PRIVACY GUIDE

July 2019 | 3725-63838-001A

Polycom RealPresence Resource Manager Privacy Guide

Contents

Before You Begin

Topics:

This Guide provides information on RealPresence Resource Manager privacy data.

Related Documentation

You can find additional information on the RealPresence Resource Manager documentation.

Getting Help

For more information about installing, configuring, and administering Polycom products, refer to **Documents and Downloads** 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

There are different configuration options for RealPresence Resource Manager which may affect the privacy options.

System Reports

The RealPresence Resource Manager system provides various reports that you can view and export.

Use these reports to identify return on investment, troubleshoot problems, provide information about network traffic, and ensure accurate billing for Polycom video calls.

Related Links

Right to Access on page 50
Right to Data Portability on page 51

System Maintenance and Troubleshooting

You can troubleshoot problems with RealPresence Resource Manager system logs, Troubleshooting Utilities, and other functions.

Related Links

Right to Data Portability on page 51

Managing System Logs using a Syslog Server

If your IT environment includes an external syslog server, you can choose to have system logs automatically sent to that server to be stored and managed externally from the RealPresence Resource Manager system.

Related Links

How Personal Data Is Deleted on page 58

User Account Configuration Settings

Configure the settings on the **User Account Configuration** page.

Field	Description
Account Lockout	
Failed login threshold	Specify how many consecutive login failures cause the system to lock an account. Possible value is 2 to 10.
Failed login window (hours)	Specify the time span within which the consecutive failures must occur in order to lock the account. Possible value is 1 to 24.
Customized user account lockout duration (minutes)	Specify how long the user's account remains locked. Possible value is 1 to 480.
Account Inactivity	
Customize account inactivity threshold (days)	Specify the inactivity threshold that triggers disabling of inactive accounts. Possible value is 30 to 180.

Managing Endpoints and Peripherals

You can manage and monitor endpoints and peripherals using the RealPresence Resource Manager system.

UC Endpoint Management

You can use the RealPresence Resource Manager system as a central provisioning server for supported UC endpoints.

Related Links

Right to Access on page 50
Right to Rectification on page 52

Managing Directories

Integrating the RealPresence Resource Manager with an enterprise directory server enables you to manage the directories from the RealPresence Resource Manager system.

Managing the Guest Book and Favorites Lists

The RealPresence Resource Manager system provides two ways that you can customize and expand the user directories.

The system has a Guest Book and a Favorites List.

Conference and Participant Details

When scheduling and configuring a conference, see the conference and participant detail fields.

System Backup and Recovery

The backup and recovery of a RealPresence Resource Manager system includes backup and recovery of the RealPresence Resource Manager system internal database and the backup of the RealPresence Resource Manager system configuration settings.

Related Links

Right to Data Portability on page 51

Encryption

The following table lists the product capabilities that are supported but not necessarily required. Requirements vary based on the customer environment.

Product Capabilities

Application	Encryption Function	Description	Protocol Used
HTTP	Confidentiality Integrity	Management API: Server provides a local management interface over encrypted HTTP(used for Web GUI, Rest API and Provisioning)	SSL 3.0 TLS 1.0 TLS 1.1 TLS 1.2
LDAP	Confidentiality Integrity	AD integration: Allows product to retrieve enterprise directory entries from a Microsoft active directory-compatible server over an encrypted LDAPs channel; Directory service: provides AD-compatible directory service for devices.	SSL 3.0 TLS 1.0 TLS 1.1 TLS 1.2
XMPP	Confidentiality Integrity	Presence service: Allows product to post its current presence state to a configured XMPP server and obtain presence information for other users/devices from XMPP server, using an encrypted TLS channel; Note: This product also supports the XMPP Chat service.	SSL 3.0 TLS 1.0 TLS 1.1 TLS 1.2
File Stored Data	Confidentiality	System Backup/Restore encryption	N/A
		Upgrade file encryption	
Remote Password	Confidentiality	It is used to store the password of the account for login remote entity.	N/A

Application	Encryption Function	Description	Protocol Used
SNMP Agent	Confidentiality	SNMP Agent: Allows SNMP console applications to connect to the product over an encrypted SNMPv3 channel.	SNMPv3

Security Certificates

User certificates between systems within your video conferencing environment (such as servers and endpoints) to build a trust/authentication and to support encryption.

