



PRIVACY GUIDE

1.0 | January 2020 | 3725-49159-001A

Poly VVX Business IP Phones, OBi Edition

Getting Help

For more information about installing, configuring, and administering Poly/Polycom products or services, go to Polycom Support.

Plantronics, Inc. (Poly — formerly Plantronics and Polycom)
345 Encinal Street
Santa Cruz, California
95060

© 2020 Plantronics, Inc. All rights reserved. Poly, the propeller design, and the Poly logo are trademarks of Plantronics, Inc. All other trademarks are the property of their respective owners.

Contents

- Before You Begin.....2**
 - Related Poly and Partner Resources.....2

- Privacy-Related Options.....3**
 - Option Locations3
 - Option Descriptions.....3

- How Data Subject Rights Are Supported.....6**
 - Right To Be Informed.....6
 - Right to Access.....6
 - Right to Rectification.....7
 - Right to Erasure7
 - Right to Data Portability.....7
 - Right to Restrict Processing.....8
 - Right to Object.....8

- Purposes for Processing Personal Data.....9**

- How Administrators Are Informed of Any Security Anomalies..... 10**

- How Personal Data is Deleted..... 11**

Before You Begin

Topics:

- [Related Poly and Partner Resources](#)

The *Poly VVX Business IP Phones, OBi Edition Privacy Guide* provides information regarding the implementation of Privacy by Design for this product.

This guide contains details about configurable privacy options and how personal data is processed.

Related Poly and Partner Resources

See the following sites for information related to this product.

- The [Polycom Support Site](#) is the entry point to online product, service, and solution support information including **Licensing & Product Registration**, **Self-Service**, **Account Management**, **Product-Related Legal Notices**, and **Documents & Software** downloads.
- The [Polycom Document Library](#) provides support documentation for active products, services, and solutions. The documentation displays in responsive HTML5 format so that you can easily access and view installation, configuration, or administration content from any online device.
- The [Polycom Community](#) provides access to the latest developer and support information. Create an account to access Poly support personnel and participate in developer and support forums. You can find the latest information on hardware, software, and partner solutions topics, share ideas, and solve problems with your colleagues.
- The [Polycom Partner Network](#) are industry leaders who natively integrate the Poly standards-based RealPresence Platform with their customers' current UC infrastructures, making it easy for you to communicate face-to-face with the applications and devices you use every day.
- The [Polycom Collaboration Services](#) help your business succeed and get the most out of your investment through the benefits of collaboration.

Privacy-Related Options

Topics:

- [Option Locations](#)
- [Option Descriptions](#)

Option Locations

Locations in the following table refer to the system web interface and device local interface. Each configuration parameter on the web page can be equivalently configured on the phone by using a configuration file. The phone can be configured to download a configuration file from a server on each boot up, periodically, or during certain times of the day.

All password fields are masked on the system web interface and device local interface and are excluded from configuration backup files. That is, by design, all password fields are hidden, and no one can backup any password fields from the device.

OBi Edition software has two levels of call logs. System-level call logs contain more call details without statistics and can be accessed via the system web interface only. User-level call logs record the call statistics as well as caller ID details of each call and can be accessed via the device local interface only.

Option Descriptions

Privacy-Related Options

Option Name	Location
System Web Interface Login Credentials: <ul style="list-style-type: none">▪ UserPassword▪ AdminPassword	System Web Interface: The admin can configure a user login password and an admin login password in the System Management/Device Admin page/Web Server section.
Syslog Config: <ul style="list-style-type: none">▪ Server▪ Port▪ Level	System Web Interface: System Management/Device Admin page/Syslog section. Syslog function is disabled if server or port is not provided. Note: The phone doesn't store syslogs internally. It can only send syslog messages to an external syslog server for storage and processing.

Option Name	Location
SIP Credentials: <ul style="list-style-type: none"> ▪ AuthUserName ▪ AuthPassword ▪ URI ▪ X_XsiUsername ▪ X_XsiPassword ▪ X_XmppUserName ▪ X_XmppPassword 	System Web Interface: Voice Services/SPn Service/page/Credentials section.
Network Credentials: <ul style="list-style-type: none"> ▪ 802_1XIdentity ▪ 802_1XPassword ▪ 802_1XAnonymousID 	System Web Interface: System Management/WAN Settings page/Internet Settings section
WiFi Credentials: <ul style="list-style-type: none"> ▪ 802_1XIdentity ▪ 802_1XPassword ▪ 802_1XAnonymousID For each Access Point (1 – 20): <ul style="list-style-type: none"> ▪ SSID ▪ Passwords 	System Web Interface: ObiWiFi Configuration/WiFi Settings page/Internet Settings section System Web Interface: ObiWiFi Configuration/WiFi Settings page/Access Point n section, where $n = 1 – 20$
Remote PCAP: <ul style="list-style-type: none"> ▪ Enable ▪ Port ▪ Clients 	System Web Interface: System Management/Device Admin page/Remote PCAP Server section
Internal PCAP: <ul style="list-style-type: none"> ▪ On ▪ Interface ▪ Storage ▪ PromiscuousMode ▪ WebAccessExcluded 	System Web Interface: System Management/Device Admin page/Packet Capture section
System-Level Call Logs: <ul style="list-style-type: none"> ▪ Remove All ▪ Save All 	System Web Interface: Status/Call History page
User-Level Call Logs: <ul style="list-style-type: none"> ▪ Clear List 	Device Local Interface: Main Menu/Call History

Option Name	Location
Personal Phone Book:	Device Local Interface: Main Menu/Contacts
<ul style="list-style-type: none"> ▪ New Entry 	

How Data Subject Rights Are Supported

Topics:

- [Right To Be Informed](#)
- [Right to Access](#)
- [Right to Rectification](#)
- [Right to Erasure](#)
- [Right to Data Portability](#)
- [Right to Restrict Processing](#)
- [Right to Object](#)

The following information shows how data subject rights are supported.

