Alcatel-Lucent Enterprise
Myriad and Halo Series DeskPhone

Administration Manual

8AL91477ENAA ed04

Legal Notice

1. Introduction

The ALE SIP DeskPhones Administration Manual provides general guidance on setting up phone network, provisioning and managing phones.

This manual 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 manual:

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

This manual is applicable to the following ALE SIP DeskPhones:

- Myriad series phones, including M3s, M5s, M7s, M7s Pro and M8.
- Halo series phones, including H3G and H6.

2. Phone Network

The ALE SIP DeskPhones operate on an Ethernet local area network (LAN) or wireless network.

2.1 IPv4 and IPv6 Network Settings

The ALE SIP DeskPhones 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 SIP DeskPhones 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 parameters 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	
Web UI	Network → IP Parameters → Internet Port → IP Stack Mode	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → WAN Port → IP Stack → IP Stack	

Note: If you change this parameter, the SIP deskphone 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 → WAN Port → 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 → WAN Port → 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 → WAN Port → 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 → WAN Port → IP Config → IPv4 Settings → Gateway	
Parameter	**DeviceNetworkDns1**	**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	0.0.0.0	
Web UI	Network → IP parameters → DNS1	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → WAN Port → IP Config → IPv4 Settings → DNS1	
Parameter	**DeviceNetworkDns2**	**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	0.0.0.0	
Web UI	Network → IP parameters → DNS2	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → WAN Port → IP Config → IPv4 Settings → DNS2	

Note: If you change this parameter, the SIP deskphone 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 SIP deskphone to obtain the IPv6 address and other network settings either from SLAAC or from DHCPv6. If the SLAAC server is not working, the SIP deskphone 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	
Web UI	Network → IP Parameters → IPv6 → DHCP Mode	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → WAN Port → IP Config → IPv6 Settings → IPv6 Mode	
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	::	
Web UI	Network → IP Parameters → IPv6 → IP Address **Note:** Only the M8 phone supports the IPv6 configuration in phone web.	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → WAN Port → IP Config → IPv6 Settings → IP	
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	
Web UI	Network → IP Parameters → IPv6 → IPv6 Prefix (0~128) **Note:** Only the M8 phone supports the IPv6 configuration in phone web.	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → WAN Port → IP Config → IPv6 Settings → Prefix6	
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	::	
Web UI	Network → IP Parameters → IPv6 → Gateway **Note:** Only the M8 phone supports the IPv6 configuration in phone web.	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → WAN Port → IP Config → IPv4 Settings → Router	
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	::	
Web UI	Network → IP Parameters → IPv6 → DNS1	

	Note: Only the M8 phone supports the IPv6 configuration in phone web.	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → WAN Port → IP Config → IPv6 Settings → DNS1	
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	::	
Web UI	Network → IP Parameters → IPv6 → DNS2	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → WAN Port → IP Config → IPv6 Settings → DNS2	

2.2 DHCP Options for IPv4

The SIP deskphone 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 SIP DeskPhones.

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

<table>
<tr><th></th><th></th><th>Option 66</th><th>Option 67</th><th></th></tr>
<tr><td>http(s)://172.24.190.159</td><td></td><td rowspan="7" colspan="2">no data</td><td>http(s)://172.24.190.159/</td></tr>
<tr><td>http(s)://172.24.190.159</td><td>/provisioning</td><td>http(s)://172.24.190.159/provisioning</td></tr>
<tr><td>http(s)://172.24.190.159</td><td>http(s)://172.24.190.160</td><td>http(s)://172.24.190.159/</td></tr>
<tr><td>172.24.190.159</td><td>172.24.190.160</td><td>https://172.24.190.159/</td></tr>
<tr><td>172.24.190.159</td><td>http(s)://172.24.190.160</td><td>http(s)://172.24.190.160</td></tr>
<tr><td></td><td>/provisioning
Or
172.24.190.160</td><td>https://provisioning
Or
https://172.24.190.160</td></tr>
<tr><td></td><td>http://172.24.190.160</td><td>http://172.24.190.160</td></tr>
<tr><td rowspan="7" colspan="2">any data</td><td>http://172.24.190.161</td><td></td><td>http://172.24.190.161</td></tr>
<tr><td>http://172.24.190.161</td><td>/provisioning</td><td>http://172.24.190.161/provisioning</td></tr>
<tr><td>http://172.24.190.161</td><td>http://172.24.190.162</td><td>http://172.24.190.161</td></tr>
<tr><td>172.24.190.161</td><td>172.24.190.162</td><td>https://172.24.190.161</td></tr>
<tr><td>172.24.190.161</td><td>http://172.24.190.162</td><td>http://172.24.190.162</td></tr>
<tr><td></td><td>/provisioning</td><td>https://provisioning</td></tr>
<tr><td></td><td>http://172.24.190.162</td><td>http://172.24.190.162</td></tr>
</table>

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 SIP DeskPhones 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	
Phone UI	Menu → Basic Setting → Time & Date → General → SNTP Settings → SNTP Server 1	
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	
Phone UI	Menu → Basic Setting → Time & Date → General → SNTP Settings → SNTP Server 2	

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 SIP DeskPhones support configuring DHCP option 132 to define 802.1Q VLAN ID.

2.2.6 DHCP Option 133

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

2.2.7 DHCP Option 100

The SIP deskphones 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.,MT, PST, NZST)
- <offset> is the offset added to the local time to get UTC, specified as [+|-]hh[:mm[:ss]] (e.g., 0, 8, -12)
- <dst name> is the name of the timezone when in daylight savings (e.g., 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	String within 64 characters	
Default	aledevice	

2.3 DHCP Options for IPv6

The SIP deskphone 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 SIP deskphone is to insert a tag with VLAN information to the packets generated by the SIP deskphone. When VLAN is properly configured for the ports (Internet port and PC port) on the SIP deskphone, the SIP deskphone 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 SIP deskphones allows simultaneous access to a regular PC. This feature allows a PC to be daisy chained to an SIP deskphone and the connection for both PC and SIP deskphone to be trunked through the same physical Ethernet cable.

In addition to manual configuration, the SIP deskphone 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 SIP deskphones 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 SIP deskphones, the SIP deskphones periodically advertise their own information to the directly connected LLDP-enabled switch. The SIP deskphones can also receive LLDP packets from the connected switch. When the application type is “voice”, the SIP deskphones decide whether to update the VLAN configurations obtained from the LLDP packets. When the VLAN configurations on the SIP deskphones are different from the ones sent by the switch, the SIP deskphones perform an update and reboot. This allows the SIP deskphones 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 SIP deskphone.	
Permitted Values	true - Enable false - Disable	
Default	true	
Web UI	Network → LLDP&CDP → 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 SIP deskphones by default. You can configure VLAN for the Internet port and PC port manually. Before configuring VLAN on the SIP deskphone, 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 → 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 → 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 → 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 → Vlan → Data Vlan Config → ID	

2.4.3 DHCP VLAN

The ALE SIP DeskPhones 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.

2.4.4 CDP Configuration

Cisco Discovery Protocol (CDP) is a private binary-layer networking protocol developed by Cisco. It is automatically loaded by most Cisco devices upon startup. By using CDP, Cisco devices can share information such as operating system software version, device identifiers, address tables, port identifiers, and performance metrics among themselves and their direct connected devices.

Like HP's LLDP and Huawei/H3C's NDP protocols, CDP uses a set of rules and filters to discover and enumerate all network devices on the local network. The main difference between CDP and these other protocols is that CDP provides a more private and secure way to discover and enumerate network devices on a local network.

In addition to the direct sharing of device information, CDP also supports the discovery of other network devices. When a device is connected to a network, it notifies the local device of the presence of other network devices and allows the local device to discover these devices. This allows for a more seamless and secure network operation.

Overall, CDP is a powerful networking protocol that allows Cisco devices to work together more seamlessly and securely on the local network.

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

Parameter	DeviceNetworkCdpEnable	config.xml
Description	It enables or disables the CDP (Cisco Discovery Protocol) feature on the SIP deskphone.	
Permitted Values	true - Enable false - Disable	
Default	true	
Web UI	Network → LLDP&CDP → CDP → Enable	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → CDP→ enable	
Parameter	DeviceNetworkCdpPacketInterval	config.xml
Description	It configures the interval for sending CDP packets	
Permitted Values	1-3600 seconds	
Default	60	
Web UI	Network → LLDP&CDP → CDP → Packet Interval	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → CDP → Packet Interval	

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 features are applicable to the ALE SIP DeskPhones.

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

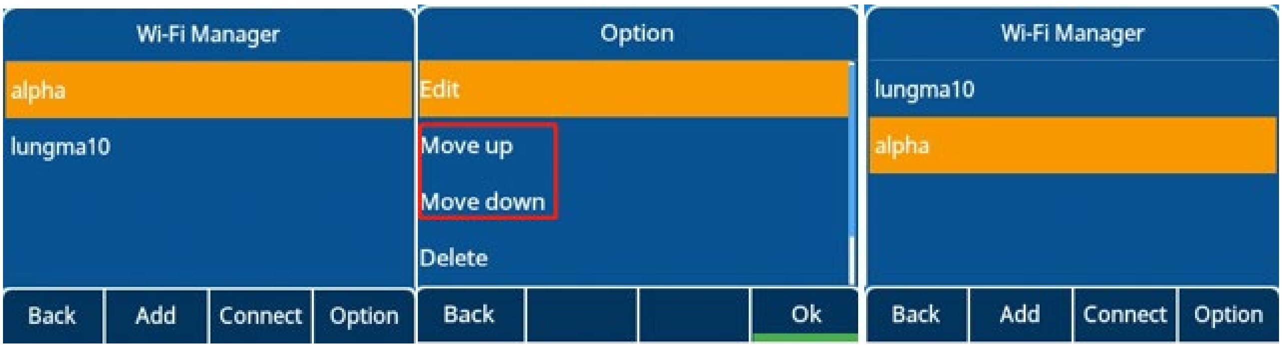
You can store up to 5 frequently used wireless networks on your phone.

You can configure for the ALE SIP DeskPhones: Menu → Basic Setting → Wi-Fi → Wi-Fi Manager (phone user interface).

Note: To use Wi-Fi feature on the ALE SIP DeskPhones H6/M5s/M7s, 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 M7s Pro and M8, Wi-Fi is built in.

The H6/M5s/M7s/M7s Pro/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	false	
Web UI	Network → Wi-Fi	
Phone UI	Menu → Basic Setting → Wi-Fi → Enable WiFi	
Parameter	**DeviceNetworkRedundancyMode**	**config.xml**
Description	It configures preferentially network type.	

Permitted Values	0 - Wi-Fi only 1 - Wi-Fi preferentially 2 - Wired preferentially	
Default	2	
Parameter	**DeviceWifi[1-5]Ssid**	**config.xml**
Description	It configures the AP SSIDs.	
Permitted Values	Strings	
Default	Blank	
Web UI	Network → Wi-Fi	
Phone UI	Menu → Basic Setting → Wi-Fi → Wi-Fi Manager	
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 3 - 802.1x EAP	
Default	0	
Web UI	Network → Wi-Fi	
Phone UI	Menu → Basic Setting → Wi-Fi → Wi-Fi Manager	
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	Blank	
Web UI	Network → Wi-Fi	
Phone UI	Menu → Basic Setting → Wi-Fi → Wi-Fi Manager	
Parameter	**DeviceWifi[1-5]Priority**	**config.xml**
Description	It configures the priority for the wireless network for the SIP deskphone. 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	
Web UI	Network → Wi-Fi	
Phone UI	Menu → Basic Setting → Wi-Fi → Wi-Fi Manager	
Parameter	**DeviceWifi[1-5]8021xMethod**	**config.xml**
Description	It configures the 802.1x EAP authentication method of a specific wireless network. **Note:** It works only if "**DeviceWifi[1-5]AuthMode**" is set to 3.	
Permitted Values	0 – EAP-PWD 1 - EAP-TLS 2 - EAP-PEAP/MSCHAPv2 3 - EAP- PEAP/GTC 4 - EAP-TTLS/ MSCHAPv2	
Default	0	
Web UI	Network → Wi-Fi → Add	
Phone UI	Menu → Basic Setting → Wi-Fi → Wi-Fi Manager → Add	
Parameter	**DeviceWifi[1-5]8021xIdentity**	**config.xml**
Description	It configures the 802.1x EAP authentication username of a specific wireless network.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Network → Wi-Fi → Add	
Phone UI	Menu → Basic Setting → Wi-Fi → Wi-Fi Manager → Add	
Parameter	**DeviceWifi[1-5]8021xPassword**	**config.xml**
Description	It configures the 802.1x EAP authentication password of a specific wireless network.	
Permitted Values	String within 256 characters	
Default	Blank	
Web UI	Network → Wi-Fi → Add	
Phone UI	Menu → Basic Setting → Wi-Fi → Wi-Fi Manager → Add	
Parameter	**DeviceWifi[1-5]8021xAnonymousIdentity**	**config.xml**

Description	It configures the anonymous identity (user name) for Wi-Fi 802.1x EAP authentication. **Note:** It works only if "**DeviceWifi[1-5]8021xMethod**" is set to 1, 2, 3 or 4.	
Permitted Values	String within 256 characters.	
Default	Blank	
Web UI	Network → Wi-Fi → Add	
Phone UI	Menu → Basic Setting → Wi-Fi → Wi-Fi Manager → Add	
Parameter	**DeviceWifi8021xAuthEnable**	**config.xml**
Description	It enables or disables 802.1x EAP-TLS server certificate verification of a specific wireless network.	
Permitted Values	false – disable true - enable	
Default	false	

2.5.1 IPv4 Configuration

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

Parameter	**DeviceWifiDhcpMode**	**config.xml**
Description	It configures the Internet port type for wifi IPv4. **Note:** It works only if "**DeviceWifiIpStackMode**" is set to IPv4.	
Permitted Values	Static Dynamic DynamicAlcatel	
Default	Dynamic	
Web UI	Network → Wi-Fi → DHCP Mode	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → Wi-Fi Port → IP Stack → IPv4 Mode	
Parameter	**DeviceWifiIpAddress**	**config.xml**
Description	It configures the wifi IPv4 address. **Note:** It works only if "**DeviceWifiIpStackMode**" is set to IPv4, and "**DeviceWifiDhcpMode**" is set to Static.	
Permitted Values	IPv4 wifi Address	
Default	0.0.0.0	
Web UI	Network → Wi-Fi → IP Address	

Phone UI	Menu → Advanced Setting (default password: 123456) → Network → Wi-Fi Port → IP Config → IPv4 Settings → IP	
Parameter	**DeviceWifiSubnetMask**	**config.xml**
Description	It configures the IPv4 subnet mask. **Note:** It works only if "**DeviceWifiIpStackMode**" is set to IPv4, and "**DeviceWifiDhcpMode**" is set to Static.	
Permitted Values	Subnet Mask	
Default	255.255.255.255	
Web UI	Network → Wi-Fi → Subnet Mask	
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → Wi-Fi Port → IP Config → IPv4 Settings → S/net	
Parameter	**DeviceWifiGateway**	**config.xml**
Description	It configures the IPv4 default gateway. **Note:** It works only if "**DeviceWifiIpStackMode**" is set to IPv4, and "**DeviceWifiDhcpMode**" is set to Static.	
Permitted Values	IPv4 Address	
Default	0.0.0.0	
Web UI	Network → Wi-Fi → Gateway	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → Wi-Fi Port → IP Config → IPv4 Settings → Gateway	
Parameter	**DeviceWifiDns1**	**config.xml**
Description	It configures the primary IPv4 DNS server. **Note:** It works only if "**DeviceWifiIpStackMode**" is set to IPv4, and "**DeviceWifiDhcpMode**" is set to Static, and "**DeviceNetworkStaticDnsEnable**" is set to true	
Permitted Values	IPv4 Address	
Default	Blank	
Web UI	Network → Wi-Fi → DNS1	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → Wi-Fi Port → IP Config → IPv4 Settings → DNS1	
Parameter	**DeviceWifiDns2**	**config.xml**
Description	It configures the secondary IPv4 DNS server. **Note:** It works only if "**DeviceWifiIpStackMode**" is set to IPv4, and "**DeviceWifiDhcpMode**" is set to Static, and "**DeviceNetworkStaticDnsEnable**" is set to true	

Permitted Values	IPv4 Address	
Default	Blank	
Web UI	Network → Wi-Fi → DNS2	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → Wi-Fi Port → IP Config → IPv4 Settings → DNS2	

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

2.5.2 IPv6 Configuration

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

Parameter	**DeviceWifiIpv6DhcpMode**	**config.xml**
Description	It configures the Internet port type for IPv6. **Note:** It works only if "**DeviceWifiIpStackMode**" is set to IPv6.	
Permitted Values	Static Dynamic	
Default	Dynamic	
Web UI	Network → Wi-Fi → IPv6 → DHCP Mode	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → Wi-Fi Port → IP Config → IPv6 Settings → IPv6 Mode	
Parameter	**DeviceWifiIpv6Address**	**config.xml**
Description	It configures the IPv6 address. **Note:** It works only if "**DeviceWifiIpStackMode**" is set to IPv6, and "**DeviceWifiIpv6DhcpMode**" is set to Static.	
Permitted Values	IPv6 Address	
Default	::	
Web UI	Network → Wi-Fi → IPv6 → IP Address	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → Wi-Fi Port → IP Config → IPv6 Settings → IP	
Parameter	**DeviceWifiIpv6PrefixLen**	**config.xml**
Description	It configures the IPv6 prefix. **Note:** It works only if "**DeviceWifiIpStackMode**" is set to IPv6, and "**DeviceWifiIpv6DhcpMode**" is set to Static.	
Permitted Values	Integer from 0 to 128	
Default	64	
Web UI	Network → Wi-Fi → IPv6 → IPv6 Prefix (0~128)	

Phone UI	Menu → Advanced (default password: 123456) Setting → Network → Wi-Fi Port → IP Config → IPv6 Settings → Prefix	
Parameter	**DeviceWifiIpv6Gateway**	**config.xml**
Description	It configures the IPv6 default gateway. **Note:** It works only if "**DeviceWifiIpStackMode**" is set to IPv6, and "**DeviceWifiIpv6DhcpMode**" is set to Static.	
Permitted Values	IPv6 Address	
Default	::	
Web UI	Network → Wi-Fi → IPv6 → Gateway	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → Wi-Fi Port → IP Config → IPv6 Settings → Gateway	
Parameter	**DeviceWifiDns1**	**config.xml**
Description	It configures the primary IPv6 DNS server. **Note:** It works only if "**DeviceWifiIpStackMode**" is set to IPv6, and "**DeviceWifiIpv6DhcpMode**" is set to Static, and "**DeviceNetworkStaticDnsEnabl**e" is set to true.	
Permitted Values	IPv6 Address	
Default	::	
Web UI	Network → Wi-Fi → IPv6 → DNS1	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → Wi-Fi Port → IP Config → IPv6 Settings → DNS1	
Parameter	**DeviceWifiDns2**	**config.xml**
Description	It configures the secondary IPv6 DNS server. **Note:** It works only if "**DeviceWifiIpStackMode**" is set to IPv6, and "**DeviceWifiIpv6DhcpMode**" is set to Static, and "**DeviceNetworkStaticDnsEnable**" is set to true.	
Permitted Values	IPv6 Address	
Default	::	
Web UI	Network → Wi-Fi → IPv6 → DNS2	
Phone UI	Menu → Advanced (default password: 123456) Setting → Network → Wi-Fi Port → IP Config → IPv6 Settings → DNS2	

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 addresses.

The ALE SIP DeskPhones can work with Rport type of NAT.

2.6.1 Rport Configuration

The ALE SIP DeskPhones 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. It can be number 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8, 1-3 for H3G, 1-4 for H6.	
Permitted Values	false - Disable true - Enable	
Default	false	
Web UI	Account → Advanced → Rport	

2.7 Internet Port and PC Port

The ALE SIP DeskPhones support two Ethernet ports: Internet port and PC port. You can enable or disable the PC port on the SIP deskphones.

2.7.1 Supported Transmission Methods

Three methods of configuration transmission for SIP deskphone Internet port and PC port:

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

Auto-negotiate is configured for both Internet port and PC port on the SIP deskphone 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 – 10Mb/s 100 – 100Mb/s	
Default	100	
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	Full	
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 – 10Mb/s 100 – 100Mb/s	
Default	100	
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	Full
Web UI	Network → Port → PC Duplex
Phone UI	Menu → Advanced Setting (default password: 123456) → Network → Ethernet → PC → PC duplex

2.8 OpenVPN

The ALE SIP DeskPhones use OpenVPN to achieve VPN features. After you configure VPN feature on the SIP deskphone, the phone will act as a VPN client and use the certificate or username 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), userinfo (user.txt) and the configuration file (vpn.cnf) of the OpenVPN client.

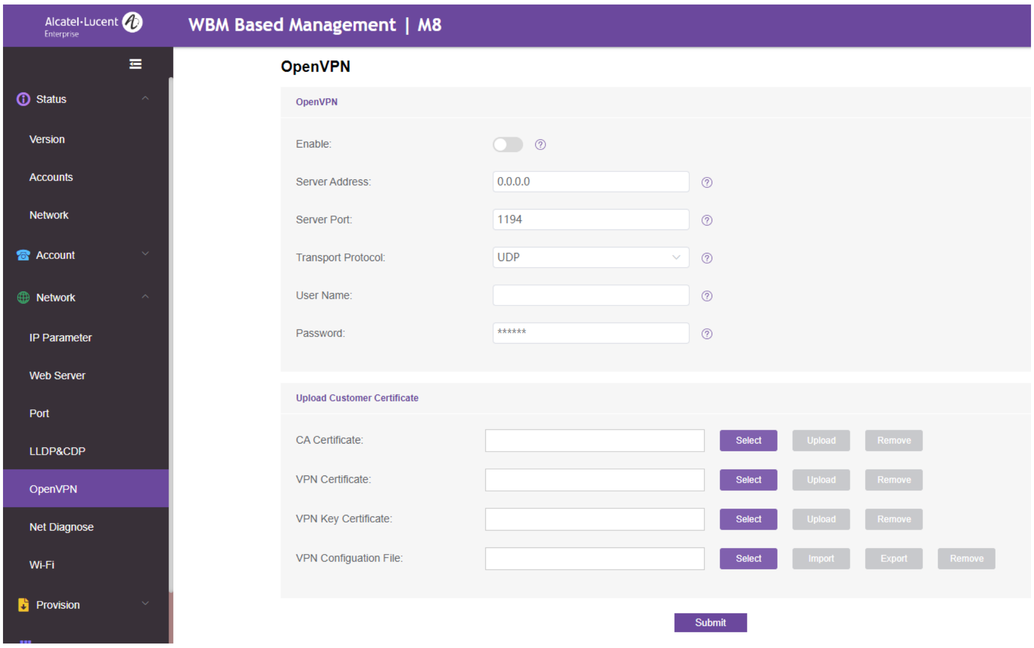
The following table lists the unified directories of the OpenVPN certificates and key in the configuration file (vpn.cnf) for the ALE SIP DeskPhones:

OpenVPN Files	Description	Unified Directories
ca.crt	CA certificate	/config/cert/openvpn/openvpn-ca.crt
client.crt	Client certificate	/config/cert/openvpn/openvpn-client.crt
client.key	Private key of the client	/config/cert/openvpn/openvpn-client.key
User.txt	Username and password file	/config/cert/openvpn/openvpn-user.txt

2.8.2 OpenVPN Configuration

You can configure the OpenVPN feature via the Web UI path: Network → OpenVPN for the ALE SIP DeskPhones.

In addition, you can import VPN certificates and configuration files in batches by using compressed packages.



If the username and password are downloaded as an auto-p file, you should use the following format:

(1) unix file format

(2) username on the first line and the password on the second line, for example:

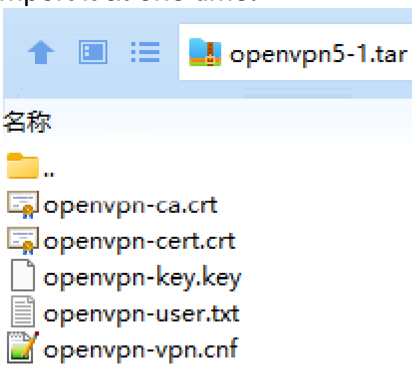
```
$
$ cat /config/cert/openvpn/openvpn-user.txt
username
password$
```

(3) Inside the OpenVPN configuration files need to add a line:

auth-user-pass /config/cert/openvpn/openvpn-user.txt

- Compressed packet mode:

You can refer to the following example, after all the files of the VPN are named according to the convention, then unified compression into a tar file, and then upload the compressed package through the auto-p way, you can import it at one time.