Certificates confirm that the servers within your infrastructure can communicate and have the option to encrypt the data. Each digital certificate is identified by its public key. The collection of all public keys used in an enterprise to determine trust is known as a Public Key Infrastructure (PKI).

The CA, or certificate authority, is a single, centralized authority such as an enterprise's IT department or a commercial certificate authority that each computer on the network is configured to trust. Each server on the network has a public certificate that identifies it. When a client connects to a server, the server shows its signed public certificate to the client. The certificate authority signs the public certificates of those servers that clients should trust. Trust is established because the certificate has been signed by the certificate authority (CA), and the client has been configured to trust the CA.

View the Global Address Book

You must have the **Administrator** role and permissions to view the Global Address Book.

Procedure

1. Go to **Admin** > **Directories** > **Global Address Book**.
2. As needed, click **Filter**  to customize the **Global Address Book**.

   It can be filtered by **Endpoint Name** or **IP Address**.

Related Links

Purposes of Processing Personal Data on page 53

Create Conference Usage Report

Use the **Conference Usage Report** option to review usage information about system conferences.

Only reports for scheduled conference calls are created. Reports for ad hoc conference calls are not created.

Procedure

1. Go to **Reports** > **Conference Usage Report**.
2. As needed, change the **Start Date** and **End Date** to select the date range for the report.
3. Select the number of reports to be displayed on the page from the **Conferences per page** drop-down list.
4. Select **Summary Report** or **Detail Report**.
5. Click **Export as CSV File** .

   The file is saved to the default Download folder of your browser.

Related Links

Purposes of Processing Personal Data on page 53

Setting Up the Global Address Book

This section describes how to manage the Global Address Book in the Polycom RealPresence® Resource Manager system.

The Polycom Global Address Book is a system-managed endpoint directory that enables users with video endpoints to look up and call other users with video endpoints in their video communications network.

Managing Directories

Integrating the RealPresence Resource Manager with an enterprise directory server enables you to manage the directories from the RealPresence Resource Manager system.

Managing the Guest Book

Users with the schedulers, operator, or administrator role have access to the Guest Book.

The Guest Book provides a way to store conference participants that aren't managed by the RealPresence Resource Manager system.

The **Guest Book** is a local system directory that includes guest participants who were either explicitly added to the Guest Book or saved to the Guest Book while being added as conference participants.

Guest book entries are static and are not imported through the dynamically updated enterprise directory nor included in the system **Global Address Book**. The **Guest Book** is limited to 500 entries.

Users with the schedulers, operator, or administrator role have access to the Guest Book. The Guest Book provides a way to store conference participants that aren't managed by the RealPresence Resource Manager system.

LDAP Searches

If the RealPresence Resource Manager system is integrated with an Active Directory, the RealPresence Resource Manager uses the LDAP search function for searches of the directory.

LDAP searches are prefix-searches that include an appended wildcard. In this case, when you enter a search string, the system looks for that search string only at the beginning of the indexed fields.

