHistoryEnable**	**config.xml**
Description	It enables or disables dialing rule in history. **Note:** It includes: 1. Dial from History tab 2. Select a number in dialing screen by right key, which is provided by Call log. 3. Select a number on dialing screen by left key, which is provided by Call log, then choose “Call” or “Forward” key. 4. Dial by press redial key	
Permitted Values	true - enable false - disable	
Default	false	
Web UI	Setting → Dialing Rule → Dialing Rule Enabled in History → Enable/Disable	
Parameter	**AccountXDialingRuleInContactEnable**	**config.xml**
Description	It enables or disables dialing rule works in contact **Note:** It includes: 1. Dial from contacts tab 2. Select a number in dialing screen by right key, which is provided by contact. 3. Select a number on dialing screen by left key, which is provided by contact, then choose “Call” or “Forward” key.	
Permitted Values	true - enable false - disable	
Default	true	
Web UI	Setting → Dialing Rule → Dialing Rule Enabled in Contact → Enable/Disable	
Parameter	**AccountXDialingRuleInManualEnable**	**config.xml**
Description	It enables or disables dialing rule works in manual **Note:** It includes Input number directly / off-hook then dialing / handsfree then dialing.	
Permitted Values	true - enable false - disable	
Default	false	
Web UI	Setting → Dialing Rule → Dialing Rule Enabled in Manual → Enable/Disable	

10.1.2 Dial Plan Defined by Digit Map

Digit maps, described in RFC 3435, are defined by a single string or a list of strings. If a number entered matches any string of a digit map, the call is automatically placed. If a number entered matches no string - an impossible match - you can specify the phone’s behavior. You can specify the digit map timeout, the period of time before the entered number is dialed out.

10.1.2.1 Basic Regular Expression Syntax for Digit Map

You need to know the following basic regular expression syntax when creating a new dial plan:

.	The dot “.” can be used as a placeholder or multiple placeholders, including zero, of occurrences of the preceding construct. Examples: “123.T” would match “123”, “1233”, “12333”, “123333”, and so on. “x.T” would match an arbitrary number. “[x*#+].T” would match an arbitrary character. **Note:** If the string ends with a dot (e.g., 123.), a match will occur immediately after inputting the characters before the dot (e.g.123) since the dot allows for zero occurrences of the preceding construct. Therefore, we recommend that you add a letter “T” after the dot (for example, 123.T) for inputting more characters.
x	The “x” can be used as a placeholder for any digit from 0 to 9. Example: “12x” would match “121”, “122”, “123”, and so on.
-	The dash “-” can be used to match a range of digits within the brackets. Example: “[35-7]” would match the number “3”, “5”, ”6” or ”7”. **Note:** The digits must be concrete. For example, [3-x] is invalid.
,	The comma “,” can be used as a separator to generate a secondary dial tone. Example: “9, xx”: After entering digit “9”, secondary dial tone plays and you can complete the remaining two-digit numbers.
[ ]	The square bracket "[]" can be used as a placeholder for a single character which matches any of a set of characters. Example: "91[5-7]1234" would match “9151234”, “9161234”, and “9171234”.
T	The timer letter “T” indicates a timer expiry. If “T” is used alone (for example, 123T), the default timeout value of 3 will be used. If “T” is not used alone (for example, 123Tx, x can be a digit from 0 to 99), a complete match occurs when waiting x seconds after inputting 123. If “T” is not used (for example,123), a complete match occurs immediately after inputting 123.
R	The letter “R” indicates that certain matched strings are replaced. Using an RRR syntax, you can replace the digits between the first two Rs with the digits between the last two Rs. Example: “R12R234R” would replace 12 with 234.
!	The exclamation mark “!” can be used to prevent users from dialing out specific numbers. It can only be put last in each string of the digit map. Example: “235x!” would match “2351”, “2352”, “2353”, and so on. The number starting with 235 will be blocked to dial out.

10.1.2.2 Digit Map for All Accounts Configuration

The following table lists the parameters you can use to configure all accounts digit map:

Parameter	DigitMapEnable	config.xml

Description	It enables or disables the digit map feature. **Note:** Compatible rules for Digit Map and Old Dialing Rule: When enabling Digit Map, the Dialing rules defined by Digit Map are used instead of the old Dialing Rule.	
Permitted Values	true - enable false - disable	
Default	false	
Parameter	**DigitMap**	**config.xml**
Description	It configures the digit map pattern used for the dial plan.	
Permitted Values	String within 2048 characters	
Default	[2-9]11;0T;+011xxx.T;0[2-9]xxxxxxxxx;+1[2-9]xxxxxxxx;[2-9]xxxxxxxxx;[2-9]xxxT	
Parameter	**DigitMapTimer**	**config.xml**
Description	It configures the dial rule to match the timeout (the value of T), in seconds.	
Permitted Values	0-18	
Default	3	
Parameter	**DigitMapInHistoryEnable**	**config.xml**
Description	It enables or disables the digit map to be applied to the numbers (received calls or missed calls) dialed from the call history list.	
Permitted Values	true - enable false - disable	
Default	true	
Parameter	**DigitMapInDirectoryEnable**	**config.xml**
Description	It enables or disables the digit map to be applied to the numbers dialed from the directory.	
Permitted Values	true - enable false - disable	
Default	true	
Parameter	**DigitMapInForwardEnable**	**config.xml**
Description	It enables or disables the digit map to be applied to the numbers that you want to forward to when performing call forward.	
Permitted Values	true - enable false - disable	
Default	true	
Parameter	**DigitMapInManualEnable**	**config.xml**

Description	It enables or disables the entered number to match the predefined string of the digit map after pressing a send key. It is only applicable to the off-hook dialing.
Permitted Values	true - enable false - disable
Default	true

10.1.2.3 Digit Map for a Specific Line Configuration

The following table lists the parameters you can use to specific account digit map:

Note: X means account ID and it can be number 1~8 for M3/M5/M7, 1-20 for M8.

Parameter	**AccountXDigitMapEnable**	**config.xml**
Description	It enables or disables the digit map feature for a specific account.	
Permitted Values	true - enable false - disable	
Default	true	
Parameter	**AccountXDigitMap**	**config.xml**
Description	It enables or disables the digit map feature for a specific account.	
Permitted Values	String within 2048 characters	
Default	Blank	
Parameter	**AccountXDigitMapTimer**	**config.xml**
Description	It configures the dial rule to match the timeout (the value of T) in seconds.	
Permitted Values	0-18	
Default	Blank	
Parameter	**AccountXDigitMapInHistoryEnable**	**config.xml**
Description	It enables or disables the digit map to be applied to the numbers (received calls or missed calls) dialed from the call history list.	
Permitted Values	true - enable false - disable	
Default	true	
Parameter	**AccountXDigitMapInDirectoryEnable**	**config.xml**
Description	It enables or disables the digit map to be applied to the numbers dialed from the directory.	
Permitted Values	true - enable false - disable	

Default	true	
Parameter	**AccountXDigitMapInForwardEnable**	**config.xml**
Description	It enables or disables the digit map to be applied to the numbers that you want to forward to when performing call forward.	
Permitted Values	true - enable false - disable	
Default	true	
Parameter	**AccountXDigitMapInManualEnable**	**config.xml**
Description	It enables or disables the entered number to match the predefined string of the digit map after pressing a send key. It is only applicable to the off-hook dialing.	
Permitted Values	true - enable false - disable	
Default	true	

10.2 Hotline

Hotline, sometimes referred to as hot dialing, is a point-to-point communication link in which a call is automatically directed to the preset hotline number. If you lift the handset, press the loudspeaker key or the account key, and do nothing for a specified time interval, the IP phone will automatically dial out the hotline number that you configured.

Note: Hotline doesn't discriminate the accounts and you can configure only one hotline number.

The following table lists the parameters you can use to configure hotline.

Parameter	**FeatureHotlineEnable**	**config.xml**
Description	It enables or disables the phone to use hotline feature.	
Permitted Values	true - enable false - disable	
Default	false	
Web UI	Features → Hotline → Hotline	
Phone UI	Menu → Features → Hotline	
Parameter	**FeatureHotlineNumber**	**config.xml**
Description	It configures the hotline number that the IP phone automatically dials out when you lift the handset, press the loudspeaker key or the account key.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → Hotline → Hotline Number	
Phone UI	Menu → Features → Hotline → Number	

Parameter	FeatureHotlineDelayTimeout	config.xml
Description	It configures the waiting time (in seconds) for the IP phone to automatically dial out the preset hotline number. **Note:** If it is set to 0, the IP phone will dial out the configured hotline number immediately when you lift the handset, press the loudspeaker key or press the account key	
Permitted Values	Integer from 0 to 10	
Default	0	
Web UI	Features → Hotline → Delay Time	
Phone UI	Menu → Features → Hotline → Delay	

10.3 Recall

Recall, also known as last call return, allows you to dial the last received call. Recall is implemented on IP phones using a programming key.

The following table lists the parameter you can use for recall configuration:

Note: X means programmable key ID and it can be number 1~20 for M3,1~28 for M5/M7 and 1-36 for M8.

```
<?xml version="1.0" encoding="UTF-8" ?>
<settings>
        <setting id=" PhoneProgKey4Type" value="18" override="true"/>
        <setting id=" PhoneProgKey4Label " value="Recall" override="true"/>
</settings>
```

After configuration, a recall key is available on the phone.

When you press the recall key, the phone will dial the last received call.

10.4 Speed Dial

Speed dial allows you to speed up dialing the contacts on the phone's idle screen using dedicated programmable keys.

The following table lists the parameter you can use to speed dial configuration:

Note: X means programmable key ID and it can be number 1~20 for M3,1~28 for M5/M7 and 1-36 for M8.

```
<?xml version="1.0" encoding="UTF-8" ?>
<settings>
        <setting id="PhoneProgKey6Type" value="1" override="true"/>
            <setting id="PhoneProgKey6Account " value="1" override="true"/>
        <setting id="PhoneProgKey6Number" value="1234" override="true"/>
<setting id=" PhoneProgKey6Label " value="SpeedDail" override="true"/>
</settings>
```

After correct configuration, a Speed Dial key is available on the phone.

You can configure multiple Speed Dial keys for different contacts which are used frequently or hard to remember.

10.5 Call Timeout

Call timeout defines a specific period of time after which the IP phone will cancel the dialing if the call is not answered.

The following table lists the parameter you can use to configure call timeout.

Parameter	**FeatureRingBackTimeout**	**config.xml**
Description	It configures the duration time (in seconds) in the ringback state. If you set it to 60s, the phone will cancel the dialing when the call is not answered after 60 seconds.	
Permitted Values	Integer from 0 to 120	
Default	60	

10.6 Auto Dial Out Timer

It configures the timer when the phone dial out the number after inputting the last digit.

The following table lists the parameter you can use to configure the auto dial out timer.

Parameter	**FeatureAutoDialOutTimer**	**config.xml**
Description	It configures the timer when the phone dials out the number after inputting the last digit.	
Permitted Values	Integer from 0 to 18	
Default	5	

Web UI	Features → General → Auto Dial Out Timer

10.7 Anonymous Call

Anonymous call allows the caller to conceal the identity information shown to callee. The callee's phone LCD screen prompts an incoming call from anonymity (there is no name, number or other information displayed).

Anonymous calls can be performed locally or on the server. When performing an anonymous call on local, the IP phone sends an INVITE request message with a call source "From: Anonymous <sip:anonymous@anonymous.invalid>;tag=878106cc5e". If performing an anonymous call on a specific server, you may need to configure the anonymous call on code and off code to activate and deactivate the function of anonymous call on the server side.

The following table lists the parameters to configure an anonymous call.

Note: X means account ID and it can be number 1~8 for M3/M5/M7, and 1-20 for M8.

Parameter	**AccountXAnonymousCallEnable**	**config.xml**
Description	It enables or disable the anonymous call feature for account.	
Permitted Values	true - enable false - disable	
Default	false	
Web UI	Account → Advanced → Anonymous Call	
Phone UI	Menu → Features → Anonymous → AccountX → Anonymous	
Parameter	**AccountXAnonymousCallOnCode**	**config.xml**
Description	It configures the on code for accountX to activate anonymous call feature on the server side. **Note:** The parameter AccountXAnonymousCallEnable must set to true, the phone will send the on code to server.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Account → Advanced → Anonymous Call On Code	
Phone UI	Menu → Features → Anonymous → AccountX → On Code	
Parameter	**AccountXAnonymousCallOffCode**	**config.xml**
Description	It configures the off code for accountX to deactivate anonymous call feature on server side. **Note:** The parameter AccountXAnonymousCallEnable must set to false, the phone will send the off code to server.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Account → Advanced → Anonymous Call Off Code	

Phone UI	Menu → Features → Anonymous → AccountX → Off Code

10.8 Anonymous Call Rejection

Anonymous call rejection allows an IP phone to automatically reject incoming calls from callers whose identity has been deliberately concealed.

Anonymous call rejection can be performed locally or on the server. If performing anonymous call rejection on a specific server, you may need to configure anonymous call rejection on code and off code to activate and deactivate server-side anonymous call rejection feature.

The following table lists the parameters to configure anonymous call rejection.

Note: X means account ID. It can be number 1~8 for M3/M5/M7, and 1-20 for M8.

Parameter	**AccountXAnonymousCallRejectionEnable**	**config.xml**
Description	It enables or disables the anonymous call rejection feature.	
Permitted Values	true - enable false - disable.	
Default	false	
Web UI	Account → Advanced → Anonymous Rejection	
Phone UI	Menu → Features → Anonymous Reject → Account X	
Parameter	**AccountXAnonymousCallRejectionOnCode**	**config.xml**
Description	It configures the anonymous call rejection on code. The IP phone will send the code to activate anonymous call rejection feature on server side when you activate it on the IP phone.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Account → Advanced → Anonymous Rejection On Code	
Phone UI	Menu → Features → Anonymous Reject → Account X	
Parameter	**AccountXAnonymousCallRejectionOffCode**	**config.xml**
Description	It configures the anonymous call rejection off code. The IP phone will send the code to deactivate anonymous call rejection feature on server side when you deactivate it on the IP phone.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Account → Advanced → Anonymous Rejection Off Code	
Phone UI	Menu → Features → Anonymous Reject → Account X	

10.9 Call Number Filter

Call number filter feature allows an IP phone to filter designated characters automatically when dialing.

The following table lists the parameters you can use to configure call number filter.

Parameter	FeatureCallNumberFilter	config.xml
Description	It configures the characters that the IP phone will filter when dialing. If the dialed number contains configured characters, the IP phone will automatically filter these characters when dialing. If you dial 10-1, the IP phone will filter the character - and then dial out 101.	
Permitted Values	String within 32 characters	
Default	,-()	
Web UI	Setting → General → Call Number Filter	

10.10 IP Address Call

You can configure the phone whether to receive or place an IP call.

10.10.1 IP Address Call Configuration

The following table lists the parameter you can use to configure an IP address call.

Parameter	SIPIpCallEnable	config.xml
Description	It enables or disables IP address call feature. **Note:** The parameter can only control the outgoing IP address call. If you don't want to answer the IP address call, you should set the parameter "SIPIpCallEnable" to false.	
Permitted Values	true - enable false - disable	
Default	false	
Web UI	SIP Features → SIP → Allow IP Call	

10.10.2 Accept SIP Trust Server Only Configuration

Accept SIP Trust Server Only enables the IP phone to only accept the SIP messages from your SIP server and outbound proxy server. It can prevent the phone from receiving ghost calls from random numbers. If you enable this feature, the IP phone cannot accept an IP address call.

The following table lists the parameters to configure the Accept SIP Trust Server Only feature.

Parameter	SIPPeerFilterEnable	config.xml
Description	It enables or disables filtering the IP address call. **Note:** The parameter can only control the incoming IP address call. If you want to make an outgoing IP address call, you should set the parameter "SIPIpCallEnable" to true.	
Permitted Values	true - enable false - disable	
Default	false	

Web UI	Features → SIP → SIP Peer Filter

10.11 Auto Answer

The ALE Myriad Series phones support answering a SIP call or an IP address call automatically. Auto answer is configurable on a per-line basis, while IP address call is not.

By default, the IP phones will not automatically answer the incoming call during a call even if auto answer is enabled; and the incoming call will not be automatically answered after you end the current call.

The following table lists the parameters you can use to configure auto answer.

Note: X means account ID. It can be number 1~8 for M3/M5/M7, and 1-20 for M8.

Parameter	**AccountXAutoAnswerEnable**	**config.xml**
Description	It enables or disables auto answering a SIP call for accountX. **Note:** The IP phone cannot automatically answer the incoming call during a call even if auto answer is enabled.	
Permitted Values	true - enable false - disable	
Default	false	
Web UI	Account → Advanced → Auto Answer	
Phone UI	Menu → Features → Auto answer → AccountX → Enable/Disable	

10.12 Call Waiting

While Call waiting feature enabled, the phone will be able to answer the second call when there is already an active call on your phone. If it is disabled, the second incoming call will be rejected automatically.

You can enable call waiting feature and configure the phone to play a warning tone to avoid missing important calls during a call. They may vary on different servers.

You can activate and deactivate the call waiting feature by On Code and Off Code which generally also requests server to support call waiting feature.

The following table lists the parameters you can use to configure call waiting.

Parameter	**FeatureCallWaitingEnable**	**config.xml**
Description	It enables or disables the call waiting feature.	
Permitted Values	true - enable false - disable	
Default	true	
Parameter	**FeatureCallWaitingToneEnable**	**config.xml**
Description	It enables or disables the IP phone to play the call waiting tone when the IP phone receives an incoming call during a call. **Note:** It works only if “SIPMaxCall” is set to 2 (Enabled).	
Permitted Values	0 - disable 1 - enable	
Default	1	

Web UI	Features → General → Call Waiting Tone Enable	
Parameter	**FeatureCallWaitingOnCode**	**config.xml**
Description	It configures the On Code of the call waiting feature. The phone will send on code number to server to enable call waiting function on server.	
Permitted Values	String (within 32 characters)	
Default	Blank	
Web UI	Features → General → Call Waiting On Code	
Parameter	**FeatureCallWaitingOffCod**	**config.xml**
Description	It configures the Off Code of the call waiting feature. The phone will send on code to server to enable call waiting function on server.	
Permitted Values	String (within 32 characters)	
Default	Blank	
Web UI	Features → General → Call Waiting Off Code	

10.13 Do Not Disturb (DND)

DND feature enables the phone to reject all incoming calls automatically when you do not want to be interrupted. You can choose to implement DND locally on the phone or on the server side.

Usually, you can activate DND when the phone is idle. The phone stays in the DND state until you deactivate DND manually.

10.13.1 DND Settings Configuration

You can change the following DND settings:

- Choose a DND mode. You can configure DND for all accounts (Phone mode) or specific account (Custom mode).
- The IP phone displays a DND icon on the idle screen or program key for account when the DND feature is enabled. It helps users to clearly view that DND is activated or not.

The following table lists the parameters you can use to configure DND setting.

Parameter	**FeatureDndMode**	**config.xml**
Description	It configures the DND mode for the IP phone.	
Permitted Values	0: Phone. DND feature is effective for the phone system. 1: Custom. You can configure DND feature for each or all accounts.	
Default	0	
Web UI	Features → DND → DND Mode	

10.13.2 DND Feature Configuration

After you choose a DND mode, you can configure DND feature for all lines or a specific line. It depends on the DND mode:

- **Phone** (default): DND feature is effective for all lines.
- **Custom**: DND feature can be configured for a specific line or multiple lines.

The IP phones also support 2 methods to activate and deactivate server-side DND feature. They may vary on different servers.

- **Prefix mode:** (default) The IP phone will send on code or off code to synchronize the status of the DND between the IP phone and the server.
- **Subscribe mode:** The IP phone will send subscribe message to synchronize the status of the DND between the IP phone and the server when forward states change. With this phone, you don't need to configure on code or off code on IP phone.

10.13.3 DND in Phone Mode Configuration

The following table lists the parameters you can use to configure DND in Phone mode.

Parameter	**FeatureDndEnable**	**config.xml**
Description	It turns on or off the DND feature. **Note:** It works only if "FeatureDndMode" is set to 0 (Phone).	
Permitted Values	false - disable true - enable: The IP phone will reject incoming calls on all accounts.	
Default	false	
Web UI	Features → DND → Enable DND	
Phone UI	Menu → Features → DND	
Parameter	**FeatureDndOnCode**	**config.xml**
Description	It configures the DND on code to activate the server-side DND feature. The IP phone will send the DND on code to the server when you activate DND feature on the IP phone. **Note:** It works only if "FeatureDndMode" is set to 0 (Phone).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → DND → On Code	
Phone UI	Menu → Features → DND → On Code	
Parameter	**FeatureDndOffCode**	**config.xml**
Description	It configures the DND off code to deactivate the server-side DND feature. The IP phone will send the DND off code to the server when you deactivate DND feature on the IP phone. **Note:** It works only if "FeatureDndMode" is set to 0 (Phone).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → DND → Off Code	
Phone UI	Menu → Features → DND → Off Code	

10.13.4 DND in Custom Mode Configuration

The following table lists the parameters you can use to configure DND in Custom mode.

Note: X means account ID. It can be number 1~8 for M3/M5/M7, and 1-20 for M8.

Parameter	**AccountXDndEnable**	**config.xml**
Description	It turns on or off the DND feature. **Note:** It works only if “FeatureDndMode” is set totrue1 (Custom).	
Permitted Values	false - disable true - enable: The IP phone will reject incoming calls on all accounts.	
Default	false	
Web UI	Features → DND → Account ID → Enable DND	
Phone UI	Menu → Features → DND → Account ID → DND Status	
Parameter	**AccountXDndOnCode**	**config.xml**
Description	It configures the DND on code to activate the server-side DND feature. The IP phone will send the DND on code to the server when you activate DND feature on the IP phone. **Note:** It works only if “FeatureDndMode” and “FeatureDndEnable2” are both set to 1 (Custom).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → DND → Account ID → On Code	
Phone UI	Menu → Features → DND → Account ID → On Code	
Parameter	**AccountXDndOffCode**	**config.xml**
Description	It configures the DND off code to deactivate the server-side DND feature. The IP phone will send the DND off code to the server when you deactivate DND feature on the IP phone. **Note:** It works only if “FeatureDndMode” set to 1 (Custom) and “FeatureDndEnable2” set to false.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → DND → Account ID → Off Code	
Phone UI	Menu → Features → DND → Account ID → Off Code	

10.13.5 DND Synchronization for Server-side Configuration

DND synchronization feature provides the capability to synchronize the status of the DND features between the IP phone and the server.

If the DND is activated in Phone mode, the DND status changing locally will be synchronized to registered default accounts on the server.

If the DND is activated in Custom mode, the DND status changing locally will be synchronized to the specific accounts on the server.

The IP phone support 2 methods to synchronize the status of the DND between the IP phone and the server.

Prefix mode:

The IP phone will send on code or off code to synchronize the status of the DND between the IP phone and the server.

Subscribe mode:

The IP phone will send subscribe message to synchronize the status of the DND between the IP phone and the server when forward states change.

With Subscribe mode the IP phone don't need config on code or off code.

The following table lists the parameters you can use to configure DND synchronization for the server side.

Note: X means account ID. It can be number 1~8 for M3/M5/M7, and 1-20 for M8.

Parameter	**FeatureDNDMethod**	**config.xml**
Description	It configures the DND method for the IP phone. **Note:** It works only if "DNDModeAccount" is set to 0 (Phone).	
Permitted Values	0: Prefix 1: Subscribe. The IP phone sends a SUBSCRIBE message with event "as-feature-event" to the server.	
Default	0	
Web UI	Features → DND → DND method	
Parameter	**AccountXDndMethod**	**config.xml**
Description	It configures the DND method for the IP phone accountX. **Note:** It works only if "DNDModeAccount" is set to 1 (Custom).	
Permitted Values	0: Prefix 1: Subscribe. The IP phone sends a SUBSCRIBE message with event "as-feature-event" to the server.	
Default	0	
Web UI	Features → DND → DND method	

10.13.6 DND Enable/Disable Prompt Enhancement

The following table lists the parameters you can use to configure DND enable/disable prompt enhancement.

Parameter	**FeatureDNDPromptMode**	**config.xml**
Description	It enables or disables the IP phone to display a large DND icon on the idle screen. **Note:** It works only if "FeatureDNDPromptMode" is set to 1 (Enabled).	
Permitted Values	0 - default mode 1 - strong prompt mode	
Default	0	

10.14 Call Forward

You can forward calls from any line on your phone to a contact. There are two ways of forwarding your calls:

- Forward calls in special situations, such as when the phone is busy or there is no answer, or forwarding all incoming calls to a contact immediately.
- Manually forward an incoming call to a number.

10.14.1 Call Forward Setting Configuration

You can change the following call forward settings:

- Choose a call forward mode. You can configure call forward for all lines (Phone mode) or specific lines (Custom mode).
- Allow or disallow users to forward an incoming call to a telephone number.

The following table lists the parameters you can use to configure DND setting.

Parameter	**FeatureFwdMode**	**config.xml**
Description	It configures the FWD mode for the IP phone.	
Permitted Values	0: Phone. Call forward feature is effective for the phone system. 1: Custom. You can configure call forward feature for each or all accounts.	
Default	0	
Web UI	Features → Forward → Forward Mode	

10.14.2 Call Forward Feature Configuration

After you choose a forward mode, you can configure call forward feature for all accounts or a specific account. It depends on the forward mode:

- **Phone** (default): Call forward feature is effective for all accounts.
- **Custom**: Call forward feature can be configured for a specific account or multiple accounts.

The IP phones also support call forward on code and off code to activate and deactivate server-side call forward feature. They may vary on different servers.

10.14.3 Call forward in Phone Mode Configuration

The following table lists the parameters you can use to configure call forward in Phone mode.

Parameter	**FeatureImmFwdEnable**	**config.xml**
Description	It triggers the always forward feature to on or off on a phone basis. **Note:** It works only if “FeatureFwdMode” is set to 0 (Phone).	
Permitted Values	false - disable true - enable: Incoming calls are forwarded to the destination number (configured by the parameter “FeatureImmFwdNumber”) immediately.	
Default	false	
Web UI	Features → Forward → Immediate FWD → On/Off	
Phone UI	Menu → Features → Call Forward → Always Forward → Always Forward	
Parameter	**FeatureImmFwdNumber**	**config.xml**
Description	It configures the destination number of the always forward on a phone basis. **Note:** It works only if “FeatureFwdMode” is set to 0 (Phone).	

Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → Forward → Immediate FWD Phone Number	
Phone UI	Menu → Features → Call Forward → Always Forward → Forward To	
Parameter	**FeatureImmFwdOnCode**	**config.xml**
Description	It configures the always forward on code to activate the server-side always forward feature. The IP phone will send the always forward on code and the pre-configured destination number (configured by the parameter “FeatureImmFwdNumber”) to the server when you activate always forward feature on a phone basis. **Note:** If default account is account 2 and the value of the parameter “FeatureFwdMode” is set to 0 (Phone).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → Forward → On Code (under Immediate FWD)	
Phone UI	Menu → Features → Call Forward → Always Forward → On Code	
Parameter	**FeatureImmFwdOffCode**	**config.xml**
Description	It configures the always forward off code to deactivate the server-side always forward feature. The IP phone will send the always forward off code to the server when you deactivate always forward feature on the IP phone. **Note:** If default account is account 2 and the value of the parameter “FeatureFwdMode” is set to 0 (Phone).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → Forward → Off Code (under Immediate FWD)	
Phone UI	Menu → Features → Call Forward → Always Forward → Off Code	
Parameter	**FeatureBusyFwdEnable**	**config.xml**
Description	It turns on or off the busy forward feature on a phone basis. **Note:** It works only if “FeatureFwdMode” is set to 0 (Phone).	
Permitted Values	false - disable true - enable: Incoming calls are forwarded to the destination number (configured by the parameter “FeatureBusyFwdNumber”) when the callee is busy.	
Default	false	
Web UI	Features → Forward → Busy FWD → On/Off	
Phone UI	Menu → Features → Call Forward → Busy Forward → Busy Forward	
Parameter	**FeatureBusyFwdNumber**	**config.xml**

Description	It configures the destination number of the busy forward feature on a phone basis. **Note:** It works only if “FeatureFwdMode” is set to 0 (Phone).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → Forward → Busy FWD Phone Number	
Phone UI	Menu → Features → Call Forward → Busy Forward → Forward To	
Parameter	**FeatureBusyFwdOnCode**	**config.xml**
Description	It configures the busy forward on code to activate the server-side busy forward feature. The IP phone will send the busy forward on code and the pre-configured destination number (configured by the parameter “FeatureBusyFwdNumber”) to the server when you activate busy forward feature on a phone basis. **Note:** It works only if “ForwardModeAccount” is set to 0 (Phone).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → Forward → On Code (under Busy FWD)	
Phone UI	Menu → Features → Call Forward → Busy Forward → On Code	
Parameter	**FeatureBusyFwdOffCode**	**config.xml**
Description	It configures the busy forward off code to deactivate the server-side busy forward feature. The IP phone will send the busy forward off code to the server when you deactivate busy forward feature on the IP phone. **Note:** It works only if “ForwardModeAccount” is set to 0 (Phone).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → Forward → Off Code(under Busy FWD)	
Phone UI	Menu → Features → Call Forward → Busy Forward → Off Code	
Parameter	**FeatureNoReplyFwdEnable**	**config.xml**
Description	It turns on or off the no answer forward feature on a phone basis. **Note:** It works only if “FeatureFwdMode” is set to 0 (Phone).	
Permitted Values	false - disable true - enable: Incoming calls are forwarded to the destination number (configured by the parameter “FeatureNoReplyFwdNumber”) after a period of ring time.	
Default	false	
Web UI	Features → Forward → No Reply FWD → On/Off	
Phone UI	Menu → Features → Call Forward → No reply Forward → No Reply Forward	
Parameter	**FeatureNoReplyFwdNumber**	**config.xml**
Description	It configures the destination number of the no answer forward feature on a phone basis. **Note:** It works only if “FeatureFwdMode” is set to 0 (Phone).	

Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → Forward → No Reply FWD Phone Number	
Phone UI	Menu → Features → Call Forward → No Reply Forward → Forward To	
Parameter	**FeatureNoReplyFwdOnCode**	**config.xml**
Description	It configures the no answer forward on code to activate the server-side no answer forward feature. The IP phone will send the no answer forward on code and the pre-configured destination number (configured by the parameter "FeatureNoReplyFwdNumber") to the server when you activate no answer forward feature on a phone basis. **Note:** If the default account is account 2, set the value of the parameter "FeatureFwdMode to 0 (Phone).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → Forward → On Code(under No Reply FWD)	
Phone UI	Menu → Features → Call Forward → No Answer Forward → On Code	
Parameter	**FeatureNoReplyFwdOffCode**	**config.xml**
Description	It configures the no answer forward off code to deactivate the server-side no answer forward feature. The IP phone will send the no answer forward off code to the server when you deactivate no answer forward feature on the IP phone. **Note:** If the default account is account 2, set the value of the parameter "FeatureFwdMode" to 0 (Phone).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → Forward → Off Code (under No Reply FWD)	
Phone UI	Menu → Features → Call Forward → No Reply Forward → Off Code	
Parameter	**FeatureNoReplyFwdDuration**	**config.xml**
Description	The incoming calls will be forwarded when not answered after M (M is configurable by "FeatureNoReplyFwdDuration") seconds.	
Permitted Values	Integer from 10 to 60	
Default	10	
Web UI	Features → Forward → Forward Duration Noreply (under No Reply FWD)	

10.14.4 Call Forward in Custom Mode Configuration

The following table lists the parameters you can use to configure call forward in Custom mode.

Note: X means account ID. It can be number 1~8 for M3/M5/M7, and 1-20 for M8.