2.8.3 OpenVPN Parameters List

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

Parameter	DeviceNetworkOpenVpnEnable	config.xml
Description	It enables or disables OpenVPN.	

Permitted Values	false - disable true - enable	
Default	false	
Web UI	Network → OpenVPN → Enable	
Parameter	**DeviceNetworkOpenVpnServerAddr**	**config.xml**
Description	It configures OpenVPN server address.	
Permitted Values	String within 256 characters.	
Default	0.0.0.0	
Web UI	Network → OpenVPN → Server Address	
Parameter	**DeviceNetworkOpenVpnServerPort**	**config.xml**
Description	It configures OpenVPN server port.	
Permitted Values	1-65535	
Default	1194	
Web UI	Network → OpenVPN → Server Port	
Parameter	**DeviceNetworkOpenVpnTransport**	**config.xml**
Description	It configures OpenVPN transport protocot	
Permitted Values	UDP TCP	
Default	UDP	
Web UI	Network → OpenVPN → Transport Protocol.	
Parameter	**DeviceNetworkOpenvpnAuthFileUrl**	**config.xml**
Description	It configures OpenVPN username and password file.	
Permitted Values	String within 256 characters. Note: Based on the OpenVPN standard format, the text is in unix format. The first line is the username, and the second line is the password.	
Default	Blank	
Web UI	Network → OpenVPN → Username & Password	
Parameter	**DeviceNetworkOpenvpnCaCertUrl**	**config.xml**
Description	It configures the download url of OpenVPN CA file.	
Permitted Values	String within 256 characters.	
Default	Blank	
Web UI	Network → OpenVPN → CA Certificate	

Parameter	**DeviceNetworkOpenvpnClientCertUrl**	**config.xml**
Description	It configures the download url of OpenVPN client cert file.	
Permitted Values	String within 256 characters.	
Default	Blank	
Web UI	Network → OpenVPN → VPN Certificate	
Parameter	**DeviceNetworkOpenvpnClientKeyUrl**	**config.xml**
Description	It configures the download url of OpenVPN client cert key file.	
Permitted Values	String within 256 characters.	
Default	Blank	
Web UI	Network → OpenVPN → VPN Key Certificate	
Parameter	**DeviceNetworkOpenvpnConfigFileUrl**	**config.xml**
Description	It configures the download url of OpenVPN config file.	
Permitted Values	String within 256 characters.	
Default	Blank	
Web UI	Network → OpenVPN → VPN Configuation File	
Parameter	**DeviceNetworkOpenvpnUrl**	**config.xml**
Description	Add a compressed package to import all OpenVPN certificates and files at one time to complete deployment. The compressed package contains CA certificate, VPN certificate, VPN private key, VPN configuration file, and auth file. The file name must be strictly matched: openvpn-ca.crt openvpn-cert.crt openvpn-key.key openvpn-user.txt openvpn-vpn.cnf	
Permitted Values	String within 256 characters.	
Default	Blank	

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. SIP deskphones 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 SIP deskphones 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 tfor SIP messages.	
Permitted Values	[0-63]	
Default	40	

2.10 802.1x Authentication

The ALE SIP DeskPhones support the following protocols for 802.1x authentication:

- EAP-MD5
- EAP-TLS (requires Device and CA certificates, requires no password)
- EAP-PEAP/MSCHAPv2 (requires CA certificates)
- EAP-PEAP/GTC (requires CA certificates)
- EAP-TTLS/MSCHAPv2 (requires CA certificates)

2.10.1 802.1X Configuration

The following table lists the parameters you can use to configure 802.1X.

Parameter	**DeviceNetwork8021xMethod**	**config.xml**
Description	It configures the 802.1x authentication method.	
Permitted Values	0 - EAP-None 1 - EAP-MD5 2 - EAP-TLS 3 - EAP-PEAP/MSCHAPv2 4 - EAP- PEAP/GTC 5 - EAP-TTLS/ MSCHAPv2	
Default	0	
Parameter	**DeviceNetwork8021xIdentity**	**config.xml**
Description	It configures the identity (username) for 802.1x authentication.	
Permitted Values	String within 64 characters	
Default	Blank	
Parameter	**DeviceNetwork8021xPassword**	**config.xml**
Description	It configures the password for 802.1x authentication. **Note:** It is required for all methods except EAP-TLS.	
Permitted Values	String within 64 characters	
Default	Blank	
Parameter	**DeviceNetwork8021xAnonymousIdentity**	**config.xml**
Description	It configures the anonymous identity (username) for 802.1X authentication. It is used for constructing a secure tunnel for 802.1X authentication. **Note:** It works only if “**DeviceNetwork8021xMethod**” is set to 2, 3, 4 or 5.	
Permitted Values	String within 256 characters	
Default	Blank	
Parameter	**DeviceNetwork8021xClientCertUrl**	**config.xml**
Description	It configures the URL for uploading the 802.1x client certificate.	

	The format of the certificate must be *.pem. You can configure the value to “delete” to delete the certificate. **Note:** It works only if “**DeviceNetwork8021xMethod**” is set to 2 (EAP-TLS).
Permitted Values	String within 256 characters
Default	Blank

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 SIP deskphones.

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 512 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	|mac|	
Web UI	Provision → TR069 → ACS Username	
Parameter	**DeviceTr069AcsPwd**	**config.xml**
Description	It configures ACS account password.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Provision → TR069 → ACS Password	
Parameter	**DeviceTr069AcsPeriodicEnable**	**config.xml**
Description	It enables ACS Periodic informing.	

Permitted Values	true - Enable false - Disable	
Default	true	
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	Blank	
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	Blank	
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	3478	
Web UI	Provision → STUN → STUN Server Port	

3. Phone Provisioning

This chapter provides basic instructions for setting up your SIP deskphones with a provisioning server.

The H3G/H6/M3s/M5s/M7s/M7s Pro/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 SIP deskphones 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 SIP deskphones via web user interface, you are required to enter a username and password for access.

The default username and password is admin/123456.

3.1.1 Accessing the Web User Interface

Procedures:

- Step 1: Find the ALE Myriad Series SIP DeskPhones' 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 username 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.

3.1.3 Web Server Type Configuration

The ALE SIP DeskPhones 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 the 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 SIP deskphone using the HTTPS protocol by default.	
Permitted Values	false - Disable true - Enable	
Default	true	

3.2 Phone User Interface

The 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 SIP DeskPhones support three configuration template files: Common config file, MAC-Oriented config file and Device config file.

3.3.1 Common Config File

A common config file, named config.xml, contains parameters that affect the basic features of the deskphone, such as setting language and volume. It will be effective for all deskphones.

3.3.2 MAC-Oriented Config File

MAC-Oriented config file is named after the MAC address of the deskphone. For example, if the MAC address of a deskphone is 3C28A6200088, the name of MAC-Oriented config 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 deskphone.

3.3.3 Device Config File

Device config file is named after the device model of the deskphone. For example, if the device model of deskphone is M8, the name of device config file is config.M8.xml.

It contains common parameters that affect the same model deskphones. The device config file has a fixed name for each phone model.

3.4 EDS (Easy Deployment Server)

EDS (Easy Deployment Server) is a server which provides 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 refer to the EDS Administration Manual for more information.

3.5 Provisioning Methods

The ALE SIP DeskPhones 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.

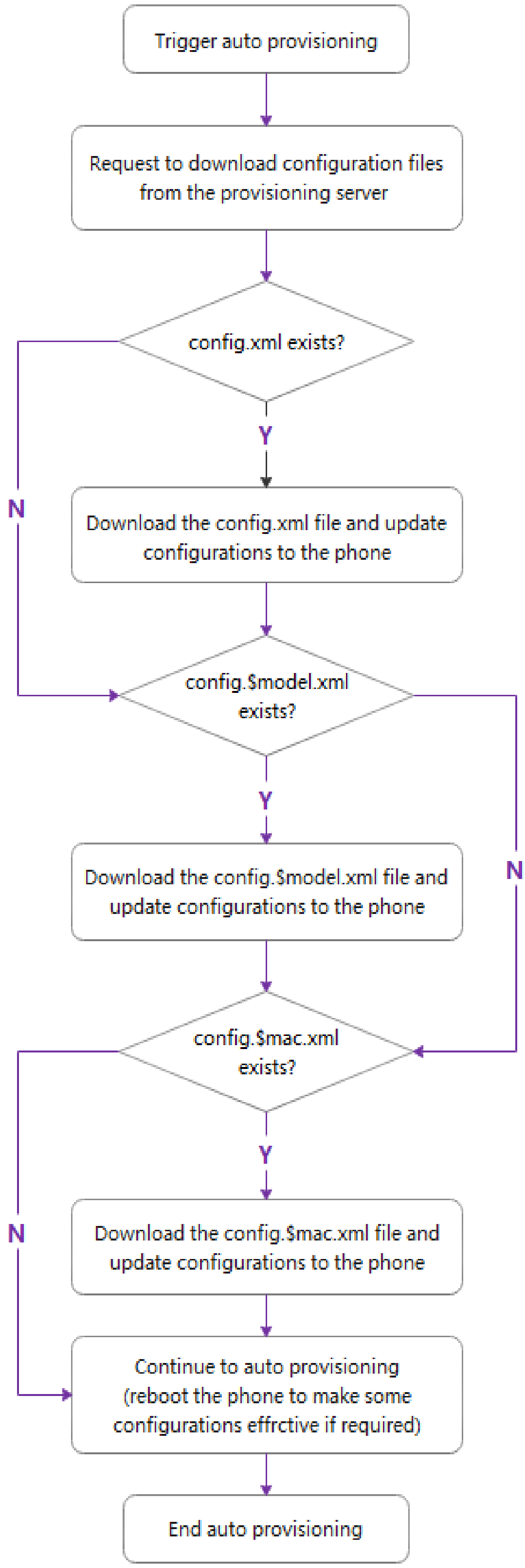
3.6 Auto Provisioning

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 → Local → EDS → RDDS. At any of the four 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 the wrong format during the auto provisioning process, parsing fails, and the phone will continue auto provisioning process.

To make the deployment more flexible, we made the PnP process independent, not limited by priority, and also to support long listening.



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 512 Characters	
Default	config.xml	
Parameter	**DeviceProvisionFileSecond**	**config. xml**
Description	It configures the second requested configuration file.	
Permitted Values	String within 512 Characters	
Default	config.$model.xml	
Parameter	**DeviceProvisionFileThird**	**config.xml**
Description	It configures the third requested configuration file.	
Permitted Values	String within 512 Characters	
Default	config.$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 SIP deskphone 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 SIP DeskPhones 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 newly 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 parameters 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 who 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 SIP deskphone 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 SIP deskphone 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 512 characters	
Default	Blank	
Parameter	**DeviceProvisionUserConfigUploadMethod**	**config.xml**
Description	It configures the way the SIP deskphone 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 a network connection, a provisioning server address should be obtained for configuration settings.

The SIP deskphone supports the following methods to discover the provisioning server address:

PnP: PnP feature allows SIP deskphones to discover the provisioning server address by broadcasting the PnP SUBSCRIBE message during startup. And also support out of dialog notify.

DHCP: DHCP option can be used to provide the address or URL of the provisioning server to SIP deskphones. When the SIP deskphone 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 parameters you can use to configure PnP provisioning.

Parameter	**DeviceProvisionPnPEnable**	**config.xml**
Description	It enables or disables PNP function.	
Permitted Values	false - Disable true - Enable	
Default	true	

Web UI	Provision → Auto Provision → PnP Provision	
Parameter	**DeviceProvisionPnpPort**	**config.xml**
Description	Configure pnp srouce port.	
Permitted Values	Integer from 1 to 65535	
Default	5082	

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 disables DHCP option for acquiring auto provisioning server URL.	
Permitted Values	false - Disable true - Enable	
Default	true	
Web UI	Provision → Auto Provision → DHCP 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 → IPv4 Custom Option	
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 → IPv6 Custom Option	

3.8.3 Static Provisioning Configuration

To use the static provision method, you need to obtain the provisioning server address first when configuring a provisioning server.

The provisioning server address can be IP address, domain name or URL. If a user name and password are specified as part of the provisioning server address, for example, http://username:password@server, they will be used only if the server supports them.

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

Parameter	**DeviceProvisionServerUrl**	**config.xml**
Description	It configures the access URL of the provisioning server.	
Permitted Values	URL within 512 characters	
Default	Blank	
Web UI	Provision → Auto Provision → DM URL	
Phone UI	Menu → Advanced Setting (default password: 123456) → Auto Provision → URL	
Parameter	**DeviceProvisionBackupServerUrl**	**config.xml**
Description	It configures the access URL of the backup provisioning server.	
Permitted Values	URL within 512 characters	
Default	Blank	
Web UI	Provision → Auto Provision → Backup DM URL	
Phone UI	Menu → Advanced Setting (default password: 123456) → Auto Provision → URL BAK	
Parameter	**DeviceProvisionServerUsername**	**config.xml**
Description	It configures the username for provisioning server access.	
Permitted Values	Strings within 64 characters	
Default	Blank	
Web UI	Provision → Auto Provision → Username	
Phone UI	Menu → Advanced Setting (default password: 123456) → Auto Provision → Username	
Parameter	**DeviceProvisionServerPassword**	**config.xml**
Description	It configures the password for provisioning server access.	
Permitted Values	Strings within 64 characters	
Default	Blank	
Web UI	Provision → Auto Provision → Password	
Phone UI	Menu → Advanced Setting (default password: 123456) → Auto Provision → Password	

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 is reached. Furthermore, the SIP deskphone also allows users to define the phone downloading the configuration files weekly.

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 period.	
Permitted Values	false - Disable true - Enable	
Default	false	
Web UI	Provision → Auto Provision → Polling By Interval	
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 → Polling Timeout (Second)	
Parameter	**DeviceProvisionPollingByWeekdaysEnable**	**config.xml**
Description	It enables or disables polling weekly.	
Permitted Values	false - Disable true - Enable	
Default	false	
Web UI	Provision → Auto Provision → Polling By Weekdays	
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 → Polling Time	
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 → Polling Time	

Parameter	**DeviceProvisionPollingDayofWeek**	**config.xml**
Description	It configures polling day of week. **Note:** It works only if the value of "**DeviceProvisionPollingByWeekdaysEnable**" is set to 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 → Polling Day Of Week	

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.

The H3G and H6 DeskPhones use sipH3_6X binary.

The M3s, M5s, M7s and M7s Pro DeskPhones use sipM357s binary.

The M8 DeskPhone use sipM8 binary.

4.2 Firmware Upgrade Configuration

4.2.1 Firmware Upgrade from Provisioning Server with Configuration File

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

Parameter	**DeviceFirmwareUpgradeUrl**	**config.xml**
Description	It configures the access URL of the firmware file.	
Permitted Values	URL within 512 characters	
Default	Blank	

4.2.2 Firmware Upgrade via Web User Interface

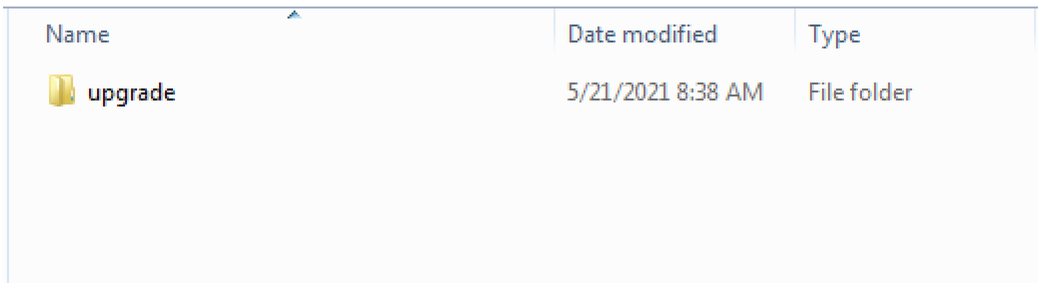
Before upgrading firmware, you need to know the following:

- Do not close and refresh the browser when the SIP deskphone is upgrading firmware.
- Do not unplug the network cables and power cables when the SIP deskphone 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 its “upgrade”.
- Step 3: Put the firmware binary files into the upgrade folder.



- Step 4: Plug the USB disk into the phone’s USB port when the phone is powered off.
- Step 5: Power on the phone.
- Step 6: During LCD showing Alcatel-Lucent Enterprise logo when the phone initializing, pressing “4” + “7” + “8” + “*” keys successively. 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 SIP DeskPhones 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 users is “user/user”. Both “administrator” and “user” can log into the web user interface, and administrator will see all the user options.

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 username of the user.	
Permitted Values	String within 32 characters	
Default	user	
Parameter	**DeviceSecurityVarName**	**config.xml**
Description	It configures the username of the var.	
Permitted Values	String within 32 characters	
Default	var	
Parameter	**DeviceSecurityAdminName**	**config.xml**
Description	It configures the username 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	123456	
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 your 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.

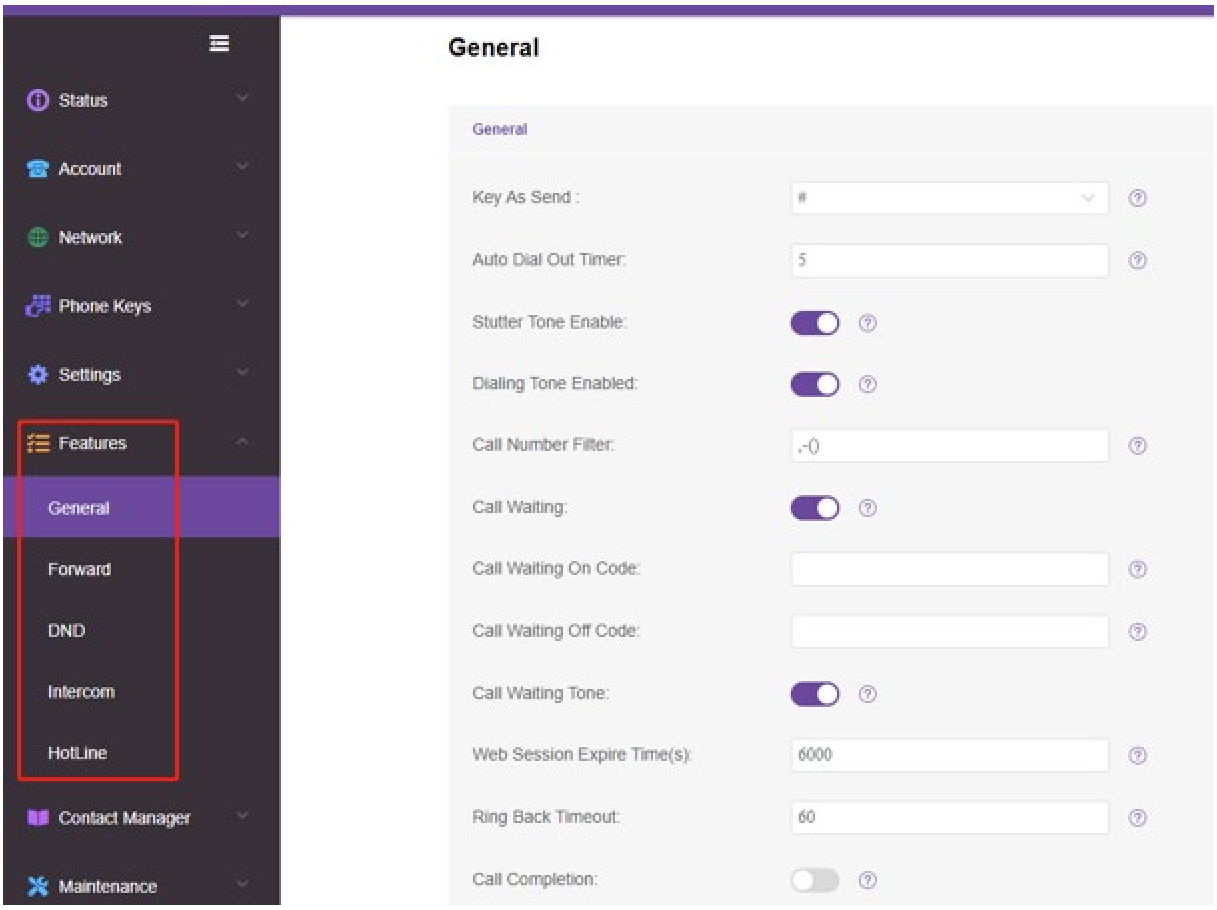
Note: If you change the web user interface permission parameters, the SIP deskphone will reboot to make the changes take effect.