For example, all of the following searches for a participant will find Barbara Smithe:

- `Barbara`
- `Smithe`
- `Bar`
- `Smi`

To optimize LDAP searches, the RealPresence Resource Manager system searches only indexed LDAP fields and a limited set of attributes. The attributes include:

- `ObjectCategory`
- `memberOf`
- `DisplayName`
- `GivenName`
- `Sn`
- `Cn`
- `Samaccountname`
- `groupType`

- `distinguishedName`
- `objectGuid`

These are the requested attributes to be returned by the search:

- `Sn`
- `Givenname`
- `Mail`
- `Ou`
- `Objectguid`
- `Telephonenumber`
- `Cn`
- `Samaccountname`
- `Memberof`
- `Displayname`
- `Objectclass`
- `Title`
- `localityName`
- `department`

Related Links

Purposes of Processing Personal Data on page 53

View Endpoint Usage Report

Topics:

The **Endpoint Usage Report** is based on the CDRs extracted from selected endpoints and includes entries for ISDN and IP calls.

Calls from WebRTC participants are not recorded in CDRs.

Use data from the **Endpoint Usage Report** to troubleshoot problems, provide information about network traffic, and ensure accurate billing for Polycom video calls.

Procedure

1. Go to **Reports** > **Endpoint Usage Report**.

   The **Endpoint Usage Report** page displays the information for the endpoints for which CDRs are available.

   The CDRs are displayed in alphabetical order for the default **Start Date** and **End Date**. By default, the CDRs for the last week are reported.
2. To restrict the report to a different time period, change the **Start Date** and **End Date**.

   The report is dynamically updated.
3. Click **Filter** to customize the report by endpoint **Type**, **Name**, **IP Address**, **ISDN Video Number**, **Dial String**, **Site**, or **VIP** status.

   You can also filter on **Area** when areas are enabled and you manage more than one area.
4. Select the number of reports to be displayed on the page from the **Items per page** drop-down list.
5. To generate the Endpoint Usage report, select one or more endpoints to include in the report and go to **More** > **Generate Report**.

   Use the CTRL key to select multiple endpoints.
6. To select a different group of endpoints, click **Change Selected**, select the endpoints, and go to **More** > **Generate Report** again.
7. Click **Call Times** to see a chart that identifies the number of calls versus the start time for the calls.
8. Click **People Count** to see a chart that identifies people count for conference usage.
9. Click **Inbound** to see a chart that identifies the endpoints from which the inbound calls to the selected endpoints originated.
10. Click **Outbound** to see a chart that identifies the endpoints to which the selected endpoints called.
11. Click **Summary CDR Report** to see a grid that displays information for each of the selected endpoints that participated in calls.

    If any of the selected endpoints did not participate in calls during the selected time period, it is not included in the **Summary CDR Report**.
12. To export the information in the **Summary CDR Report**, click **Export as Excel File** and either **Open** or **Save** the file as needed.

    Note that only the first 1000 lines of the report are exported to the Excel file.
13. Click **Detail CDR Report** to see information for each of the endpoints that participated in calls.
14. To export the information, click **Download Report**.

- Click **For *endpoint_name* ONLY (Excel File)** to save the report Microsoft Excel format for the selected endpoint.
- Click **For All Selected Endpoints (CSV File)** to save the CDR report in or in CSV format.Only the first 1000 lines of the report are exported to the Excel file.

15. Click **Change Selected** to return to the **Endpoint Usage Report** page to select a different endpoint.

Related Links

Purposes of Processing Personal Data on page 53

Create Conference Usage Report

Use the **Conference Usage Report** option to review usage information about system conferences.

Only reports for scheduled conference calls are created. Reports for ad hoc conference calls are not created.

Procedure

1. Go to **Reports** > **Conference Usage Report**.
2. As needed, change the **Start Date** and **End Date** to select the date range for the report.
3. Select the number of reports to be displayed on the page from the **Conferences per page** drop-down list.
4. Select **Summary Report** or **Detail Report**.
5. Click **Export as CSV File** .

   The file is saved to the default Download folder of your browser.

Related Links

Purposes of Processing Personal Data on page 53

User Management

The RealPresence Resource Manager system uses roles to define permissions.

Users can be assigned management roles, associated with endpoints, and organized in groups.

You can assign roles and provisioning profiles to sets of users by using groups.

