Poly ATA 400 Series Administrator Guide

SUMMARY

This guide provides administrators with information about configuring, maintaining, and troubleshooting the featured products.

Legal information

Copyright and license

© Copyright 2023 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Trademark credits

All third-party trademarks are the property of their respective owners.

Privacy policy

Poly complies with applicable data privacy and protection laws and regulations. Poly products and services process customer data in a manner consistent with the Poly Privacy Policy. Please direct comments or questions to privacy@poly.com.

Open source software used in this product

This product contains open source software. You may receive the open source software from Poly up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to Poly of shipping or distributing the software to you. To receive software information, as well as the open source software code used in this product, contact Poly by email at open.source@poly.com.

Table of contents

1 Before You Begin 1

Audience, Purpose, and Required Skills 1

2 Getting Started 2

Supported Devices 2

Poly ATA Device Features 2

Key Features 3

Robust Telephony Features 3

Powerful Call Routing and Voice Service Features 4

LED Description and LED Behaviour 4

Poly ATA 400 LED Status Indicators 4

Poly ATA 402 LED Status Indicators 5

Port Connections 6

Poly ATA 400 Port Connections 6

Poly ATA 402 Port Connections 8

Accessibility Features 9

3 Configuration and Management Interfaces 10

Interactive Voice Response System 10

Find Device IP Address 10

Configure Basic Settings Using the IVR System 10

IVR Local Configuration Options 11

System-Level Configuration Options 12

Network-Related Configuration Options 13

OBiWiFi-Related Configuration Options 14

SIP Service Provider Configuration Options 15

PDMS-SP Configuration Options 19

Auto Attendant Configuration Options 20

Customized AA Prompt Recording Options 20

System Web Interface-Based Local Configuration 21

Access Levels 22

Access the system web interface 22

Updating and Managing a Device Locally 23

Update Firmware 23

Maintaining Customized AA Prompts 23

Back Up Customized AA Prompts 23

Restore Customized AA Prompts 24

Backing Up and Restoring Configuration 24

Back Up Your Configuration 24

Restore Your Configuration from a File 25

Reset Configuration to Factory Default 25

Zero-Touch, Massive Scale Remote Provisioning 26

4 UC Software Configuration on Poly ATA 400 Series 27
Creating Configuration Files 27
Configure the UC Software Provisioning Server Address 27
Add Poly ATA 400 Series to Your Primary Configuration File 28
Supported UC Software Parameters 28
5 Configuring Call Settings 31
Configuring Secure RTP 31
Enable Secure RTP 31
Configure the Cryptographic Parameters for Secure RTP 31
Configuring Multicast Paging 32
Configure Multicast Page Groups 32
Configuring Emergency Call Settings 33
Configure Emergency Call Settings 34
Enhanced 911 and HTTP-Enabled Location Delivery 34
Enable the Location Information Service for E911 34
Configure the Location Information Service for E911 34
Configure the HTTP-Enabled Location Delivery (HELD) for E911 35
Enable the Emergency Geolocation Settings for E911 36
Enable the Inclusion of X-Switch-Info Header in SIP REGISTER Message 37
Enter Device Location Information 37
6 Device Interface 39
Phone Settings 39
Phone Port Signaling and Messaging 39
Configure the Device to Use as a Paging System 40
Primary Line 41
Configure the Primary Line 41
Service Route Access Codes 42
Customize Service Route Access Codes 42
Customize Service Route Access Codes for the Auto Attendant. 43
Call Forward Numbers 43
User Features Available on the Device 44
Place a Call On the Primary Line 44
Call Forwarding 44
Enable Call Forward All 44
Enable Call Forward on Busy 45
Enable Call Forward on No Answer 45
Caller ID - Name and Number 45
Call Waiting 46
3-Way Calling 46
Call Transfer (Attended) 46
Nordic Style Feature Invocation 46
Select Nordic Style Feature Invocation 47
Caller ID Block (Anonymous Calling) 47
Automatic Call Back (Call Return) 48

Repeat Dialing 48
Anonymous Call Block 48
Do Not Disturb 48
Message Waiting Indication - Visual and Tone Based 48
Speed Dialing of 99 OBi Endpoints or Numbers 48
Phone Ports Collaborative Features 49
Service Star Code Features 49

7 Star Code Features 52

Set the Star Code Profile 52

Star Code Scripts 52
Star Code Script Variables 53
Star Code Script Actions (ACT) 54
Star Code Script Format 55
Star Code Script Examples 55
Program a Star Code 56

8 Status Pages 58

System Status 58
View WAN status 58
View Wi-Fi status 58
Product Information 58
View SPn Services Stats (n = 1, 2, 3, 4) 59
View OBiTALK Service Status 59

Call status 60

Call history 60

SP Services Stats 60

Phone Port Status 60

9 Device Settings 61

Repeat Dialing Service 61

Codec Profile Features 61

User Settings 62
Configure speed dial numbers 62
Use a Speed Dial Number as Ad Hoc Gateway 63

10 Configuring Network Settings 64

Network Connectivity 64
Configure the Ethernet Ports 64
Configure the WAN Interface 64

Set the 802.1X Authentication Mode 65

Web Proxy Server 66
Configure Web Proxy Server 66

DNS Lookup 67
Configure Lookup Order 67
Configure DNS Query Delay 67

Define Local DNS Records 68
Configure the Local DNS Record Mode 69
NTP Servers and Local Time 69
Configure NTP Servers 69
Disable SNTP Discovery 70
Set the Local Time Zone 70
Enable Daylight Saving Time 70
Specify Start and End Rules for Daylight Saving Time 70
Configure Amount of Time to Adjust for Daylight Saving Time 71
DHCP Options 71
Configure Additional DHCP Options 71
Configuring Wi-Fi Settings 72
OBiWiFi5G Wireless USB Adapter 72
Connect to a WiFi Access Point 72
Configure the Wi-Fi Interface 73
11 Call Routing 74
Inbound and Outbound Call Routing 74
Inbound Call Route Configuration 74
InboundCallRoute Examples 77
Outbound Call Route Configuration 77
OutboundCallRoute Examples 79
Digit Map Configuration 80
Digit Map Rules and Elements 80
Matching Against Multiple Rules in Digit Map 82
Forcing Interdigit Timeout With A Pound Key 84
Invoke Second Dial Tone in Digit Map 85
Change Inter-digit Long Timer Dynamically After Partial Match 85
User-Defined Digit Maps 86
A User-Defined Digit Map For IPv4 Dialing 86
Configure a User-Defined Digit Map 86
Call Routing and Digit Map 87
Trunks, Endpoints, and Terminals 87
Supported 2-way Call Bridges 87
12 Service Providers 90
ITSP Profile 90
SP Service 90
SIP registration 90
SIP Outbound Proxy Server 91
DNS Lookup of SIP Servers 91
NAT Traversal Considerations 92
SIP Proxy Server Redundancy and Dual Registration 92
SIP privacy 93
STUN and ICE 94
SIP Service Provider Features 95
ITSP Driven Distinctive Ringing 96

RTP Statistics - the X-RTP-Stat Header 96
Media Loopback Service 97
The OBiTALK Service 98
Enable the OBiTALK Service 98
Limit OBiTALK Calls 99
OBiTALK Service Settings 99
Auto Attendant Service 99
Automated Attendant 99
AA Callback Service 100
User Recorded Prompts 100
Enable Auto Attendant 101
Configure the Auto Attendant Callback Service 101
Customize Service Route Access Codes for the Auto Attendant. 101
Customizing AA Prompt Lists 102
Voice Gateways 103
Configure a Gateway for Direct Dialing 104
Voice Gateway Examples 104
Trunks 105
Trunk Groups 105
Configure a Trunk Group 105
13 Troubleshooting 107
System Logs 107
Activate Syslog Messaging 107
Include Detailed SIP Messages in Syslog Messaging 107
View SPN Service Status Messages 108
SPN Service Status Error Messages 108
Locate the Serial Number on the Device 109
Locate the Serial Number in the System Web Interface. 109
Packet Capture 109
Start and Stop a Local Packet Capture 109
Configure the Remote PCAP Server 110
Firmware Update Error Messages 110
14 Appendix A 111
Tone Profile Features 111
Tone Field-1 Composition 111
Tone Field-2 Composition 111
Tone Field-3 to Field-6 Composition 112
Tone Examples 113
Dial Tone 113
Busy Tone 113
Prompt Tone 113
SIT Tone 114
Stutter Tone 114
Ring Profile A & B 115

Ring Profile Features 115
Ring Field-1 Composition 115
Ring Field-2 to Field-5 Composition 115

15 Getting help 117

1 Before You Begin

This guide describes how to configure, maintain, and troubleshoot Poly ATA devices.

The information in this guide applies to the following Poly ATA devices:

- Poly ATA 400
- Poly ATA 402

Audience, Purpose, and Required Skills

This audience includes Internet Telephony Service Providers (ITSP), Voice Service Providers (VSP), Managed Service Value Added Resellers (VAR), Internet Telephony Professionals, and Technology Hobbyists.

You must be familiar with the following concepts before beginning:

- Current telecommunications practices, protocols, and principles
- Telecommunication basics, video teleconferencing, and voice or data equipment
- Open SIP networks and VoIP endpoint environments

2 Getting Started

Understand how to administer, configure, and provision Poly ATA devices.

As you read this guide, keep in mind that certain features are configurable by your system provider, configurable by your system administrator, or determined by your network environment. As a result, some features may not be enabled or may operate differently on your device. Additionally, the examples in this guide may not directly reflect what is available on your device.

NOTE: The terms *the device* and *your device* refer to any of the Poly ATA devices. Unless specifically noted in this guide, all device models operate in similar ways.

Supported Devices

The following table lists the product names, model names, and part numbers for Poly ATA devices.

The Poly ATA 400 series consists of the following device models:

- Poly ATA 400
- Poly ATA 402

Table 2-1 Poly ATA Device Product Name, SKU, and Part Number

Product Name	SKU	Item Number	Item Description
Poly ATA 400	NA	8F3H4AA#ABA	Poly ATA 400 1FXS VP VoIP Adptr SIP US
Poly ATA 400	ANZ, EU, UK	8F3H4AA#AC3	Poly ATA 400 1FXS VP VoIP Adptr SIP WW
Poly ATA 402	NA	8F3H5AA#ABA	Poly ATA 402 2FXS VP VoIP Adptr SIP US
Poly ATA 402	ANZ, EU, UK	8F3H5AA#AC3	Poly ATA 402 2FXS VP VoIP Adptr SIP WW

Poly ATA Device Features

Built with a high-performance, system-on-a-chip platform to ensure high-quality voice conversations, Poly ATA devices are dedicated systems targeted at applications for VoIP services.

Poly ATA devices have high availability and reliability because they're always-on to make or receive calls. If you use a Poly ATA device, you don't need to use a computer, or have a computer turned on, to talk to people. To get started, all you need is a phone, power, and a connection to the internet.

Key Features

Poly ATA devices implement the following features and functionalities.

Table 2-2 Poly ATA Devices

Poly ATA Device Model	VoIP Account Support	No. of Phone Ports	No. of Ethernet Ports	No. of USB Ports
Poly ATA 400	4	1	1	1
Poly ATA 402	4	2	2	1

The key features of the Poly ATA are:

- SIP Service Provider support for up to four SIP accounts
- Four SIP accounts on Poly ATA 400 and Poly ATA 402
- Any available service is accessible from each **Phone** port independently
- Automatic Attendant (AA) for simplified call routing
- Callback service: automatic callback to connect you to the AA to make a new call or call you back on the attached phone later

Your device is configurable to work with any SIP-compliant internet telephone service (ITSP).

The device supports using the Poly Device Management Service for Service Providers (PDMS-SP) web portal. PDMS-SP is the customer portal for device management allowing administrators to remotely inventory, monitor, and troubleshoot Poly devices.

IMPORTANT: *PDMS-SP* and *OBiTALK* are both terms used in the system web interface and the documentation to refer to the same functionality.

Using the PDMS-SP web portal integration lets you:

- Configure and manage your Poly ATA 400 series devices.
- Upgrade your Poly ATA 400 series devices.
- Troubleshoot and capture additional logs for your Poly ATA 400 series devices.

Robust Telephony Features

Connect an analog phone to one of the **Phone** ports on your device to access a robust set of telephony features.

Poly ATA 400 series devices provide the following telephony features:

- Message waiting indication—visual and tone based
- Speed dialing of 99 Poly endpoints or numbers

- Three-way conference calling with local mixing
- Hook flash event signaling
- Caller ID—name and number
- Call waiting
- Call forward unconditional
- Call forward on busy
- Call forward on no answer
- Call transfer
- Anonymous call
- Block anonymous call
- Do Not Disturb
- Call return
- Repeat dialing

Powerful Call Routing and Voice Service Features

Poly ATAs offer voice service features and call routing.

The Poly ATA 400 series devices give you the following features:

- SIP support for voice and fax over IP from internet telephony service providers (ITSPs)
- PDMS-SP managed VoIP network for Poly endpoint devices and applications
- High-quality voice encoding using G.711, G.722, G.726, G.729, iLBC, and Opus algorithms
- Recursive digit maps and associated call routing for outbound and inbound calls

LED Description and LED Behaviour

Each Poly ATA device has LEDs on the front which give indicators of the device status.

Poly ATA 400 LED Status Indicators

There are three LEDs on the front of the Poly ATA 400 device.

The LEDs give you a visual indication of the working order and general status of key functional aspects of the device. Under normal operating conditions, the LEDs show green (solid, flashing, or blinking) signals.

The following figure displays the LEDs on the front of the Poly ATA 400. The table lists each LED numbered in the figure.

Figure 2-1 Poly ATA 400 LEDs

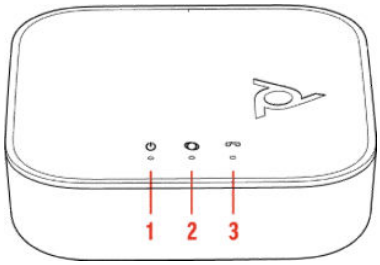

Table 2-3 LED Status Indicators

Reference Number	LED	LED Description
1	Power indicator	The color and pattern of the power indicator shows the following states: LED off: No power Solid green: Powered on and working Flashing green: Searching for a DHCP IP address Flashing orange: Upgrading (Do not unplug power.) Solid red: Not operational
2	LAN Ethernet port indicator	Blinking green: Data activity on the LAN Ethernet port
3	Phone port indicator	The color and pattern of the phone port indicator shows the following states: LED off: Port not enabled Solid green: Phone ready (standby) Flashing green: Phone in use

Poly ATA 402 LED Status Indicators

There are five LEDs on the front of the Poly ATA 402 device.

The LEDs give you a visual indication of the working order and general status of key functional aspects of the device. Under normal operating conditions, the LEDs show green (solid, flashing, or blinking) signals.

The following figure displays the LEDs on the front of the Poly ATA 402. The table lists each LED numbered in the figure.

Figure 2-2 Poly ATA 402 LEDs

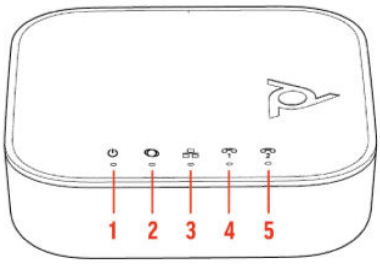

Table 2-4 LED Status Indicators

Reference Number	LED	LED Description
1	Power indicator	The color and pattern of the power indicator shows the following states: LED off: No power Solid green: Powered on and working Flashing green: Searching for a DHCP IP address Flashing orange: Upgrading (Do not unplug power.) Solid red: Not operational
2	LAN Ethernet port indicator	Blinking green: Data activity on the LAN Ethernet port
3	PC Ethernet port indicator	Blinking green: Data activity on the PC Ethernet port
4, 5	Phone ports indicators: Phone 1, Phone 2	The color and pattern of the phone ports indicators show the following states: LED off: Port not enabled Solid green: Phone ready (standby) Flashing green: Phone in use

Port Connections

Learn about the different port connections on the devices in the Poly ATA 400 series.

Poly ATA 400 Port Connections

Become familiar with the physical ports on your Poly ATA 400 device.

The following figures display the ports on the back and side of the Poly ATA 400. The tables list each port numbered in the figure.

Figure 2-3 Poly ATA 400 Ports

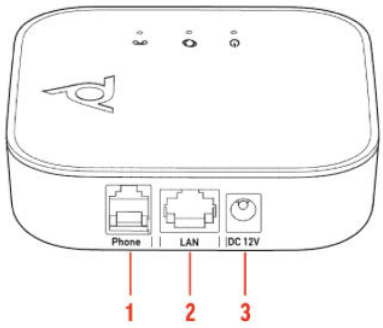

Table 2-5 Port Connections

Reference Number	Port	Port Description
1	Phone Port connection	The **Phone** port on the Poly ATA supports input and output signaling and control messages. You can only connect a touch-tone land line phone to your device's **Phone** port. Phones that use pulse dialing aren't supported.
2	LAN Ethernet port	Use an Ethernet cable to connect the **LAN** port on your device to an Ethernet port on your internet router or switch. By default, the device requests an IP address, DNS, and Internet (WAN) Gateway IP addressing via DHCP.
3	Power connection	Use only the 12-volt power adapter supplied with the original packaging to power the device. The use of a power adapter other than the one given with the device voids the warranty. It might also cause the unit not to work or malfunction.

Figure 2-4 Poly ATA 400 Side View

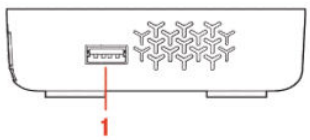

Table 2-6 Port Connections

Reference Number	Port	Port Description
1	USB port	Connect an OBiWiFi5G dongle.

Poly ATA 402 Port Connections

Become familiar with the physical ports on your Poly ATA 402 device.

The following figures display the ports on the back and side of the Poly ATA 402. The tables list each port numbered in the figure.

Figure 2-5 Poly ATA 402 Ports

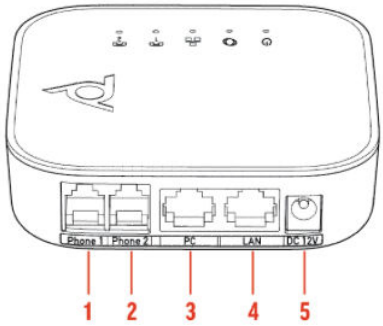

Table 2-7 Port Connections

Reference Number	Port	Port Description
1, 2	Phone Port connections	The **Phone** ports on the Poly ATA support input and output signaling and control messages. You can only connect a touch-tone land line phone to your device's **Phone** ports. Phones that use pulse dialing aren't supported. You can connect a second analog phone, or another analog device such as a fax machine or an alarm panel, to the second **Phone** port.
3	PC Ethernet port	The device **PC** port enables you to daisy-chain a local device such as a computer.
4	LAN Ethernet port	Use an Ethernet cable to connect the **LAN** port on your device to an Ethernet port on your internet router or switch. By default, the device requests an IP address, DNS, and Internet (WAN) Gateway IP addressing via DHCP.
5	Power connection	Use only the 12-volt power adapter supplied with the original packaging to power the device. The use of a power adapter other than the one given with the device voids the warranty. It might also cause the unit not to work or malfunction.

Figure 2-6 Poly ATA 402 Side Callout

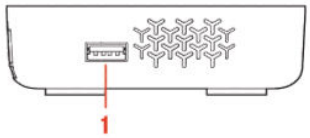

Table 2-8 Port Connections

Reference Number	Port	Port Description
1	USB port	Connect an OBiWiFi5G dongle.

Accessibility Features

Poly products include a number of features to accommodate users with disabilities.

Table 2-9 Accessibility Features

Accessibility Feature	Description
Hardware status indicators	LED indicators provide status and functionality information on the hardware interface.
Connection status indicators	LED indicators provide status and functionality information on the connections between the device and the network or other devices.

3 Configuration and Management Interfaces

Poly offers several methods to configure or provision your phone.

You can configure and manage your Poly ATA device using the following local interfaces:

- Interactive Voice Response System (IVR)
- System web interface

Alternatively, you can choose to configure and manage your Poly ATA device remotely using the PDMS-SP.

Interactive Voice Response System

You can use the IVR system as an automated attendant that you can ask for device configuration information, such as the IP address, and it provides a verbal response. You can also use the IVR to instruct the device to act on the placement or routing of a call to a particular interface.

There are two IVR menus:

- Auto Attendant IVR 1: This menu is referred to as “aa” (or "aa1") for call processing commands. For more information about the Auto Attendant IVR for Poly ATA call processing, see *Poly ATA Call Routing and Digit Map*.
- Auto Attendant IVR 2: This menu is referred to as “aa2” for local configuration. If changing the settings requires that you reboot the device, it’s done automatically when you quit the IVR. You invoke IVR (AA2) by pressing `***` on a phone connected to the **Phone** port of your ATA device.

Find Device IP Address

Find the IP address of your Poly ATA device so that you can log into the system web interface.

1. From a phone attached to the device, enter `***` to access the device Config Attendant.
2. Choose **1** to hear the IP address of the device read back to you.

> **TIP:** Write this down.

Configure Basic Settings Using the IVR System

Use the IVR system's main menu to configure basic settings or to access additional configuration menus.

For a list of the IVR System basic settings, see the *Poly OBi Device Technical Reference*, at Poly Support.

1. From a phone attached to one of the **Phone** ports of your ATA device, dial *** to access the IVR system.
2. Enter the single digit number for the configuration menu item that you want to access.
3. Press ## or hang up to exit IVR.

TIP: By pressing the appropriate button sequence on the telephone key pad, you can move to the next menu of the IVR or invoke a command without first waiting for the previous announcement to end.

IVR Local Configuration Options

The Main Menu after invoking the IVR is a list of operations that you can select by pressing the corresponding 1-digit option number.

Table 3-1 IVR Main Menu Configuration Options

Selection	Announcement	What Can You Do?
1	**Basic Network Status** Reads the IP address and DHCP status.	Press 0 to repeat the information.
2	**Advanced Network Status** Reads the primary and back-up DNS server, primary and back-up NTP server.	Press 0 to repeat the information.
3	**DHCP Current Value** Reads the current value and you have the option to change the value.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information.
4	**IP Address Current Value** Reads the current value and you have the option to change the value. If you elect to enter a new value (static IP address), DHCP is disabled.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information.
5	**Password Current Value** Reads the current IVR password value and you have the option to change the value.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information.
6	**Please Wait** One of the following messages plays: • **Software Update Available. Press 1 to update software** • **Software Update Not Available.**	If an update is available, press 1 to proceed with the update. The software update process starts as soon as you hang up the phone. Warning: Once the software upgrade process starts, the device's power LED blinks rapidly. Make sure the power and network cable stay connected to the unit until the process is complete.

Table 3-1 IVR Main Menu Configuration Options (continued)

Selection	Announcement	What Can You Do?
8	**Restore Factory Default**	Press 1 to confirm device restore to factory default settings. Press # to return to device configuration menu. Press # # to exit IVR.
9	**Reboot**	Press 1 to confirm device reboot. Press # to return to device configuration menu. Press # # or hang up to exit IVR.
0	**Additional Options** Access other configuration options of your phone.	Enter option followed by the # key.

System-Level Configuration Options

Additional configuration options are available with the device IVR after pressing *****0**.