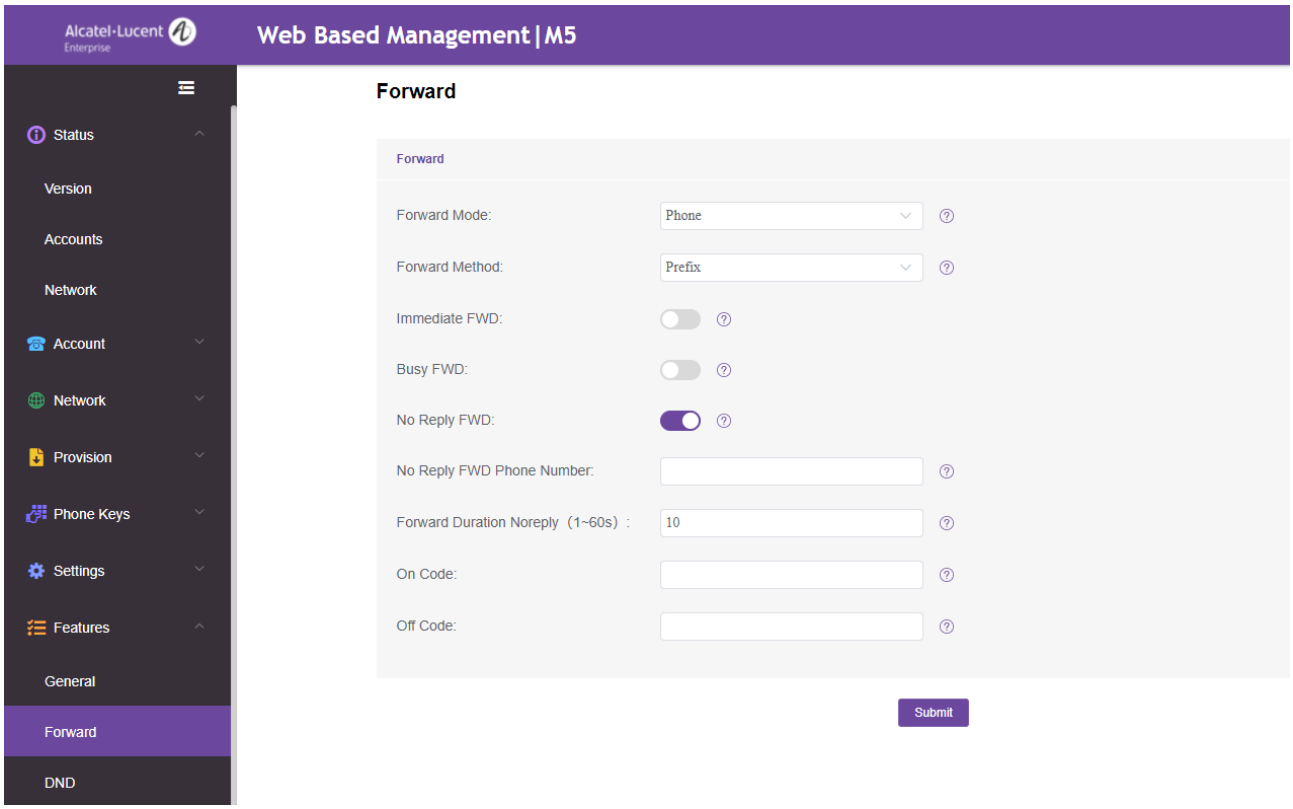
Parameter	**AccountXImmFwdEnable**	**config.xml**
Description	It triggers the always forward feature to on or off on a phone basis. **Note:** It works only if “FeatureFwdMode” is set to 1 (Custom).	
Permitted Values	false - disable true - enable: Incoming calls are forwarded to the destination number (configured by the parameter “AccountXImmFwdNumber”) immediately.	
Default	false	
Web UI	Features → Forward → Immediate FWD → On/Off	
Phone UI	Menu → Features → Call Forward → Always Forward → account ID → Always Forward	
Parameter	**AccountXImmFwdNumber**	**config.xml**
Description	It configures the destination number of the always forward feature on a phone basis. **Note:** It works only if “FeatureFwdMode” is set to 1 (Custom).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → Forward → Immediate FWD Phone Number	
Phone UI	Menu → Features → Call Forward → Always Forward → account ID → Forward To	
Parameter	**AccountXImmFwdOnCode**	**config.xml**
Description	It configures the always forward on code to activate the server-side always forward feature. The IP phone will send the always forward on code and the pre-configured destination number (configured by the parameter “AccountXImmFwdNumber”) to the server when you activate always forward feature on a phone basis. **Note:** It work only if “FeatureFwdMode” is set to 1 (Custom).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → Forward → On Code(under Immediate FWD)	
Phone UI	Menu → Features → Call Forward → Always Forward → account ID → On Code	
Parameter	**AccountXImmFwdOffCode**	**config.xml**
Description	It configures the always forward off code to deactivate the server-side always forward feature. The IP phone will send the always forward off code to the server when you deactivate always forward feature on the IP phone. **Note:** It work only if “FeatureFwdMode” is set to 1 (Custom).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → Forward → Off Code (under Immediate FWD)	
Phone UI	Menu → Features → Call Forward → Always Forward → account ID → Off Code	

Parameter	**AccountXBusyFwdEnable**	**config.xml**
Description	It turns on or off the busy forward feature on a phone basis. **Note:** It work only if “FeatureFwdMode” is set to 1 (Custom).	
Permitted Values	false - disable true - enable: Incoming calls are forwarded to the destination number (configured by the parameter “AccountXBusyFwdNumber”) when the callee is busy.	
Default	false	
Web UI	Features → Forward → Busy FWD → On/Off	
Phone UI	Menu → Features → Call Forward → Busy Forward → account ID → Busy Forward	
Parameter	**AccountXBusyFwdNumber**	**config.xml**
Description	It configures the destination number of the busy forward feature on a phone basis. **Note:** It work only if “FeatureFwdMode” is set to 1 (Custom).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → Forward → Busy FWD Phone Number	
Phone UI	Menu → Features → Call Forward → Busy Forward → account ID → Forward To	
Parameter	**AccountXBusyFwdOnCode**	**config.xml**
Description	It configures the busy forward on code to activate the server-side busy forward feature. The IP phone will send the busy forward on code and the pre-configured destination number (configured by the parameter “AccountXBusyFwdNumber”) to the server when you activate busy forward feature on a phone basis. **Note:** It work only if “FeatureFwdMode” is set to 1 (Custom).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → Forward → On Code (under Busy FWD)	
Phone UI	Menu → Features → Call Forward → Busy Forward → account ID → On Code	
Parameter	**AccountXBusyFwdOffCode**	**config.xml**
Description	It configures the busy forward off code to deactivate the server-side busy forward feature. The IP phone will send the busy forward off code to the server when you deactivate busy forward feature on the IP phone. **Note:** It work only if “FeatureFwdMode” is set to 1 (Custom).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → Forward → Off Code (under Busy FWD)	
Phone UI	Menu → Features → Call Forward → Busy Forward → account ID → Off Code	
Parameter	**AccountXNoReplyFwdEnable**	**config.xml**

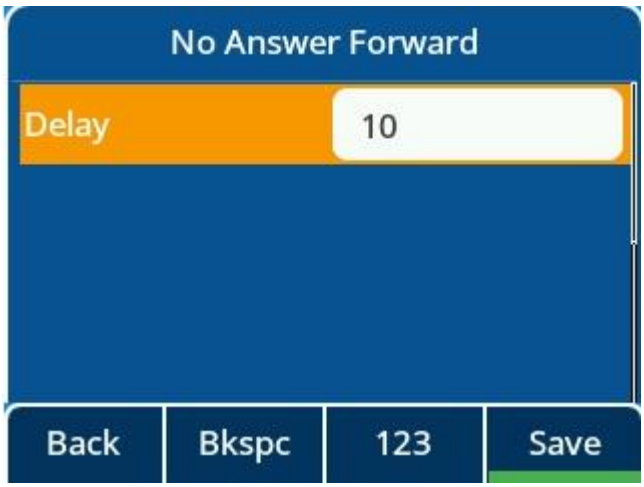
Description	It turns on or off the no answer forward feature on a phone basis. **Note:** It work only if “FeatureFwdMode” is set to 1 (Custom).	
Permitted Values	false - disable true - enable: Incoming calls are forwarded to the destination number (configured by the parameter “AccountXNoReplyFwdNumber”) after a period of ring time.	
Default	false	
Web UI	Features → Forward → No Reply FWD → On/Off	
Phone UI	Menu → Features → Call Forward → No reply Forward → account ID → No Reply Forward	
Parameter	**AccountXNoReplyFwdNumber**	**config.xml**
Description	It configures the destination number of the no answer forward feature on a phone basis. **Note:** It work only if “FeatureFwdMode” is set to 1 (Custom).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → Forward → No Reply FWD Phone Number	
Phone UI	Menu → Features → Call Forward → No Reply Forward → account ID → Forward To	
Parameter	**AccountXNoReplyFwdOnCode**	**config.xml**
Description	It configures the no answer forward on code to activate the server-side no answer forward feature. The IP phone will send the no answer forward on code and the pre-configured destination number (configured by the parameter “AccountXNoReplyFwdNumber”) to the server when you activate no answer forward feature on a phone basis. **Note:** It work only if “FeatureFwdMode” is set to 1 (Custom).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → Forward → On Code(under No Reply FWD)	
Phone UI	Menu → Features → Call Forward → No Answer Forward → account ID → On Code	
Parameter	**AccountXNoReplyFwdOffCode**	**config.xml**
Description	It configures the no answer forward off code to deactivate the server-side no answer forward feature. The IP phone will send the no answer forward off code to the server when you deactivate no answer forward feature on the IP phone. **Note:** It work only if “FeatureFwdMode” is set to 1 (Custom).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → Forward → Off Code (under No Reply FWD)	
Phone UI	Menu → Features → Call Forward → No Reply Forward → account ID → Off Code	

You can configure the no reply forward waiting time via web or Phone UI.

- Configure no reply forward time via web



- Configure no reply time via Phone UI



10.14.5 Call Forward Synchronization for Server-side Configuration

Call forward synchronization feature provides the capability to synchronize the status of the call forward features between the IP phone and the server.

If the call forward is activated in phone mode, the forward status changing locally will be synchronized to registered default accounts on the server.

If the call forward is activated in custom mode, the forward status changing locally will be synchronized to the specific accounts on the server. But if the forward status of the specific account is changed on the server, the forward status locally will be changed.

The IP phone support 2 methods to synchronize the status of the call forward between the IP phone and the server.

Prefix mode:

The IP phone will send on code or off code to synchronize the status of the call forward between the IP phone and the server.

Subscribe mode:

The IP phone will send subscribe message to synchronize the status of the call forward between the IP phone and the server when forward states change.

The following table lists the parameters you can use to configure call forward synchronization for server-side.

Note: X means account ID and it can be number 1~8 for M3/M5/M7, and 1-20 for M8.

Parameter	**FeatureFwdMethod**	**config.xml**
Description	It configures the FWD method for the IP phone. **Note:** It works only if “FeatureFwdMode” is set to 0 (Phone).	
Permitted Values	0 - Prefix 1 - Subscribe, the IP phone send a SUBSCRIBE message with event “as-feature-event” to the server.	
Default	0	
Web UI	Features → Forward → Forward method	
Parameter	**AccountXFwdMethod**	**config.xml**
Description	It configures the FWD method for the IP phone account X. **Note:** It works only if “FeatureFwdMode” is set to 1 (Custom).	
Permitted Values	0: Prefix 1: Subscribe. The IP phone sends a SUBSCRIBE message with event “as-feature-event” to the server.	
Default	0	
Web UI	Features → Forward → Forward method	

10.15 DND & FWD Synchronization

After the function synchronization is enabled, the DND&FWD on the phone side and the DND&FWD on the server side can be synchronized with each other. The user can conveniently turn on or off DND&FWD on the phone side or the web page.

The following table lists the parameters you can use to configure this feature.

Note: X means account ID. It can be number 1~8 for M3/M5/M7, and 1-20 for M8.

Parameter	**AccountXDndSyncServerLocalProcessingEnable**	**config.xml**
Description	In the case of server synchronization, it configures the phone’s each account to handle the local DND. **Note:** It only works when FeaturedDndMethod is set to 1 (Phone mode) or AccountXDndMethod is set to 1 (Custom mode).	
Permitted Values	false - disable true - enable	
Default	false	
Parameter	**AccountXDndShareLineSyncServerEnable**	**config.xml**

Description	It configures shared line account DND sync. **Note:** Only works when FeaturedDndMethod = 1 (Phone mode) or AccountXDndMethod = 1 (Custom mode).	
Permitted Values	false - disable true - enable	
Default	true	
Parameter	**AccountXFwdSyncServerLocalProcessingEnable**	**config.xml**
Description	It configures share line account Forward sync. **Note:** It only works when FeatureFwdMethod = 1 (Phone mode) or Account[1-8]FwdMethod = 1 (Custom mode).	
Permitted Values	false - disable true - enable	
Default	false	

10.16 Multiple Call Appearances

You can enable each registered line to support multiple concurrent calls. For example, you can place one call on hold, switch to another call on the same registered line, and have both calls displayed.

You can set the maximum number of concurrent calls per line key on all-lines basis or a per-line basis. For example, if you specify 3 concurrent-calls for account 1, you can only have three call appearances on a corresponding line key. The additional incoming calls will be rejected.

You can specify the maximum concurrent-call numbers per line key.

The following table lists the parameters you can use to configure multiple call appearances.

Parameter	**SIPMaxCall**	**config.xml**
Description	It configures the maximum number of concurrent calls for all registered accounts.	
Permitted Values	NUMERIC [1,4] **Note**: For M8, the permitted value for this parameter is NUMERIC [1,11].	
Default	2 **Note**: For M8, the default value for this parameter is 11.	
Web UI	Features → SIP → SIP MAX Call	

10.17 Call Hold

Call hold provides a service of placing an active call on hold. It enables you to pause activity on an active call so that you can use the phone for another task, for example, to place or receive another call.

When a call is placed on hold, the IP phones send an INVITE request with HOLD SDP to request remote parties to stop sending media and to inform them that they are being held. The IP phones support two call hold methods. One is RFC 3264, which has the “a” (media attribute) in the SDP to sendonly, recvonly or inactive (for example, a=sendonly). The other is RFC 2543, which has the “c” (connection addresses for the media streams) in the SDP to zero (for example, c=0.0.0.0).

When you place an active call on hold or the call is held by remote party, a call hold tone or held tone alerts you after a specific period of time that a call is still on hold or is still held by the remote party. You can configure the call hold tone and held tone.

10.17.1 Call Hold Configuration

The following table lists the parameters you can use to configure Call Hold.

Parameter	**SIPRfc2543HoldEnable**	**config.xml**
Description	It enables or disables the IP phone to use RFC 2543 (c=0.0.0.0) outgoing hold signaling.	
Permitted Values	False - SDP media direction attributes (such as a=sendonly) per RFC 3264 is used when placing a call on hold. True - SDP media connection address c=0.0.0.0 per RFC 2543 is used when placing a call on hold.	
Default	false	
Web UI	Features → SIP → RFC2543 Hold Enable	
Parameter	**AudioCHoldTone**	**config.xml**
Description	It configures the tone for the IP phone to play the initial call hold tone.	
Permitted Values	LIST[NUMERIC[-60,*],8,74]	
Default	0;4;-1;200;420;335;-37;-37;-1;200;0;0;0;0;-1;200;420;335;-37;-37;-1;5000;0;0;0;0	
Parameter	**FeatureHoldUseInactiveEnable**	**config.xml**
Description	It enables or disables the phone to inactive outgoing hold signaling.	
Permitted Values	false - disable true - enable	
Default	false	
Parameter	**FeaturePlayHoldToneEnable**	**config.xml**
Description	It enables or disables the IP phone to play the call hold tone when you place a call on hold.	
Permitted Values	false - disable true - enable	
Default	true	
Parameter	**FeaturePlayHoldToneDelay**	**config.xml**
Description	It configures the time (in seconds) to wait for the IP phone to play the initial call hold tone. If it is set to 30 (30s), the IP phone will wait 30 seconds to play the initial call hold tone after you place a call on hold. **Note:** It works only if “FeaturePlayHoldToneEnable” is set to true (Enabled).	
Permitted Values	Integer from 3 to 3600	
Default	30	
Parameter	**FeaturePlayHoldToneInterval**	**config.xml**
Description	It configures the time (in seconds) between subsequent call hold tones. If it is set to 3 (3s) and “FeaturePlayHoldToneDelay” is set to 30 (30s), the IP phone will begin to play a hold tone after you place a call on hold for 30 seconds, and repeat the call hold tone every 3 seconds.	

	Note: It works only if “FeaturePlayHoldToneEnable” is set to true (Enabled).	
Permitted Values	Integer from 3 to 3600	
Default	30	
Parameter	**FeaturePlayHeldToneEnable**	**config.xml**
Description	It enables or disables the IP phone to play the call held tone when a call is held by the other party.	
Permitted Values	false - disabled true - enabled	
Default	false	
Parameter	**FeaturePlayHeldToneDelay**	**config.xml**
Description	It configures the time (in seconds) to wait for the IP phone to play the initial call held tone. If it is set to 30 (30s), the IP phone will wait 30 seconds to play the initial call held tone after you are held by the other party. **Note:** It works only if the Music on Hold feature is disabled and “FeaturePlayHeldToneEnable” is set to true (Enabled).	
Permitted Values	Integer from 3 to 3600	
Default	30	
Parameter	**FeaturePlayHeldToneInterval**	**config.xml**
Description	It configures the time (in seconds) between subsequent call held tones. If it is set to 3 (3s) and “FeaturePlayHeldToneDelay” is set to 30 (30s), the IP phone will begin to play a held tone after a call is held by the other party for 30 seconds, and repeat the call held tone every 3 seconds. **Note:** It works only if the Music on Hold feature is disabled and “FeaturePlayHeldToneEnable” is set to true (Enabled).	
Permitted Values	Integer from 3 to 3600	
Default	30	

10.17.2 Music on Hold

When a call is placed on hold, the IP phone will send an INVITE message to the specified MoH server account according to the SIP URI. The MoH server account automatically responds to the INVITE message and immediately plays audio from some source located anywhere (LAN, Internet) to the held party. For more information, refer to RFC worley-service-example.

10.17.3 How to Hold call

When party A is in an active call with party B, party A can Hold this call by pressing “Hold”. Then, party B will be held on. Party A can resume this call by pressing “Retrieve”.

10.18 Call Mute

You can mute the microphone of the active audio device (handset, headset or speakerphone) on ALE phones during an active call or when the phone is on the calling/ringing screen. The call is automatically muted when setting up successfully. Muting before a call is answered prevents the other party from hearing local discussion. You can activate the mute feature by pressing the MUTE key.

Normally, the mute feature is automatically deactivated when the active call ends. You can use keep mute feature to keep the mute state persisting across the calls. In a call center or meet room, if incoming calls are answered automatically, the callers may hear the local discussion. Therefore, you can mute the phone in an idle state to prevent the unintended situation. The mute state persists across calls until you unmute the microphone manually or until the phone restarts. You can activate the mute feature by pressing the MUTE key in idle/ dial/ringing/calling/talking state.

The following table lists the parameter you can use to enable or disable keep mute.

Parameter	**FeatureKeepMuteEnable**	**config.xml**
Description	It configures the keep mute feature for the IP phone.	
Permitted Values	false - disable true - enable	
Default	false	

10.19 Call Transfer

Call transfer enables the IP phones to transfer an existing call to a third party. For example, if party A is in an active call with party B, party A can transfer this call to party C (the third party). Then, party B will begin a new call with party C, and party A will disconnect.

The ALE Myriad Series phones support call transfer using the REFER method specified in RFC 3515 and offer two types of transfer:

- **Blind Transfer** - Transfer a call directly to another party without consulting. Blind transfer is implemented by a simple REFER method without Replaces in the Refer-To header.
- **Attended Transfer (Consultative Transfer)** - Transfer a call with prior consulting. Attended transfer is implemented by a REFER method with Replaces in the Refer-To header.

10.19.1 Call Transfer Configuration

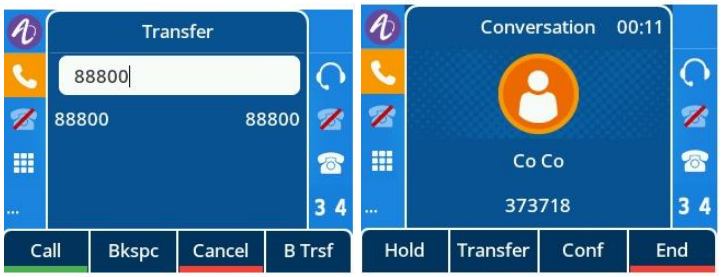
The following table lists the parameters you can use to configure call transfer.

Parameter	**TelephonyTransferAllowed**	**config.xml**
Description	It enables or disables the transfer feature of the IP phone.	

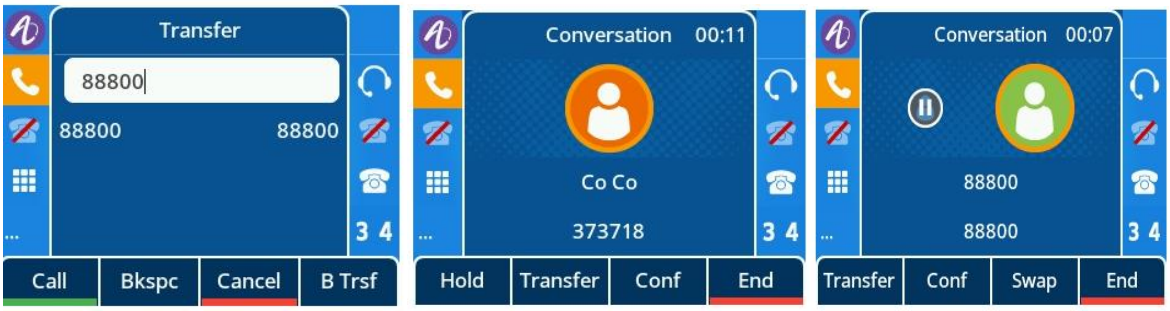
Permitted Values	false - disable true - enable	
Default	true	
Parameter	**TelephonyBlindTransferAllowed**	**config.xml**
Description	It enables or disables the blind transfer.	
Permitted Values	false - disable true - enable	
Default	true	

10.19.2 How to Make a Transfer Call

- **Blind Transfer call**: When in an active call with party B, party A presses “Transfer” to input party C Number, and then party A can transfer this call to party C (the third party) by pressing “B Trsf”. Party B will begin a new call with party C, and party A will disconnect.



- **Consultative Transfer call**: When in an active call with party B, party A presses “Transfer” to input party C Number, and party A will begin a new call with party C by pressing “Call”. Then, party A can transfer this call to party B (the third party) by pressing “Transfer”, and party A will disconnect.



10.19.3 Transfer Mode Configuration for Programmable Key

You can configure the transfer mode for the IP phone when transferring the current call via a specified programmable key. The ALE Myriad Series phones support the transfer modes: New Call, Blind Transfer.

The following table lists the parameter you can use to configure the transfer mode for a programmable key.

Parameter	**FeatureTransferKeyAsBlindTransferEnable**	**config.xml**
Description	It configures the transfer mode for a programmable key. When the user presses the DSS Key during a call, the programmable key behavior depends on the transfer mode.	
Permitted Values	false - disable true - enable	
Default	false	

10.20 Conference

The ALE Myriad Series phones support three-way local conference and multi-way network conference.

10.20.1 Local Conference Configuration

The local conference requires a host phone to process the audio of all parties. The ALE Myriad Series phones support up to 3 parties (5 parties for the M7 IP phone) (12 parties for the M8 IP phone) (including yourself) in a local conference call.

You can enable or disable the local conference feature and configure the way to set up a local conference.

For the ALE Myriad Series deskphones, you can merge two calls into a conference directly by pressing the Conf soft key or Conf hard key.

For a local three-way conference, if the conference initiator leaves the conference, all parties are disconnected and the conference call ends. You can enable Transfer on Conference Hang Up feature and allow the other two parties to remain connected when the conference initiator drops the conference call.

The following table lists the parameters you can use to configure local conference.

Note: X means account ID. It can be number 1~8 for M3/M5/M7, and 1-20 for M8.

Parameter	**AccountXLocalConfEnable**	**config.xml**
Description	It enables or disables the local conference feature of the IP phone.	
Permitted Values	false - disable true - enable	
Default	true	
Web UI	Features → SIP → Local Conference Enable	

10.20.1.1 Transfer on Conference

You can enable Transfer on Conference Hang Up feature and allow the other two parties to remain connected when the conference initiator drops the conference call.

10.20.2 Network Conference Configuration

Network conference, also known as a centralized conference, provides you with the flexibility of call with multiple participants (more than three). The IP phones implement network conference using the REFER method specified in RFC 4579. This feature depends on the support from a SIP server.

For network conference, if any party leaves the conference, the remaining parties are still connected.

The following table lists the parameter you can use to configure network conference.

Note: X means account ID. It can be number 1~8 for M3/M5/M7, and 1-20 for M8.

Parameter	AccountXNConfUri	config.xml
Description	It configures the network conference URI for a specific account. **Note:** Network conference URI takes effect only when local conference is set to false.	
Permitted Values	TEXT	
Default	Blank	
Web UI	Account → Advanced → N-conference URI	

10.21 Keep Mute

The user can mute the phone in an idle state to prevent the unintended situation. The mute state remains during the calls until the user unmutes the microphone manually or until the phone restarts.

The following table lists the parameter you can use to enable or disable Keep Mute.

Parameter	FeatureKeepMuteEnable	config.xml
Description	It configures the Keep Mute feature of the IP phone.	
Permitted Values	false - disable true - enable	
Default	false	

10.22 Auto Redial

You can configure the phone to automatically redial the last dialed number when the call is temporarily unavailable. Both the number of attempts and waiting time between redials are configurable.

The following table lists the parameters you can use to configure auto redial.

Parameter	FeatureAutoRedialEnable	config.xml
Description	It enables or disables the IP phone to automatically redial the last dialed number when the callee is temporarily unavailable.	
Permitted Values	false - disable true - enable	
Default	false	
Web UI	Features → General → Auto Redial	
Phone UI	Menu → Features → Auto Redial	
Parameter	FeatureAutoRedialTimes	config.xml
Description	It configures the interval (in seconds) for the IP phone to wait between redials. The IP phone redials the last dialed number at regular intervals till the callee answers the call.	
Permitted Values	Integer from 1 to 10	
Default	5	
Web UI	Features → General → Auto Redial Times (1~10)	
Phone UI	Menu → Features → Auto Redial	

Parameter	**FeatureAutoRedialInterval** **Note:** This feature is only for Myriad phones.	**config.xml**
Description	It configures the auto redial times when the callee is temporarily unavailable. The IP phone tries to redial the callee as many times as configured till the callee answers the call.	
Permitted Values	Integer from 1 to 60	
Default	10	
Web UI	Features → General → Auto Redial Interval (1~60s)	
Phone UI	Menu → Features → Auto Redial	

10.23 USB Recording

ALE phones support manual recording during a call or automatic recording once the call is set up. Before recording, ensure that the USB disk has been connected to the IP phone.

Parameter	**FeatureUsbCallRecordingEnable**	**config.xml**
Description	It enables or disables the call recording (using a USB flash drive) feature of the IP phone.	
Permitted Values	false - disable true - enable	
Default	false	
Parameter	**FeatureAutoRecordingEnable**	**config.xml**
Description	It enables or disables the automatic recording feature of the IP phone.	
Permitted Values	false - disable true - enable	
Default	false	

10.24 Confidential Dial

Password dial feature allows the callee number to be partially displayed on the IP phone when placing a call. The hidden digits are displayed as asterisks on the phone screen. The number in the placed call list is also partially displayed on the IP phone. This feature is especially useful for users who often place important and confidential calls.

The following table lists the parameters you can use to configure password dial.

Parameter	**FeatureConfidentialDialEnable**	**config.xml**
Description	It configures whether to enable or disable the password dial feature.	
Permitted Values	false - disable true - enable	
Default	false	
Web UI	Setting → General → Confidential Dial Enable	
Parameter	**FeatureConfidentialDialPrefix**	**config.xml**
Description	It configures the prefix of the number that needs to be partially displayed.	

Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → General → Confidential Dial Prefix	
Parameter	**FeatureConfidentialDialLength**	**config.xml**
Description	It configures how many digits need to be displayed as asterisks.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → General → Confidential Dial Length (0-32)	

10.25 Multicast Paging

Multicast Paging allows you to easily and quickly broadcast instant audio announcements to users who are listening to a specific multicast group on a specific channel.

The ALE Myriad Series phones support the following 25 channels:

1 to 25: Broadcasts are sent to channel 1 to 25.

The IP phones can only send and receive broadcasts to/from the listened channels. Other channels' broadcasts will be ignored automatically by the IP phone.

10.25.1 Multicast Paging Group Configuration

The ALE Myriad Series phones support up to 25 groups for paging. You can assign multicast IP address with a channel for each group, and specify a label to each group to identify the phones in the group, such as All, Sales, or HR.

Tip: You can set a Program key as Multicast Paging key or Paging list key on the phone, which allows you to send announcements to the phones with the pre-configured multicast address(es) on the specific channel(s). For more information

The following table lists the parameters you can use to configure a multicast paging group.

Parameter	**MulticastPagingAddress[1-25]**	**config.xml**
Description	It configures the IP address and port number of the multicast paging group in the paging list.	
Permitted Values	IP address: port (224.0.0.1-239.255.255.255 port: 1-65535)	
Default	Blank	
Web UI	Features → Multicast Paging → Paging List	
Parameter	**MulticastPagingAddress[1-25]Label**	**config.xml**
Description	It configures the name of the multicast paging group to be displayed in the paging list. It will be displayed on the phone screen when placing the multicast paging calls.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Features → Multicast Paging → Paging List	

Parameter	MulticastPagingAddress[1-25]Channel	config.xml
Description	It configures the channel of the multicast paging group in the paging list.	
Permitted Values	1-25	
Default	1	
Web UI	Features → Multicast Paging → Paging List	

10.25.2 Multicast Listening Group Configuration

The ALE Myriad Series phones support up to 25 groups for listening. You can assign multicast IP address with a channel for each group, and specify a label to each group to identify the phones in the group, such as All, Sales, or HR.

The following table lists the parameters you can use to configure the multicast listening group.

Parameter	MulticastListeningAddress[1-25]	config.xml
Description	It configures the multicast address and port number that the phone listens to.	
Permitted Values	IP address: port (224.0.0.1-239.255.255.255 port: 1-65535)	
Default	Blank	
Web UI	Features → Multicast Paging → Listening List	
Parameter	MulticastListeningAddress[1-25]Label	config.xml
Description	It configures the label to be displayed on the phone screen when receiving the multicast paging calls.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Features → Multicast Paging → Listening List	
Parameter	MulticastListeningAddress[1-25]Channel	config.xml
Description	It configures the channel that the phone listens to.	
Permitted Values	1-25	
Default	1	
Web UI	Features → Multicast Paging → Listening List	

10.25.3 Multicast Paging Settings

You can configure some general settings for multicast paging, for example, specify a codec, and configure the volume and audio device for listening to a paging call.

By default, all the listening groups are considered with a certain priority from 1 (lower priority) to 25 (higher priority).If you neither want to receive some paging calls nor miss urgent paging calls when there is a voice call or paging call, or when DND is activated, you can use the priority to define how your phone handles different incoming paging calls.

Paging Barge

You can set your phone whether an incoming paging call interrupts an active call.

The Paging Barge defines the lowest priority of the paging group from which the phone can receive a paging call when there is a voice call (a normal phone call rather than a multicast paging call) in progress. You can specify a priority that the incoming paging calls with higher or equal priority are automatically answered, and the lower ones are ignored.

If it is disabled, all incoming paging calls will be automatically ignored.

Paging Priority

You can set your phone whether a new incoming paging call interrupts a current paging call.

The Paging Priority feature decides how the phone handles incoming paging calls when there is already a paging call on the phone. If enabled, the phone will ignore incoming paging calls with lower priorities, otherwise, the phone will answer incoming paging calls automatically and place the previous paging call on hold. If disabled, the phone will automatically ignore all incoming paging calls.