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="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>
```

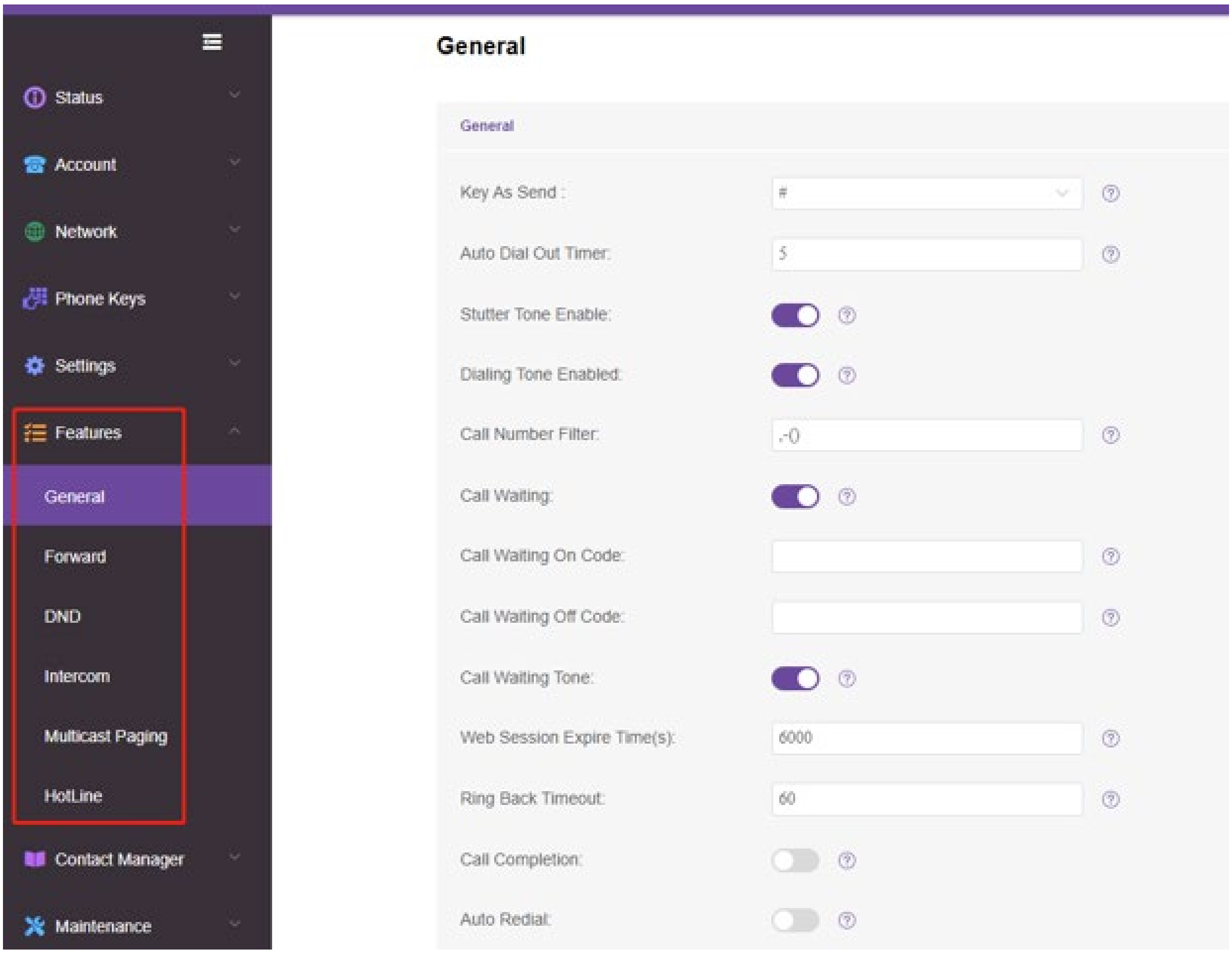
Based on the above configuration of access level:

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

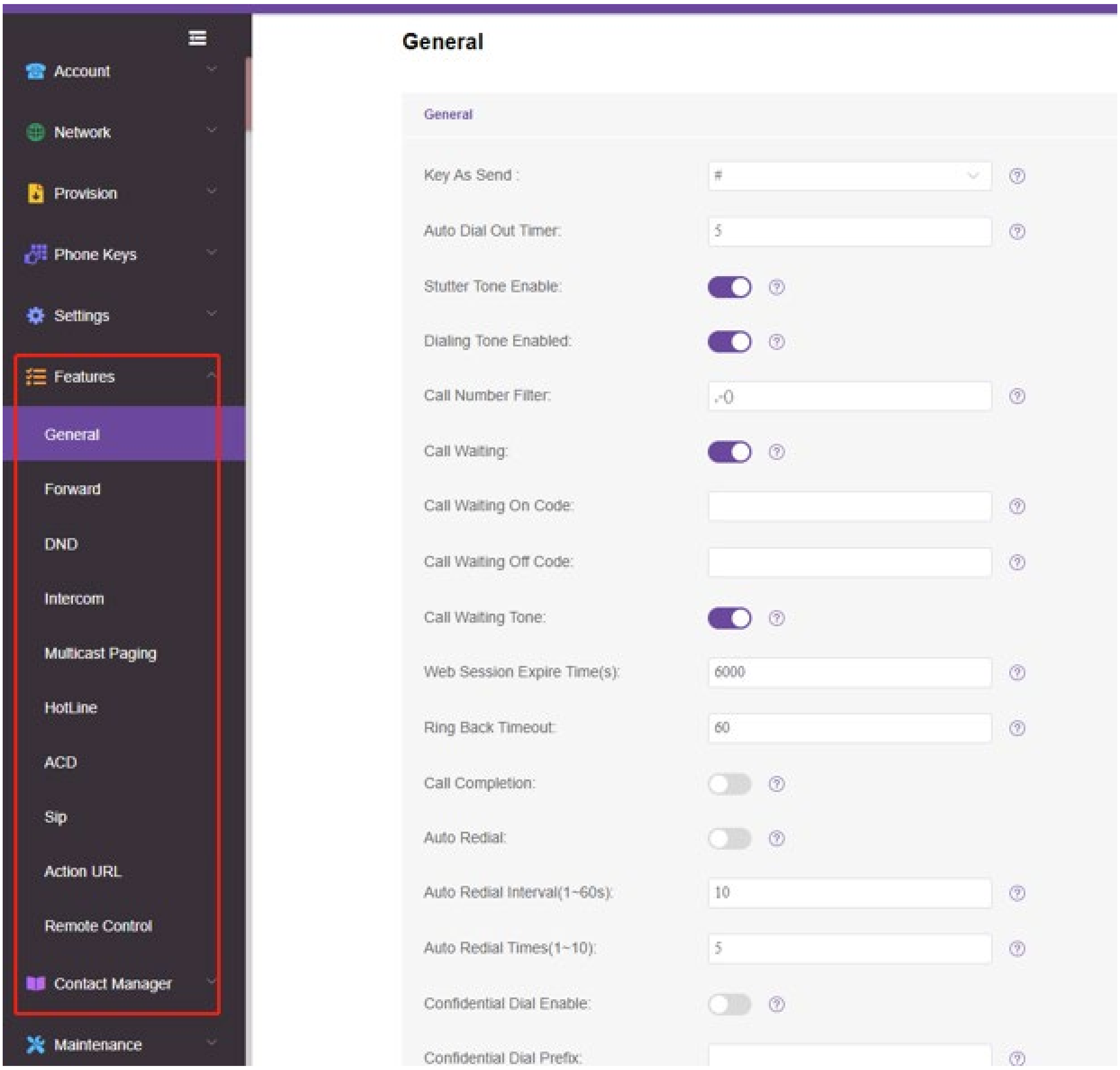


Status
Account
Network
Phone Keys
Settings
Features
General
Forward
DND
Intercom
HotLine
Contact Manager
Maintenance
General
General
Key As Send :
Auto Dial Out Timer:
5
Stutter Tone Enable:
Dialing Tone Enabled:
Call Number Filter:
,-()
Call Waiting:
Call Waiting On Code:
Call Waiting Off Code:
Call Waiting Tone:
Web Session Expire Time(s):
6000
Ring Back Timeout:
60
Call Completion:

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



When logging in to 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).

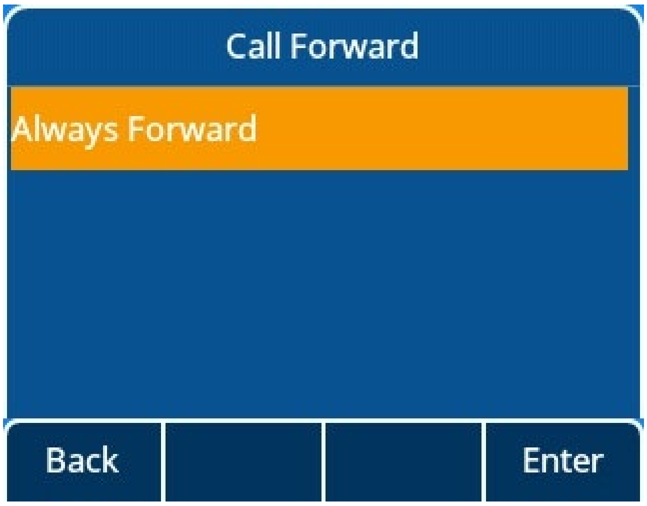
Example: Configuration items in the UserAccessPermission.xml for call forward menu and its submenu settings for phone user interface:

```
<?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:

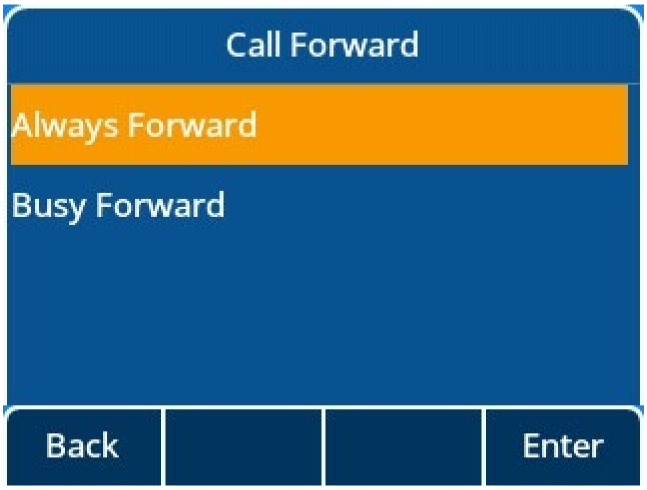
When logging in to the phone user interface with user access level, the access permission of each submenu is displayed as follows:

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

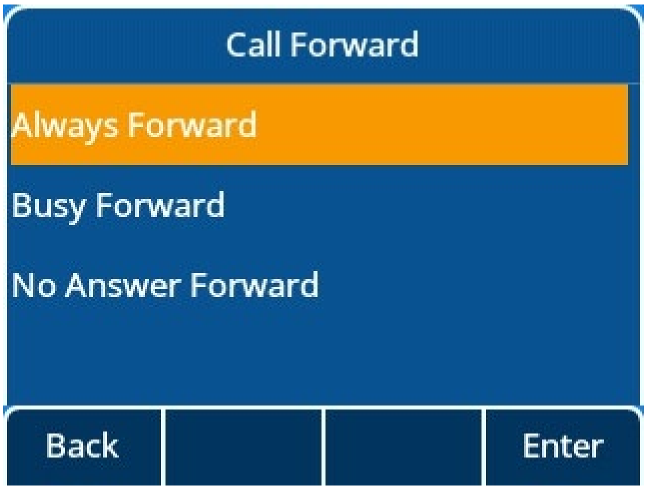


When logging in to the phone user interface with var access level, the access permission of each submenu is displayed as follows:

No answer forward submenu is hidden for var access level.



When logging in to 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 to the web/phone user interface with different access levels.

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

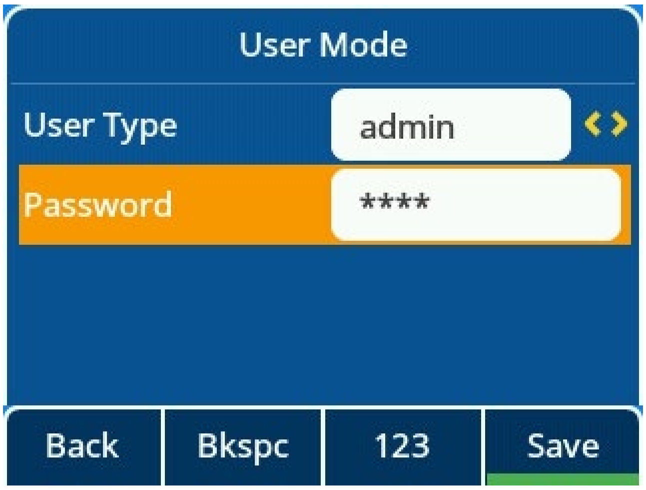
1. Enter the IP address in the address bar of the web browser on your PC and then press the **Enter** key.
2. Enter the username (admin/var/user) and password (admin/var/user) in the login page.
3. Click **Login** to log in.

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** softkey to select the desired access level in the User Type field.

3. Enter the password in the Password field.

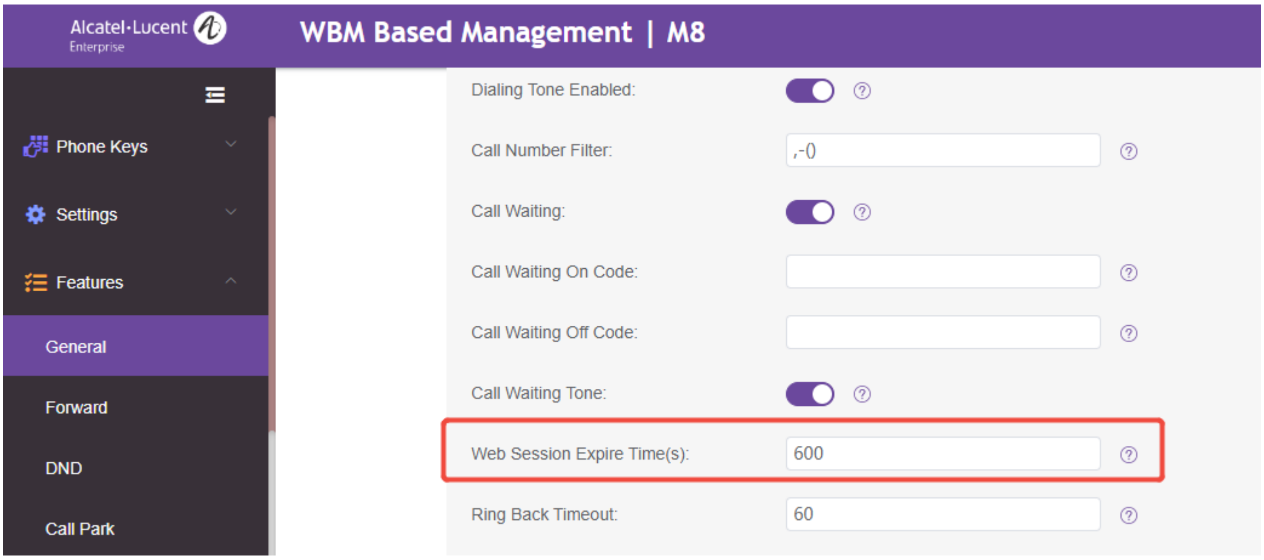


4. Press the Save softkey to accept the change.

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 10 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 the username and password for web access authentication and then log in again.



5.3 Phone Lock

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

You can set waiting time intervals 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 parameters you can use to configure the emergency number.

Parameter	**SettingEmergencyNumber**	**config.xml**
Description	It configures the emergency phone numbers when the screen is locked.	
Permitted Values	TEXT	
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	**SettingPhoneLockEnable**	**config.xml**
Description	It enables or disables the phone lock feature.	
Permitted Values	false - Disable true - Enable	
Default	true	
Web UI	Setting → Phone Lock → Phone Lock	
Phone UI	Menu → Basic Setting → Phone Lock → Basic → Lock Enable	
Parameter	**SettingPhoneAutoLockEnable**	**config.xml**
Description	It enables or disables automatic phone locking.	
Permitted Values	false - Disable true - Enable	
Default	false	
Web UI	Setting → Phone Lock → Automatic Lock	
Phone UI	Menu → Basic Setting → Phone Lock → Basic → Auto Lock Enable	
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	Menu → Basic Setting → Phone Lock → Basic → Wait Time	
Parameter	**SettingPhoneUnlockPwd**	**config.xml**

Description	It configures screen lock password.
Permitted Values	Integer
Default	0000
Web UI	Setting → Phone Lock → Unlock Password
Phone UI	Menu → Basic Setting → Phone Lock → Change PIN

5.4 Transport Layer Security (TLS)

TLS is a commonly used protocol for providing communications privacy and managing the message transmission security, allowing SIP deskphones 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 SIP DeskPhones 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 Digest Algorithm

- MD5
- SHA256
- SHA512
- CRC32

5.4.2 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 SIP DeskPhones support the following cipher suites:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_PSK_WITH_AES_256_GCM_SHA384
- TLS_DHE_PSK_WITH_AES_256_GCM_SHA384
- TLS_RSA_PSK_WITH_CHACHA20_POLY1305_SHA256
- TLS_DHE_PSK_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_PSK_WITH_CHACHA20_POLY1305_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_PSK_WITH_AES_256_GCM_SHA384
- TLS_PSK_WITH_CHACHA20_POLY1305_SHA256
- TLS_RSA_PSK_WITH_AES_128_GCM_SHA256
- TLS_DHE_PSK_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_PSK_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA
- TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA
- TLS_SRP_SHA_WITH_AES_256_CBC_SHA
- TLS_RSA_PSK_WITH_AES_256_CBC_SHA384
- TLS_DHE_PSK_WITH_AES_256_CBC_SHA384
- TLS_RSA_PSK_WITH_AES_256_CBC_SHA
- TLS_DHE_PSK_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_PSK_WITH_AES_256_CBC_SHA384
- TLS_PSK_WITH_AES_256_CBC_SHA
- TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA
- TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA
- TLS_SRP_SHA_WITH_AES_128_CBC_SHA
- TLS_RSA_PSK_WITH_AES_128_CBC_SHA256
- TLS_DHE_PSK_WITH_AES_128_CBC_SHA256
- TLS_RSA_PSK_WITH_AES_128_CBC_SHA
- TLS_DHE_PSK_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_PSK_WITH_AES_128_CBC_SHA256
- TLS_PSK_WITH_AES_128_CBC_SHA

5.4.3 Supported Trusted and Server Certificates

The SIP deskphone 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 ALE SIP DeskPhones default certificate is RSA-2048, and RSA-4096 is supported for custom certificates.

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

- Trusted Certificate: When the SIP deskphone requests a TLS connection with a server, the SIP deskphone should verify the certificate sent by the server to decide whether it is trusted based on the trusted certificates list. The SIP deskphone 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 SIP deskphone, the SIP deskphone sends the server certificate to the clients for authentication. The SIP deskphone 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 SIP deskphone. 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 SIP deskphone (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.
- Support importing customer certificates through SCEP.
  For the DHCP server configuration, to add the new parameters addressed above, we add2 sub options applied for this reason.
  Option 43-> Sub-option 70 for SCEP URL.
  For example: https://au.scep.com/cql/scep_client.exe
  Option 43->Sub-option 71 for Challenge password
  This option is optional when SCEP URL is configured, if not configured or configured with an errorformat (too long or too short or including unsupported characters), we consider as without challenge password configured.
  New sub-option 73 is supported to allow user to customize some parameter of SCEP
  Option 43->Sub-option 73 for CSR customization.
  This option is optional when SCEP URL is configured, if not configured or configured with an errorformat (too long or too short or including unsupported characters or with unrecognized format), we consider the whole option invalid and use default value.

The SIP deskphone 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 SIP deskphone 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 SIP DeskPhones 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.

5.4.4 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 SIP deskphone 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 SIP deskphone 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	Features → Sip → SIP Peer Verify	
Parameter	**SIPCertificateUrl**	**config.xml**
Description	It configures the path of the certificate.	
Default	Blank	
Web UI	Maintenance → Certificate Management → Customer CA Upload	
Parameter	**DeviceSecurityClientCertUrl**	**config.xml**
Description	It configures the customer client certificate download url.	
Default	Blank	
Web UI	Maintenance → Certificate Management → Certificate Upload	

5.5 Secure Real-Time Transport Protocol (SRTP)

Secure Real-Time Transport Protocol (SRTP) encrypts the audio streams during VoSIP deskphone 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 SIP deskphones. This negotiation process is compliant with RFC 4568.

When you place a call on the enabled SRTP phone, the SIP deskphone 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.

Supports the RFC6188 protocol, adds the AES algorithm, and provides more secure communication data protection.

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=crypto:4 AES_256_CM_HMAC_SHA1_80
inline:9ztKi]vaFHwrol9aDHzDhThY3wi+1uewRkJtmdsi/5yLpyZroddKiTHyJ8MLA=
a=crypto:5 AES_256_CM_HMAC_SHA1_32
inline:Fc2UsA5aeEp73VSBnwGm6igieG8415i0B4ZnZZuv3mpvFdi7in4NsBVdKobbaA=
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 SIP deskphones, RTP streams will be encrypted, and a lock icon appears on the LCD screen of each SIP deskphone after successful negotiation.

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

Parameter	**AccountXSrtpWorkingMode**	**config.xml**
Description	It configures whether to use voice encryption service. **Note:** X means account ID. It can be number 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8, 1-3 for H3G, 1-4 for H6.	
Permitted Values	0 - None 1 - Best effort 2 - Strict	
Default	0	
Web UI	Account → Advanced → SRTP Working Mode	
Parameter	**SIPAesKeyPriority**	**config.xml**
Description	It configures the priority of AES algorithm in SDP negotiation	
Permitted Values	0 - AES_CM_128_HMAC_SHA1_80 1 - AES_CM_128_HMAC_SHA1_32 2 - AES_256_CM_HMAC_SHA1_80 3 - AES_256_CM_HMAC_SHA1_32	
Default	0;1	

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 disables the SSH session.	
Permitted Values	false - Disable true - Enable	
Default	false	
Web UI	Maintenance → Security → SSH Activation	
Parameter	**DeviceSecuritySshPort**	**config.xml**
Description	It configures the ssh port.	
Permitted Values	0-65535	
Default	22	

5.7 HTTPS Peer Verification

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

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

Parameter	**DeviceSecurityHttpsPeerVerifyEnable**	**config.xml**
Description	It enables or disables HTTPS peer verification.	
Permitted Values	0 - disable 1 - enable	
Default	1	
Web UI	Maintenance → Certificate Management → HTTPS Peer Verify	

5.8 Encrypting and Decrypting Files

Myriad SIP deskphones 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 SIP DeskPhones provide several types of phone directories.

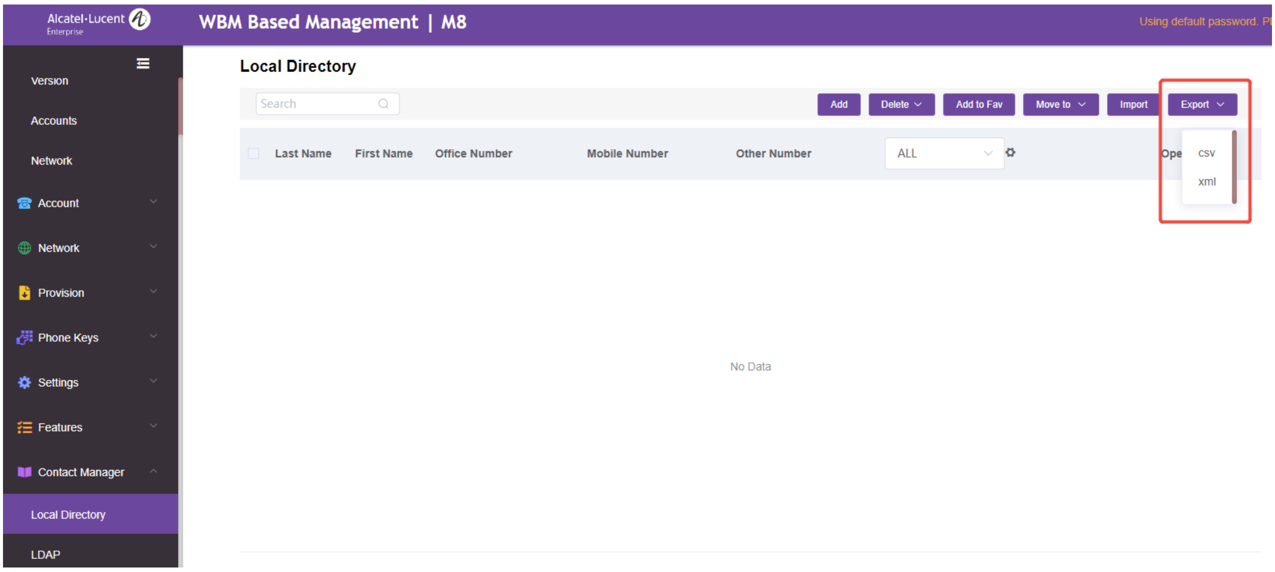
6.1 Local Directory

The ALE SIP DeskPhones 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 SIP DeskPhones support *.xml or *.csv format contact files.

6.1.1 Local Contact File Customization

You can download local contact template from WBM.



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	GroupName	Specify the group name. For example: All Contacts, Blacklist or Friend
Contact	FirstName/ LastName	Specify the FirstName and LastName
	OfficeNumber	Specify the Office number
	MobileNumber	Specify the mobile number
	OtherNumber	Specify the other number
	HomeNumber	Specify the home number
	line Account	Specify a registered line for this contact for calling.

		Valid Values: 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.
	GroupName	Specify which group the contact adds to. Built-in group: All Contacts,Blacklist Custom group: XXX (for example, Friend)
	AvatarSmall	Built-in avatar: Resource: avatar name Value: default, image1~image20 Support Model: H6/M5s/M7s/M7s Pro/M8
	AvatarBig	Built-in avatar: Resource: avatar name Value: default, image1~image20 Support Model: H6/M5s/M7s/M7s Pro/M8
	Favorite	Specify: tag following contact Value: true/false Default: False/Null
	CustomerRingMelody	Set the pairing of the user with the ringtone. Value: Auto, Light Bounce, Discovery, Lounge, Uptown, Morning, Lights, Miami, Far East, Hight Speed, Rain Drops, Deep Space, Steam Train, Happy, Decrescendo, Strident, Peacefulness, Verticals, Classic Ring1, Classic Ring2, Classic Ring3, Classic Ring4

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 XML example:

```
<?xml version="1.0" encoding="utf-8"?>
<!--Phonebook generated at Tue Mar 28 10:28:14 2023-->
<PhoneDirectory>
  <Contacts>
    <Contact>
      <FirstName>TA</FirstName>
      <LastName>testA</LastName>
      <Account>1</Account>
```

```
        <GroupName>All Contacts</GroupName>
        <AvatarSmall>avatar_small_default</AvatarSmall>
        <AvatarBig>avatar_large_default</AvatarBig>
        <OfficeNumber>123456789</OfficeNumber>
        <MobileNumber></MobileNumber>
        <OtherNumber></OtherNumber>
        <HomeNumber></HomeNumber>
        <Favorite>False</Favorite>
        <CustomerRingMelody></CustomerRingMelody>
      </Contact>
    </Contacts>
    <Groups>
      <Group>
        <GroupName>All Contacts</GroupName>
      </Group>
      <Group>
        <GroupName>Blacklist</GroupName>
      </Group>
      <Group>
        <GroupName>Whitelist</GroupName>
      </Group>
      <Group>
        <GroupName>AAA</GroupName>
      </Group>
      <Group>
        <GroupName>BBB</GroupName>
      </Group>
      <Group>
        <GroupName>CCC</GroupName>
      </Group>
    </Groups>
</PhoneDirectory>
```


For CSV example:

#FirstName	LastName	Account	GroupName	AvatarSmall	AvatarBig	OfficeNumber	MobileNumber	HomeNumber	OtherNumber	Favorite	CustomerRingMelody
TA	testA	1	All Contacts	avatar_small_default	avatar_large_default	123456789				FALSE	

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 and Resource Upload

You can upload local contact files to add multiple contacts at a time or upload the contact resource, such as contact avatar.