By default all users can be scheduled into conferences, and call into conferences. However, the system cannot call out to them until they are associated with endpoints.

Related Links

Right to Access on page 50
Right to Data Portability on page 51

Endpoint Information

The following table explains the endpoint information.

Field	Description
Status	The state of the endpoint. Possible values include: • Online  • Offline  • Licensed  • In a call  • Gatekeeper/SIP/Cloud Service Registered  • Gatekeeper/SIP/Cloud Service/Signaling Unregistered  • Registration Status Unknown/Not Applicable • Endpoints behind Firewall  • Error  • Warning  • All paired peripherals are connected without alerts  • One or more paired peripherals are turned off or no longer connected  • One or more paired peripherals has an error  **Note:** If a phone crashes while in a call, the phone status may not update after it reconnects to the RealPresence Resource Manager system. When the RealPresence Resource Manager system gets a new call status from the phone or detects that the phone is offline, the system updates the phone's call status.

Field	Description
Mode	The management mode for the endpoint. Possible values include: • Non-dynamically Managed Endpoints • Dynamically Managed endpoints • Synced RealPresence DMA Endpoints • Synced CUCM Phones • • • Auto-Added UC Device • Manually Added UC Device Note: Auto-added and Manually UC devices refer to the phones and other Polycom UC endpoints such as Polycom Studio.
Name	The assigned name of the endpoint.
Model	The type of endpoint.
MAC Address	The MAC address of the endpoint.
IP Address	The IP address assigned to the endpoint.
Area	(Available only when Areas are enabled.) The area with which the endpoint is associated. Users can only view area information for the areas to which they belong or have been assigned to manage.
Dial String	The dial string for the endpoint. If the endpoint has more than one dial string, it displays one based on this order: • SIP • H.323 • ISDN
Owner	The user associated with the endpoint.
Endpoint Groups	The endpoint group to which the endpoint belongs.
Software Version	Endpoint's version.

Related Links

Purposes of Processing Personal Data on page 53

Endpoint Management

The RealPresence Resource Manager system can manage, monitor, and provision Polycom and third-party endpoints.

Endpoint management eliminates the need to configure each endpoint individually through the hand-held remote or the endpoint's web interface. It also helps you easily enforce network, group, and system policies for each device.

Endpoint management consists of two aspects of remotely configuring endpoints: updating software and provisioning settings.

UC Endpoint Management

You can use the RealPresence Resource Manager system as a central provisioning server for supported UC endpoints.

Related Links

Right to Access on page 50
Right to Rectification on page 52

Managing Conferences and Participants

You can manage conferences and participants in the RealPresence Resource Manager system.

Related Links

Right to Access on page 50
Right to Rectification on page 52
Right to Data Portability on page 51

System Maintenance and Troubleshooting

You can troubleshoot problems with RealPresence Resource Manager system logs, Troubleshooting Utilities, and other functions.

Related Links

Right to Data Portability on page 51

Working with Users

Use the following guidelines when assigning user roles and types.

The RealPresence Resource Manager system uses roles to define permissions:

- Users can be assigned management roles, associated with endpoints, and organized in groups.
- You can assign roles and provisioning profiles to sets of users by using groups.
- By default all users can be scheduled into conferences, and call into conferences. However, the system cannot call out to them until they are associated with endpoints.

The RealPresence Resource Manager system supports two types of users:

- Users that are local to the management system. These users are added manually to the system or imported from a file.
- Enterprise users that come directly from the enterprise directory.

If your company has implemented multi-tenancy, you can also assign local users or enterprise users to an area or areas that you manage.

Related Links

Right to Rectification on page 52

Managing Conferences and Participants

You can manage conferences and participants in the RealPresence Resource Manager system.

Related Links

Right to Access on page 50
Right to Rectification on page 52
Right to Data Portability on page 51

Edit a User

For local users added manually to the RealPresence Resource Manager system, you can edit all user information.

You need the **Administrator** role to edit users.

