Polycom ISDN Gateway

Contents

Before You Begin

Topics:

- [Related Documentation](#)
- [Getting Help](#)

The Polycom ISDN Gateway Privacy Guide provides information on how Polycom products utilize customer data and how customers can configure Polycom ISDN Gateway to process personal data.

Related Documentation

You can view the following types of documents on each product page on [Polycom Support](#):

- Setup Sheet — The document is included in the system package and describes the contents of your package, how to assemble the system and accessories, and how to connect the system to the network.
- Administrator Guide — This guide provides detailed information about setting up your network and configuring features.
- Regulatory Notice — Describes safety and legal considerations for using Polycom products.
- Release Notes — Includes the latest features, known and resolved issues, and interoperability details for a release.

Getting Help

For more information about installing, configuring, and administering Polycom products, refer to the [Polycom Documentation Library](#) or **Documents & Software** at [Polycom Support](#).

Polycom and Partner Resources

To find all Polycom partner solutions, see [Strategic Global Partner Solutions](#).

The Polycom Community

The [Polycom Community](#) gives you access to the latest developer and support information. Participate in discussion forums to share ideas and solve problems with your colleagues. To register with the Polycom Community, simply create a Polycom online account. When logged in, you can access Polycom support personnel and participate in developer and support forums to find the latest information on hardware, software, and partner solutions topics.

Privacy-Related Options

Topics:

- [Call Detail Report (CDR)](#)
- [Configure Local Access](#)
- [Download System Log Files](#)
- [Transfer System Log Files](#)

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

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.

The size of a CDR is virtually unlimited, but can become unmanageable if you don't download the record periodically. If you consider that 150 calls result in a CDR of approximately 50 KB, you might set up a schedule to download and save the CDR after about every 1000 - 2000 calls just to keep the file easy to download and view. Remember that your connection speed also affects how fast the CDR downloads.

Enable the Call Detail Report

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. You can download the data in CSV format for sorting and formatting.

Procedure

1. In the system web interface, go to **Admin Settings** > **General Settings** > **System Settings** > **Recent Calls** .
2. Under **Recent Calls**, mark the **Call Detail Report** check box.

Download a Call Detail Report (CDR)

You can download a CDR using the Polycom ISDN Gateway system web interface.

Procedure

1. In the system web interface, click **Utilities** > **Services** > **Call Detail Report (CDR)**.
2. Click **Most Recent Call Report** and then specify whether to open or save the file on your computer.

Related Links

Configure Local Access

You can configure local access so that users can reach a system through the local interface.

Login credentials are user IDs and passwords that identify the user and define the user's ability to access the Polycom ISDN Gateway.

Procedure

1. In the system web interface, go to **Admin Settings** > **Security** > **Local Accounts** > **Login Credentials**.
2. Configure the following settings.

Setting	Description
Admin ID	Specifies the ID for the administrator account. The default Admin ID is `admin`. The administrator can change the **User Name** at any point of time.
Admin Password	Specifies the password for the local administrator account used when logging in to the system. Passwords are case sensitive and should not have spaces. The maximum length of the password is 40 characters. The default password is the 14-digit system serial number. The serial number can be viewed either on the **System Information** screen or at the bottom of the Polycom ISDN Gateway.
User ID	Specifies the ID for the user account. The default User ID is `user`. The administrator can change the **User Name** at any point of time.
User Password	Specifies the password for the local user account used when logging in to the system. Passwords are case sensitive and should not have spaces. The maximum length of the password is 40 characters. The default password is `user`.
Auditor ID	Specifies the ID for the auditor account. The default Auditor ID is `Auditor`. The administrator can change the **User Name** at any point of time.
Auditor Password	Specifies the password for the auditor account used when logging in to the system. Passwords are case sensitive and should not have spaces. The maximum length of the password is 40 characters. The default password is `auditor`.

> **Note:** When you enable the Maximum Security profile, the system forces you to change the
> default values of the following parameters or fields:
>
> - Admin account User ID
> - User account User ID
> - Auditor account User ID

Related Links

Enable H.323

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

A gatekeeper manages functions such as bandwidth control and admission control. The gatekeeper also handles address translation, which allows users to make calls using static aliases instead of IP addresses that may change each day.

Procedure

1. In the system web interface, go to **Admin Settings** > **Network** > **IP Network** > **H.323**.
2. Configure the following settings on the **H.323 Settings** screen.

Setting	Description
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.
	The **H.323 Name** is the same as the **System Name**, if you have changed the system name. Your organization's dial plan might define the names you can use.
H.323 Extension (E.164)	Allows users to place point-to-point calls using the extension if both systems are registered with a gatekeeper, and specifies the extension or prefix that gatekeepers and gateways use to identify this system.
	Your organization's dial plan might define the extensions you can use.
Enable IP H.323	Enables the H.323 interface.
Registration Status	Displays the registration status of the gatekeeper. It displays if the gatekeeper registration is successful or not. This is a read-only field.

Related Links

Download System Log Files

You can download system log files to save system log information. Several types of log files are available that are useful for troubleshooting. The date and time of system log entries for the Polycom ISDN Gateway are shown in GMT.

Procedure

1. Go to **Diagnostics** > **System** > **Download Logs**.
2. Under **Download Log**, click on your preferred log type:

Log Type	Description
Download Support information package	Displays all logs of the ISDN Gateway.
Download System log	Displays current logs of the ISDN Gateway, may have only last call traces.
Download error log	Displays thread dump for all the threads used in ISDN gateway. This is helpful only for crash issues reported

Related Links
[Right to Data Portability](#) on page 9

Transfer System Log Files

You can transfer logs to a USB flash drive to free up space on your Polycom ISDN Gateway system.