DND for Ignoring Paging Call

If you do not want to miss some urgent paging calls when DND is activated. You can use the Ignore DND feature to define the lowest priority of paging group from which the phone can receive an urgent paging call when DND is activated. You can specify a priority that the incoming paging calls with higher or equal priority are automatically answered, and the lower ones are ignored.

If it is disabled, all the incoming paging calls will be ignored when DND is activated in phone mode.

The following table lists the parameters you can use to change multicast paging settings.

Parameter	**MulticastCodec**	**config.xml**
Description	It configures the codec for multicast paging.	
Permitted Values	0 - PCMU mulaw 8 - PCMA alaw 9 - G722 18 - G729	
Default	9	
Web UI	Features → Multicast Paging → Multicast Paging Codec	
Parameter	**MulticastReceiveCallBargePriority**	**config.xml**
Description	It configures the priority of the voice call (a normal phone call rather than a multicast paging call) in progress.	
Permitted Values	0-25	
Default	0	
Web UI	Features → Multicast Paging → Paging Barge	
Parameter	**MulticastReceiveIgnoreDndPriority**	**config.xml**

Description	It configures the lowest priority of the multicast paging call that can be received when DND is activated in phone mode.	
Permitted Values	0-25	
Default	0	
Web UI	Features → Multicast Paging → Ignore Dnd	
Parameter	**MulticastReceivePriorityEnable**	**config.xml**
Description	It enables or disables the phone to handle the incoming multicast paging calls when there is an active multicast paging call on the phone.	
Permitted Values	false - disable true - enable	
Default	true	
Web UI	Features → Multicast Paging → Paging Priority	
Parameter	**MulticastReceiveUseHandfree**	**config.xml**
Description	It enables or disables the phone to always use the speaker as the audio device when receiving the multicast paging calls.	
Permitted Values	false - disable true - enable	
Default	false	
Parameter	**MulticastPagingAutoResumeEnable**	**config.xml**
Description	It enables or disables the phone to automatically resume the held multicast paging call after the second multicast paging call or a new call ends.	
Permitted Values	false - disable true - enable	
Default	false	
Parameter	**MulticastPagingCallId**	**config.xml**
Description	Configure the Call ID to use for Multicast Paging	
Permitted Values	String within 13 characters	
Default	Pegasus	

10.26 Action URL

Action URL allows IP phones to interact with web server applications by sending an HTTP or HTTPS GET request.

You can specify a URL that triggers a GET request when a specified event occurs. Action URL can only be triggered by the pre-defined events (for example, Open DND). The valid URL format is: http(s)://IP address of the server/help.xml?.

An HTTP or HTTPS GET request may contain a variable name and a variable value, separated by “=”. Each variable value starts with $ in the query part of the URL. The valid URL format is: http(s)://IP address of server/help.xml?variable namee=$ variable value. The variable name can be customized by users, while the

variable value is pre-defined. For example, a URL “http://192.168.1.10/help.xml?mac=$mac” is specified for the event Mute, $mac will be dynamically replaced with the MAC address of the IP phone when the IP phone mutes a call.

10.26.1 Pre-defined Events List

The following table lists the pre-defined events for action URL.

Event	Description
Setup Completed	When the IP phone completes startup.
Register Succeeded	When the IP phone successfully registers an account.
Unregistered	When the IP phone logs out of the registered account.
Register Failed	When the IP phone fails to register an account.
Off Hook	When the IP phone is off hook.
On Hook	When the IP phone is on hook.
Incoming Call	When the IP phone receives an incoming call.
Reject Incoming Call	When the IP phone rejects an incoming call.
Answer Incoming Call	When the IP phone answers a new call.
Outgoing Call	When the IP phone places a call.
Cancel Outgoing Call	When the phone cancels an outgoing call in the ring-back state.
Remote Busy	When an outgoing call is rejected.
Call Remote Canceled	When the remote party cancels the outgoing call in the ringing state.
Missed Call	When the IP phone misses a call.
Call Established	When the IP phone establishes a call.
Call Terminated	When the IP phone terminates a call.
DND Enabled	When the IP phone enables the DND mode. **Note:** When the DND mode is Phone, the phone sends the action URL for all accounts; When the DND mode is Custom, the phone only sends the action URL for the corresponding account.
DND Disabled	When the IP phone disables the DND mode. **Note:** When the DND mode is Phone, the phone sends the action URL for all accounts; When the DND mode is Custom, the phone only sends the action URL for the corresponding account.
Immediate Forward Enabled	When the IP phone enables the always forward. **Note:** When the forward mode is Phone, the phone sends the action URL for all accounts; When the forward mode is Custom, the phone only sends the action URL for the corresponding account.
Immediate Forward Disabled	When the IP phone disables the always forward.

	Note: When the forward mode is Phone, the phone sends the action URL for all accounts; When the forward mode is Custom, the phone only sends the action URL for the corresponding account.
Busy Forward Enabled	When the IP phone enables the busy forward. **Note:** When the forward mode is Phone, the phone sends the action URL for all accounts; When the forward mode is Custom, the phone only sends the action URL for the corresponding account.
Busy Forward Disabled	When the IP phone disables the busy forward. **Note:** When the forward mode is Phone, the phone sends the action URL for all accounts; When the forward mode is Custom, the phone only sends the action URL for the corresponding account.
No Reply Forward Enabled	When the IP phone enables the no answer forward. **Note:** When the forward mode is Phone, the phone sends the action URL for all accounts; when the forward mode is Custom, the phone only sends the action URL for the corresponding account.
No Reply Forward Disabled	When the IP phone disables the no answer forward. **Note:** When the forward mode is Phone, the phone sends the action URL for all accounts; When the forward mode is Custom, the phone only sends the action URL for the corresponding account.
Forward Incoming Call	When the IP phone forwards an incoming call.
Call Transfer	When the IP phone transfers a call.
Blind Transfer	When the IP phone performs the blind transfer.
Attended Transfer	When the IP phone performs the semi-attended/attended transfer.
Transfer Failed	When the IP phone fails to transfer a call.
Transfer Failed	When the IP phone completes transferring a call.
Call Waiting Enabled	When the IP phone enables the call waiting.
Call Waiting Enabled	When the IP phone disables the call waiting.
Call Hold	When the IP phone places a call on hold.
Call Resume	When the IP phone resumes a held call.
Mute	When the IP phone mutes a call.
UnMute	When the IP phone un-mutes a call.
IP Changed	When the IP address of the IP phone changes.
Idle To Busy	When the state of the IP phone changes from idle to busy.
Busy To Idle	When the state of phone changes from busy to idle.
Autop Start	When the IP phone starts auto provisioning.

Autop Finish	When the IP phone completes auto provisioning via power on.
Headset	When the IP phone presses the HEADSET key.
Handfree	When the IP phone presses the Speakerphone key.
Peripheral Information	When the accessory is unplugged or plugged.
VPN IP	When the phone IP address assigned by the VPN server changes.
Reboot	When the IP phone starts reboot.
Reset	When the IP phone starts reset.
Screen Active	When the IP phone screen is active.
Screen Inactive	When the IP phone screen is inactive.
Conference Established	When the IP phone establishes a conference.

10.26.2 Variable Values List

The following table lists pre-defined variable values.

Variable Value	Description
$mac	The MAC address of the IP phone.
$ip	The IP address of the IP phone.
$model	The IP phone model.
$firmware	The firmware version of the IP phone.
$active_url	The SIP URI of the current account when the IP phone places a call, receives an incoming call or establishes a call.
$active_user	The user part of the SIP URI for the current account when the IP phone places a call, receives an incoming call or establishes a call.
$active_host	The host part of the SIP URI for the current account when the IP phone places a call, receives an incoming call or establishes a call.
$local	The SIP URI of the caller when the IP phone places a call. The SIP URI of the callee when the IP phone receives an incoming call.
$remote	The SIP URI of the callee when the IP phone places a call. The SIP URI of the caller when the IP phone receives an incoming call.
$display_local	The display name of the caller when the IP phone places a call. The display name of the callee when the IP phone receives an incoming call.
$display_remote	The display name of the callee when the IP phone places a call. The display name of the caller when the IP phone receives an incoming call.

$call_id	The call-id of the active call.
$callerID	The display name of the caller when the IP phone receives an incoming call.
$calledNumber	The phone number of the callee when the IP phone places a call.
$addon_number	The number of connected Addon.
$udisk_number	The number of connected USB flash drives.
$usbheadset_number	The number of connected USB headset devices.
$vpn_ip	The phone IP address assigned by the VPN server.

10.26.3 Action URL Configuration

The following table lists the parameters you can use to configure action URL.

Parameter	**ActionUrlSetupCompleted**	**config.xml**
Description	It configures the action URL the phone sends after startup.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Setup Completed	
Parameter	**ActionUrlRegisterSucceeded**	**config.xml**
Description	It configures the action URL the phone sends after an account is registered.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Register Succeeded	
Parameter	**ActionUrlRegisterFailed**	**config.xml**
Description	It configures the action URL the phone sends after registration fails.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Register Failed	
Parameter	**ActionUrlUnregistered**	**config.xml**
Description	It configures the action URL the phone sends after an account is unregistered.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Unregistered	

Parameter	**ActionUrlOffHook**	**config.xml**
Description	It configures the action URL the phone sends when off hook.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Off Hook	
Parameter	**ActionUrlOnHook**	**config.xml**
Description	It configures the action URL the phone sends when on hook.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → On Hook	
Parameter	**ActionUrlIncomingCall**	**config.xml**
Description	It configures the action URL the phone sends when receiving an incoming call.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Incoming Call	
Parameter	**ActionUrlRejectIncomingCall**	**config.xml**
Description	It configures the action URL the phone sends when rejecting an incoming call.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Reject Incoming Call	
Parameter	**ActionUrlAnswerIncomingCall**	**config.xml**
Description	It configures the action URL the phone sends when answering a new incoming call.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Answer Incoming Call	
Parameter	**ActionUrlOutgoingCall**	**config.xml**
Description	It configures the action URL the phone sends when placing a call.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Outgoing Call	
Parameter	**ActionUrlCancelOutgoingCall**	**config.xml**

Description	It configures the action URL the phone sends when canceling the outgoing call in the ring-back state.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Cancel Outgoing Call	
Parameter	**ActionUrlRemoteBusy**	**config.xml**
Description	It configures the action URL the phone sends when the outgoing call is rejected.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Remote Busy	
Parameter	**ActionUrlCallRemoteCanceled**	**config.xml**
Description	It configures the action URL the phone sends when the remote party cancels the outgoing call in the ringing state.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Call Remote Canceled	
Parameter	**ActionUrlMissedCall**	**config.xml**
Description	It configures the action URL the phone sends when missing a call.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Missed Call	
Parameter	**ActionUrlCallEstablished**	**config.xml**
Description	It configures the action URL the phone sends when establishing a call.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Call Established	
Parameter	**ActionUrlCallTerminated**	**config.xml**
Description	It configures the action URL the phone sends when terminating a call.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Call Terminated	
Parameter	**ActionUrlDNDEnabled**	**config.xml**

Description	It configures the action URL the phone sends when DND feature is activated.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → DND Enabled	
Parameter	**ActionUrlDNDDisabled**	**config.xml**
Description	It configures the action URL the phone sends when DND feature is deactivated.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → DND Disabled	
Parameter	**ActionUrlImmediateForwardEnabled**	**config.xml**
Description	It configures the action URL the phone sends when the always forward feature is activated.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Immediate Forward Enabled	
Parameter	**ActionUrlImmediateForwardDisabled**	**config.xml**
Description	It configures the action URL the phone sends when the always forward feature is deactivated.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Immediate Forward Disabled	
Parameter	**ActionUrlBusyForwardEnabled**	**config.xml**
Description	It configures the action URL the phone sends when the busy forward feature is activated.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Busy Forward Enabled	
Parameter	**ActionUrlBusyForwardDisabled**	**config.xml**
Description	It configures the action URL the phone sends when the busy forward feature is deactivated.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Busy Forward Disabled	

Parameter	**ActionUrlNoReplyForwardEnabled**	**config.xml**
Description	It configures the action URL the phone sends when the no answer forward feature is activated.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → No Reply Forward Enabled	
Parameter	**ActionUrlNoReplyForwardDisabled**	**config.xml**
Description	It configures the action URL the phone sends when the no answer forward feature is deactivated.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → No Reply Forward Disabled	
Parameter	**ActionUrlForwardIncomingCall**	**config.xml**
Description	It configures the action URL the phone sends when forwarding an incoming call.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Forward Incoming Call	
Parameter	**ActionUrlCallTransfer**	**config.xml**
Description	It configures the action URL the phone sends when performing a transfer.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Call Transfer	
Parameter	**ActionUrlBlindTransfer**	**config.xml**
Description	It configures the action URL the phone sends when performing a blind transfer.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Blind Transfer	
Parameter	**ActionUrlAttendedTransfer**	**config.xml**
Description	It configures the action URL the phone sends when performing an attended/semi-attended transfer.	
Permitted Values	URL within 511 characters	
Default	Blank	

Web UI	Features → Action URL → Attended Transfer	
Parameter	**ActionUrlTransferFailed**	**config.xml**
Description	It configures the action URL the phone sends when transferring a call fails.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Transfer Failed	
Parameter	**ActionUrlTransferFinished**	**config.xml**
Description	It configures the action URL the phone sends when completing a call transfer.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Transfer Finished	
Parameter	**ActionUrlCallWaitingEnabled**	**config.xml**
Description	It configures the action URL the phone sends when the call waiting feature is enabled.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Call Waiting Enabled	
Parameter	**ActionUrlCallWaitingDisabled**	**config.xml**
Description	It configures the action URL the phone sends when the call waiting feature is disabled.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Call Waiting Disabled	
Parameter	**ActionUrlCallHold**	**config.xml**
Description	It configures the action URL the phone sends when placing a call on hold.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Call Hold	
Parameter	**ActionUrlCallUnhold**	**config.xml**
Description	It configures the action URL the phone sends when resuming a hold call.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Call Resume	

Parameter	**ActionUrlMute**	**config.xml**
Description	It configures the action URL the phone sends when muting a call.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Mute	
Parameter	**ActionUrlUnmute**	**config.xml**
Description	It configures the action URL the phone sends when un-muting a call.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → UnMute	
Parameter	**ActionUrlIpChanged**	**config.xml**
Description	It configures the action URL the phone sends when changing the IP address of the phone.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → IP Changed	
Parameter	**ActionUrlIdleToBusy**	**config.xml**
Description	It configures the action URL the phone sends when changing the state of the IP phone from busy to idle.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Idle To Busy	
Parameter	**ActionUrlBusyToIdle**	**config.xml**
Description	It configures the action URL the phone sends when changing the state of the phone from idle to busy.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Busy To Idle	
Parameter	**ActionUrlAutopStart**	**config.xml**
Description	It configures the action URL the phone sends when starting auto provisioning.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Autop Start	

Parameter	**ActionUrlAutopFinish**	**config.xml**
Description	It configures the action URL the phone sends when completing auto provisioning via power on.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Autop Finish	
Parameter	**ActionUrlHeadset**	**config.xml**
Description	It configures the action URL the phone sends when pressing the HEADSET key.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Headset	
Parameter	**ActionUrlHandfree**	**config.xml**
Description	It configures the action URL the phone sends when pressing the Speakerphone key.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Handfree	
Parameter	**ActionUrlPeripheralInformation**	**config.xml**
Description	It configures the action URL the phone sends when you unplug or plug the accessory.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Peripheral Information	
Parameter	**ActionUrlVpnIp**	**config.xml**
Description	It configures the action URL the phone sends when the IP address assigned by the VPN server changes.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → VPN IP	
Parameter	**ActionUrlReboot**	**config.xml**
Description	It configures the action URL the phone sends when start to reboot.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Reboot	

Parameter	ActionUrlReset	config.xml
Description	It configures the action URL the phone sends when start to reset.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Reset	
Parameter	ActionUrlScreenActive	config.xml
Description	It configures the action URL the phone sends when the screen is active.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Screen Active	
Parameter	ActionUrlScreenInactive	config.xml
Description	It configures the action URL the phone sends when the screen is inactive.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Screen Inactive	
Parameter	ActionUrlConferenceEstablished	config.xml
Description	It configures the action URL the IP phone sends when establishing a conference.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Features → Action URL → Conference Established	

10.27 Action URI

The ALE Myriad Series phones can perform the specified action by receiving and handling an HTTP or HTTPS GET request or accept a SIP NOTIFY message with the “Event: ACTION-URI” header from a SIP proxy server.

10.27.1 Supported HTTP/HTTPS GET Request

Opposite to action URL, action URI allows IP phones to interact with web server application by receiving and handling an HTTP or HTTPS GET request. When receiving a GET request, the IP phone will perform the specified action and respond with a 200 OK message.

A GET request may contain a variable named as “key” and a variable value, which are separated by “=”. The valid URI format is: http(s)://<phoneIPAddress>/servlet?key=variable value. For example: http://10.3.20.10/servlet?key=OK.

For security reasons, IP phones do not handle HTTP/HTTPS GET requests by default. You need to specify the trusted IP address for action URI. When the IP phone receives a GET request from the trusted IP address for the first time, the phone screen prompts the message “Allow remote control?”. Press the “OK” soft key on the phone to allow remote control.

You can specify one or more trusted IP addresses on the IP phone, or configure the IP phone to receive and handle the URI from any IP address.

10.27.2 Supported SIP Notify Message

In addition, ALE Myriad Series phones can perform the specified action immediately by accepting a SIP NOTIFY message with the “Event: ACTION-URI” header from a SIP proxy server. The message body of the SIP NOTIFY message may contain a variable named as “key” and a variable value, which are separated by “=”.

This method is especially useful for users who always work in the small office/home office where a secure firewall may prevent the HTTP or HTTPS GET request from the external network.

Note: If you want to only accept the SIP NOTIFY message from your SIP server and outbound proxy server, you have to enable the Accept SIP Trust Server Only feature.

If you use SIP NOTIFY message method, you do not need to specify the trusted IP address for action URI. However, you should enable the IP phone to receive the action URI requests. When the IP phone receives a SIP NOTIFY message with the “Event: ACTION-URI” header from a SIP proxy server for the first time, the LCD screen also prompts the message “Allow remote control?”. Press the “OK” soft key on the phone to allow remote control.

Example of a SIP Notify with the variable value (OK):

NOTIFY sip:[toUsername]@[remote_ip]:[remote_port];transport=[transport] SIP/2.0

Via: SIP/2.0/[transport] [local_ip]:[local_port];branch=[branch]

From: <sip:[fromUsername]@[remote_ip]:[remote_port]>;tag=452352542352354325

To: <sip:[toUsername]@[remote_ip]:[remote_port]>;[peer_tag_param]

Call-ID: [call_number]@[local_ip]

CSeq: [cseq+1] NOTIFY

Allow-Events: message-summary, refer, dialog, line-seize, presence, call-info, as-feature-event, calling-name, ua-profile

Max-Forwards: 70

Contact: <sip:[fromUsername]@[local_ip]:[local_port];transport=[transport]>

User-Agent:

Event: ACTION-URI

Content-Type: message/sipfrag

Content-Length: [len]

key=OK«

10.27.3 Variable Values List

The ALE Myriad Series phones also support a combination of the variable values in the URI, but the order of the variable value is determined by the operation of the phone. The valid URI format is shown below:

http(s)://<phoneIPAddress>/servlet?key=variable value[;variable value].

Variable values are separated by a semicolon from each other.

Note: For M8, (F_) CONFERENCE/ F_ CONFERENCE_ LONGPRESS are replaced by (F_) HEADSET/ F_ HEADSET_ LONGPRESS.

Variable Value	Phone Action
(F_) OK	Short Press the OK key
(F_) UP/DOWN/LEFT/RIGHT/	Short Press the navigation keys
(F_) CANCEL	Short press the Cancel key
F_CANCEL_LONGPRESS	Long Press Cancel key
(F_) VOLUME_UP	Short press the Volume up key
(F_) VOLUME_DOWN	Short press the Volume down key
LX	M3 X(1-6), M5/M7X(1-8), M8 X(1-10) Short press the line key
F_LX_LONGPRESS	Long Press Line key M3 X(1-6), M5/M7 X(1-8), M8 X(1-10)
FX	M3/M5/M7 X(1-4), M8 X(1-5) Short press the SOFT key
(F_) 0-9/*/ F_STAR/F_POUND	Short press the number key
(F_) RD	Short Press the RD/Redial key
(F_) HOLD	Short Press the Hold key
(F_) TRANSFER	Short Press the Transfer key
(F_) CONFERENCE	Short press the Conference key (for M3/M5/M7)
F_ CONFERENCE_ LONGPRESS	Long Press Conference key (for M3/M5/M7)
(F_) HEADSET	Short press the Conference key (for M8)
F_ HEADSET_ LONGPRESS	Short press the Conference key (for M8)
(F_) RELEASE	Short press the Release key
(F_) MUTE	Short press the Mute key
F_ MUTE_ LONGPRESS	Long Press Mute key
(F_) MESSAGE	Short press the Message key
(F_) HANDSFREE	Short press the Handsfree key
OFFHOOK	Pick up the handset.
ONHOOK	Hang up the handset
BACK_IDLE	Return the phone to idle
REBOOT(case insensitive)	Reboot the phone
RESET(case insensitive)	Reset factory
DND_ON	Set dnd on
DND_OFF	Set dnd off
ANSWER/ASW	Answer a call
ATrans=xxx	Perform a semi-attended/attended transfer to xxx.
BTrans=xxx	Perform a blind transfer to xxx
CallWaitingOn	Activate the call waiting feature
CallWaitingOff	Deactivate the call waiting feature

CALLEND	End a call
ASW/CANCEL/HOLD/UNHOLD:xxx	Answer/end/hold/unhold a call (xxx refers to the call-id of the active call)
AlwaysFwdOn/BusyFwdOn/NoAnswFwdOn =xxx	Activate an always/busy/no answer forward feature to xxx for the IP phone (“xxx” means the destination number)
AlwaysFwdOff/BusyFwdOff/NoAnswFwdOff	Deactivate the always/busy/no answer forward feature for the IP phone
number=xxx&outgoing_uri=y	Use y call to xxx Eg: https://10.4.0.62/servlet?key=number=1000&outgoing_uri=1001 Use 1001 call 1000
Autop	Perform auto provisioning
screencapture	Gets the current screen capture Eg: https://10.4.0.62/screencapture https://10.4.0.62/servlet?command=screencapture If you want to download screen shots https://10.4.0.62/screencapture/download

10.27.4 Action URI Configuration

The following table lists the parameters you can use to configure action URI.

Parameter	**FeatureActionUriEnable**	**config.xml**
Description	It enables or disables the phone to receive action URI requests.	
Permitted Values	false - disable true - enable	
Default	false	
Parameter	**FeatureActionUriPromptEnable**	**config.xml**
Description	It enables or disables the phone to pop up the Allow Remote Control prompt when receiving action URI requests.	
Permitted Values	false - disable true - enable	
Default	true	
Parameter	**FeatureActionUriLimitIp**	**config.xml**
Description	It configures server address from which the phone receives the action URI requests. Multiple addresses are separated by commas. For discontinuous IP addresses, multiple IP addresses are separated by commas. For continuous IP addresses, the format likes *.*.*.* and the “*” stands for the values 0~255. **Note:** It works only if “**FeatureActionUriEnable**” is set to true (Enabled).	

Permitted Values	IP address Blank - The phone will reject any HTTP GET request. Any **-** The phone will accept and handle HTTP GET requests from any IP address.
Default	Blank

11. Phone Customization

11.1 Multiple Languages

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

11.1.1 Phone Language Configuration

The following table lists the parameters you can use to configure the phone SettingLanguage.

Parameter	SettingLanguage	config.xml
Description	It configures phone display SettingLanguage.	
Permitted Values	0 - English 1 - French 2 - Deutsch 3 - Italian 4 - Spanish 5 - Nederlands 6 - Portuguese 7 - Hungarian 8 - Czech 9 - Slovak 10 - Slovenian 11 - Estonian 12 - Polish 13 - Lithuanian 14 - Latvian 15 - Turkish 16 - Greek 17 - Sweden 18 - Norway 19 - Denmark 20 - Finland 21 - Icelandic 22 - Chinese_simplified 23 - Chinese_traditional 24 - Korean 25 - Japanese 26 - Arabic 27 - Hebrew 28 - Russian	
Default	0	
Phone UI	Menu → Basic Setting → Language	

11.2 Screen Saver

The screen saver will automatically start when the IP phone is idle for the preset waiting time. You can stop the screen saver at any time by pressing any key. When your phone is idle again for a preset waiting time, the screen saver starts again.

By default, the phone screen displays a built-in image when the screen saver starts. The following shows the built-in screen saver displayed on the ALE Myriad Series phones:

You can also configure the display of time & date, certain status icons (for example, miss call, a new text message), or custom information (for example, company logo) on the screen saver.

The following table lists the parameters you can use to configure screensaver.

Parameter	**SettingScreensaverEnable**	**config.xml**
Description	It configures whether to enable or disable screensaver	
Permitted Values	false - disable true - enable	
Default	true	
Web UI	Settings → Display → Screensaver	
Phone UI	Menu → Basic Setting → Display → Screen saver → Screen saver	
Parameter	**SettingScreensaverTimeout**	**config.xml**
Description	It configures the time (in seconds) to wait in the idle state before the screen saver starts.	
Permitted Values	60-1min 120-2min 300-5min 600-10min 1800-30min 3600-1h 7200-2h 10800-3h 21600-6h	
Default	300-5min	
Web UI	Display → Timeout	
Phone UI	Menu → Basic Setting → Display	

11.3 Backlight of LCD

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

You can change the screen backlight brightness and time in the following settings:

Active Level: The brightness level of the LCD screen when the phone is active. Digits (1-9) represent different brightness levels. 9 is the brightest level.

Inactive Level: The brightness of the LCD screen when the phone is inactive. You can select a low brightness or turn off the backlight.

Backlight Time: The delay time to change the brightness of the LCD screen when the phone is inactive. Backlight time includes the following settings you can choose from.

- **Always On**: Backlight is on permanently.
- **Always,15s, 30s, 60s, 2min, 5min, 10min or 30min**: Backlight is changed when the phone is inactive after the designated time (in seconds).

11.3.1 Supported Backlight Options

The following table lists available options to configure the backlight of phone models/expansion modules.

Phone Model (and the connected expansion module)	Configuration Options
Myriad Series IP phones	Inactive Level Active Level Backlight Time

11.3.2 Backlight Brightness and Time Configuration

The following table lists the parameters you can use to configure screen backlight brightness and time.

Parameter	**SettingActiveBacklightLevel**	**config.xml**
Description	It configures the intensity of the LCD screen when the phone is active.	
Permitted Values	[1,9]	
Default	5	
Web UI	Setting → Display → Active Backlight Level	
Phone UI	Menu → Basic Setting → Display → Backlight → Active Level	
Parameter	**SettingInactiveBackLightLevel**	**config.xml**
Description	It configures the intensity of the LCD screen when the phone is inactive.	
Permitted Values	[1,9]	
Default	1	
Web UI	Setting → Display → Inactive Backlight Level	
Phone UI	Menu → Basic Setting → Display → Backlight → Inactive Level	
Parameter	**SettingBacklightTimeout**	**config.xml**

Description	It configures the delay time (in seconds) to change the intensity of the LCD screen when the IP phone is inactive.
Permitted Values	0-Always On 15-15s 30-30s 60-1min 120-2min 300-5min 600-10min 1800-30min
Default	300
Web UI	Settings → Display → Backlight Timeout
Phone UI	Menu → Basic Setting → Display → Backlight → Backlight Time

11.4 Backlight of LED (Only for M8)

The M8 phone supports changing the LED backlight brightness for digital keys on dialing pad.

You can configure the display brightness level on phone UI or WBM.

Note: If the value of parameter “SettingLedSyncBacklightEnable” is true, the backlight brightness of LCD and LED will be adjusted synchronously.

11.4.1 Supported Backlight LED Options

The following table lists available options to configure the LED backlight of phone models/expansion modules.

Phone Model (and the connected expansion module)	Configuration Options
M8	LED Inactive Level LED Active Level LED Backlight Time

11.4.2 LED Backlight Brightness and Time Configuration

The following table lists the parameters you can use to configure the LED backlight brightness and time.

Parameter	**SettingLedSyncBacklightEnable**	**config.xml**
Description	It configures whether synchronized with LCD backlight configuration	
Permitted Values	true false	
Default	true	
Web UI	Settings → Display → LED Synchronize	
Phone UI	Menu → Basic Setting → Display → Backlight → LED Synchronize	
Parameter	**SettingInactiveLedLevel**	**config.xml**
Description	It configures the intensity of the LED backlight when the phone is inactive.	

Permitted Values	[0,9]	
Default	1	
Web UI	Setting → Display → LED Inactive Level	
Phone UI	Menu → Basic Setting → Display → Backlight → LED Inactive Level	
Parameter	**SettingActiveLedLevel**	**config.xml**
Description	It configures the intensity of the LED backlight when the phone is active.	
Permitted Values	[0,9]	
Default	5	
Web UI	Settings → Display → LED Active Level	
Phone UI	Menu → Basic Setting → Display → Backlight → LED Active Level	
Parameter	**SettingLedTimeout**	**config.xml**
Description	It configures the delay time (in seconds) to change the intensity of the LED when the IP phone is inactive.	
Permitted Values	0-Always On 15-15s 30-30s 60-1min 120-2min 300-5min 600-10min 1800-30min	
Default	300	
Web UI	Settings → Display → LED Timeout	
Phone UI	Menu → Basic Setting → Display → Backlight → LED Working Time	

11.5 ECO Mode (Only for M8)

The M8 phone supports the ECO (Ecology Conservation Optimization) mode. If the phone is set to ECO mode, the LED lights on digital keys will be off.

The following table lists the parameters you can use to configure ECO mode.

Parameter	**SettingEcoModeEnable**	**config.xml**
Description	It configures whether to enable or disable ECO mode of the M8 phone.	
Permitted Values	true false	
Default	false	
Web UI	Settings → Display → ECO Mode	
Parameter	**SettingEcoModeOffHourTimeout**	**config.xml**

Description	It configures the delay time the phone enters ECO mode when in non-working time.	
Permitted Values	[1,10]	
Default	5	
Web UI	Settings → Display → Off Hour Timeout	
Parameter	**SettingEcoModeOfficeHourTimeout**	**config.xml**
Description	It configures the delay time the phone enters ECO mode when in working time.	
Permitted Values	[1,240]	
Default	120	
Web UI	Settings → Display → Office Hour Timeout	
Parameter	**SettingEcoOfficeHourSunStartTime**	**config.xml**
Description	It configures the start time of Sunday.	
Permitted Values	[0,23]	
Default	9	
Web UI	Settings → Display → Sunday	
Parameter	**SettingEcoOfficeHourSunEndTime**	**config.xml**
Description	It configures the end time of Sunday.	
Permitted Values	[0,23]	
Default	9	
Web UI	Settings → Display → Sunday	
Parameter	**SettingEcoOfficeHourMonStartTime**	**config.xml**
Description	It configures the start time of Monday.	
Permitted Values	[0,23]	
Default	9	
Web UI	Settings → Display → Monday	
Parameter	**SettingEcoOfficeHourMonEndTime**	**config.xml**
Description	It configures the end time of Monday.	
Permitted Values	[0,23]	
Default	17	
Web UI	Settings → Display → Monday	
Parameter	**SettingEcoOfficeHourTuesStartTime**	**config.xml**
Description	It configures the start time of Tuesday.	

Permitted Values	[0,23]	
Default	9	
Web UI	Settings → Display → Tuesday	
Parameter	**SettingEcoOfficeHourTuesEndTime**	**config.xml**
Description	It configures the end time of Tuesday.	
Permitted Values	[0,23]	
Default	17	
Web UI	Settings → Display → Tuesday	
Parameter	**SettingEcoOfficeHourWedStartTime**	**config.xml**
Description	It configures the start time of Wednesday.	
Permitted Values	[0,23]	
Default	9	
Web UI	Settings → Display → Wednesday	
Parameter	**SettingEcoOfficeHourWedEndTime**	**config.xml**
Description	It configures the end time of Wednesday.	
Permitted Values	[0,23]	
Default	17	
Web UI	Settings → Display → Wednesday	
Parameter	**SettingEcoOfficeHourThurStartTime**	**config.xml**
Description	It configures the start time of Thursday.	
Permitted Values	[0,23]	
Default	9	
Web UI	Settings → Display → Thursday	
Parameter	**SettingEcoOfficeHourThurEndTime**	**config.xml**
Description	It configures the end time of Thursday.	
Permitted Values	[0,23]	
Default	17	
Web UI	Settings → Display → Thursday	
Parameter	**SettingEcoOfficeHourFriStartTime**	**config.xml**
Description	It configures the start time of Friday.	