If you change the user ID, the user must log into the associated endpoints with the new ID.

For users added through the enterprise directory, you can edit their roles (unless the role is inherited from a group) and associate them to endpoints, but you cannot change user names, user IDs, or passwords.

Procedure

1. Go to **User** > **Users**.
2. Search for the user you want to edit.
3. Select the user you want to edit and click **Edit** .
4. As required, edit the **General Info**, **Associated Endpoints,Associated Roles,Managed Areas**, **Associated Alert Profile**, and **Dial String Reservations** sections of the **Edit User** dialog.

   If the user has multiple associated endpoints, list the endpoints in order of priority, with the primary endpoint first.

   When scheduling a user in a conference, the RealPresence Resource Manager system will, by default, schedule the user's primary endpoint. The scheduler can choose to change the request to schedule one of the user's other endpoints.
5. Click **Update**.

Related Links

Right to Rectification on page 52

Configuring Alert Settings

You can configure the RealPresence Resource Manager system to send alerts to users via e-mail for specific types of system and endpoint events

Related Links

How Admin Can Be Informed of Any Security Anomalies (Including Data Breach) on page 57

Managing Audit Log Files

Audit logs provide a way to monitor the system for security and system access activity.

The following table identifies the RealPresence Resource Manager system audit log files.

Log Name	Description
localhost_access.log	Log file that shows every web request that was made from client systems. The system may have more than one such log.
ResourceManager_audit_jserver.log	Log file that captures security-related authentication issues.
kernel.log	Logs are useful not only for understanding the internal operation of a system but also the timing and relationships of activities within the system through the time-ordered messages within a time-stamped log.
hids.log	Log file that captures intrusion detection alerts.

Related Links

How Admin Can Be Informed of Any Security Anomalies (Including Data Breach) on page 57

UC Endpoint Management

You can use the RealPresence Resource Manager system as a central provisioning server for supported UC endpoints.

Related Links

Right to Access on page 50
Right to Rectification on page 52

Roll Locally Stored Log Files

You can use the **Roll Log** action to close and archive locally stored log files and start new log files.

Although you can configure an automatic window in which logs are rolled (restarted), you can also manually roll the logs whenever you need to troubleshoot a particular incident.

When you roll locally-stored logs, the following subset of locally-stored logs are archived and restarted.

- Jserver
- DeviceManager
- Conference
- Corosync
- Redundancy
- AudioPhone

Procedure

1. Go to **Admin** > **Maintenance** > **System Log Files**.
2. Click **Roll Logs**  .

   A message displays confirming the operation and detailing which logs were rolled.
3. Click **Close** to close the information dialog.

Related Links

How Personal Data Is Deleted on page 58

Call Detail Record Report Administration

By default, the RealPresence Resource Manager system stores the conference and endpoint call detail records (CDRs) for 30 days.

You can modify the CDR retention period and you can schedule a weekly archive of the CDRs. These procedures are described in the following topics.

Related Links

How Personal Data Is Deleted on page 58

Backup and Delete Audit Files

The RealPresence Resource Manager system enables you to store audit logs locally until the maximum file storage limit of 2 GB is met.

You should periodically roll the logs, and then backup the archived files and delete them from the local system.

You can create a backup of audit files and then delete the files from the server. After you create a backup (a zip file) you are prompted to verify that the files are authentically from the server from which they were downloaded and have not been modified since being downloaded. You need to verify the zip file with the Polycom Verification Utility which is provided.

You must have the auditor role in order to download and delete audit log files.

Procedure

1. Navigate to **Admin** > **Maintenance** > **Audit Log Files**.
2. Select the audit log file(s) that you want to backup and delete.
3. Click **Backup and Delete**.
4. The files will be saved in your browser's download folder.
5. In the **Backup and Delete** dialog, ensure that each audit log file that you want to backup is selected.

