PRIVACY GUIDE

1.1.0 | February 2020 | 3725-32915-002A

Poly G200

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 G200 Privacy Guide provides information on how Poly products utilize customer data and how customers can configure Poly G200 systems to process personal data.

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:

There are different deployment options for G200 which may affect the privacy options and supporting requirements described below. These details apply specifically to G200 deployed in a customer premises and managed by the customer.

Call Detail Report (CDR)

The Call Detail Report (CDR) feature keeps a record of every incoming, outgoing, and missed call that occurs on the system. The Call Detail Report in Poly G200 system only includes the basic call information: time and call number. It can be viewed from the local user interface and the system web interface.

The CDR is not downloadable in the first release.

The CDR database is limited to the most recent 150 entries. Entries are automatically deleted by the system (oldest first) when the system reaches the entries limit. These entries cannot be deleted manually, neither from the user interface nor from the API.

The CDR is enabled as default. There is no user interface to enable or disable CDR feature.

Related Links

Right to Access on page 11

Related Links

Configure H.323 Settings on page 6
Configure SIP Settings on page 7
Configure SVC Call Settings on page 8
Add, Edit, or Delete Contacts on page 4

View 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:

- Call number
- If the call was placed or received
- Date and time

Procedure

» Do one of the following:
  - In the system web interface, go to **Place a Call** > **Recent Calls**.
  - In the local interface, go to **Place a Call** > **Recent**.

Change the Password

You can change the G200 system admin password from the system web interface.

Poly recommends that only administrators access the Poly G200 system configuration. Therefore, Poly provides only one credential for the system web interface.

Procedure

1. Go to **Admin Settings** > **Password**.
2. Configure the following settings and select **Submit**.

Setting	Description
Old Password	Specifies the existing password for the administrator account used when logging in through the system web interface. When creating a password for the first time, leave this setting blank.
New Password	Specifies a new password. The password is case sensitive and must be less than 40 characters without spaces.
Confirm Password	Confirms the new password.

Related Links

Right to Rectification on page 12

Add, Edit, or Delete Contacts

You can add, edit, and delete contact information from the G200 system web interface.

You can manage up to 1000 contacts. The contact information only includes name and number, IP address, or SIP URL.

Procedure

1. In the system web interface, go to **Contacts.**
2. Do one of the following:
   - Click **Add Contact** and enter contact information.
   - Click **Edit Contact** to modify the contact.
   - Click **Delete Contact** to delete the contact.

Related Links

Right to Access on page 11
Call Detail Report (CDR) on page 3
Right to Data Portability on page 12
Importing and Exporting System Settings on page 9
Right to Erasure on page 12
Right to Rectification on page 12

Import Directory Contacts

You can import directory contacts to your G200 system from the system web interface.

Make sure the system isn't in a call when you begin the import.

Note the following when importing directory contacts:

- The size of the uploaded CSV file can't exceed 100 kilobytes.
- The number of contacts in the file must be less than 1000.
- When the uploaded CSV file includes entries already on your G200 system, the system deletes the duplicate files.

Procedure

1. In the system web interface, go to **Contacts** and select **Import Contacts**.
2. In the dialog box, select the *directory*.csv file you want to import and select **Open**.
3. Select **Import** to upload the *directory*.csv file to the G200 system.

Export Directory Contacts

You can export directory contacts from the G200 system web interface to local devices, such as computers and tablets, in CSV file format.

Make sure the system isn't in a call when you begin the export.

Procedure

1. In the system web interface, go to **Contacts** and select **Export Contacts**.
2. Save the downloaded *directory*.csv file on your local device.

Configure Deployment Mode

You can manually configure the deployment mode from the system user interface.

You can't configure the deployment mode when the G200 system is in a call, sharing content, or upgrading the camera.

Procedure

1. In the system web interface, go to **System Settings** > **Deployment Mode**.
2. Choose the mode from the drop-down list and select **Submit**.

Note: The system automatically reboots to apply the change.

Configure H.323 Settings

If your network uses a gatekeeper, the G200 system can register its H.323 name and extension. This enables others to call the system by entering the H.323 name or extension instead of the IP address.

The following settings are only available for AVC mode.

Procedure

1. In the system web interface, go to **Server Settings** > **Call Server**.
2. Configure the following settings and select **Submit**.

Setting	Description
Communication Protocol	Specifies the registrar protocol. Select **H.323**.
Enable H.323 Registration	Enables you to display and configure the H.323 settings.
Gatekeeper Address	Gatekeeper address that the network is using.
H.323 Name	Specifies the name that gatekeepers and gateways use to identify this system. You can make point-to-point calls using H.323 names if both systems are registered to a gatekeeper.
H.323 Extension (E. 164) (My Number)	Enables users to place point-to-point calls using the extension if both systems are registered with a gatekeeper, and specifies the extension that gatekeepers and gateways use to identify this system. Your organization's dial plan might define the extensions you can use.
Require Authentication	Enables support for H.235 Authentication. When H.235 Authentication is enabled, the H.323 gatekeeper ensures that only trusted H.323 endpoints are allowed to access the gatekeeper. This setting is available when **Enable H.323 Registration** is set to **Enable**.