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 512 characters	
Default	Blank	
Parameter	**LocalContactUploadMode**	**config.xml**
Description	It configures the mode for uploading local contacts.	
Permitted Values	0 - Override mode 1 - Incremental mode	
Default	0	
Parameter	**DirectoryAvatarUrl**	**config.xml**
Description	It configures the access URL of a contact avatar file. • Need to configure the absolute path. • Format: png, jpg, bmp, jpeg, single file size ≤1MB, resolution ≤ 0.5 mega-pixels. • Support upload multiple avatars by zip file.	
Permitted Values	URL within 512 characters.	
Default	Blank	
Parameter	**DirectoryAvatarDelete**	**config.xml**
Description	Used to delete the contact avatar file.	
Permitted Values	/all – Delete all custom avatar *Filename* – Delete the specified custom avatar file	
Default	Blank	

Example: Adding Contacts Using a Contact File

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

Example:

1. Customize the contact file “contact.xml” and place the contact file “directory.xml” to the provisioning server http://192.168.10.25 .
2. Add following parameter into “config.xml” file:
   <setting id="LocalContactUploadUrl" value="http://192.168.10.25/directory.xml" override="true"/>

During auto provisioning, the SIP deskphone 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.

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 SIP deskphones 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 SIP deskphones.

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 SIP deskphone.	
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 512 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.	
Permitted Values	String within 99 characters. Support key: sn; telephoneNumber; givenName; mobileNumber; otherNumber; firstname; name; officephone; department;title. Can customize the mapping using the above key.	
Default	{"firstname":"givenname", "name":"sn", "officephone":"telephonenumber"}	
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	[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	[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	[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	
Parameter	**LdapExtraDisplay**	**config.xml**

Description	It configures additional LDAP attributes to be displayed on the call screen. After the configuration is complete, additional properties are displayed after the name of the call screen and call screen. Support parameters: sn; telephoneNumber; givenName; mobileNumber; otherNumber; firstname; name; officephone; department;title. **Note:** If you want to configure more parameters, you need use “,”.	
Permitted Values	String within 126 characters	
Default	Blank	
Parameter	**LdapFieldsMapping**	**config.xml**
Description	It configures the LDAP fields mapping.	
Permitted Values	String within 126 characters.	
Default	{"firstname":"givenname","name":"sn", "officephone":"telephonenumber"}	

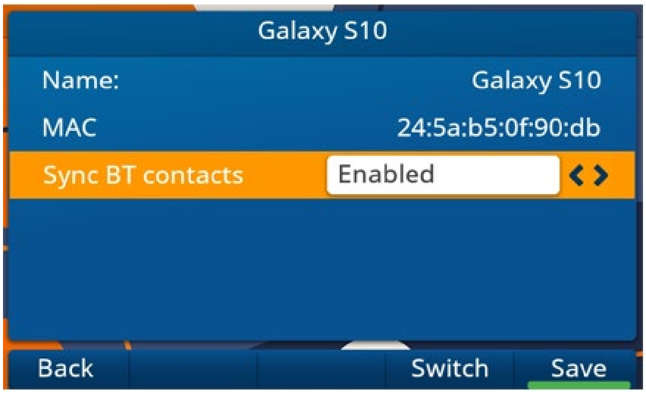
6.3 External Directory

After a mobile phone is paired with a deskphone via Bluetooth, users could choose synchronizing of contacts or not. In addition, manual synchronizing of contacts is also supported after a mobile phone has been paired. After synchronizing contacts automatically or manually, all the contacts from the mobile phone are grouped into a special group named “External Directory”.

Note: Only the M7s Pro and M8 deskphones support this feature.

During pairing with mobile phone process, the deskphone could accept or reject synchronizing of contacts.

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 SIP deskphone will search whether phoneNumber1/phoneNumber2/phoneNumber3/firstName/lastName contain/start with the entered character(s).
- If the first character is not digit, the SIP deskphone 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 - Start with	
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 SIP deskphone 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 SIP DeskPhones support up to 6 remote phone book groups.

The following table lists the parameters you can use to configure the 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 enables or disables the forced update mode.	
Permitted Values	0 - disable 1 - enable	
Default	0	
Parameter	**RemotePhoneBookPeriodUpdateEnable**	**config.xml**
Description	It enables or disables the periodically 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	[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 of remote phone book. X can be 1~6.	
Permitted Values	Strings	
Default	Blank	
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 name 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 SIP deskphone will automatically upload contact files at regular intervals to the provisioning server or a specific server. If the contact file exists on the server, it will be overwritten. The SIP deskphone 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	[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 method to upload files.	
Permitted Values	0 – Put 1 - Post	
Default	0	
Parameter	**DeviceContactBackupEnable**	**config.xml**
Description	It enables or disables contact backup.	
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 to Blacklist.

6.8 Directory List for Directory/Dir Softkey

Users can access frequently used directory lists by pressing the Directory/Dir softkey when the SIP deskphone is idle. The lists include Local Directory by default.

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

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

Parameter	DirectoryList	config.xml
Description	It configures the list that is quickly accessible via Directory softkey or program Key.	
Permitted Values	0 - Local Directory 1 - Remote Phone Book 2 - LDAP 3 - Blacklist 4 - Favorites 5 - External Directory 6 - Network Contacts 7 - Network Directory 8 - Enterprise Directory	
Default	0	
Web UI	Contact Manager → Settings → Directory List	

6.9 Favorite Contacts

Users can mark local contacts as favorite contacts, and the favorite contacts will be stored in the Favorites directory.

6.9.1 Favorites Configuration

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

Parameter	DirectoryFavoriteMode	config.xml
Description	It configures the favorite contact mode.	
Permitted Values	0 - Adding Favorite Contact will not automatically generate Speed Dial key	

	1 - Adding a Favorite Contact will automatically generate a Speed Dial key
Default	0

7. Audio Features

This chapter describes the audio sound quality features and options you can configure for the SIP deskphone.

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/unread 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 SIP deskphone in advance.

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

7.3.1 Custom Ringtone Limit

Phone Model	Format	File Size
H3G/H6/M3s/M5s/M7s/M7s Pro/M8	.wav	.wav file <= 200kb .zip file <= 1.2M

7.3.2 Ringtone Configuration

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

Parameter	**SettingRingInternal**	**config.xml**
Description	It configures internal call ring melody.	
Permitted Values	String within 512 Characters	
Default	Light Bounce	
Web UI	Settings → Ringing → Internal Melody	
Phone UI	Menu → Basic Setting → Sound → Ringing → Int Melody	
Parameter	**SettingRingExternal**	**config.xml**
Description	It configures external call ring melody.	
Permitted Values	String within 512 Characters	
Default	Light Bounce	
Web UI	Settings → Ringing → External Melody	
Phone UI	Menu → Basic Setting → Sound → Ringing → Ext Melody	
Parameter	**SettingRingProgressive**	**config.xml**
Description	It configures ring progressive.	
Permitted Values	0 – Normal Ring 1 - Progressive Ring	
Default	0	
Web UI	Settings → Ringing → Progressive Ringing	
Parameter	**SettingRingSilentEnable**	**config.xml**
Description	It enables or disables ring silent mode.	
Permitted Values	false - Disable true - Enable	
Default	false	
Web UI	Settings → Ringing → Silent Mode	
Phone UI	Menu → Basic Setting → Sound → Ringing → Ring mode → Silent mode	
Parameter	**SettingRingBeep**	**config.xml**
Description	It configures the beep tone played before the phone starts ringing.	
Permitted Values	0 - BeepNone 1 - BeepSingle	

	3 – BeepTriple	
Default	0	
Web UI	Settings → Ringing → Beeps Before Ringing	
Phone UI	Menu → 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 512 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 *File name* – delete specific ringtone	
Default	Blank	
Web UI	Settings → Ringing → Custom Melody	
Parameter	**Account[X]RingInternal**	**config.xml**
Description	It configures the ringtone for incoming calls from internal numbers of individual accounts.	
Permitted Values	Common (default value), indicating the global ringtone set using the AudioRingInternalChoice parameter Light Bounce Discovery Lounge Uptown Morning Lights Miami Far East Hight Speed Rain Drops Deep Space Steam Train Happy Decrescendo Strident Peacefulness	

	Verticals Classic Ring1 Classic Ring2 Classic Ring3 Classic Ring4	
Default	Common	
Web UI	Account → Advanced → Internal Melody	
Parameter	**Account[X]RingExternal**	**config.xml**
Description	It configures the ringtone for incoming calls from external numbers of individual accounts.	
Permitted Values	Common (default value), indicating the global ringtone set using the AudioRingInternalChoice parameter Light Bounce Discovery Lounge Uptown Morning Lights Miami Far East Hight Speed Rain Drops Deep Space Steam Train Happy Decrescendo Strident Peacefulness Verticals Classic Ring1 Classic Ring2 Classic Ring3 Classic Ring4	
Default	Common	
Web UI	Account → Advanced → External Melody	

7.4 Distinctive Ring Tones

The feature of distinctive ring tones allows certain incoming calls to trigger SIP deskphones to play distinctive ring tones. The SIP deskphone inspects the INVITE request for an "Alert-Info" header when receiving an incoming call. If the INVITE request contains an "Alert-Info" header, the SIP deskphone 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 SIP deskphone will process the keywords in the following order:
<urn:alert:tone:internal/external> >> ringtone/ MyMelody >> Bellcore-dr >> info=.

When desk 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	Settings → Ringing → Internal Ring TextX	
Parameter	**SettingRingerFileX**	**config.xml**
Description	It configures internal call ring melody X. The X can be 1-10.	
Permitted Values	Light Bounce Discovery Lounge Uptown Morning Lights Miami Far East Hight Speed Rain Drops Deep Space Steam Train Happy Decrescendo Strident Peacefulness Verticals Classic Ring1 Classic Ring2	

	Classic Ring3 Classic Ring4
Default	Blank
Web UI	Settings → Ringing → Internal Ring FileX

7.4.1.1 Alert-Info: Bellcore-drN

When the Alter-Info header contains the keyword “Bellcore-dr**N**”, the deskphone will play the desired ring tone.

The following table identifies the corresponding ring tone:

Value of N	Ring Tone
0	Bellcore-dr0
1	Bellcore-dr1
2	Bellcore-dr2
3	Bellcore-dr3
4	Bellcore-dr4
5	Bellcore-dr5
6	Bellcore-dr6
7	Bellcore-dr7
8	Bellcore-dr8
9	Bellcore-dr9
10	Bellcore-dr10
11	Bellcore-dr11
12	Bellcore-dr12
13	Bellcore-dr13
14	Bellcore-dr14

Examples:

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

7.4.1.2 Alert Info for Auto Answer

If the INVITE request contains the following type of strings, the deskphone 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

SIP deskphones 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 loudspeaker.

If the ringer device is configured on headset or Headset & Speaker, the headset should be connected to the SIP deskphone 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 + Headset	
Default	0	
Web UI	Settings → Ringing → Ring Device	
Phone UI	Menu → Basic Setting → Sound → Ringing → Ring Device	

7.6 Tones

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

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 the country tone for the phones.	
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 99 - Custom	
Default	0	
Web UI	Settings → Tone → Country Tone	

7.6.3 Custom tone

Although we have prefabricated a complete set of audio configuration options for different regions, you may want to customize your own audio to be more local, such as different frequencies, different duration, custom customer audio is a good way to meet this requirement.

Custom Tone example:

Tone = Freq/Duration[;Freq/Duration][; Freq/Duration]...

Freq = Freq1[+Freq2][+Freq3][+Freq4]

Description:

1. Freq/Duration indicates a group of frequencies. A Tone can contain a maximum of eight frequencies.

2. A group of frequencies supports the juxtaposition of a maximum of two frequencies.

3. Freq ranges from 200 to 4000 Hz, Duration ranges from 0 to 30000ms; Freq=0 indicates that the mute Duration is not played. You can set the mute duration by 0/Duration.

4. Setting example: SettingDialTone = 200/1000; 0/1000; 200+2000/1000: After the Dial Tone is triggered, the frequency of 200Hz is played for 1s, and then muted for 1s, and then the two frequencies are played for 1s at the same time.

5. Special value description:

a. Freq without /Duration indicates the frequency of the group. For example, 200/1000; 300 means that the frequency of 200Hz is played for 1s, and then the frequency of 300Hz is played all the way.

b. Tone with "!" It is played only once. For example: ! 200/1000; 0/1000; 200+300/1000, which means to play 1s at 200Hz, then mute 1s, then play 1s at both 200Hz and 300Hz, and then end Tone play.

7.6.4 Custom Tones Configuration

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

Parameter	SettingDialTone	config.xml
Description	It customizes the dial tone. **Note**: It works only if “**SettingCountryTone**” is set to 99.	
Permitted Values	String within 512 Characters.	
Default	Blank	
Web UI	Settings → Tone → Dial	
Parameter	**SettingSecondaryDialTone**	**config.xml**
Description	It customizes the secondary dial tone. **Note**: It works only if “**SettingCountryTone**” is set to 99.	

Permitted Values	String within 512 Characters.	
Default	Blank	
Web UI	Settings → Tone → Secondary Dial	
Parameter	**SettingRingBackTone**	**config.xml**
Description	It customizes the ring back tone. **Note**: It works only if "**SettingCountryTone**" is set to 99.	
Permitted Values	String within 512 Characters.	
Default	Blank	
Web UI	Settings → Tone → Ring Back	
Parameter	**SettingBusyTone**	**config.xml**
Description	It customizes the busy tone. **Note**: It works only if "**SettingCountryTone**" is set to 99.	
Permitted Values	String within 512 Characters.	
Default	Blank	
Web UI	Settings → Tone → Busy	
Parameter	**SettingCallWaitingTone**	**config.xml**
Description	It customizes the call waiting tone. **Note**: It works only if "**SettingCountryTone**" is set to 99.	
Permitted Values	String within 512 Characters.	
Default	Blank	
Web UI	Settings → Tone → Call Waiting	
Parameter	**SettingStutterTone**	**config.xml**
Description	It customizes the stutter tone. **Note**: It works only if "**SettingCountryTone**" is set to 99.	
Permitted Values	String within 512 Characters.	
Default	Blank	
Web UI	Settings → Tone → Stutter	

7.7 Key Tone

Allow the phone to play a key tone when you press any key.

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

Parameter	FeatureKeyToneEnable	config.xml
Description	It enables or disables the phone to play a key tone when a user presses any key on your phone keypad.	
Permitted Values	false - Disable true - Enable	
Default	true	

7.8 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 SIP deskphone 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.

7.8.1 Supported Audio Codecs

The following table summarizes the supported audio codecs by deskphones:

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
G726-16	G726-16	RFC 3351	16 Kbps	16 Kbps	20ms
G726-24	G726-24	RFC 3351	24 Kbps	24 Kbps	20ms
G726-32	G726-32	RFC 3351	32 Kbps	32 Kbps	20ms
G726-40	G726-40	RFC 3351	40 Kbps	40 Kbps	20ms

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

Abbreviation	Audio Bandwidth	Sample Rate (Effective)
NB (Narrow Band)	4 kHz	8 kHz
WB (Wide Band)	8 kHz	16 kHz
SWB (Super Wide Band)	20 kHz	48 kHz

7.8.2 Audio Codecs Configuration

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

Note: X means account ID. It can be number 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.

Parameter	**AccountXAudioCodec**	**config.xml**
Description	It configures the codec list which is supported by phone for account.	
Permitted Values	8 - pcma 0 - pcmu 9 - g722 18 - g729AB 98 - iLbc 125 – opus 111 – g726-16 112 – g726-24 113 – g726-32 114 – g726-40	
Default	0;8;18;9;98	
Web UI	Account → Codec → Audio Codec	
Parameter	**AccountXOpusBandwidth**	**config.xml**
Description	It configures Opus bandwidth for account.	
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 account.	
Permitted Values	20 - 20 30 - 30	
Default	30	

Web UI	Account → Codec → ILBC Frame Mode	
Parameter	**Account[X]OpusPayloadType**	**config.xml**
Description	It configures the payload type of OPUS codec.	
Permitted Values	96-127	
Default	125	

7.9 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.

7.9.1 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
G726-16	10ms	30ms
G726-24	10ms	30ms
G726-32	10ms	30ms
G726-40	10ms	30ms

7.9.2 PTime Configuration

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

Note: X means account ID. It can be 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.

Parameter	**AccountXPtime**	**config.xml**
Description	It configures the ptime (in milliseconds) for the codec.	

Permitted Values	10 20 30 40 50 60	
Default	20;20;20;20;20;20	
Web UI	Account → Codec → Ptime	

7.10 Early Media

The early media refers to the media played to the caller before a SIP call is established. Current implementation supports early media through the 183 messages. 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 an early media stream for the caller.

The processing capability in the 18x SDP ringback tone scenario has been optimized. After the terminal device receives the 18x SDP message, if the remote device fails to provide effective ringback tone audio in time, ALE phone will switch to the local ringtone based on the timeout parameter.

Parameter	**SIPEarlyMediaMonitorTimeout**	**config.xml**
Description	Configure how long the phone waits to play the local ringback tone when the 180 or 183 messages received by the phone have SDP but early media fails to play.	
Permitted Values	0: Do not play local ringback tones 1-100: Play the local ringback tone after the specified time (unit: seconds)	
Default	1	

7.11 Acoustic Clarity Technology

To optimize the audio quality of your network, the ALE SIP DeskPhones 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.

7.11.1 Acoustic Echo Cancellation (AEC)

The ALE SIP DeskPhones 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.

7.11.2 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 SIP DeskPhones by default.

7.11.3 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.

7.11.4 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.

7.11.5 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 parameters you can use to configure VAD.

Note: X means account ID. It can be number 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 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	

7.11.6 Comfort Noise Generation (CNG)

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

7.11.7 Jitter Buffer

The ALE SIP DeskPhones support two types of jitter buffers: static and adaptive. A static jitter buffer adds the fixed delay to voice packets. You can configure the delay time for the static jitter buffer on the phones. An adaptive jitter buffer is capable of adapting the changes in the network's delay. The range of the delay time for the dynamic jitter buffer added to packets can be also configured on the phones.

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

Parameter	**SettingJitterBufferMode**	**config.xml**
Description	It configures the mode of jitter buffer in the wired network.	
Permitted Values	0 – Adaptive 1 - Static	
Default	0	
Parameter	**SettingJitterBufferMin**	**config.xml**

Description	It configures the minimum delay time (in milliseconds) of the jitter buffer in the wired network. **Note:** It works only if "**SettingJitterBufferMode**" is set to 0 (Adaptive). The value of this parameter should be less than or equal to that of "**SettingJitterBufferMax**".	
Permitted Values	Integer from 0 to 600	
Default	20	
Parameter	**SettingJitterBufferMax**	**config.xml**
Description	It configures the maximum delay time (in milliseconds) of the jitter buffer in the wired network. **Note:** It works only if "**SettingJitterBufferMode**" is set to 0 (Adaptive). The value of this parameter should be greater than or equal to that of "**SettingJitterBufferMin**".	
Permitted Values	Integer from 0 to 600	
Default	250	
Parameter	**SettingJitterBufferNormal**	**config.xml**
Description	It configures the normal delay time (in milliseconds) of the jitter buffer in the wired network. **Note:** The value of this parameter should be greater than or equal to that of "**SettingJitterBufferMin**" and less than or equal to that of "**SettingJitterBufferMax**".	
Permitted Values	Integer from 0 to 600	
Default	50	
Parameter	**SettingWifiJitterBufferMode**	**config.xml**
Description	It configures the mode of jitter buffer in the wireless network.	
Permitted Values	0 – Adaptive 1 - Static	
Default	0	
Parameter	**SettingWifiJitterBufferMin**	**config.xml**
Description	It configures the minimum delay time (in milliseconds) of the jitter buffer in the wireless network. **Note:** It works only if "**SettingWifiJitterBufferMode**" is set to 0 (Adaptive). The value of this parameter should be less than or equal to that of "**SettingWifiJitterBufferMax**".	

Permitted Values	Integer from 0 to 600	
Default	20	
Parameter	**SettingWifiJitterBufferMax**	**config.xml**
Description	It configures the maximum delay time (in milliseconds) of the jitter buffer in the wireless network. **Note:** It works only if "**SettingWifiJitterBufferMode**" is set to 0 (Adaptive). The value of this parameter should be greater than or equal to that of "**SettingWifiJitterBufferMin**".	
Permitted Values	Integer from 0 to 600	
Default	250	
Parameter	**SettingWifiJitterBufferNormal**	**config.xml**
Description	It configures the normal delay time (in milliseconds) of the jitter buffer in the wireless network. **Note:** The value of this parameter should be greater than or equal to that of "**SettingWifiJitterBufferMin**" and less than or equal to that of "**SettingWifiJitterBufferMax**".	
Permitted Values	Integer from 0 to 600	
Default	50	

7.12 DTMF

DTMF (Dual Tone Multi-frequency) tone better known as touch tone. DTMF is the signal sent from the SIP deskphone to the network, which is generated when pressing the SIP deskphone's keypad during a call. Each key pressed on the SIP deskphone generates one sinusoidal tone of two frequencies. One is generated from a high-frequency group and the other from a low-frequency group. Currently we support the DTMF code:0-9 * # ABCD.

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 4733 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 DTMF digits are transmitted SIP INFO and RTP (RTP EVENT).
- SIP_INFO or RFC4733 DTMF digits are transmitted SIP INFO and RTP (RTP EVENT).

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

Note: X means account ID. It can be number 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.

Parameter	**AccountXDtmfMode**	**config.xml**
Description	It configures the DTMF mode.	
Permitted Values	0 - None 1 - InBand 2 - RFC2833 3 - RFC4733 4 - SIP_INFO 5 - SIP_INFO+RFC2833 6 - SIP_INFO or RFC4733	
Default	2	
Web UI	Account → Advanced → DTMF Mode	
Parameter	**SettingDtmfDuration**	**config.xml**
Description	It configures 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 tone.	
Permitted Values	false - Disable true - Enable	
Default	true	
Web UI	Settings → 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	Settings → Audio → DTMF Level

7.13 Voice Quality Monitoring (VQM)

Voice quality monitoring feature allows the SIP deskphones 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.

7.13.1 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.

7.13.2 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 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.

Parameter	**AccountXVoIPTicketsCollector**	**config.xml**
Description	The VoIP ticket collector name is used for publishing VoIP tickets. If the value is empty, no PUBLISH request will be sent at the end of each call.	
Permitted Values	String within 128 characters	
Default	Blank	
Web UI	Account → Advanced → SIP VoIP Tickets Collector	

7.14 Suppress DTMF Display

Suppress DTMF Display allows SIP deskphones 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 SIP deskphone 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 SIP DeskPhones.

8.1 Account Registration

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

8.1.1 Supported Accounts

The ALE H3G deskphone supports 3 accounts, H6 supports 4 accounts, M3s/M5s/M7s/M7s Pro support 8 accounts, and M8 supports 20 accounts.

8.1.2 SIP Accounts Registration Configuration

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

Note: X means account ID. It can be number 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.

Parameter	**AccountXEnable**	**config.xml**
Description	It enables or disables the account.	
Permitted Values	true - Disable. false - Enable	
Default	true	
Web UI	Account → Basic → Account Active	
Phone UI	Menu → Advanced Setting (default password: 123456) → Account → AccountX → Account Enable	
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 → Account Label	
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 username.	
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	
Phone UI	Menu → Advanced Setting (default password: 123456) → Account → AccountX → SIP Port1	
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.	
Permitted Values	Integer from 0 to 65535	
Default	5060	
Web UI	Account → Basic → OutBound Proxy Port	
Phone UI	Menu → Advanced Setting (default password: 123456) → Account → AccountX → Proxy Port1	
Parameter	**AccountXServer1Expire**	**config.xml**
Description	It configures the registration expiration time (in seconds).	
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 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.