Right To Be Informed

What personal data is collected?

See [Purposes for Processing Personal Data](#) on page 9.

How is personal data used?

See [Purposes for Processing Personal Data](#) on page 9.

How long is personal data kept?

Customer personal data is kept until a factory reset is performed. See [How Personal Data is Deleted](#). In addition, a user can remove the personal phone book and user-level call logs directly from the device local interface without needing factory reset.

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

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

If personal data is made available when working with Polycom support, this data may be shared with Polycom's engineering team (which may include third parties / 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. The product administrator is able to monitor and identify when certain security anomalies have occurred. See [How Administrators Are Informed of Any Security Anomalies](#) on page 10.

Right to Access

View system details

Information pertaining to the device such as device IP address, serial number, and MAC address are shown on the system web interface and device local interface. An administrator can check them on web page or on the device local interface (under the **Product Information** menu). A user can access the call logs and phone book on the device local interface.

Note: Password information isn't revealed in the system web interface or the device local interface.

Procedure:

1. Connect the phone to the network.
2. From the device local interface, go to the **Product Information** menu and note the IP address of the phone.
3. From a web browser, go to the IP address of the phone and log in as admin.
4. Click the link on the left side panel to view the corresponding pages.

A copy of any personal data made available to Polycom when working with Polycom support is available by requesting it from your Polycom support representative.

Right to Rectification

A data subject has the right to make corrections to their own inaccurate or incomplete personal data. Personal data specific to device configuration can be edited or updated by the device administrator. See [Privacy-Related Options](#) on page 3.

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

Right to Erasure

A data subject has the right to remove all his or her own personal data. For details on how to erase customer personal data from the system, see [How Personal Data is Deleted](#) on page 11.

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

Right to Data Portability

Subject to approval by the device admin, the user may obtain a backup copy of all the web pages in XML file format. These backup pages can be viewed directly as text files or restored into a similar device to be viewed as web pages. Similarly, the user can get a copy of the personal phone book and user-level call logs by uploading each to a server in an XML format. A backup copy of the system-level call history can be obtained from the system web interface with help from the device admin. Note that all password fields are excluded from backup copies of the web pages.

Right to Restrict Processing

Not applicable because the customer is the controller.

Right to Object

Not applicable because the customer is the controller.

Purposes for Processing Personal Data

Purposes for Processing Personal Data

Personal Data Category	Type of Personal Data	Purpose of Processing	Interface Type
Call Logs	Peer Caller ID Name and Number, Timestamp	Provides call history for each call	System web interface for system-level call logs Device local interface for user-level call logs
Personal Phone Book	Contact information: <ul style="list-style-type: none"> Name Number Address Email Company Thumbnail picture 	Allows user to make calls from the phone book. Also allows matching caller ID name/picture by number.	Device local interface
System Web Interface Login Credentials	<ul style="list-style-type: none"> UserPassword AdminPassword 	System web interface login	System web interface
SIP Credentials	<ul style="list-style-type: none"> AuthUserName AuthPassword URI X_XsiUsername X_XsiPassword X_XmppUserName X_XmppPassword 	SIP authentication	System web interface or device local interface
Network Credentials	<ul style="list-style-type: none"> 802_1XIdentity 802_1XPassword 	Network authentication	System web interface or device local interface
Wi-Fi Credentials	<ul style="list-style-type: none"> 802_1XIdentity 802_1XPassword 	Wi-Fi authentication	System web interface or device local interface

How Administrators Are Informed of Any Security Anomalies

How Administrators Are Informed of Any Security Anomalies (Including Data Breaches)

Security Anomaly Type	Where to Check	Recommended Frequency to Check
System reboots and crashes	<ul style="list-style-type: none"> Device LED and local interface indicate clearly if the device has rebooted. Reboot events are recorded in syslog logs that indicate the reason for each reboot (or no reason if the system crashes). 	Check the log file after each reboot to analyze the reason for the reboot.

Log Type

Log Type	Description	Purpose	Location
SYSLOG	<p>The detail types of data to include are configurable.</p> <p>Data may include: boot up/system initialization information, network initialization information, call events, network/system events.</p> <p>It can include SIP Transactions for REGISTER, SUBSCRIBE/NOTIFY, and Call Signaling for all calls on certain lines.</p> <p>Note that the phone does not store syslog files internally. It only sends the log to the configured syslog server to be stored and processed.</p>	Troubleshooting	System web interface
PCAP	All network traffic.	Troubleshooting	System web interface

How Personal Data is Deleted

How Personal Data is Deleted

Data Type	Steps to Delete	Deletion Method
SIP, Web, Network, and Wi-Fi Credentials	Factory Reset via system web interface: Go to the Device Management/Device Update web page and press Reset with the Voice Configuration option checked	Internal configuration file removal with disk overwritten.
User-Level Call Logs	From the device local interface: Go to Main Menu/Call History and select Clear List . From the system web interface: Go to the Device Management/Device Update page and press Reset with the User Data option checked.	Internal call history file removal with disk overwritten.
System-Level Call Logs	From the system web interface: Go to the Device Management/Device Update page and press Reset with the User Data option checked. Note that this method also removes user-level call logs and personal phone book.	Internal call history file removal with disk overwritten.
Phone Book	From the device local interface: Go to Main Menu/Contacts and select Remove All . From the system web interface: Go to the Device Management/Device Update page and press Reset with the User Data option checked. Note that this method also removes the system-level and user-level call logs.	Internal phone book file removal with disk overwritten.