   All audit logs are selected by default, you can deselect the files that you do not want to include in the archive.
6. Click **Download Verification Utility** if you want to delete the backed-up logs.

   The Polycom File Verification Utility generates a checksum number that can be used as a verification code to ensure that the audit log files have not been modified after they were downloaded.
7. Execute the File Verification Utility and browse to the location of the audit file backup.

   After doing so, the File Verification Utility will output a value that can be copied to the clipboard.
8. Copy the **Verification Value** and enter it into the **Verification Code** section of the RealPresence Resource Manager system dialog.
9. Click **Verify and Delete**.

   The audit logs are deleted from the RealPresence Resource Manager system.

Related Links

How Personal Data Is Deleted on page 58

Delete a Conference

You can delete scheduled or past conferences.

You cannot delete active conferences.

Procedure

1. Go to **Conference** > **Monitor View.**
2. If necessary, filter the **All Conferences** list to include the conference you want to delete.
3. Select the conference of interest and click **Delete** .
4. If you select a recurring conference, a dialog appears asking you if you want to delete just the conference you selected or all conferences in the series.

   Make the appropriate choice. You cannot deleted active conferences in the series.
5. Click **OK** to confirm the deletion.

   The conference is deleted. For future conferences, the system emails the change to the conference owner and participants and releases the participant and room resources.

Related Links

How Personal Data Is Deleted on page 58

Delete a UC Endpoint

You can only delete manually added or imported endpoints.

Phones synced from the Cisco Unified Communications Manager system cannot be deleted manually. In order to delete phones synced from Cisco Unified Communications Manager, you must unassociate the phone from that system.

Procedure

1. Go to **Endpoint** > **Monitor View.**
2. Select a manually added endpoint.
3. Click **Delete** .
4. Click **Delete** to confirm the deletion.

Delete an Endpoint

When you delete an endpoint, you remove the endpoint from the RealPresence Resource Manager system.

You also delete all the associations with the endpoint.

Procedure

1. Go to **Endpoint** > **Monitor View**
2. Select an endpoint you want to delete.
3. Click **Delete** .
4. If the endpoint is dynamically-managed, choose one of the following options:
   - **Delete Endpoint Only**: Deletes the endpoint
   - **Delete with dial string reservation**: Deletes the endpoint and any dial string reservations associated with the endpoint.
   - **Cancel**: Cancels the action.
5. Click **Delete** for other endpoints types.

Related Links

How Personal Data Is Deleted on page 58

Delete a Local User

You can only delete local users from the RealPresence Resource Manager system.

You need the **Administrator** role to delete users.

You cannot delete users added through integration with an enterprise directory.

Procedure

1. Go to **User** > **Users**.
2. Search the user you want to delete.
3. Select the user and click **Delete** .

   To delete multiple users, hold the Shift key down while you make your selections.
4. Click **OK** to confirm the deletion.

   The user is deleted from the system.

Related Links

How Personal Data Is Deleted on page 58

How Data Subject Rights Are Supported

Topics:

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 related to users who are Administrators and Operators can be viewed or exported using RealPresence Resource Manager.
- Personal data about endpoint usage can be viewed or downloaded via the endpoint usage report.
- Personal data about participant information in conferences can be viewed or downloaded via the conference monitor page or conference usage report.
- Personal data about endpoint details can be viewed or exported on endpoint monitor view.
- A copy of any customer personal data made available to Polycom when working with Polycom support is available by requesting it from your Polycom support representative.

Related Links

Managing Conferences and Participants on page 35
System Reports on page 7
User Management on page 30
UC Endpoint Management on page 12

Right to Be Informed

What personal data is collected?

See Purposes of Processing Personal Data on page 53.

How is personal data is used?

See Purposes of Processing Personal Data on page 53.

How long is personal data kept?

Personal data is retained as long as the data subject is using the product.

The local system and audit log files are kept based on log rolling (action to close and archive locally stored logs and restart new log files) frequency, file counts and rotation sizes.

