PRIVACY GUIDE

September 2021 | 3725-86188-004A

Poly G7500 and Poly Studio X Family

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

Contents

Before You Begin

Topics:

The *Poly G7500 and Poly Studio X Family Privacy Guide* provides information on how Poly products utilize customer data and how customers can configure G7500 and Studio X Family systems to process personal data.

Related Poly and Partner Resources

See the following sites for information related to this product.

- The Poly Online Support Center is the entry point to online product, service, and solution support information including Video Tutorials, Documents & Software, Knowledge Base, Community Discussions, Poly University, and additional services.
- The Poly 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 Poly 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 Poly Partner Network is a program where resellers, distributors, solutions providers, and unified communications providers deliver high-value business solutions that meet critical customer needs, making it easy for you to communicate face-to-face using the applications and devices you use every day.
- The Poly Services help your business succeed and get the most out of your investment through the benefits of collaboration.

Privacy-Related Options

Topics:

There are different deployment options for your system that may affect the privacy options and supporting requirements described below. These details apply specifically to G7500 and Studio X Family systems deployed in a customer premises and managed by the customer.

System Usage Data Collected by Poly

Poly automatically collects and analyzes product usage data, device data, call detail records (CDRs), and quality of service (QoS) data from your system.

Data collected is used for the purposes of license verifications, product improvements, support operations, improving overall user experience, and future product innovations.

The system sends the following information to Poly:

- Device information, including the hardware and software versions of primary and secondary devices
- Device health data, including CPU and memory usage
- Call experience statistics
- Call detail record (CDR) and call health
- Device-level network analytics
- Data and statistics related to device or feature usage

Send Usage Data to Poly

You can help Poly improve its products and services by allowing the collection of usage data from your system.

With your agreement, the system sends the following information to Poly Cloud Services and the Device Analytics service:

- Basic device information, including hardware and software versions
- Basic device configuration data
- Data and statistics related to device or feature usage
- Device health data, including CPU and memory usage

Procedure

1. In the system web interface, go to **Servers** > **Cloud** > **Preferences**.
2. Click the link to read the “Terms and Conditions”.
3. Select the check box to agree to the data collection.

Call Detail Report (CDR)

When enabled, the Call Detail Report (CDR) feature keeps a record of every incoming, outgoing, and missed call that occurs on the system. If a call does not connect, the report shows the reason. In multipoint calls, each far site is shown as a separate call, but all have the same conference number.

You can find the CDR in the system logs.

Enable the Call Detail Report Feature

Enable the Call Detail Report feature to keep a record of the system's most recent call entries. When enabled, you can download call records and view the room system's call history. Within five minutes after ending a call, the CDR is written to memory.

Procedure

1. In the system web interface, go to **Call Configuration** > **Recent Calls**.
2. Mark the **Call Detail Report** check box.

Configure the Recent Calls List

You can display recent calls on the **Place a Call** page in the system web interface.

The recent calls list includes the following information:

- Name or number
- If the system placed or received the call
- Date and time

Procedure

1. In the system web interface, go to **Call Configuration** > **Recent Calls**.
2. Configure the following settings (your changes save automatically):

Setting	Description
Call Detail Report	Call detail record (CDR) information is in the system logs. When disabled, the system doesn’t write call information.
Enable Recent Calls	Specifies whether to show recent calls on the local interface and the system web interface.
Maximum Number to Display	The maximum number of calls the system displays in the recent calls list.

Create Local Administrator Credentials

You can require local administrator credentials for in-room and remote access to the system.

Passwords for logging in to the system are case sensitive and can't contain more than 40 characters.

Procedure

1. In the system web interface, go to **Security** > **Local Accounts**.
2. Configure the following settings:

Setting	Description
Admin ID	The local administrator account name (default is `admin`).
Room Password	You must enter this password to change administrator settings in the local interface. The default password is the last six characters of the serial number listed in **System Details** and on the back of the device.
Remote Access Password	If you set this option, you must enter this password to access the system through the system web interface or command-line API (SSH or telnet). This password lets you perform device management tasks, such as updating the system's software.

3. Optional: Do one of the following:
   - To use the local administrator **Room Password** for remote logins, leave the **Use Room Password for Remote Access** option enabled.

     Note: Password requirements for the local administrator password and remote access password must be configured separately.

   - If you don't want to use the local administrator **Room Password** for remote logins, disable the **Use Room Password for Remote Access** option.

   This setting specifies that the system uses the local administrator **Room Password** for remote logins. This setting is enabled by default.
4. Select **Save**.