Procedure

1. In the web interface, go to **Admin Settings** > **Security** > **Log Management**.
2. Configure the following settings.

Setting	Description
Current Percent Filled	Displays how full the log file is, as a percentage of the total size.
Percent Filled Threshold	Specifies a threshold for the percent filled value. Reaching the threshold triggers an alarm, creates a log entry, and transfers the log if **Transfer Frequency** is set to **Auto at Threshold**. **Off** disables logging threshold notifications.

Setting	Description
Folder Name	Specifies the name to give the folder for log transfers. Select one of the following: ▪ **System Name and Timestamp**: Folder name is the system name and the timestamp of the log transfer, in the date and time format specified on the location screen. For example, if the system name is "Marketing", the folder name could be `marketing_MMddyyyymmssSSS`. ▪ **Timestamp**: Folder name is the timestamp of the log transfer, in the date and time format specified on the Location screen, for example `yyyyMMddhhmmssSSS`. ▪ **Custom**: Optional folder name for manual log transfers.
Storage Type	Specifies the type of storage device used for log file transfers.
Transfer Frequency	Specifies when the logs are transferred: ▪ **Manual**: Transfer starts when you click the **Start Log Transfer** button, which is visible only on the web interface. If the log fills before being transferred, new events overwrite the oldest events. ▪ **Auto at Threshold**: Transfer starts automatically when the Percent Filled Threshold is reached.

3. Click **Save**.

Related Links

How Data Subject Rights Are Supported

Topics:

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

The following information shows how data subject rights are supported.

Right to Access

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

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

Personal data related to users who are Administrators, Operators and Auditors can be viewed through web UI of Polycom ISDN Gateway.

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.

Related Links
[Call Detail Report (CDR)](#)
Related Links
[Enable H.323](#) on page 5

Right to Be Informed

What customer personal data is collected?

See the [Purposes for processing personal data](#) table in this topic.

How is customer personal data used?

See the [Purposes for processing personal data](#) table in this topic.

How long is customer personal data kept?

The local system and audit log files will be kept based on log rolling (action to close and archive locally stored logs and restart new log files) frequency and file counts. Administrator has an option to transfer the logs to USB device connected to the Polycom ISDN Gateway box and this is configurable by the device administrator.

Any personal data made available when working with Polycom support is only retained until each specific issue is resolved and then it is purged.

Is it 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 3rd parties / contractors).

How to notify a data subject of a data breach or security anomalies?

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 security anomalies have occurred.

See How Administrators are Informed of Any Security Anomalies (Including Data Breaches) on page 12.

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 XML format to a local machine.
- System log files can be downloaded in plain text format.

Related Links
Download a Call Detail Report (CDR) on page 3
Download System Log Files on page 6
Transfer System Log Files on page 6

Right to Erasure

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

For details on how to erase customer personal data from the system, see the topic How Personal Data is Deleted on page 13.

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

Related Links
Perform a Factory Restore on page 13

Right to Rectification

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

Personal data related to users who are Administrators, Operators and Auditors can be edited or updated using Polycom ISDN Gateway (if configured).

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

Polycom 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

Right to Object to Processing

Not applicable.

Right to Restrict Processing

Not applicable.

Purposes of Processing Personal Data

Purposes of Processing Personal Data

Category	Type of Personal Data	Purpose of Processing	Interface Type
Call Detail Records (CDR)	IP address or E.164 number ISDN number Device name	Provide call history Troubleshooting call errors or performance issues View call statistics	Web interface
Administrator and user credentials	User name Password	Login and authentication	Web interface
System Logging	Admin and user credentials (excluding passwords) Admin and user actions	Admin and user activity logging Maintain history of configuration changes Troubleshooting system issues	Download to USB 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
System Crash	Front panel Boot LED will start blinking red Error will appear in system log file	Front panel Boot LED will show immediately Check log file just after reboot
All active alarms	See the *System Status*, *Alarm*, and *Log Management* sections in *Polycom ISDN Gateway Administrator and Integrator Guide*.	If there is new alarm, the alarm list is updated with a new list of alarms. Recommend to review log once daily.

How Personal Data is Deleted

Topics:

▪ [Perform a Factory Restore](#)

How Customer Personal Data is Deleted

Data Type	Steps to Delete	Deletion Method
Call detail record (CDR)	▪ Through the Telnet Port 24 API using the command `resetsystem deletecdr.` ▪ CDRs are also deleted by performing a comprehensive restore operation.	Simple delete
Audit and System log files	▪ Telnet using IP address of the ISDNGW with port 23 give command: `resetsystem deletelogs.` ▪ Audit and log files are also deleted by performing a comprehensive restore operation.	Simple delete

Perform a Factory Restore

The factory restore resets the Polycom ISDN Gateway to default factory settings. After the factory reset, all the previous configurations, software updates, CDR data, certificates, username and passwords are lost.

A factory restore completely erases:

▪ Configuration of the Polycom ISDN Gateway and restores it to the default configuration stored in its factory partition

▪ Flash memory of the Polycom ISDN Gateway and reinstalls the factory software version

Procedure

» When the Polycom ISDN Gateway is powered on, insert a straightened paper clip through the pinhole and press and hold the Reset button for more than ten seconds.

The factory restore takes approximately 3.5 minutes to complete. The Polycom ISDN Gateway automatically reboots when the factory reset is complete.

Related Links