Parameter	**AccountXSendUserPhoneEnable**	**config.xml**
Description	It enables or disables the SIP deskphone 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	
Parameter	**AccountXRedirectMessageProcessingPriority**	**config.xml**
Description	It configures the priority of processing when the phone receives a redirect message with multiple addresses.	
Permitted Values	UDP; TCP; TLS the one or more. **For example:** UDP;TLS;TCP or UDP;TCP or TCP;TLS;UDP.	
Default	Blank It is means use UDP;TCP;TLS	
Parameter	**AccountXRegisterRenewalIntervalProportion**	**config.xml**
Description	It configures the policy for phone register renewal. The default value is 50%. You can modify the renewal interval.	
Permitted Values	Integers 1 to 99.	
Default	50	

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 SIP deskphone 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 SIP deskphone 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 SIP deskphone 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 SIP deskphone 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 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 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 SIP server.	
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 SIP server.	
Permitted Values	Integer from 0 to 65535	
Default	5060	
Web UI	Account → Basic → Secondary SIP Port	
Phone UI	Menu → Advanced Setting (default password: 123456) → Account → AccountX → SIP Port2	
Parameter	**AccountXServer2Expire**	**config.xml**
Description	It configures the registration expiration time (in seconds) of secondary SIP server.	
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.	
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.	
Permitted Values	Integer from 0 to 65535	
Default	5060	
Web UI	Account → Basic → Secondary Outbound Proxy Port	
Phone UI	Menu → Advanced Setting (default password: 123456) → Account → AccountX → Proxy Port2	
Parameter	**AccountXServerFailoverSubscribeEnable**	**config.xml**
Description	It enables or disables re-subscribe immediately after registering to a different IP address.	

Permitted Values	false - Disable true - Enable
Default	false

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 SIP deskphone to adapt to various deployment environments. The SIP deskphone 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 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 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 SIP deskphone performs the DNS NAPTR and SRV queries for the service type and port.	
Default	0	
Web UI	Account → Basic → Transport Mode	
Phone UI	Menu → Advanced Setting (default password: 123456) → Account → AccountX → Transport Mode1	

8.4 SIP Default Account

When multiple accounts are configured, you can specify the default account to set the default outgoing number and modify the display policy on home bar to display the default account information.

Note: The phone support number 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.

Parameter	**SIPDefaultAccount**	**config.xml**
Description	It configures the SSIP deskphone default account.	

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 9 - Account 9 10 - Account 10 11 - Account 11 12 - Account 12 13 - Account 13 14 - Account 14 15 - Account 15 16 - Account 16 17 - Account 17 18 - Account 18 19 - Account 19 20 - Account 20	
Default	1	
Web UI	Features → Sip → Default Account	
Phone UI	Menu → Features → Default Account	
Parameter	**SettingDefaultAccountDisplayMode**	**config.xml**
Description	It configures set whether to display default account information on home bar.	
Permitted Values	0 – Do not display default account on home bar. 1 – Display default account on home bar.	
Default	0	

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 the Local History page. Users can switch the tabs by pressing the left/right keys.

9.1 Call Log Display

You can access the call history information via phone user interface by using the History softkey 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 saving call history.	
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 SIP DeskPhones:

10.1 Dial Plan

Dial plan is a string of characters that governs the way SIP deskphones process the inputs received from the SIP deskphone's keypads. You can use the regular expression to define the dial plan.

10.1.1 Dial Plan Defined by Dialing Rule

The ALE SIP DeskPhones 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. It can be number 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.

Parameter	**AccountXDialingRuleCountryCode**	**config.xml**
Description	It configures the country code. **Note:** This is mandatory for dialing rule feature.	
Permitted Values	ISO 3166 country code (Alpha-2)	
Default	Blank	
Web UI	Settings → Dialing Rule → Country Code	
Parameter	**AccountXDialingRuleAreaCode**	**config.xml**
Description	It configures the area code.	
Permitted Values	String within 16 characters	
Default	Blank	
Web UI	Settings → Dialing Rule → Area Code	
Parameter	**AccountXDialingRuleExternalPrefix**	**config.xml**
Description	It configures the external prefix.	
Permitted Values	String within 16 characters	
Default	Blank	
Web UI	Settings → Dialing Rule → External Prefix	
Parameter	**AccountXDialingRuleMinNumberLength**	**config.xml**
Description	It configures the minimum length of number.	

Permitted Values	Integer from 0 to 120	
Default	Blank	
Web UI	Settings → 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	Settings → 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	Settings → Dialing Rule → Dialing Rule Enabled in History	
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	Settings → Dialing Rule → Dialing Rule Enabled in Contact	
Parameter	**AccountXDialingRuleInForwardEnable**	**config.xml**
Description	It enables or disables dialing rule in forward.	

Permitted Values	true - Enable false - Disable	
Default	false	
Web UI	Settings → Dialing Rule → Dialing Rule Enabled in Forward	
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	Settings → Dialing Rule → Dialing Rule Enabled in Manual	

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 (eg 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	false - Disable true - enable	
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	false - Disable true - Enable	
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	false - Disable true - Enable	
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	false - Disable true - Enable	
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. It can be number 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.

Parameter	**AccountXDigitMapEnable**	**config.xml**
Description	It enables or disables the digit map feature for a specific account.	
Permitted Values	false - Disable true - Enable	
Default	true	
Parameter	**AccountXDigitMap**	**config.xml**
Description	It configures the digit map of account.	
Permitted Values	String within 2048 characters	
Default	Blank	
Parameter	**AccountXDigitMapTimer**	**config.xml**
Description	It configures the timer to dial the number which match the digit map for account.	
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	false - Disable true - Enable	
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	false - Disable true - Enable	
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	false - Disable true - Enable	

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	false - Disable true - Enable	
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 SIP deskphone 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	false - Disable true - Enable	
Default	false	
Web UI	Features → Hotline → Hotline	
Phone UI	Menu → Features → Hotline → Status	
Parameter	**FeatureHotlineNumber**	**config.xml**
Description	It configures the hotline number that the SIP deskphone 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 SIP deskphone to automatically dial out the preset hotline number.	

	Note: If it is set to 0, the SIP deskphone 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 SIP deskphones using a Recall key.

The following shows configuration for a Recall key:

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

After provisioning, a Recall key is available on the phone. When you press the Recall key, the phone places a 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 shows configuration for Speed Dial key:

```
<?xml version="1.0" encoding="UTF-8" ?>
<settings>
        <setting id="PhoneProgKey6Type" value="1"/>
        <setting id="PhoneProgKey6Account " value="1"/>
       <setting id="PhoneProgKey6Number" value="1001"/>
<setting id=" PhoneProgKey6Label " value="Allen"/>
</settings>
```

After provisioning, a Speed Dial key for Allen (1001) is available on the phone, and you can press the Speed Dial key to call Allen (1001) quickly.

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 SIP deskphone 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 dials out the number after inputting the last digit.

The following table lists the parameters 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 the caller. 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 SIP deskphone 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. It can be number 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.

Parameter	**AccountXAnonymousCallEnable**	**config.xml**
Description	It enables or disables the anonymous call feature for account.	

Permitted Values	false - Disable true - Enable	
Default	false	
Web UI	Account → Advanced → Anonymous Call	
Phone UI	Menu → Features → Anonymous → AccountX → Anonymous	
Parameter	**AccountXAnonymousCallOnCode**	**config.xml**
Description	It configures the anonymous call on code. The phone will send the code to activate the anonymous call feature on server side when you activate it on the phone.	
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 anonymous call off code. The phone will send the code to deactivate the anonymous call feature on server side when you deactivate it on the phone.	
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 SIP deskphone 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 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 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 → Anonymous Reject	
Parameter	**AccountXAnonymousCallRejectionOnCode**	**config.xml**
Description	It configures the anonymous call rejection on code. The SIP deskphone will send the code to activate anonymous call rejection feature on server side when you activate it on the SIP deskphone.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Account → Advanced → Anonymous Rejection → On Code	
Phone UI	Menu → Features → Anonymous Reject → Account X → On Code	
Parameter	**AccountXAnonymousCallRejectionOffCode**	**config.xml**
Description	It configures the anonymous call rejection off code. The SIP deskphone will send the code to deactivate anonymous call rejection feature on server side when you deactivate it on the SIP deskphone.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Account → Advanced → Anonymous Rejection → Off Code	
Phone UI	Menu → Features → Anonymous Reject → Account X → Off Code	

10.9 Call Number Filter

The call number filter feature allows an SIP deskphone to filter designated characters automatically when dialing.

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

Parameter	**FeatureCallNumberFilter**	**config.xml**
Description	It configures the characters that the SIP deskphone will filter when dialing. If the dialed number contains configured characters, the SIP deskphone will automatically filter these characters when dialing. If you dial 10-1, the SIP deskphone will filter the character - and then dial out 101.	

Permitted Values	String within 32 characters
Default	,-()
Web UI	Features → 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 "**SIPPeerFilterEnable**" to true.	
Permitted Values	false - Disable true - Enable	
Default	true	
Web UI	Features → SIP → Allow IP Call	

10.10.2 Accept SIP Trust Server Only Configuration

Accept SIP Trust Server Only enables the SIP deskphone 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 SIP deskphone 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	false - Disable true - Enable	
Default	false	
Web UI	Features → SIP → SIP Peer Filter	

10.11 Auto Answer

The ALE SIP DeskPhones 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 SIP deskphones 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 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.

Parameter	**AccountXAutoAnswerEnable**	**config.xml**
Description	It enables or disables auto answering a SIP call for accountX. **Note:** The SIP deskphone cannot automatically answer the incoming call during a call even if auto answer is enabled.	
Permitted Values	false - Disable true - Enable	
Default	false	
Web UI	Account → Advanced → Auto Answer	
Phone UI	Menu → Features → Auto answer → AccountX → Auto Answer	
Parameter	**FeatureAutoAnswerDelay**	**config.xml**
Description	It configures the delay time (in seconds) before the phone automatically answers an incoming call. Note: It works only if "**AccountXAutoAnswerEnable**" is set to true (Enabled).	
Permitted Values	1-60	
Default	1	
Parameter	**FeatureAutoAnswerToneEnable**	**config.xml**
Description	It configures the auto answer whether the prompt tone is played.	
Permitted Values	false - Disable true - Enable	
Default	false	

10.12 Call Waiting

While the Call waiting feature is 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 the 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.

ALE SIP DeskPhones will use 182 to respond to the second call when call waiting is enabled.

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	false - Disable true - Enable	
Default	true	
Web UI	Features → General → Call Waiting	
Phone UI	Menu → Features → Call Waiting → Call Waiting	
Parameter	**FeatureCallWaitingToneEnable**	**config.xml**
Description	It enables or disables the SIP deskphone to play the call waiting tone when the SIP deskphone receives an incoming call during a call. **Note:** It works only if "**FeatureCallWaitingEnable**" is set to true (Enabled).	
Permitted Values	false - Disable true - Enable	
Default	true	
Web UI	Features → General → Call Waiting Tone	
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	**FeatureCallWaitingOffCode**	**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	
Parameter	**FeatureKeepCallWaitingEnable**	**config.xml**

Description	It configures whether to keep the operation of the call waiting feature in the previous call after the call ends.	
Permitted Values	false - Disable true - Enable	
Default	true	
Parameter	**SettingSecondCallReplyMethod**	**config.xml**
Description	It configures the signaling for replying to new incoming call during a call.	
Permitted Values	0 - 180 Ringing 1 - 182 Queued	
Default	0	
Parameter	**SettingDeal182Enable**	**config.xml**
Description	It configures whether the phone will ring a special tone after receiving the 182 message.	
Permitted Values	false - disable true - enable	
Default	false	

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 SIP deskphone 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 SIP deskphone.	
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 the 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 SIP deskphones also support 2 methods to activate and deactivate server-side DND feature. They may vary on different servers.

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

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 enables or disables the DND feature. **Note:** It works only if “**FeatureDndMode**” is set to 0 (Phone).	
Permitted Values	false - Disable true - Enable. The SIP deskphone will reject incoming calls on all accounts.	
Default	false	
Web UI	Features → DND → Enable DND	
Phone UI	Menu → Features → Do not disturb → DND Status	
Parameter	**FeatureDndOnCode**	**config.xml**
Description	It configures the DND on code to activate the server-side DND feature. The SIP deskphone will send the DND on code to the server when you activate DND feature on the SIP deskphone. **Note:** It works only if “**FeatureDndMode**” is set to 0 (Phone).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → DND → DND On Code	
Phone UI	Menu → Features → Do not disturb → On Code	
Parameter	**FeatureDndOffCode**	**config.xml**
Description	It configures the DND off code to deactivate the server-side DND feature. The SIP deskphone will send the DND off code to the server when you deactivate	

	DND feature on the SIP deskphone. **Note:** It works only if “**FeatureDndMode**” is set to 0 (Phone).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features → DND → DND Off Code	
Phone UI	Menu → Features → Do not disturb → 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 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.

Parameter	**AccountXDndEnable**	**config.xml**
Description	It enables or disables the DND feature. **Note:** It works only “**FeatureDndMode**” is set to 1 (Custom).	
Permitted Values	false - Disable true - Enable. The SIP deskphone 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 SIP deskphone will send the DND on code to the server when you activate DND feature on the SIP deskphone. **Note:** It works only if “**FeatureDndMode**” is set to 1 (Custom) and “**FeatureDndEnable**” is set to true (Enabled).	
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 SIP deskphone will send the DND off code to the server when you deactivate DND feature on the SIP deskphone.	

	Note: It works only if "**FeatureDndMode**" set to 1 (Custom) and "**FeatureDndEnable**" set to false (Disabled).
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 SIP deskphone 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 SIP deskphone supports 2 methods to synchronize the status of the DND between the SIP deskphone and the server.

Prefix mode:

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

Subscribe mode:

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

With Subscribe mode the SIP deskphone doesn'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 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.

Parameter	**FeatureDNDMethod**	**config.xml**
Description	It configures the DND method for the phone. **Note:** It works only if "**FeatureDndMode**" is set to 0 (Phone).	
Permitted Values	0 - Prefix 1 - Subscribe. The SIP deskphone 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 account. **Note:** It works only if "**FeatureDndMode**" 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 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 SIP deskphone to display a large DND icon on the idle screen.	
Permitted Values	0 - default mode 1 - string 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.

Note: When Busy forward and DND are enabled at the same time, the Busy forward has a higher priority than DND.

10.14.1 Call Forward Setting Configuration

You can change the following call forward settings:

- Choose the 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 forward mode.

Parameter	**FeatureFwdMode**	**config.xml**
Description	It configures the FWD mode for the SIP deskphone.	
Permitted Values	0 - Phone. The 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 the 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 SIP deskphones 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	
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 SIP deskphone 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 SIP deskphone will send the always forward off code to the server when you deactivate always forward feature on the SIP deskphone. **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	
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 SIP deskphone 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 SIP deskphone will send the busy forward off code to the server when you deactivate busy forward feature on the SIP deskphone. **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	
Phone UI	Menu → Features → Call Forward → No Answer Forward → No Answer 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 Answer 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 SIP deskphone 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 SIP deskphone will send the no answer forward off code to the server when you deactivate no answer forward feature on the SIP deskphone. **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 Answer 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)	
Phone UI	Menu → Features → Call Forward → No Answer Forward → Delay	

Parameter	FeatureNoReplyFwdInterval	config.xml
Description	It configures Single ring interval. For example: 1. After FWD synchronization is enabled, the SIP deskphone calculates No Reply Forward Duration based on the ringcount (N) sent by the server and Interval (M) configured locally. The specific rule is Duration=N x M. Duration calculated is written directly to the arguments. 2. Similarly, if the Duration is changed locally, calculate the ringcount based on the rule and synchronize the ringcount to the server. If it's a decimal, round it up, like 5.3, and the ringcount is 6.	
Permitted Values	Integer from 1 to 60. The unit is seconds.	
Default	5	

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 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 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	
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 SIP deskphone 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 SIP deskphone will send the always forward off code to the server when you deactivate always forward feature on the SIP deskphone. **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	
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 SIP deskphone 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 SIP deskphone will send the busy forward off code to the server when you deactivate busy forward feature on the SIP deskphone. **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	

Phone UI	Menu → Features → Call Forward → No reply Forward → account ID → No Answer 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 Answer 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 SIP deskphone 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 SIP deskphone will send the no answer forward off code to the server when you deactivate no answer forward feature on the SIP deskphone. **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 Answer Forward → account ID → Off Code	

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 SIP deskphone 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 SIP deskphone supports 2 methods to synchronize the status of the call forward between the SIP deskphone and the server.

Prefix mode:

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

Subscribe mode:

The SIP deskphone will send subscribe message to synchronize the status of the call forward between the SIP deskphone 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. It can be number 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.

Parameter	FeatureFwdMethod	config.xml
Description	It configures the FWD method for the SIP deskphone. **Note:** It works only if "**FeatureFwdMode**" is set to 0 (Phone).	
Permitted Values	0 - Prefix 1 - Subscribe, the SIP deskphone 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 SIP deskphone account X. **Note:** It works only if "**FeatureFwdMode**" is set to 1 (Custom).	
Permitted Values	0 - Prefix 1 - Subscribe. The SIP deskphone 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 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 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 works only if "**FeaturedDndMethod**" is set to 1 (Subscribe) or "**AccountXDndMethod**" is set to 1 (Subscribe).	
Permitted Values	false - Disable true - Enable	
Default	false	
Parameter	**AccountXDndShareLineSyncServerEnable**	**config.xml**
Description	It configures shared line account DND sync. **Note:** It works only if "**FeaturedDndMethod**" is set to 1 (Subscribe) or "**AccountXDndMethod**" is set to 1 (Subscribe).	
Permitted Values	false - Disable true - Enable	
Default	true	
Parameter	**AccountXFwdSyncServerLocalProcessingEnable**	**config.xml**
Description	It configures share line account Forward sync. **Note:** It works only if "**FeatureFwdMethod**" is set to 1 (Subscribe) or "**AccountXFwdMethod**" is set to 1 (Subscribe).	
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	[1,5] **Note**: For M8, the permitted value is [1,11].	
Default	6 **Note**: For M8, the default value 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 SIP deskphones 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 SIP deskphones 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 SIP deskphone 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	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 SIP deskphone 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 SIP deskphone to play the initial call hold tone. If it is set to 30 (30s), the SIP deskphone 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.	
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 SIP deskphone 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.	
Permitted Values	Integer from 3 to 3600	
Default	30	
Parameter	**FeaturePlayHeldToneEnable**	**config.xml**
Description	It enables or disables the phone to play the call held tone when a call is held by the other party.	
Permitted Values	false - Disable true - Enable	
Default	false	
Parameter	**FeaturePlayHeldToneDelay**	**config.xml**
Description	It configures the time (in seconds) to wait for the SIP deskphone to play the initial call held tone. If it is set to 30 (30s), the SIP deskphone 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.	

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 SIP deskphone 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 "**FeaturePlayHeldToneEnable**" is set to true.	
Permitted Values	Integer from 3 to 3600	
Default	30	

10.17.2 Music on Hold

When a call is placed on hold, the SIP deskphone 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.

10.18 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 the keep mute feature to keep the mute state persisting across the calls. In a call center or meeting 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 unintended situations. 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 parameters you can use to enable or disable keep mute.

Parameter	**FeatureKeepMuteEnable**	**config.xml**
Description	It enables or disables the keep mute feature.	
Permitted Values	false - Disable true - Enable	
Default	false	

10.19 Call Transfer

Call transfer enables the SIP deskphones 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 SIP DeskPhones 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.
- **Semi-attended Transfer** - Transfer a call without consulting but need ringing. 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	**FeatureBlindTransferOnHookEnable**	**config.xml**
Description	It enables or disables the phone to complete the blind transfer through on-hook.	
Permitted Values	false - Disable true - Enable	
Default	true	
Parameter	**FeatureAttendedTransferOnHookEnable**	**config.xml**
Description	It enables or disables the phone to complete the semi-attended/attended transfer through on-hook.	
Permitted Values	false - Disable true - Enable	
Default	true	
Parameter	**FeatureTransAfterConfEnable**	**config.xml**
Description	It enables or disables the phone to transfer the local conference call to the other two parties after the conference initiator drops the local conference call.	
Permitted Values	false - Disable true - Enable	
Default	false	
Parameter	**FeatureTransProgKeyDealType**	**config.xml**
Description	It configures the transfer mode for the program key. When the user presses the program Key during a call, the program Key behavior depends on the transfer mode. **Note:** This feature is only applicable to the Speed Dial key, BLF/BLF List key or Transfer key with an assigned value.	

Permitted Values	0 - New Call 1 - Attended Transfer 2 - Blind Transfer 3 - Optional, users can choose to transfer the call via New Call, Attended Transfer or Blind Transfer manually	
Default	2	
Parameter	**FeatureSemiAttendTransEnable**	**config.xml**
Description	It enables or disables the semi-attend transfer feature.	
Permitted Values	false - Disable true - Enable	
Default	false	
Parameter	**SIPTranSuccessfulNotify**	**config.xml**
Description	It configures which signaling is received to indicate that the transfer is successful.	
Permitted Values	0 - Notify with 200 OK 1 - Notify with 100 Trying 2 - Notify with 180 Ringing 3 - 202 Accepted 4 - Notify with Terminated	
Default	0	

10.19.2 Transfer Mode Configuration for Programmable Key

You can configure the transfer mode for the SIP deskphone when transferring the current call via a specified programmable key. The ALE SIP DeskPhones support the transfer modes: New Call, Blind Transfer.

The following table lists the parameters 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 programmable key during a call, the behavior depends on the transfer mode.	
Permitted Values	false - Disable true - Enable	
Default	false	

10.20 Conference

The ALE SIP DeskPhones support multi-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 SIP DeskPhones support up to 6 parties for H3G/H6/M3s/M5s/M7s/M7s Pro, and 12 parties for M8 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 deskphones, you can merge two calls into a conference directly by pressing the Conf softkey 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 conferences.

Note: X means account ID. It can be number 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.

Parameter	**AccountXLocalConfEnable**	**config.xml**
Description	It enables or disables the local conference feature.	
Permitted Values	false - Disable true - Enable	
Default	true	
Web UI	Features → SIP → Local Conference Enable	
Parameter	**FeatureLocalConfOnePressSetUpEnable**	**config.xml**
Description	It configures to enable or disable the one-click meeting creation function.	
Permitted Values	False - Disabled. After the user establishes a call with a third party, they need to press the Conference Key again to establish a Local Conference (default value). True - Enabled. After the user establishes a call with a third party, it will be directly pulled into the Local Conference	
Default	false	

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 SIP deskphones 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 parameters you can use to configure network conference.

Note: X means account ID. It can be number 1-3 for H3G, 1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 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	String within 512 characters	
Default	Blank	
Web UI	Account → Advanced → N-conference URI	
Parameter	AccountXNConfMethod	config.xml
Description	It configures the network conference method.	
Permitted Values	0 - Send refer to peer call. 1 - Direct call out.	
Default	0	

10.21 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 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 auto redial times when the callee is temporarily unavailable. The phone tries to redial the callee as many times as configured 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 → Redial Times	
Parameter	**FeatureAutoRedialInterval**	**config.xml**
Description	It configures the interval (in seconds) for the phone to wait between redials. The phone redials the last dialed number at regular intervals untill 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 → Redial Interval	

10.22 USB Recording

10.22.1 USB Recording Switch

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 SIP deskphone. This is for devices that have USB A ports on them. Currently, support FAT32 and NFTS format. Supports a maximum of 64 GB memory space.

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

10.22.2 USB Recording File Upload

ALE phones support backup recording file to server.

After the upload function is enabled, the phone can use http or https to upload files using put or post to back up files to the server. It also supports automatic upload and manual upload for easy operation.

Parameter	**FeatureRecordingUploadEnable**	**config.xml**
Description	It enables or disables the local recording automatic upload feature.	