The local endpoint and conference usage reports are kept for 30 days by default.

Any customer personal data made available when working with Polycom support, specific to a support incident, is only retained until the incident is resolved, and then it is purged. Customer contact information is retained by Polycom support until the support relationship ends or is requested to be removed by the customer.

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

Personal data processed by this product is not shared with any third parties.

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 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. The product administrator is able to monitor and identify when security anomalies have occurred.

Related Links

Purposes of Processing Personal Data on page 53
How Admin Can Be Informed of Any Security Anomalies (Including Data Breach) on page 57

Right to Data Portability

Polycom customers have a right to receive a copy of all personal data in a commonly-used, machine-readable format.

Steps are outlined below for how an administrator can support the data portability right of personal data. For more information on REST API options, see the *Polycom RealPresence Platform API Guide* available on Polycom Support Center.

- Personal data related to users' aliases can be exported as CSV files on the RealPresence Resource Manager UI or via the REST API of user.
- Personal data about endpoint usage can be downloaded via the endpoint usage report on the RealPresence Resource Manager UI or via the REST API of billing.
- Personal data about participant information in conferences can be downloaded via the conference monitor page or conference usage report on the RealPresence Resource Manager or via the REST API of reservation or billing.
- Personal data about endpoint details can be exported on endpoint monitor view on RealPresence Resource Manager UI or via the REST API of device.
- Personal data in system backup can be downloaded on the RealPresence Resource Manager UI or auto FTP transfer to remote server. The backup file is encrypted but can be restored on the other RealPresence Resource Managerservers.
- Personal data in system log or audit files can be downloaded on RealPresence Resource Manager UI or remote transfer to syslog servers.

Related Links

User Management on page 30
System Reports on page 7
Managing Conferences and Participants on page 35
System Backup and Recovery on page 16
System Maintenance and Troubleshooting on page 8

Right to Erasure

A data subject has the right to remove all personal data for a specific data subject.

Any customer 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.

Related Links

How Personal Data Is Deleted on page 58

Right to Rectification

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

For local users added manually to RealPresence Resource Manager, for details on how to edit any inaccurate or incomplete personal data.

For users added via an enterprise directory integration, you can edit their roles and change their associated endpoint. Any other personal data cannot be edited because the information derives from the enterprise directory.

Personal data about participant information in conferences can be edited via the conference monitor page.

Personal data about endpoint details can be edited on endpoint monitor view, provisioning profiles, endpoint naming and E.164 numbering, and SIP URI settings.

Polycom 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.

Related Links

Working with Users on page 37
Managing Conferences and Participants on page 35
UC Endpoint Management on page 12

Related Links

Edit a User on page 39

Purposes of Processing Personal Data

Purposes for processing personal data

Personal Data Category	Type of Personal Data	Purpose of Processing	Interface type
Endpoint usage report	▪ Endpoint Name ▪ Serial Number ▪ Account Number ▪ Remote System Name ▪ Call Number 1 ▪ Call Number 2 ▪ Far Site Endpoint Alias ▪ Far Site Endpoint Additional Alias ▪ Far Site Endpoint Transport Address	▪ Maintaining call history ▪ Troubleshooting call and billing issues	▪ UI ▪ API ▪ File Exported
Conference usage report	▪ Conference Name ▪ Conference Scheduler ▪ Conference Scheduler ID ▪ Conference Owner ▪ Conference Owner ID ▪ Conference Alias	▪ Maintaining conference history ▪ Troubleshooting conference and billing issues	▪ UI ▪ REST API ▪ File Exported

