



Poly ATA 400 Series Privacy Guide PVOS- L ATA 4.0.1

SUMMARY

This guide provides end-users and administrators with information about how the featured product collects, shares, and uses data.

Legal information

Copyright and license

© Copyright September 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 About this guide	1
Audience, purpose, and required skills	1
Icons used in Poly documentation	1
2 Privacy-Related Options	2
Access the system web interface	2
Configure speed dial numbers	2
Reset configuration to factory default	3
Call history	3
View SPn Services Stats (n = 1, 2, 3, 4)	4
View WAN status	4
View Wi-Fi status	4
Call status	4
SIP privacy	5
SIP registration	5
3 How Data Subject Rights Are Supported	7
Right to access	7
Right to be informed	7
Right to data portability	7
Right to erasure	7
Right to Object to Processing	8
Right to Restrict Processing	8
Right to rectification	8
4 Purposes of processing personal data	9
5 How admin can be informed of any security anomalies (including data breach)	11
6 How personal data is deleted	12
Appendix A Appendix	13
Find Device IP Address	13
Access Levels	13

1 About this guide

This section provides clarifying information about this guide.

Audience, purpose, and required skills

This guide is intended for the following users.

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

Icons used in Poly documentation

This section describes the icons used in Poly Documentation and what they mean.

-
-  **WARNING!** Indicates a hazardous situation that, if not avoided, **could** result in serious injury or death.
 -  **CAUTION:** Indicates a hazardous situation that, if not avoided, **could** result in minor or moderate injury.
 -  **IMPORTANT:** Indicates information considered important but not hazard-related (for example, messages related to property damage). Warns the user that failure to follow a procedure exactly as described could result in loss of data or in damage to hardware or software. Also contains essential information to explain a concept or to complete a task.
 -  **NOTE:** Contains additional information to emphasize or supplement important points of the main text.
 -  **TIP:** Provides helpful hints for completing a task.
-

2 Privacy-Related Options

There are different configuration options for Poly ATA devices which may affect the privacy options.

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 13](#).

Ensure that you have the password for the Admin user. See [Access Levels on page 13](#) 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.

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.

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.

Reset configuration to factory default

The device can be reset to the factory default condition.

Call history and various statistical information are removed at the same time. Resetting the device configuration should be used with extreme caution as the operation cannot be undone. To do this, press the **Reset** button in the **Reset Configuration** section. A confirmation window will pop up. The device then proceeds to reset the configuration once you confirm that this is indeed what you want to do. The device reboots automatically when factory reset completed.

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`.

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 4xx 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 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.

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.

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.

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.

3 How Data Subject Rights Are Supported

The following information shows how data subject rights are supported.

Right to access

A data subject has the right to view and/or obtain a copy of all personal data for a specific data subject.

Right to be informed

What personal data is collected?

See [Purposes of processing personal data on page 9](#).

How is personal data is used?

See [Purposes of processing personal data on page 9](#).

How long is personal data kept?

Is personal data shared with any third parties and if so, who?

- If personal data is made available when working with Poly support, this data may be shared with Poly's engineering team (which may include 3rd parties and contractors).

How can a data subject be notified of a data breach?

Data Subjects have a right to be notified when their data has been processed without authorization. Please contact your system administrator for the most appropriate method to receive this information.

Right to data portability

A data subject has the right to receive a copy of all personal data in a commonly-used, machine-readable format.

Log files can be downloaded in plain text format.

Right to erasure

A data subject has the right to remove all of his or her own personal data.

Any customer personal data made available when working with Poly support, specific to a support incident, is retained until the information is requested to be removed by the customer.

Right to Object to Processing

The data subject shall have the right to object to certain processing under certain conditions.

Not applicable.

Right to Restrict Processing

The data subject shall have the right to obtain from the controller restriction of processing under certain conditions.

Not applicable.

Right to rectification

A data subject has the right to make corrections to inaccurate or incomplete personal data.

Poly does not manipulate data made available during the support process, so any rectification of inaccuracies of personal data must be performed by the customer directly.

4 Purposes of processing personal data

Poly is the processor of customer data while the customer is the data controller. If someone is an individual user, and the purchase of this product or service has been made by their employer as the customer, all the privacy information relating to personal data in the following table is subject to their employer's privacy policies as controller of such personal data.

Table 4-1 Personal data

Source from where PI collected	Categories of PI collected	Business purpose for collection	Disclosed to the following service providers
Device Identifier Information	<ul style="list-style-type: none">• MAC address (primary device and IP peripherals)• Serial number• Device ID• Display name• System name• IP address• Device geolocation data including Time zone	<ul style="list-style-type: none">• Internal research (product improvement, development and analytics)• Activities to verify or maintain the quality (Product and Sales Engineering Support)• Detecting security incidents• Debugging	AWS (PDMS-SP)

Table 4-1 Personal data (continued)

Source from where PI collected	Categories of PI collected	Business purpose for collection	Disclosed to the following service providers
Device User Information	<ul style="list-style-type: none">• SIP username• SIP URI• SIP alias name• Admin and usernames and passwords• System log files• Tenant ID• Site ID• Room ID• Org ID• DNS information• Network• Identifiers• Email address• Obi number• PCS account code• PCS number	<ul style="list-style-type: none">• Internal research (product improvement, development and analytics)• Activities to verify or maintain the quality (Product and Sales Engineering Support)• Detecting security incidents• Debugging• Short-term, transient use (login)	AWS (PDMS-SP)

5 How admin can be informed of any security anomalies (including data breach)

This table describes how admin can be informed of any security anomalies (including data breach).

Table 5-1 How admin can be informed of any security anomalies (including data breach)

Where to check	Recommended frequency to check
Log files	Daily

6 How personal data is deleted

This table lists how personal data is deleted.

Table 6-1 How personal data is deleted

Data type	Steps to delete	Deletion method
Device Administration	Device information is deleted when the system is reset to factory default configuration. Perform a pinhole factory reset or restore default configuration using the UI.	Reset to factory default configuration.

A Appendix

Use the following topics as reference for the information in this document.

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.

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.

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: 3725-13783-001A

Last update: September 2023

Email us at documentation.feedback@hp.com with queries or suggestions related to this document.