Permitted Values	false - Disable true - Enable	
Default	false	
Parameter	**FeatureRecordingUploadServerUrl**	**config.xml**
Description	It configures the IP address of the server for uploading local recording files. **Note:** It works only if "**FeatureRecordingUploadEnable**" is set to true.	
Permitted Values	URL within 512 characters	
Default	Blank	
Parameter	**FeatureRecordingUploadServerUsername**	**config.xml**
Description	It configures the authentication username of the server where the local recording file uploaded is specified. **Note:** It works only if "**FeatureRecordingUploadEnable**" is set to true.	
Permitted Values	String within 64 characters	
Default	Blank	
Parameter	**FeatureRecordingUploadServerPassword**	**config.xml**
Description	It configures the authentication password of the server where the local recording file uploaded is specified. **Note:** It works only if "**FeatureRecordingUploadEnable**" is set to true.	
Permitted Values	String within 64 characters	
Default	Blank	
Parameter	**FeatureRecordingUploadAutoEnable**	**config.xml**
Description	It enables or disables the automatic uploading of local recording files to the server immediately after the generation of local recording files. **Note:** It works only if "**FeatureRecordingUploadEnable**" is set to true.	
Permitted Values	false - Disable true - Enable	
Default	false	
Parameter	**FeatureRecordingUploadDailyEnable**	**config.xml**
Description	It configures to enable the scheduled upload of local recording files. **Note:** It works only if "**FeatureRecordingUploadEnable**" is set to true.	
Permitted Values	false - Disable true - Enable	
Default	false	

Parameter	**FeatureRecordingUploadBeginTime**	**config.xml**
Description	It configures to enable the scheduled upload of local recording files start time. **Note:** It works only if "**FeatureRecordingUploadDailyEnable**" is set to true.	
Permitted Values	Time from 00:00 to 23:59	
Default	00:00	
Parameter	**FeatureRecordingUploadEndTime**	**config.xml**
Description	It configures to enable the scheduled upload of local recording files end time. **Note:** It works only if "**FeatureRecordingUploadDailyEnable**" is set to true.	
Permitted Values	Time from 00:00 to 23:59	
Default	00:00	
Parameter	**FeatureRecordingAutoDeleteEnable**	**config.xml**
Description	It enables or disables the feature of automatically deleting USB flash drive recording files.	
Permitted Values	false – Disable true - Enable	
Default	true	
Parameter	**FeatureRecordingAutoDeleteThreshold**	**config.xml**
Description	It configures the remaining capacity of the USB flash drive, the earliest recording files are automatically deleted.	
Permitted Values	The integer ranges from 0 to 1024. The unit is MB.	
Default	20	
Parameter	**FeatureRecordingFileDeleteMethod**	**config.xml**
Description	It configures the method for automatically deleting recording files. Delete or not delete recording files after uploading successfully. **Note:** It works only if "**FeatureRecordingUploadEnable**" is set to true.	
Permitted Values	0 - Do not delete local recording files. 1 - Delete recording files after uploading successfully.	
Default	0	
Parameter	**FeatureRecordingUploadRetryTimes**	**config.xml**
Description	It configures retry times when recording file upload failed. **Note:** It works only if "**FeatureRecordingUploadEnable**" is set to true.	
Permitted Values	0-5 **Note:** 0 means that do not retry.	

Default	2	

10.23 Confidential Dial and Incoming call

Confidential dial/incoming call feature allows the peer number to be partially displayed on the SIP deskphone when placing a call or receiving a call. The hidden digits are displayed as asterisks on the phone screen. The number in the placed/received call list is also partially displayed on the 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 confidential dial.

Parameter	**FeatureConfidentialDialEnable**	**config.xml**
Description	It enables or disables the confidential 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. **Note:** It works only if “**FeatureConfidentialDialEnable**” is set to true.	
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. **Note:** It works only if “**FeatureConfidentialDialEnable**” is set to true.	
Permitted Values	Integer from 0 to 32	
Default	0	
Web UI	Features → General → Confidential Dial Length (0-32)	
Parameter	**FeatureConfidentialIncomingCallEnable**	**config.xml**
Description	It enables or disables the confidential incoming call feature.	
Permitted Values	false - Disable true - Enable	
Default	false	
Parameter	**FeatureConfidentialIncomingCallPrefix**	**config.xml**
Description	It configures the prefix of the number that needs to be partially displayed.	

	Note: It works only if "**FeatureConfidentialIncomingCallEnable**" is set to true.	
Permitted Values	String within 32 characters	
Default	Blank	
Parameter	**FeatureConfidentialIncomingCallLength**	**config.xml**
Description	It configures how many digits need to be displayed as asterisks. **Note:** It works only if "**FeatureConfidentialIncomingCallEnable**" is set to true.	
Permitted Values	String within 32 characters	
Default	Blank	

10.24 Multicast Paging

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

The ALE SIP DeskPhones support the following 26 channels:

0 to 25: Broadcasts are sent to channel 0 to 25.

The SIP deskphones can only send and receive broadcasts to/from the listened channels. Other channels' broadcasts will be ignored automatically by the SIP deskphone.

10.24.1 Multicast Paging Group Configuration

The ALE SIP DeskPhones support up to 25 groups for paging. You can assign multicast IP addresses 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).

The following table lists the parameters you can use to configure the 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	0-25	
Default	1	
Web UI	Features → Multicast Paging → Paging List	

10.24.2 Multicast Listening Group Configuration

The ALE SIP DeskPhones support up to 25 groups for listening. You can assign multicast IP addresses 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	0-25	

Default	1
Web UI	Features → Multicast Paging → Listening List

10.24.3 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 0 (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 to 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 8 - PCMA 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 – disable. All incoming multicast paging calls will be automatically ignored when a voice call is in progress. [1-25] – The phone will receive the incoming multicast paging call with a higher or equal priority and ignore the one with a lower priority when a voice call is in progress.	
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 – disable. All incoming multicast paging calls will be automatically ignored when DND is activated in phone mode. [1-25] – The phone will receive the incoming multicast paging call with a higher or same priority than this value and ignore that with a lower priority than this value when DND is activated in phone mode.	
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. The engaged audio device will be used when receiving the multicast paging calls. 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 end.	
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 32 characters	
Default	Pegasus	

10.25 Action URL

The action URL allows SIP deskphones 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 SIP deskphone when the SIP deskphone mutes a call.

10.25.1 Pre-defined Events List

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

Event	Description
Setup Completed	When the SIP deskphone completes startup.
Register Succeeded	When the SIP deskphone successfully registers an account.
Unregistered	When the SIP deskphone logs out of the registered account.
Register Failed	When the SIP deskphone fails to register an account.
Off Hook	When the SIP deskphone is off hook.
On Hook	When the SIP deskphone is on hook.
Incoming Call	When the SIP deskphone receives an incoming call.
Reject Incoming Call	When the SIP deskphone rejects an incoming call.
Answer Incoming Call	When the SIP deskphone answers a new call.
Outgoing Call	When the SIP deskphone 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 SIP deskphone misses a call.
Call Established	When the SIP deskphone establishes a call.
Call Terminated	When the SIP deskphone terminates a call.
DND Enabled	When the SIP deskphone 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 SIP deskphone 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 SIP deskphone 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 SIP deskphone 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 SIP deskphone 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 SIP deskphone 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 SIP deskphone 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 SIP deskphone 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 SIP deskphone forwards an incoming call.
Call Transfer	When the SIP deskphone transfers a call.
Blind Transfer	When the SIP deskphone performs the blind transfer.
Attended Transfer	When the SIP deskphone performs the semi-attended/attended transfer.
Transfer Failed	When the SIP deskphone fails to transfer a call.
Transfer Finished	When the SIP deskphone completes transferring a call.
Call Waiting Enabled	When the SIP deskphone enables the call waiting.
Call Waiting Disabled	When the SIP deskphone disables the call waiting.
Call Hold	When the SIP deskphone places a call on hold.
Call Resume	When the SIP deskphone resumes a held call.
Mute	When the SIP deskphone mutes a call.
UnMute	When the SIP deskphone un-mutes a call.
IP Changed	When the IP address of the SIP deskphone changes.
Idle To Busy	When the state of the SIP deskphone changes from idle to busy.
Busy To Idle	When the state of phone changes from busy to idle.
Autop Start	When the SIP deskphone starts auto provisioning.
Autop Finish	When the SIP deskphone completes auto provisioning via power on.
Headset	When the SIP deskphone presses the HEADSET key.
Handsfree	When the SIP deskphone 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 SIP deskphone starts reboot.
Reset	When the SIP deskphone starts reset.
Screen Active	When the SIP deskphone screen is active.
Screen Inactive	When the SIP deskphone screen is inactive.

Conference Established	When the SIP deskphone establishes a conference.

10.25.2 Variable Values List

The following table lists pre-defined variable values.

Variable Value	Description
$mac	The MAC address of the SIP deskphone.
$ip	The IP address of the SIP deskphone.
$model	The SIP deskphone model.
$firmware	The firmware version of the SIP deskphone.
$active_url	The SIP URI of the current account when the SIP deskphone 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 SIP deskphone 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 SIP deskphone places a call, receives an incoming call or establishes a call.
$local	The SIP URI of the caller when the SIP deskphone places a call. The SIP URI of the callee when the SIP deskphone receives an incoming call.
$remote	The SIP URI of the callee when the SIP deskphone places a call. The SIP URI of the caller when the SIP deskphone receives an incoming call.
$display_local	The display name of the caller when the SIP deskphone places a call. The display name of the callee when the SIP deskphone receives an incoming call.
$display_remote	The display name of the callee when the SIP deskphone places a call. The display name of the caller when the SIP deskphone receives an incoming call.
$call_id	The call-id of the active call.

$callerID	The display name of the caller when the SIP deskphone receives an incoming call.
$calledNumber	The phone number of the callee when the SIP deskphone 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.

10.25.3 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 512 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 SIP deskphone from busy to idle.	
Permitted Values	URL within 512 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 512 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 512 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 512 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 512 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 512 characters	
Default	Blank	
Web UI	Features → Action URL → Handsfree	
Parameter	**ActionUrlPeripheralInformation**	**config.xml**
Description	It configures the action URL the phone sends when you unplug or plug the accessory.	
Permitted Values	URL within 512 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 512 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 512 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 512 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 512 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 512 characters	
Default	Blank	
Web UI	Features → Action URL → Screen Inactive	
Parameter	ActionUrlConferenceEstablished	config.xml
Description	It configures the action URL the SIP deskphone sends when establishing a conference.	
Permitted Values	URL within 512 characters	
Default	Blank	
Web UI	Features → Action URL → Conference Established	

10.26 Action URI

The ALE SIP DeskPhones can perform the specified action by receiving and handling an HTTP or HTTPS GET request or accepting a SIP NOTIFY message with the "Event: ACTION-URI" header from a SIP proxy server.

10.26.1 Supported HTTP/HTTPS GET Request

Opposite to action URL, action URI allows SIP deskphones to interact with web server application by receiving and handling an HTTP or HTTPS GET request. When receiving a GET request, the SIP deskphone 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, SIP deskphones do not handle HTTP/HTTPS GET requests by default. You need to specify the trusted IP address for the action URI. When the SIP deskphone 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" softkey on the phone to allow remote control.

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

10.26.2 Supported SIP Notify Message

In addition, ALE SIP DeskPhones 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 the SIP NOTIFY message method, you do not need to specify the trusted IP address for action URI. However, you should enable the SIP deskphone to receive the action URI requests. When the SIP deskphone 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" softkey 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
```

10.26.3 Variable Values List

The ALE SIP DeskPhones 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	Short press the line key. H3G: X=1-3 H6: X=1-4 M3s: X=1-6 M5s/M7s/M7s Pro: X=1-8 M8: X=1-10
F_LX_LONGPRESS	Long Press Line key. H3G: X=1-3 H6: X=1-4 M3s: X=1-6 M5s/M7s/M7s Pro: X=1-8 M8: X=1-10
FX	Short press the Softkey. H3G/H6/M3s/M5s/M7s/M7s Pro: X=1-4 M8: X=1-5
(F_) 0-9/*/ F_STAR/F_POUND	Short press the number key
(F_) E{x}_{y}	X=AOM index y=Corresponding AOM key. For example: E1_1 = AOM 1 first key E2_2 = AOM 2 second key
F_ E{x}_{y}_LONGPRESS	X=AOM index y=Corresponding AOM key. For example: E1_1_LONGPRESS = Long press AOM 1 first key E2_2_LONGPRESS = Long press AOM 2 second key
E{x}_LEFT / E{x}_RIGHT / E{x}_HOME	X=AOM index. Press the bottom three buttons on the AOM.
(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 H3G/H6 M3s/M5s/M7s/M7s Pro)
F_ CONFERENCE_ LONGPRESS	Long Press Conference key (for H3G/H6 M3s/M5s/M7s/M7s Pro)
(F_) HEADSET	Short press the Headset key (for M8)
F_ HEADSET_ LONGPRESS	Long press the Headset 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 SIP deskphone (“xxx” means the destination number)
AlwaysFwdOff/BusyFwdOff/NoAnswFwdOff	Deactivate the always/busy/no answer forward feature for the SIP deskphone
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

10.26.4 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	

10.27 Call Refused Code

When traffic is busy in different scenarios, ALE phones can customize refused code in different scenarios so that the peer end can receive customized information.

Parameter	**FeatureNormalRefuseCode**	**config.xml**
Description	It configures normal refuse code.	
Permitted Values	404 - 404(Not Found) 480 - 480(Temporarily Unavailable) 486 - 486(Busy Here) 600 - 600(Busy Everywhere) 603 - 603(Decline)	
Default	486	
Parameter	**FeatureDndRefuseCode**	**config.xml**
Description	It configures DND refuse code.	
Permitted Values	404 - 404(Not Found) 480 - 480(Temporarily Unavailable) 486 - 486(Busy Here) 600 - 600(Busy Everywhere) 603 - 603(Decline)	
Default	486	
Parameter	**FeatureNoAnswerCode**	**config.xml**
Description	It configures no answer refuse code.	
Permitted Values	404 - 404(Not Found) 480 - 480(Temporarily Unavailable) 486 - 486(Busy Here) 600 - 600(Busy Everywhere) 603 - 603(Decline)	
Default	486	

11. Phone Customization

11.1 Multiple Languages

The ALE SIP DeskPhones 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 setting language.

Parameter	**SettingLanguage**	**config.xml**
Description	It configures phone display setting language.	
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 30 – Thai 99 - Customer
Default	0
Phone UI	Menu → Basic Setting → Language
WEB UI	Settings → Display → Language

11.1.2 Phone customer Language Configuration

To better satisfy the user's local language configuration and add user-defined functions, the current version has supported the customer language feature, user can modify or add the language.

Format:

It should be noted that the file is a txt format file.

The inner separator is the tab key, not the space key. Example: tab is between S_PLACED_CALLS and Chinese_simplified0

Only be one translation in a row.

Translation Source Country Name Translation Value

Example:

```
S_PLACED_CALLS	French	AppelsAAA passés
S_PLACED_CALLS	Chinese_simplified	呼叫
S_PLACED_CALLS	English	Place Call
S_PLACED_CALLS	Custom	Call
```

Description:

S_PLACED_CALLS: This is the translation source, which corresponds to the id of the phone in it.

French/Chinese_simplified: This is the language option identifier, which identifies the type of language that needs to be changed. In the example, four languages were changed.

AppelsAAA passes / Place call: This is the last character you want to translate. The spacing between characters in this option is space, not tab.

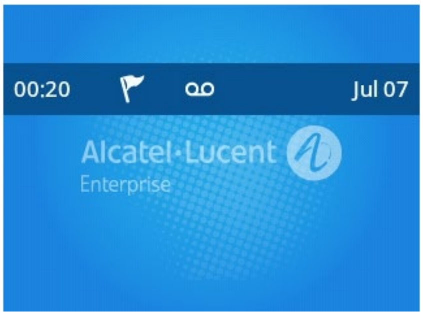
The following table lists the parameters you can use to configure the phone.

Parameter	**SettingCustomLanguageUploadUrl**	**config.xml**
Description	It configures the URL of custom language file.	
Permitted Values	URL within 512 characters **Note:** It works only if "**SettingLanguage**" is set to 99.	
Default	BLANK	

11.2 Screen Saver

The screen saver will automatically start when the SIP deskphone 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 SIP DeskPhones:



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

Parameter	**SettingScreensaverEnable**	**config.xml**
Description	It enables or disables screen saver	
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	Settings → Display → Timeout	
Phone UI	Menu → Basic Setting → Display → Screen Saver → Wait Time	

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
H3G/H6/M3s/M5s/M7s/M7s Pro/M8	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	[0,9]	
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 SIP deskphone 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.

11.4.1 Supported Backlight LED Options

The following table lists available options to configure the digital keys LED.

Phone Model	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 digital keys LED.

Parameter	**SettingInactiveLedLevel**	**config.xml**
Description	It configures the intensity of the LED backlight when the phone is inactive.	
Permitted Values	0 – Disable 1 - Enable	
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 – Disable 1 - Enable	
Default	1	
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 SIP deskphone 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 Timeout	

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 enables or disables ECO mode.	
Permitted Values	false – Disable true - Enable	
Default	false	
Web UI	Settings → Display → LED → 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 → LED → 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 → LED → 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 → LED → Sunday	
Parameter	**SettingEcoOfficeHourSunEndTime**	**config.xml**
Description	It configures the end time of Sunday.	
Permitted Values	[0,23]	
Default	9	
Web UI	Settings → Display → LED → Sunday	
Parameter	**SettingEcoOfficeHourMonStartTime**	**config.xml**
Description	It configures the start time of Monday.	
Permitted Values	[0,23]	
Default	9	
Web UI	Settings → Display → LED → Monday	
Parameter	**SettingEcoOfficeHourMonEndTime**	**config.xml**
Description	It configures the end time of Monday.	
Permitted Values	[0,23]	
Default	17	
Web UI	Settings → Display → LED → Monday	
Parameter	**SettingEcoOfficeHourTuesStartTime**	**config.xml**

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

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

11.6 Time and Date

The ALE SIP DeskPhones 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	-11:00 to +14:00 For available time zones, refer to Time Zone.	
Default	0	
Web UI	Settings → Time & Date → Time Zone	

11.6.2 NTP Settings and SIP Signaling Sync

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.

In addition to NTP synchronization time, ALE SIP DeskPhones also support SIP signaling time synchronization. The phone used the time in SIP signaling as the time to be synchronized through the 200 OK carried by the corresponding date header field returned by the server during registration.

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

Parameter	SettingTimeMethod	config.xml
Description	Configure time synchronization through the NTP server or SIP signaling or manually set the time.	
Permitted Values	0 - SNTP 1 - SIP Server 2 - Manual	
Default	0	
Web UI	Settings → Time & Date →Time Method	
Phone UI	Menu → Basic Setting → Time & Date → General	
Parameter	SettingSntpServer	config.xml
Description	It configures the IP address or the domain name of the NTP server. The SIP deskphone 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	
Phone UI	Menu → Basic Setting → Time & Date → General SNTP Settings	
Parameter	SettingSntpServer2	config.xml

Description	It configures the IP address or the domain name of the NTP server2. The SIP deskphone 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	
Phone UI	Menu → Basic Setting → Time & Date → General SNTP Settings	
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	[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 SIP deskphone 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 - Disable 1 - Enable 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.	
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.	
Permitted Values	week - By week date - By date	
Default	week	
Web UI	Setting → Time & Date → DST Type	
Parameter	**SettingDstStartMonth**	**config.xml**
Description	It configures the Daylight-Saving Time (DST) start month. **Note:** It works only if "**SettingDstEnable**" is set to 1.	
Permitted Values	Jan - January Feb - February Mar - March Apr - April May - May Jun - June Jul - July Aug - August Sep - September Oct - October Nov - November Dec - December	
Default	Jan	
Web UI	Setting → Time & Date → DST Start Date → Month	
Parameter	**SettingDstEndMonth**	**config.xml**
Description	It configures the Daylight-Saving Time (DST) end month. **Note:** It works only if "**SettingDstEnable**" is set to 1.	
Permitted Values	Jan - January Feb - February Mar - March Apr - April May - May Jun - June Jul - July Aug - August Sep - September Oct - October	

	Nov - November Dec - December	
Default	Dec	
Web UI	Setting → Time & Date → DST End Date → Month	
Parameter	**SettingDstStartDate**	**config.xml**
Description	It configures the Daylight-Saving Time (DST) start date. **Note:** It works only if “**SettingDstEnable**” is set to 1 and “**SettingDstType**” is set to date.	
Permitted Values	[1,31]	
Default	1	
Web UI	Setting → Time & Date → DST Start Date → 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 and “**SettingDstType**” is set to date.	
Permitted Values	[1,31]	
Default	30	
Web UI	Setting → Time & Date → DST End Date → 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 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 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	**SettingDstStartWeekDay**	**config.xml**
Description	It configures the Daylight-Saving Time (DST) start weekday. **Note:** It works only if "**SettingDstEnable**" is set to 1 and"**SettingDstType**" is set to week.	
Permitted Values	Sun - Sunday Mon - Monday Tue - Tuesday Wed - Wednesday Thu – Thursday Fri - Friday Sat – Saturday	
Default	Sun	
Web UI	Setting → Time & Date → DST Start Date → Week	
Parameter	**SettingDstEndWeekDay**	**config.xml**
Description	It configures the Daylight-Saving Time (DST) end weekday. **Note:** It works only if "**SettingDstEnable**" is set to 1 and"**SettingDstType**" is set to week.	
Permitted Values	Sun - Sunday Mon - Monday Tue - Tuesday Wed - Wednesday Thu – Thursday Fri - Friday Sat – Saturday	
Default	Sun	
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 1.	
Permitted Values	[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.	
Permitted Values	[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.	
Permitted Values	[-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.

The following table lists the parameter you can use to configure time and date manually.

Parameter	**SettingTimeMethod**	**config.xml**
Description	Configure time synchronization through the NTP server or SIP signaling or manually set the time.	
Permitted Values	0 - SNTP 1 - SIP Server 2 - Manual	
Default	0	
Web UI	Settings → Time & Date →Time Method	
Phone UI	Menu → Basic Setting → Time & Date → General	

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 the 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, 1:00 PM displays as 13:00).	
Default	0	
Web UI	Settings → Time & Date → Time Format	
Phone UI	Menu → Basic Setting → Time & Date → Time & Date Format → Time	
Parameter	**SettingDateFormat**	**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 & Date → Time & Date Format → Date	

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 - disable. 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 → Key as Send
Phone UI	Menu → Features → Key as Send

11.8 Bluetooth

The ALE Myriad Series M7s Pro and M8 deskphones support built-in Bluetooth. You can pair and connect a Bluetooth Headset or Bluetooth-enabled mobile phone with the SIP deskphone. After connecting the Bluetooth-Enabled mobile phone, you can choose to synchronize the mobile contacts to the SIP deskphone.

You can activate or deactivate the Bluetooth mode and personalize the Bluetooth device name for the SIP deskphone. 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 SIP deskphone.

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

Parameter	**SettingBluetoothDeviceName**	config.xml
Description	It configures the Bluetooth device name.	
Permitted Values	String within 64 characters	
Default	For M7s Pro: M7s Pro DeskPhone For M8: 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.	
Permitted Values	0 - no auto-connect 1 - low sensitive auto-connect	
Default	1	
Parameter	**SettingBluetoothEnable**	config.xml
Description	It enables or disables the Bluetooth feature.	
Permitted Values	false - Disable true - Enable	
Default	true	
Phone UI	Menu → Basic Setting → Bluetooth → Bluetooth Enable	

11.9 Handset/Headset/Speakerphone Mode

The ALE SIP DeskPhones 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 audio ring device.	
Permitted Values	0 - handsfree 1 - headset 2 - handsfree and headset	
Default	0	
Web UI	Settings → Ringing → Ring Device	
Phone UI	Menu → Basic Setting → Sound → Ringing → Ringing Device	
Parameter	**FeatureHeadsetPriorEnable**	config.xml
Description	It configures to enable the headset prior function.	
Permitted Values	false – disable. The headset mode will be deactivated after the call, if you switch the headset mode to speakerphone/handset mode. true - Enable. The headset mode will not be deactivated after the call, even if you switch the headset mode to speakerphone/handset mode.	
Default	false	
Web UI	Features → General → Headset Prior	

11.10 Programmable Keys

The ALE SIP DeskPhones 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
H3G	8	N/A
H6	12	N/A
M3s	20	60 * 3
M5s	28	60 * 3
M7s	28	60 * 6
M7s Pro	28	60 * 6
M8	36	60 * 6

11.10.2 Supported Programmable Key Types

The supported key function types vary by programmable keys and EM keys.

ID	Programmable Key Types
0	Not Used
1	Speed Dial
2	BLF List
3	DND
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	Audio Hub
24	Private Hold
42	ACD
58	Hold
59	BLF
60	Account
61	USB Recording
62	Broadsoft Recording
63	Disposition Code
64	Emergency Escalation

65	Customer Originated 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
76	Network Call Log
77	Network Directory
78	Park Reminder
84	LDAP

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 softkey. For example, if the phone does not have a Do Not Disturb hard key, you can create a Do Not Disturb softkey. The programmable key takes effect only when the SIP deskphone is idle.

11.10.3.1 Programmable Keys Configuration

In R130 release, programmable keys layout of the ALE SIP DeskPhones is changed to tree arrangement.

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

Note: X can be 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.

Parameter	**ProgramKeyXType**	**config.xml**
Description	It configures key features for a specific programmable key.	
Permitted Values	0 - Not Used 1 - Speed Dial 2 - BLF List 3 - DND 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 – Audio Hub 24 - Private Hold 42 - ACD 58 – Hold 59 - BLF 60 - Account 61 - Usb Recording 62 - Broadsoft Recording 63 - Disposition Code 64 - Emergency Escalation 65 - Customer Originated 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 76 - Network Call Log 77 - Network Directory 78 - Park Reminder 83 - Enterprise Directory

	84 - LDAP	
Default	0	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable Keys	
Parameter	**ProgramKeyXAccount**	**config.xml**
Description	It configures the desired account to apply the programmable key feature.	
Permitted Values	N - Account N (N is 1-3 for H3G,1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8)	
Default	1	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable Keys	
Parameter	**ProgramKeyXLabel**	**config.xml**
Description	It configures the label displayed on the phone screen for a specific programmable key.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable Keys	
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 “**ProgramKeyXType**” is set to 1, 59, 5, 14, 13, 15, 16,17,19,21,22 or 73.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable Keys	
Parameter	**ProgramKeyXExtension**	**config.xml**
Description	For BLF feature: It configures the pickup code. For multicast paging:	

	It configures the channel of the multicast paging group. **Note:** It is only applicable when "**ProgramKeyXType**" is set to 59 or 66.
Permitted Values	String within 64 characters
Default	Blank
Web UI	Phone Keys → Program Key
Phone UI	Menu → Features → Programmable Keys

11.10.3.2 Dynamic Keys Configuration

This feature supports configuring the programming hard keys and softkeys 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 following table lists the parameters you can use to configure dynamic keys.

Parameter	**DynamicSoftKeyXType**	**config.xml**
Description	It configures the key type for a specific programmable key. **Note:** X can be 1- 4 for H3G/H6/M3s/M5s/M7s/M7s Pro, and 1-5 for M8.	
Permitted Values	0 - Empty 1 - Speed Dial 3 - DND 4 - Directory 7 - Forward 10 - Headset 11 - Hot Desking 12 - Phone Lock 13 - Prefix 18 - Recall 19 - XML Browser 21 - Intercom 23 – Audio Hub 66 - Paging 67 - Paging List 71 - Logout 72 - Network Call List 73 - Network Contacts 74 - Network Message List 75 - Call Waiting	

	76 - Network Call Log 77 - Network Directory 78 - Park Reminder 83 - Enterprise Directory 84 - LDAP 101 - Menu 102 - History 103 - Status 104 - Login	
Default	101	
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 H3G/H6/M3s/M5s/M7s/M7s Pro, and 1-5 for M8.	
Permitted Values	N - Account N (N is 1-3 for H3G,1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 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 H3G/H6/M3s/M5s/M7s/M7s Pro, and 1-5 for M8.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Phone Keys → Dynamic key	
Parameter	**DynamicSoftKeyXValue**	**config.xml**
Description	It configures the value for some programmable key features. **Note:** X can be 1- 4 for H3G/H6/M3s/M5s/M7s/M7s Pro, and 1-5 for M8.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Phone Keys → Dynamic key	
Parameter	**DynamicSoftKeyXExtension**	**config.xml**
Description	For multicast paging: It configures the channel of the multicast paging group.	

	Note: 1. X can be 1- 4 for H3G/H6/M3s/M5s/M7s/M7s Pro, and 1-5 for M8. 2. It is only applicable when "**DynamicSoftKeyXType**" is set to 66.	
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 70 - Push To Talk 71 - Logout 72 - Network Call List 73 - Network Contacts 74 - Network Message List 75 - Call Waiting 76 - Network Call Log 77 - Network Directory 78 - Park Reminder 83 - Enterprise Directory 84 - LDAP 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	N - Account N (N is 1-3 for H3G,1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 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***Value	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 following tables list dynamic keys for each phone model.

Key Name	H3G/H6	M3s/M5s/M7s/M7s Pro	M8
Softkey1	√	√	√
Softkey2	√	√	√
Softkey3	√	√	√
Softkey4	√	√	√
Softkey5	X	X	√
Redial	√	√	√

Release	√	√	√
Hold	√	√	√
Mute	√	√	√
Transfer	√	√	√
Message	√	√	√
Conference	√	√	X
Handsfree	√	√	√
Headset	X	X	√
Up	√	√	√
Down	√	√	√
Left	√	√	√
Right	√	√	√
OK	√	√	√
Cancel	√	√	√
VolUp	√	√	X
VolDown	√	√	X

11.10.3.3 EM Keys Configuration

The ALE Smart Expansion Module EM200 is a deskphone accessory that extends the capabilities of Myriad deskphones.

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

Parameter	**AomXProgKeyYType**	**config.xml**
Description	It configures the key type for a specific EM key. **Note:** X can be 1-3, Y can be 1-200.	
Permitted Values	0 - Not Used 1 - Speed Dial 2 - BLF List 3 - DND 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 – Audio Hub 24 - Private Hold 42 - ACD 58 – Hold 59 - BLF 60 - Account 61 - Usb Recording 62 - Broadsoft Recording 63 - Disposition Code 64 - Emergency Escalation 65 - Customer Originated 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 76 - Network Call Log 77 - Network Directory 78 - Park Reminder 83 - Enterprise Directory 84 - LDAP
Default	0

Web UI	Phone Keys → Program Key → EMx	
Parameter	**AomXProgKeyYAccount**	**config.xml**
Description	It configures the desired account to apply the EM key feature. **Note:** X can be 1-3, Y can be 1-200.	
Permitted Values	N - Account N (N is 1-3 for H3G,1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8)	
Default	1	
Web UI	Phone Keys → Program Key → EMx	
Parameter	**AomXProgKeyYLabel**	**config.xml**
Description	It configures the label displayed on the phone screen for a specific EM key. **Note:** X can be 1-3, Y can be 1-200.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Phone Keys → Program Keys → EMx	
Parameter	**AomXProgKeyYValue**	**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. **Note:** X can be 1-3, Y can be 1-200.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Phone Keys → Program Keys → EMx	
Parameter	**AomXProgKeyYExtension**	**config.xml**
Description	For BLF feature: It configures the pickup code. For multicast paging: It configures the channel of the multicast paging group. **Note:** X can be 1-3, Y can be 1-200.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Phone Keys → Program Key → EMx	

11.11 Wallpaper

Wallpaper is a picture which is used as the background of the phone. The phone comes with a default picture. You can change it to a built-in picture or custom wallpaper from personal pictures. The wallpaper is only applicable to H6/M5s/M7s/M7s Pro/M8 deskphones.

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	
Parameter	**SettingWallpaperDisplay**	**config.xml**
Description	It configures the 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:

Phone Model	Format	Resolution	Single File Size
H6/M5s/M7s/M7s Pro	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.

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

Note: X means account ID. It can be number 1-3 for H3G, 1-4 for H6,1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.

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	
Parameter	**SIPPaiRefreshNum**	**config.xml**
Description	It configures multiple PAI headers that are received, select the number of PAI packets to display.	
Permitted Values	1 - Use the first PAI header to display. 2 - Use the second PAI header to display. 3 - Use the third PAI header to display. **Note:** If the configured value is greater than the actual number of PAI headers received, the first headers will be use.	
Default	1	
Parameter	**FeatureDiversionInfoEnable**	**config.xml**
Description	It enables or disables to display an incoming call with the Diversion header information. This scenario is mostly when the number is forwarded.	
Permitted Values	false - Disable true - Enable	
Default	true	
Parameter	**AccountXCallerSource**	**config.xml**
Description	It configures the identity of the caller.	

	Note: X means account ID. It can be number 1-3 for H3G, 1-4 for H6,1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.	
Permitted Values	0 - PAI 1 - RPID 2 - From/To **Note:** The order of values represents priority, and all three values must be configured.	
Default	0;1;2	
Parameter	**AccountXCalleeSource**	**config.xml**
Description	It configures the identity of the callee. **Note:** X means account ID. It can be number 1-3 for H3G, 1-4 for H6,1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.	
Permitted Values	0 - PAI 1 - RPID 2 - From/To **Note:** The order of values represents priority, and all three values must be configured.	
Default	0;1;2	

11.13 Notification Pop-ups

This feature is used to control the popup of a new voicemail and a missed call.

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

Parameter	**FeatureVmPopupEnable**	**config.xml**
Description	It enables or disables the popup of new voicemail.	
Permitted Values	false - Disable true - Enable	
Default	true	
Parameter	**FeatureMissedCallPopupEnable**	**config.xml**
Description	It enables or disables the popup of missed call.	
Permitted Values	false - Disable true - Enable	
Default	true	

11.14 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.

Parameter	**DirectorySearchInDialingList**	**config.xml**
Description	It configures the range and priority of the search to match the entries by the dial screen.	
Permitted Values	0 - Local Directory 1 - History 2 - Remote Phone Book 3 - LDAP 4 - External Directory	
Default	0;1	

11.15 Softkey Layout

Softkey layout is used to customize the softkeys at the bottom of the phone screen for best meeting user's requirements. In addition to specifying which softkeys are to be displayed, you can also determine their display order. The configurations for softkey layout are based on call states.

11.15.1 Supported Call States and Softkeys

The following table lists softkeys available for SIP deskphones in different call states.

State	**Default Value**		**Allowed Value**
	H3G/H6/M3s/M5s/M7s/M7s Pro	**M8**	
Dial	Call Backspace IME Cancel	Call Directory Backspace IME Cancel	Call Backspace IME 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 Silent Forward Reject	Take Empty Silent Forward Reject	Take Silent Forward Reject Empty
New Callin	Empty Take	Take Empty	Take Reject

	Reject End	Empty Reject End	End Empty
Conference New Callin	Empty Take Reject End	Take Empty Empty Reject End	Take Reject End Empty
Conversatio n	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 Empty

		End	
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

11.15.2 Softkey 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 softkey that you want to enable/disable, move the string from the disabled/enabled softkey list to enabled/disabled softkey list in the file or replace the Empty in the enabled softkey list.

  The following shows a portion of the softkey layout file “CallIn.xml”:

```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.

11.15.3 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	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.	
Permitted Values	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 - Listening	
Default	Dial;DialEmpty;TransDial;TransDialEmpty;ConfDial;ConfDialEmpty;Calling;Transferring;CallFailed;Ringing;NewCallin;ConfNewCallin;Conversation;Hold;Held;Conf;ConfHold;BeTrans;Paging;Listenning	
Web UI	Settings → Softkey Layout	
Parameter	**SettingCustomSoftkeyDynamicEnable**	**config.xml**
Description	It enables or disables the phone to display the softkeys relevant to the features (call center, centralized call recording, and executive-assistant). **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true.	
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.	
Permitted Values	URL within 512 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.	
Permitted Values	URL within 512 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.	
Permitted Values	URL within 512 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.	
Permitted Values	URL within 512 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.	
Permitted Values	URL within 512 characters	
Default	Blank	
Parameter	**SettingCustomSoftkeyDial**	**config.xml**
Description	It configures the custom softkey layout of Dial state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true.	
Permitted Values	Call Backspace IME Cancel Directory History Empty	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: Call;Backspace;IME;Cancel M8: Call;Directory;Backspace;IME;Cancel	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyDialEmpty**	**config.xml**

Description	It configures the custom softkey layout of Dial Empty state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true.	
Permitted Values	Directory History IME Cancel Empty	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: Directory;Empty;IME;Cancel M8: Directory;Emoty;Empty;IME;Cancel	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyTransDial**	**config.xml**
Description	It configures the custom softkey layout of Transfer Dial state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true.	
Permitted Values	Blind Transfer Call Backspace Cancel IME Directory History Empty	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: 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 the custom softkey layout of Transfer Dial Empty state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true.	
Permitted Values	Directory History IME Cancel Empty	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: Directory;Empty;IME;Cancel M8: Directory;Empty;Empty;IME;Cancel	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyConfDial**	**config.xml**

Description	It configures the custom softkey layout of Conference Dial state. **Note:** It works only if “**SettingCustomSoftkeyEnable**” is set to true.	
Permitted Values	Call Backspace IME Cancel Directory History Empty	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: Call;Backspace;IME;Cancel M8: Call;Directory;Backspace;IME;Cancel	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyConfDialEmpty**	**config.xml**
Description	It configures the custom softkey layout of Conference Dial Empty state. **Note:** It works only if “**SettingCustomSoftkeyEnable**” is set to true.	
Permitted Values	Directory History IME Cancel Empty	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: Directory;Empty;IME;Cancel M8: Directory;Empty;Empty;IME;Cancel	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyCalling**	**config.xml**
Description	It configures the custom softkey layout of Calling state. **Note:** It works only if “**SettingCustomSoftkeyEnable**” is set to true.	
Permitted Values	End Empty	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: Empty;Empty;Empty;End M8: Empty;Empty;Empty;Empty;End	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyTransferring**	**config.xml**
Description	It configures the custom softkey layout of Transferring state. **Note:** It works only if “**SettingCustomSoftkeyEnable**” is set to true.	

Permitted Values	Transfer End Empty	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: Transfer;Empty;Empty;End M8: Transfer;Empty; Empty;Empty;End	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyCallFailed**	**config.xml**
Description	It configures the custom softkey layout of Call Failed state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true.	
Permitted Values	End New Call Empty	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: 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 the custom softkey layout of Ringing state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true.	
Permitted Values	Take Slient Forward Reject Empty	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: Take;Silent;Forward;Reject M8: Take;Empty;Silent;Forward;Reject	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyNewCallin**	**config.xml**
Description	It configures the custom softkey layout of New Callin state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true.	
Permitted Values	Take Reject End Empty	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: Empty;Take;Reject;End M8: Take;Empty;Empty;Reject;End	

Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyConfNewCallin**	**config.xml**
Description	It configures the custom softkey layout of Conference New Callin state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true.	
Permitted Values	Take Reject End Empty	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: Empty;Take;Reject;End M8: Take;Empty;Empty;Reject;End	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyConversation**	**config.xml**
Description	It configures the custom softkey layout of Conversation state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true.	
Permitted Values	Hold Transfer Conference End Swap Empty	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: Hold;Transfer;Conference;End M8: Hold;Empty;Transfer;Conference;End	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyHold**	**config.xml**
Description	It configures the custom softkey layout of Hold state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true.	
Permitted Values	New Call Transfer Resume End Empty	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: 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 the custom softkey layout of Held state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true.	
Permitted Values	End Empty	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: Empty;Empty;Empty;End M8: Empty;Empty;Empty;Empty;End	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyConf**	**config.xml**
Description	It configures the custom softkey layout of Conference state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true.	
Permitted Values	Conference Manage Hold Split End Transfer Empty	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: 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 the custom softkey layout of Conference Hold state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true.	
Permitted Values	New Call Resume Split End Empty	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: 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 the custom softkey layout of Be Transferred state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true.	

Permitted Values	End Empty	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: Empty;Empty;Empty;End M8: Empty;Empty;Empty;Empty;End	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyPaging**	**config.xml**
Description	It configures the custom softkey layout of Multicast Paging state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true.	
Permitted Values	Hold End Empty	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: Hold;Empty;Empty;End M8: Hold;Empty;Empty;Empty;End	
Web UI	Settings → Softkey Layout → Call States	
Parameter	**SettingCustomSoftkeyListening**	**config.xml**
Description	It configures the custom softkey layout of Multicast Paging state. **Note:** It works only if "**SettingCustomSoftkeyEnable**" is set to true.	
Permitted Values	Hold End Empty	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: Hold;Empty;Empty;End M8: Hold;Empty;Empty;Empty;End	
Web UI	Settings → Softkey Layout → Call States	

11.15.4 Example: Setting the Softkeys Layout in Talking State

The following example shows the configuration for setting the softkey 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 softkeys during a call.

12. Advanced Features

12.1 Audio Hub

The ALE Myriad Series M3s/M5s/M7s/M7s Pro/M8 DeskPhones can act as an external audio device of PC or mobile. When a PC or mobile 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.

12.1.1 Audio Hub Programmable Key Configuration Parameters

The following table lists the parameters you can use to configure the Audio Hub programmable key.

Parameter	ProgramKeyXType	config.xml
Description	It configures the programmable key type. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	23 Audio Hub 23 - Audio Hub	
Default	0	
Web UI	Phone Keys → Program key	
Phone UI	Menu → Features → Programmable keys	

12.1.2 Audio Hub via BT Programmable Key Configuration Parameters

The following table lists the parameters you can use to configure the Mobile Account programmable key.

Parameter	ProgramKeyXType	config.xml
Description	It configures the programmable key type. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	68 - Mobile Account	
Default	0	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	

12.2 X-party Conference

The ALE H3G/H6/M3s/M5s/M7s/M7s Pro DeskPhones have the capability to launch a 6-party conference by local.

The M8 phone has the capability to launch a 12-party conference by local.

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.	
Permitted Values	false - Disable true - Enable	
Default	true	
Web UI	Features → Sip → Local Conference Enable	
Parameter	**SIPMaxCall**	**config.xml**
Description	It configures the max number of calls the phone can support.	
Permitted Values	H3G/H6/M3s/M5s/M7s/M7s Pro: 1-5 M8: 1-11	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: 5 M8: 11	
Web UI	Features → Sip → SIP Max Call	
Parameter	**SIPConfPartyMax**	**config.xml**
Description	It defines the max party capacity of a phone conference.	
Permitted Values	H3G/H6/M3s/M5s/M7s/M7s Pro: 3-6 M8: 3-12	
Default	H3G/H6/M3s/M5s/M7s/M7s Pro: 6 M8: 12	
Web UI	Features → Sip →Local Conference Max Party	

12.3 Hot Desking

The ALE SIP DeskPhones 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 to a shared phone by hot desking feature. Hot desking allows the user to clear pre-registration configurations of all accounts on the SIP deskphone and then login to their own user account.

On the shared phone, you first need to assign a hot desking key.

The following table lists the parameters you can use to configure hot desking key.

Parameter	**ProgramKeyXType**	**config.xml**
Description	It configures the programmable key type. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	

Permitted Values	11 - Hot Desking
Default	0
Web UI	Phone Keys → Program Key
Phone UI	Menu → Features → Programmable keys

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 Outgoing Intercom Configuration Parameters

The following table lists the parameters you can use to configure intercom for outgoing call.

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	
Web UI	Features → Intercom → Outgoing Intercom Method	
Parameter	**ProgramKeyXType**	**config.xml**
Description	It configures the programmable key type. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	21 - Intercom	
Default	0	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	
Parameter	**ProgramKeyXAccount**	**config.xml**
Description	It configures the account index of the program key. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	N - Account N (N is 1-3 for H3G,1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8)	
Default	1	

Web UI	Phone Keys → Program Key
Phone UI	Menu → Features → Programmable keys

12.4.2 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. It can be number 1-3 for H3G, 1-4 for H6 ,1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.

Parameter	**AccountXIntercomEnable**	**config.xml**
Description	It enables or disables to auto answer an incoming call if requested by SIPUA layer.	
Permitted Values	false - Disable true - Enable	
Default	true	
Web UI	Features → Intercom → Enable Intercom	
Phone UI	Menu → Feature → Intercom → AccountX → Allow	
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	
Web UI	Features → Intercom → Intercom Mute	
Phone UI	Menu → Features → Intercom → AccountX → 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	
Web UI	Features → Intercom → Intercom Tone	
Phone UI	Menu → Features → Intercom → AccountX → 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
Web UI	Features → Intercom → Intercom Barge
Phone UI	Menu → Features → Intercom → AccountX → Barge

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: The 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.

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

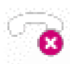
Note: X means account ID. It can be number 1-3 for H3G,1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.

Parameter	**AccountXVmNumber**	**config.xml**
Description	It configures voicemail number.	
Permitted Values	String 64 characters	
Default	Blank	
Web UI	Account → Advanced → Voice Mail Number	
Phone UI	Menu → Message → Voicemail → Set Voicemail Number	
Parameter	**AccountXMwiUri**	**config.xml**
Description	It configures message waiting indication server address for account.	
Permitted Values	String 64 characters	
Default	Blank	
Web UI	Account → Advanced → Message Waiting Indication URI	

12.7 Busy Lamp Field

The Busy Lamp Field (BLF) feature enables the phone to monitor specific remote lines for state changes on the phone.

The following table shows the LED/icons indicator associated with the line you are monitoring.

Notify	Icon	LED State	Description
Terminated		Solid blue	The monitoring account is idle. Note: If the notify message does not carry a clear status, it is regarded as idle.
Early/proceeding		Fast-flashing red	The monitoring account is ringing.
Confirmed		Solid red	The monitoring account is in call talking.
Confirmed-hold		Slow-flashing red	The monitoring account is on hold.
Parked		Slow-flashing red	The monitoring account is on parked.
Offline/Unregister		Off	The monitoring account is offline or not registered. Not subscribed.
Unknow		Off	The monitoring account is unknown, that is, the Notify message carries other states than the preceding ones. or only receive 200OK, but no notify.

12.7.1 BLF Key Configuration Parameters

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

Parameter	ProgramKeyXType	config.xml
Description	It configures the programmable key type. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	59 - BLF	
Default	0	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	
Parameter	**ProgramKeyXAccount**	**config.xml**
Description	It configures the account index of the program key. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	

Permitted Values	N - Account N (N is 1-3 for H3G,1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8)	
Default	1	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	
Parameter	**ProgramKeyXLabel**	**config.xml**
Description	It configures the programmable key label. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	String 64 characters	
Default	Blank	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	
Parameter	**ProgramKeyXValue**	**config.xml**
Description	It configures the program key value. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	String 64 characters	
Default	Blank	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	
Parameter	**ProgramKeyXExtension**	**config.xml**
Description	It configures the pickup code. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	String 64 characters	
Default	Blank	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	

12.8 Call Pickup

You can use call pickup to answer someone's incoming call on your phone using a pickup code.

The ALE SIP DeskPhones 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 Key Configuration Parameters

The following table lists the parameters you can use to configure the direct pickup key.

Parameter	**ProgramKeyXType**	**config.xml**
Description	It configures the programmable key type. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	15 - Direct Pickup	
Default	0	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	
Parameter	**ProgramKeyXAccount**	**config.xml**
Description	It configures the account index of the program key. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	N - Account N (N is 1-3 for H3G,1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8)	
Default	1	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	
Parameter	**ProgramKeyXLabel**	**config.xml**
Description	It configures the programmable key label. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	String 64 characters	
Default	Blank	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	
Parameter	**ProgramKeyXValue**	**config.xml**

Description	It configures the program key value **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.
Permitted Values	String 64 characters
Default	Blank
Web UI	Phone Keys → Program Key
Phone UI	Menu → Features → Programmable keys

12.8.2 Group Pickup Configuration Parameters

The following table lists the parameters you can use to configure the group pickup key.

Parameter	**ProgramKeyXType**	**config.xml**
Description	It configures the programmable key type. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	16 - Group Pickup	
Default	0	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	
Parameter	**ProgramKeyXAccount**	**config.xml**
Description	It configures the account index of the program key. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	N - Account N (N is 1-3 for H3G,1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8)	
Default	1	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	
Parameter	**ProgramKeyXLabel**	**config.xml**
Description	It configures the programmable key label. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	String 64 characters	

Default	Blank	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	
Parameter	**ProgramKeyXValue**	**config.xml**
Description	It configures the program key value **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	String 64 characters	
Default	Blank	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	

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 Configuration Parameters

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

Parameter	**ProgramKeyXType**	**config.xml**
Description	It configures the programmable key type. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	17 - Call Park	
Default	0	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	
Parameter	**ProgramKeyXAccount**	**config.xml**
Description	It configures the account index of the program key. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	N - Account N (N is 1-3 for H3G,1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8)	
Default	1	

Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	
Parameter	**ProgramKeyXLabel**	**config.xml**
Description	It configures the programmable key label. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	String 64 characters	
Default	Blank	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	
Parameter	**ProgramKeyXValue**	**config.xml**
Description	It configures the program key number. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	String 64 characters	
Default	Blank	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	
Parameter	**FeatureCallParkMode**	**config.xml**
Description	It configures the call park mode.	
Permitted Values	0 - FAC 1 - Transfer	
Default	0	
Web UI	Features → Call Park → Call Park Mode	
Parameter	**FeatureCallParkEnable**	**config.xml**
Description	It enables or disables the call park feature.	
Permitted Values	false - Disable true - Enable	
Default	false	
Web UI	Features → Call Park → Call Park	
Parameter	**FeatureCallParkParkCode**	**config.xml**

Description	It configures the call park code for FAC call park mode or configures shared parking lot for Transfer call park mode.	
Permitted Values	String within 64 characters.	
Default	Blank	
Web UI	Features → Call Park → Call Park Code	
Parameter	**FeatureCallParkRetrieveCode**	**config.xml**
Description	It configures the park retrieve code for FAC call park mode or configures retrieve parking lot for Transfer call park mode.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Features → Call Park → Retrieve Park Code	
Parameter	**FeatureCallParkDirectCallEnable**	**config.xml**
Description	It enables or disables the phone to dial out the call park code/park retrieve code directly when pressing the Park/Retrieve softkey. **Note:** It works only if "**FeatureCallParkMode**" is set to 0 (FAC) and you have configured the call park code/park retrieve code.	
Permitted Values	false - Disable true - Enable	
Default	true	

12.9.2 Retrieve Park key Configuration Parameters

The following table lists the parameters you can use to configure the retrieve park key.