Setting	Description
Authentication User Name	When authentication is required, specifies the user name for authentication with H.235.
Password	When authentication is required, specifies the password for authentication with H.235.

Related Links

Right to Access on page 11
Call Detail Report (CDR) on page 3

Configure SIP Settings

If your network supports SIP, you can use SIP to connect IP calls.

The SIP protocol has been widely adapted for voice over IP communications and basic video conferencing; however, many of the video conferencing capabilities are not yet standardized. Many capabilities also depend on the SIP server.

The following settings are only available for AVC mode.

Procedure

1. In the system web interface, go to **Server Settings** > **Call Server**.
2. Configure the following settings and select **Submit**.

Setting	Description
Communication Protocol	Specifies the registrar protocol. Select **SIP**.
Transport Protocol	Indicates the protocol the system uses for SIP signaling. The SIP network infrastructure your G200 system operates within determines which protocol is required. • **TCP**: Provides reliable transport via TCP for SIP signaling. • **UDP**: Provides best-effort transport via UDP for SIP signaling. • **TLS**: Provides secure communication of the SIP signaling. TLS is available only when the system is registered with a SIP server that supports TLS. When you choose this setting, the system ignores TCP/UDP port 5060. Select TLS if you want to encrypt AVC calls.
Enable SIP Registration	Enables you to configure the SIP settings.
Server Address	Specifies the DNS FQDN or IP address of the SIP proxy server. By default for TCP, the SIP signaling is sent to port 5060 on the proxy server. By default for TLS, the SIP signaling is sent to port 5061 on the proxy server.
Domain	Specifies the domain of the SIP proxy server.

Setting	Description
SIP Address (My Number)	Specifies the SIP address or SIP name of the system, for example, `mary.smith@department.company.com`. If you leave this field blank, the system's IP address is used for authentication.
User Name	Specifies the user name to use for authentication when registering with a SIP proxy server, for example, `marySmith`. If the SIP proxy server requires authentication, this field and the password cannot be blank.
Password	Specifies the password associated with the user name used to authenticate the system to the proxy server. The password can be up to 47 characters in length.

Related Links

Right to Access on page 11
Call Detail Report (CDR) on page 3

Configure SVC Call Settings

If you use SVC mode, use the Poly RealPreasence Clariti Ensemble server as the call server.

Make sure to enable SVC deployment mode.

Important: Poly RealPreasence Clariti Ensemble 1.0 only supports English device names.

Procedure

1. In the system web interface, go to **Server Settings** > **Call Server**.
2. Configure the following settings and select **Submit**.

Setting	Description
Device Name	Specifies the name of your G200 system registered to the RealPreasence Clariti Ensemble server. **Note:** To avoid duplicate device names, you must change the default device name.
Server Address	Specifies the RealPresence Clariti Ensemble server you want to use. **Note:** If the RealPresence Clariti Ensemble server doesn't use the default FQDN/IP port 443, you need to specify the port in the server address as *<ip>*:*<port>*. For example: `10.11.12.13:446`.
User Name	Specifies the user name that registers the system to the RealPresence Clariti Ensemble server.
Password	Specifies the password that registers the system to the RealPresence Clariti Ensemble server.

Related Links
Right to Access on page 11
Call Detail Report (CDR) on page 3

Importing and Exporting System Settings

You can export existing G200 system settings to local devices, such as computers or tablets, in .cfg format.

You can also import system web interface settings from a device to a G200 system to enable quick manual configuration.

Related Links
Right to Data Portability on page 12
Related Links
Add, Edit, or Delete Contacts on page 4
Download System Logs on page 9

Import System Settings

You can import G200 system settings from the system web interface.

Procedure

1. In the system web interface, go to **System Settings** > **Import and Export Configuration**.
2. Select **Choose File** and select a .cfg file to import.
3. Select **Import** to upload the .cfg file to the G200 system.

   The G200 system restarts after the file successfully imports.

Export System Settings

You can export G200 settings from the system web interface.

Procedure

1. In the system web interface, go to **System Settings** > **Import and Export Configuration**.
2. Select **Export** and save the downloaded .cfg file to your system.

Download System Logs

You can download system logs of your G200 system.

The date and time of the log entries display in GMT.

Procedure

1. In the system web interface, go to **Diagnostics** > **System Log**.
2. Select **Export**.

   The `Poly_G200_<SN>_<time>.tar.gz.enc` file downloads to your local drive.

Note: You need the serial number of your system to open the log file because it's encrypted.