Permitted Values	[0,23]	
Default	9	
Web UI	Settings → Display → Friday	
Parameter	**SettingEcoOfficeHourFriEndTime**	**config.xml**
Description	It configures the end time of Friday.	
Permitted Values	[0,23]	
Default	17	
Web UI	Settings → Display → Friday	
Parameter	**SettingEcoOfficeHourSatStartTime**	**config.xml**
Description	It configures the start time of Saturday.	
Permitted Values	[0,23]	
Default	9	
Web UI	Settings → Display → Saturday	
Parameter	**SettingEcoOfficeHourSatEndTime**	**config.xml**
Description	It configures the end time of Saturday.	
Permitted Values	[0,23]	
Default	9	
Web UI	Settings → Display → Saturday	

11.6 Time and Date

The ALE Myriad Series phones maintain a local clock. You can choose to get the time and date from SNTP (Simple Network Time Protocol) time server to have the most accurate time and phone DST (Daylight Saving Time) to make better use of daylight and to conserve energy, or you can set the time and date manually. The time and date can be displayed in several formats on the idle screen.

11.6.1 Time Zone

Time Zone	Time Zone Name
-11:00	Midway, Niue, Pago_Pago
-10:00	Adak, Honolulu, Rarotonga, Tahiti
-9:30	Marquesas
-9:00	Anchorage, Gambier, Juneau, Metlakatla, Nome, Sitka, Yakutat
-8:00	Dawson, Los_Angeles, Pacific-New, Pitcairn, Tijuana, Vancouver, Whitehorse
-7:00	Boise, Cambridge_Bay, Chihuahua, Creston, Dawson_Creek, Denver, Edmonton, Fort_Nelson, Hermosillo, Inuvik, Ojinaga, Mazatlan, Phoenix, Yellowknife
-6:00	Bahia_Banderas, Belize, Chicago, Costa_Rica, Easter, El_Salvador, Galapagos, Guatemala, Indiana/Knox, Indiana/Tell_City, Managua, Matamoros, Menominee, Merida,

	Mexico_City, Monterrey, North_Dakota/Beulah, North_Dakota/Center, North_Dakota/New_Salem, Rainy_River, Rankin_Inlet, Regina, Resolute, Swift_Current, Tegucigalpa, Winnipeg
-5:00	Atikokan, Bogota, Cancun, Cayman, Detroit, Eirunepe, Grand_Turk, Guayaquil, Havana, Indiana/Indianapolis, Indiana/Marengo, Indiana/Petersburg, Indiana/Vevay, Indiana/Vincennes, Indiana/Winamac, Iqaluit, Jamaica, Kentucky/Louisville, Kentucky/Monticello, Lima, Nassau, New_York, Nipigon, Panama, Pangnirtung, Port-au-Prince, Rio_Branco, Thunder_Bay, Toronto
-4:00	Anguilla, Antigua, Aruba, Asuncion, Barbados, Bermuda, Blanc-Sablon, Boa_Vista, Campo_Grande, Caracas, Cuiaba, Curacao, Dominica, Glace_Bay, Goose_Bay, Grenada, Guadeloupe, Guyana, Halifax, Kralendijk, La_Paz, Lower_Princes, Manaus, Marigot, Martinique, Moncton, Montserrat, Port_of_Spain, Porto_Velho, Puerto_Rico, Santiago, Santo_Domingo, St_Barthelemy, St_Kitts, St_Lucia, St_Thomas, St_Vincent, Thule, Tortola
-3:30	St_Johns
-3:00	Araguaina, Argentina/Buenos_Aires, Argentina/Catamarca, Argentina/Cordoba, Argentina/Jujuy, Argentina/La_Rioja, Argentina/Mendoza, Argentina/Rio_Gallegos, Argentina/Salta, Argentina/San_Juan, Argentina/San_Luis, Argentina/Tucuman, Argentina/Ushuaia, Bahia, Belem, Cayenne, Fortaleza, Godthab, Maceio, Miquelon, Montevideo, Palmer, Paramaribo, Punta_Arenas, Recife, Rothera, Santarem, Sao_Paulo, Stanley
-2:00	Noronha, South_Georgia
-1:00	Azores, Cape_Verde
0	GMT, UTC, Universal, Abidjan, Accra, Bamako, Banjul, Bissau, Canary, Conakry, Dakar, Danmarkshavn, Faroe, Freetown, Greenwich, Guernsey, Isle_of_Man, Jersey, Lisbon, Lome, London, Madeira, Monrovia, Nouakchott, Ouagadougou, Reykjavik, Sao_Tome, St_Helena, Troll, Zulu
+1:00	Algiers, Amsterdam, Andorra, Bangui, Belgrade, Berlin, Bratislava, Brazzaville, Brussels, Budapest, Busingen, Casablanca, Ceuta, Copenhagen, Douala, Dublin, El_Aaiun, Gibraltar, Kinshasa, Lagos, Libreville, Ljubljana, Longyearbyen, Luanda, Luxembourg, Madrid, Malabo, Malta, Monaco, Ndjamena, Niamey, Oslo, Paris, Podgorica, Porto-Novo, Prague, Rome, San_Marino, Sarajevo, Scoresbysund, Skopje, Stockholm, Tirane, Tunis, Vaduz, Vatican, Vienna, Warsaw, Zagreb, Zurich
+2:00	Amman, Athens, Beirut, Blantyre, Bucharest, Bujumbura, Cairo, Chisinau, Damascus, Famagusta, Gaborone, Gaza, Harare, Hebron, Helsinki, Jerusalem, Johannesburg, Kaliningrad, Khartoum, Kiev, Kigali, Lubumbashi, Lusaka, Maputo, Mariehamn, Maseru, Mbabane, Nicosia, Riga, Sofia, Tallinn, Tripoli, Uzhgorod, Vilnius, Windhoek, Zaporozhye
+3:00	Addis_Ababa, Aden, Antananarivo, Asmara, Baghdad, Bahrain, Comoro, Dar_es_Salaam, Djibouti, Istanbul, Juba, Kampala, Kirov, Kuwait, Mayotte, Minsk, Mogadishu, Moscow, Nairobi, Qatar, Riyadh, Simferopol, Syowa
+3:30	Tehran
+4:00	Astrakhan, Baku, Dubai, Mahe, Mauritius, Muscat, Reunion, Samara, Saratov, Tbilisi, Ulyanovsk, Volgograd, Yerevan
+4:30	Kabul

+5:00	Aqtau, Aqtobe, Ashgabat, Atyrau, Dushanbe, Karachi, Kerguelen, Maldives, Mawson, Oral, Qyzylorda, Samarkand, Tashkent, Yekaterinburg
+5:30	Colombo, Kolkata
+5:45	Kathmandu
+6:00	Almaty, Bishkek, Chagos, Dhaka, Omsk, Qostanay, Thimphu, Urumqi, Vostok
+6:30	Cocos, Yangon
+7:00	Bangkok, Barnaul, Christmas, Davis, Ho_Chi_Minh, Hovd, Jakarta, Krasnoyarsk, Novokuznetsk, Novosibirsk, Phnom_Penh, Pontianak, Tomsk, Vientiane
+8:00	Brunei, Casey, Choibalsan, Hong_Kong, Irkutsk, Kuala_Lumpur, Kuching, Macau, Makassar, Manila, Perth, Shanghai, Singapore, Taipei, Ulaanbaatar
+8:45	Eucla
+9:00	Chita, Dili, Jayapura, Khandyga, Palau, Pyongyang, Seoul, Tokyo, Yakutsk
+9:30	Adelaide, Broken_Hill, Darwin
+10:00	Brisbane, Chuuk, Currie, DumontDUrville, Guam, Hobart, Lindeman, Melbourne, Port_Moresby, Saipan, Sydney, Ust-Nera, Vladivostok
+10:30	Lord_Howe
+11:00	Bougainville, Efate, Guadalcanal, Kosrae, Macquarie, Magadan, Norfolk, Noumea, Pohnpei, Sakhalin, Srednekolymsk
+12:00	Anadyr, Auckland, Fiji, Funafuti, Kamchatka, Kwajalein, Majuro, McMurdo, Nauru, Tarawa, Wake, Wallis
+12:45	Chatham
+13:00	Apia, Enderbury, Fakaofo, Tongatapu
+14:00	Kiritimati

The following table lists the parameters you can use to configure the time zone.

Parameter	**SettingTimeZone**	**config.xml**
Description	It configures the time zone.	
Permitted Values	CHOICE	
Default	0	
Web UI	Settings → Time & Date	

11.6.2 NTP Settings

You can configure an NTP time server for the desired area as required. The NTP time server address can be offered by the DHCP server or configured manually.

The following table lists the parameters you can use to configure the NTP.

Parameter	**SettingSntpServer**	**config.xml**
Description	It configures the IP address or the domain name of the NTP server. The IP phone will obtain the current time and date from the NTP server	

Permitted Values	IP_DOMAIN	
Default	0.pool.ntp.org	
Web UI	Settings → Time & Date → SNTP Address	
Parameter	**SettingSntpServer2**	**config.xml**
Description	It configures the IP address or the domain name of the NTP server2. The IP phone will obtain the current time and date from the NTP server2	
Permitted Values	IP_DOMAIN	
Default	time.nist.gov	
Web UI	Settings → Time & Date → SNTP Secondary Address	
Parameter	**SettingSntpRefreshPeriod**	**config.xml**
Description	It configures the interval (in seconds) at which the phone updates time and date from the NTP server.	
Permitted Values	NUMERIC[0,*]	
Default	3600	
Web UI	Settings → Time & Date → SNTP Refresh Period	

11.6.3 DST Settings

You can set DST for the desired area as required. By default, the DST is disabled. If set to Automatic, it can be adjusted automatically from the current time zone setting. The time zone and corresponding DST pre-configurations exist in the AutoDST file. If the DST is set to Automatic, the IP phone obtains the DST configuration from the AutoDST file.

11.6.3.1 DST Configuration

The following table lists the parameters you can use to configure DST.

Parameter	**SettingDstEnable**	**config.xml**
Description	It configures the Daylight Saving Time (DST) feature.	
Permitted Values	0 - Disabled 1 - Enabled 2 - Automatic	
Default	0	
Web UI	Settings → Time & Date → DST Enable	
Parameter	**SettingTimeZoneLocation**	**config.xml**
Description	It configures the Daylight Saving Time (DST) Location. **Note:** It works only if “SettingDstEnable” is set to 2 (Automatic).	
Permitted Values	Strings - country or area name	
Default	Universal	

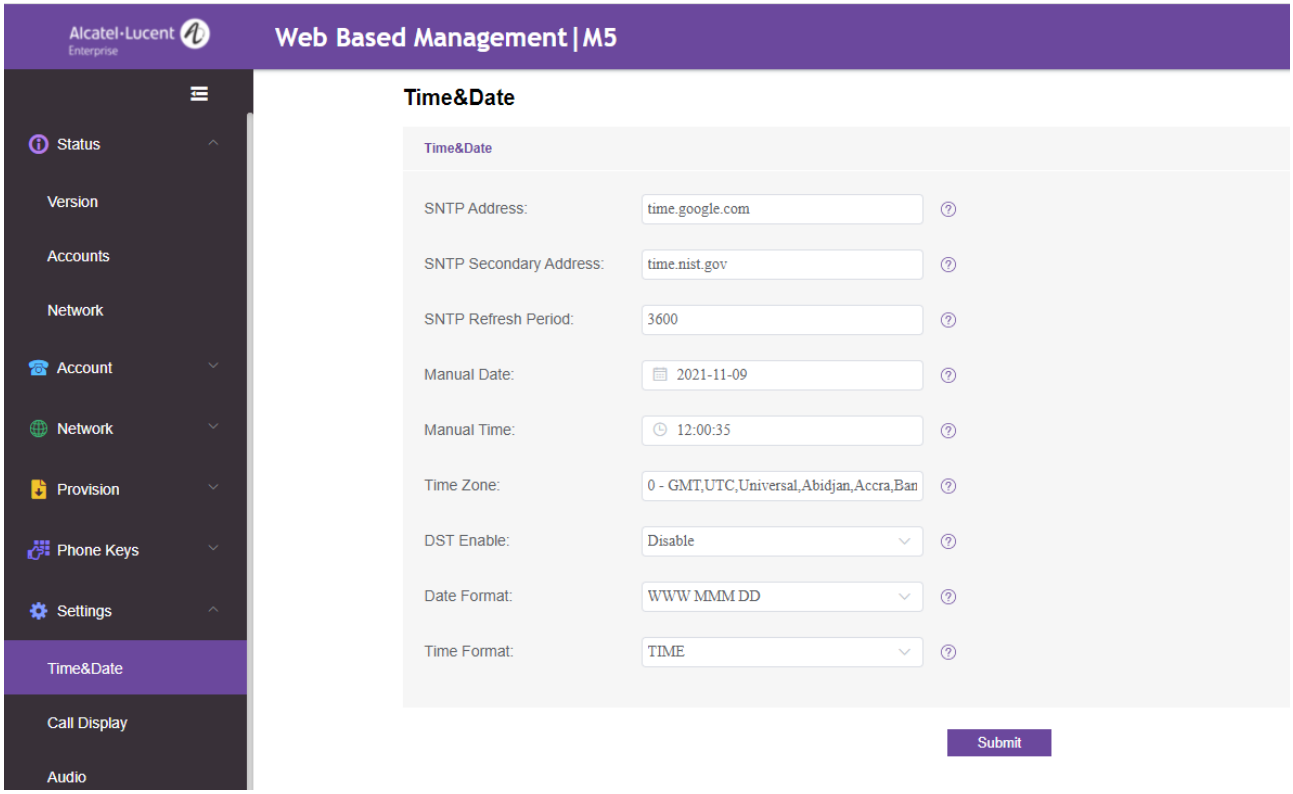
Web UI	Setting → Time & Date → Location	
Parameter	**SettingDstType**	**config.xml**
Description	It configures the Daylight Saving Time (DST) Type. **Note:** It works only if “SettingDstEnable” is set to 1 (Enabled).	
Permitted Values	week - By week date - By date	
Default	week	
Web UI	Setting → Time & Date → DST Type	
Parameter	**SettingDstStartDate**	**config.xml**
Description	It configures the Daylight Saving Time (DST) start date. **Note:** It works only if “SettingDstEnable” is set to 1 (Enabled) and SettingDstType is set to date	
Permitted Values	Strings	
Default	1	
Web UI	Setting → Time & Date → DST Start Date	
Parameter	**SettingDstEndDate**	**config.xml**
Description	It configures the Daylight Saving Time (DST) end date. **Note:** It works only if “SettingDstEnable” is set to 1 (Enabled) and SettingDstType is set to date.	
Permitted Values	Strings	
Default	30	
Web UI	Setting → Time & Date → DST End Date	
Parameter	**SettingDstStartWeek**	**config.xml**
Description	It configures the Daylight Saving Time (DST) start week. **Note:** It works only if “SettingDstEnable” is set to 1 (Enabled) and SettingDstType is set to week.	
Permitted Values	1 - First week 2 - Second week 3 - Third week 4 - Fourth week 5 - Last week	
Default	5	
Web UI	Setting → Time & Date → DST Start Date → Week	
Parameter	**SettingDstEndWeek**	**config.xml**
Description	It configures the Daylight Saving Time (DST) end week. **Note:** It works only if “SettingDstEnable” is set to 1 (Enabled) and SettingDstType is set to week.	

Permitted Values	1 - First week 2 - Second week 3 - Third week 4 - Fourth week 5 - Last week	
Default	5	
Web UI	Setting → Time & Date → DST End Date → Week	
Parameter	**SettingDstStartHour**	**config.xml**
Description	It configures the Daylight Saving Time (DST) start hour. **Note:** It works only if "SettingDstEnable" is set to 1 (Enabled) and SettingDstType is set to week or day.	
Permitted Values	NUMERIC[0,23]	
Default	0	
Web UI	Setting → Time & Date → DST Start Date → Hour	
Parameter	**SettingDstEndHour**	**config.xml**
Description	It configures the Daylight Saving Time (DST) end hour. **Note:** It works only if "SettingDstEnable" is set to 1 (Enabled) and SettingDstType is set to week or day.	
Permitted Values	NUMERIC[0,23]	
Default	23	
Web UI	Setting → Time & Date → DST End Date → Hour	
Parameter	**SettingDstOffset**	**config.xml**
Description	It configures the offset time (in minutes) of Daylight Saving Time (DST). **Note:** It works only if "SettingDstEnable" is set to 1 (Enabled)	
Permitted Values	NUMERIC[-300,300]	
Default	60	
Web UI	Setting → Time & Date → Offset(min)	

11.6.4 Manual Configuration of Time and Date

You can configure the time and date manually if the phone cannot obtain the time and date from the NTP time server via Web or Phone UI.

- Configuration via Web UI



- Configuration via Phone UI

You can set date and time manually on phone UI by path: Menu → Basic Setting → Time & Date → General → Manual Settings

11.6.5 Time and Date Format Configuration

You can customize the time and date by choosing between a variety of time and date formats, including options to date format with the day, month, or year, and time format in 12 hours or 24 hours, or you can also customize the date format as required.

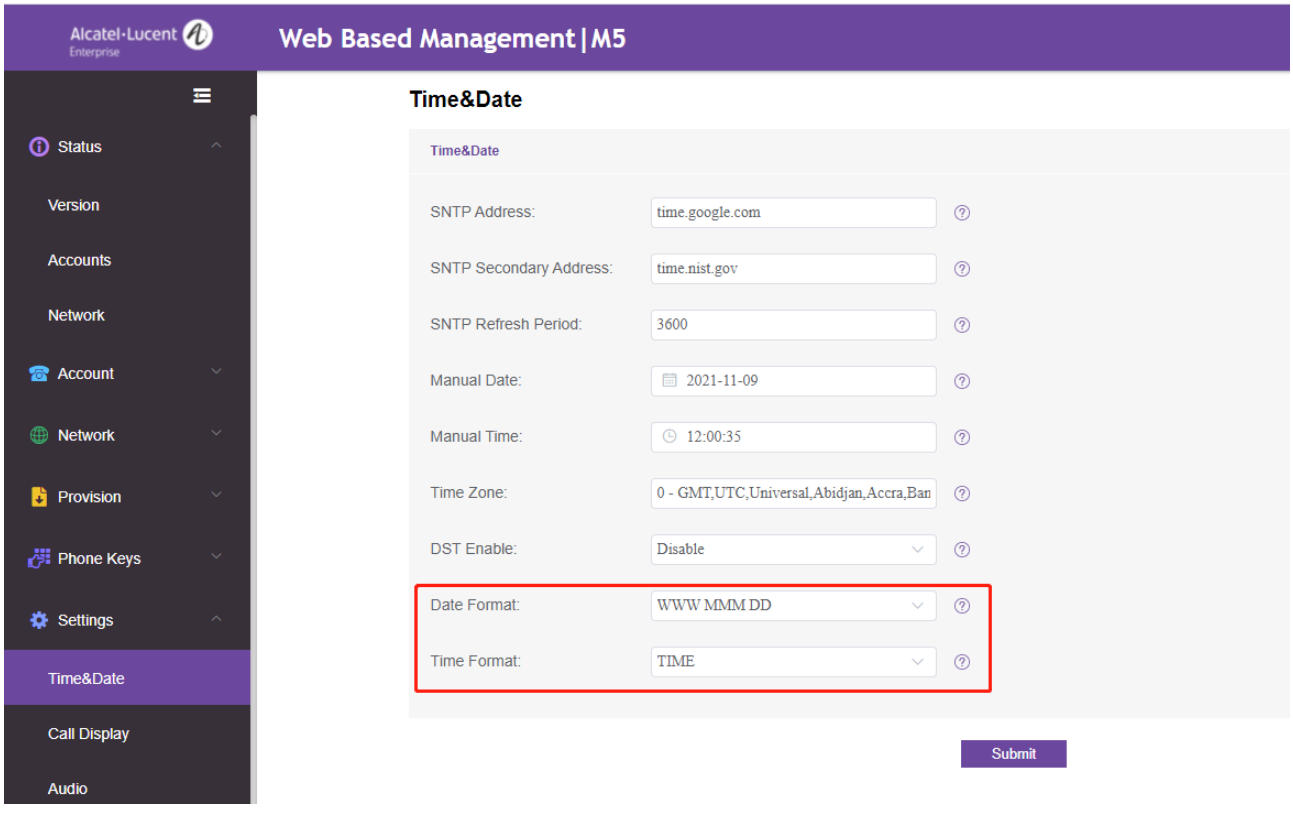
The following table lists the parameters you can use to configure time and date format.

Parameter	**SettingTimeFormat**	**config.xml**
Description	It configures the time format.	
Permitted Values	0: Hour 12. The time will be displayed in 12-hour format with AM or PM specified. 1: Hour 24. The time will be displayed in 24-hour format (for example, 2:00 PM displays as 14:00).	

Default	0	
Web UI	Settings → Time & Date → Time Format	
Phone UI	Menu → Basic Setting → Time and Date → Time	
Parameter	**DateFormat**	**config.xml**
Description	It configures the date format.	
Permitted Values	0 - WWW MMM DD 1 - DD-MMM-YY 2 - YYYY-MM-DD 3 - DD/MM/YYYY 4 - MM/DD/YY 5 - DD MMM YYYY 6 - WWW DD MMM 7 - MM DD WWW 8 - YY-MM-DD 9 - YYYY/MM/DD 10 - YY/MM/DD 11 - YYYY MM DD	
Default	0	
Web UI	Settings → Time & Date → Date Format	
Phone UI	Menu → Basic Setting → Time and Date → Date	

You can configure the time and date format through WEB or on phone UI.

- Configure Time & Date Format through WEB



- Configure Time & Date Format on phone UI

You can set date and time format manually on phone UI by path: Menu → Basic Setting → Time & Date → Time & Date Format

11.7 Key As Send

Key As Send allows you to assign the pound key ("#") or asterisk key ("*") as the Send key.

The following table lists the parameters you can use to configure the Key As Send feature.

Parameter	**FeatureKeyAsSend**	**config.xml**
Description	It configures the "#" or "*" key as the Send key.	
Permitted Values	0: Disabled. Neither "#" nor "*" can be used as the Send key. 1: # key. The pound key is used as the Send key. 2: * key. The asterisk key is used as the Send key.	
Default	1	
Web UI	Features → General	
Phone UI	Menu → Features → Key as Send	

11.8 Bluetooth

The ALE Myriad Series M7/M8 phones support Bluetooth. You can pair and connect a Bluetooth Headset or Bluetooth-enabled mobile phone with the IP phone. After connecting the Bluetooth-Enabled mobile phone, you can choose to synchronize the mobile contacts to the IP phone. It is only applicable to the M7/M8 phones.

You can activate or deactivate the Bluetooth mode, and personalize the Bluetooth device name for the IP phone. The pre-configured Bluetooth device name will be displayed in the scanning list of other devices. The Bluetooth device name helps the other Bluetooth devices to identify and pair with your IP phone.

The following table lists the parameters you can use to configure Bluetooth.

Parameter	SettingBluetoothDeviceName	config.xml
Description	It configures the Bluetooth device name. **Note:** It works only for the M7/M8 phones.	

Permitted Values	Strings	
Default	M7 DeskPhone/M8 DeskPhone	
Phone UI	Menu → Basic Setting → Bluetooth → Edit My Device Info	
Parameter	SettingBluetoothReconnectMode	config.xml
Description	It enables or disables the phone to prompt users to confirm the reconnection request from the Bluetooth device. **Note:** It works only for the M7 phone.	
Permitted Values	0 - no auto-connect 1 - low sensitive auto-connect	
Default	1	
Phone UI	Menu → Basic Setting → Bluetooth → BT Smart Phone Connected Mode	
Parameter	SettingBluetoothEnable	config.xml
Description	It enables or disables the Bluetooth feature. Note: It works only for the M8 phone.	
Permitted Values	false - disable true - enable	
Default	true	
Phone UI	Menu → Basic Setting → Bluetooth → Bluetooth Enable	

11.9 Handset/Headset/Speakerphone Mode

The ALE Myriad Series phones support three ways to place/answer a call: using the handset, using the headset or using the speakerphone. You can choose the frequently used audio device as required.

The following table lists the parameters you can use to configure handset/headset/speakerphone mode.

Parameter	SettingRingDevice	config.xml
Description	It configures the SettingRingDevice.	
Permitted Values	0 - handsfree 1 - headset 2 - handsfree_plus_headset	
Default	0	
Web UI	Settings → Ringing	
Phone UI	Menu → Basic Setting → Sound → Ringing → Ringing Device	

You need to press Headset program key to activate/deactivate Headset function for the ALE Myriad Series phones. If the Headset is in use, Headset icon will be displayed as red.

Note: Regarding how to configure Headset program key, please refer to DSS Keys chapter.

11.10 Programmable Keys

The ALE Myriad Series phones support programmable Keys in phone and EM Keys in AOM module. You can configure different functions to programmable keys. This section explains how to configure programmable keys and EM Keys.

11.10.1 Supported Programmable Keys

The following table lists the number of programmable keys you can configure for each phone model:

Phone Model	Programmable Keys	EM Keys
M3	20	N/A
M5	28	N/A
M7	28	N/A
M8	36	N/A

11.10.2 Supported Programmable Key Types

The supported key function types are varied by programmable keys and EM keys.

For M8, 19-XML Browser is not supported.

ID	Programmable Key Types
0	N/A
1	SpeedDial
2	BLF List
3	Do Not Disturb
4	Directory
5	VoiceMail
6	Conference
7	Forward
8	Transfer
9	Group Listening
10	Headset

11	Hot Desking
12	Phone Lock
13	Prefix
14	DTMF
15	Direct Pickup
16	Group Pickup
17	Call Park
18	Recall
19	XML Browser
21	Intercom
22	Retrieve Park
23	AudioHub
24	Private Hold
58	Hold
59	BLF
60	Account
61	USB Recording
62	Broadsoft Recording
63	Dispostion Code
64	Emergency Escalation
65	Customer Orignated Trace
66	Paging
67	Paging List
68	Mobile Account
69	Hoteling
70	Push To Talk
71	Logout
72	Network Call List
73	Network Contacts
74	Network Message List
75	Call Waiting

11.10.3 Programmable Keys

You can customize programmable keys on the phone to enable users to access frequently used functions. If your phone does not have a specific hard key, you can create a soft key. For example, if the phone does not have a Do Not Disturb hard key, you can create a Do Not Disturb soft key. The programmable key takes effect only when the IP phone is idle.

11.10.3.1 Programmable Keys Configuration

In R130 release, programmable keys layout of the ALE Myriad Series phones is changed to tree arrangement.

The following table lists the parameters you can use to configure programmable keys.

Note: For M8, 19-XML Browser is not supported.

Parameter	ProgramKeyXType	config.xml
Description	It configures key feature for a specific programmable key. **Note**: X can be 1-20 for M3, 1-28 for M5/M7 and 1-36 for M8.	
Permitted Values	0 - Not Used 1 - Speed Dial 59 - BLF 2 - BLF List 3 - Do Not Disturb 4 - Directory 5 - VoiceMail 6 - Conference 7 - Forward 8 - Transfer 9 - Group Listening 10 - HeadSet 11 - Hot Desking 12 - Phone Lock 13 - Prefix 14 - DTMF 15 - Direct Pickup 16 - Group Pickup 17 - Call Park 18 - Recall 19 - XML Browser 21 - Intercom 22 - Retrieve Park 23 - AudioHub 24 - Private Hold 42 - ACD 58 - Hold 60 - Account 61 - Usb Recording 62 - Broadsoft Recording 63 - Dispostion Code 64 - Emergency Escalation 65 - Customer Orignated Trace 66 - Paging	

	67 - Paging List 68 - Mobile Account 69 - Hoteling 70 - Push To Talk 71 - Logout 72 - Network Call List 73 - Network Contacts 74 - Network Message List 75 - Call Waiting	
Default	0 **Note**: For M8, 19 - XML Browser is not supported.	
Web UI	Phone Keys → Program Key	
Phone UI	Long press softkey to enter programmable key configuration menu.	
Parameter	**ProgramKeyXAccount**	**config.xml**
Description	It configures the desired account to apply the programmable key feature. **Note**: X can be 1-20 for M3, 1-28 for M5/M7 and 1-36 for M8.	
Permitted Values	1 - Account 1 2 - Account 2 3 - Account 3 4 - Account 4 5 - Account 5 6 - Account 6 7 - Account 7 8 - Account 8 N - Account N (N is 9-20, only for M8)	
Default	1	
Web UI	Phone Keys → Program Keys	
Phone UI	Long press softkey to enter programmable key configuration menu.	
Parameter	**ProgramKeyXLabel**	**config.xml**
Description	It configures the label displayed on the phone screen for a specific programmable key. This is an optional configuration. **Note**: X can be 1-20 for M3, 1-28 for M5/M7 and 1-36 for M8.	
Permitted Values	String within 64 characters	
Default	empty	
Web UI	Phone Keys → Program Keys	
Phone UI	Long press softkey to enter programmable key configuration menu.	
Parameter	**ProgramKeyXValue**	**config.xml**
Description	It configures the value for some programmable key features.	

	For example, when you assign the Speed Dial to the programmable key, this parameter is used to specify the contact number you want to dial out. It is also used to specify the contact number with the DTMF sequence. The contact number and DTMF sequence are separated by commas. **Note:** You need to configure this parameter when “programablekey.X.type” is set to 1, 59, 5, 14, 13, 15, 16,17,19,21,22 or 73. X can be 1-20 for M3, 1-28 for M5/M7 and 1-36 for M8.	
Permitted Values	String within 64 characters	
Default	empty	
Web UI	Phone Keys → Program Keys	
Phone UI	Long press softkey to enter programmable key configuration menu.	
Parameter	**ProgramKeyXExtension**	**config.xml**
Description	For BLF feature: It configures the pickup code. **Note:** It is only applicable when “programablekey.X.type” is set to 59. X can be 1-20 for M3, 1-28 for M5/M7 and 1-36 for M8.	
Permitted Values	String within 64 characters	
Default	empty	
Web UI	Phone Keys → Program Keys	
Phone UI	Long press softkey to enter programmable key configuration menu.	

11.10.3.2 Dynamic Keys Configuration

This feature supports configuring the programming hard keys and soft keys such as key Redial/key Hold/key conference and so on.

Users can configure these keys for custom functions such as Speed Dial/DND/Forward and so on.

The *** in the table will be replaced by Key Name in the actual database.