Parameter	**ProgramKeyXType**	**config.xml**
Description	It configures the programmable key type. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	22 – Retrieve Park	
Default	0	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	
Parameter	**ProgramKeyXAccount**	**config.xml**

Description	It configures the account index of the program key. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	N - Account N (N is 1-3 for H3G,1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8)	
Default	1	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	
Parameter	**ProgramKeyXLabel**	**config.xml**
Description	It configures the programmable key label. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	String 64 characters	
Default	Blank	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	
Parameter	**ProgramKeyXValue**	**config.xml**
Description	It configures the program key number. **Note:** X can 1-8 for H3G, 1-12 for H6, 1-20 for M3s, 1-28 for M5s/M7s/M7s Pro, 1-36 for M8.	
Permitted Values	String 64 characters	
Default	Blank	
Web UI	Phone Keys → Program Key	
Phone UI	Menu → Features → Programmable keys	

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 can 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

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

Parameter	**AccountXSlaEnable**	**config.xml**
Description	It enables or disables the SLA function for account. **Note:** X can 1-3 for H3G,1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.	
Permitted Values	false - Disable true - Enable	
Default	false	
Web UI	Account → Advanced → SLA Enable	

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 the 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 → Call Completion	

12.12 Automatic Call Distribution (ACD)

ACD enables the use of SIP deskphones 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 softkeys. 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 SIP deskphone remains in the unavailable status until the agent manually changes the SIP deskphone status. You can configure how long the SIP deskphone 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.

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

Note: X means account ID. It can be number 1-3 for H3G,1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.

Parameter	**AccountXAcdEnable**	**config.xml**
Description	It enables or disables ACD feature.	
Permitted Values	false - Disable true - Enable	
Default	false	
Parameter	**FeatureAcdAutoAvailableEnable**	**config.xml**
Description	It enables or disables the SIP deskphone 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	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**	**config.xml**
Description	It configures the ACD reason code. **Note:** X can be 1-10	
Permitted Values	String within 64 characters	
Default	Blank	

Parameter	**FeatureAcdReasonNameX**	**config.xml**
Description	It configures the ACD reason name. **Note:** X can be 1-10.	
Permitted Values	String within 64 characters	
Default	Blank	
Parameter	**FeatureAcdSoftkeyEnable**	**config.xml**
Description	It enables or disables the phone to display ACD softkeys such as **Login** or **Logout** on the idle screen.	
Permitted Values	false - Disable true - Enable	
Default	false	

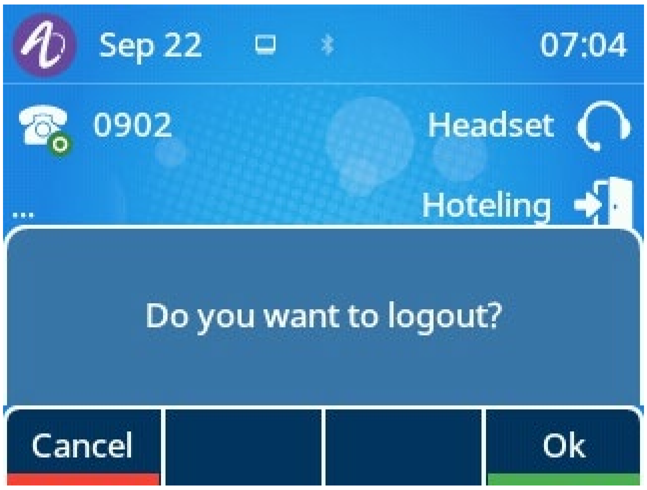
12.13 Broadsoft Hoteling

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 to the Broadsoft platform.

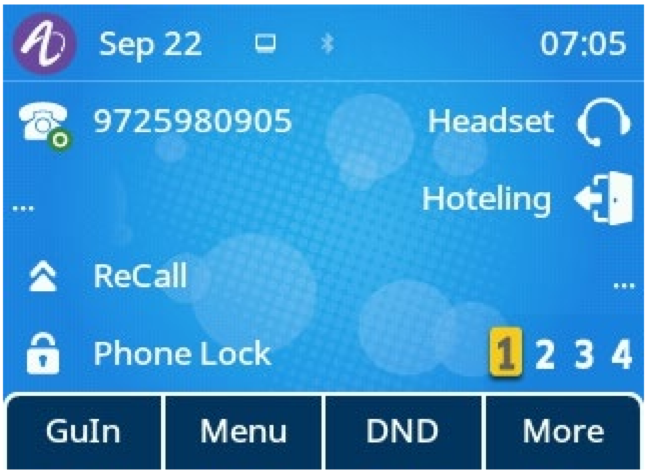
- If the hoteling feature is properly configured and the device is powered on, the device will send an initial subscription to get the hoteling status. If the phone is in guest in state, the receiving HotelingEvent NOTIFY will contain the Guest identity.

  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).

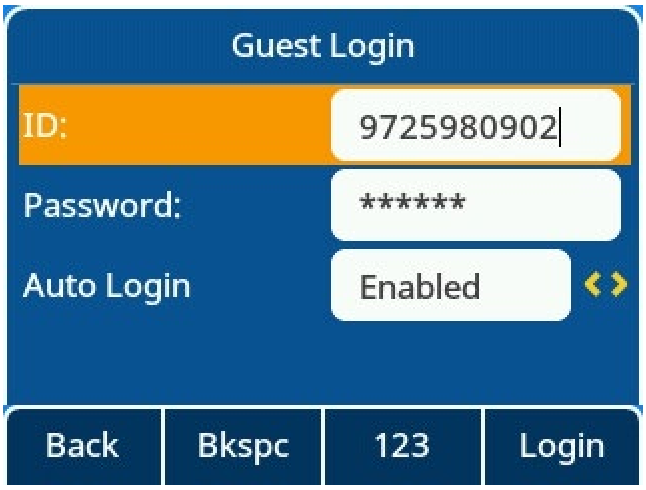
- When you guest out by pressing the menu "GuOut" or "Hoteling" programmable key, there will be a popup for confirmation.



- 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 programmable 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 1-3 for H3G,1-4 for H6, 1-8 for M3s/M5s/M7s/M7s Pro, 1-20 for M8.

Parameter	**AccountXHotelingEnable**	**config.xml**
Description	It enables or disables the hoteling feature. **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	String within 64 characters	
Default	Blank	
Parameter	**AccountXHotelingPwd**	**config.xml**
Description	It configures the password used to log into the guest. **Note:** It works only if "**AccountXServerType**" is set to 6 (Broadsoft).	
Permitted Values	String within 99 characters	
Default	Blank	
Parameter	**HotelingAutoLoginEnable**	**config.xml**
Description	It enables or disables hotel auto login. **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

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

Parameter	**DeviceSyslogRemoteEnable**	**config.xml**
Description	It enables or disables syslog.	
Permitted Values	false – disable true - Enable	
Default	false	
Web UI	Maintenance → Log Collection → Syslog enable	
Parameter	**DeviceSyslogRemoteServerAddr**	**config.xml**
Description	It configures the syslog server address.	
Permitted Values	String within 512 characters	
Default	Blank	
Web UI	Maintenance → Log Collection → Syslog server	
Parameter	**DeviceSyslogRemoteServerPort**	**config.xml**
Description	It configures the syslog server port.	
Permitted Values	[0-65535]	
Default	514	
Web UI	Maintenance → Log Collection → Syslog port	
Parameter	**DeviceSyslogRemoteServerProtocol**	**config.xml**
Description	It configures the syslog server protocol.	
Permitted Values	udp tcp	
Default	udp	

Web UI	Maintenance → Log Collection → Syslog protocol

13.1.2 Call Log File Backup

The phone can automatically upload call log files 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	**DeviceBackupUploadTime**	**config.xml**
Description	It configures the interval time (in seconds) of uploading a backup file.	
Permitted Values	[1, 86400]	
Default	3600	
Parameter	**DeviceBackupUrl**	**config.xml**
Description	It configures the URL which is used to upload and download the backup file.	
Permitted Values	String within 512 characters	
Default	Blank	
Parameter	**DeviceBackupUploadMethod**	**config.xml**
Description	It configures the way to upload files.	
Permitted Values	0 - PUT 1 - POST	
Default	0	
Parameter	**DeviceCallLogBackupEnable**	**config.xml**
Description	It configures whether to enable or disable call log backup feature.	
Permitted Values	false - Disable true - Enable	
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 SSIP deskphones support 6 levels for log recording, and more content 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 issues, debug level is recommended.

13.1.3.1 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 following table lists the parameters you can use to enable SSH.

Parameter	**DeviceSecuritySshEnable**	**config. xml**
Description	It enables or disables SSH connection for the phone.	
Permitted Values	false - Disable true - Enable	
Default	false	
Web UI	Maintenance → Security → SSH Activation	

- 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
```

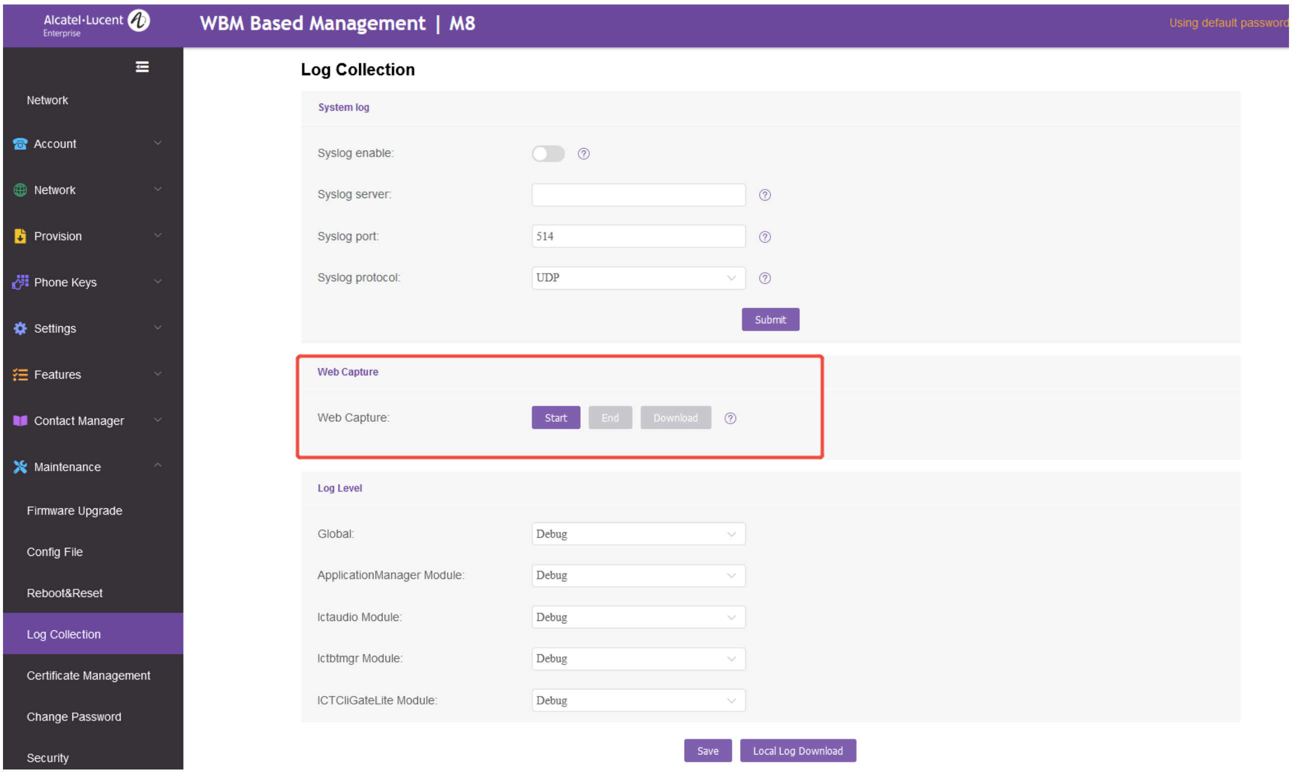
13.1.4 Web Capture

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".

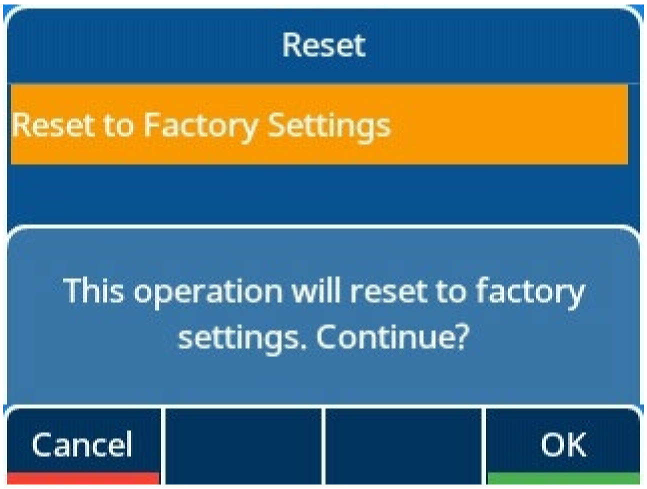
Note: All the configuration on the phone will be erased after resetting to factory settings.

Parameter	**Feature Reset By Long Press Enable**	**config. xml**
Description	It enables or disables the phone to reset to factory by long pressing Conference/Headset key.	
Permitted Values	false - Disable true - Enable	
Default	true	

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 the OK button to restore the phone to factory configuration.



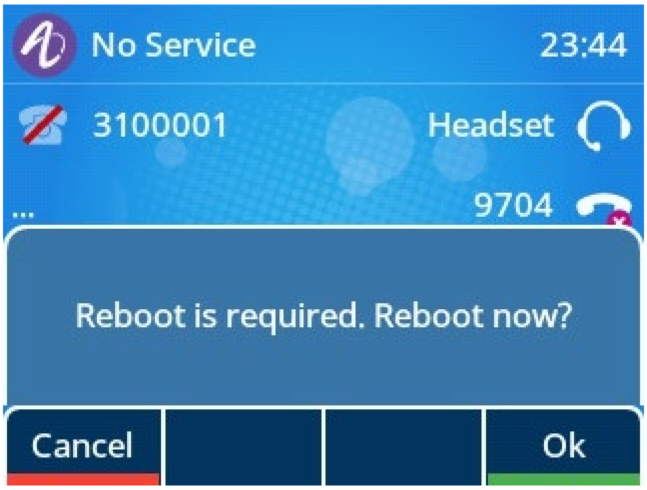
13.3 One Key Reboot

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.

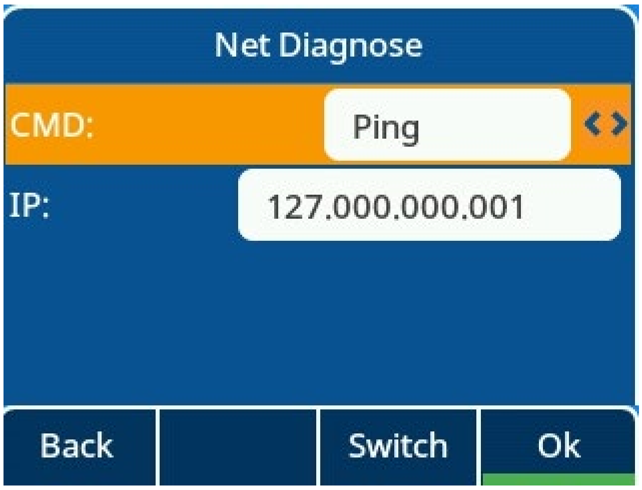
Cancel: By pressing “Cancel”, the deskphone will cancel the operation.

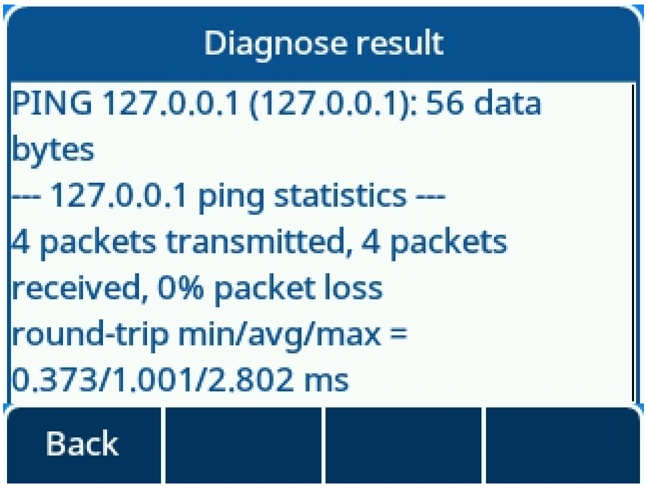


13.4 Network Diagnostics

You can use ping and traceroute diagnostics for troubleshooting network connectivity via phone user interface.

Go to the phone UI: Menu → Basic 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 parameters you can use to configure PC port mirror function.

Parameter	**DeviceNetworkSpanToPcType**	**config.xml**
Description	It enables or disables the SIP deskphone to span data packets received from the LAN port to the PC port.	
Permitted Values	0 - Idle 1 – LAN 2 - CPU	
Default	0	

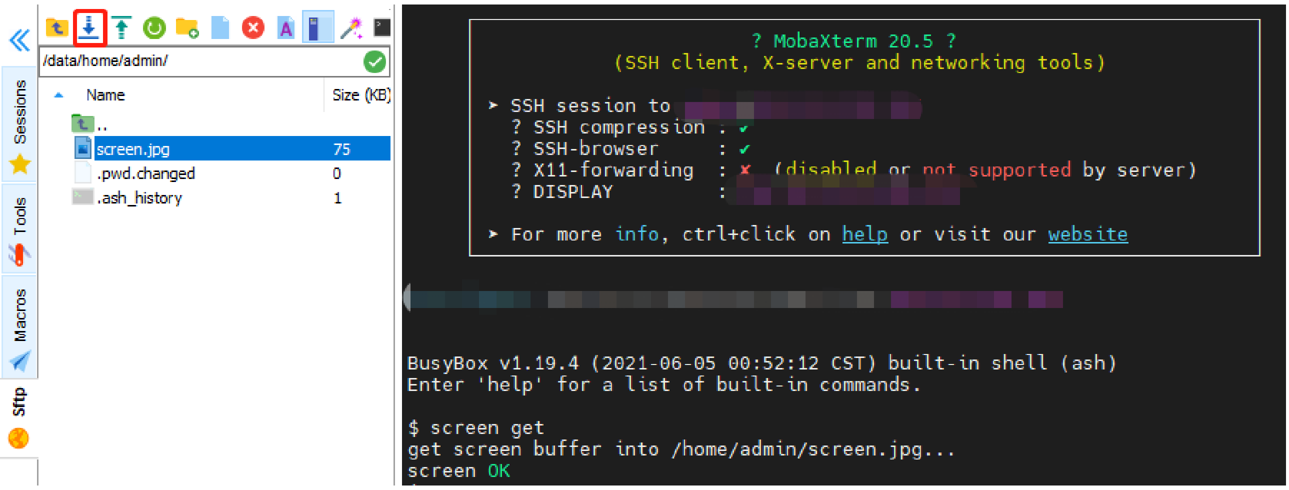
While the PC port is mirroring the LAN port, you can connect PC on PC port to capture ethernet traffic from LAN port.

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 13.1.3.1

For example, assuming you login to the phone by SSH connection with tool Mobaxterm, you can make a screenshot with command and download it in local PC.

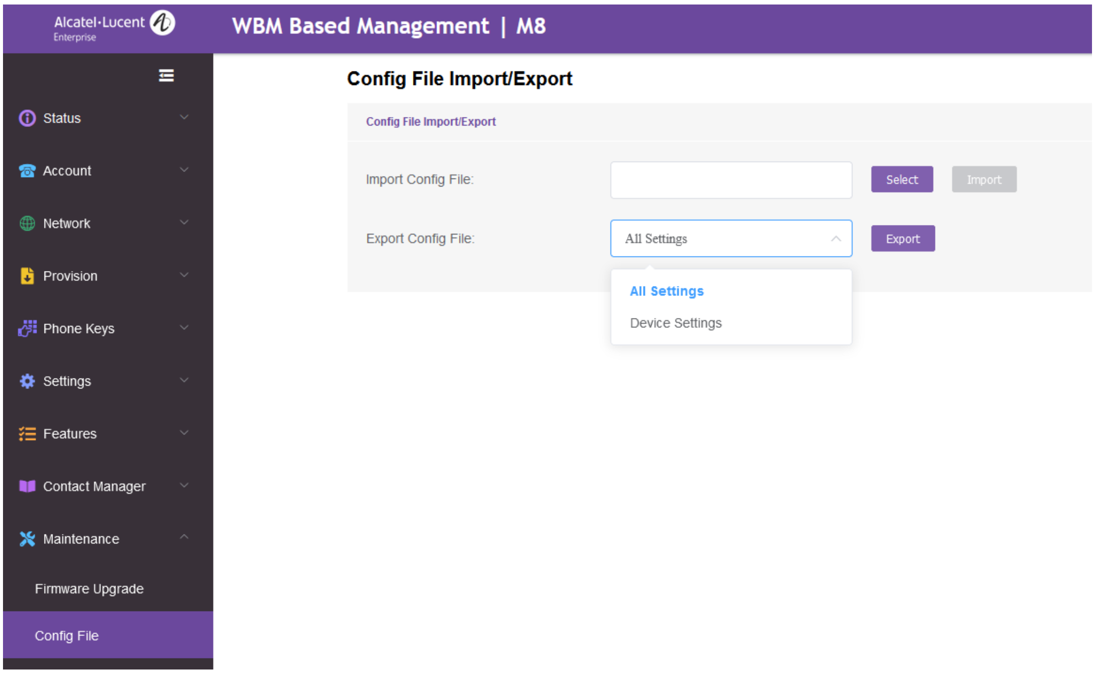


13.7 Import and Export config file

On the web management interface, you can back up and restore the configuration file of ALE phone. You can back up all the modified configurations, device type configurations, and all configurations.

In case of security risks, the exported configuration will not contain the password configuration.

Web UI path: Maintenance -> Config File -> Config File Import/Export.



In addition, config file backup can be performed using the SIP protocol. After the administrator sends the SIP Notify message, the phone uses http (s) to post data to a specified server.

For this format, need sip notify include headers:event:report.

The following table lists the parameters you can use to configure the config file upload feature.

Parameter	**DeviceConfigUploadEnable**	**config.xml**

Description	It enables or disables uploading config file.	
Permitted Values	false - Disable true - Enable	
Default	true	
Parameter	**DeviceConfigUploadUrl**	**config.xml**
Description	It configures config file uploading address. **Note:** The Value can only be a directory and cannot be a fixed file name. If "http://" or "http://" is not specified, http is used. If "https://" is specified, https is used. It works only if "**DeviceConfigUploadEnable**" is set to true.	
Permitted Values	String within 512 characters	
Default	Blank	
Parameter	**DeviceConfigExportMode**	**config.xml**
Description	It configures to export only the modified configurations or all configurations.	
Permitted Values	0 - Export modified configurations 1 - Export all configurations	
Default	0	
Parameter	**DevicePostUriAbsolutePathEnable**	**config.xml**
Description	It enables or disables POST requests to carry absolute paths.	
Permitted Values	false - Disable true - Enable	
Default	false	