Setting Up a Directory

You can register your system with a directory to call contacts in your organization.

The system supports the following directory features:

- Up to 2,000 local contacts
- Up to 2,000 Favorites

- Up to 200 Favorites groups
- Global groups (local groups aren't supported)
- Up to 4,000 contacts from a Polycom GDS server

Register with the Polycom Global Directory Server

You can register your system with the Polycom Global Directory Server (GDS).

Enable H.323 on your system before you register it with this directory server.

Procedure

1. In the system web interface, go to **Servers** > **Directory Servers**.
2. In the **Server Type** field, select **Polycom GDS**.
3. Configure the following settings:

Setting	Description
Server Address	Specifies the IP or DNS address of the Polycom GDS.
Password	The Polycom GDS password, if one exists.

4. Select **Save**.

Register with an LDAP Directory Server

You can register your system with an LDAP directory server.

Procedure

1. In the system web interface, go to **Servers** > **Directory Servers**.
2. In the **Server Type** field, select **LDAP**.
3. Configure the following settings:

Setting	Description
Server Address	Specifies the address of the LDAP directory server. When provisioned, this setting is read-only.
Server Port	Specifies the port for connecting with the LDAP server. When provisioned, this setting is read-only.
Base DN (Distinguished Name)	Specifies the top level of the LDAP directory where searches begin. When provisioned, this setting is read-only. To avoid LDAP registration issues, make sure the base DN is at least one level deeper than your domain. For example, enter `ou=users,dc=example,dc=com` instead of `dc=example,dc=com`.

Setting	Description
Multitiered Directory Default Group DN	Specifies the top-level group of the LDAP directory required to access its hierarchical structure. When provisioned, this setting is read-only.
Authentication Type	Specifies the protocol for authenticating with the LDAP server: ▪ **NTLM** ▪ **Basic** ▪ **Anonymous**
Bind DN (Distinguished Name)	Specifies the bind DN when using basic authentication. Available only when you set **Authentication Type** to **Basic**. When provisioned, this setting is read-only.
Use SSL (Secure Socket Layer)	When enabled, encrypts data to and from the LDAP server.
Domain Name	Specifies the domain name for registering with the LDAP server.
User Name	Specifies the user name for registering with LDAP server.
Password	Specifies the password for registering with the LDAP server.

4. Select **Save**.

Managing Contacts and Favorites

You can create local contacts and designate favorites for your system.

Types of Favorites

The system web interface displays several types of favorites.

Directory Server Registration	Types of Contacts
Polycom GDS	▪ Directory entries created locally by the user. ▪ References to Polycom GDS entries added to **Favorites** by the user. These entries are available only if you successfully register the system with Polycom GDS. Users can delete these entries from **Favorites**, but they can't edit these entries. Users can copy these entries to other **Favorites** and remove them from those groups.

Directory Server Registration	Types of Contacts
LDAP with H.350	▪ Directory entries created locally by the user. ▪ References to LDAP directory entries added to **Favorites** by the user. These entries are available only if the system can successfully access the LDAP server. Users can delete these entries from **Favorites**, but they can't edit these entries. Users can copy these entries to other **Favorites** and remove them from those groups.

Manage Contacts

You can add contacts individually or in bulk in the system web interface.

You need local administrator access for this feature.

Procedure

1. Do one of the following:
   - Go to **Dashboard** > **Contacts**.
   - Go to **Place a Call** > **Contacts**.
2. Select **More** ⋮ and choose one of the following options:
   - **New Contact**: Create a single contact.
   - **Import**: Upload contacts in bulk using an XML file (can't exceed 3 MB).
   - **Export**: Download local contacts to an XML file (doesn't include contacts available through a directory server).

Unfavorite a Contact

Unfavorite a contact to remove the contact from your **Favorites** list.

Procedure

1. Go to **Place a Call** > **Favorites**.
2. Choose a favorite card, then select **Unfavorite**.

   The contact is removed from the **Favorites** list.

Register the System with RealPresence Resource Manager Provisioning Service

Before you can provision a system, you must register it with a provisioning service.

Note: Make sure to configure your provisioning server (for example, RealPresence Resource Manager) ahead of time so that it recognizes and works with your endpoint.

For information on how to provision your system with RealPresence Resource Manager, see the *Polycom RealPresence Resource Manager System Operations Guide*.

Procedure

1. In the system web interface, go to **Servers** > **Provisioning Server**.
2. Select **Enable Provisioning**.
3. Select **Load Discovered Information**.