The feature can be configured by the following parameters in the configuration file:

Parameter	**DynamicSoftKeyXType**	**config.xml**
Description	It configures the key type for a specific programmable key. **Note:** X can be 1- 4 for M3/M5/M7, or 1-5 for M8.	
Permitted Values	0 - Not Used 1 - Speed Dial 3 - Do Not Disturb 4 - Directory 7 - Forward 10 - Headset 11 - Hot Desking 12 - Phone Lock 13 - Prefix	

	18 - Recall 19 - XML Browser 21 - Intercom 23 - Audio Hub 101 - Menu 102 - History 103 - Status 104 - Login	
Default	0 **Note**: For M8, 19 - XML Browser is not supported.	
Web UI	Phone Keys → Dynamic Key	
Parameter	**DynamicSoftKeyXAccount**	**config.xml**
Description	It configures the desired account to apply the programmable key feature. **Note:** X can be 1- 4 for M3/M5/M7, or 1-5 for M8.	
Permitted Values	1 - Account 1 2 - Account 2 3 - Account 3 4 - Account 4 5 - Account 5 6 - Account 6 7 - Account 7 8 - Account 8 N - Account N (N is 9-20, only for M8)	
Default	1	
Web UI	Phone Keys → Dynamic Softkey	
Parameter	**DynamicSoftKeyXLabel**	**config.xml**
Description	It configures the label displayed on the phone screen for a specific programmable key. This is an optional configuration. **Note:** X can be 1- 4 for M3/M5/M7, or 1-5 for M8.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Phone Keys → Dynamic key	
Parameter	**DynamicSoftKeyXNumber**	**config.xml**
Description	It configures the value for some programmable key features. **Note:** X can be 1- 4 for M3/M5/M7, or 1-5 for M8.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Phone Keys → Dynamic key	

Parameter	**DynamicSoftKeyXExtension**	**config.xml**
Description	This configuration is not applicable for programmable hard key types. **Note:** X can be 1- 4 for M3/M5/M7, or 1-5 for M8.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Phone Keys → Dynamic key	
Parameter	**DynamicKey***Type**	**config.xml**
Description	It configures the key type for a specific programmable key.	
Permitted Values	0 - Not Used 1 - Speed Dial 3 - Do Not Disturb 4 - Directory 7 - Forward 10 - Headset 11 - Hot Desking 12 - Phone Lock 13 - Prefix 18 - Recall 19 - XML Browser 21 - Intercom 23 - Audio Hub 101 - Menu 102 - History 103 - Status	
Default	0	
Web UI	Phone Keys → Dynamic Key	
Parameter	**DynamicKey***Account**	**config.xml**
Description	It configures the desired account to apply the programmable key feature.	
Permitted Values	1 - Account 1 2 - Account 2 3 - Account 3 4 - Account 4 5 - Account 5 6 - Account 6 7 - Account 7 8 - Account 8 N - Account N (N is 9-20, only for M8)	
Default	1	
Web UI	Phone Keys → Dynamic Softkey	

Parameter	**DynamicKey***Label**	**config.xml**
Description	It configures the label displayed on the phone screen for a specific programmable key. This is an optional configuration.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Phone Keys → Dynamic key	
Parameter	**DynamicKey***Number**	**config.xml**
Description	It configures the value for some programmable key features.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Phone Keys → Dynamic key	
Parameter	**DynamicKey***Extension**	**config.xml**
Description	This configuration is not applicable for programmable hard key types.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Phone Keys → Dynamic key	

The Key Names supported are listed as follows:

Note: For M8, conference hard key is replaced by headset key. And VolUp/ VolDown keys are not available for M8.

Key Name	Default Type	Default Account	Default Label	Default Number	Default Extension
Redial	N/A	1			
Release	N/A	1			
Hold	N/A	1			
Mute	N/A	1			
Transfer	N/A	1			
Message	N/A	1			
Conference	N/A	1			
Handsfree	N/A	1			
Headset	N/A	1			
Up	N/A	1			
Down	N/A	1			
Left	N/A	1			
Right	N/A	1			

OK	N/A	1			
Cancel	N/A	1			
VolUp	N/A	1			
VolDown	N/A	1			

11.10.3.3 EM Keys Configuration

The Alcatel-Lucent Enterprise SMART Expansion Module EM20/EM200 is a deskphone accessory, which extends Myriad IP phones' functionality.

The parameters which are configured for EM20/EM200 in the configuration template are described as follows:

Parameter	**AomXProgKey[1,200]Type** **Note:** The ALE Myriad Series phones support connecting up to 3 expansion modules. (3*EM20,3*EM200) (X=1-3)	**config.xml**
Description	It configures the key type for a specific EM key.	
Permitted Values	0 - Not Used 1 - Speed Dial 59 - BLF 2 - BLF List 3 - Do Not Disturb 4 - Directory 5 - VoiceMail 6 - Conference 7 - Forward 8 - Transfer 9 - Group Listening 10 - HeadSet 11 - Hot Desking 12 - Phone Lock 13 - Prefix 14 - DTMF 15 - Direct Pickup 16 - Group Pickup 17 - Call Park 18 - Recall 19 - XML Browser 21 - Intercom 22 - Retrieve Park 23 - AudioHub 24 - Private Hold 42 - ACD 58 - Hold 60 - Account	

	61 - Usb Recording 62 - Broadsoft Recording 63 - Dispostion Code 64 - Emergency Escalation 65 - Customer Orignated Trace 66 - Paging 67 - Paging List 68 - Mobile Account 69 - Hoteling 70 - Push To Talk 71 - Logout 72 - Network Call List 73 - Network Contacts 74 - Network Message List	
Default	0 **Note:** For M8, XML Browser is not supported.	
Web UI	Phone Keys → Program Key → EM1/EM2/EM3	
Parameter	**AomXProgKey[1,200]Account** **Note:** The ALE Myriad Series phones support connecting up to 3 expansion modules. (3xEM20,3xEM200) (X=1-3)	**config.xml**
Description	It configures the desired account to apply the EM key feature.	
Permitted Values	1 - Account 1 2 - Account 2 3 - Account 3 4 - Account 4 5 - Account 5 6 - Account 6 7 - Account 7 8 - Account 8 N - Account N (N is 9-20, only for M8)	
Default	1	
Web UI	Phone Keys → Program Key → EM1/EM2/EM3	
Parameter	**AomXProgKey[1,200]Label** **Note:** The ALE Myriad Series phones support connecting up to 3 expansion modules. (3xEM20,3xEM200) (X=1-3)	**config.xml**
Description	It configures the label displayed on the phone screen for a specific the EM key. This is an optional configuration.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Phone Keys → Program Keys → EM1/EM2/EM3	

Parameter	**AomXProgKey[1,200]Number** **Note:** The ALE Myriad Series phones support connecting up to 3 expansion modules. (3xEM20,3xEM200) (X=1-3)	**config.xml**
Description	It configures the value for some EM key features. For example, when you assign the Speed Dial to the EM key, this parameter is used to specify the contact number you want to dial out.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Phone Keys → Program Keys → EM1/EM2/EM3	
Parameter	**AomXProgKey[1,200]Extension** **Note:** The ALE Myriad Series phones support connecting up to 3 expansion modules. (3xEM20,3xEM200) (X=1-3)	**config.xml**
Description	For BLF feature: It configures the pickup code.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Phone Keys → Program Key → EM1/EM2/EM3	

11.11 Wallpaper

Wallpaper is a picture which is used as the background of the IP phones. The phones have 5 default pictures. And the user can also change it to custom wallpaper using personal pictures. The wallpaper is only applicable to M5/M7 phones.

11.11.1 Wallpaper Configuration

The following table lists the parameters you can use to change the wallpaper.

Parameter	**SettingWallpaperUploadUrl**	**config.xml**
Description	It configures the access URL of the custom wallpaper picture.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Settings → Display → Wallpaper upload	
Parameter	**SettingWallpaperDelete**	**config.xml**
Description	The custom image file name which the user wants to delete.	
Permitted Values	String within 64 characters, for example: custom.png	
Default	Blank	
Web UI	Settings → Display→ Wallpaper upload (delete the picture which is selected)	
Parameter	**SettingWallpaperDisplay**	**config.xml**

Description	Custom wallpaper image file name
Permitted Values	String within 64 characters
Default	default.png
Web UI	Settings → Display → Current Wallpaper

11.11.2 Custom Wallpaper Picture Limit

The wallpaper picture format must meet the following requirements:

Phone Model	Format	Resolution	Single File Size
M5/M7	PNG/JPG/JPEG/BMP	320 * 240	1MB
M8	PNG/JPG/JPEG/BMP	800 * 480	1MB

11.12 Call Display

Call Display is used in phone ringing, calling process, hold and other scenarios. This function is mainly used by users to configure the full name display method according to their own habits.

There are two main configuration items, defined as SettingCallInfoDisplayMode and SettingCallInfoDisplaySource.

- SettingCallInfoDisplayMode is used for defining the call information display mode.
- SettingCallInfoDisplaySource is used for displaying the priority of the call number.

The following table lists the parameters you can use to configure call display.

Parameter	**SettingCallInfoDisplayMode**	**config.xml**
Description	It configures Call Display Part.	
Permitted Values	0: Name Number 1: Number Name 2: Name 3: Number 4: Full Contact Info	
Default	0	
Web UI	Settings → Call Display → Call Info Display Mode	
Parameter	**SettingCallInfoDisplaySource**	**config.xml**
Description	It configures Call Display Source.	
Permitted Values	0 - Local Directory → Remote Phone Book → LDAP Directory → Network signaling 1 - Network signaling	
Default	0	

11.13 Notification Pop-ups

This feature is used to control the popup of a new voicemail and a missed call.

- If the FeatureVmPopupEnable is set to true, the notification of voice mail and missed call will pop up when the SIP phone misses an incoming call or receives a voicemail.

- If the FeatureVmPopupEnable is set to false, the notification of voice mail and missed call will not pop up when the SIP phone misses an incoming call or receives a voicemail.

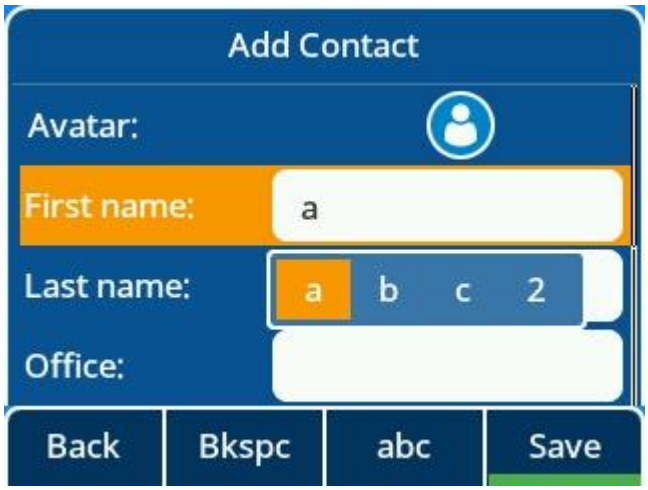
The following table lists the parameters you can use to configure notification popups.

Parameter	FeatureVmPopupEnable	config.xml
Description	It configures whether to enable of disable the popup of voicemail and missed call.	
Permitted Values	false - disable true - enable	
Default	true	

11.14 IME Optimization

In Myriad R120 release, when the user uses an input method other than 123 (eg: abc ABC Abc 2ab...).

The phone provides an input field to prompt the user for the current input character and displays the next few characters.



11.15 Search Source List in Dialing

Search Source List in Dialing allows you to search entries from the source list when the phone is on the pre-dialing/dialing screen. You can select the desired entry to dial out quickly.

The following table lists the parameters you can use to configure the search source list.

11.16 Soft Key Layout

Soft key layout is used to customize the soft keys at the bottom of the phone screen for best meeting users' requirements.

In addition to specifying which soft keys to be displayed, you can also determine their display order. The configurations for soft key layout are based on call states.

11.16.1 Supported Call States and Soft Keys

The following table lists soft keys available for IP phones in different call states.

State	Default Value		Allowed Value
	M3/M5/M7	M8	
Dial	Call Backspace	Call Directory	Call Backspace IME

	IME Cancel	Backspace IME Cancel	Cancel Directory History Empty
Dial Empty	Directory Empty IME Cancel	Directory Empty Empty IME Cancel	Directory History IME Cancel Empty
Transfer Dial	Blind Transfer Call Backspace Cancel	Call Directory Backspace Cancel Blind Transfer	Blind Transfer Call Backspace Cancel IME Directory History Empty
Transfer Dial Empty	Directory Empty IME Cancel	Directory Empty Empty IME Cancel	Directory History IME Cancel Empty
Conference Dial	Call Backspace IME Cancel	Call Directory Backspace IME Cancel	Call Backspace IME Cancel Directory History Empty
Conference Dial Empty	Directory Empty IME Cancel	Directory Empty Empty IME Cancel	Directory History IME Cancel Empty
Calling	Empty Empty Empty End	Empty Empty Empty Empty End	End Empty
Transferring	Transfer Empty Empty End	Transfer Empty Empty Empty End	Transfer End Empty

Call Failed	Empty Empty Empty End	New Call Empty Empty Empty End	End New Call Empty
Ringing	Take Slient Forward Reject	Take Empty Slient Forward Reject	Take Slient Forward Reject Empty
New Callin	Empty Take Reject End	Take Empty Empty Reject End	Take Reject End Empty
Conference New Callin	Empty Take Reject End	Take Empty Empty Reject End	Take Reject End Empty
Conversation	Hold Transfer Conference End	Hold Empty Transfer Conference End	Hold Transfer Conference End Swap Empty
Hold	New Call Transfer Resume End	New Call Empty Transfer Resume End	New Call Transfer Resume End Empty
Held	Empty Empty Empty End	Empty Empty Empty Empty End	End Empty
Conference	Conference Manage Hold Split End	Conference Transfer Manage Hold Split End	Conference Manage Hold Split End Transfer Empty

Conference Hold	New Call Resume Split End	New Call Empty Resume Split End	New Call Resume Split End Empty
Be Transferred	Empty Empty Empty End	Empty Empty Empty Empty End	End Empty
Multicast Paging	Hold Empty Empty End	Hold Empty Empty Empty End	Hold End Empty
Multicast Listening	Hold Empty Empty End	Hold Empty Empty Empty End	Hold End Empty

11.16.2 Soft Key Layout File Customization

xml File	States
Dial.xml	Dial; DialEmpty; TransDial; TransDialEmpty; ConfDial; ConfDialEmpty
CallOut.xml	Calling; Transferring
CallFailed.xml	CallFailed
CallIn.xml	Ringing; NewCallin; ConfNewCallin
Talking.xml	Conversation; Hold; Held; Conf; ConfHold; BeTrans; Paging; Listening

Customizing Softkey Layout File:

- Step 1: Open the template file.
- Step 2: For each soft key that you want to enable/disable, move the string from the disabled/enabled soft key list to enabled/disabled soft key list in the file or replace the Empty in the enabled soft key list.

  The following shows a portion of the softkey layout file “CallIn.xml”:

```
<?xml version="1.0"?>
<Ringing>
 <Enable>
  <Key value="Take"/>
  <Key value="Forward"/>
  <Key value="Silent"/>
  <Key value="Reject"/>
 </Enable>
 <Allowed>
  <Key value="Take"/>
  <Key value="Forward"/>
  <Key value="Silent"/>
  <Key value="Reject"/>
  <Key value="Empty"/>
 </Allowed>
</Ringing>
```

- Step 3: Save the change and place this file on the provisioning server.

11.16.3 Softkey Layout Configuration

The following table lists the parameters you can use to configure the softkey layout.

Parameter	**SettingCustomSoftkeyEnable**	**config.xml**
Description	It enables or disables the custom softkey layout feature.	
Permitted Values	false - disable true - enable	
Default	false	
Web UI	WEB → Settings → Softkey Layout → Custom Softkey	
Parameter	**SettingCustomSoftkeyStateList**	**config.xml**
Description	It configures the desired call state to apply the custom softkey layout. **Note:** Multiple call states are separated by commas. It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	Blank - all call states will use the custom softkey layout) Dial - Dial state DialEmpty - DialEmpty state TransDial - TransDial state TransDialEmpty - TransDialEmpty state ConfDial - ConfDial state ConfDialEmpty - ConfDialEmpty state Calling - Calling state Transferring - Transferring state CallFailed - CallFailed state Ringing - Ringing state NewCallin - NewCallin state ConfNewCallin - ConfNewCallin state Conversation - Conversation	

	Hold - Hold Held - Held Conf - Conf ConfHold - ConfHold BeTrans - BeTrans Paging - Paging Listening - Listenning	
Default	Blank	
Parameter	**SettingCustomSoftkeyDynamicEnable**	**config.xml**
Description	It enables or disables the phone to display the soft keys relevant to the features (call center, centralized call recording, and executive-assistant). **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	false - disable true - enable	
Default	true	
Parameter	**SettingCustomSoftkeyDialUrl**	**config.xml**
Description	It configures the access URL of the custom softkey layout file in the Dial state. The states that the XML file contains: Dial; DialEmpty; TransDial; TransDialEmpty; ConfDial; ConfDialEmpty **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	URL within 511 characters	
Default	Blank	
Parameter	**SettingCustomSoftkeyCallOutUrl**	**config.xml**
Description	It configures the access URL of the custom softkey layout file in the Callout state. The states that the XML file contains: Calling; Transferring **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	URL within 511 characters	
Default	Blank	
Parameter	**SettingCustomSoftkeyCallFailedUrl**	**config.xml**
Description	It configures the access URL of the custom softkey layout file in the Callfailed state. The state that the XML file contains: CallFailed **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	URL within 511 characters	
Default	Blank	
Parameter	**SettingCustomSoftkeyCallInUrl**	**config.xml**

Description	It configures the access URL of the custom softkey layout file in the CallIn state. The states that the XML file contains: Ringing; NewCallin; ConfNewCallin **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	URL within 511 characters	
Default	Blank	
Parameter	**SettingCustomSoftkeyTalkingUrl**	**config.xml**
Description	It configures the access URL of the custom softkey layout file in the Taking state. The states that the XML file contains: Conversation; Hold; Held; Conf; ConfHold; BeTrans; Paging; Listenning **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	URL within 511 characters	
Default	Blank	
Parameter	**SettingCustomSoftkeyDial**	**config.xml**
Description	It configures custom Softkey in the Dial state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	Call Backspace IME Cancel Directory History Blank - String within 511 characters	
Default	M3/M5/M7: Call;Backspace;IME;Cancel M8: Call;Directory;Backspace;IME;Cancel	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyDialEmpty**	**config.xml**
Description	It configures custom Softkey in the DialEmpty state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	Directory;History;IME;Cancel;Empty String within 511 characters	
Default	M3/M5/M7: Directory;Empty;IME;Cancel M8: Directory;Emoty;Empty;IME;Cancel	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyTransDial**	**config.xml**
Description	It configures custom Softkey in the TransDial state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	

Permitted Values	Blind Transfer;Call;Backspace;Cancel;IME;Directory;History;Empty String within 511 characters	
Default	M3/M5/M7: Blind Transfer;Call;Backspace;Cancel M8: Call;Directoey;Backspace;Cancel;Blind Transfer	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyTransDialEmpty**	**config.xml**
Description	It configures custom Softkey in the DialEmpty state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	Directory;History;IME;Cancel;Empty String within 511 characters	
Default	M3/M5/M7: Directory;Empty;IME;Cancel M8: Directory;Empty;Empty;IME;Cancel	
Web UI	WEB-Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyConfDial**	**config.xml**
Description	It configures custom Softkey in the ConfDial state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	Call;Backspace;IME;Cancel;Directory;History;Empty String within 511 characters	
Default	M3/M5/M7: Call;Backspace;IME;Cancel M8: Call;Directory;Backspace;IME;Cancel	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyConfDialEmpty**	**config.xml**
Description	It configures custom Softkey in the DialEmpty state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	Directory;History;IME;Cancel;Empty String within 511 characters	
Default	M3/M5/M7: Directory;Empty;IME;Cancel M8: Directory;Empty;Empty;IME;Cancel	
Web UI	WEB → Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyCalling**	**config.xml**
Description	It configures custom Softkey in the Calling state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	End;Empty String within 511 characters	
Default	M3/M5/M7: Empty;Empty;Empty;End M8: Empty;Empty;Empty;Empty;End	
Web UI	Settings → Softkey Layout → Call States	

Parameter	**SettingCustomSoftkeyTransferring**	**config.xml**
Description	It configures custom Softkey in the Transferring state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	Transfer - Transfer End - End Empty - Empty	
Default	M3/M5/M7: Transfer;Empty;Empty;End M8: Transfer;Empty; Empty;Empty;End	
Web UI	WEB → Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyCallFailed**	**config.xml**
Description	It configures custom Softkey in the CallFailed state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	End;NewCall;Empty String within 511 characters	
Default	M3/M5/M7: Empty;Empty;Empty;End M8: New Call;Empty;Empty;Empty;End	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyRinging**	**config.xml**
Description	It configures custom Softkey in the Ringing state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	Take;Slient;Forward;Reject;Empty String within 511 characters	
Default	M3/M5/M7: Take;Silent;Forward;Reject M8: Take;Empty;Silent;Forward;Reject	
Web UI	WEB → Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyNewCallin**	**config.xml**
Description	It configures custom Softkey in the NewCallin state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	Take;Reject;End;Empty String within 511 characters	
Default	M3/M5/M7: Empty;Take;Reject;End M8: Take;Empty;Empty;Reject;End	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyConfNewCallin**	**config.xml**
Description	It configures custom Softkey in the NewCallin state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	

Permitted Values	Take;Reject;End;Empty String within 511 characters	
Default	M3/M5/M7:Empty;Take;Reject;End M8: Take;Empty;Empty;Reject;End	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyConversation**	**config.xml**
Description	It configures custom Softkey in the Conversation state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	Hold;Transfer;Conference;End;Swap;Empty String within 511 characters	
Default	M3/M5/M7: Hold;Transfer;Conference;End M8: Hold;Empty;Transfer;Conference;End	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyHold**	**config.xml**
Description	It configures custom Softkey in the Hold state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	NewCall;Transfer;Resume;End;Empty String within 511 characters	
Default	M3/M5/M7: NewCall;Transfer;Resume;End M8: New Call;Empty;Transfer;Resume;End	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyHeld**	**config.xml**
Description	It configures custom Softkey in the Held state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	End;Empty String within 511 characters	
Default	M3/M5/M7: Empty;Empty;Empty;End M8: Empty;Empty;Empty;Empty;End	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyConf**	**config.xml**
Description	It configures custom Softkey in the Conf state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	Conference;Manage;Hold;Split;End;Transfer;Empty String within 511 characters	
Default	M3/M5/M7: Conference;Manage;Hold;Split;End M8: Conference;Transfer;Manage;Hold;Split;End	
Web UI	Settings → Softkey Layout → Call States	

Parameter	SettingCustomSoftkeyConfHold	config.xml
Description	It configures custom Softkey in the Hold state **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	NewCall;Resume;Split;End;Empty String within 511 characters	
Default	M3/M5/M7: NewCall;Resume;Split;End M8: New Call;Empty;Resume;Split;End	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyBeTrans**	**config.xml**
Description	It configures custom Softkey in the BeTrans state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	End;Empty String within 511 characters	
Default	M3/M5/M7: Empty;Empty;Empty;End M8: Empty;Empty;Empty;Empty;End	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyPaging**	**config.xml**
Description	It configures custom Softkey in the Paging state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	Hold;End;Empty String within 511 characters	
Default	M3/M5/M7: Hold;Empty;Empty;End M8: Hold;Empty;Empty;Empty;End	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyListening**	**config.xml**
Description	It configures custom Softkey in the paging Listening state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true (Enabled).	
Permitted Values	Hold;End;Empty String within 511 characters	
Default	M3/M5/M7: Hold;Empty;Empty;End M8: Hold;Empty;Empty;Empty;End	
Web UI	Settings → Softkey Layout → Call States	

11.16.4 Example: Setting the Soft Keys Layout in Talking State

The following example shows the configuration for setting the soft key layout in the talking state.

Customize a softkey layout file "Talking.xml" and place this file on the provisioning server "http://10.11.5.140".

Example:

<setting value="true" id=" SettingCustomSoftkeyEnable " override="true"/>

<setting value="http://10.11.5.140/Talking.xml" id="SettingCustomSoftkeyTalkingUrl " override="true"/>

The states that the XML file contains: Conversation; Hold; Held; Conf; ConfHold; BeTrans; Paging; Listening

After provisioning, you can use the enabled soft keys during a call.

12. Advanced Features

12.1 Audio Hub

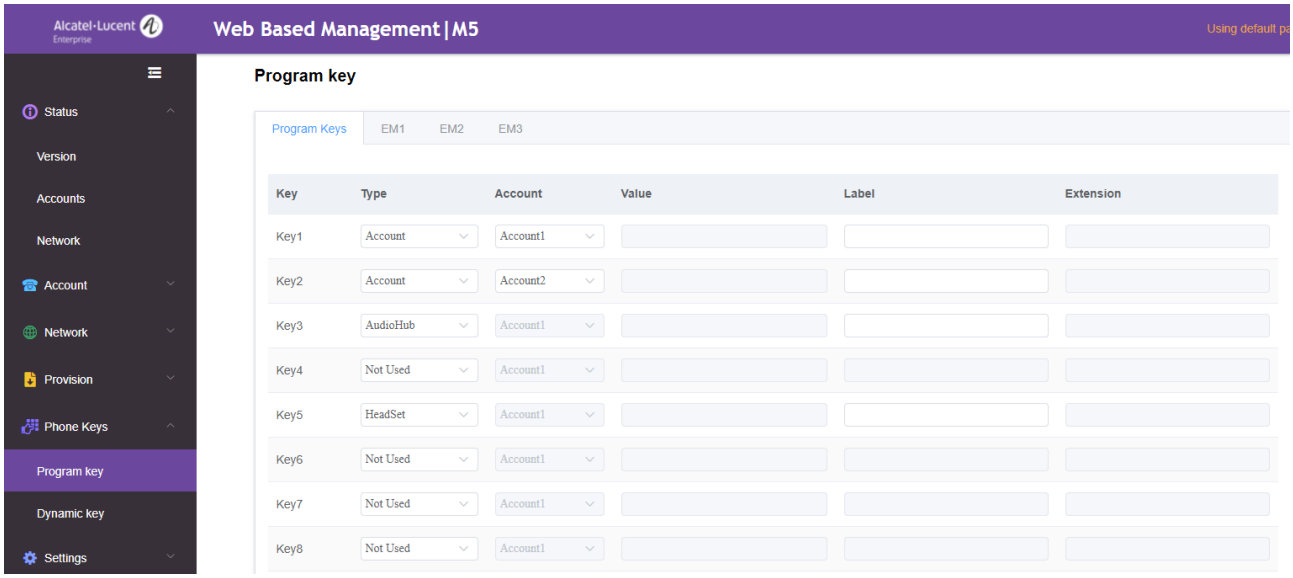
The ALE Myriad Series M3/M5/M7 DeskPhones can act as an external audio device of a PC. When a PC plays audio application or video application or plays music, the voice can be transmitted to the ALE Myriad Series phones. The audio hub playing music can be controlled to play or pause by a programmable key named Audio Hub.

USB-C port supports Audio Hub by default.

The ALE Myriad Series phones support Audio Hub through BT, contact sync, audio transmission and call control.

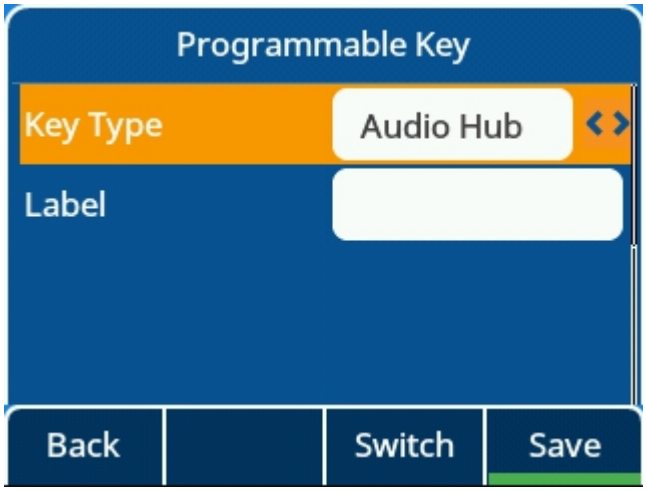
12.1.1 AudioHub Programmable Key Configuration via Web UI

You can configure the AudioHub programmable key via the Web UI path Phone Keys → Program key and setting the programmable key's type to Audio Hub.



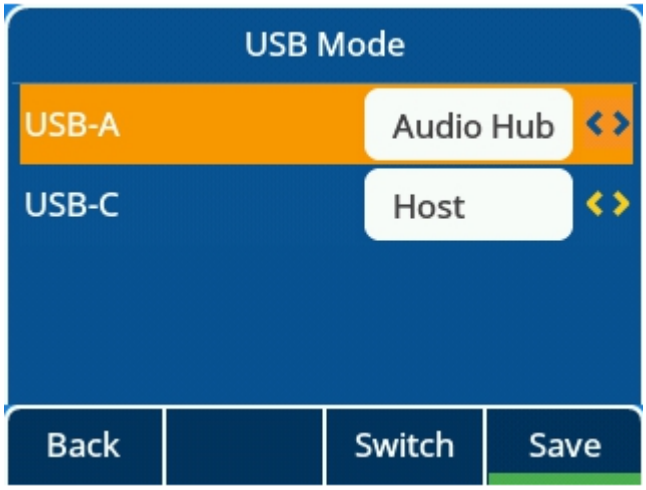
12.1.2 AudioHub Programmable Key Configuration via Phone UI

You can configure the AudioHub programmable key via Phone UI by long pressing a programmable key and then setting the programmable key's type to Audio Hub.



To use Audio Hub from USB-A port, you can change USB mode from Phone UI via path: Menu → Basic Setting → USB.

If you change this parameter, the IP phone will reboot for the change to take effect.



Note: This configuration is not available for the M8 Phone.

12.1.3 AudioHub Programmable Key Configuration Parameters

The following table lists the parameters you can use to configure the AudioHub programmable key.

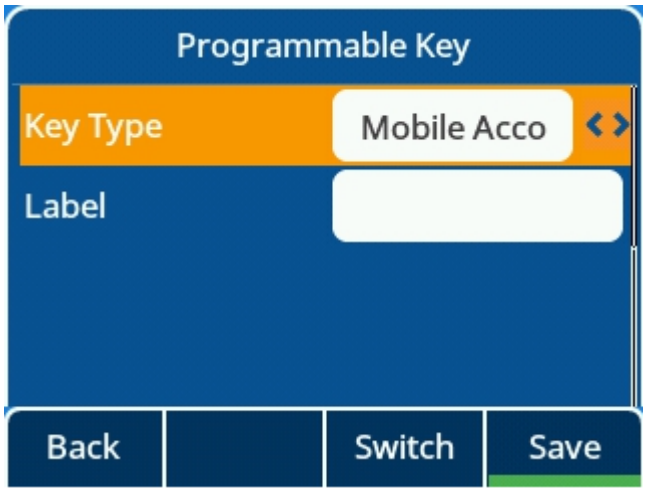
Parameter	**UsbAMode**	**config.xml**
Description	It configures the USB-A mode. It can be set to Host which can plugin audio accessories such as USB headset and USB external handsfree or set to Audio Hub which can be regarded as PC's sound equipment. **Note:** This configuration is not available for the M8 Phone.	
Permitted Values	0 - Host 1 - Audio Hub	
Default	0	
Phone UI	Menu → Basic Setting → USB	
Parameter	**UsbCMode**	**config.xml**
Description	It configures the USB-C mode. It can be set to Host which can plugin audio accessories such as USB headset and USB external handsfree or set to Audio Hub which can be regarded as PC's sound equipment.	
Permitted Values	0 - Host 1 - Audio Hub	
Default	1	
Phone UI	Menu → Basic Setting → USB	
Parameter	**ProgramKeyXType**	**config.xml**
Description	It configures the programmable key type. X can be number 1~20 for M3 or 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	23 - AudioHub	
Default	0	
Phone UI	Select one program key, then long press it for 2s, and select Key Type as Audio Hub.	

Web UI	Phone Keys → Program key	
Parameter	**ProgramKeyXLabel**	**config.xml**
Description	It configures the programmable key label. X can be number 1~20 for M3 or 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	strings	
Default	Blank	
Phone UI	Select one program key, then long press it for 2s, and input strings for Label to define a name.	
Web UI	Phone Keys → Program Key	

12.1.4 AudioHub via BT Programmable Key Configuration through Phone UI

After the M7 DeskPhone connects with a mobile phone via Bluetooth, you can make and receive mobile calls on the IP phone, and hold/retrieve/end mobile calls from the IP phone. You can also use your IP phone as a Bluetooth speaker for your mobile phone.

When a mobile phone is connected via Bluetooth, the phone UI will generate a mobile account programmable key automatically. You can also long press a programmable key to manually configure a mobile account programmable key.



12.1.5 AudioHub via BT Programmable Key Configuration Parameters

The following table lists the parameters you can use to configure the AudioHub function.