Related Links

Right to Data Portability on page 12
Importing and Exporting System Settings on page 9

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 personal data for a specific data subject.

Personal data about specific participants in conferences can be viewed.

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

Related Links

Call Detail Report (CDR) on page 3

Related Links

Configure H.323 Settings on page 6
Configure SIP Settings on page 7
Configure SVC Call Settings on page 8
Add, Edit, or Delete Contacts on page 4

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?

Any 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.

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/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.

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.

- The address book can be exported in CSV format.
- Audit and log files can be downloaded in plain text format.
- Web user interface configured file can be downloaded in plain text format.

Related Links

Importing and Exporting System Settings on page 9

Related Links

Download System Logs on page 9
Add, Edit, or Delete Contacts on page 4

Right to Erasure

A data subject has the right to remove all of his or her own personal data. A data subject may request deletion of their data, but based on the legal basis the controller employs, deletion may not be feasible in every case.

For details on how to erase customer personal data from the system, see #unique_25.

Any 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.

Related Links

Add, Edit, or Delete Contacts on page 4
Reset Your G200 System on page 15
Factory Restore Your System on page 16

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.

Related Links

Add, Edit, or Delete Contacts on page 4
Change the Password on page 4

Purposes of Processing Personal Data

Purposes of Processing Personal Data

Category	Type of Personal Data	Purpose of Processing	Interface Type
Call Detail Records (CDR)	The following information for near and far endpoints: ▪ System name ▪ Call number (IP or SIP address or ISDN number)	▪ Maintaining call history ▪ Troubleshooting call errors or performance issues	▪ User interface ▪ Web interface
Directory/Address Book	▪ Contact name ▪ IP address ▪ SIP address ▪ Alias name (H.323 only)	▪ Ease of use for dialing participant ▪ Store frequently used information	▪ User interface ▪ Web interface
Administrator and user credentials	Password	Login and authentication	Web interface
Device information	▪ Device name ▪ MAC address ▪ IP address ▪ SIP address ▪ H.323 alias name ▪ Serial number	Endpoint management	▪ User interface ▪ Web interface
Audit and system log files	▪ Admin and user credentials (excluding passwords) ▪ Admin and user actions ▪ Endpoint call status and usage data ▪ System troubleshooting details	▪ Admin and user activity logging ▪ Maintain history of configuration changes ▪ Troubleshooting system issues	Web interface

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 access and user activities	Log files record user activities and all login attempts (successful and unsuccessful)	Daily

How Personal Data Is Deleted

Topics:

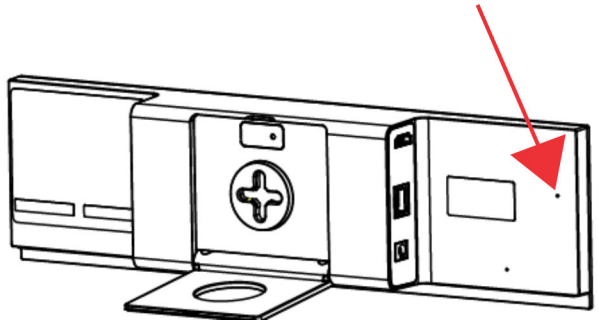
How Customer Personal Data Is Deleted

Data Type	Steps to Delete	Deletion Method
Contacts	▪ Contacts can be deleted by performing a comprehensive restore operation. ▪ Contacts can also be deleted one by one on system web interface.	Simple delete from database.
Audit and System log files	▪ Audit and log files are automatically deleted by the system (oldest first) when the system reaches the auditor event file limit of 30MB. These settings can be configured by the device administrator. ▪ Audit and log files are also deleted by performing a comprehensive restore operation.	File delete with overwrite.

Reset Your G200 System

If your G200 system isn't functioning correctly or you forgot the password, you can reset the system.

This procedure effectively refreshes your system, deleting all settings except the current software version. The G200 system restore button pinhole is located on the back of the system, as displayed in the following figure:



You can also reset the system from the system web interface from **Admin Settings** > **Factory Reset**.

Procedure

1. Using the paper clip, press and hold the restore button.
2. In the system web interface, go to **Admin Settings** > **Factory Reset** and click **Reset**.

After about 15 seconds, the system restarts and displays the setup wizard.

Related Links

Right to Erasure on page 12

Factory Restore Your System

A factory restore completely erases the system's flash memory and restores the system to the software version and default configuration stored in its factory partition.

A factory restore deletes the following items:

- Software updates
- Contacts
- System configurations
- Logs

Procedure

1. Power off the system.
2. Straighten a paper clip and insert it into the reset pinhole.
3. Press and hold the restore button while powering on the system.
4. After the screen shows that system enters the update process, release the reset button.

   The system restarts automatically when the process is complete.

Related Links

Right to Erasure on page 12