There are many additional options beyond the top-level IVR operations options 1 - 9. Unlike the top-level options, however, the list of available additional options in Menu 0 is not announced.

1. Enter *****0#**
2. Enter your desired option number, followed by **#**
3. Follow any additional prompts, as desired.

You must enter the corresponding option number (followed by the **#** key) to select the particular option. The following tables list the available additional options (grouped by function):

Table 3-2 System-Level Configuration Options

Selection	Announcement	What Can You Do?
1	Firmware Version Reads the current value of the firmware version.	Press 0 to repeat the information. Press # to enter another configuration selection.
2	IVR Password Reads the current value of the IVR password.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.

Table 3-2 System-Level Configuration Options (continued)

Selection	Announcement	What Can You Do?
3	Debug Level Reads the current value of the debug level.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
4	Syslog Server IP Address Reads the current IP address of the syslog server.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
5	Syslog Server Port Reads the current value of the syslog server port.	Press 1 to enter a new value. Press 2 to set the default value of 514. Press 0 to repeat the information. Press # to enter another configuration selection.
81	Factory Reset just the Voice configuration parameters.	Press 1 to confirm. Press # to enter another configuration selection

Network-Related Configuration Options

Additional network-related configuration options are available with the device IVR after pressing ***** 0**.

Table 3-3 Network Related Configuration Options

Selection	Announcement	What Can You Do?
20	DHCP Configuration Reads the current value of the DHCP configuration.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
21	IP Address Reads the current value of the IP address.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.

Table 3-3 Network Related Configuration Options (continued)

Selection	Announcement	What Can You Do?
22	Default Gateway Reads the current value of the default Internet gateway.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
23	Subnet Mask Reads the current value of the subnet mask.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
24	DNS Server (Primary) Reads the current value of the primary DNS server.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
26	NTP Server (Primary) Reads the current value of the primary NTP server.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.

OBiWiFi-Related Configuration Options

Additional OBiWiFi-related configuration options are available with the device IVR after pressing ***** 0**.

Table 3-4 OBiWiFi Network Related Configuration Options

Selection	Announcement	What Can You Do?
40	DHCP Configuration The current value of the DHCP configuration is read back.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
41	IP Address The current value of the IP address is read back.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.

Table 3-4 OBiWiFi Network Related Configuration Options (continued)

Selection	Announcement	What Can You Do?
42	Default Gateway The current value of the default internet gateway is read back.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
43	Subnet Mask The current value of the subnet mask is read back.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
44	DNS Server (Primary) The current value of the primary DNS server is read back.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
46	NTP Server (Secondary) The current value of the Secondary NTP server is read back.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.

SIP Service Provider Configuration Options

Additional configuration options are available with the device IVR after pressing *** * * 0** for SIP service provider 1 (SP1).

Table 3-5 SP1 Configuration Options

Selection	Announcement	What Can You Do?
100	Enable Service Provider One (SP1) Reads the current value.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
101	Registration State of SP1 Reads the current value.	Press 0 to repeat the information. Press # to enter another configuration selection.

Table 3-5 SP1 Configuration Options (continued)

Selection	Announcement	What Can You Do?
102	SP1 User ID Reads the current value.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
167	SP1 Block Caller ID Enable	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
168	SP1 Block Anonymous Call Enable	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
172	SP1 Call Forward ALL - Enable / Disable	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
173	SP1 Call Forward ALL Number	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
174	SP1 Call Forward on Busy - Enable / Disable	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
175	SP1 Call Forward on Busy Number	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.

Table 3-5 SP1 Configuration Options (continued)

Selection	Announcement	What Can You Do?
176	SP1 Call Forward on No Answer - Enable / Disable	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
177	SP1 Call Forward on No Answer Number	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.

Additional configuration options are available with the device IVR after pressing *** * 0** for SIP service provider 2 (SP2).

Table 3-6 SP2 Configuration Options

Selection	Announcement	What Can You Do?
200	Enable Service Provider Two (SP2). Reads the current value.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
201	Registration State of SP2. Reads the current value.	Press 0 to repeat the information. Press # to enter another configuration selection.
202	SP2 User ID. Reads the current value.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
267	SP2 Block Caller ID Enable.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.

Table 3-6 SP2 Configuration Options (continued)

Selection	Announcement	What Can You Do?
268	SP2 Block Anonymous Call Enable	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
272	SP2 Call Forward ALL - Enable / Disable	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
273	SP2 Call Forward ALL Number	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
274	SP2 Call Forward on Busy - Enable / Disable	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
275	SP2 Call Forward on Busy Number	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
276	SP2 Call Forward on No Answer - Enable / Disable	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
277	SP2 Call Forward on No Answer Number	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.

PDMS-SP Configuration Options

PDMS-SP service configuration options are available with the device IVR after pressing ***** 0**.

Table 3-7 PDMS-SP Service Options

Selection	Announcement	What Can You Do?
900	Enable PDMS-SP Service Reads the current value.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
901	Registration State of PDMS-SP Reads the current value.	Press 0 to repeat the information. Press # to enter another configuration selection.
967	PDMS-SP Block Caller ID Enable	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
968	PDMS-SP Block Anonymous Call Enable	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
972	PDMS-SP Call Forward ALL - Enable / Disable	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
973	PDMS-SP Call Forward ALL Number	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
974	PDMS-SP Call Forward on Busy - Enable / Disable	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.

Table 3-7 PDMS-SP Service Options (continued)

Selection	Announcement	What Can You Do?
975	PDMS-SP Call Forward on Busy Number	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
976	PDMS-SP Call Forward on No Answer - Enable / Disable	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.
977	PDMS-SP Call Forward on No Answer Number	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.

Auto Attendant Configuration Options

Auto Attendant configuration options are available with the device IVR after pressing ***0.

Table 3-8 Auto Attendant Options

Selection	Announcement	What Can You Do?
80	Enable / Disable Auto Attendant.	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection.

Customized AA Prompt Recording Options

You can record as many as 10 prompts, which you can arrange in any combination and use as customized AA prompts.

Customized AA prompt recording options are available with the device IVR after pressing * * * 0:

Table 3-9 Customized AA Prompt Recording Options

Selection	Announcement	What Can You Do?
1001	Option 1001 current value is: (the recorded prompt)	Press 1 to enter a new value. Press 2 to set the default value. Press 0 to repeat the information. Press # to enter another configuration selection. Note: After pressing 1 to record a new prompt, the device says "Enter value followed by the # key)\". At that point, you can press any digit (0-9) to start recording, and then press # to end recording. Tips: Leave about 1 second of gap at the end of recording to avoid unintended truncation by the device. After a new prompt is recorded, the device immediately plays back the recorded audio, and then presents the following options: Press 1 to save (save the recorded prompt permanently in long term memory) Press 2 to re-enter (the last recorded prompt is discarded) Press 3 to review Press # to cancel (the last recorded prompt is discarded)
	Similarly for Options 1002 through 1010	

With these options you can record as many as 10 prompts for your customized AA prompts. Each prompt recording is limited to 60 seconds, where the prompt duration is rounded to the nearest number of seconds. A total of 122 seconds is available to store all the recordings. The device reboots automatically when you hang up if any of the prompts have been modified and saved. You can enter a text description for each recorded prompt as a reminder of the contents of the prompt. For more information, see the Auto Attendant Prompt Parameters table in the *Poly ATA 400 Series Parameter Reference Guide*.

System Web Interface-Based Local Configuration

The device has an integrated device management web server, known as the system web interface, that can be accessed from a PC or similar device using a web browser.

Although all popular web browsers are tested for compatibility with the system web interface, there may be inconsistencies that arise from time to time. Contact Poly Support if you have any questions about the system web interface and how it appears in your web browser window.

Access Levels

You can select from two levels of access to the system web interface: administrator and user.

When you access the system web interface, you must enter a username and password.

Administrator (Admin) access
Username: admin
Password: admin
Default

User access
Username: user
Password: user

When you sign in for the first time, or you run a factory reset, the system web interface prompts you to change the Admin password.

IMPORTANT: The Admin or User passwords might be changed using the system web interface, provisioning by a service provider, or via the PDMS-SP web portal (Admin only). Be sure you have access to the correct Admin or User password before you attempt to log on to the system web interface. Check with your System Administrator if the password has changed.

Access the system web interface

You can access the Poly ATA system web interface from a computer using a web browser. You need administrator-level access to complete any device configuration tasks in the system web interface.

Use the IVR system to find the IP address of your device. See Find Device IP Address on page 10.

Ensure that you have the password for the Admin user. See Access Levels on page 22 for more information.

1. Enter the IP address in a web browser on your computer.
2. When prompted, enter the default admin **Username** and **Password** (`admin`/`admin`).

NOTE: If you're signing in for the first time, you must change the password from the default.

The system web interface is organized into sections. The sections allow a manageable and compartmentalized approach to configuring the many hundreds of parameters available on the device. Use the expandable/collapsible menu tree on the left side of the page to move easily through the various configuration parameter sections of the device.

IMPORTANT: Submit every configuration page individually after you change the page. Otherwise those changes are discarded once you move to another page. Most changes require a reboot of the unit, by clicking the **Reboot** button, to take effect. However, you can reboot the unit once after you have made and submitted all the necessary changes on all the pages.

Updating and Managing a Device Locally

Run maintenance tasks on your device.

Update Firmware

You can upgrade the firmware for your device from the system web interface.

The firmware file with which you want to upgrade the device must be stored locally on a computer that you can access with a web browser.

Follow these steps to upgrade:

1. In the system web interface, go to **System Management** > **Device Update**.
2. Under **Firmware Update**, press the **Browse** button to specify the path of the firmware file.

   This action opens a file browser window where you can navigate to and select the firmware file.
3. Upon selection of the firmware file, press the **Update** button to start the upgrade process.

The process takes about 30 seconds to complete. You MUST NOT disconnect the power from the device during this procedure. If the new firmware is upgraded successfully, the device reboots automatically to start running the new firmware. Otherwise, the web page shows an error message explaining why the upgrade failed. For information on possible error messages, see Firmware Update Error Messages on page 110.

Maintaining Customized AA Prompts

You can record as many as 10 individual AA prompts through the device IVR interface. Back up your customized prompts to restore them later, or to copy them to other devices.

You can back up your customized prompts into a single file from the system web interface. The default name of the file is `backupaa.dat`. The backup file also includes the annotations entered for each recorded prompt.

Back Up Customized AA Prompts

Back up your device's customized AA prompts to restore them later or to copy them to another device.

To back up your AA prompts to a file, follow the steps for backing up your configuration using the web system interface. See Back Up Your Configuration on page 24 for more information.

1. In the system web interface, go to **System Management** > **Device Update**.
2. Under **Backup Configuration**, choose one of the backup options and press the **Backup** button.

3. Select **Save**.

> ⚠ **WARNING!** All the existing prompts in the device are removed first when applying the backup file. This process cannot be undone.

Restore Customized AA Prompts

Restore your customized AA prompts from a backup file to your device.

To restore an AA prompt file onto a device, follow the steps for a firmware upgrade using the system web interface. Instead of using a firmware file, use the prompt file. The device can detect from the file header that you're trying to upload a prompt file and process the file accordingly. See Update Firmware on page 23 for more information.

1. In the system web interface, go to **System Management** > **Device Update**.
2. Specify the path to the backup file by clicking the **Browse** button in the **Firmware Update** section of the page.

   This opens a file browser window where you can navigate to and select the file.
3. Upon selection of the backup file, press the **Update** button to start the restoration process.

Backing Up and Restoring Configuration

Back up your device configuration and save it as an XML file. You can then use it to restore your device configuration.

Back Up Your Configuration

Back up the current configuration of the device and store as an XML file at a user-specified location.

When you back up the current configuration of the device, the system creates the backup file with the default name of `backup xxxxxxxxxxxx .xml`, where the `xxxxxxxxxxxx` represents the MAC address of the unit.

> **NOTE:** Different web browsers might handle this operation differently. If the operation is blocked due to the security setting of the web browser, change the security setting temporarily to allow this operation to complete.

1. In the system web interface, go to **System Management** > **Device Update**.
2. Under **Backup Configuration**, choose one of the following options:

Table 3-10 Configuration Backup and Restore

Option	Description	Default Setting
Incl. Running Status	If checked, the values of all status parameters are included in backup file. Otherwise, status parameters are excluded from the backup.	No

Table 3-10 Configuration Backup and Restore (continued)

Option	Description	Default Setting
Incl. Default Value	If checked, the default values of parameters are included in the backup file. Otherwise, default values are excluded from the backup.	No
Use Poly ATA Version	If not checked, the backup file uses XML tags that are compliant with the TR-104 standard. Otherwise, the backup file is stored in a Poly ATA proprietary format where the XML tags aren't compliant with TR-104, but the file size is smaller and the file is more readable.	No
Encrypt Content	If checked, the backup file is encrypted. Otherwise, the backup file isn't encrypted.	No
Non-default Only	If checked, only the parameters that have values that are different from the default are included in the backup file. Otherwise, all parameters are included in the backup file.	No

3. Select **Backup**.

   All passwords and PINs are excluded from the backup file. Hence they are not available to restore. Call history is excluded from the backup, but can be saved as an XML formatted file separately from the *Call History* web page.

4. Select **Save**.

   You can change the file name and the location to save the backup file from the default options.

Restore Your Configuration from a File

You can restore the device configuration that you previously backed up to a file. Call history and various statistical information are removed at the same time.

⚠ CAUTION: Resetting the device configuration should be used with extreme caution as the operation can't be undone.

1. In the system web interface, go to **System Management** > **Device Update**.
2. Under **Restore Configuration**, choose a backup configuration file and select **Open**.
3. Select **Restore**.
4. Press **Ok** to confirm the action.

   Your device restarts automatically when the restoration completes.

Reset Configuration to Factory Default

You can reset the device configuration to the factory default condition.

1. In the system web interface, go to **System Management** > **Device Update**.
2. Under **Reset Configuration**, select **Reset**.

   Your device restarts automatically when the reset completes.

Zero-Touch, Massive Scale Remote Provisioning

Poly ZT or Zero Touch provisioning is a system level approach to deploying and maintaining thousands or millions of Poly devices with high security and control at the device level down to the individual parameter provisioned on each device.

For information regarding the capability, process and practice of using Poly ZT Provisioning, contact HP | Poly Support.

4 UC Software Configuration on Poly ATA 400 Series

You can use your UC Software provisioning server and configuration files to provision and configure features on Poly ATA devices.

Using UC Software configuration files, you can provision and configure your devices, and you can include a mix of UC Software parameters and OBi Edition parameters within the configuration file.

Creating Configuration Files

Create a Configuration file that includes a mixture of UC Software and OBi parameters.

Use a small subset of UC Software parameters to configure your devices, mainly for registering the device with a SIP service. Then use OBi parameters in UC Software parameter syntax to configure any additional features you want to include on your device.

IMPORTANT: Define OBi parameters using the UC Software parameter syntax when using the UC Software configuration file.

The following code is an example configuration with both UC Software parameters in standard XML format and OBi parameters in the same format as UC Software parameters.

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<PHONE_CONFIG>
<config
tcpIpApp.sntp.address="ntp.poly.com"
reg.1.server.1.address="server.poly.com"
reg.1.address="0123456789"
reg.1.auth.userId="0123456789"
reg.1.auth.password="poly"
reg.1.server.1.transport="TCPOnly"
VoiceService.1.VoiceProfile.6.SIP.ProxyServer="i3.voip.polycom.com"
VoiceService.1.VoiceProfile.6.SIP.ProxyServerPort="5066"
VoiceService.1.VoiceProfile.6.SIP.ProxyServerTransport="TLS"
VoiceService.1.VoiceProfile.1.Line.6.X_ServProvProfile="F"
>
</config>
</PHONE_CONFIG>
```

Configure the UC Software Provisioning Server Address

Configure the device to request and download a UC Software configuration file. It first requests the `MAC.cfg` or `000000000000.cfg` (if it doesn't find `MAC.cfg`

on the server) primary configuration file at the configured provisioning server address. Then it requests any configuration files listed in the CONFIG_FILES attribute.

1. In the system web interface, go to **System Management** > **Auto Provisioning**.
2. Under **ITSP Provisioning**, clear the check boxes in the **Default** column for the following settings:
   - **ProvisioningOption**
   - **UCSServer**
3. In the **Value** column, configure the following settings:

Table 4-1 Parameter List

Parameter Name	Value
`ProvisioningOption`	UCSServer
`UCSServer`	The URL of the path to the primary configuration file on the provisioning server. For example, https://provisioning.example.com/poly/ata

4. Select **Submit**.

Add Poly ATA 400 Series to Your Primary Configuration File

Add ATA 400 Series devices to your UC Software primary configuration file to fetch the latest firmware and configuration files on your provisioning server.

Add the device firmware and configuration files to your provisioning server.

1. In your primary configuration file (`MAC.cfg` or `000000000000.cfg`), enter the following parameters and values:

```
APP_FILE_PATH_ATA_ATA400="<Name of ATA 400 firmware file name>.fw"
CONFIG_FILES_ATA_ATA400="<Name of ATA 400 configuration file>.cfg"
APP_FILE_PATH_ATA_ATA402="<Name of ATA 402 firmware file name>.fw"
CONFIG_FILES_ATA_ATA402="<Name of ATA 402 configuration file>.cfg"
```

2. Save the configuration file.

Supported UC Software Parameters

Poly ATA 400 Series devices support a small list of UC Software parameters.

NOTE: For the `reg.x.server.y.*` parameters, the devices only support configuring the system to only one server, so use `reg.1.server.1.` for all related parameters.

`device.dns.altSrvAddress`
Sets the secondary server where the phone directs DNS queries.
Server Address
Change causes system to restart or reboot.

device.dns.serverAddress
Sets the primary server where the phone directs DNS queries.
Server Address
Change causes system to restart or reboot.

device.prov.serverName
IP address
Domain name string
URL
If you modify this parameter, the phone provisions again. The phone also reboots if the configuration on the provisioning server changes.

device.sntp.serverName
Enter the SNTP server where the phone obtains the current time.
IP address
Domain name string

reg.x.address
The user part (for example, 1002) or the user and the host part (for example, `1002@poly.com`) of the registration SIP URI.
Null (default)
String address

reg.x.displayName
The display name used in SIP signaling and the label that displays on the phone key line.
Null (default)
UTF-8 encoded string

reg.x.outboundProxy.address
The IP address or hostname of the SIP server where the phone sends all requests.
Null (default)
IP address or hostname

reg.x.outboundProxy.port
The port of the SIP server where the phone sends all requests.
0 (default)
1 to 65535

reg.x.outboundProxy.transport
The transport method the phone uses to communicate with the SIP server.
DNSnaptr (default)
DNSnaptr, TCPpreferred, UDPOnly, TLS, TCPOnly

If this parameter is set, it takes precedence even if the DHCP server is available.
IP address or hostname - SIP server that accepts registrations.

The phone's requested registration period in seconds. The period negotiated with the server may be different. The phone attempts to reregister at the beginning of the overlap period.
3600 (default)
Positive integer, minimum 10

Null (default) - The port of the SIP server doesn't specify registrations.
1 to 65535 - The port of the SIP server that specifies registrations.

The transport method the phone uses to communicate with the SIP server.
TCPpreferred-
UDPOnly
TLS
TCPOnly

reg.x.srtp.enable
1 (default) - The registration accepts SRTP offers.
0 - The registration always declines SRTP offers.
Change causes system to restart or reboot.

reg.x.srtp.require
0 (default) - Secure media streams are not required.
1 - The registration is only allowed to use secure media streams.
Change causes system to restart or reboot.

reg.x.type
private (default) - Use standard call signaling.
shared - Use augment call signaling with call state subscriptions and notifications and use access control for outgoing calls.

tcpIpApp.sntp.address
Specifies the SNTP server address.
NULL (default)
Valid hostname or IP address.

tcpIpApp.sntp.gmtOffsetcityID
NULL (Default)
0 to 127

tcpIpApp.sntp.gmtOffset
Specifies the offset in seconds of the local time zone from GMT.
0 (Default) - GMT
3600 seconds = 1 hour
-3600 seconds = -1 hour
Positive or negative integer

5 Configuring Call Settings

Configure call settings including secure RTP, multicast paging, and emergency call settings for your device.

Configuring Secure RTP

Configure your phone to use secure RTP for encrypted audio.

Enable Secure RTP

Enable secure RTP for encrypted audio.

1. In the system web interface, go to **Voice Services** > **SIP/Service**.
2. Under **Calling Features**, in the `Value` column, select the desired value for `X_SRTP`:
   - `Disable SRTP` = No encryption
   - `Use SRTP Only` = Require SRTP
   - `Use SRTP When Possible` = SRTP is optional
3. Select **Submit**.
4. Restart your system when you complete your changes.

Configure the Cryptographic Parameters for Secure RTP

Configure the cryptographic parameters for the secure RTP stream.

1. In the system web interface, go to **Voice Services** > **SIP/Service**.
2. Under **Calling Features**, in the `Value` column, enter the desired cryptographic parameters in a comma-separate list for `X_SRTPCryptos`:
   - `AES_CM_128_HMAC_SHA1_32`
   - `AES_CM_128_HMAC_SHA1_80`
   - `AES_CM_192_HMAC_SHA1_32`
   - `AES_CM_192_HMAC_SHA1_80`
   - `AES_CM_256_HMAC_SHA1_32`
   - `AES_CM_256_HMAC_SHA1_80`
   - `AES_192_CM_HMAC_SHA1_32`
   - `AES_192_CM_HMAC_SHA1_80`

- `AES_256_CM_HMAC_SHA1_32`
- `AES_256_CM_HMAC_SHA1_80`

3. Select **Submit**.
4. Restart your system when you complete your changes.

Configuring Multicast Paging

Your device supports multicast paging. Each device supports two multicast groups and up to 10 page groups.

Configure Multicast Page Groups

Configure the page groups on your device. Each device supports two multicast groups and up to 10 page groups.

1. In the system web interface, go to **Service Providers** > **Page Groups**.
2. Under **Page Group** *n*, clear the check boxes in the **Default** column for the following settings, then configure the settings in the **Value** column.

Table 5-1 Page Group Parameters

Parameter	Description
`GroupName`	A user-friendly name to label the group on the phone UI.
`MulticastAddress`	This must be a valid IPv4 multicast address. The default is `224.1.1.100` for all paging groups.
`Emergency`	Designate this page group as the emergency group. Pages on this group are auto answered.
`Polycast`	Use Poly UC Software multicast paging format.
`PolycastListen`	Enable listening on this Poly UC Software multicast page group.
`PolycastGroup`	The Poly UC Software multicast paging group to use.

Table 5-1 Page Group Parameters (continued)

Parameter	Description
`MulticastPort`	The default is `65322` for page group 1 and `65324` for page group 2. • 65326 for page group 3 • 65328 for page group 4 • 65330 for page group 5 • 65332 for page group 6 • 65334 for page group 7 • 65336 for page group 8 • 65338 for page group 9 • 65340 for page group 10 **NOTE:** Each group must use a different port number. If Polycast group paging is used, the same port can be used for all Polycast groups.
`TTL`	The TTL value of outgoing (multicast) RTP packets. The default is `2`.
`AudioCodec`	Audio codec to use for outgoing page. Default is G711U.
`TxPacketSize`	The outgoing RTP packetization in milliseconds. The default is `20`.
`RTCPTxInterval`	The interval, in milliseconds, between sending outgoing RTCP packets when paging. No RTCP packets are sent if the value is `0` (default). An RTCP Bye packet is always sent when ending an outgoing page regardless of this setting.
`SilenceSuppression`	A Boolean option to control if Silence Suppression is used for an outgoing page. The default is `false`.
`PlayToneOnIncomingPage`	A Boolean option to control whether to play a short Paging Tone before playing a new incoming page. The default is `true`.
`StartTalkingOnJoin`	Select the check box to enable talking immediately on joining the group.
`TalkingAlertTone`	Select a tone to alert the user periodically that the device is in talking mode.
`SwitchToTalkModeDigit`	Select the digit to enter to switch from listening mode to talking mode.
`SwitchToListenModeDigit`	Select the digit to enter to switch from talking mode to listening mode.

3. Select **Submit**.
4. Restart your system when you complete your changes.

Configuring Emergency Call Settings

Set up the various components of emergency calling support in your device.

Configure Emergency Call Settings

You can define one or more numbers as emergency numbers by adding the prefix EM# to those numbers using the `DigitMap` parameter and a corresponding rule with `OutboundCallRoute` to route those calls to a specific voice service to handle the call.

1. In the system web interface, go to **PHONE /VPort** > **Phone Settings**.
2. In the **Value** column, configure the following parameters:

   Table 5-2 Required Parameters

Parameter	Description
`DigitMap`	Enter a digit map by adding the prefix EM# to those numbers. For example, `DigitMap = (<EM#>911|other rules …)`
`OutboundCallRoute`	Enter the routing rule for outbound calls made from this phone. For example, `OutboundCallRoute = {('EM'#xx.):sp1}, {(311):sp2},other rules ...`

3. Select **Submit**.
4. Restart your system when you complete your changes.

Enhanced 911 and HTTP-Enabled Location Delivery

Service providers can also provide location-based Enhanced 911 (E911) and HTTP-Enabled Location Delivery (HELD) services to the device users.

Enable the Location Information Service for E911

Configure the device to use the Location Information Service (LIS) for E911.

1. In the system web interface, go to **System Management** > **Device Admin**.
2. Under **Location Information Service**, in the **Value** column for the **Enable** parameter, select the check box.
3. Select **Submit**.
4. Reboot your system when you complete your changes.

Configure the Location Information Service for E911

Define the preferred source of location information for the Poly ATA device. When the user makes an emergency call, the phone looks up the selected source of location information to collect the details required for the call INVITE message.

1. In the system web interface, go to **System Management** > **Device Admin**.
2. Under **Location Information Service**, in the **Value** column, select a location information source from the following options for the **PreferredSource** parameter.

LLDP	The network switch that the phone is connected to has the LLDP-MED configured to deliver the location of the phone.
LIS	The Location Information Server (LIS), in this case, the HELD server, is configured to deliver the location of the phone.
DHCP	The DHCP server in the network is configured to deliver the location of the phone, via DHCP Option 99.
Configuration	Use the statically configured location values set up on the phone.

If the **PreferredSource** location information isn't available at the time of the emergency call, the phone searches for location information in the following order: LLDP, LIS, DHCP, or Configuration.

3. Select **Submit**.
4. Reboot your system when you complete your changes.
5. Check the value in **CurrentLocation** to ensure that the location information is correct.

Configure the HTTP-Enabled Location Delivery (HELD) for E911

Define how to retrieve location information from the Location Information Server (LIS) using the HELD protocol. You can choose to retrieve the phone's location information by value from the LIS or by reference.

1. In the system web interface, go to **System Management** > **Device Admin**.
2. Under **HTTP-Enabled Location Delivery**, in the **Value** column for the **Enable** parameter, select the check box.
3. In the **Value** column, configure the following settings:

Table 5-3 HTTP-Enabled Location Delivery

Parameter	Description
`RequestType`	Set the type of the request to the LIS. The options are: • Any: Request to return the location either by reference or by value. **NOTE:** This isn't the *Any* value referred to in RFC 6442. • Civic: Request to return a civic address. • RefID: Request to return a set of Location URIs.
`Identity`	Set the vendor-specific element to include in a location request message such as **companyID**.
`IdentityValue`	Set the value for the vendor-specific element to include in a location request message.

Table 5-3 HTTP-Enabled Location Delivery (continued)

Parameter	Description
Network Access Identifier (NAI)	Omit or include the specified NAI in the location request message. • Omit: Omit the NAI in the request message. • SPx User Info: Use SPx's user information to compose the NAI. SPx: SP1 ... SP6 service provider configuration. • Custom Value: Specify the NAI with a string in the NAICustomValue parameter. NOTE: The following rules compose the NAI when using the SPx user information: • If SPx's URI is empty, the NAI is "AuthUserName@ProxyServer" • If the URI isn't empty and it contains the "@" character, the NAI is that value • If the URI isn't empty but doesn't contain the "@" character, the NAI is "URI@ProxyServer"
NAICustomValue	Specify the custom NAI value to include in a location request message, when the NAI is a Custom Value.
PrimaryServer	Specify the host name, IP address, or URL of the primary LIS such as lis.example.com or https://lis.example.com:8443.
PrimaryServerUsername	The username used to authenticate to the primary server. For no authentication requirement, enter NULL.
PrimaryServerPassword	The password used to authenticate to the primary server. For no authentication requirement, enter NULL.
SecondaryServer	Specify the host name, IP address, or URL of the secondary LIS such as lis.example.com or https://lis.example.com:8443.
SecondaryServerUsername	The username used to authenticate to the secondary server. For no authentication requirement, enter NULL.
SecondaryServerPassword	The password used to authenticate to the secondary server. For no authentication requirement, enter NULL.
TLSSecurityProfile	Sets the TLS Security Profile to use with HTTPS.
X_VerifyServerDomain	Enable verification of server domain against its certificate on HTTPS connections.
RetryTimer	Specify the retry timeout value in seconds for location requests sent to the LIS. Range: 60 - 86400. NOTE: An out of range value rounds to the nearest valid number.

4. Select **Submit**.
5. Restart your system when you complete your changes.

Enable the Emergency Geolocation Settings for E911

You can optionally enable the provision of the P-Emergency-Info Header, and the use of a static or dynamic geolocation reference in the Geolocation Header of

an emergency call INVITE message. This is in addition to the phone's location. This additional information helps to route decisions along the emergency call's signaling path.

1. In the system web interface, go to **System Management** > **Device Admin**.
2. Under **Emergency Geolocation Settings**, in the **Value** column for the **E911Enable** parameter, select the check box.
3. In the **Value** column, configure the following parameters:

Table 5-4 Emergency Geolocation Settings

Parameter	Description
`GeolocationRoutingEnable`	Select the check box to set the value of the Geolocation-Routing header in the E911 INVITE message to **Yes**. The Default is **Disabled**. The value is set to **No**.
`UsageRuleRetransmission`	Select the check box to allow the recipient of this location object to share the enclosed location information, or the object as a whole, with other parties. The Default is **Disabled**.
`PEmergencyInfoHeader`	Select the check box to include the P-Emergency-Info, which contains the phone's MAC address in the E911 INVITE message. The Default is **Disabled**.

4. Select **Submit**.
5. Reboot your system when you complete your changes.

Enable the Inclusion of X-Switch-Info Header in SIP REGISTER Message

When you enable the X-Switch-Info Header in SIP REGISTER messages, the phone gathers the MAC address and port information from LLDP and sends that data to the server. The server then determines the phone's location based on the location configuration.

1. In the system web interface, go to **Service Providers**.
2. Under **ITSP Profile X** > **SIP**, in the **Value** column for the **X_SwitchInfoHeader** parameter, select the check box.
3. Select **Submit**.
4. Reboot your system when you complete your changes.

Enter Device Location Information

Enter the static location information for a Poly ATA device. This information is the primary way to specify the location of a phone if there's no other method set. Usually, this method is a backup method for use when the HELD server is unavailable.

1. In the system web interface, go to **System Management** > **Device Admin**.
2. Under **Enter Device Location Information**, in the **Value** column for the **URI** parameter, enter a semicolon-separated URI location list.

NOTE: If you enable this parameter, you can use the macros `chassisId` and `portId` in the statically configured **Device Location Information URI**, or

in the **Location URI** from the LIS or HELD service. The `portId` populates if the LLDP ID for `portId` contains the MAC address type.

3. In the **Value** column for the following parameters, configure the following settings:

Table 5-5 Device Location Information Parameters

Parameter	Description
`Country`	Enter the country.
`A1`	Enter the national subdivision such as a state or province.
`A3`	Enter the city.
`PRD`	Enter the leading direction of the street location.
`RD`	Enter street or road name.
`STS`	Enter the suffix name used in RD such as a street or avenue.
`POD`	Enter the trailing street direction such as southwest.
`HNO`	Enter the street address number.
`HNS`	Enter a suffix for the street address used in HNO such as A or ½.
`LOC`	Enter any additional information that identifies the location.
`NAM`	Enter a proper name to associate with the location.
`PC`	Enter the ZIP or postal code.
`Label`	Enter a label for the location.

4. Select **Submit**.
5. Reboot your system when you complete your changes.

6 Device Interface

The device provides an FSX **Phone** port for connecting between your phone and your phone provider.

Your phone provider can be an Internet Telephony Service Provider (ITSP), an Internet Service Provider (ISP), an analog telco provider, or a mixture of other VoIP providers.

Phone Settings

Configure the settings for making calls from the phone attached to the **Phone** port of your device or via the Auto Attendant.

Phone Port Signaling and Messaging

Learn about the input and output signaling and control messages supported on the **Phone** ports.

The device **Phone** port can select from the following services to which it can complete a call:

- SP1 Service (SP1)
- SP2 Service (SP2)
- SP3 Service (SP3)
- SP4 Service (SP4)
- PDMS-SP Service (PP1)

The device **Phone** port supports input signaling and control messages comprising:

- On Hook
- Off Hook
- Hook Flash
- DTMF tones

The device **Phone** port supports output signaling and control messages comprising:

- Caller ID/CWCID
- MWI
- DTMF tone
- Ring

- Polarity Reversal
- CPC
- Power Denial

Maximum Session Capacity

The device **Phone** port has a Maximum Sessions capacity of two. This value is not configurable. The device **Phone** port replies BUSY to a new incoming call when:

- The **Phone** port already has two calls in session.
- The **Phone** port is ringing the phone.
- The phone is in a dialing or fast busy "Invalid" state.
- The device is already in a FAX call.

The device **Phone** port supports Call Waiting when a second call is an inbound call:

- A Hook-Flash (or depressing the Flash button) invokes switching between two calls.
- When the device **Phone** port goes On-Hook, this ends the current call and invokes a ring for the holding call. The device **Phone** port supports 3-way Calling when the second call is an outbound call.

On the first Hook-Flash during an active call, the device can make a second outbound call.

On the second Hook-Flash, the first call and the second outbound call are placed in a conference. To remove the second conferenced party, invoke a third Hook-Flash.

When the device goes On-Hook during a 3-way Call, this action becomes a transfer when a second (outbound) call is ringing or connected. If the second (outbound) call doesn't succeed, for example, no answer or busy, then the device **Phone** port can go to an On Hook state. It will ring as the holding call is still on the line, or Hook-Flash to resume the first call.

Configure the Device to Use as a Paging System

You can connect a **Phone** port on the device to an external PA system via an RJ11-to-Line-Out connector (available at many popular electronics shops).

In this configuration, the **Phone** port is expected to be off-hook all the time. The device automatically answers incoming calls. It doesn't accept call-waiting.

When the **Phone** port goes from on-hook to off-hook, in case the user needs to dial `* * *` to invoke the IVR, the device plays a dial tone for 5 seconds. After 5 seconds, the device turns silent and is ready to accept an incoming call to the paging system.

1. In the system web interface, go to **Physical Interfaces** > **PHONE *N*Port** > **Phone Settings**.
2. In the **Default** column, clear the check box for `UseForPagingOnly`.

3. In the **Value** column, select the check box to enable the port for paging.
4. Select **Submit**.
5. Reboot your system when you complete your changes.

Primary Line

Defining a Primary Line means that when you dial a new number using the phone connected to your device, or the AA, you don't need to first dial a service route access code.

You can add as many as four SP VoIP services to your device. The VoIP services are SIP-based services. In addition, all device models come with the PDMS-SP (peer-to-peer) service. In this document, any one of these voice services is referred to as a *trunk*. A *trunk group* (TG) is a comma-separated ordered list of trunks. If a TG is selected for making an outbound call, the device picks the first available member in that trunk group for the call. As many as four TGs can be defined for a device. See the Trunk Groups on page 105 section for details.

You can designate one of the available trunks, or TGs, as the Primary Line for outbound calls. This trunk is then used when users make calls without dialing any service route access codes. See Place a Call On the Primary Line on page 44 for more information.

To call a number via a service that isn't the Primary Line, you need to first dial that service's access code, then dial the number. See Service Route Access Codes on page 42 for more information.

Configure the Primary Line

Use the system web interface to configure a line as the Primary Line for outbound calls made from the **Phone** port and via the device Auto Attendant. The primary line is the default service used to make calls when users aren't using an explicit access code prefix.

When you set the name of the primary line, occurrences of (`Mpli`) and `pli` are substituted internally with the abbreviated trunk name of the selected primary line, in the device `DigitMap` and `OutboundCallRoute` parameters as follows:

Table 6-1 Primary Line Parameter Mapping

Primary Line	Parameter Value
SP1	sp1
SP2	sp2
SP3	sp3
SP4	sp4
PDMS-SP	pp
Trunk Group 1	tg1
Trunk Group 2	tg2

1. In the system web interface, go to **Physical Interfaces** > **PHONE n Port**.

2. In the **Default** column for the `PrimaryLine` parameter, clear the check box.
3. In the **Value** column for the `PrimaryLine` parameter, select the service you want to set as the primary line.
4. Select **Submit**.
5. Restart your system when you complete your changes.

Service Route Access Codes

To make a call via a service that is not the Primary Line, you need to dial that service's access code before the destination number.

The default service route access codes are defined as:

- ****1**: SIP Service Provider 1 (SP1)
- ****2**: SIP Service Provider 2 (SP2)
- ****3**: SIP Service Provider 3 (SP3)
- ****4**: SIP Service Provider 4 (SP4)
- ****9**: PDMS-SP Network (PP)

Customize Service Route Access Codes

If necessary, modify the service route access codes with the `DigitMap` and `OutboundCallRoute` parameters. Customizing the service route access codes helps when you prefer not to use the default service route access code for SP1 (**1), SP2 (**2), ... , SP4 (**4) and want to change it to something else.

NOTE: The phone handles the *PrimaryLine* setting by substituting internally all occurrences of `pli` with the abbreviated name of the trunk named as the primary line in the `DigitMap` and `OutboundCallRoute` parameters of the same parameter group.

NOTE: `**5` is a reserved internal star code, so you cannot use `**5` as a service route access code.

1. In the system web interface, go to **Physical Interfaces** > **PHONE n Port**.
2. In the **Default** column, clear the check boxes for `DigitMap` and `OutboundCallRoute`.
3. In the **Value** column, configure the following parameters:

Table 6-2 Parameter Values

Parameter	Value
`DigitMap`	Modify the digit map to limit the numbers that you can dial or modify the service route access codes. For example, to change the service route access code to SP2 from **2 to **7, replace `**2(Msp2)` with `**7(Msp2)`.

Table 6-2 Parameter Values (continued)

Parameter	Value
`OutboundCallRoute`	Modify the routing rule for outbound calls made from the phone. For example, after changing the service route access code to SP2 from **2 to **7, replace the entry `{(<**2:>(Msp2)):sp2}` to with `{(<**7:>(Msp2)):sp2}`.

4. Select **Submit**.
5. Restart your system when you complete your changes.

Customize Service Route Access Codes for the Auto Attendant.

Customize the service route access codes, including the outbound call route and digit map, for calling via the Auto Attendant.

1. In the system web interface, go to **Voice Services** > **Auto Attendant**.
2. Under **Auto Attendant 1**, in the **Default** column, clear the check boxes for **DigitMap** and **OutboundCallRoute**.
3. In the **Value** column, enter the rules for the Auto Attendant for **DigitMap** and **OutboundCallRoute**.
4. Select **Submit**.
5. Restart your system when you complete your changes.

Call Forward Numbers

Each voice service on the device has one set of Call Forward settings. These settings only apply to incoming calls on that service.

Call Forward Format

You can, however, forward calls to numbers on the same service or on another service. To do so, you must store the call routing information for each call forward number in the device configuration.

The general format of a call forward number is:

```
TK(number)
```

where *TK* is the abbreviated name of a voice service.

Valid values of *TK* are SP1 for the SP1 Voice Service (with ITSP A or B), SP2 for the SP2 Voice Service (with ITSP A or B), or PP1 for the PDMS-SP Service.

The *number* to forward calls to must be in the final form that is acceptable by the service provider. The device doesn't apply any Digit Map or Call Routing Rules on it.

Call Forward Examples

The following are examples of correctly formatted call forward numbers to a number through the voice service, and through the PDMS-SP service:

```
SP1(14089991234)
```

```
PP1(ob200333456)
```

You can also set the call forward number to a **Phone** port (`ph`, `ph1`, or `ph2`) or to the AA (`aa`).

User Features Available on the Device

Learn about the user features that are available on the device.

NOTE: The star codes described in this section are the default on the device. You can modify them by following the steps in Program a Star Code on page 56.

Place a Call On the Primary Line

The Primary Line is the preferred line to use for outgoing calls. Users don't need to first dial a service route access code.

Using a phone connected to the **Phone** port of the device, you can place calls in numerous ways, including local and international calls, calls from recent calls lists or directories, or calls to contacts or favorites.

IMPORTANT: The phone number to enter needs to consist only of the phone number itself, with any area code, international dialing code, and country code only if required for the type of call.

- Depending on the type of phone, do one of the following:
  - Lift the handset from the cradle, enter the number, and press the **Dial** button or softkey.
  - Enter a number using the dialpad, press the speakerphone button.
  - Enter a number using the dialpad, press the headset button.

Call Forwarding

Call Forwarding allows you to send incoming calls to another number of your choosing.

You can forward calls to a number reachable from the VoIP service or the PDMS-SP network. You can enable the following types of call forwarding on the device:

- Call Forward All
- Call Forward on Busy
- Call Forward on No Answer

Enable Call Forward All

When you use Call Forward All, all calls are immediately forwarded to the number you indicate when you turn on the feature.

1. To enable Call Forward All, from a phone attached to the **Phone** port of your Poly ATA device, dial `*72`.

   You hear a prompt to enter the destination number.

2. Enter the number followed by the `#` key.

   You hear a confirmation tone.

3. To disable Call Forward All, dial `*73`.

   You hear a confirmation tone.

Enable Call Forward on Busy

When you use Call Forward on Busy, all calls are forwarded to the number you indicate only when you're already engaged in a call with your phone attached to the Poly ATA device.

1. To enable Call Forward on Busy, from a phone attached to the **Phone** port on your Poly ATA device, dial `*60`.

   You hear a prompt to enter the destination number.

2. Enter the number followed by the `#` key.

   You hear a confirmation tone.

3. To disable Call Forward on Busy, dial `*61`.

   You hear a confirmation tone.

Enable Call Forward on No Answer

When you use Call Forward on No Answer, all calls are forwarded to the number you indicate only when you don't answer the call with your phone attached to the Poly ATA device.

1. To enable Call Forward on No Answer, from a phone attached to the **Phone** port on your Poly ATA device, dial `*62`.

   You hear a prompt to enter the destination number.

2. Enter the number followed by the `#` key.

   You hear a confirmation tone.

3. To disable Call Forward on No Answer, dial `*63`.

   You hear a confirmation tone.

Caller ID - Name and Number

Caller ID allows you to see the number and, if available, the name of the person calling you.

You can use this information to decide whether or not to answer the call. You must have a phone or other device that supports caller ID to use this feature.

Call Waiting

Call waiting lets you take a second call that comes in when you are already on the phone with another party without having to disconnect to take the new call.

Since Call Waiting can interfere with fax calls already in progress, you should configure your fax machine to dial the Cancel Call Waiting code before it dials the destination fax machine.

You're on a call with the first party on a phone connected to the Poly ATA device. You hear a tone indicating there is a second call coming in.

1. To answer the second call, do one of the following:

   - Press the **Flash** button on the phone handset.
   - Depress and release the switch hook on the phone.

   The first party is placed on hold and you are connected to the second party.

2. To revert to the first call, repeat the step.

3-Way Calling

3-Way Calling allows you to talk to two parties at the same time with everyone on a telephone at a different location.

To use 3-Way Calling, when you are in a call with another party and want to add a second to the conversation, press the “flash” button or depress and release the switch hook on your phone. You are presented with a second dial tone and the first party is placed on hold. Dial the second party. When they answer, you can inform them that you intend to connect them with the first party (now on hold) and have a conference. At this point press the “flash” button or depress and release the switch hook on your phone. This will connect the first party, the second party and yourself. You can all continue to talk together.

Call Transfer (Attended)

You can transfer a call to a third party using the attended transfer capabilities of the device.

To use Attended Call Transfer, while in a call with the party to be transferred, press the “flash” button or depress and release the switch hook on your phone. You are presented with a second dial tone. The party to be transferred is placed on hold. Dial the transfer target. When the transfer target answers, you can inform them that you intend to connect them with the party on hold. At this point press the “flash” button or depress and release the switch hook on your phone. This will connect the party to be transferred, the transfer target and yourself. You can continue to talk together, as this is now a 3-way call, or you can hang up the phone and the other two parties will remain connected.

Nordic Style Feature Invocation

In this description of call waiting, 3-way calling, and call transfer operations, the way the features are invoked is referred to as N. America style. In Nordic regions (such as Sweden, Norway), the same features are invoked by hook flashing

followed by a digit 0, 1, 2, 3, or 4 to control more precisely which operations to apply to the calls.

For these regions, the devices can also be equipped with an **R** button for hook flashing. The commands issued to the device are referred to as R0, R1, R2, R3, and R4. Here's a summary of the operations:

Table 6-3 Nordic Style Feature Invocation

Commands	Operations	Scenarios
R0	Reject the second incoming call.	First call connected, second call ringing.
R1	End the first call. Resume or answer the second call.	First call connected, second call on hold or ringing.
R2	Hold the first call. Resume or answer the second call (swap calls).	First call connected, second call on hold or ringing.
R3	Keep the first call. Resume or answer the second call (conference).	First call connected, second call on hold or ringing.
R4	Transfer the second call peer to the first call peer.	First call connected, second call on hold or connected.

Select Nordic Style Feature Invocation

Change the method of invoking features including call waiting, 3-way calling, and call transfer operations, from N. America style to Nordic style.

1. In the system web interface, go to **Physical Interfaces** > **PHONE /VPort** > **Phone Settings**.
2. In the **Default** column, clear the check box for the `CallCommandSignalMethod` parameter.
3. In the **Value** column, select `Nordic Regions (R1, R2, …)`.
4. Select **Submit**.
5. Reboot your system when you complete your changes.

Caller ID Block (Anonymous Calling)

Caller ID Block allows you to mask your name and number information from appearing on the phone you are calling.

To use Caller ID Block for one call only, dial ***67** and then the destination number. To use Caller ID Block on a persistent basis, dial ***81** from the handset attached to the device. All calls will use the Caller ID Block feature until you cancel the Caller ID Block. To cancel Caller ID Block, dial ***82** from the handset attached to the device.

NOTE: This service feature requires ITSP support.

Automatic Call Back (Call Return)

Automatic Call Back, also called Call Return can be used to call back the last caller who called you without actually dialing their number.

To use Automatic Call Back, from the phone attached to the device, dial ***69**. The device will then attempt to use the previous callers Caller ID information to make the call.

Repeat Dialing

Repeat Dialing is useful when you call a number that is busy and you want to keep trying so that your call gets through when the far end is available.

Repeat dialing will continue to try the last number until the device can complete the call or Repeat dialing is canceled. To enable repeat dialing, from the phone attached to the device, dial ***05** and hang up. To cancel repeat dialing, from the phone attached to the device, dial ***06**.

Anonymous Call Block

Anonymous Call Block allows you to block calls from incoming callers when there is no identifying caller ID name or number.

Incoming calls are presented with a busy signal. To use Anonymous Call Block, dial ***77** on the phone attached to your device. To cancel Anonymous Call Block, dial ***87** on the phone attached to your device.

Do Not Disturb

Do Not Disturb (DND) allows you to set the phone to immediately forward calls made to your device to the number set up as your voicemail number / account.

If no voicemail account is set up, your device returns a busy signal to the caller until you turn off DND. To turn on DND, dial ***78** on the phone attached to your device. To turn off DND, dial ***79** on the phone attached to your device.

Message Waiting Indication - Visual and Tone Based

Message Waiting Indication allows you to be notified when there is a new voice message for you.

The device supports both Visual and Tone based Message Waiting Indication. With Tone-based Message Waiting Indication, you will know there is a message for you when you hear a “stutter” dial tone right when you first pick up the phone to make a call. Typically, this stutter tone is removed once you listen to your message(s). Visual-based Message Waiting Indication turns on a light or screen icon on your phone (or phone base station) when there is a message waiting for you. Typically, this light or icon goes dark when you have listened to your new message(s).

Speed Dialing of 99 OBi Endpoints or Numbers

The device supports Speed Dialing of 99 numbers.

These numbers can be associated with phones reachable via an Internet or the PDMS-SP network. Be careful with the Speed Dial Setup, as this will conflict with

the Speed Dials set up on the PDMS-SP portal. The Speed Dials that are set up on the PDMS-SP portal always overwrite anything set up via the device.

Phone Ports Collaborative Features

While **Phone 1** and **Phone 2** can function independently of each other, the device also offers some collaborative features to enable the ports work together as a mini phone system.

With the factory default digit map and call routing rules, you can dial a single "#" digit (the pound or hash key) to make a call from one **Phone** port to the other **Phone** port. Depending on the current state of the called phone, one of the following can happen:

- Case 1: If the called phone is idle (on-hook), it rings normally with a special Caller-ID that indicates the call is from the other **Phone** port.
- Case 2: If the called phone is already on a call, the calling phone barges in to join the call.
- Case 3: If the called phone is on-hook with a call on-hold, the calling phone picks up and resumes that call.
- Case 4: If the called phone is ringing, the calling phone picks up and answers that call.
- Case 5: For all other scenarios, the calling phone hears a busy tone.

You can prevent the calling **Phone** port from doing 2, 3, and 4, by setting the `EnablePhonePortBargeIn` parameter to `False` for that port. In that case, 2 becomes normal call-waiting on the called phone, but the calling phone hears a busy tone for 3 and 4.

Transfer an External Call from Phone 1 to Phone 2

You can transfer an external call from **Phone 1** to **Phone 2** in the usual way. While connected on an external call, hook flash and dial # to ring the other phone, then hang up to transfer the call when the called phone rings or answers.

Assign Incoming Calls to a Specific Phone Port

For incoming calls on any trunk (SP1 through SP4 or PDMS-SP Service), you can set the corresponding inbound call route to ring only **Phone 1** or **Phone 2** or both. The default inbound call routes are to ring both **Phone** ports.

Use Digit Maps and Outbound Call Routes

For outgoing calls, each **Phone** port has its own digit map and outbound call route configuration. These ensure that you have full flexibility in allocating trunks for making calls from each port independently. Each port can have a different primary line assigned. However, the default is to set the primary line to SP1 for both **Phone** ports.

Service Star Code Features

The device supports service features via the handset connected to the **Phone** port.

You can use the following Star Codes to access the indicated features. Poly Star Code-enabled features apply to all voice services.

*03, Request peer device to loopback media in the next outbound call

*04, Request peer device to loopback RTP packets in the next outbound call

*05, Tell device to periodically redial the last called number until the called party rings or answers

*06, Cancel the last repeat dial request

*07, Redial

*69, Call Return

*81, Block Caller ID (Persistent Mode)

*82, Unblock Caller ID (Persistent Mode)

*67, Block Caller ID (One Time)

*68, Unblock Caller ID (One Time)

*72, Call Forward All (Enter Number + #)

*73, Disable Call Forward All

*60, Call Forward on Busy (Enter Number + #)

*61, Disable Call Forward in Busy

*62, Call Forward on No Answer (Enter Number + #)

*63, Disable Call Forward No Answer

*77, Block Anonymous Calls

*87, Unblock Anonymous Calls

*56, Enable Call Waiting

*57, Disable Call Waiting

*78, Do Not Disturb - Turn On

*79, Do Not Disturb - Disable

*66, Repeat Dial

*86, Disable Repeat Dial

*74, Speed Dial Setup (Enter Speed Dial Number [1-99] then Telephone Number + #)

NOTE: Be careful with the Speed Dial Setup, as the device setup conflicts with the Speed Dials set up on the PDMS-SP portal. The Speed Dials that are set up on the PDMS-SP portal always overwrite anything set up via the device.

*75, Speed Dial Read-Back (Enter Speed Dial Number)

*76, Clear a Speed Dial

*96, Barge In

*98, Blind Transfer

*4711, Use G711 Only on the next outbound call

*4722, Use G722 Only on the next outbound call

*4729, Use G729 Only on the next outbound call

*4678, Use OPUS Only on the next outbound call

7 Star Code Features

Star codes are short sequences of digits that users enter where each sequence serves as a command to the device to perform a certain operation.

Each sequence usually starts with the star key (*) key followed by a 2-digit code (such as *69), hence the term star code. A typical operation that you can carry out is to set the value of one or more configuration parameters. The device allows you to issue a star code from the **Phone** port only; you issue a star code the same way you dial a number to make a call.

In the device, every star code and its operation are defined with a short star code script parameter. The set of star codes that can be dialed from the **Phone** port is collectively referred to as a star code profile.

The device has two star code profiles available in its configuration, known as **Star Code Profile A** and **Star Code Profile B**. Each profile has 42 star code script parameters, known as Code1 to Code42. You can select either A or B, or None if star codes aren't to be used.

Set the Star Code Profile

You can select a Star Code Profile (A, B, or None) for interpreting the star codes users enter on the phone.

Select which star code profile to use with the `StarCodeProfile` parameter.

1. In the system web interface, go to **Physical Interfaces** > **PHONE Port** > **Calling Features**.
2. In the **Default** column for the `StarCodeProfile` parameter, clear the check box.
3. In the **Value** column for the `StarCodeProfile` parameter, choose one of the following star code profiles:
   - **A**
   - **B**
   - **None** (if you aren't using a star code)
4. Select **Submit**.
5. Restart your system when you complete your changes.

Star Code Scripts

You can define a star code script with the help of a number of predefined variables and actions. Each variable represents one or one group of configuration parameters. An action can be checking or setting the value of a variable, collecting a phone number from the user, or calling a certain number.

Star Code Script Variables

Use the predefined star code script variables.

The general format of a **Phone** port-specific variable is *$var* and it applies to the current **Phone** port where the star code is entered. The general format of a trunk-specific variable is *TK($var)*, where *TK* is the abbreviated name of a trunk (SP1, SP2, or PP1). If *TK* is not specified for a trunk-specific variable, it implies all the applicable trunks in the system.

Note that SP1 is the SP1 Service, SP2 the SP2 Service, and PP1 the PDMS-SP Service. Each service is also referred to as a "trunk" in this document.

Variable names are case-insensitive.

Here is a list of the supported *$var* variables:

Variable names are case-insensitive.

Table 7-1 Supported $var Variables

Variable	Meaning
$CFA	Call forward unconditional enable (trunk-specific; admissible value: 0 for disable, 1 for enable)
$CFB	Call forward busy enable (trunk-specific; admissible value: 0 for disable, 1 for enable)
$CFN	Call forward no-answer enable (trunk-specific; admissible value: 0 for disable, 1 for enable)
$CFAN	Call forward unconditional number (trunk-specific; admissible value: a token representing a call forward number)
$CFBN	Call forward busy number (trunk-specific; admissible value: a token representing a call forward number)
$CFNN	Call forward no-answer number (trunk-specific; admissible value: a token representing a call forward number)
$MWS	Message waiting state (trunk-specific; admissible value: 0 for no new messages, 1 for one or more new messages)
$DND	Do-not-disturb enable (trunk-specific; admissible value: 0 for disable, 1 for enable)
$BAC	Block-anonymous caller enable (trunk-specific; admissible value: 0 for disable, 1 for enable)
$BCI	Block outbound caller-ID enable (trunk-specific; admissible value: 0 for disable, 1 for enable)
$CWA	Call-waiting enable on this **Phone** port (port-specific; admissible value: 0 for disable, 1 for enable)
$BCI1	Block caller-ID once in the next call on this **Phone** port (port-specific; admissible value: 1 for enable)
$UBCI1	Unblock caller-ID once in the next call on this **Phone** port (port-specific; admissible value: 1 for enable)
$LBM1	Loopback media (audio samples) once in the next call on this **Phone** port (port-specific; admissible value: 1)
$LBP1	Loopback RTP packets once in the next call on this **Phone** port (port-specific; admissible value: 1)

Table 7-1 Supported $var Variables (continued)

Variable	Meaning
$BAR1	Barge-In once in the next call on this **Phone** port (port-specific; admissible value: 1)
$NOEC1	Disable echo canceller once in the next call on this **Phone** port (port-specific; admissible value: 1)
$NOJI1	Disable jitter buffer adjustment once in the next call on this **Phone** port (port-specific; admissible value: 1)
$IBDT	Enable in-band DTMF transmission once in the next call on this **Phone** port (port-specific; admissible value: 1)
$BCLR	Clear all blocked callers (trunk-specific; admissible value: 1)
$CIDG	Enable Generate Caller ID Generation on this **Phone** port (port-specific; admissible value: 1 for enable, 0 for disable)
$CWCIDG	Enable CWCID Generation on this **Phone** port (port-specific; admissible value: 1 for enable, 0 for disable)
$MWIG	Enable MWI (Stutter Tone) Generation on this **Phone** port (port-specific; admissible value: 1 for enable, 0 for disable)
$VMWIG	Enable VMWI Generation on this **Phone** port (port-specific; admissible value: 1 for enable, 0 for disable)
$BXRN	Blind transfer number for the current call on this **Phone** port (port-specific; admissible value: a number representing the blind transfer target). As soon as a complete blind transfer target number is collected, the device blind transfers the current call peer to the target number.
$CDM1	Codecs to enable in the next call on this **Phone** port (temporarily overriding any codec preferences in device configuration) (port-specific; admissible value: An 8-bit unsigned number where each bit of its value represents one audio codec) • Bit0(LSB) = G711u • Bit1 = G711a • Bit2 = G726r16 • Bit3 = G726r24 • Bit4 = G726r32 • Bit5 = G726r40 • Bit6 = G729
$LDN	Last dialed number on this **Phone** port (for redial) (port-specific; read-only)
$LCR	Last caller's number on this **Phone** port (for call return) (port-specific; read-only)
$SPD[n]	Number for the speed dial *n* (n = 1 - 99) (global; admissible value: literal or token representing a phone number)
$CODE	The digit(s) representing the variable part of a star code (see examples below; read-only)

Star Code Script Actions (ACT)

The general format of an action in a star code script is ACT(par, par, ...).

You can set multiple variables with multiple set() actions with a single star code. Action names are case-insensitive.

The following actions are supported:

Table 7-2 Star Code Script Actions (ACT)

Script	Actions
`set(VAR,token)`	Sets the given `VAR` to the value represented by `token`.
`call(token)`	Calls the number represented by `token`. • *PHONE Port* **::OutboundCallRoute** is applied when making the call (but not the **DigitMap**).
`rpdi(token)`	Repeat-dials the number represented by `token`.
`coll(VAR)`	Collects a number from the user and stores it as the value of the parameter(s) represented by VAR. • The number is collected with *PHONE Port* **::DigitMap** applied.
`say(token)`	Announces the value represented by `token`. Values are announced as a list of letters or numbers, where `token` can be a literal such as `1234`, or another variable, such as `$CFAN` or `SP1($CFBN)`)

Star Code Script Format

The general format of a star code script is `code, name, action1, action2, action3,...`

Table 7-3 Star Code Script Format

Script	Actions
`code`	The star code, such as `*72`. It can contain a variable part enclosed in parentheses, such as `*74(x|xx)`. The variable parts as entered by the user are stored in the variable `$code`.
`name`	Descriptive name of the function of this star code, such as Call Forward Unconditional.
`action1, action2,...`	Valid action with parameters

Actions are carried out one-by-one in the order as specified in the script.

Restrictions:

- At most 1 `coll` action per code.
- Either 1 `say` or 1 `call` action at most per code, and it must be the last action in the script.

Star Code Script Examples

The following examples are taken from some of the default star code scripts in the device.

Table 7-4 Star Code Script Examples

Star Code Script	Description
***69**, Call Return, `call($LCR)`	Calls the number of the last caller who rang the **Phone** port.
***07**, Redial, `call($Ldn)`	Redials the last dialed number.
***72**, Call Forward Unconditional, `coll($cfan),set($cfa,1)`	Collects a number from the user according to the **DigitMap**, then sets the `CallForwardUnconditionalNumber` on all trunks to the collected value, and sets the `CallForwardUnconditionalEnable` on all trunks to `Yes`.
***72**, Call Forward Unconditional SP1, `coll(SP1($cfan)),set(SP1($cfa),1)`	To modify the script to enable `CallForwardUnconditional` on SP1 only, change it to:
***67**, Block Caller ID Once, `set($BCI1,1)`	Enables masking of caller ID information once for the next call on any trunk.
***99**, Disable Echo Canceller For One Call, `set($Noec1,1)`	Disables the Echo Canceller for one call on the current **Phone** port.
***74(x|xx)**, Set Speed Dial, `coll($Spd[$code])`	After the user dials *74, the device expects one or two more digits from the user, which represent a speed dial slot index (1 to 99). The 1- or 2-digit variable part is stored in the variable `$code`. The device then plays a prompt tone and proceeds to collect a number from the user according to the **DigitMap**. Finally the device stores the collected number in the given speed dial slot. If the slot already has a number specified, it is overwritten quietly with the new value.
***75(x|xx)**, Check Speed Dial, `say($Spd[$code])`	After the user dials *75, the device expects one or two more digits from the user, which represent a speed dial slot index (1 to 99). The 1- or 2-digit variable part is stored in the variable `$code`. The device then announces the number stored in the speed dial slot, or says "not available" if the slot is empty.

For more information on Star Code parameters, see the Star Code Profile Parameters table in the *Poly ATA 400 Series Parameter Reference Guide*.

Program a Star Code

Program star codes for any enabled feature in addition to the default star codes available.

1. In the system web interface, go to **Star Codes** > **Star Code Profile N**.
2. In the **Default** column, clear the check box for a Parameter Name with an empty value column.

3. In the **Value** column, enter a star code script in the following format: `code, name, action1`

   For example, for Code30, the star code script is `*01, Page Group 1 Talk, pg1tx`. Using the star code `*01` sends a page to Group 1.

4. Select **Submit**.

5. Restart your system when you complete your changes.

8 Status Pages

The system web interface provides you with status information to help you monitor your device.

System Status

The system web interface provides you with status information to help you monitor your devices.

The *System Status* page is divided into several sections:

- WAN Status
- Wi-Fi Status
- Product Information
- SP1 - SP4 Service Status
- PDMS-SP Service Status
- OBiTALK Service Status

View WAN status

You can view the status of the WAN (Ethernet) to see information including the assigned IP address, default gateway, and subnet mask.

- In the system web interface, go to **Status**.

  Under **WAN Status**, the information for the WAN displays.

View Wi-Fi status

You can view the Wi-Fi status of the OBiWiFi5G dongle to see information including the assigned IP address, default gateway, and subnet mask.

OBiWiFi Configuration

- In the system web interface, go to **OBiWiFi Configuration**.

  Under **WiFi Settings**, the Wi-Fi status information for the OBiWiFi5G dongle displays.

Product Information

You can view basic product information about the Poly ATA device, as well as the system up-time with the last reboot reason code in parentheses.

- In the system web interface, go to **System** > **Product Information**.

  Under **Product Information**, the information for the ATA displays.

The reboot reason codes are defined in the following table.

Table 8-1 Reboot Reason Codes

Reason Code	Description
0	Reboot on power cycle.
1	Operating system reboot.
2	Reboot after firmware update by provisioning or phone (***6).
3	Reboot after new profile invoked.
4	Reboot after parameter value change or firmware has changed and invoked by the system web interface.
5	Reboot after factory reset using the device hardware PIN.
6	New profile invoked AND profile URL changed.
7	Reboot from SIP Notify (Reserved).
8	Reboot from telephone port (IVR).
9	Reboot from system web interface—no change in parameter values or firmware.
10	Reboot during PDMS-SP signup.
11	Reboot during PDMS-SP signup.
12	Reboot after DHCP server offers IP, GW-IP, and/or netmask different from what the device is currently using.
13	Reboot on data networking link reestablishment.
15	Reboot from firmware update via provisioning.
16	Reboot for DHCP renewal.
29	Reboot from LLDP-MED change.

View SP*n* Services Stats (*n* = 1, 2, 3, 4)

You can view the SP*n* service statistics to see information about the current state of the service with regard to its configuration (or not), and, if configured, its registration status.

If there are problems with the registration or authentication of the device with a prescribed service, the SIP 4*xx* error message is displayed here. This information is useful for troubleshooting issues with SIP-based services.

1. In the system web interface, go to **Status** > **SP Services Stats**.
2. Scroll down to the **SP** *n* **Service**.

   The information for the **SP** *n* service displays.

View OBiTALK Service Status

View the current status of your OBiTALK service.

The status of the OBiTALK Service includes the following values:

- Status - Possible values are:

  - Normal (User Mode): The service is functioning normally.
  - Backing Off: The service is currently down, and the device is taking a short pause before retrying the connection.
- CallState - Possible values are:
  - *N* Active Calls, where *N* = 0, 1,.., as many as the maximum number of calls allowed in the configuration.

Call status

The Call Status page shows a number of running call statistics and state parameters for each active call currently in progress.

For each entry on the call status page, the following buttons may be available:

- **Remove**: This button is available for all calls. Pressing this button ends that call.
- **Record**: This button is available for calls involving the Phone port only. Pressing this button allows you to record the current conversation in an audio (.au) file.

Call history

The Call History page shows the last 400 calls made with the device.

Detailed call information is available, including what terminals were involved, the name (if available) of the Peer endpoints making the call and the direction / path the call took.

The Call History page also captures what time various events took place.

The Call History can be saved at any time by clicking on the “Save All” button. The Call History can be saved as an XML formatted file called `callhistory.xml`.

SP Services Stats

See the *SP Services Stats* page for the statistics relevant to SP*n*, where *n* = 1, 2, 3, 4).

For information on the parameters displayed on this page, see the SP Services Status table in the *Poly ATA 400 Series Parameter Reference Guide*.

Phone Port Status

See the *PHONE Port Status* page for the statistics relevant to the **Phone** *n* ports.

For information on the parameters displayed on this page, see the Phone Port Parameters table in the *Poly ATA 400 Series Parameter Reference Guide*.

9 Device Settings

Repeat Dialing Service

Repeat dialing service is when a user dials `*05` to tell the device to redial the last called number repeatedly while the phone is on-hook, until the called party rings or answers.

When the called party rings or answers, the device rings the **Phone** port and the user can pick up the attached handset to talk to the called party. Typically, the last called number was busy when the user invokes this feature, but the device allows this feature for all cases.

This feature can be controlled with the following parameters (go to **Phone *N*> Port > Calling Feature** in the system web interface):

- `RepeatDialInterval` = the minimum number of seconds between each redial. Default is 30 seconds.
- `RepeatDialExpires` = the maximum duration in seconds when the repeat dialing remains active. Default is 1800 seconds.

Dial `*06` to cancel Repeat Dialing. Only one repeat dial request is supported. Dialing `*05` while a repeat dial is in progress is rejected with a fast busy tone. If `*05` is accepted, the device plays a normal dial tone.

Notes:

- The first redial happens 5 seconds after the phone is on-hook following `*05`.
- When the phone is off-hook or rings for an incoming call, the device pauses redial and cancels the call if it's already dialed but the peer device isn't ringing yet.
- As soon as the phone goes on-hook or ringing stops without any calls on hold, repeat dialing resumes in 5 seconds.
- If the called party answers before the local caller, the device sends a normal ringback tone over RTP to the called party.
- The ring for alerting the local user when the called party rings or answers is taken from the outgoing trunk's **RepeatDialRing** parameter.
- Repeat Dial calls aren't logged to call history, except the last and successful one when the called party rings or answers.

For more information on **Phone *N*> Port** parameters, see the Phone Port Parameters table in the *Poly ATA 400 Series Parameter Reference Guide*.

Codec Profile Features

There are two codec profiles available on the devices.

They are selectable per trunk (SP1/SP2/SP3/SP4/PDMS-SP). To select a codec as the preferred codec in this profile, set the priority of that codec to be highest among all the enabled codecs in this profile. Each of the SP1, SP2, SP3, SP4, and PDMS-SP services can be assigned a codec profile in its corresponding configuration. The codec list to use when setting up a call on the underlying service is formed from the list of enabled codecs in the chosen profile and ordered according to the assigned priorities in the profile.

For more information on codec profile parameters, see the Codec Profile Parameters table in the *Poly ATA 400 Series Parameter Reference Guide*.

User Settings

Configure the user settings for your device.

Configure speed dial numbers

Set up speed dial numbers for your device. Each Poly ATA device supports 99 speed dial numbers.

The 99 speed dial slots are numbered from 1 to 99. You can call a speed dial number by dialing a 1- or 2-digit number corresponding to the slot number from the handset connected to the **Phone** port or via the Auto Attendant.

NOTE: You can't use the 2-digit numbers "01", "02", ..., "09"; you must dial the 1-digit number "1", "2", ..., "9" for slot numbers 1-9.

You can set the speed dial values using the configuration web page, by remote provisioning, or through star codes. See Service Star Code Features on page 49 in this document for more details.

1. In the system web interface, go to **User Settings** > **Speed Dials**.
2. In the row for each speed dial number that you want to configure, clear the check boxes in the **Default** columns.
3. In the **Number or URL** column, enter the number that you normally dial, with or without any service access code prefix, such as `**9200112233`, `**214089991123`, `4280913`, and so forth.

   The number may also include explicit trunk information with the general format `TK(number)`, where `TK`= `SP1`, `SP2`, or `PP`. For example, `PP(ob200112233)`, `SP2(14089991123)`, and so forth.

   If trunk information isn't specified in the speed dial entry, the device applies `DigitMap` and `OutboundCallRoute` when making the call. Otherwise, neither `DigitMap` nor `OutboundCallRoute` is applied.
4. In the **Name** column, enter the name that you want to associate with the speed dial.
5. Select **Submit**.
6. Reboot your system when you complete your changes.

Use a Speed Dial Number as Ad Hoc Gateway

If an external gateway doesn't require authentication, store its access number in one of the 99 speed dial slots. Then use the speed dial number to allow ad hoc direct dialed gateway calls.

Store a gateway on a speed dial number.

NOTE: You can only use gateways that are accessed with an OBi number.

- Dial the gateway's speed dial, followed by a `*`, followed by the target number.

  `<gateway-speeddial>` `*` *`<target-number>`* . For example, you save the gateway access number `pp(ob200333456)` at speed dial 8. You can dial `8*14085551234` to call `14085551234` using the given gateway.

10 Configuring Network Settings

Configure the device to connect to your wireless network.

Network Connectivity

Poly ATA devices offer two interfaces for networking: Ethernet (indicated as **LAN** in the device and as **WAN** in the system web interface) and Wi-Fi (indicated as **OBiWiFi** and **WiFi** in the system web interface).

Configure the Ethernet Ports

Configure the two Ethernet ports from the system web interface. The number of Ethernet ports depends on the model of ATA device.

1. In the system web interface, go to **System Management** > **WAN Settings**.
2. In the **Default** column, clear the check box for the following parameters: **Switch Port** > **Speed** and **PC Port** > **Speed**.
3. Configure the following settings:

Parameter	Values
Switch Port > **Speed**	• Auto • 100 Full • 100 Half • 10 Full • 10 Half Poly recommends using `Auto`.
PC Port > **Speed**	• Auto • 100 Full • 100 Half • 10 Full • 10 Half Poly recommends using `Auto`.

4. Select **Submit**.
5. Restart your system when you complete your changes.

Configure the WAN Interface

The LAN interface on the device refers to the internal Ethernet switch port connected directly to the device processor.

1. In the system web interface, go to **System Management** > **WAN Settings**.
2. Configure the following settings:

Table 10-1 WAN Settings

Setting Group	Description
`VLAN`	The devices support VLAN tagging in compliance with 802.1p/q. If you enable `VLANEnable`, the device tags outbound traffic according to the `VLANID` and `VLANPriority` parameters. The devices ignore inbound traffic that doesn't belong to the same VLAN. To enable VLAN discovery using DHCP, set **VLANDiscovery** to **Fixed** (to use the standard DHCP options for VLAN discovery - 128, 144, 157, 191) or **Custom**. If set to **Custom**, set **VLANDiscoveryOption** to the desired custom DHCP Option.
`LLDP`	The devices support LLDP-MED to automatically discover network policy (VLAN and DSCP) settings and perform other related handshake functions.
`IP Address Assignment`	The devices support different methods of acquiring an IP address assigned to its WAN interface. Configure the method using the `AddressingType` parameter, which can have one of the following values: • `DHCP`: Request address assignment from a DHCP server. • `Static`: Use the statically assigned IP address, subnet mask, and default gateway from the `IPAddress`, `SubnetMask` and `DefaultGateway` parameters, respectively.
`DNS Servers`	Specify up to two DNS servers to use with the WAN interface using `DNSServer1` and `DNSServer2`. **NOTE:** If the DHCP offer includes DNS servers, the device takes as many as 16 servers from the list and uses them together with the explicitly configured servers.
`Cisco Discovery Protocol (CDP)`	The devices support CDP for automated network setting discovery. Common values included in CDP broadcast messages are: • Device Type and Model • Duplex/Speed Setting • VLAN Setting • PoE Class (Power Draw)

3. Select **Submit**.
4. Restart your system when you complete your changes.

Set the 802.1X Authentication Mode

All Poly devices support 802.1X authentication.

1. Depending on whether you are configuring 802.1X Authentication Mode for Ethernet (wired) connection or for Wi-Fi, choose one of the following:

   • In the system web interface, go to **System Management** > **WAN Settings** > **Internet Settings**.

- In the system web interface, go to **OBiWiFi Configuration** > **WiFi Settings**.

2. In the **Default** column, clear the check box for **802_1XMode**, then select one of the following modes from the drop-down menu:
   - Disable
   - MD5
   - TLS
   - TTLS/MSCHAPv2
   - PEAP-MSCHAPv2 (optional for all parameters)
3. Depending on the selected mode, configure the following additional authentication parameters:

Table 10-2 802.1X Mode Parameters

Parameter	Description	(EAP) MD5	(EAP) TLS (1.0)	TTLS/ MSCHAPv2
`802_1XIdentity`	The username. If you don't need a username, set the value as an empty string.	Required	Required	Required
`802_1XPassword`	The password or passphrase. If you don't need a password or passphrase, set the value as an empty string.	Required	Required	Required
`802_1XAnonymousID`	When empty, the device doesn't use an anonymous identity in authentication.	Not required	Required	Required
`802_1XTLSSecurityProfile`	Security profile for the 802.1X authentication.	Not required	Required	Not required

4. Select **Submit**.
5. Restart your system when you complete your changes.

Web Proxy Server

Configure the device to send outbound requests through a web proxy.

Configure Web Proxy Server

Configure the web proxy server settings.

1. In the system web interface, go to **System Management** > **Device Admin**.
2. Under **HTTP Client**, configure the following parameters:

Table 10-3 HTTP Client Parameters

Parameter	Description
`ProxyServer`	Enter the FQDN or IP address of the web proxy.

Table 10-3 HTTP Client Parameters (continued)

Parameter	Description
ProxyServerPort	Enter the port to connect to the web proxy.
ProxyAuthUsername	Enter the username to authenticate with the web proxy.
ProxyAuthPassword	Enter the password to authenticate with the web proxy.
BypassProxyServerForLocalAddresses	Enable to bypass the web proxy for local addresses.
BypassProxyForSubnets	Enter a comma-separate list of internal subnets to bypass the web proxy, for example, 10.10.10.0/24,192.168.0.0/16

3. Select **Submit**.
4. Reboot your system when you complete your changes.

DNS Lookup

The following DNS behavior applies to both the WAN and Wi-Fi network interfaces.

Configure Lookup Order

When your devices obtain DNS servers from both DHCP and statically configured values, the device queries all the servers of one type before moving to the other type. Configure the device to control the order the device queries the server types.

1. In the system web interface, go to **System Management** > **WAN Settings**.
2. Under **DNS Control**, clear the check box in the **Default** column for DNSQueryOrder.
3. In the **Value** column, select the available DNS servers for the parameter in the order you want them to be queried by the device.
4. Select **Submit**.
5. Restart your system when you complete your changes.

Configure DNS Query Delay

When there are multiple DNS servers available, the device queries as many DNS servers as necessary to resolve a domain name. Configure the device to insert a short delay between each query to stop once the device receives a positive response.

1. In the system web interface, go to **System Management** > **WAN Settings**.
2. Under **DNS Control**, clear the check box in the **Default** column for DNSQueryDelay.

3. In the **Value** column, select a value from the drop-down menu to set a delay.

   The query order follows the `DNSQueryOrder` setting. If you set the delay to `0`, the device queries all the DNS servers at the same time.

4. Select **Submit**.

5. Restart your system when you complete your changes.

Define Local DNS Records

Define as many as 32 local DNS records in the device configuration.

Once you define the DNS records, enable the device to search through these records before hitting the external DNS services when attempting to resolve a domain name. These records can be A or SRV records.

To define a local DNS A record, use the following format:

```
Name=IP1,IP2,...
```

Where:

- `Name` is the FQDN.
- `IP` is the IP address that the FQDN resolves to.

For example:

```
sbc.example.com=192.168.15.118,192.168.15.108
```

To define a local DNS SRV record, using the following format:

```
_service._proto.name={host1:port1,priority1,weight1},
{host2:port2,priority2,weight2},...
```

Where:

- `service` is the name of the service (for example, sip).
- `proto` is the transport protocol of the service (for example, udp).
- `name` is the domain name for the record.
- `host` is the host name of the machine providing the service (for example, `sbc.example.com`).
- `port` is the port where the service is found (for example, 5060).
- `priority` is the priority of the target host.
- `weight` is the relative weight for records with the same priority.

NOTE: The only way to provide a list of redundant servers to the device is through the use of DNS A or DNS SRV records.

1. In the system web interface, go to **System Management** > **WAN Settings**.

2. Under **Local DNS Records**, clear the check box in the **Default** column for each **Local DNS Record** you want to configure.
3. In the **Value** column, enter a local DNS record for each parameter.
4. Select **Submit**.
5. Restart your system when you complete your changes.

Configure the Local DNS Record Mode

Select the record mode to configure local DNS record handling.

1. In the system web interface, go to **System Management** > **WAN Settings**.
2. In the **Value** column for the `LocalDNSRecordMode` parameter, select one of the following:
3. Table 10-4 **Local DNS Record Mode Options**

Mode	Description
Persistent Cache	The local configuration is used and no query to external DNS servers is attempted.
Backup Record	The local configuration is used only when the queries to external DNS servers fail.

3. **Optional:** To configure the default TTL for each local record in the **Backup Record** mode, enter the duration in seconds for the `LocalDNSRecordTTL` parameter.

   Choose a value between 60 seconds and 604,800 seconds (one week). The default value is 120 seconds. After the time elapses, the device resends the DNS requests to the external DNS servers.
4. Select **Submit**.
5. Restart your system when you complete your changes.

NTP Servers and Local Time

The device keeps track of the current time by querying NTP servers (using SNTP).

Configure NTP Servers

Configure up to two NTP servers.

1. In the system web interface, go to **System Management** > **WAN Settings**.
2. Under **Time Service Settings**, clear the check box in the **Default** column for `NTPServer1` and `NTPServer2`.
3. In the **Value** column, enter the host names or IP addresses of the NTP servers.
4. Select **Submit**.
5. Restart your system when you complete your changes.

Disable SNTP Discovery

By default, the device discovers the SNTP server using DHCP option 42 and discovered servers take precedence. Disable SNTP discovery in DHCP and use the configured SNTP servers instead.

1. In the system web interface, go to **System Management** > **WAN Settings**.
2. Under **DHCP Client Settings**, clear the check box in the **Default** column for `ExtraOptions`.
3. In the **Value** column, delete `42` from the extra options list for `ExtraOptions`.
4. Select **Submit**.
5. Restart your system when you complete your changes.

Set the Local Time Zone

The device queries the NTP servers once per hour to update the current time, and the device uses its own local clock in between NTP refreshes.

1. In the system web interface, go to **System Management** > **WAN Settings**.
2. Under **Time Service Settings**, clear the check box in the **Default** column for `LocalTimeZome`.
3. In the **Value** column, select your local time zone from the drop-down menu for the `LocalTimeZone` parameter.
4. Select **Submit**.
5. Restart your system when you complete your changes.

Enable Daylight Saving Time

Enable daylight saving time to enable the devices to adjust automatically when daylight saving time starts and ends.

1. In the system web interface, go to **System Management** > **WAN Settings**.
2. Under **Time Service Settings**, clear the check box in the **Default** column for `DaylightSavingTimeEnable`.
3. In the **Value** column, select the check box to enable daylight saving time.
4. Select **Submit**.
5. Restart your system when you complete your changes.

Specify Start and End Rules for Daylight Saving Time

Set the start and end rules so the device automatically adjusts for daylight saving time.

1. In the system web interface, go to **System Management** > **WAN Settings**.
2. Under **Time Service Settings**, clear the check box in the **Default** column for `DaylightSavingTimeStart` and `DaylightSavingTimeEnd`.

3. In the **Value** column, enter the start and end dates for `DaylightSavingTimeStart` and `DaylightSavingTimeEnd`.

   The format for the date is `mon/day/weekday/h:m:s` using the following values:

   Table 10-5 Date and Time Format

Variable	Value
mon	1 to 12
day	1 to 31 or -1 to -31 (if counting from the end of the month)
weekday	0 for the exact day 1 = Monday 2 = Tuesday 3 = Wednesday 4 = Thursday 5 = Friday 6 = Saturday 7 = Sunday
h:m:s	hour, minute, second

4. Select **Submit**.
5. Restart your system when you complete your changes.

Configure Amount of Time to Adjust for Daylight Saving Time

Configure the amount of time to adjust when daylight saving time is in effect.

1. In the system web interface, go to **System Management** > **WAN Settings**.
2. Under **Time Service Settings**, clear the check box in the **Default** column for `DaylightSavingTimeDiff`.
3. In the **Value** column for `DaylightSavingTimeDiff`, enter the amount of time to adjust for when daylight saving time takes effect.

   The format is `h:m:s` or `-h:m:s`.
4. Select **Submit**.
5. Restart your system when you complete your changes.

DHCP Options

Configure Additional DHCP Options

Set up the additional options that the device tries to extract from the DHCP offer.

The additional options are a comma-separated list of option numbers. The phone doesn't recognize any other option numbers.

1. In the system web interface, go to **System Management** > **WAN Settings** > **DHCP Client Settings**.
2. Under **DHCP Client Setting**, clear the check box in the **Default** column for the `ExtraOptions`.
3. In the **Value** column, enter the extra DHCP options in a comma-separated list.

   If you use DHCP options 66, 150, 159, 160 or 161 for ITSP provisioning server redirect, make sure that these values are included in **ExtraOptions**.
4. Select **Submit**.
5. Restart your system when you complete your changes.

Configuring Wi-Fi Settings

Poly ATA devices support Wi-Fi via the dongle.

OBiWiFi5G Wireless USB Adapter

OBiWiFi supports the 802.11 b/g/n wireless standards so that you can use an OBiWiFi5G Wireless Adapter with the USB port of the devices.

From an IP routing point of view, OBiWiFi is an additional WAN interface. If you connect both WAN interfaces (Ethernet port and OBiWiFi), the traffic destined to the WAN side routes through the Ethernet interface only, unless both of the following conditions are true:

- The WAN (Ethernet) interface and the OBiWiFi are on different subnets.
- The destination address is on the same subnet as the OBiWiFi.

NOTE: When using Wi Fi only for network connectivity, connecting another device to the PC port, or daisy-chaining, isn't supported.

Connect to a WiFi Access Point

Connect an dongle to the USB port on the device. Then scan for and connect to access points (APs) in the neighborhood.

The *WiFi Scan* page offers a familiar user interface to let you scan for and connect to access points.

1. In the system web interface, go to **OBiWiFi Configuration** > **WiFi Scan**.
2. To connect to one of the available APs, press the **Scan for Networks** button, then select the name of an AP.
3. If the AP requires authentication but the device doesn't have any valid credentials, you must enter a password or passphrase. Then, press **Connect** to continue.
4. If your AP doesn't show up as a listed network on this page, perhaps its SSID isn't broadcast. You can enter its SSID and security credentials manually by pressing the **Add a Network** button.

Configure the Wi-Fi Interface

Poly ATA devices support Wi-Fi via the wireless network adapter.

Connect the adapter to the USB port on the device.

NOTE: VLAN and LLDP features aren't available on Wi-Fi.

1. In the system web interface, go to **OBiWiFi Configuration** > **WiFi Settings**.
2. Configure the following settings:

Table 10-6 WiFi Settings

Setting Group	Description
IP Address Assignment	The devices support different methods of acquiring an IP address assigned to its Wi-Fi interface. Configure the method using the `Basic Settings::AddressingType` parameter, which can have one of the following values: • `DHCP`: Request address assignment from a DHCP server. • `Static`: Use the statically assigned IP address, subnet mask, and default gateway from the `WAN Settings - Internet Settings::IPAddress`, `SubnetMask` and `DefaultGateway` parameters, respectively.
DNS Servers	You can specify up to two DNS servers to use with the Wi-Fi interface using `Internet Settings::DNSServer1` and `DNSServer2`. **NOTE:** If the DHCP offer includes DNS Servers, the device takes as many as 16 servers from the list and uses them together with the explicitly configured servers.

3. Select **Submit**.
4. Restart your system when you complete your changes.

11 Call Routing

Call Routing is the process by which the device sets up a call bridge or an endpoint call based on such information as the trunk on which the call originates, the caller's number, the called number, etc.

Call Routing Rules are parameters used to instruct the device how to route calls. A call can transform into a call bridge or an endpoint call after being routed by the device according to the given routing rules.

Every call has to originate from somewhere. From the device's perspective, calls originated from the trunk side are considered Inbound Calls, while calls originated from an endpoint are Outbound Calls. The call routing rule syntaxes for inbound calls and outbound calls are slightly different, and are explained in the following section.

Call Routing Rule configuration relies heavily on digit maps. If you aren't familiar with how digit maps work, see the Digit Map Configuration on page 80 section in this document first.

Inbound and Outbound Call Routing

Understand the call routing rules used by the device for handling inbound and outbound calls.

Inbound Call Route Configuration

Inbound Call Routes are rules to tell the device how to handle an inbound call. The options are sending it to the **Phone** port, and ringing the attached phone, sending it to the Auto Attendant for further routing interactively with the caller, or making another call on a specific trunk to bridge with this call.

An inbound call route is a comma-separated list of rules where each rule is also surrounded by a pair of curly braces `{}`. No extra white spaces are allowed.

The general format of a route is:

```
InboundCallRoute := {rule},{rule},....
```

If there's only one rule in the route, you can use omit the curly braces and use this format:

```
InboundCallRoute := rule.
```

A rule has the following format:

```
rule := peering-list : terminal-list
```

The following table shows the rule formats.

IMPORTANT: An inbound call matches a rule if its caller-number/callee-number matches one of the peering objects of the rule. Peering objects are tested in the order left and right, and the first matched peering object wins. Rules are also checked in the order left to right, and the first matched rule wins. Therefore it's important that you place the more specific rules first in the `InboundCallRoute` if multiple rules can potentially match the same inbound call.

Table 11-1 Rule Formats

Rule	Format	Notes
`peering-list :`	`peering,peering,…`	Comma-separated list of 0 or more peering objects `Peering-list` is optional in **InboundCallRoute**. If the peering-list is empty, the succeeding ':' can be omitted also. An empty peering-list implies a single peering object whose caller object list matches any caller number. That is, the following **InboundCallRoutes** are all equivalent: • `ph` • `{ph}` • `{:ph}` • `{?|@>@:ph}`
`terminal-list :`	`terminal,terminal,….`	Comma-separated list of 0 or more terminal objects `terminal-list` can be empty, which means to block this call. The preceding ':' can't be omitted. As many as four terminals can be specified in the list. The device calls the listed terminals simultaneously. This operation is known as forking the call. A terminal can be a trunk or an endpoint. Abbreviated terminal names are case-insensitive.
`peering :`	`caller-list > callee-list`	`caller-list` in a peering object can be empty. It implies the caller-list `@|?`, meaning any caller number including anonymous. The succeeding '>' can't be omitted if `caller-list` is empty but not the `callee-list`. `callee-list` in a peering object can be empty. It implies the callee object `@`, meaning any called number. The preceding '>' can be omitted if `callee-list` is empty.
`caller-list :`	`caller|caller|caller|…`	Vertical bar-separated list of 0 or more caller objects

Table 11-1 Rule Formats (continued)

Rule	Format	Notes
`callee-list :`	`callee|callee|callee| …`	Vertical bar-separated list of 0 or more callee objects
`caller :`	`number` OR `embedded-digit-map` OR `?` OR `@`	`?` = anonymous, `@` = any number but anonymous `number` is a literal string, such as `14089991234`.
`callee :`	`number` OR `embedded-digit-map` OR `@`	
`terminal :`	`PHx` OR `AAx` OR `SPx(arg)` OR `PPx(arg)`	The `arg` object is optional. If omitted, it implies the `arg` with the target `$2` and no `cid`. If `arg` is omitted, the succeeding parentheses `()` can be omitted also.
`arg :`	`cid > target`	The `cid` object inside an `arg` object is optional. If omitted, it implies no caller-ID spoofing when calling on the specified trunk. The succeeding '>' can be omitted if `cid` is omitted. The target object inside an `arg` object is optional. If omitted, it implies the target `$2`, which means to call the original called number after applying any necessary digit map transformation implied by the rule. The preceding '>' can't be omitted if `target` is omitted but `cid` is not.
`x :`	`1` OR `2` OR `3`…	Where applicable; can omit if x = 1
`cid :`	`spoofed-caller-number` OR `$1`	`spoofed-caller-number` is a literal string, such as `14081112233`, to be used as the caller number for making a new call on the specified trunk. `$1` is an internal variable containing the value of the caller number of this inbound call, after any digit map transformation in the matched caller object of the matched peering object in the peering-list.
`target :`	`number-to-call` OR `$2`	`number-to-call` is a literal string, such as `14089991234`. `$2` is an internal variable containing the called number of this inbound call, after any digit map transformation in the matched callee object of the matched peering object in the peering-list.

Table 11-1 Rule Formats (continued)

Rule	Format	Notes
embedded-digit-map :	(Mlabel) OR digit-map	(Mlabel) is a named digit map, where label is the abbreviated name of any terminal that has a digit map defined: SP1, SP2, SP3, SP4, PP, PH, PH2, or AA. digit-map is any digit map, such as (1xxx|xx.); make sure to include the enclosing parentheses.

InboundCallRoute Examples

This section provides examples of routing rules for handling inbound calls.

Table 11-2 Inbound Call Route Examples

Inbound Call Route	Description
ph OR {ph} OR {:ph} OR {@|?>@:ph} (all equivalent)	Ring the **Phone** port for all incoming calls. This example is the default InboundCallRoute for all trunks.
{(14081223330|15103313456):aa}, {(1800xx.|1888xx.):},{ph}	Ring both the **Phone** port and the AA for calls coming from 1 408 122 3330 or 1 510 331 3456, Block all 800, 888, and anonymous calls, and ring the **Phone** port for all other calls.
{(x.4081113333|x.4152224444):aa}, {ph}	Ring the AA for calls coming from any number that ends with 408 111 3333 or 415 222 4444. Ring the **Phone** port for all other calls. Be sure to include the enclosing parentheses in this example, since "x." is a digit map-specific syntax.
{200123456:aa},{sp1(14083335678)}	Ring the AA for calls coming from 200123456. For all any other calls, bridge it by calling 1 408 333 5678 using the SP1 Service.

Outbound Call Route Configuration

Outbound Call Routes are rules to tell the device where to send the call when the endpoint attempts to make a call. Endpoints can call each other or an outside number using one of the trunks.

The **OutboundCallRoute** syntaxes are almost identical to those of the **InboundCallRoute**. The differences between the syntaxes are mainly in the implied value when an optional field is omitted, no caller objects and one and only one terminal object per terminal-list in an **OutboundCallRoute**. Forking isn't supported when routing outbound calls.

The general format is:

OutboundCallRoute := `rule` OR `{rule},{rule},...`.

You can omit the curly braces if there's only one rule in the route. The OR operator is NOT part of the parameter syntax; it's used here to separate alternative values only.

A rule has the following format:

```
rule := callee-list : terminal
```

where

- `callee-list := callee|callee|callee|` ...(vertical bar separated list of 0 or more callee object)
- `callee := number` OR `embedded-digit-map` OR `@` (`@` = any number)
- `terminal := PHx` OR `AAx` OR `LIx(arg)` OR `SPx(arg)` OR `PPx(arg)` (`arg` object is optional)
- `arg := cid > target`
- `x := 1` OR `2` OR `3`...(where applicable; can be omitted if it's equal to 1)
- `cid = spoofed-caller-number`
- `target = number-to-call` OR `$2`
- `embedded-digit-map = (Mlabel)` OR `digit-map`

Notes

- A terminal can be a trunk or another endpoint.
- Abbreviated terminal names are case-insensitive.
- `Number` and `number-to-call` are literal strings, such as `14089991234`.
- `Digit-map` is any digit map, such as `(1xxx|xx.)`; make sure to include the enclosing parentheses.
- `Spoofed-caller-number` is a literal string, such as `14081112233`, to be used as the caller number for making a new call on the specified trunk.
- `(Mlabel)` is a named digit map where `label` is the abbreviated name of any terminal that has a digit map defined: SP1, SP2, PP, PH, or AA.
- `$2` is an internal variable containing the called number of this outbound call, after any digit map transformation in the matched callee object.
- `Callee-list` can be empty, which implies the single callee object `@`, which means any called number. The succeeding '`:`' can be omitted also when callee-list is empty.
- The `cid` object inside an `arg` object is optional. If omitted, it implies no caller-ID spoofing when calling on the specified trunk. The succeeding '`>`' can be omitted if `cid` is omitted.

- The target object inside an `arg` object is optional. If omitted, it implies the target `$2`, which means to call the original called number after applying any necessary digit map transformation implied by the rule. The preceding '>' can't be omitted if `target` is omitted but not the `cid`.
- `arg` object is optional. If omitted, it implies the arg with the target `$2` and no `cid`.

An outbound call matches a rule if its called number matches one of the callee objects of the rule. Callee objects are tested in the order left and right, and the first matched callee wins. Rules are also checked in the order left to right, and the first matched rule wins. Therefore it's important that you place the more specific rules first in the **OutboundCallRoute** if multiple rules can potentially match the same outbound call.

Every endpoint also has a digit map defined. The user-dialed number is processed with the endpoint's digit map first before it's passed to the **OutboundCallRoute** for routing decision. Therefore the number used for matching call routing rules has already incurred the transformations, if any, implied by the digit map. Remember this fact when crafting your own **OutboundCallRoute**.

OutboundCallRoute Examples

This section provides examples of routing rules for handling outbound calls.

`sp1` OR `{SP1}` OR `{:SP1}` OR `{@:Sp1}` (all equivalent)

This rule says: Make all calls using the SP1 Service, without any caller-id spoofing or digit transformation.