   The registration fields update automatically if your system detects a provisioning server.
4. Optional: If your system didn't detect a provisioning server, complete the following fields (contact your network administrator for help):

Setting	Description
Authentication Type	The type of authentication the system uses to connect to the provisioning server.
Server Address	Address of the system running the provisioning service. The format is `https://<server>/ucservice`. For example, `https://video.myrpp.poly.com/ucservice`.
Domain Name	Domain for registering with the provisioning service. This option doesn't display if you select **Basic** as the authentication type.
User Name	User ID for registering with the provisioning service.
Password	Password for registering with the provisioning service.

5. Select **Save**.
6. Verify that **Registration Status** changes from **Pending** to **Registered**.

   It might take a minute or two for the status to change.

Retrieve Log Files

You can use the web interface to download log files to a location on your computer.

Note: The date and time of the system log entries for devices are shown in GMT.

Procedure

1. Access the web interface by opening a web browser and entering the IP address of the system using the format https://IPaddress (for example, https://10.11.12.13), and go to **Diagnostics > Logs**.
2. Select **Download system logs**. A dialog window opens for you to specify how you want to open or save the .tgz file.

Related Links

Right to Access on page 10

How Data Subject Rights Are Supported

Topics:

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 of their own personal data.

Personal data about specific participants in conferences can be viewed or downloaded via the CDR.

For details about how to access personal data sent to Polycom RealPresence Resource Manager, see the User Data Collection section of the *Polycom RealPresence Resource Manager Operations Guide*. To see details of the usage data sent to Poly, see the *Security and Privacy White Paper for Poly G7500, Studio X70, Studio X50, and Studio X30*.

Related Links

Retrieve Log Files on page 9

Right to Be Informed

What personal data is collected?

See Purposes of Processing Personal Data on page 13.

How is personal data is used?

See Purposes of Processing Personal Data on page 13.

How long is personal data kept?

All data saved to the system is retained until manually deleted by the administrator. This includes saved content files, recent rooms information, and configuration settings. Log files are automatically deleted (oldest first) when the file limit is reached. By default, call detail records (CDRs) are overwritten by new CDR data via rolling logs configurable by the system administrator.

For details about how to access personal data sent to Polycom RealPresence Resource Manager, see the User Data Collection section of the *Polycom RealPresence Resource Manager Operations Guide*. To see details of the usage data sent to Poly, see the *Security and Privacy White Paper for Poly G7500, Studio X70, Studio X50, and Studio X30*.

See Purposes of Processing Personal Data on page 13 and How Personal Data is Deleted on page 15.

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 third 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.

See How Personal Data is Deleted on page 15 and How Administrators Are Informed of Any Security Anomalies (Including Data Breaches) on page 14.

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.

- CDRs can be downloaded in CSV format.
- The Address Book can be exported in XML format.
- Audit and log files can be downloaded in plain text format.

Right to Erasure

Any customer personal data made available when working with Poly support will be erased by requesting erasure through your Poly support representative.

For details on how to erase customer personal data from the system, see How Personal Data is Deleted on page 15.

Right to Rectification

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

Personal data specific to device configuration can be edited or updated by the device administrator.

Personal data about specific participants in conferences cannot be edited or updated because the information derives from the device of origin.

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

Right to Object to Processing

Not applicable.

Right to Restrict Processing

Not applicable.

Purposes of Processing Personal Data

For these details, see the *Security and Privacy White Paper for Poly G7500, Studio X70, Studio X50, and Studio X30*.

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

How Administrators are Informed of Any Security Anomalies

Security Anomaly Type	Where to Check	Recommended Frequency to Check
All active alerts	An administrator can configure alerts and monitor using the local interface, system web interface, SNMP monitoring, or Polycom RealPresence Resource Manager (if configured).	Once daily

How Personal Data is Deleted

Topics:

How Customer Personal Data is Deleted

Data Type	Steps to Delete	Deletion Method
Call detail record (CDR)	▪ By default, CDRs are overwritten by new CDRs periodically via rolling logs configurable by device administrator. ▪ CDRs can also be deleted by performing a standard or comprehensive restore operation. ▪ Factory restore the system.	File delete with overwrite.
Directory/Contacts	▪ See the "Setting Up a Directory" section in the *Poly Video Mode Administrator Guide*. ▪ The contacts can also be deleted by resetting the system.	Delete from database.
System log files	▪ Log files are automatically deleted by the system (oldest first) when the system reaches the file limit. These settings can be configured by the device administrator from **Diagnostics.** > **Logs** > **Log Management**. ▪ Log files are also deleted by resetting the system.	File delete with overwrite.
All other personal data stored locally on the system	Factory restore the system.	File delete with overwrite.