Parameter	**ProgramKeyXType**	**config.xml**
Description	It configures the programmable key type. X can be number 1~20 for M3 or 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	68 - Mobile Account	
Default	0	
Phone UI	Select one program key, then long press it for 2s, and select Key Type as Mobile Account.	
Web UI	Phone Keys → Program Key	

Parameter	ProgramKeyXLabel	config.xml
Description	It configures the programmable key label. X can be number 1~20 for M3 or 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	strings	
Default	Blank	
Phone UI	Select one program key, then long press it for 2s, and input strings for Label to define a name	
Web UI	Phone Keys → Program Key	

12.2 X-party Conference

The ALE Myriad Series M3/M5/M7 DeskPhones have the capability to launch a 5-party conference by local.

The M8 phone have the capability to launch a 12-party conference by local.

Note: When the phone audio codec is configured as Opus + Super Wide Band, it only supports 4-party conference. When the phone audio codec is configured as Opus + Wide Band, it only supports 10-party conference.

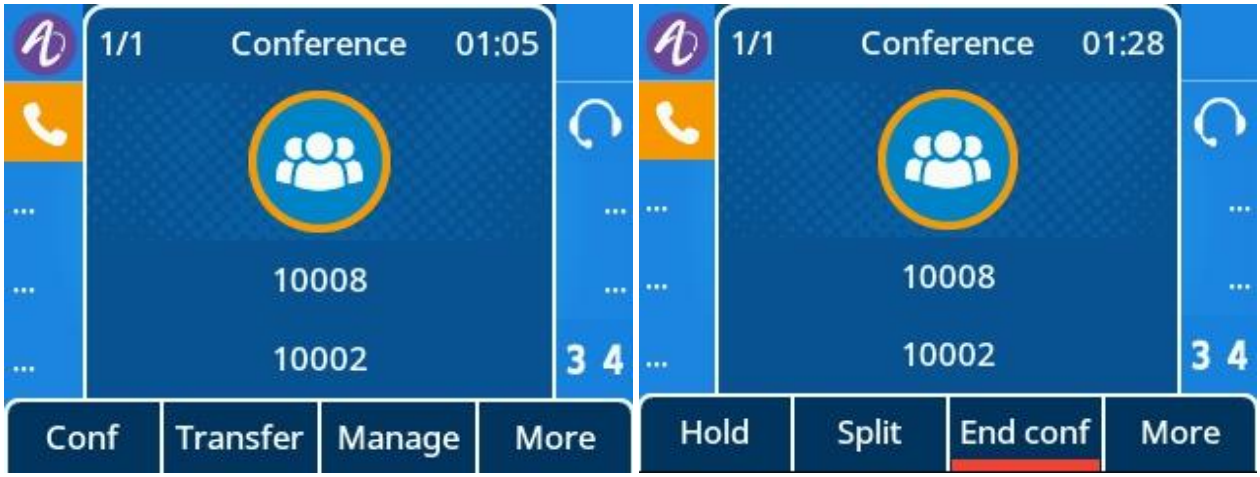
After establishing 3-party conference, users can press 'Conf' button to add a new user then press 'Join' button to merge the new user to current conference.

The phones support split/remove during conference.

The improvements include:

- Allow an incoming call when there is an active conference
- Split conference to separated hold calls
- Remove conference participants

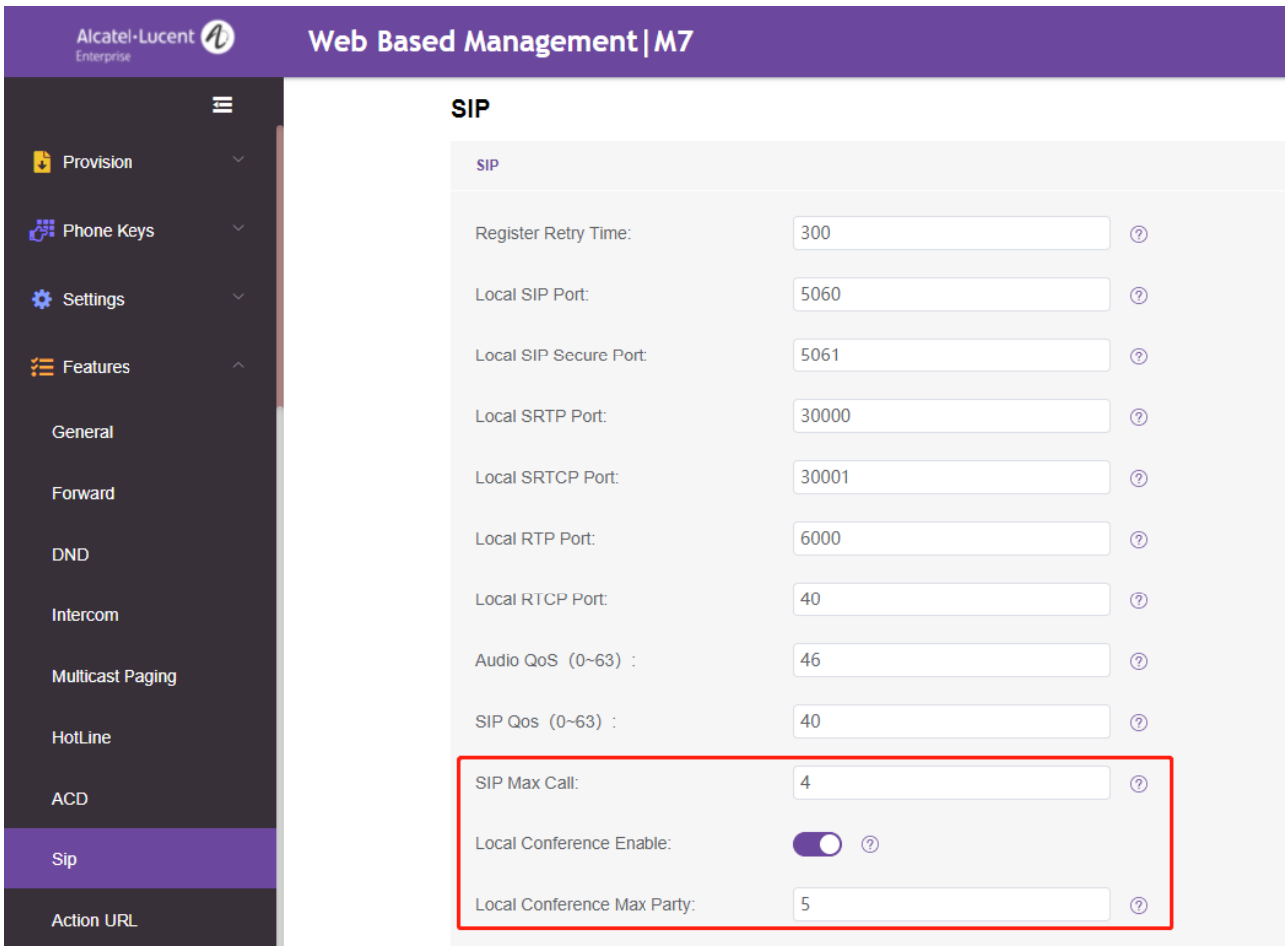
The menu in conference state has changed. It has 6 menus now and "Split" & "Manage" are added.



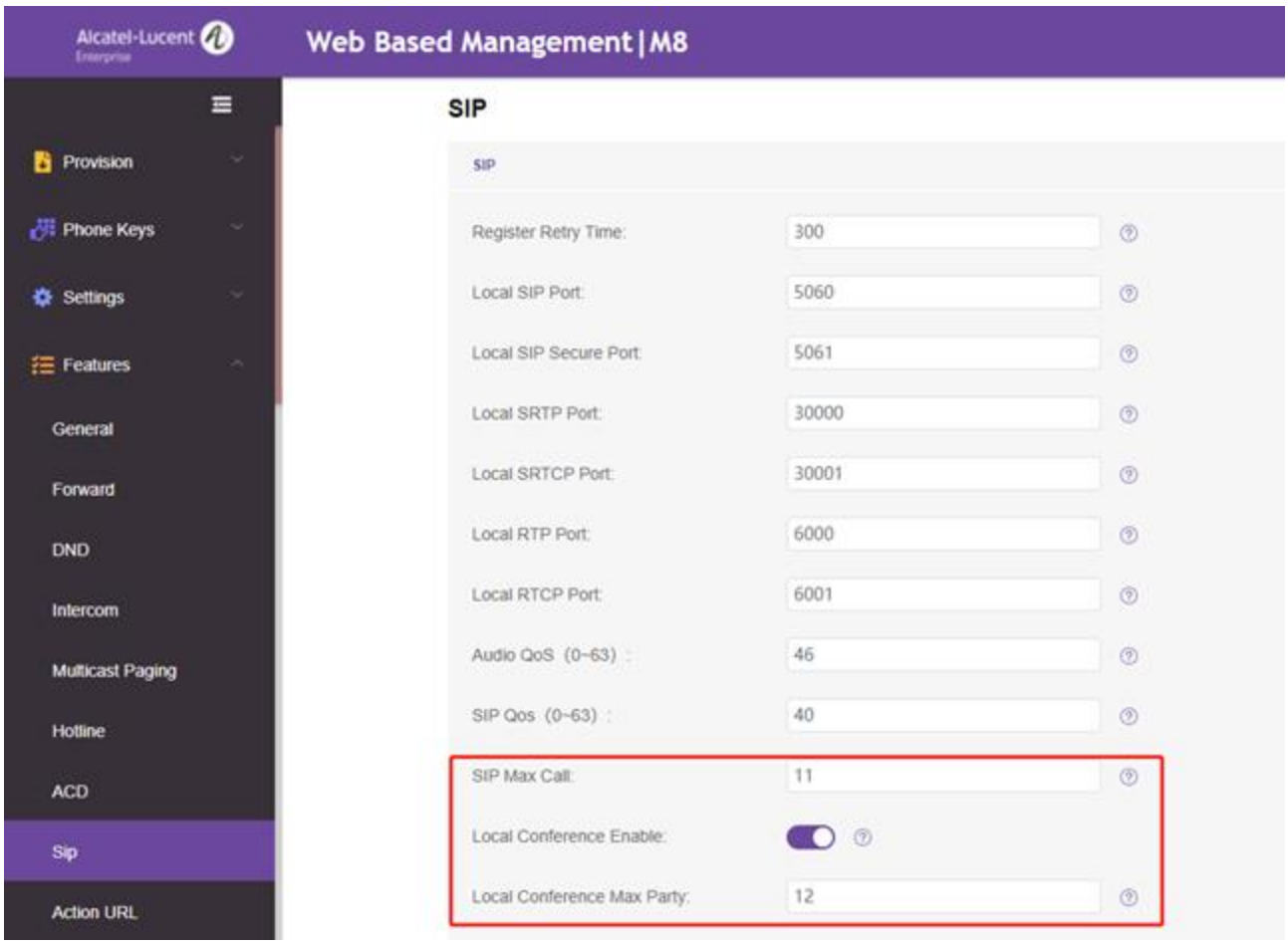
12.2.1 X-party Conference Configuration via Web UI

You can configure local conference via the Web UI path: Features → SIP.

M3/M5/M7: The following figure shows the 5-party conference configuration.

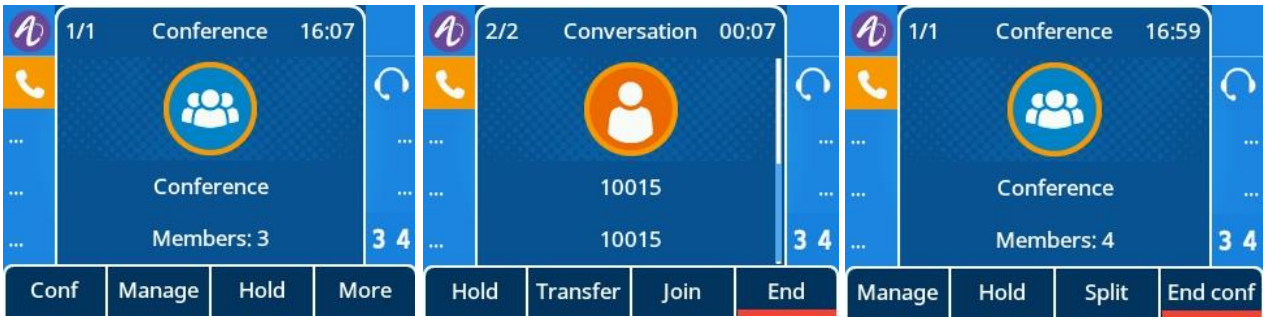


M8: The following figure shows the 12-party conference configuration.

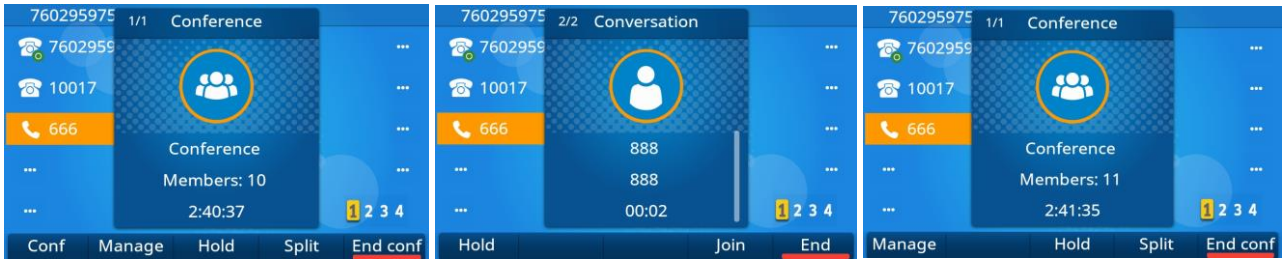


12.2.2 X-party Conference Configuration via Phone UI

5-party conference:



12-party conference:



12.2.3 X-party conference Configuration Parameters

The following table lists the parameters you can use to configure X-party conference.

Parameter	SIPLocalConfEnable	config.xml

Description	It enables or disables local conference function.	
Permitted Values	false - disable true - enable	
Default	true	
Web UI	Features → Sip	
Parameter	**SIPMaxCall**	**config.xml**
Description	It defines the max call capacity of the phone.	
Permitted Values	M3/M5/M7: 1-4 M8: 1-11	
Default	M3/M5/M7: 2 M8: 11	
Web UI	Features → Sip	
Parameter	**LocalConfPartyMax**	**config.xml**
Description	It defines the max party capacity of a phone conference.	
Permitted Values	M3/M5/M7: 3-5 M8: 3-12	
Default	M3/M5/M7: 3 M8: 12	
Web UI	Features → Sip	

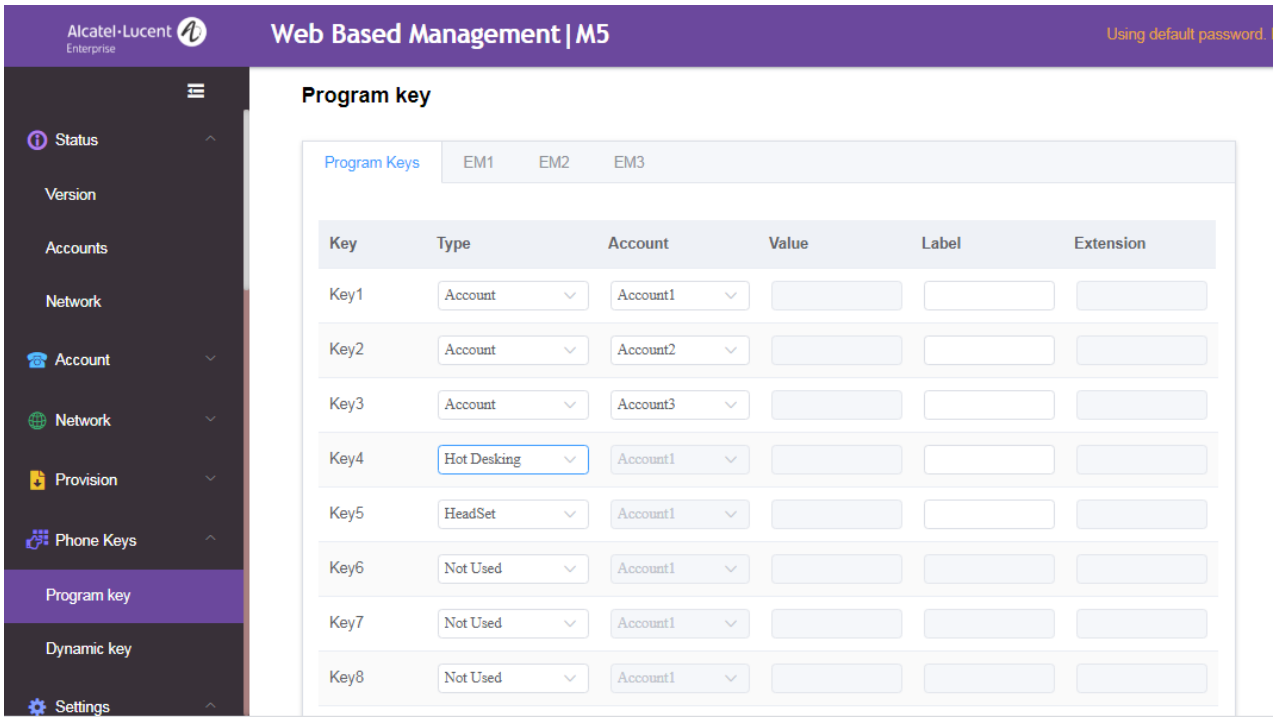
12.3 Hot Desking

The ALE Myriad Series phones all support Hot Desking feature with the same behavior.

Hot desking feature is working for a shared phone which can be used when employees are not in their office and with no phone in hand. Then they can log in a shared phone by hot desking feature. Hot desking allows the user to clear pre-registration configurations of all accounts on the IP phone and then login to their own user account.

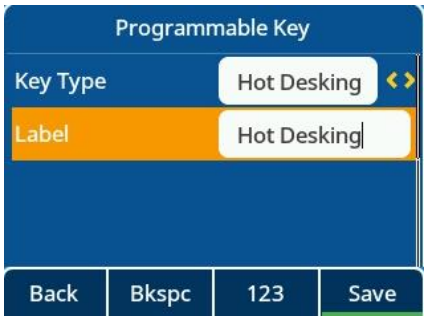
On the shared phone, you first need to assign a Hot Desking key.

12.3.1 Hot Desking Key Configuration via Web UI



12.3.2 Hot Desking Key Configuration via Phone UI

Long press a program key more than 2s and select the Key Type as Hot Desking.



Press program key to activate Hot Desking for the ALE Myriad Series phones.

Login in the number which needs to be registered in myriad phone with correct password.

12.3.3 Hot Desking Configuration Parameters

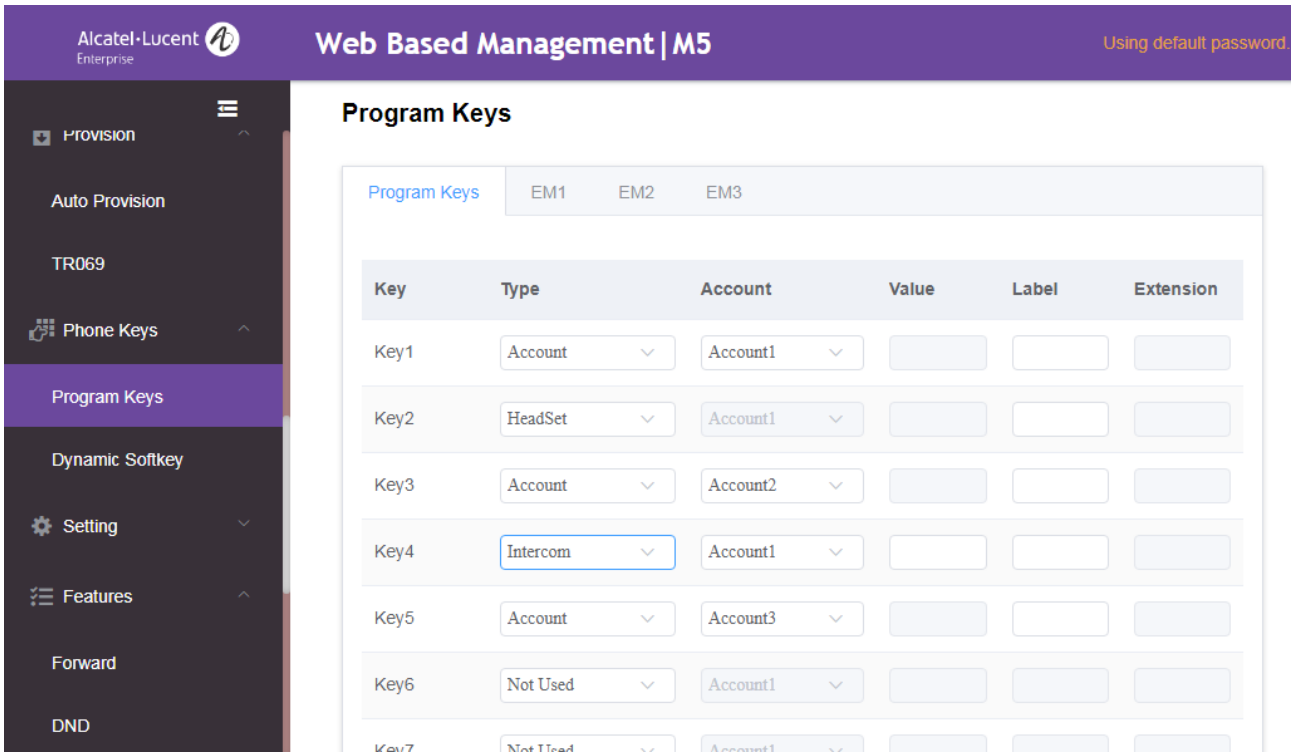
The following table lists the parameters you can use to configure hot desking.

Parameter	**ProgramKeyXType**	**config.xml**
Description	It configures the programmable key type. X can be number 1~20 for M3 or 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	11 - Hot Desking	
Default	0	
Phone UI	Select one program key, then long press it for 2s, and select KeyType as Hot Desking.	
Web UI	Phone Keys → Program Key	
Parameter	**ProgramKeyXLabel**	**config.xml**
Description	It configures the programmable key label. X can be number 1~20 for M3 or 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	strings	
Default	Blank	
Phone UI	Select one programkey, then long press it for 2s, and input strings for label to define a name	
Web UI	Phone Keys → Program Key	

12.4 Intercom

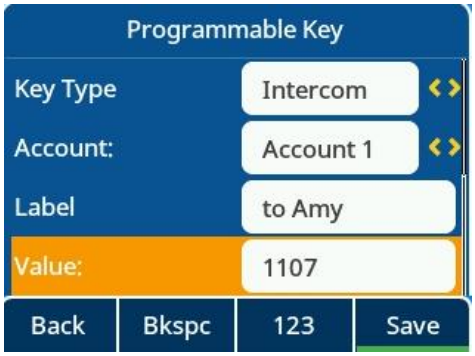
Intercom is a useful feature in an office environment to quickly connect with the operator or the secretary. You can press the intercom key to place a call to a contact that will be answered automatically on the contact's phone as long as the contact is in idle state or during an active call.

12.4.1 Intercom Key Configuration via Web UI



12.4.2 Outgoing Intercom Configuration via Phone UI

Long press a program key more than 2s, select the Key Type as Intercom, and then fill in the corresponding settings.



12.4.3 Outgoing Intercom Configuration Parameters

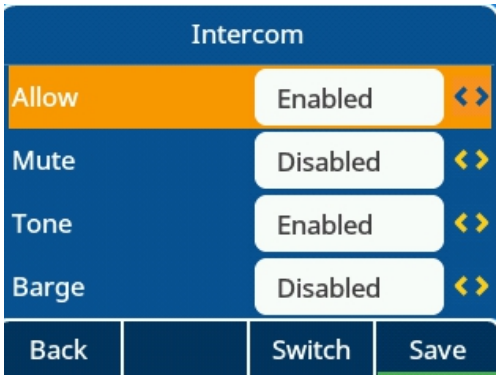
The following table lists the parameters you can use to configure intercom for outgoing call.

Parameter	**ProgramKeyXType**	**config.xml**
Description	It configures the programmable key type. X can be number 1~20 for M3 or 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	21 - Intercom	
Default	0	
Phone UI	Select one program key, then long press it for 2s, and select Key Type as Intercom.	
Web UI	Phone Keys → Program Key	
Parameter	**ProgramKeyXAccount**	**config.xml**

Description	It configures the account index of program key. X can be number 1~20 for M3 or 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	1~8 **Note**: For M8, the permitted values can be 1~20.	
Default	1	
Phone UI	Select one program key, then long press it for 2s, and select the account intended to use intercom.	
Web UI	Phone Keys → Program Key	
Parameter	**ProgramKeyXLabel**	**config.xml**
Description	It configures the programmable key label. X can be number 1~20 for M3 or 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	strings	
Default	Blank	
Phone UI	Select one program key, long press it for 2s, and then input label name.	
Web UI	Phone Keys → Program Key	
Parameter	**ProgramKeyXValue**	**config.xml**
Description	It configures program key number. X can be number 1~20 for M3 or 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	strings	
Default	Blank	
Phone UI	Select one program key, then long press it for 2s, and input the outgoing call number for this program key.	
Web UI	Phone Keys → Program Key	

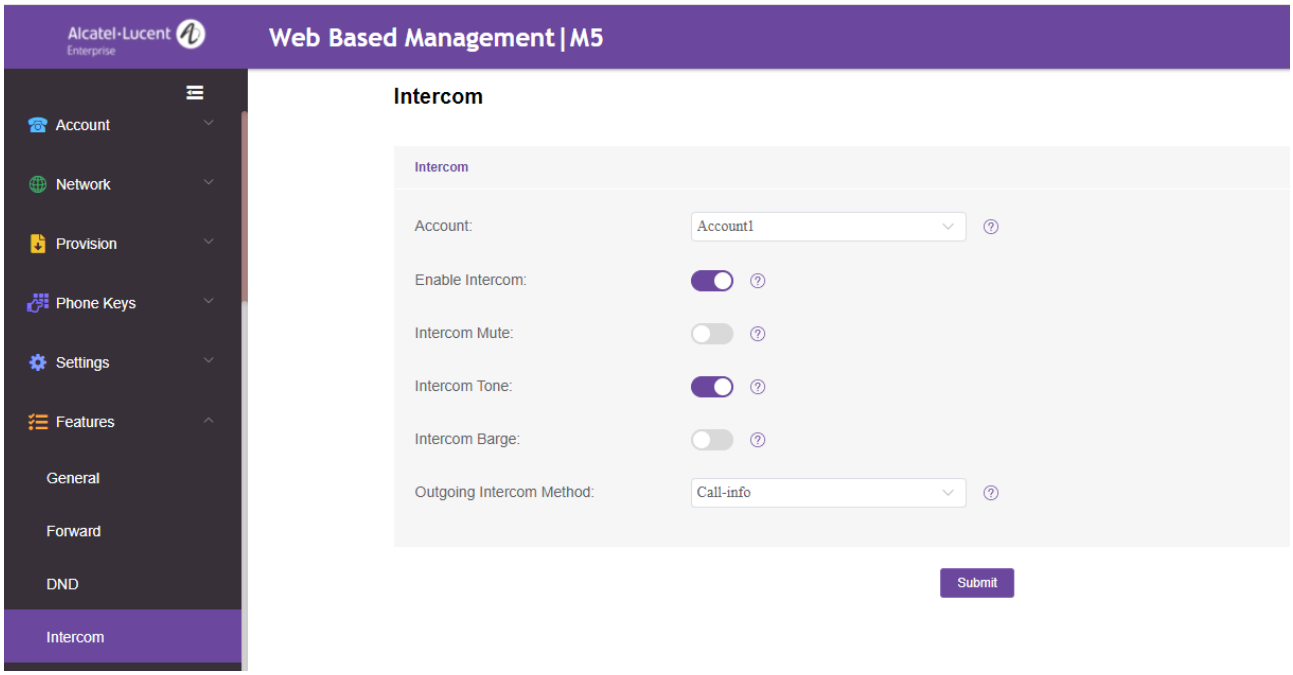
12.4.4 Incoming Intercom Configuration via Phone UI

You can configure incoming intercom via the Phone UI path Menu → Features → Intercom by selecting one account and entering the intercom setting.



12.4.5 Incoming Intercom Configuration via Web UI

You can configure incoming intercom via the Web UI path: Features → Intercom.



12.4.6 Incoming Intercom Configuration Parameters

The following table lists the parameters you can use to configure intercom for an incoming call.

Note: X means account ID and it can be number 1~8 for M3/M5/M7, 1-20 for M8.

Parameter	**AccountXIntercomEnable**	**config.xml**
Description	If it is set to true, the phone may auto answer an incoming call if requested by SIPUA layer.	
Permitted Values	false - disable true - enable	
Default	true	
Phone UI	Menu → Feature → Intercom	
Web UI	Features → Intercom → Enable Intercom	
Parameter	**AccountXIntercomMuteEnable**	**config.xml**
Description	It enables or disables when the phone auto answers an intercom call. It will mute.	
Permitted Values	false - disable true - enable	
Default	false	
Phone UI	Menu → Features → Intercom	
Web UI	Features → Intercom → Intercom Mute	
Parameter	**AccountXIntercomToneEnable**	**config.xml**

Description	It enables or disables when the phone auto answers an intercom call. It will play a warning tone.	
Permitted Values	false - disable true - enable	
Default	true	
Phone UI	Menu → Features → Intercom	
Web UI	Features → Intercom → Intercom Tone	
Parameter	**AccountXIntercomBargeEnable**	**config.xml**
Description	It enables or disables when the phone auto answers a second intercom call. It will hold the previous and answer the second.	
Permitted Values	false - disable true - enable	
Default	false	
Phone UI	Menu → Features → Intercom	
Web UI	Features → Intercom → Intercom Barge	
Parameter	**AccountXOutgoingIntercomMethod**	**config.xml**
Description	It configures the type of intercom for account.	
Permitted Values	0 - Call-info 1 - Alert-info 2 - Answer-mode	
Default	0	
Phone UI	Menu → Features → Intercom	
Web UI	Features → Intercom → Outgoing Intercom Method	

12.5 Push-To-Talk

PTT (Push-To-Talk) is the same as Intercom. It is another kind of Intercom. The main difference is that PTT feature needs long pressing the key to establish a call and release key to release the call, while Intercom is a one-click key.

Note: A Key Type “PTT” is applicable to Program Key/EM Key and the key type ID is 70.