```
                {**0:aa},{***:aa2},
{(Mpli):pli},{(<**1:>(Msp1)):sp1},{(<**2:>(Msp2)):sp2},
{(<**9:>(Mpp)):pp}
```

This is the default **OutboundCallRoute** for the **PHONE** port. Based on this, every rule dictates the following (ordered from left to right):

- Dial **0 to invoke AA1 or AA.
- Dial *** to invoke the local device configuration IVR (or AA2).
- `(Mpli)` and `pli` are substituted with the PrimaryLine's abbreviated name.
- Use SP1 Service to call all numbers that start with **1 and subsequent digits matching SP1 Service's **DigitMap**. Remove the **1 prefix from the resulting number before making the call.
- Use SP2 Service to call all numbers that start with **2 and subsequent digits matching SP2 Service's **DigitMap**. Remove the **2 prefix from the resulting number before making the call.
- Use the PDMS-SP Service to call all numbers that start with **9 and subsequent digits matching PDMS-SP Service's **DigitMap**. Remove the **9 prefix from the resulting number before making the call.

Digit Map Configuration

A digit map contains a set of one or more rules that transform and restrict the dialed or called number. The digit map determines if you dial sufficient digits to form a complete number.

Digit Map Rules and Elements

Each digit map consists of elements combined into one or more rules.

The map rule or rules are surrounded by parentheses. You **must not** omit the parentheses. Here is the general format of a digit map:

```
(rule|rule|….|rule)
```

A digit map rule is a rule for matching a given sequence of digits. It may contain extra white spaces for readability; the parsing process removes all spaces. A rule can contain one or more of the following elements:

- literals - Any combination of 0-9,*,#,+,-, A-Z, a-z, except m, M, s, S, x, X, which have special meaning in the digit map syntax. It matches digit sequences with exactly the same literals.
- 'literals' - Everything inside a pair of single quotes is treated as a literal except for the single quote (') character.
- `x` - a wildcard digit that matches any digit from 0-9. `x` is case-sensitive.
- `x.` - matches 0 or more `x`.
- `[123-7]` or `[135]` - A set of 1 or more digits surrounded by pair of `[ ]`. It matches any digit in the set. The – syntax represents an inclusive digit range, such as `0-9`, `3-7`. So `[123-7]` is equivalent to `[1-7]` or `[1234567]`.
- `S`, `S0`, `S1`, `S2`, ...`S9` - Digit timer of 0, 1, 2, ...,9 seconds. `S` is equivalent to `S1`; `S0` is the same as "blank". You can concatenate multiple `S` elements together if you need more than 9-seconds timeout, such as `S9S5` for a 14-second timeout. `S` is case-sensitive. It should only be used either as the first element of a rule for hot/warm line implementation, or as the last element of a rule as a means of overriding the default interdigit timer.
- `<elements:literals>` - Substitute the digit sequence matching elements with the given literals. Single quote syntax is NOT needed or allowed for the literals in this context. Special characters can be used here as they don't apply in this context either. Elements can be empty, in which case the ':' can be omitted. This case is useful for inserting some extra digits in certain part of the dialed digits. The literals part can be empty also but the ':' MUST NOT be omitted. This case is useful for removing part of dialed digits. Elements and literals MUST NOT be both empty.
- `X` - A wildcard digit that matches 0-9 or *. This is equivalent to `[x*]` or `[0-9*x]`
- `@` - A wildcard character that matches any alphanumeric character except `#`
- `x?` - matches 0 or 1 `x`

- `@?` - matches 0 or 1 `@`
- `[^...]` - matches any single alphanumeric character that is not in the set
- Allow alphanumeric and wildcard characters inside a set `[ ]`, such as `[x]`, `[X#]`, `[@#]`, `[a-zA-Zx]`
- `(map)` - An embedded digit map for matching subsequent digits.
- `(Mlabel)` - A named embedded digit map for matching subsequent digits, where label is one of abbreviated terminal names. Possible choices are:
  - `(Msp1)` for *SP1 Service* **::DigitMap**
  - `(Msp2)` for *SP2 Service* **::DigitMap**
  - `(Msp3)` for *SP3 Service* **::DigitMap**
  - `(Msp4)` for *SP4 Service* **::DigitMap**
  - `(Mpp)` for *PDMS-SP Service* **::DigitMap**
  - `(Mph)` for *PHONE Port* **::DigitMap**
  - `(Mph2)` for *PHONE2 Port* **::DigitMap**
  - `(Maa)` for *Auto Attendant* **::DigitMap**
  - `(MtgN)` for *TrunkGroupN* **::DigitMap**, *N*=1,2,3,4
  - `(MvgN)` for *VoiceGatewayN* **::DigitMap**, *N*=1,2,3,4,5,6,7,8

Recursive Digit Maps

The `[^...]` and `[ ]` elements imply that the device digit maps are recursive. Recursive digit maps allow digit maps to be re-used and make their specification more compact and readable. It is important that you do not specify digit maps that lead to infinite recursion. For example, a digit map must not include a named embedded digit map that references itself.

Barring Digit Maps

To bar users from calling numbers that match a rule, add a '`!`' in front of that rule in the digit map. The rule is then referred to as a barring rule. For example, you might want to bar users from calling premium or international numbers.

Digit Map Examples

See the following examples of common digit map rules.

`1408xxxxxxx` - Matches any 11-digit number that starts with `1408`.

`011xx.` - Matches any number that starts with `011` followed by one or more digits.

`<1408>xxxxxxx` - Matches any 7-digit number. The device prepends `1408` to the number when calling.

`<:1408>xxxxxxx` - Equivalent to the last example.

`<+>1xxxxxxxxxx` - Prepends '+' to any 11-digit number that starts with `1`.

`<**1:>1408xxxxxxx` - Matches any number that starts with `**11408` followed by 7 digits. The device removes the `**1` prefix when making the call.

`*74(x|xx)` - Matches any number that starts with `*74`, followed by 1 or 2 digits.

`**1(Msp1)` - Matches any number that starts with `**1` and with the rest of the digits matching the **DigitMap** in the SP1 Service.

`<:1234>` - Matches an empty phone number and replaces with `1234`. This is the syntax for a hotline to `1234`.

`<S0:1234>` - Equivalent to the last example.

`<:#>` - Hotline to the number `#`.

`<S0:#>` - Equivalent to the last example.

`<S4:1234>` - Call `1234` if no digits entered for 4 seconds. This is the syntax of a warm line.

`xx.853 7683` - Matches any number with at least 8 digits and ends with `8537683`, such as `15108537683`, `98537683`.

`(x.408 223 1122)` - Matches any number with at least 10 digits and ends with `408 223 1122`, such as `4082231122` or `1408 223 1122`.

`xx.<#>` - Adds a `#` to the end of any number with 1 or more digits.

`!1900xxx xxxx` - Barring all 11-digit numbers that start with `1900`.

`[^*]@@.` - Arbitrarily long alphanumeric sequence (except `#`) that doesn't start with `*`.

`xx?` - Any 1- or 2-digit number.

`(1xxxxxxxxxxS0|xx.)` - Arbitrarily long digit sequence not starting with `1`; otherwise it is limited to 11 digits.

Matching Against Multiple Rules in Digit Map

A digit map normally contains more than one rules. The Digit Map Processor (DMP) must return the best matched rule at some point, or declare that the input digit sequence is invalid. The DMP keeps refining its decision as each digit is entered until it reaches a final decision, or is forced to make a timely decision when the interdigit timer expires.

The DMP restarts the interdigit timer on every newly entered digit. The duration of this timer can be either long or short. The long and the short timer values are set by default to 10 seconds and 2 seconds, respectively, and are configurable per PHONE port via the **DigitMapLongTimer** and **DigitMapShortTimer** parameters. Whether to use the long or short interdigit timer depends on the current rule matching states. The DMP maintains a matching state for each rule in the digit map as it processes each input digit. The following states are defined:

Partially Matched (PM)
The rule partially matches the accumulated input sequence. Initially all rules are in this state before any digit is entered. Rules in this state have the potential of becoming Exactly Matched (EM) or Indefinitely Matched (IM) as more digits are entered.
Example: `1234` partially matches the rules `xxxxxxx`, `1xxxx`, `1234567`, `<123:>xxxx`.

Exactly Matched (EM)
The rule exactly matches the accumulated input sequence. However, any further input digit turns this rule into the Mismatch (MM) state.
Example: `1234` exactly matches the rules `xxxx`, `1234`, `1xxx`, `<123:5678>x`.

Indefinitely Matched (IM)
The rule matches the accumulated input sequence indefinitely, with a variable length such that the rule can potentially stay as IM as more matching digits are entered.
Example: 011853 indefinitely matches the rules `xx.`, `011xx.`, `<011:>xx`.

Mismatch (MM)
The rule does not match the accumulated input sequence. This state won't change as more digits are entered.
Example: `1234` mismatches the rules `123`, `1xx`, `12345`.

Rules in the EM or IM state are candidates to be selected by the DMP. After processing a new digit, the DMP returns a final decision if any of the following conditions holds:

- All rules are the MM state. The DMP returns an error.
- One or more rules are in the EM state with no rules in the IM state. The DMP returns the best matched EM rule. If the best matched rule is a barring rule, the DMP returns an error instead.

Otherwise, the DMP starts the short interdigit timer if there is at least one rule in the EM state, or else the long timer. When the interdigit timer expires, the DMP makes a timely decision by returning either the best matched rule at that moment if one is found, or else a timeout error. Again, if the best matched rule in this case is a barring rule, the DMP returns an error instead. The timer to wait for the first input digit is **not** governed by the interdigit timer, but by the duration of dial tone being played and could be a lot lengthier than the long interdigit timer.

The best matched rule is the one that has the most specific literals matching the input digit sequence. For example, the input sequence `1234` matches the rule `123x` better than `1xxx`. On the other hand, an EM rule is always selected over an IM rule.

Finally, the default interdigit timer can be overridden by appending the `S n` element at the end of the rule (*n* = 0-9).

Let's look at some examples. Consider this simple digit map:

```
(<1408>xxx xxxx)
```

As soon as 7 digits have been entered, the DMP returns a complete number by prepending the accumulated digits with `1408`.

Consider another simple map:

```
(xx.)
```

After the user dials one or more digits, the DMP returns the accumulated digits as a complete number when the long interdigit timer expires.

Let's combine the last two maps:

```
(xx. | <1408>xxx xxxx)
```

After the user dials 1 or more digits but fewer than 7 digits, the DMP returns the accumulated digits as a complete number when the (long) interdigit timer expires. As soon as 7 digits are entered, the DMP would return `1408` followed by the accumulated 7-digit when the (short) interdigit expires. On the eighth digit and beyond, however, the DMP considers the first rule only and returns the accumulated digits as-is when the (long) interdigit timer expires.

Now add an S4 timer to the second rule:

```
(xx. | <1408>xxx xxxxS4)
```

In this case, the DMP behaves exactly the same as the last, except that the short interdigit timer the DMP uses upon receiving the seventh digit is overridden by a 4-second timer; hence the user has as long as 4 seconds instead of 2 to dial the eighth digit.

Forcing Interdigit Timeout With A Pound Key

When dialing, you can force an interdigit timeout with a # key instead of waiting for the DMP to timeout its own long or short timer.

This is allowed as long as the # key does not match the current element of any PM rules. Otherwise the # key is consumed by the DMP instead of triggering a timeout.

Consider the digit map `(33xx.)`

If the user enters `333#`, the DMP return immediately with the number `333`.

Now consider the digit map `(33xx.|333#1234x.)`

If the user enters `333#`, the DMP won't return, but continues to wait for further input or for its interdigit timer to expire. Note that the first rule "`33xx`." is now in the MM state since the digit `#` does not match "`x`". You can continue to enter `1234#`, or `1234` and wait for a long interdigit timeout for the DMP to successfully return `333#1234`.

Invoke Second Dial Tone in Digit Map

You can tell the device to start a tone after a certain pattern of digits have been dialed by specifying the element `{t=<tone>}` within a digit map, where `<tone>` is a 1- to 3-letter name of the tone to play.

The tone stops when the next digit is entered. For example:

```
(**1{t=di2}(Msp)|**8{t=od}(Mli))
```

tells the device to play Second Dial Tone when **1 is dialed, or play Outside Dial Tone when **8 is dialed. Here is a full list of acceptable (case-insensitive) values of `<tone>`:

- `bu` = Busy Tone
- `cf` = Call Forwarded Dial Tone
- `cm` = Confirmation Tone
- `co` = Conference Tone
- `cw1 - cw10` = Call Waiting Tone 1-10
- `di` = Dial Tone
- `di2` = Second Dial Tone
- `fb` = Fast Busy Tone
- `ho` = Holding Tone
- `od` = Outside Dial Tone
- `pr` = Prompt Tone
- `rb` = Ringback Tone
- `ro` = Reorder Tone (same as fast busy)
- `si1 - si4` = SIT TONE 1 - 4
- `st` = Stutter Tone
- `0 - 9, *, #, a - d` = DTMF 0 - 9, *, #, A - D

Change Inter-digit Long Timer Dynamically After Partial Match

The device starts off with the inter-digit long timer set to the configured **DigitMapLongTimer** value when processing a new digit sequence by a digit map.

You can change the long timer as some patterns are partially matched by embedding the syntax `{L=<time>}` within a rule in the digit map, where `<time>` is the desired number of seconds for the long timer. For example:

```
(011 853 xxxx xxxx{L=5}x. |xx.)
```

Here the long timer is shortened to 5 seconds after the user has entered `011 853` + 8 digits. Hence the device declares that a complete number is collected in 5

seconds when no more digits are received. Without the `{L=5}` syntax the user has to wait for 10 seconds (by default) for the same to happen.

User-Defined Digit Maps

These digit maps are referred to as User-Defined Digit Map 1 to 10. Each user-defined digit map is specified with two parameters:

- **Label**: An arbitrary string for referencing this digit map in other digit map specification. The value should be 2 to 16 characters long. For example, "friends". In this case, `(Mfriends)` can be referenced in other digit maps, such as *PHONE Port* **::DigitMap**.
- **DigitMap**

By default both parameters are empty, except for User-Defined Digit Map 1. See the following section.

A User-Defined Digit Map For IPv4 Dialing

User-Defined Digit Map 1 is configured to support IPv4 dialing.

The default values of the parameters for User-Defined Digit Map 1 are set to the following values to support IPv4 dialing:

- Label: `ipd`
- Digit Map: `(xx.<*:@>xx?x?<*:.>xx?x?<*:.>xx?x?<*:.>xx?x?|xx.<*:@>xx?x?<*:.>xx?x?<*:.>xx?x?<*:.>xx?x?<*::>xx?x?x?x?)`

The map (Mipd) is referenced in the default setting of the **DigitMap** in ITSP Profiles A and B. It supports the following two forms of IPv4 dialing:

- `<user-id>*<a>*<b>*<c>*<d>`
- `<user-id>*<a>*<b>*<c>*<d>*<port>`

where `<user-id>` is an arbitrary length numeric user-id, such as `100345`, `<port>` is a port number in the range 0-65535, and each of `<a>`,`<b>`,`<c>`,`<d>` is a 1- to 3-digit pattern in the range 1-255 that identifies one byte of an IP address. The dialed number is translated into `<user-id>@<a>.<b>.<c>.<d>` and `<user-id>@<a>.<b>.<c>.<d>:<port>`.

Here are some examples:

`1234*192*168*15*113` maps to `1234@192.168.15.113`

`123456*192*168*15*180*5061` maps to `123456@192.168.15.180:5061`

Configure a User-Defined Digit Map

You can define up to ten digit maps in the system web interface.

1. In the system web interface, go to **User Settings** > **User Defined Digit Maps**.

2. In the **Default** column, clear the check box for the following parameters:
   - `Label`
   - `DigitMap`
3. In the **Value** column, configure the following parameters:

Table 11-3 User Defined Digit Map

Parameter Name	Value
`Label`	Enter an arbitrary string for referencing this digit map in other digit map specification. The value should be 2 to 16 characters long. For example, "friends". In this case, `(Mfriends)` can be referenced in other digit maps, such as *PHONE Port* **::DigitMap**. By default empty, except for User-Defined Digit Map 1 that is predefined to support IPv4 dialing. The map is referenced in the default setting of the **DigitMap** in ITSP Profiles A and B.
`DigitMap`	Enter the digit map rule or rules surrounded by parentheses. By default empty, except for User-Defined Digit Map 1.

4. Select **Submit**.
5. Reboot your system when you complete your changes.

Call Routing and Digit Map

Your device is a voice service bridge (VSB) that supports multiple voice services.

Trunks, Endpoints, and Terminals

The device can bridge calls across any of the supported voice services. A call bridge refers to a voice connection connecting two calls on the same or different voice services.

The device allows four concurrent independent call bridges. The following matrix shows the possible call bridge connections on the device.

Supported 2-way Call Bridges

Table 11-4 Supported 2-way Call Bridges on the Device

	SP1 Service	SP2 Service	SP3 Service	SP4 Service	PDMS-SP Service
SP1 Service	yes	yes	yes	yes	yes
SP2 Service	yes	yes	yes	yes	yes
SP3 Service	yes	yes	yes	yes	yes
SP4 Service	yes	yes	yes	yes	yes

Table 11-4 Supported 2-way Call Bridges on the Device (continued)

	SP1 Service	SP2 Service	SP3 Service	SP4 Service	PDMS-SP Service
PDMS-SPService	yes	yes	yes	yes	yes

NOTE: Highlighted services may not be available on some models and/or require additional accessories.

Each supported service is also referred to as a trunk (a traditional telco term for a physical wire or wires that deliver phone services to homes or businesses). Each trunk is represented with two-letter abbreviation and a numeral-based instance identifier:

- SP1 = the SP1 voice service (with ITSP A, B, C, or D)
- SP2 = the SP2 voice service (with ITSP A, B, C, or D)
- SP3 = the SP3 voice service (with ITSP A, B, C, or D)
- SP4 = the SP4 voice service (with ITSP A, B, C, or D)
- PP1 = the PDMS-SP service

The instance identifier can be omitted when it equals 1. Thus, SP is equivalent to SP1, PP is equivalent to PP1, and so forth. These short-hand notations are used heavily in configuring the device, as found in call routes, call forward numbers, and speed dials parameters. Unless stated otherwise, the abbreviated trunk names are case-insensitive.

In addition to all the call bridging functionalities, each device has two built-in physical **Phone** ports for hooking up analog telephones or FAX machines. The device includes a set of features to support its **Phone** ports to make it work also as a full-featured ATA device. Users can place and receive calls on the **Phone** ports over any of the trunks.

The device also comes with an Auto Attendant for helping callers to direct their calls landed on the device. When an inbound call is received on the device, it can be routed to the AA, which then offers a menu of options to the caller to direct it further. It could be directed to ring any one or all of the available **Phone** ports, or bridged with another call on a trunk (which the AA "dials" or sets up on behalf of the caller).

The **Phone** ports and the AA are the two entities in the device where calls can terminate (that is, start or end there), as opposed to the trunks, which rely on the corresponding service providers to terminate the call. In this document, the **Phone** ports and the AA are endpoints. Like the trunks, each endpoint is represented by a 2-letter abbreviation and a numeral-based instance identifier:

- PH1 = the **Phone** port (same as PHONE1 port)
- PH2 = the PHONE2 port
- AA1 = the Auto Attendant

Unless stated otherwise, abbreviated endpoint names are case-insensitive. A trunk or an endpoint is also referred to as a terminal in this document.

The following matrix shows the possible call connections between the endpoints and the trunks.

Table 11-5 Supported Endpoint Calls on the Device

	Any Trunk	Phone Port (PHONE1 Port)	PHONE2 Port	AA
Any Trunk	N/A	Yes	Yes	Yes
Phone Port (PHONE1 Port)	Yes	No	Yes	Yes
PHONE2 Port	Yes	Yes	No	Yes
AA	Yes	Yes	Yes	No

12 Service Providers

This section of the configuration of the Poly ATA device concerns all SIP-based configurations. Each ITSP configuration is grouped together as an ITSP profile. The Poly ATA device refers to them as ITSP Profile A, B, C, and D. On the other hand, the SP service account specifics are grouped under the heading SP*n* service, where *n* = 1, 2, 3, or 4.

ITSP Profile

The **Service Providers** > **ITSP Profile** includes parameters such as `ProxyServer`, `Outbound Proxy`, and `DigitMap`, but doesn't include account-specific parameters.

SP Service

The **Voice Services** > **SP Service** profiles include account-specific parameters such as `AuthUserName`, `AuthPassword`, `CallerIDName`, and `X_ServProvProfile`. The `X_ServProvProfile` parameter serves to match and determine which ITSP Profile parameters to use.

SIP / ITSP Voice Services

The voice services include the following services:

- SP1-4
- PDMS-SP
- AA
- Gateways and Trunk Groups

SIP registration

Devices can be set periodically register with a SIP Proxy Server or SIP Registration Server.

SIP Proxy Server and SIP Registration Server can be different, although they are usually the same in practice. SIP Proxy Server is a required parameter that must be configured on the device. The Registration Server is optional and assumed to be the same as the SIP Proxy Server if it is not configured on the device.

The main purpose of registration is to create and maintain a dynamic binding of the SIP account to the device's local contact address. The service provider can also rely on this periodic message to infer if the device is online and functional. Each device takes only one local IP address that is either statically assigned in the device's configuration, or dynamically obtained from a local DHCP server. The SP*n* services (for *n* = 1, 2, 3, and 4) each use a different local contact port for sending and receiving SIP messages (defaults are 5060, 5061, 5062, and 5063).

Note that dynamic address binding through periodic registration is not strictly necessary if the local IP address of the device does not change; the device's contact address can be statically configured on the Registration Server.

SIP Outbound Proxy Server

An outbound proxy server can be configured on the device such that all outbound requests are sent via the outbound proxy server instead of directly to the SIP Proxy Server or Registration Server.

If the outbound proxy server is listening at a non-standard port, the correct port value must be specified in the `OutboundProxyPort` parameter. The `OutboundProxy` can use a different transport protocol from the `ProxyServer`. The transport protocol to use to communicate with the `OutboundProxy` can be set in the `OutboundProxyTransport` parameters. If `OutboundProxyTransport` is TCP or TLS, your device initiates a TCP or TLS connection only with the `OutboundProxy`. All subsequent messages exchanged between your device and the servers MUST use the same connection. If for any reason the connection is closed, your device attempts to re-establish the connection with the `OutboundProxy` following an exponential back-off retry pattern.

Even though your device only exchanges messages directly with the `OutboundProxy`, the `ProxyServer`, `ProxyServerPort`, and `ProxyServerTransport` parameters are still very much relevant and important. The reason is that the SIP requests sent by your phone to the server are formed based on these values, not based on the `OutboundProxy` value. The `OutboundProxy` value should never appear in the SIP requests generated by your device, unless the `OutboundProxy` parameter has the same value as `ProxyServer`.

Some server implementations include the outbound proxy server in a Record-Route header such that your device shouldn't respect the locally configured `OutboundProxy` value after the initial INVITE is sent for a new call. This behavior can be achieved by enabling the ITSP *Profile X* - *SIP* `::X_BypassOutboundProxyInCall` option. However, this option has no effect when the `OutboundProxyTransport` is TCP or TLS, as your device always uses the same connection to send messages to the server.

DNS Lookup of SIP Servers

When sending out SIP requests to the server, the device looks up the IP address of the server using standard DNS query if the server is specified as a domain name instead of an IP address.

If an Outbound Proxy Server is configured, it is used instead of the SIP Proxy Server or SIP Registration Server. The resolution of the server domain name into IP address is performed in the following manner:

- Try looking up the name as DNS A Record. If not found,
- Try looking up the name as DNS SRV Record. If not found,
- Try looking up the name as DNS SRV Record with "_sip._udp." prepended to the host name. If not found, fail the request.

If the result from the DNS query is an SRV record, the server port is taken from that record also. The server port value configured on the device is ignored. Otherwise, the server port is taken from the configured value or uses port 5060 if none is specified.

NAT Traversal Considerations

If the device sits behind a NAT router (typically the case), it can discover the mapped external address corresponding to its local SIP contact address as seen by the server in one of the following ways:

- From the "received=" and "rport=" parameters of the VIA header of the REGISTER response sent by the server. These two parameters tell the device its mapped IP address and port number. This method is used if periodic registration is enabled on the device.
- From the response to a STUN binding request the device sent to a STUN server. This method is used by enabling **X_KeepAliveEnable** and setting **X_KeepAliveMsgType** to "stun". In that case, the STUN server is taken from **X_KeepAliveServer**, if it is specified. Otherwise, the keep-alive messages are sent to the same server where a REGISTER request would be sent to. The latter is the most effective way of using STUN to discover the mapped external contact address.

The device always uses the mapped external contact address in all outbound SIP requests instead of its local contact address if one is discovered by either method discovered above.

SIP Proxy Server Redundancy and Dual Registration

Server Redundancy specifically refers to the device's capability to look for a working server to REGISTER to from a list of candidates, and switch to another server once the server that it currently registers to becomes unresponsive.

Device registration must be enabled in order to use the server redundancy feature. Other SIP requests, such as INVITE or SUBSCRIBE, are sent to the same server that the device currently registers with.

If Outbound Proxy Server is provided, server redundancy is applied to the Outbound Proxy Server instead of the registration server. Server redundancy behavior is enabled by enabling the *ITSP Profile X - SIP::* **X_ProxyServerRedundancy** parameter, which is disabled by default.

Another requirement for using the server redundancy feature is that the underlying server must be configured in the device as a domain name instead of an IP address. This allows the device to collect a list of candidate servers based on DNS query.

The domain name can be looked up as DNS A record or DNS SRV record. For A records, all the IP addresses returned by the DNS server are considered to have the same priority. For SRV records, the hosts returned by the DNS server can be each assigned a different priority.

After a list of candidate servers are obtained, the device first looks for a working server according to the stated priority. A *working server* means one that the device can successfully registers to. This is known as the *Primary Server*. Subsequently, the device maintains registration to the primary server the usual

way. However, if no working server is found after traversing the entire list, the device takes a short break and repeats the search in the same order.

While maintaining registration with the Primary Server, the device continually attempts to fall back to one of the candidate servers that has higher priority than the primary server, if any. The list of candidate servers that the device is trying to fall back on is known as the *primary fallback list*, which may be empty.

In addition, the device can be configured to maintain a secondary registration to a server that has lower or equal priority than the primary server. Secondary registration can be enabled by setting the parameter **X_SecondaryRegistration** to YES. If **X_ProxyServerRedundancy** is NO, however, **X_SecondaryRegistration** does not take any effect. If this feature is enabled, as soon as a primary server is found, the device searches for a working secondary server in the same manner from the list of candidate servers that are of lower or equal priority than the primary server. Similarly, once a secondary server is found, the device forms a *secondary fallback list* to continually attempt to fall back on if the list is not empty.

The interval for checking the primary fallback list and the secondary fallback list are configured in the **X_CheckPrimaryFallbackInterval** and **X_CheckSecondaryFallbackInterval** parameters. These parameters are specified in seconds and the default value is 60 for both.

Notes:

- A secondary server exists implies a primary server exists.
- If the secondary server exists, it immediately becomes the primary server when the current primary server fails. The device then starts searching for a new secondary server if the candidate set is not empty.
- The candidate list can change (be lengthened, shortened, priority changed, etc.) on every DNS renewal (based on the entry's TTL). The device rearranges the primary and secondary servers and fallback lists accordingly, whichever applies.

If the server redundancy feature is disabled, the device resolves only one IP address from the server's domain name, and won't try other IP addresses if the server is not responding.

SIP privacy

The device observes inbound caller privacy and decodes caller's name and number from SIP INVITE requests by checking the FROM, P-Asserted-Identity (PAID for short), and Remote-Party-ID (RPID for short) message headers.

All these headers can carry caller's name and number information.

If PAID is present, device takes the name and number from it. Otherwise, it takes the name and number from RPID if it is present, or from the FROM header otherwise. RPID, if present, includes the privacy setting desired by the caller. This privacy can indicate one of the following options:

- *off* = no privacy requested; the device shows name and number.
- *full* = full privacy requested; the device hides both name and number.

- *name* = name privacy requested; the device shows the number but hide the name.
- *uri* = uri privacy requested; the device shows the name but hide the number.

Regardless, if PAID exists or not, the device always takes the privacy setting from the RPID if it is present in the INVITE request. Note that if the resulting caller name is “Anonymous” (case-insensitive), device treats it as if the caller is requesting full privacy.

For outbound calls, caller's preferred privacy setting can be stated by the device in a RPID header of the outbound INVITE request. To enable this behavior, the *ITSP Profile X - SIP* **::X_InsertRemotePartyID** parameter must be set to YES or TRUE, which is the default value of this parameter. The device supports only two outbound caller privacy settings: privacy=off or privacy=full. The RPID header generated by the device carries the same name and number as the FROM header. If outbound caller-ID is blocked, the device sets privacy=full in RPID, and also sets the display name in the FROM and RPID headers to “Anonymous” for backward compatibility. The device won't insert PAID in outbound INVITE requests.

STUN and ICE

The device supports standard STUN based on RFC3489 and RFC5389 for passing inbound RTP packets to the device sitting behind NATs.

The parameters that control the STUN feature are found in the **ITSP Profile X - General::** section:

- **STUNEnable** - Enables this feature (default is NO or FALSE).
- **STUNServer** - The IP address or domain name of the external STUN server to use. STUN feature is disabled if this value is blank, which is the default.
- **X_STUNServerPort** - The STUN Server's listening UDP port. Default value is `3478` (standard STUN port).

The STUN feature used in this context is only for RTP packets, not SIP signaling packets, which typically do not require STUN. The device sends a STUN binding request right before making or answering a call on SP1/2. If the request is successful, the device decodes the mapped external address and port from the binding response and uses them in the m= and c= lines of its SDP offer or answer sent to the peer device. If the request fails, such as STUN server not found or not responding, the call goes on without using external address in the SDP.

Standard RTP requires the use of an even-numbered port in the m= line. If the external port is not an even number, the device changes the local RTP port and redoes STUN, and continues to do this as many as four times or until an even external port number is found. If the fourth trial still results in an odd external port number, the call goes on without using an external address in the SDP.

The device supports standard ICE based on RFC5245. ICE is done on a per-call basis for automatically discovering which peer address is the best route for sending RTP packets. To enable ICE on the device, set the *ITSP Profile X - General* **::X_ICEEnable** parameter to YES (or TRUE). The default is NO (or FALSE).

ICE is effective if STUN is also enabled. However, STUN not a requirement for using ICE on the device. If STUN is enabled and an external RTP address different from its local address is discovered, the device offers two ICE candidates in its SDP:

- The local (host) address (highest priority)
- The external (srflx or server reflexive) address

Otherwise, only the local host candidate is shown in the device's SDP. Note that the device uses the srflx address in the m= and c= lines of the SDP if STUN is enabled and successful.

If ICE is enabled and the peer's SDP has more than one candidate, the device sends STUN requests to each peer candidate from its local RTP port. As soon as it receives a response from the highest priority candidate, the device concludes ICE and uses this candidate to communicate with the peer subsequently. Otherwise, the device allows as long as 5 seconds to wait for the response from all the candidates, and selects the highest priority candidate that has a response. Once ICE completes successfully, the device further applies symmetric RTP concept to determine the peer's RTP address (that is, sends them to the address from which the the peer's RTP packets are coming).

SIP Service Provider Features

Learn about some of the SIP Trunk service features that are supported on your Poly ATA device.

You can configure as many as four SIP accounts or SIP Trunks on the device. For the purposes of this document and elsewhere on the device system information page, documentation, and the PDMS-SP portal, the term ITSP describes the logical entity providing the SIP Trunk service to the device. When you use the device with an IP PBX, the IP PBX takes the place of the ITSP if it is the entity providing the SIP Trunk account credential and connectivity to the device.

ITSP Profiles and SP Services

Each ITSP configuration is grouped together as an ITSP Profile, referred to as ITSP Profiles A, B, C, and D; SP service account specifics are grouped under the heading **SPn Service**, where *n* = 1, 2, 3 or 4.

An ITSP Profile includes such parameters as `ProxyServer`, `OutboundProxy`, and `DigitMap`, but doesn't include account-specific parameters.

An SP Service includes account-specific parameters such as `AuthUserName` (usually the phone number of the account), `AuthPassword`, `CallerIDName`, and `X_ServProvProfile`. The `X_ServProvProfile` parameter connects the service subscriber with the service provider.

If the SP Services use the same ITSP, then you only need to configure one ITSP Profile with all SP Services referred to the same profile.

From the device point of view, the SP*n* Service using ITSP Profile *X* is enabled with the following minimal settings:

Table 12-1 Service Provider Minimal Settings

Parameter	Value
ITSP Profile X > **SIP** > **ProxyServer**	Not Blank
Voice Services > **SPn Service** > **Enable**	Yes
Voice Services > **SPn Service** > **AuthUsername**	Not Blank

Where *X* = A or B, and *n* = 1, 2, 3, or 4. Otherwise, the service is considered disabled.

ITSP Driven Distinctive Ringing

The device offers 10 ring and 10 call-waiting tone patterns in each ring profile.

These patterns are numbered from 1 to 10. Each pattern also comes with a configurable name. You can assign a different default ring to each trunk on the device.

An ITSP can tell the device which ring to use by name for a call routed to SP1/SP2 by inserting an Alert-Info header in the SIP INVITE sent to the device. The Alert-Info must include a URI. For example:

Alert-Info: `<http://www.xyz.com/some-folder/bellcore-dr4>`

When the device receives this information, it looks for a ringtone name or call-waiting tone name in the ring profile that matches the Alert-Info URI. Ringtone names are compared case-insensitively. If a match is found, the device plays the corresponding ring or call-waiting tone. Otherwise, the device plays the default ring.

RTP Statistics - the X-RTP-Stat Header

When ending an established call, the device can include a summary of the RTP statistics collected during the call in the SIP BYE request or the 200 response to the SIP BYE request sent by the peer device.

The summary is carried in an X-RTP-Stat header in the form of a comma-separated list of fields. The reported fields are:

- `PS` = Number of Packets Sent
- `PR` = Number of Packets Received
- `OS` = Number of bytes sent
- `OR` = Number of bytes received
- `PL` = Number of packets lost
- `JI` = Jitter in milliseconds
- `LA` = Decode latency or jitter buffer size in milliseconds

- `DU` = Call duration in seconds
- `EN` = Last Encoder Used
- `DE` = Last Decoder Used
- `MOS` = Mean Opinion Score

For example:

```
X-RTP-
Stat:PS=1234,OS=34560,PR=1236,OR=24720,JI=1,DU=1230,PL=0,EN=G711U
```

To enable the X-RTP-Stat feature, set the *ITSP Profile X - SIP* **::X_InsertRTPStats** parameter to YES (or TRUE).

Media Loopback Service

The device supports the media loopback draft as described in *draft-mmusic-media-loopback-13.txt.*

The device supports the following media loopback features:

- Loopback modes: `loopback-source` and `loopback-mirror`
- Loopback types: `rtp-media-loopback` and `rtp-packet-loopback`
- Loopback packet formats: `encaprtp`, `loopbkprimer`

When the device acts as a loopback mirror, it always sends primer packets so that incoming packets can get through NAT/Firewall. The media loopback feature is controlled by the following parameters under **PHONE *N*> Port** > **Calling Features**:

- `AcceptMediaLoopback` - Enable the device to accept an incoming call that requests media loopback. Default is YES.
- `MediaLoopbackAnswerDelay` - The delay in ms before the device answers a media loopback call. Default is 0.
- `MediaLoopbackMaxDuration` - The maximum duration to allow for an incoming media loopback call. Default is 0, which means the duration is unlimited.

The device rejects an incoming media loopback call if:

- **Phone** port is off-hook.
- **Phone** port is ringing.

The device terminates an inbound media loopback call already in progress when:

- **Phone** port is off-hook.
- **Phone** port is ringing.

To make an outgoing loopback call, dial one of the following star codes before dialing the target number:

- `*03` - Make a Media loopback call.
- `*04` - Make an RTP packet loopback call.

Note that an outbound Media Loopback Call is not subjected to a call duration limit; it lasts until the user hangs up or until the called device ends the call.

For more information on general ITSP parameters, see the ITSP Profile (General and SP Info Settings) Parameters table in the *Poly ATA 400 Series Parameter Reference Guide*.

For more information on ITSP SIP settings parameters, see the ITSP SIP Settings Parameter table in the *Poly ATA 400 Series Parameter Reference Guide*.

For more information on ITSP RTP settings parameters, see the ITSP RTP Settings Parameter table in the *Poly ATA 400 Series Parameter Reference Guide*.

The OBiTALK Service

OBiTALK is a proprietary protocol for communications among Poly ATA devices and OBiTALK device management servers.

The protocol is intended for two main purposes:

- Peer-to-peer calling between OBiTALK devices
- Device management by OBiTALK servers

Every phone or Poly ATA device comes with one instance of the OBiTALK service with the (fixed) factory-assigned 9-digit device OBi number as the user ID of the service. devices can call each other by dialing the other party's OBi number.

The OBiTALK service also enables you to view and change the settings of your phones from the PDMS-SP portal. If you disable the OBiTALK service in your phone's configuration, you can't place OBiTALK voice calls or manage device features through the PDMS-SP portal.

Enable the OBiTALK Service

The OBiTALK service is enabled by default, unless disabled through Zero Touch Provisioning.

For information on Zero Touch customization, see the *Poly VVX Business IP Phones, OBi Edition Provisioning Guide*.

1. In the system web interface, go to **Voice Services** > **OBiTALK Service**.
2. Under **OBiTALK Service Settings**, clear the check box in the **Default** column for **Enable**.
3. In the **Value** column, select the check box for **Enable**.
4. Select **Submit**.
5. Restart your system when you complete your changes.

Limit OBiTALK Calls

Limit OBiTALK calls to just the OBihai echo server.

A simple way to disable OBiTALK voice calls completely is by setting `MaxSessions="0"`. If you do, however, you can't perform an echo test.

1. In the system web interface, go to **Voice Services** > **OBiTALK Service**.
2. In the **Default** column, clear the check box for **DigitMap**.
3. In the **Value** column for **DigitMap**, enter a value of `(<ob>222222222 | ob222222222)`.

   You can change or add more OBi numbers to this digit map by following the same pattern.
4. Select **Submit**.
5. Restart your system when you complete your changes.

OBiTALK Service Settings

View detailed information about the OBiTALK Service under **Voice Services** > **OBiTALK Service**.

IMPORTANT: *PDMS-SP* and *OBiTALK* are both terms used in the system web interface and the documentation to refer to the same functionality.

For more information on PDMS-SP service settings parameters, see the PDMS-SP Service Settings Parameters table in the *Poly ATA 400 Series Parameter Reference Guide*.

For more information on PDMS-SP calling features parameters, see the PDMS-SP Calling Features Parameters table in the *Poly ATA 400 Series Parameter Reference Guide*.

For more information on PDMS-SP inbound direct dialing authentication parameters, see the PDMS-SP Inbound Direct Dialing Authentication Parameters table in the *Poly ATA 400 Series Parameter Reference Guide*.

For more information on PDMS-SP jitter buffer parameters, see the PDMS-SP Jitter Buffer Parameters table in the *Poly ATA 400 Series Parameter Reference Guide*.

Auto Attendant Service

Learn about the auto attendant features on your Poly ATA device.

Automated Attendant

The device call processing Auto Attendant (AA) invoked by including "aa" in the inbound call routing rule associated the interface on the device processing an incoming call.

When connecting to the AA in this manner, there are two options at present.

Note: A Poly ATA device supports only one session of AA at a time. Additional calls routed to the AA while a session is in progress are rejected by the AA as busy.

AA Callback Service

The device offers two methods for the AA to call you back at a number that you picked (or designated by the admin of the device).

The first method is by statically configuring a trunk's **InboundCallRoute**. A rule can be added to the **InboundCallRoute** parameter to have the AA call back the caller's or any other number, if the caller hangs up before the AA answers. The rule should indicate that "aa(*callback-number*)" is the target destination of the call, where *callback-number* is the number that the AA should call back if the caller hangs up before the AA answers the call. For example, the following rule

```
{(<**1>(14089913313|12121559801)):aa($1)}
```

says that if `14089913313` or `12121559801` calls, the call is routed to AA. If the caller hangs up before the AA answers, AA calls the number represented by `$1`. Recall that `$1` is expanded into the caller number after processing by the digit map on the left side of the colon. In this case, it is the caller's number prepended by `**1`. The `**1` is required for outbound call routing when AA calls back; here it indicates SP1 is to be used for calling back (assuming default value of the AA **OutboundCallRoute** parameter).

The *AA Service* **::CallbackAnswerDelay** parameter controls the number of milliseconds before AA answers when a callback number is specified. The default value is 10000 ms (10 seconds). Without the (*callback-number*) argument, the AA behaves the normal way and the answer delay is governed by the *AA Service* **::AnswerDelay** parameter.

The second method is by selecting AA option 3 to "Enter a callback number" after the AA answers the call. The caller can explicitly enter the number to be called back by the AA. If a valid number is entered, AA says "Thank You" and "Goodbye", and then starts calling back 2 seconds after the current call has ended. If number entered is invalid, AA plays SIT tone followed by an error message. Note that the variable $1 (representing the caller's number) is carried over to the subsequent AA callback call. The AA **DigitMap** can include $1 to be used in a callback context. For example, the following rule in the AA **DigitMap**

```
(<00:**1$1>|… )
```

says that if the AA dials 00, the device transforms it into the caller's number prepended by **1. In other words, if the caller wants the AA to callback the current number (typically the case), he can simple enter 00# after selecting option 3 on the AA menu. Note that $1 can only be used as part of a substitution element in the digit map; it must not be used for matching elements since its value is unknown.

User Recorded Prompts

The device supports 10 user-recordable prompts, which are referred to as the *User1* to *User10* prompts.

See the IVR Local Configuration Options on page 11 section on how they can be recorded, or the Maintaining Customized AA Prompts on page 23 section on how they can be duplicated from one device onto another device.

Enable Auto Attendant

You must enable the Auto Attendant feature on the phone to use it.

1. In the system web interface, go to **Voice Services** > **Auto Attendant**.
2. Under **Auto Attendant 1**, in the **Default** column, clear the check box for `Enable`.
3. In the **Value** column, select the check box for `Enable`.
4. Select **Submit**.
5. Restart your system when you complete your changes.

Configure the Auto Attendant Callback Service

Your phone offers two methods for the Auto Attendant to call you back at the calling number or a number that you pick.

Statically configure the routing rule for inbound calls on a trunk with the `InboundCallRoute` parameter. The outbound service to be used for the AA to call back is determined according to the `OutboundCallRoute` parameter.

The `CallbackAnswerDelay` parameter controls the number of milliseconds before AA answers when a callback number is specified.

1. In the system web interface, go to **Voice Services** > **SIPNService**.
2. In the **Default** column, clear the check box for **X_InboundCallRoute**.
3. In the **Value** column, enter a routing rule for `X_InboundCallRoute` to direct an auto attendant to call back the caller's or another number if the caller hangs up before auto attendant answers.
4. Go to **Voice Services** > **Auto Attendant**.
5. Clear the check box for the following parameters in the **Default** column, then configure them in the **Value** column.
   - `OuboundCallRoute`: Enter a routing rule for outbound calls made via this AA.
   - `CallbackAnswerDelay`: Enter the number of milliseconds before AA answers when a callback number is specified.
6. Select **Submit**.
7. Restart your system when you complete your changes.

Customize Service Route Access Codes for the Auto Attendant.

Customize the service route access codes, including the outbound call route and digit map, for calling via the Auto Attendant.

1. In the system web interface, go to **Voice Services** > **Auto Attendant**.
2. Under **Auto Attendant 1**, in the **Default** column, clear the check boxes for **DigitMap** and **OutboundCallRoute**.

3. In the **Value** column, enter the rules for the Auto Attendant for **DigitMap** and **OutboundCallRoute**.
4. Select **Submit**.
5. Restart your system when you complete your changes.

Customizing AA Prompt Lists

The AA doesn't play individual user prompts directly.

Instead it plays a comma-separated list of prompt elements, known as a *Prompt List*. A prompt element can be a user prompt with optional parameters, or a control element. A user prompt is referred as

`%User<N>%` where `<N>` = 1 - 10.

In a prompt list, this can be followed by a `;r=<start>-<end>` parameter that specifies the range to play for that prompt, where

`<start>` = starting time mark in milliseconds. 0 is the default if `<start>` is omitted.

`<end>` = ending time mark in milliseconds. The end of the prompt is the default if `<end>` is omitted.

If the `r=` parameter is omitted, the full range of the prompt is played.

In a prompt list, each control element begins with a '`&`'. The following control elements are supported:

```
&pause(<duration>)
```

The device interprets these controls as pause playing the prompts for the number of seconds as given by the `<duration>` parameter.

Table 12-2 Prompt Examples

Prompt	Description
`%User1%;r=1000`	Play the User1 prompt, starting at the 1000 ms mark to the end.
`%User2%`	Play the entire User2 prompt, from start to finish.
`%User3%;r=1300-3720`	Play the User3 prompt, starting from the 1300 ms mark to the 3720 ms mark.
`%User4%;r=3200-1200`	Don't play anything since `<end>` is less than `<start>`.
`%User1%;r=105,&pause(3),%User5%,%User9%;r=0-1350,&pause(15)`	Play the User1 prompt, starting at the 105 ms mark to the end, pause for 3 sec, play the entire User5 prompt, from start to finish, play the User9 prompt, from the start to the 1350 ms mark, then pause for 15 sec.

You can replace any of the following AA prompt lists with your own specified prompt lists:

Table 12-3 Automated Attendant Prompt Lists

AA Prompt List	System Default	Prompt To Be Played
Welcome	Welcome to OBi Attendant.	Once, at the beginning when the AA starts.
InvalidPin	Invalid PIN.	After the user enters an invalid PIN.
EnterPin	Enter PIN.	Prompts the user to enter a valid PIN.
MenuTitle	Main Menu.	Once, after Welcome and before announcing the menu options.
Menu	Press 1 to continue this call. Press 2 to make a new call. Press 3 to enter a callback number.	A couple of times after MenuTitle.
PleaseWait	Please wait while your call is being connected.	Once, after the user enters a phone number to call.
EnterNumber	Enter number followed by the # key.	Prompts the user to enter a valid number after option 2 or option 3 is selected by the user.
Bye	Thank you. Goodbye.	When the user presses the * or # key to leave the AA.

For more information on user prompts parameters, see the User Prompts Parameters table in the *Poly ATA 400 Series Parameter Reference Guide*.

For more information on Auto Attendant parameters, see the Automated Attendant Parameters table in the *Poly ATA 400 Series Parameter Reference Guide*.

For more information on Auto Attendant prompt parameters, see the Auto Attendant Prompt Parameters table in the *Poly ATA 400 Series Parameter Reference Guide*.

Voice Gateways

A voice gateway (VG) is another ATA device that enables incoming callers to call farther by using one or more of its trunks, supporting two-stage dialing.

Incoming OBiTALK callers call the gateway first with a normal OBiTALK call, get the auto attendant, and then dial the target number. For authentication, the auto attendant may ask the user to enter a PIN before establishing the second call, or second stage.

A gateway is conceptually a trunk with its own digit map, and you can specify as many as eight gateways. Address each gateway using its factory-assigned OBi Number and refer to a gateway and its associated digit map with the short trunk name VG*n* and (Mvgn). You can use VG*n* and (Mvgn) in call routing rules and digit maps just like other real trunks.

For more information on voice gateways, see the *Poly OBi Device Technical Reference* at Poly Support.

Configure a Gateway for Direct Dialing

Configure a gateway with one-stage or direct dialing so that the caller can dial the target number directly without going through the auto attendant.

Because a user can't enter a PIN when direct dialing, you can configure an optional user ID and password so the device can automatically authenticate with the gateway.

1. In the system web interface, go to **Voice Services** > **Gateways and Trunk Groups**.
2. In the **Default** column, clear the check boxes for **AuthUserID** and **AuthPassword**.
3. In the **Value** column, enter the values for **AuthUserID** and **AuthPassword**.
4. Select **Submit**.
5. Restart your system when you complete your changes.

Voice Gateway Examples

The following examples illustrate setting up voice gateways.

VG for all calls to numbers starting with 1

Setting up a voice gateway involves the following:

- Add the rule `{(1xxx xxx xxxx):vg2}` in the **PHONE** port's `OutboundCallRoute` parameter to let the device dial out using `VG2` when a caller dials any 11-digit number starting with 1.
- On the gateway side, add the corresponding rule `{>(1 xxx xxx xxxx):sp1}` to the `PDMS-SP Service InboundCallRoute` parameter to make the call on its `SP1` trunk.

  You can change the last rule to `{(290 333 100|200 444 101)>(1 xxx xxx xxxx):sp1}` if you want to limit the gateway to allow just the two stated caller numbers to make such calls.

VG for calls with access via SIP URL

You can configure a gateway with a SIP URL as the access number that the device accesses over one of the SP trunks. For example, you can set the gateway access number as SP1(`"some-sip- server.mydomain.com"`), or SP2(`"192.168.15.111:5062"`), etc.

When using an SP trunk to access a (SIP) gateway, the device:

- Doesn't use the outbound proxy, ICE, or STUN regardless of the settings on the SP trunk.
- Uses only the device's local address as the SIP Contact, and ignores any NATed address discovered by the device.
- Uses the gateway's SIP URL to form the FROM header of the outbound INVITE.

- Uses the gateway's `AuthUserID` and `AuthPassword` for authentication.
- Applies the symmetric RTP concept.

For more information on Voice Gateway parameters, see the Voice Gateway Parameters table in the *Poly ATA 400 Series Parameter Reference Guide*.

Trunks

Each supported voice service on your device is referred to as a *trunk*, from the telco term for a physical wire or wires that deliver phone services to homes or businesses.

Each trunk is represented with 2-letter abbreviation and a 1-based instance identifier:

- SP1 = the SP1 Voice Service (with ITSP A, B, C, D, E, or F)
- SP2 = the SP2 Voice Service (with ITSP A, B, C, D, E, or F)
- SP3 = the SP3 Voice Service (with ITSP A, B, C, D, E, or F)
- SP4 = the SP4 Voice Service (with ITSP A, B, C, D, E, or F)
- PP1 = the OBiTALK Service

When configuring your phones, you can omit the instance identifier if it's equal to 1. For example, PP is equivalent to PP1. You use these short-hand notations heavily when configuring your phone, as they're found in call routes, call forward numbers, and speed dials parameters. Unless stated otherwise, the abbreviated trunk names are case insensitive.

Trunk Groups

A trunk group is a group of trunks. If a call is routed to a trunk group, your phone picks one of the available trunks from the group to make the call.

The availability of a trunk is based on the following criteria:

- Whether the trunk's digit map allows the number to call, AND
- Whether the trunk has capacity to make one more call

You can configure as many as four trunk groups on your phone.

Configure a Trunk Group

Reference a trunk group and its associated digit map using the short name TG*n* and (Mtgn). Then reference them in other digit maps and call routing rules so that the system can route calls to a particular trunk group.

Only trunks can be added to a trunk group. These include: PP, SP1 - SP4, VG1, VG2, ..., VG8, TG1, TG2, TG3, and TG4.

NOTE: A trunk group can include another trunk group (it can be recursive). However, you must make sure this doesn't result in infinite recursion.

1. In the system web interface, go to **Voice Services** > **Gateways and Trunk Groups**.
2. In the **Default** column, clear the check boxes for the following settings, then configure them in the **Value** column.

Table 12-4 Trunk Group Parameters

Parameter	Value
`Enable`	Select the check box to enable the use of the trunk group.
`Name`	Enter a user-friendly name to describe the trunk group.
`TrunkList`	Enter a comma-separated list of trunks to include in this group.
`DigitMap`	Enter a digit map to direct calls to use this trunk group.

3. Select **Submit**.
4. Restart your system when you complete your changes.

13 Troubleshooting

Use the following information to troubleshoot issues with your Poly ATA device.

System Logs

Logs contain information about system activities and configurations to help you troubleshoot issues.

Activate Syslog Messaging

Enable your Poly ATA 400 Series system to send syslog messages for troubleshooting.

1. In the system web interface, go to **System Management** > **Device Admin** > **Syslog**.
2. In the **Default** column, clear the check boxes for **Server**, **Port**, and any **Level** settings you want to modify.
3. In the **Value** column, enter the hostname, FQDN, or IP address for your syslog server for `Server`.
4. Set the `Port` to `514`.
5. For the **Level*X*** settings, choose options from the drop-down menus for the reporting levels you require.
6. For the **Reporting*X*** settings, configure the options to enable the system to periodically upload buffered syslog files to a web server.
7. Select **Submit**.
8. Restart your system when you complete your changes.

Include Detailed SIP Messages in Syslog Messaging

Include detailed SIP messages in your syslog messages.

1. In the system web interface, go to **Voice Services** > **SP*N*Service**.
2. Under **Debug Options**, set the `X_SipDebugOption` parameter to the reporting level you require.
3. In the `X_SipDebugExclusion` parameter, enter a list of SIP methods (requests and responses) to exclude from the log.

   For troubleshooting a call flow, you can exclude methods such as `OPTIONS` that are used for keep-alive purpose in most cases.

View SPN Service Status Messages

View any error messages displayed if there's a problem with the registration or authentication with a service.

If a problem exists with the registration or authentication of your system with a prescribed service, a SIP 4xx error message displays.

- In the system web interface, go to **Status** > **System Status** > **SPN Service Status**.

  The status for this service displays, including any error messages.

SPN Service Status Error Messages

The following table lists some of the SPN Service Status error messages you might encounter when a firmware upgrade fails.

Table 13-1 SPn Service Status Error Messages

Error Message	Description
400 Bad Request	The server can't understand the request.
401 Unauthorized	The request must perform authentication.
402 Payment Required	Indicates that payment is required for further processing of request.
403 Forbidden	Sent when the server understands the request and found the request to be formulated correctly, but isn't servicing the request.
404 Not Found	The server hasn't found the SIP URI indicated by the user.
405 Method Not Allowed	The request contains a list of methods that aren't allowed.
406 Not Acceptable	The request can't be processed due to a requirement in the request message.
407 Proxy Authentication Required	Indicates that the UAC first has to authenticate itself with the proxy before the request can be processed.
408 Request Timeout	The specified time period in the Expires header field of INVITE request has passed.
423 Interval Too Brief	Returned by a registrar that is rejecting a registration request because the requested expiration time on one or more Contacts is too brief.
480 Temporarily Unavailable	Indicates that the request has reached the correct destination, but the called party isn't available for some reason.
481 Dialog/Transaction Does Not Exist	Indicates that a response referencing an existing call or transaction has been received for which the server has no record or state information.
483 Too Many Hops	Indicates that the request has been forwarded the maximum number of times as set by the Max-Forwards header.
486 Busy Here	Indicates that the user agent is busy and can't accept the call.
487 Request Terminated	Sent by a User Agent that has received a CANCEL request for a pending INVITE request.

Locate the Serial Number on the Device

You can find the serial number on the product label sticker on the bottom side of the device.

1. On the bottom of the device, find the serial number **SN: XXXXXXXXXXXX** (typically 12 digits) on the product label.

   The callout **1** indicates the product label sticker in the diagram.

2. Write down the entire serial number.

Locate the Serial Number in the System Web Interface.

You can locate the serial number for your voice device in the system web interface.

1. Log in to the system web interface.
2. Go to **Status** > **System Status**.
3. Locate the **SerialNumber** in the **Product Information** table.

Packet Capture

The phone can perform a local packet capture to help in troubleshooting.

There are two packet capture options:

- Local packet capture
- Remote PCAP server

Start and Stop a Local Packet Capture

You can start and stop a local packet capture.

1. In the system web interface, go to **System Management** > **Device Admin** > **Packet Capture**.
2. In the **Default** column, clear the check box for **On**.
3. In the **Value** column, select the check box to enable **On**.
4. If you need the device to start a packet capture on reboot, in the **Default** column, clear the check box for `RestartCaptureOnReboot`.
5. If you need the device to start a packet capture on reboot, select the check box in the **Value** column for `RestartCaptureOnReboot`.
6. Select **Submit**.
7. Reproduce the issue.
8. Clear the boxes in the following columns:
   - **On**

- **RestartCaptureOnReboot**

9. Select **Submit**.
10. Go to **System Management** > **Device Update**.
11. Under **Extracting PCAP Capture Result**, select **Extract**. The PCAP file is downloaded to your local computer.

Configure the Remote PCAP Server

Your device can stream PCAP data to a Wireshark client running on your local computer.

On the Wireshark client on your local computer, configure a remote interface for the device using the device's IP address and port.

1. In the system web interface, go to **System Management** > **Device Admin**.
2. Under **Remote PCAP Server**, clear the check box in the **Default** column for **Enable**.
3. Under **Remote PCAP Server**, select the check box in the **Value** column for **Enable**.
4. If you need to change the port that the device uses for the PCAP server, clear the check box in the **Default** column for **Port**.
5. If you need to change the port that the device uses for the PCAP server, enter the port number in the **Value** column for **Port**.
6. Select **Submit**.

Firmware Update Error Messages

The following table lists some of the error messages that you might encounter when a firmware update fails.

If a firmware update fails, an error message displays on the *System Management → Device Update* page in the system web interface.

Table 13-2 Possible Error Messages on Firmware Update Failure

Error Message	Description	Suggested Solution
Firmware Package Checksum Error	A corrupted Firmware package file was used for the update.	Check the file and / or re-download the firmware package and try again.
System Is Busy	The device is busy because one of the phone services is in an active call or device provisioning is in progress.	Try to update again later.
Firmware Is Not Modified	The device is already running the same firmware as the one selected for update.	No need to upgrade.

14 Appendix A

Use the following reference information to create ringtones.

Tone Profile Features

Understand the configuration fields that define a tone profile.

You use a semicolon to separate the configuration field.

You cannot use spaces in a tone profile pattern.

Tone Field-1 Composition

This field describes frequency components used for tone synthesis and it supports as many as three different frequencies.

The frequency expression is a string of numeric values with the notation '+' or '-'. The numeric values are the frequency's decimal values in Hz and amplitude in dBm (maximum 3 dBm). Different frequencies are separated by a comma.

Example: `350-18,440-18,550+2`

This example means:

- The first frequency at 350 Hz with strength at -18 dBm
- The second frequency at 440 Hz with strength at -18 dBm
- The third frequency at 550 Hz with strength at +2 dBm

Tone Field-2 Composition

This field describes the overall tone playback duration in seconds.

The expression is a numeric value, and supports as many as 3 decimated digits. The numeric value can negative, zero, positive, or skipped:

- Negative value: tone plays indefinitely
- Zero value: tone playback is skipped
- Positive value: Normal playback duration
- No value: tone plays indefinitely

Example: `30.234`

This example means:

- Tone playback terminates after 30.234 seconds

Tone Field-3 to Field-6 Composition

Field - 3/4/5/6 share the same definition, and each field describes one single cadence segment.

Together, the four fields form a macro-segment, which is repeated until tone playback expires.

The expression is a string of numeric values with the special notation '/', '(', ')' and ','.

Its format is: `t(f_0/on_0+off_0,f_1/on_1+off_1,f_2/on_2+off_2,f_3/on_3+off_3)`

- `t`: the cadence segment duration in seconds
  - Negative value: tone plays indefinitely
  - No value: tone plays indefinitely
  - Zero value: the duration of this particular segment is zero
  - Positive value: Normal playback duration
- `f_0/1/2/3`: a digit to describe which frequency component(s) are used for the synthesis, and can be one of following 8 options (0 through 7)
  - 0: No frequency specified (silent tone)
  - 1: The first frequency
  - 2: The second frequency
  - 3: The first and second frequencies
  - 4: The third frequency
  - 5: The first and third frequencies
  - 6: The second and third frequencies
  - 7: The first and second frequencies if two or more than two frequency components, or the first frequency if only one frequency component is available.

    If no value is provided for `f_0/1/2/3`, it automatically uses the combination of the first one or two available frequency components.
- `on_0/1/2/3`: the tone active time in seconds
  - Negative value: Not allowed
  - No value: infinite tone active time
  - Others: normal tone active time (as many as 3 decimated digits)
- `off_0/1/2/3`: the tone inactive time in seconds

- Negative value: Not allowed
- No value: infinite tone inactive time
- Others: normal tone inactive time (as many as 3 decimated digits)

Example: `4(1/.3+2.34,3/2+1.5)`

This example means:

- Use the first frequency to generate a tone for 0.3 seconds
- Follow this tone with 2.34 seconds of silence
- Use a combination of the first and second frequencies to generate a tone for 2 seconds
- Follow this tone with 1.5 seconds of silence
- The cadence operates repeatedly for 4 seconds.

Tone Examples

The examples in this section demonstrate how to interpret some of the common tone patterns.

Dial Tone

View an example of a dial tone definition. A dial tone plays to prompt a user to enter the target number to call.

```
DIAL, "350-18,440-18"
```

The dial tone is generated as a mixture of two frequency components:

350 Hz at -18 dBm and 440 Hz at -18 dBm

The expiration time is infinite, and the tone active time is infinite.

Busy Tone

View an example of a busy tone definition. A busy tone plays to indicate to the user that the target number is on another call.

```
BUSY, "480-18,620-18;10;(.5+.5)"
```

The busy tone is generated as a mixture of two frequency components:

480 Hz at -18 dBm and 620 Hz at -18 dBm

The expiration time is exactly 10 seconds. It has only one cadence segment, which has a tone active 0.5 second and a tone inactive 0.5 second.

Prompt Tone

View an example of a prompt tone definition. A prompt tone plays to prompt a user to enter a number for configuration, such as speed dial.

```
PROMPT, "480-16;10"
```

The prompt tone is generated from a single frequency component:

480 Hz at -16 dBm. The expiration time is exactly 10 seconds. It has only one cadence segment, which has a tone infinite active time.

SIT Tone

View an example of a special information tone (SIT) definition. A SIT tone plays to prompt a user that a call has failed.

```
SIT_1, "985-16,1428-16,1777-16;20;
(1/.380+0,2/.380+0,4/.380+0,0/0+4)"
```

The SIT is generated from a set of frequency components:

- First frequency: 985 Hz at -16 dBm
- Second frequency: 1428 Hz at -16 dBm
- Third frequency: 1777 Hz at -16 dBm

The expiration time is exactly 20 seconds. It has only one cadence segment, which includes 4 on-off sections. The segment has infinite repeating time:

- The first on-off section: generated by the first frequency component, and it has 0.38 seconds tone active time and 0 seconds inactive time.
- The second on-off section: generated by the second frequency component, and it has 0.38 seconds tone active time and 0 seconds inactive time.
- The third on-off section: generated by the third frequency component, and it has 0.38 seconds tone active time and 0 seconds inactive time.
- The fourth on-off section: only generate silence since no frequency component is specified. It has 0 seconds tone active time and 4 seconds inactive time.

Stutter Tone

View an example of a stutter tone definition. A stutter dial tone plays to prompt a user that they have voicemail messages.

```
STUTTER, "350-18,440-18;20;.2(.1+.1);()"
```

The stutter dial tone is generated from a mixture of two frequency components:

350 Hz at -18 dBm and 440 Hz at -18 dBm. The expiration time for the entire tone is exactly 20 seconds. It has two cadence segments.

- The first segment includes only one on-off section, on 0.1 second and off 0.1 second, and on-off repeats for 2 seconds.
- The second segment includes one on-off section, and has infinite repeating time and infinite tone active time, and plays until the entire tone duration has elapsed.

For more information on Tone Profile A & B parameters, see the Tone Profile A Parameters and Tone Profile B Parameters tables in the *Poly ATA 400 Series Parameter Reference Guide*.

Ring Profile A & B

Use Tone and Ring Profile A default settings for North American telephone standards. Tone and Ring Profile B default settings are set for Australian telephone standards.

You can download tone profiles for other countries from Poly Support.

Ring Profile Features

Understand the configuration fields that define a tone profile.

```
[field-1];[field-2];...;[field - 5]
```

Use a semicolon to separate as many as five configuration fields.

You cannot use spaces in a tone profile pattern.

Ring Field-1 Composition

Field-1 describes the overall ringing duration in seconds.

The expression is a numeric value, and supports as many as 3 decimated digits.

The numeric value can negative, zero, and positive:

- Negative value: Ringing lasts indefinitely
- No value: Ringing lasts infinitely
- Zero value: Ringing is skipped
- Positive value: Normal ringing duration

Example: `30.5`

This example illustrates a ringing tone that terminates after 30.5 seconds.

Ring Field-2 to Field-5 Composition

Fields-2/3/4/5 share the same definition, and each field describes one single cadence segment.

Together, the four fields form a macro-segment, which is repeated until ringing expires.

The expression is a string of numeric values with the special notation '(' , ')' and ','

It has the format as per the following construct:
`t(on_0+off_0,on_1+off_1,on_2+off_2,on_3+off_3)`

`t`: The cadence segment duration in seconds.

- Negative value: Ringing indefinitely

- No value: Ringing indefinitely
- Zero value: Ringing is skipped
- Positive value: Normal ringing duration

`on_0/1/2/3`: The ring active time in seconds.

- Negative value: Not allowed
- 1No value: Infinite ring active time
- Others: Normal ring active time (as many as 3 decimated digits)

`off_0/1/2/3`: The ring inactive time in seconds

- Negative value: Not allowed
- No value: Infinite ring inactive time
- Others: Normal ring inactive time (as many as 3 decimated digits)

Example: `4(.3+2.34,2+1.5)`

This example illustrates a ringing tone comprised of two segments. Ringing is active for 0.3 seconds, followed by 2.34 seconds of silence, then ringing for 2 seconds, and followed by 1.5 seconds of silence.

This cadence operates repeatedly for 4 seconds.

For more information on call waiting tone parameters, see the Ring Profile A or B Call Waiting Tone Parameters tables in the *Poly ATA 400 Series Parameter Reference Guide*.

For more information on ring profile pattern parameters, see the Ring Profile A or B Ring Pattern Parameters tables in the *Poly ATA 400 Series Parameter Reference Guide*.

15 Getting help

Poly is now a part of HP. The joining of Poly and HP will pave the way for us to create the hybrid work experiences of the future.

During the merge of our two organizations, information about Poly products will transition from the Poly Support site to the HP® Support site.

The Poly Documentation Library will continue to host the installation, configuration, and administration guides for Poly products in HTML and PDF format. In addition, the Poly Documentation Library will provide Poly customers with up-to-date status information about the transition of Poly content from the Poly Support site to the HP® Support site.

HP Inc. addresses

HP US
HP Inc.
1501 Page Mill Road
Palo Alto 94304, U.S.A.
650-857-1501

HP Germany
HP Deutschland GmbH
HP HQ-TRE
71025 Boeblingen, Germany

HP UK
HP Inc UK Ltd
Regulatory Enquiries, Earley West
300 Thames Valley Park Drive
Reading, RG6 1PT
United Kingdom

Document information

Model ID: Poly ATA 400, Poly ATA 402

Document part number: 3725-49162-001A

Last update: September 2023

Email us at documentation.feedback@hp.com with queries or suggestions related to this document.