Personal Data Category	Type of Personal Data	Purpose of Processing	Interface type
Directory / address book	▪ Endpoint Name ▪ Global Address Book Display name ▪ IP Address ▪ Endpoint Alias ▪ Primary ISDN ▪ Secondary ISDN ▪ Endpoint Owner ▪ Endpoint Type ▪ ObjectCategory ▪ memberOf ▪ DisplayName ▪ GivenName ▪ Sn ▪ Cn ▪ Samaccountname ▪ groupType ▪ distinguishedName ▪ objectGuid ▪ Mail ▪ Objectguid ▪ Ou ▪ Telephonenumber ▪ Title ▪ localityName ▪ department	▪ Directory service for devices ▪ Address book management	▪ UI ▪ GDS ▪ LDAP

Personal Data Category	Type of Personal Data	Purpose of Processing	Interface type
User information	▪ First Name ▪ Last Name ▪ User ID ▪ Email address ▪ Password ▪ Title ▪ Department ▪ City ▪ Phone Number ▪ Associated Endpoints ▪ Groups ▪ Roles	User authentication, authorization, directory service, endpoint provisioning, conference scheduling	▪ UI ▪ LDAP ▪ REST API ▪ File Exported
Device information	▪ Name ▪ MAC Address ▪ IP Address ▪ Owner ▪ Serial Number ▪ Device ID	Endpoint management and provisioning	▪ UI ▪ REST API ▪ H.350 ▪ File Exported

Personal Data Category	Type of Personal Data	Purpose of Processing	Interface type
Conference and participant Information	Conference details: ▪ Creator ▪ Owner ▪ Start Date/Time ▪ Duration ▪ End Date/Time ▪ Type ▪ Status ▪ Recurring ▪ Connection ▪ Bit Rate ▪ And etcetera Participant details: ▪ Name ▪ Endpoint Name ▪ Address ▪ Number ▪ Area	Conference management	▪ UI ▪ REST API ▪ File Exported
Audit and system log files	▪ Admin and user actions ▪ Endpoint provisioning message exchange details ▪ Conference management messages with MCU and endpoints ▪ Endpoint call status and usage data ▪ System troubleshooting details	▪ Admin and user activity logging ▪ Troubleshooting system issues	▪ UI ▪ REST API ▪ File Downloaded ▪ Syslog

Related Links

LDAP Searches on page 25
Endpoint Information on page 31
Right to Be Informed on page 50

Related Links

View the Global Address Book on page 20
View Endpoint Usage Report on page 28
Create Conference Usage Report on page 21

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).

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

Security anomaly type	Where to check	Recommended frequency to check
All active alerts and security anomalies	An administrator can configure alerts and then monitor on the UI, SNMP client or via email. Active alerts and audit log files. Audit logs provide a way to monitor the system for security and system access activity for details regarding audit log names, descriptions on what they capture.	Once daily

Related Links

Configuring Alert Settings on page 40
Managing Audit Log Files on page 41
Right to Be Informed on page 50

How Personal Data Is Deleted

This table lists how personal data is deleted.

Data type	Steps to delete	Deletion method
Endpoint usage report	By default, these reports are auto purged after 30 days. The retention setting can be modified.	Auto purged from database
User		Simple delete from database
Device information		Simple delete from database
Conference information		Simple delete from database
Audit and system log files	For locally stored log files, the administrator can use the **Roll Log** action to close and archive locally stored log files and start new log files (restart log files). For logs that are stored remotely or downloaded, they aren't automatically restarted as part of the log rolling process and must be deleted separately using a secure deletion method.	Simple delete and restart logs (roll log) from file system
Backups	System backups are never stored locally on RealPresence Resource Manager and therefore must be deleted separately using a secure deletion method.	

Related Links

Call Detail Record Report Administration on page 44
Managing System Logs using a Syslog Server on page 9
Right to Erasure on page 52

Related Links

Delete a Local User on page 49
Delete an Endpoint on page 48
Delete a Conference on page 46
Backup and Delete Audit Files on page 45
Roll Locally Stored Log Files on page 43

6001 America Center Drive
San Jose, CA 95002
USA

Customer Feedback We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocumentationFeedback@polycom.com.

Polycom Support Visit the Polycom Support Center for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.