12.6 Voicemail

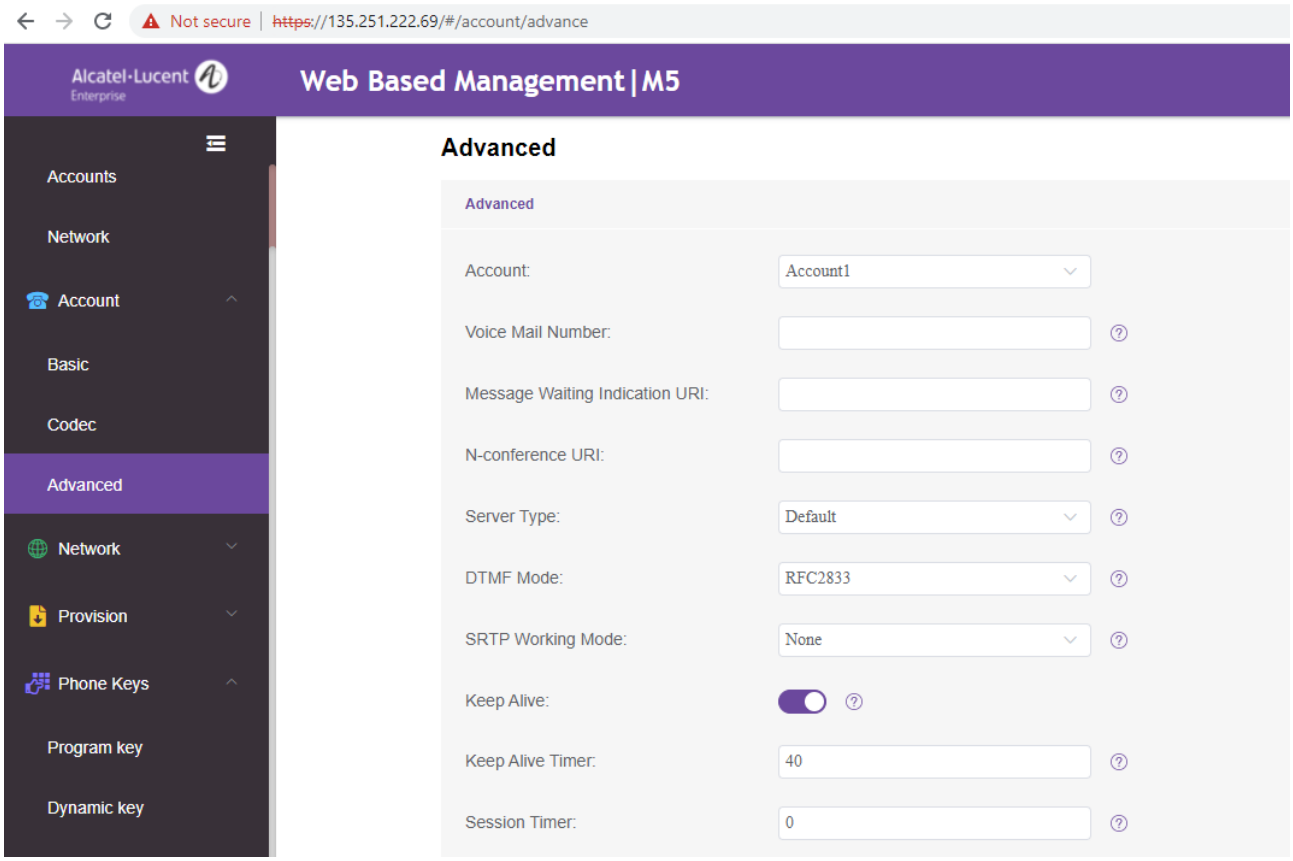
Voicemail is an application which can save voice messages from other users when the phone is busy or unavailable. The user can also send messages to other users by his voicemail box.

12.6.1 Voicemail Configuration via Phone UI

You can view the Voicemail via the Phone UI path: Menu → Message → Voicemail → View Voicemail, and also can set voice mail number by path: Menu → Message → Voicemail → Set Voicemail Number.

12.6.2 Voicemail Configuration via Web UI

You can configure voicemail via Web UI in Account Advanced setting.



12.6.3 Voicemail Configuration Parameters

The following table lists the parameters you can use to configure intercom for incoming call.

Note: X means account ID and it can be number 1~8 for M3/M5/M7, and 1-20 for M8.

Parameter	**AccountXVmNumber**	**config.xml**
Description	It configures voicemail number for accountX.	
Permitted Values	string	
Default	Blank	
Phone UI	Menu → Message → Voicemail → Set Voicemail Number	
Web UI	Account → Advanced	

Parameter	AccountXMwiUri	config.xml
Description	It configures message waiting indication server address for account. It enables or disables phone to pop up the message notification when receiving new voicemail.	
Permitted Values	string	
Default	Blank	
Web UI	Account → Advanced	

12.7 BLF

The ALE Myriad Series phones support BLF feature. BLF (Busy Lamp field) is a function which can monitor another phone number's call status and can display the status on the BLF programkey LED. You can also make speed dial call to the monitored phone number.

For the M3/M5/M7 phone, the LED status for BLF feature is shown as below:

LED Status	Description
On (Blue)	Subscribe successfully and the monitored user is idle.
Fast-flashing Blue	The monitored user receives an incoming call.
Slow-flashing Blue	The monitored user is talking. The monitored user's conversation is placed on hold. The monitored user is dialing. The call is parked against the monitored user's phone number.
Off	Subscribe failed or the monitored user does not exist.

For the M8 phone, the LED status for BLF feature is shown as below:

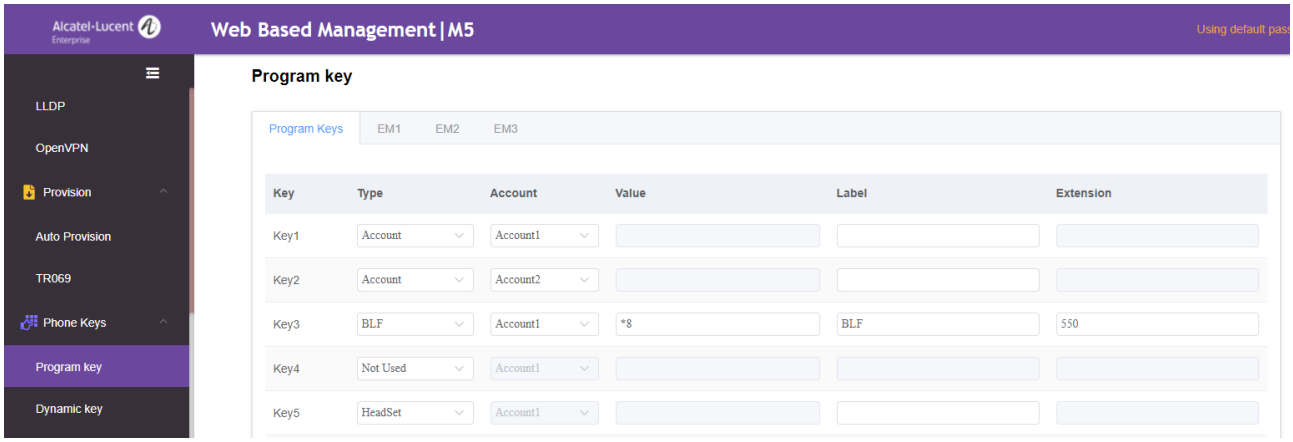
LED Status	Description
On (Blue)	Subscribe successfully and the monitored user is idle.
Fast-flashing Red	The monitored user is ringing or dialing.
Solid-Red	The monitored user is busy or in a call.
Slow-flashing Red	The monitored user's conversation is placed on hold. The call is parked against the monitored user's phone number.
Off	Subscribe failed or the monitored user does not exist.

12.7.1 BLF Configuration via Phone UI

You can configure BLF programmable key on the phone by selecting one soft key, long pressing it for 2s, and choosing the Key Type as BLF.

12.7.2 BLF Configuration via Web UI

You can configure one soft key as BLF on web by Phone Keys → Program Key.



12.7.3 BLF Configuration Parameters

The following table lists the parameters you can use to configure one softkey as BLF.

Parameter	**ProgramKeyXType**	**config.xml**
Description	It configures the programmable key type. X can be number 1~20 for M3 or 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	59 - BLF	
Default	0	
Phone UI	Select one soft key, long press it for 2s, and select Key Type as BLF.	
Web UI	Phone Keys → Program Key	
Parameter	**ProgramKeyXAccount**	**config.xml**
Description	It configures the account index of program key. X can be number 1~20 for M3, 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	1~8 **Note**: For M8, the permitted values can be 1~20.	
Default	1	
Phone UI	Select one program key, long press it for 2s, and select the account intended to use BLF.	
Web UI	Phone Keys → Program Key	

Parameter	ProgramKeyXLabel	config.xml
Description	It configures the programmable key label. X can be number 1~20 for M3 or 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	strings	
Default	Blank	
Phone UI	Select one program key, long press it for 2s, and input strings for Label to define a name	
Web UI	Phone Keys → Program Key	
Parameter	ProgramKeyXValue	config.xml
Description	It configures program key number. X can be number 1~20 for M3, 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	strings	
Default	Blank	
Phone UI	Select one program key, long press it for 2s, and input the outgoing call number for this programmable key	
Web UI	Phone Keys → Program Key	
Parameter	ProgramKeyXExtension	config.xml
Description	It configures program key extension. X can be number 1~20 for M3, 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	strings	
Default	Blank	
Phone UI	Select one programmable key, long press it for 2s, and input the pickup code prefix for this programmable key	
Web UI	Phone Keys → Program Key	

12.8 Call Pickup

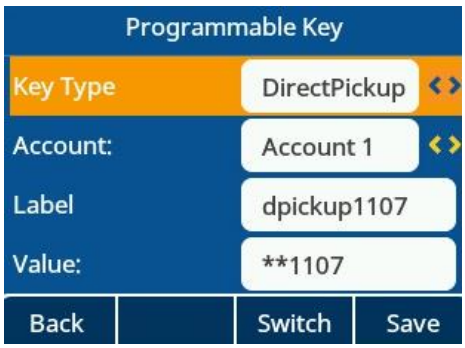
You can use call pickup to answer someone's incoming call on your phone using a pickup code.

The ALE Myriad Series phones support Directly Call Pickup and Group Call Pickup types.

- **Direct Call Pickup**: It allows you to pick up incoming calls to a specific phone.
- **Group Call Pickup**: It allows you to pick up incoming calls to any phone within a predefined group of phones.

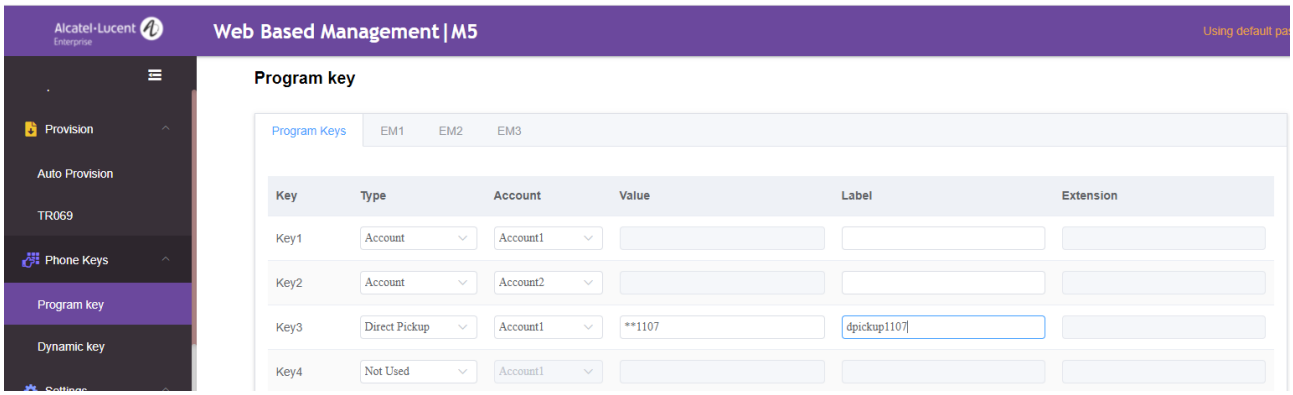
12.8.1 Direct Pickup Configuration via Phone UI

On the phone, you can select one softkey key, long press it for 2s, and choose the Key Type as DirectPickup.



12.8.2 Direct Pickup Configuration via Web UI

You can program one soft key as Direct Pickup type to perform directly pick up function.



12.8.3 Direct Pickup Configuration Parameters

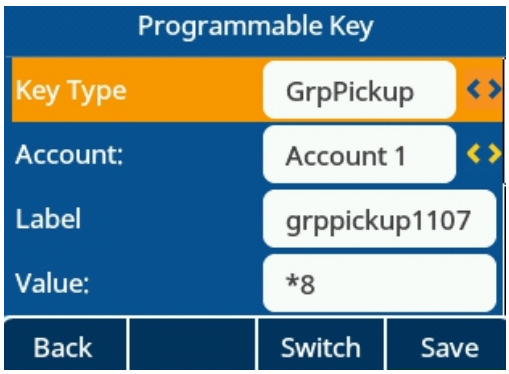
The following table lists the parameters you can use to configure one softkey to perform direct pickup function.

Parameter	**ProgramKeyXType**	**config.xml**
Description	It configures the programmable key type. X can be number 1~20 for M3, 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	15 - Direct Pickup	
Default	0	
Phone UI	Select one program key, long press it for 2s, and select Key Type as Direct Pickup.	
Web UI	Phone Keys → Program Key	
Parameter	**ProgramKeyXAccount**	**config.xml**
Description	It configures the account index of program key. X can be number 1~20 for M3, 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	1~8 **Note**: For M8, the permitted values can be 1~20.	
Default	1	
Phone UI	Select one program key, long press it for 2s, and select the account to use Direct Pickup	

Web UI	Phone Keys → Program Key	
Parameter	**ProgramKeyXLabel**	**config.xml**
Description	It configures the programmable key label. X can be number 1~20 for M3, and 1~28 for M5/M7.	
Permitted Values	strings	
Default	Blank	
Phone UI	Select one programmable key, long press it for 2s, and input the label name.	
Web UI	Phone Keys → Program Key	
Parameter	**ProgramKeyXValue**	**config.xml**
Description	It configures program key number. X can be number 1~20 for M3, and 1~28 for M5/M7.	
Permitted Values	strings	
Default	Blank	
Phone UI	Select one programmable key, long press it for 2s, and input the label name.	
Web UI	Phone Keys → Program Key	

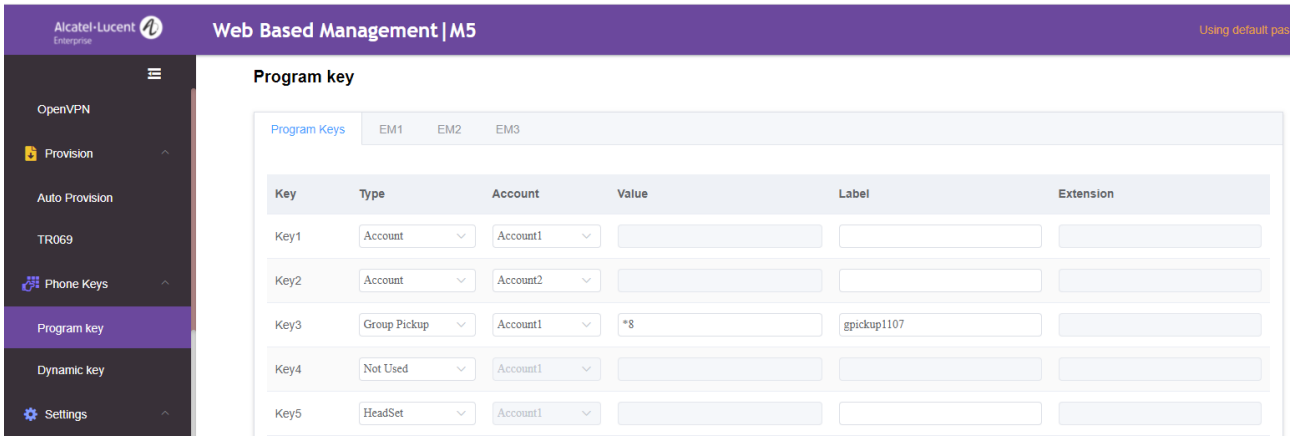
12.8.4 Group Pickup Configuration via Phone UI

You can program one soft key as Group Pickup by long pressing it for 2s, and selecting Key Type as GrpPickup.



12.8.5 Group Pickup Configuration via Web UI

You can program one softkey as Group Pickup type and define the Value and Label by path Phone Keys → Program Key.



12.8.6 Group Pickup Configuration Parameters

The following table lists the parameters you can use to configure one softkey to perform group pickup function.

Parameter	**ProgramKeyXType**	**config.xml**
Description	It configures the programmable key type. X can be number 1~20 for M3, 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	16 - Group Pickup	
Default	0	
Phone UI	Select one program key, long press it for 2s, and select Key Type as GrpPickup.	
Web UI	Phone Keys → Program Key	
Parameter	**ProgramKeyXAccount**	**config.xml**
Description	It configures the account index of program key. X can be number 1~20 for M3, 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	1~8 **Note**: For M8, the value can be 1~20.	
Default	1	
Phone UI	Select one program key, long press it for 2s, and select the account intended to use GrpPickup.	
Web UI	Phone Keys → Program Key	
Parameter	**ProgramKeyXLabel**	**config.xml**
Description	It configures the programmable key label. X can be number 1~20 for M3, 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	strings	
Default	Blank	

Phone UI	Select one program key, long press it for 2s, and input strings for label to define a name	
Web UI	Phone Keys → Program Key	
Parameter	**ProgramKeyXValue**	**config.xml**
Description	It configures program key number. X can be number 1~20 for M3, 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	strings	
Default	Blank	
Phone UI	Select one program key, long press it for 2s, and input strings for label to define pickup code	
Web UI	Phone Keys → Program Key	

12.9 Call Park & Retrieve

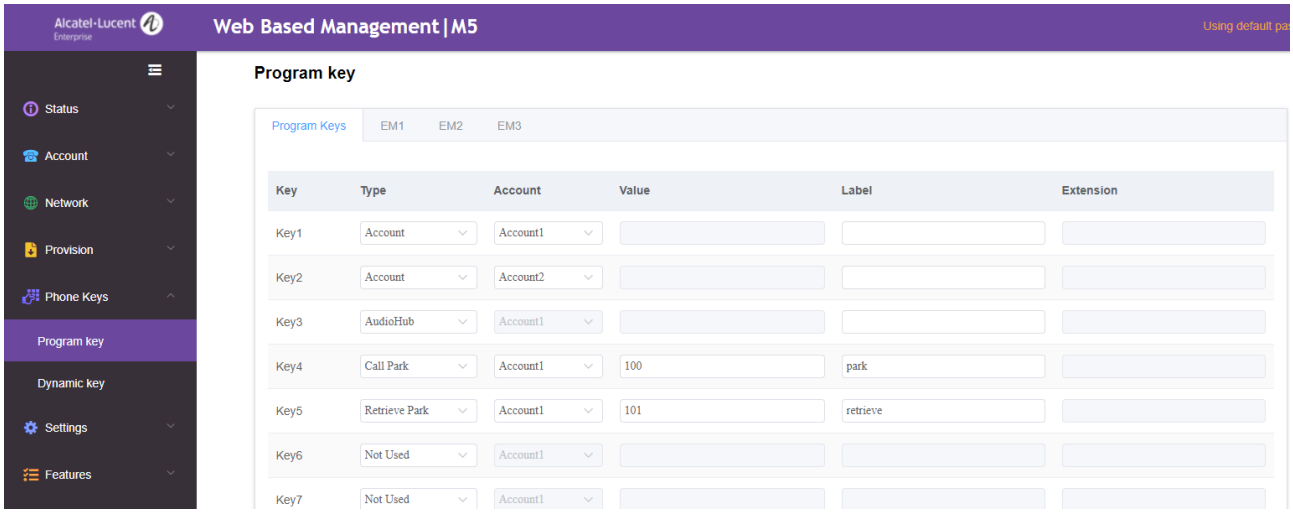
Call park allows users to park a call on a special extension. Retrieve park allows users to retrieve a parked call from another phone.

12.9.1 Call Park & Retrieve Configuration via Phone UI

You can program one softkey by long pressing it for 2s, and select Key Type as Call Park or Retrieve.

12.9.2 Call Park & Retrieve Configuration via Web UI

You can program one softkey as Call Park or Retrieve Park type and define the Value and Label by path Phone Keys → Program Key.



12.9.3 Call Park Configuration Parameters

The following table lists the parameters you can use to configure one softkey to perform call park function.

Parameter	**ProgramKeyXType**	**config.xml**
Description	It configures the programmable key type. X can be number 1~20 for M3, 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	17 - Call Park	
Default	0	
Phone UI	Select one program key, long press it for 2s, and select Key Type as Call Park.	
Web UI	Phone Keys → Program Key	
Parameter	**ProgramKeyXAccount**	**config.xml**
Description	It configures the account index of program key. X can be number 1~20 for M3, 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	1~8 **Note**: For M8, the value can be 1~20.	
Default	1	
Phone UI	Select one program key, long press it for 2s, and select the account intended to use Call Park.	
Web UI	Phone Keys → Program Key	
Parameter	**ProgramKeyXLabel**	**config.xml**
Description	It configures the programmable key label. X can be number 1~20 for M3 , 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	strings	
Default	Blank	
Phone UI	Select one program key, long press it for 2s, and input a label name.	
Web UI	Phone Keys → Program Key	
Parameter	**ProgramKeyXValue**	**config.xml**
Description	It configures program key number. X can be number 1~20 for M3, 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	strings	
Default	Blank	
Phone UI	Select one program key, long press it for 2s, and input a label name	
Web UI	Phone Keys → Program Key	

Parameter	FeatureCallParkMode	config.xml
Description	It configures the call park method.	
Permitted Values	0 - Direct call 1 - Blind transfer call	
Default	1	

12.9.4 Retrieve Park configuration parameters

The following table lists the parameters you can use to configure one softkey to perform retrieve park function.

Parameter	ProgramKeyXType	config.xml
Description	It configures the programmable key type. X can be number 1~20 for M3, 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	22 – Retrieve Park	
Default	0	
Phone UI	Select one program key, long press it for 2s, and select Key Type as Retrieve.	
Web UI	Phone Keys → Program Key	
Parameter	ProgramKeyXAccount	config.xml
Description	It configures the account index of program key. X can be number 1~20 for M3, 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	1~8 **Note**: For M8, the value can be 1~20.	
Default	1	
Phone UI	Select one program key, long press it for 2s, and select the account intended to use Retrieve.	
Web UI	Phone Keys → Program Key	
Parameter	ProgramKeyXLabel	config.xml
Description	It configures the programmable key label. X can be number 1~20 for M3, 1~28 for M5/M7 and 1~36 for M8.	
Permitted Values	strings	
Default	Blank	
Phone UI	Select one program key, long press it for 2s, and input a label name.	
Web UI	Phone Keys → Program Key	
Parameter	ProgramKeyXValue	config.xml

Description	It configures program key number. X can be number 1~20 for M3, 1~28 for M5/M7 and 1~36 for M8.
Permitted Values	strings
Default	Blank
Phone UI	Select one program key, long press it for 2s, and input a label name.
Web UI	Phone Keys → Program Key

12.10 Shared Line Appearance (SLA)

ALE phones support Shared Line Appearance (SLA) to share a line.

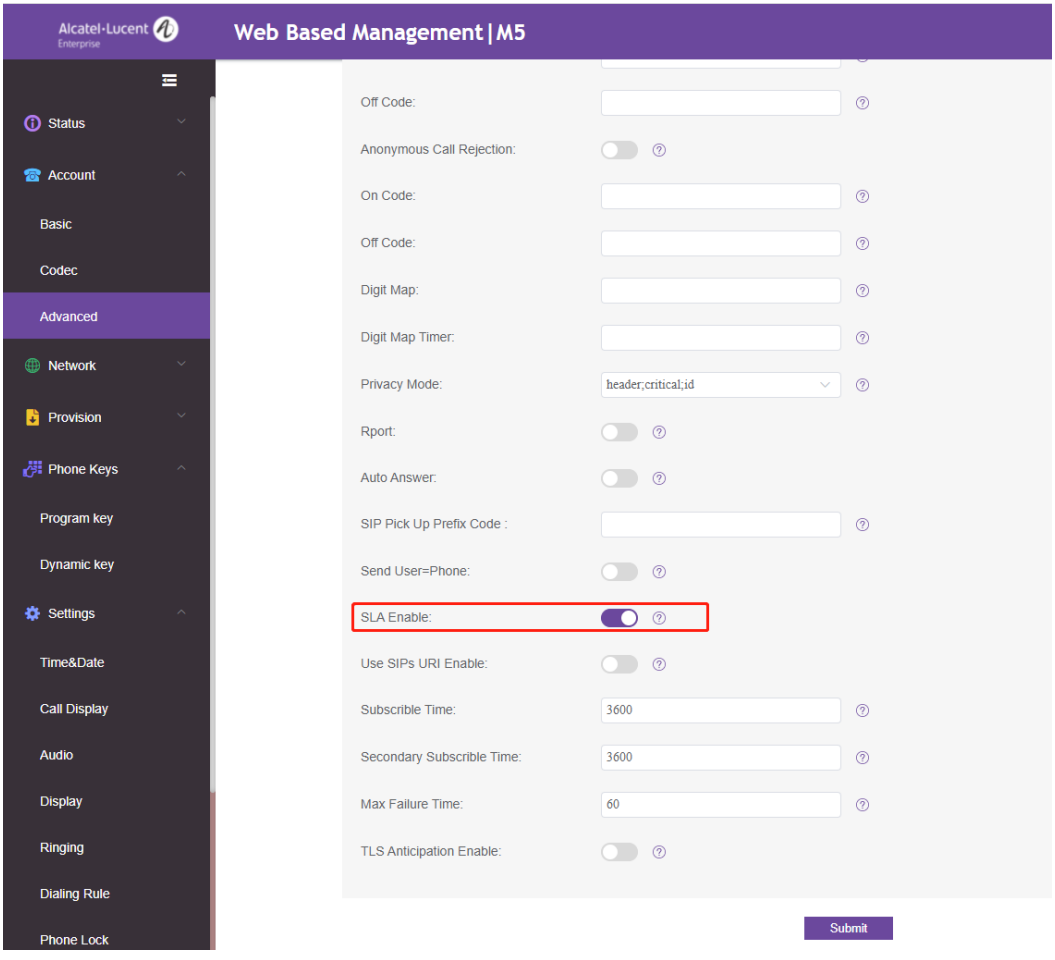
Shared line appearances enable more than one phone to share the same line or registration. The methods you use vary with the SIP server you are using.

The shared line users have the ability to do the following:

- Place and answer calls
- Place a call on hold
- Retrieve a held call remotely
- Barge in an active call
- Pull a shared call

12.10.1 SLA Configuration via Web UI

You can enable SLA feature for specific account via the Web UI path: Account → Advanced.



12.10.2 SLA Configuration Parameters

The following table lists the parameters you can use to enable SLA feature for one account.

Parameter	AccountXSlaEnable	config.xml
Description	It enables or disables the SLA function for account X. X can be number 1~8 for M3/M5/M7 and 1~20 for M8.	
Permitted Values	false - disable true - enable	
Default	false	
Web UI	Account → Advanced	

12.11 Call Completion

When the user places a call and the callee is temporarily unavailable to answer the call, SIPMMI will save the callee's number and use the SUBSCRIBE/NOTIFY method to subscriber callee's status.

When the phone receives NOTIFY message with "terminal" status:

- If the phone is idle, the phone screen will prompt whether to dial the number; If yes, the phone will dial the last outgoing failed number.
- If the phone is not idle, the phone will not prompt until the phone is idle.

The following table lists the parameters you can use to configure Call Completion feature.

Parameter	FeatureCallCompletionEnable	config.xml
Description	It enables or disables Call Completion feature.	
Permitted Values	false - disable true - enable	
Default	false	
Web UI	Features → General	

12.12 Automatic Call Distribution (ACD)

ACD enables the use of IP phones in a call-center role by automatically distributing incoming calls to available users or agents. You can enable users to use their phone in a call center agent/a supervisor role on a supported call server.

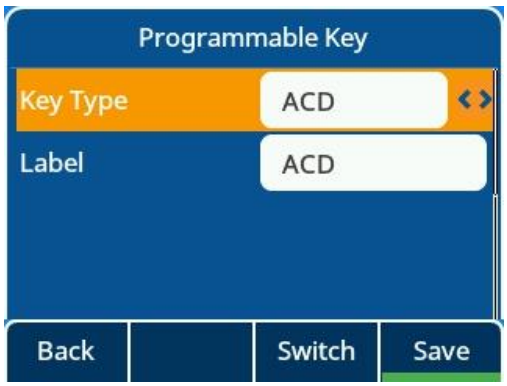
The users can sign in and sign out of the ACD state as call center agent using soft keys. The server distributes calls to the agent when the agent state is available, and stops distributing calls when the agent changes state to unavailable.

The IP phone remains in the unavailable status until the agent manually changes the IP phone status. You can configure how long the IP phone remains unavailable state and changes to available automatically on a supported call server. The methods you use vary with the SIP server you are using.

12.12.1 ACD Key Configuration via Phone UI

You can configure a soft key as ACD key to log into the ACD system. The ACD key on the IP phone indicates the ACD state.

On the phone, select one soft key, long press it for 2s, and select Key Type as ACD.



The following shows configuration for an ACD key.

<setting id="ProgramKey4Type" value="42"/>

<setting id="ProgramKey4Label" value="ACD"/>

After provisioning, an ACD key is available on the phone, and you can press the ACD key to log into the ACD system.

12.12.2 ACD Configuration Parameters

The following table lists the parameters you can use to configure ACD function.

Note: X means account ID and it can be number 1~8 for M3/M5/M7, and 1-20 for M8.

Parameter	**AccountXAcdEnable**	**config.xml**
Description	It enables or disables Acd feature for account.	
Permitted Values	false - disable true - enable	
Default	false	
Parameter	**FeatureAcdAutoAvailableEnable**	**config.xml**
Description	It enables or disables the IP phone to automatically change the status of the ACD agent to available after the designated time.	
Permitted Values	false - disable true - enable	
Default	false	
Web UI	Features → ACD → ACD Auto Available Enable	
Parameter	**FeatureAcdAutoAvailableTimeout**	**config.xml**
Description	It configures the interval (in seconds) for the status of the ACD agent to be automatically changed to available.	
Permitted Values	NUMERIC[0,120]	
Default	60	
Web UI	Features → ACD → ACD Auto Available Timeout (0~120s)	
Parameter	**AccountXAcdInitialState**	**config.xml**

Description	It configures the initial agent state for account.	
Permitted Values	1 - Available 2 - Unavailable	
Default	1	
Parameter	**FeatureAcdReasonCodeX** **Note:** X can is 1~10	**config.xml**
Description	It configures the ACD Reason Code for account.	
Permitted Values	strings	
Default	Blank	
Parameter	**FeatureAcdReasonNameX** **Note:** X can is 1~10	**config.xml**
Description	It configures the ACD Reason Name for account.	
Permitted Values	Strings	
Default	Blank	
Parameter	**FeatureAcdSoftkeyEnable**	**config.xml**
Description	It enables or disables the IP phone to display the ACD menu keys such as Login or Logout on desktop screen.	
Permitted Values	false - disable true - enable	
Default	false	

12.13 Broadsoft Hoteling

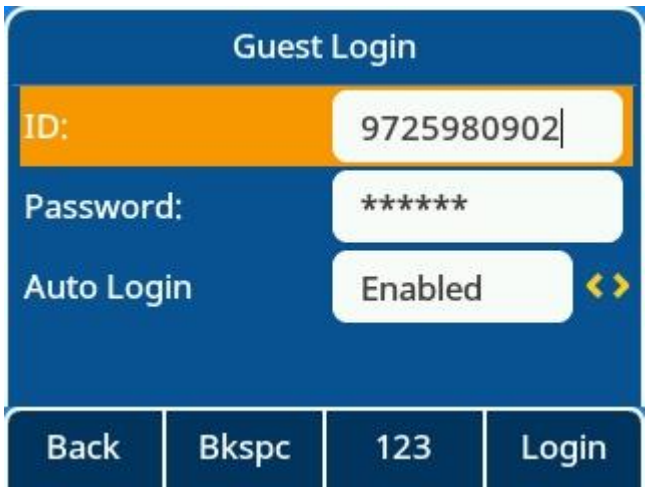
Cisco BroadWorks provides the capability to synchronize the hoteling guest user identity between the phone and Cisco BroadWorks. This enables the phone to display the hoteling guest's identity on the phone and also provides the signaling basis for the phone to allow a hoteling guest login via the phone interface. This feature is dedicated for Broadsoft platform.

- If hoteling feature is properly configured and the device is powered on, the device will send an initial subscription to get the hoteling status. If the phone is in guest in state, the receiving HotelingEvent NOTIFY will contain the Guest identity; if "FeatureHotelingSoftkeyEnable" is set to true (default is true), there will be a "GuOut" menu inserting into bottom bar used to help user to check out hoteling. The relevant account programmable key will also be changed to display as the guest number (as below 0902).

- When you guest out by pressing the menu “GuOut” or “Hoteling” programmable key, there will be a popup for confirmation.

- When you guest out successfully, the device will receive a HotelingEvent NOTIFY with empty guest identity, then the relevant account key display will refresh back to the host display (as below 9725980905). “GuOut” menu will be removed and replaced by “GuIn” menu.

- You can press “GuIn” or “Hoteling” programmable key to Guest In, and input guest user ID and password in login page.



12.13.1 Hoteling Key Configuration

You can configure a line key as Hoteling key to log into the Hotel system.

On the phone, select one programmable key, long press it for 2s, and select Key Type as Hoteling.

The following shows configuration for a Hoteling Key.