For details about how personal data is deleted on Polycom RealPresence Resource Manager, see the User Data Collection section of the *Polycom RealPresence Resource Manager Operations Guide*.

Reset System Settings

You can reset your system to its default configuration settings.

You may need to perform a system reset for a variety of reasons, for example, when moving a device to a new location.

Resetting your system deletes all but the following data:

- Current software version
- User-installed PKI certificates
- Local directory entries
- Logs
- Call detail record (CDR)

You also can choose not to retain some of this data after the system resets.

Note: A system reset restores your system to its original mode of operation (for example, Poly Video Mode or Poly Partner Mode).

Procedure

1. In the system web interface, go to **Diagnostics** > **System Reset**.
2. Select **Reset All System Configurations**.
3. Optional: Clear any of the following check boxes for data you want to delete as part of the reset:
   - **Keep installed certificates.**
   - **Keep the directory entries.**
   - **Keep the system logs.**
   - **Keep the system call detail reports.**
4. Select **Reset**.

Factory Restore the System

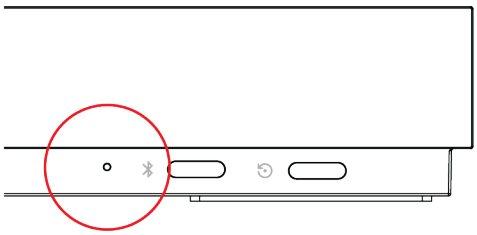
A factory restore completely erases the system's flash memory and restores it to a stable software version. See the *Poly VideoOS Release Notes*, Version History section, for the current factory restore version.

The system doesn't save the following data with a factory restore:

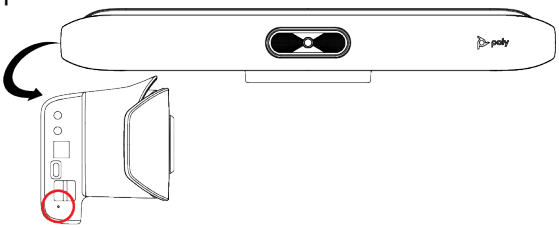
- Current software version
- Logs
- User-installed PKI certificates
- Local directory entries
- Call detail record (CDR)

Procedure

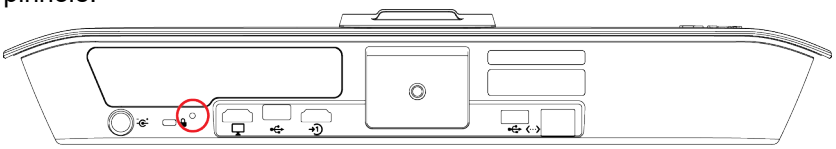
1. Disconnect the power supply to turn off the system.
2. Do one of the following:
   - On the front of the G7500, insert a straightened paper clip through the factory restore pinhole.



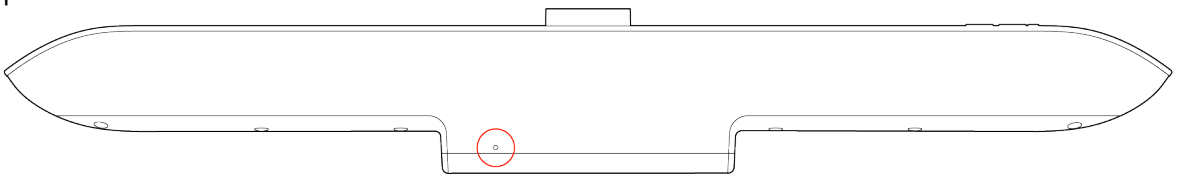
- On the side of the Studio X50, insert a straightened paper clip through the factory restore pinhole.



- On the bottom of the Studio X30, insert a straightened paper clip through the factory restore pinhole.



- On the bottom of the Studio X70, insert a straightened paper clip through the factory restore pinhole.



3. While continuing to hold the restore button, reconnect the power supply to turn the system on.
4. When the system LED indicator light turns amber, stop pressing the restore button.

   You can only view the restore progress on a display connected to the secondary monitor HDMI output port.

   Note: You can’t view the restore progress for a Studio X30 system because it doesn't support a secondary monitor connection.