<setting id="ProgramKey5Type" value="69"/>

<setting id="ProgramKey5Label" value="Hoteling"/>

12.13.2 Hoteling Configuration Parameters

The following table lists the parameters you can use to configure Hoteling function.

Note: X means account ID. It can be number 1~8 for M3/M5/M7, and 1-20 for M8.

Parameter	**AccountXHotelingEnable**	**config.xml**
Description	It enables or disables the hoteling feature for account. **Note:** It works only if “AccountXServerType” is set to 6 (Broadsoft).	
Permitted Values	false - disable true - enable	
Default	false	
Parameter	**AccountXHotelingUserId**	**config.xml**
Description	It configures the user ID used to log into the guest profile.	
Permitted Values	strings	
Default	Blank	
Parameter	**AccountXHotelingPwd**	**config.xml**
Description	It configures the password used to log into the guest for account. **Note:** It works only if “AccountXServerType” is set to 6 (Broadsoft).	
Permitted Values	String within 99 characters	
Default	Blank	

Parameter	**HotelingAutoLoginEnable**	**config.xml**
Description	**Note:** It works only if “AccountXServerType” is set to 6 (Broadsoft).	
Permitted Values	false - disable true - enable	
Default	false	
Parameter	**FeatureHotelingSoftkeyEnable**	**config.xml**
Description	It enables or disables to display the ‘Guout’ menu in bottom bar. **Note:** It works only if “AccountXServerType” is set to 6 (Broadsoft).	
Permitted Values	false - disable true - enable	
Default	true	

13. Troubleshooting

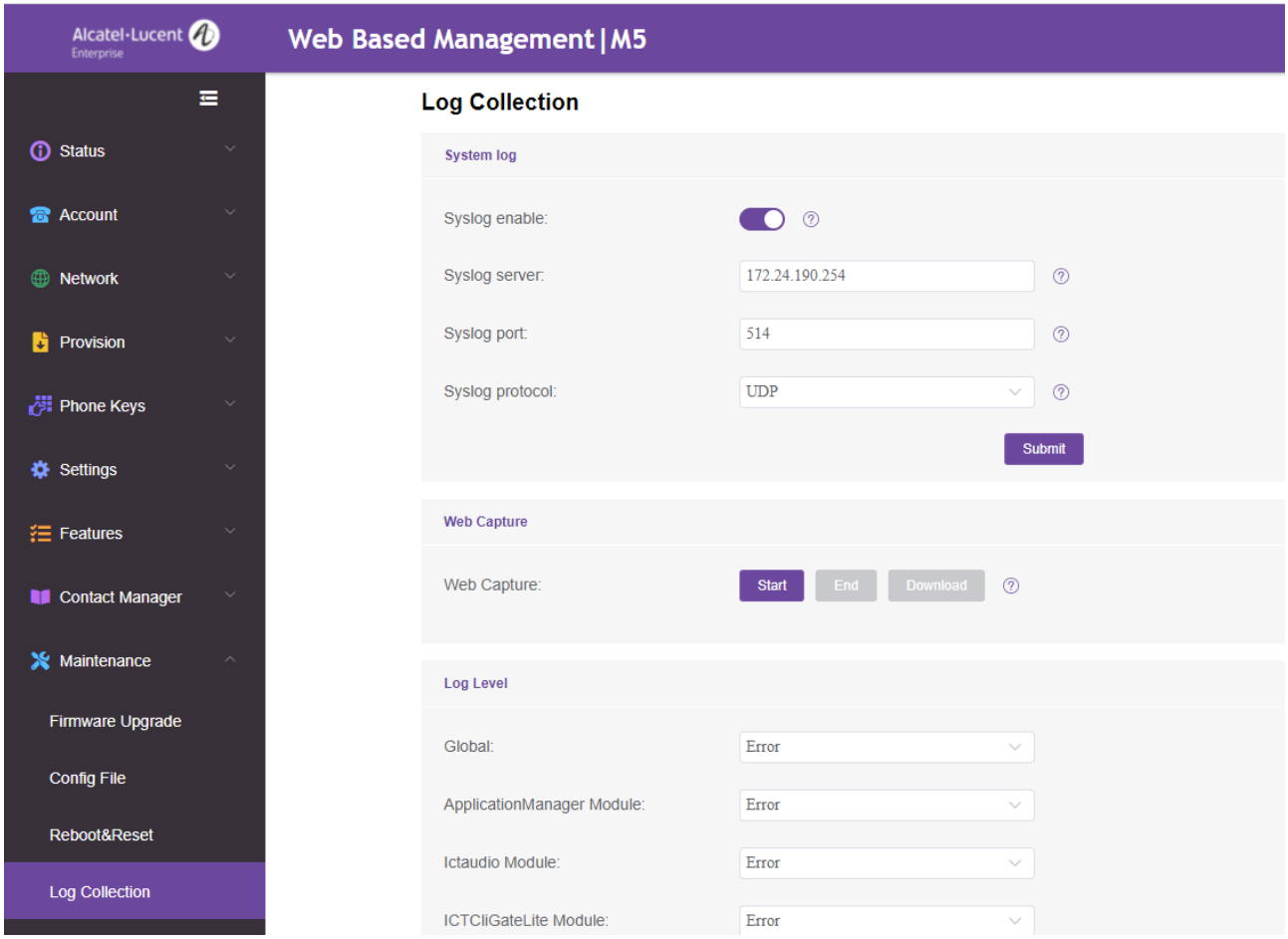
When the phone is not functioning normally, the user can try the following methods to restore normal operation of the phone or collect relevant information and send a problem report to the manufacture's technical support for analysis.

13.1 Log Collection

You can choose to generate the log files locally or send the log files to syslog server in real time, and use these log files to generate informational, analytic and troubleshoot phones.

13.1.1 Syslog Server

You can configure syslog via the Web UI path: Maintenance → Log Collection → Syslog



The following table lists the parameters you can use to configure syslog.

Parameter	**DeviceSyslogRemoteServerAddr**	**config.xml**
Description	It configures the syslog server address.	
Permitted Values	strings	
Default	Blank	
Web UI	Maintenance → Log Collection → Syslog	
Parameter	**DeviceSyslogRemoteServerPort**	**config.xml**
Description	It configures the syslog server port.	

Permitted Values	strings	
Default	514	
Web UI	Maintenance → Log Collection → Syslog	
Parameter	**DeviceSyslogRemoteServerProtocol**	**config.xml**
Description	It configures the syslog server protocol.	
Permitted Values	udp tcp	
Default	udp	
Web UI	Maintenance → Log Collection → Syslog	

13.1.2 Log File Backup

The IP phone can automatically upload call log file at regular intervals to the provisioning server or a specific server. If a call log file exists on the server, it will be overwritten.

The following table lists the parameters you can use to configure call log backup.

Parameter	**BackupUploadTime**	**config.<mac>.xml**
Description	It configures the interval time of uploading a backup file.	
Permitted Values	String	
Default	3600	
Parameter	**DeviceBackupUrl**	**config.<mac>.xml**
Description	It configures the URL which is used to upload and download the backup file.	
Permitted Values	String	
Default	Blank	
Parameter	**DeviceBackupUploadMethod**	**config.<mac>.xml**
Description	It configures the way (POST/PUT) to upload files.	
Permitted Values	0 - put 1 - post	
Default	0	
Parameter	**DeviceCallLogBackupEnable**	**config.<mac>.xml**
Description	It configures whether to enable or disable callLogBackup.	
Permitted Values	false true	
Default	false	

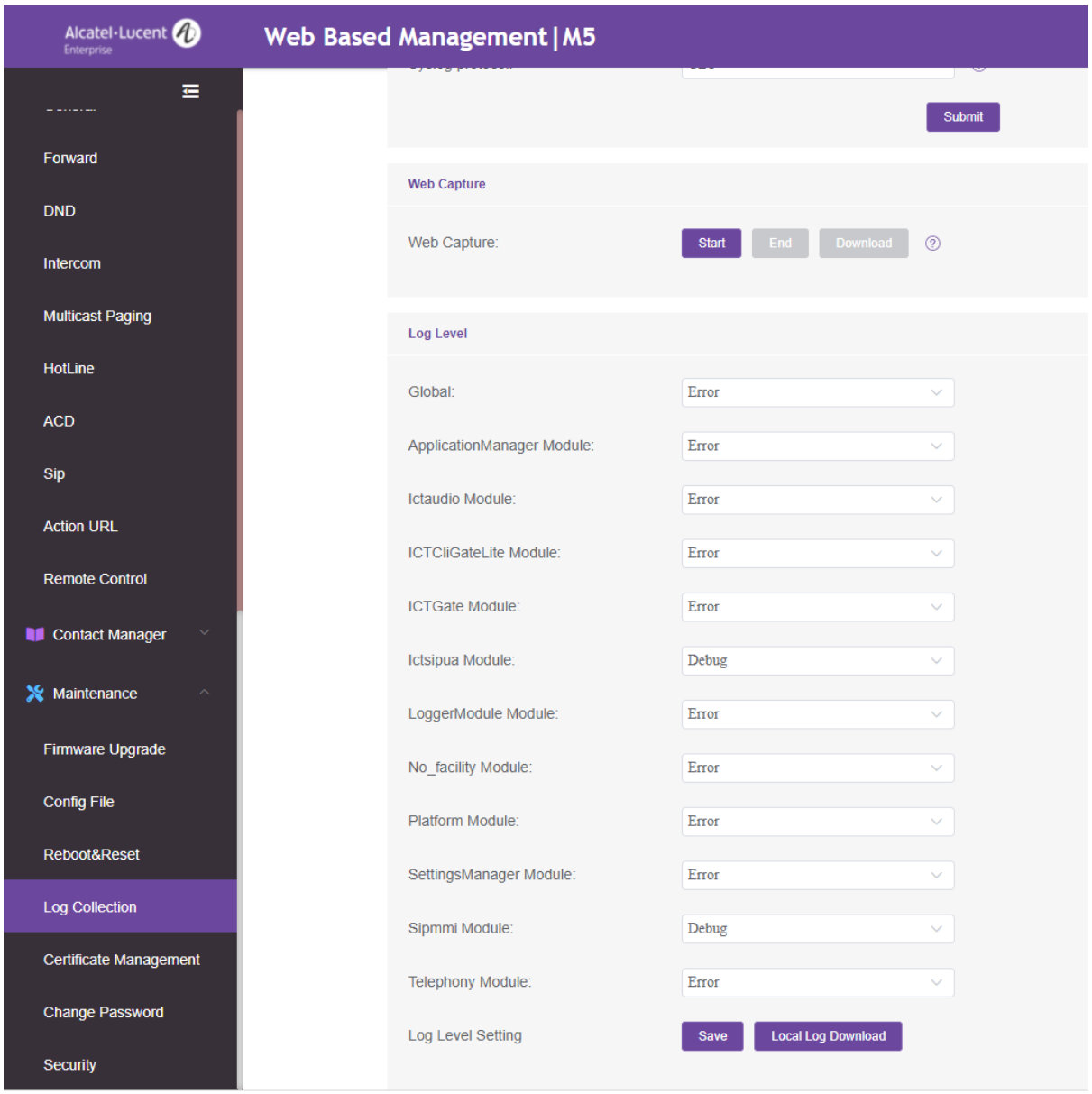
13.1.3 Log Level Setting

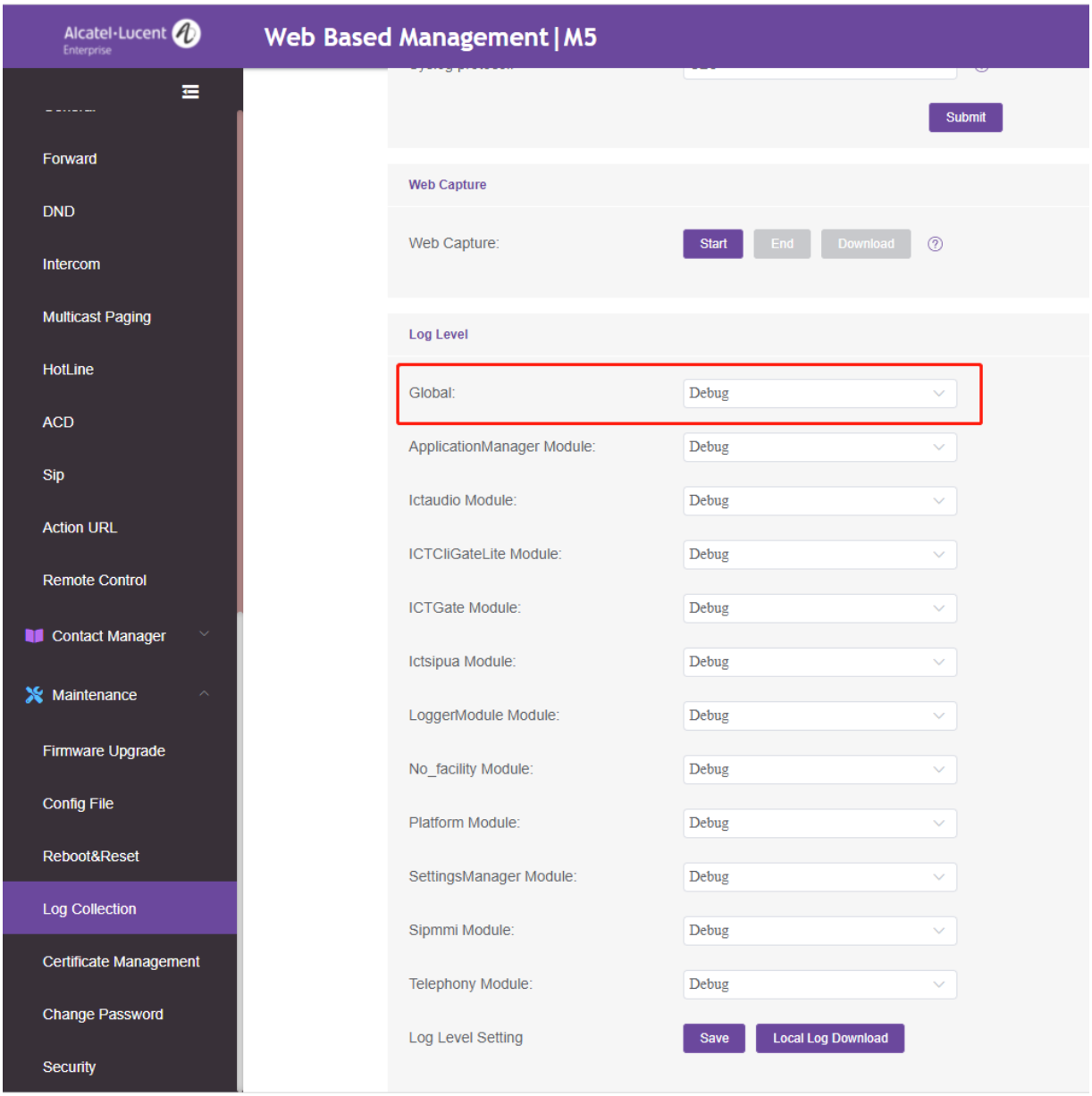
Log information is helpful when encountering a problem. The phone will generate log files according to the log level. ALE SIP phones support 6 levels for log recording, and more contents will be recorded with a higher level. The level from lowest to highest is: Emergency → Error → Warning → Notice → Informational → Debug. The default log level is Error. Generally, for serious issue, debug level is recommended.

13.1.3.1 Log Level Configuration via Web UI

To get the phone log information, you need to log into the phone web page, and then go to the menu: Maintenance → Log Collection.

- In log level field define either the relevant log level to debug in dropdown menu, or define all modules to debug level in “Global” drop down menu list. Then press “Save” button to save the configuration.





You can also configure global level via the parameter below:

Parameter	**DeviceLogLevel**	**config.<mac>.xml**
Description	It configures the minimum level of local log information recording.	
Permitted Values	0 - Emergency 1 - Error 2 - Warning 3 - Notice 4 - Informational 5 - Debug	
Default	1	
Web UI	Maintenance → Log Collection	

- Perform the operation and try to reproduce the problem.
- Download the log files.

Then you can send the log files to the technician to identify the problem.

13.1.3.2 Configure Log Level by Commands

Procedures to configure log level by command for each service module:

- Step 1: Enable SSH connection for the phone.

The table below shows how to enable SSH by parameters.

Parameter	**DeviceSecuritySshEnable**	**config. xml**
Description	It enables or disables SSH connection for the phone.	
Permitted Values	false - disable true - enable	
Default	1	
Web UI	Maintenance → Security	

- Step 2: Connect the phone and login with admin.
- Step 3: Input command “level” to check current log level setting.

```
$ level
   ACTIVITY           LEVEL      SUPPORT          DESTINATION
ApplicationManager     err        file        /var/log/ApplicationManager.log
ExternalProxy          err        file        /var/log/ExternalProxy.log
ictaudio               err        file        /var/log/ictaudio.log
ictbtmgr               err        file        /var/log/ictbtmgr.log
ICTCliGateLite         err        file        /var/log/ICTCliGateLite.log
ICTGate                err        file        /var/log/ICTGate.log
ictsipua               err        file        /var/log/ictsipua.log
LoggerModule           err        file        /var/log/LoggerModule.log
no_facility            err        file        /var/log/no_facility.log
Platform               err        file        /var/log/Platform.log
SettingsManager        err        file        /var/log/SettingsManager.log
sipmmi                 err        file        /var/log/sipmmi.log
Telephony              err        file        /var/log/Telephony.log
```

- Step 4: Set log level for specific the phone’s service module. For example, set “ictsipua” module as debug level, and then input “level ictsipua debug”.

```
$ level ictsipua debug
Level debug for facility : ictsipua OK
```

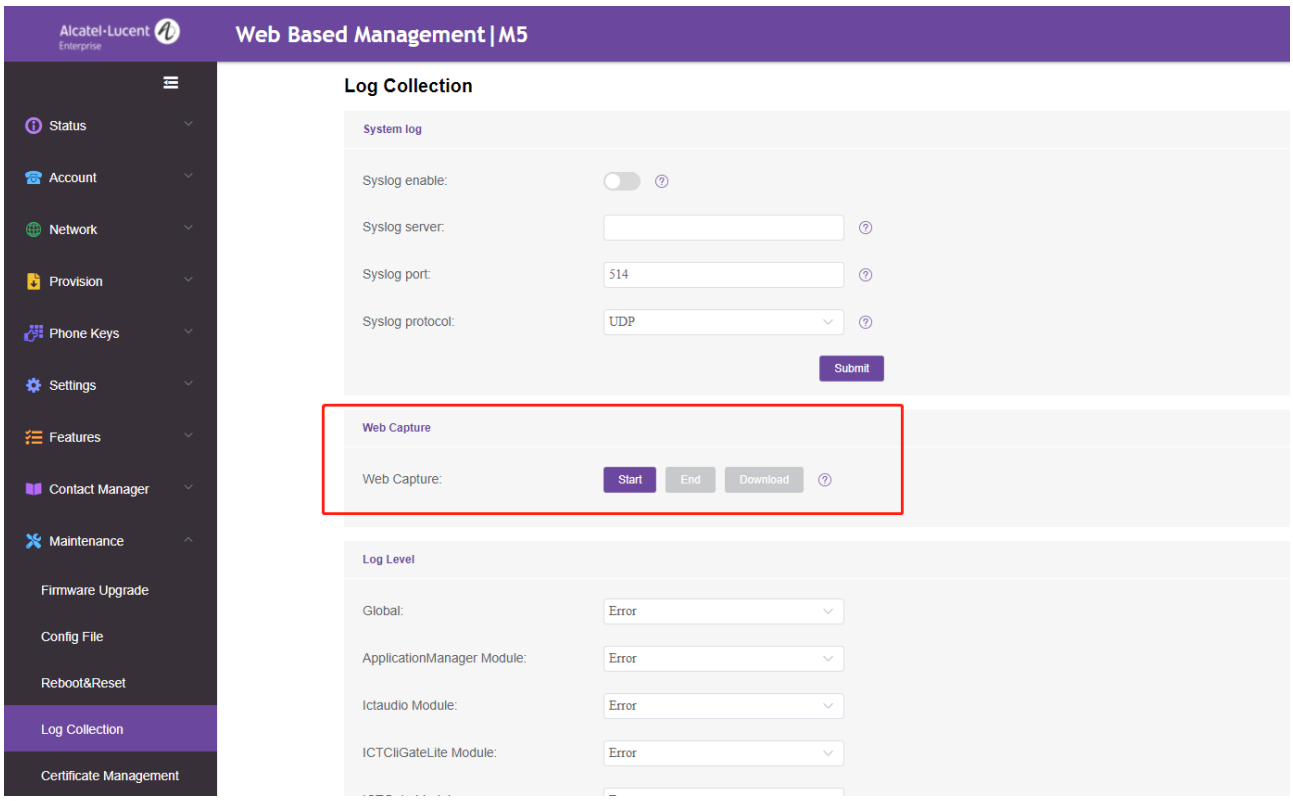
13.1.4 Web Capture

Sometimes dumping the network packets of the device helps issue identification.

To get the device packets, log in to the device web portal, go to Maintenance → Log Collection → Web Capture, click Start in “Web Capture” section.

The user then performs relevant operations such as activating/deactivating an account or making telephone calls and clicks the “End” button in the web page when the operation is finished.

Then the user can press the “Download” button to download the packets for analysis.



13.2 Resetting Device to Factory Settings

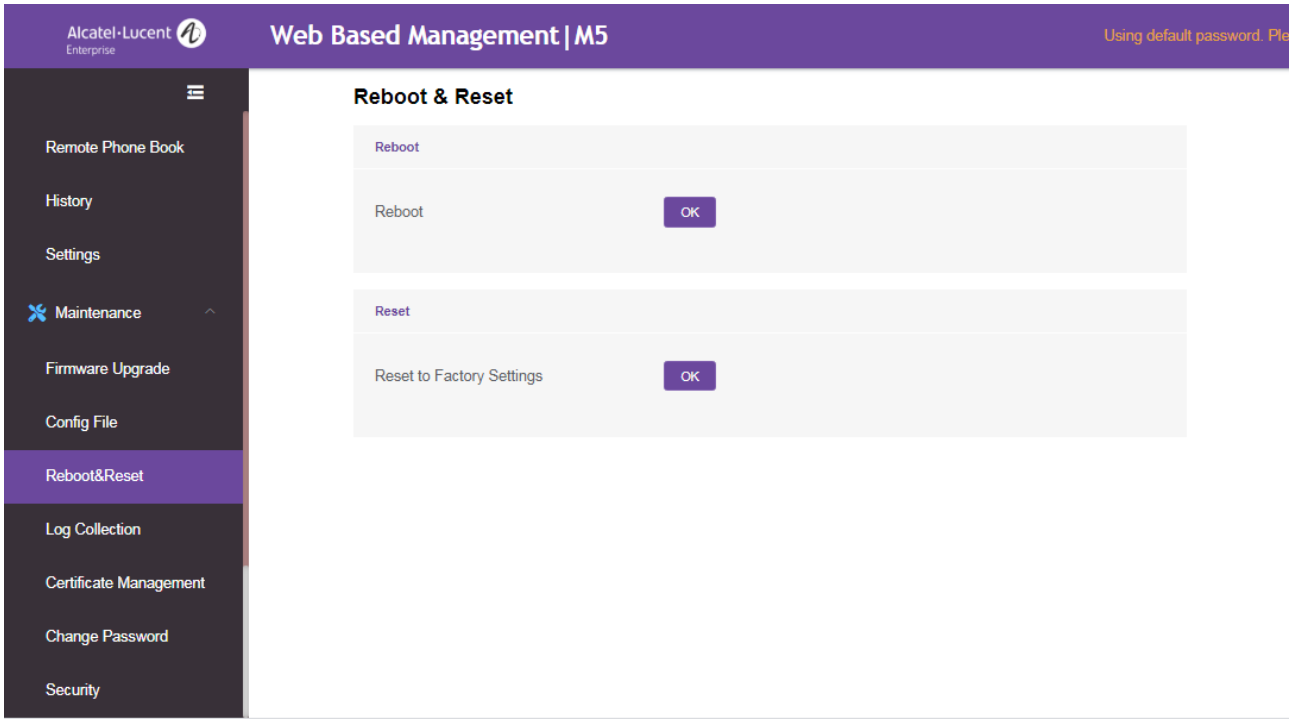
13.2.1 Resetting Device to Factory Settings via Web UI

You can reset or reboot the phone via the Web UI path: Maintenance → Reboot & Reset

The phone will restart when clicking OK button of “Reboot”.

The phone will be reset to factory configuration when clicking OK button of “Reset to Factory Settings”.

Note: All the configuration on the phone will be erased after resetting to factory settings.



13.2.2 Resetting Device to Factory Settings via Phone UI

You can reset the phone to factory setting on phone UI by path: Menu → Advanced Setting (default password: 123456) → Reset → Reset to Factory Settings.

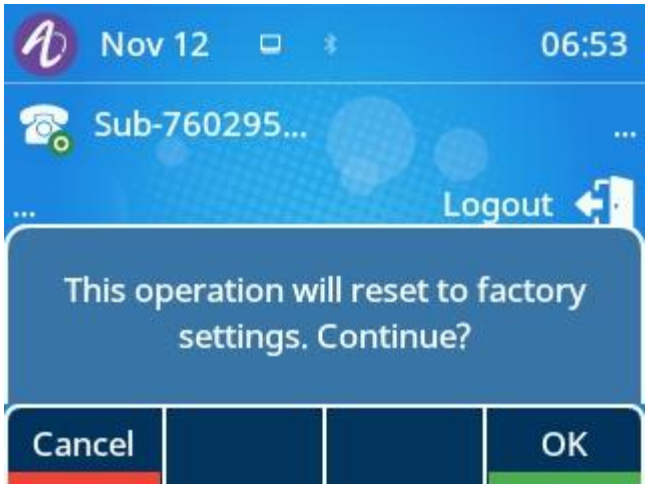
Press OK button to restore the phone to factory configuration.

13.2.3 Resetting Your Device to Factory Settings on Keyboard

For the M3/M5/M7 DeskPhone, you can reset the phone to factory settings by long pressing Conference Key over 10s while the phone is in idle status. Press OK button when the warning page pops up to reset the phone to factory settings.

For the M8 DeskPhone, you could long press Headset Hard Key to trigger resetting the phone to factory settings.

Note: All the configuration on the phone will be erased after the phone rebooting.



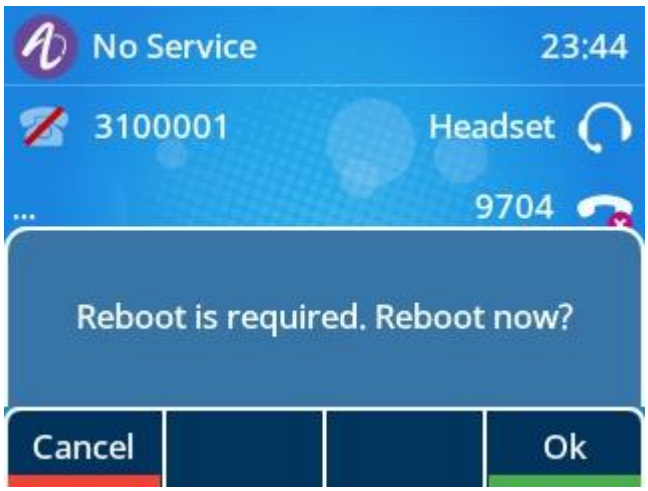
13.3 One Key Reboot

The phone provides a quick way to reboot. You need to press the C key for 10 seconds.

An inquiry box will pop up to ask whether to restart.

OK: By pressing “OK”, the deskphone will reboot in a few seconds.

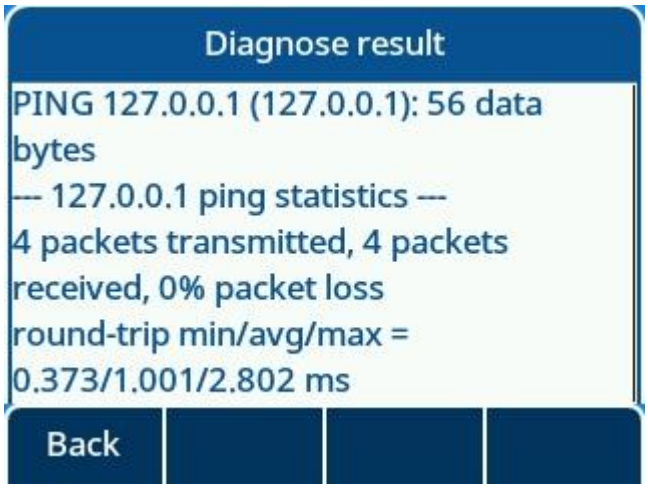
Cancel: By pressing “Cancel”, the deskphone will cancel the operation.



13.4 Network Diagnostics

You can use ping and traceroute diagnostics for troubleshooting network connectivity via phone user interface.

Go to the phone UI: Menu → Advanced Setting (default password:123456) → Net Diagnose, and then input the IP address to trigger “ping” or “traceroute” command. The diagnosis result will be displayed on the screen.



13.5 Packets Capture via PC port

You can capture data packets of the phone with PC port mirror function.

The following table lists the parameter you can use to configure PC port mirror function.

Parameter	DeviceNetworkSpanToPcType	config.<mac>.xml
Description	It enables or disables the IP phone to span data packets received from the LAN port to the PC port.	
Permitted Values	0 - Idle status without mirror setting 1 - enable PC port mirroring LAN port	
Default	0	

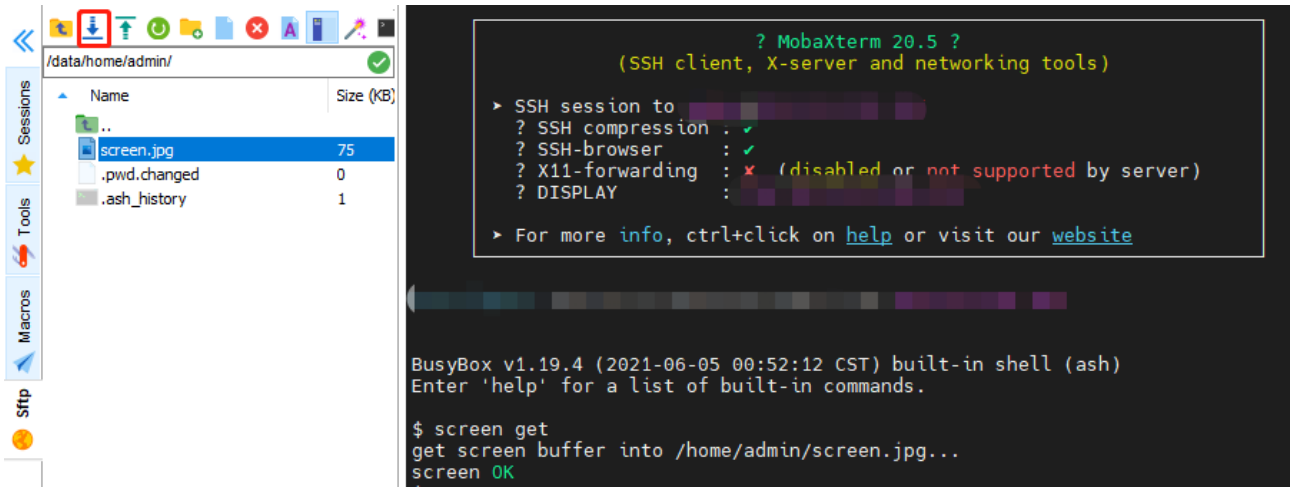
While the PC port is mirroring the LAN port, you can connect PC on PC port to capture ethernet traffic from LAN port.

13.6 Screen Capture

If there is a problem with the phone, the screenshot can help the technician identify the problem. You can get the screenshots with command by logging into the phone with **SSH** connection (default login username/password: admin/123456). After connecting, input command “screen get”.

Regarding how to enable SSH connection on the phone, please refer to section 13.1.3.2.

For example, assuming you login the phone by SSH connection with tool Mobaxterm, you can make a screenshot with command and download it in local PC.



ALE M3-M5-M7-M8 DeskPhones

Administrator Guide

www.aledevice.com

Alcatel·Lucent Enterprise