



PRIVACY GUIDE

| March 2019 | 3725-63838-001A

Polycom Device Management Service for Enterprises



Contents

Before You Begin.....	2
Related Documentation.....	2
Getting Help.....	2
Polycom and Partner Resources.....	2
The Polycom Community.....	2
Privacy-Related Options.....	3
Managing User Profiles.....	3
User Management.....	3
Update Your Profile.....	6
Account Management.....	7
View Activity Logs.....	7
Managing Device Profiles.....	8
Bulk Edit Devices.....	8
Adding Devices.....	9
Edit a Device.....	9
Delete a Device.....	10
Download Activity Logs.....	10
How Data Subject Rights Are Supported.....	12
Right to Access.....	12
Right to Be Informed.....	12
Right to Data Portability.....	13
Right to Erasure.....	13
Right to Rectification.....	14
Purposes of Processing Personal Data.....	15
How Admin Can Be Informed of Any Security Anomalies (Including Data Breach).....	16
How Personal Data Is Deleted.....	17

Before You Begin

Topics:

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

This Guide provides information on Polycom Device Management Service for Enterprises privacy data.

Related Documentation

The following documentation provides additional information on PDMS-E.

You can view [Polycom Device Management Service for Enterprises Administration Guide](#) for more information.

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

Topics:

- [Managing User Profiles](#)
- [Managing Device Profiles](#)

There are different configuration options for Polycom Device Management Service for Enterprises which may affect the privacy options.

Managing User Profiles

The Polycom Cloud Service Administration Portal has different deployment options that can determine the privacy options and requirements available on the system. Administrators can configure the privacy options detailed in this section.


Polycom Device Management Service for Enterprises uses Polycom Cloud Service user accounts to authenticate and access services in Polycom Device Management Service for Enterprises. All management of information related to user accounts and profiles must therefore be performed through the Polycom Cloud Service web portal.

A user whose Polycom Cloud Service user account has been granted the “User Admin” role can view, edit or delete other Polycom Cloud Service user accounts within the organization.

Note: Deleting a user account from the Polycom Cloud Service portal does not terminate subscription to the Polycom Cloud Service service. This may only be done by contacting Polycom support.

Any Polycom Cloud Service user can view and update their own user profile information. The user profile contains the user’s first name, last name and their email address. The first and last name can be updated; the email address cannot be changed.

User Management

You must have the **User Admin** role assigned to your user account to access the **Users**  functions.

User accounts have different permissions and sign in capabilities depending on the **User Role** and **Sign In Account** settings that you select for them.

Each user is listed in a table with the following information:

User Information

User Information	Description
User Name	User's name and email address
Sign In Account	Sign in account type: <ul style="list-style-type: none">▪ Enterprise Only▪ Enterprise and Local

User Information	Description
User Role	User roles assigned to the user account. These are associated with various access permissions within the Polycom Cloud Services portal.

You can click **Refresh** to refresh all the device information manually.

Related Concepts

[Right to Rectification](#) on page 14

Add a New User Account

You can add additional Polycom Cloud Services user accounts using the users' email addresses.

Users can be from your own organization (meaning they have email addresses from one of the domains associated to your Polycom Cloud Services account), or from partner or external organizations (with email address domains outside of those associated with your account)—these users are considered **Guest** users.

Procedure

1. In the Polycom Cloud Services portal, go to **Administration > Users**.
2. Click **Add**.
3. Enter the user's email address in the **Email Address** field.
4. In the **User Role** field, select one or more predefined user roles for the new account.

User Role	Permissions
Device Admin	The role provides full access to Register Devices and use PDMS-E functions.
Device Operator	The role provides read-only access to connected devices.
Enterprise Admin	The role provides full access to the Administration > Account Management , Authentication Providers and Domain Management functions.
License Admin	The role provides full access to the Administration > Licenses functions.
User Admin	The role provides full access to the Administration > Users functions.
OTD Admin	The role provides administer access to the Polycom One Touch Dial (OTD) service. For more information, see the Polycom One Touch Dial Support Documentation .

5. In the **Sign In Account** field, select one of the following account types.

You can select the **Sign In Account** type only when you add a new user from your organization. If you add a guest user from another organization, you can't select this field.

Account Type	Description
Enterprise and Local	<p>Enables users to sign in using either their Polycom Cloud Services account credentials or their enterprise account credentials from any of the configured authentication providers.</p> <p>This is the only option the service provides when you haven't configured any external authentication providers. Polycom recommends that you configure some users with this sign in type so that they can always sign in with their local account credentials if enterprise authentication service temporarily fails.</p>
Enterprise Only	<p>Enables users to sign in using their enterprise account credentials from any of the configured authentication providers.</p> <p>This option is available only when you configure at least one external authentication provider.</p> <p>Select this option for users who don't need a local account and can use their enterprise account credentials exclusively.</p>

6. Click **Save**.

If you add a guest user from another organization, the user's **Sign In Account** field changes to **Guest** automatically.

A new user from your organization receives one of the following welcome email messages, depending on the account type you selected.

- If you selected **Enterprise and Local** in the **Sign In Account** field, the user receives a welcome email message with an activation link to begin activating the Polycom Cloud Services account.
- If you selected **Enterprise Only** in the **Sign In Account** field, the user receives a welcome email message indicating the system added the user as an administrative user and to use the user's enterprise account credentials when signing in.

A new guest user from another organization receives a welcome email message indicating the system added the user as an administrative user to your organization.

Activate the New or Changed User Account

You can activate your Polycom Cloud Services account from your welcome email.

Procedure

1. In the "Welcome to Polycom Cloud Services" email you received, click **Activate Your Account**.
A browser session will be launched taking you to the **Activate Account** screen.

Note: The activation link in the initial Welcome email message is valid only for 72 hours. If you click on it after that amount of time, the browser session will instead take you to a page that indicates that the link was no longer valid; a new email message is then sent containing a fresh activation link.

2. Enter your name in **First Name** and **Last Name** fields.
3. Create a password in the **Set Password** field.

Note: Password must be between 8 and 32 characters in length and must contain at least one uppercase letter, one lowercase letter, one number, and one special character.

4. Re-enter the password in the **Confirm Password** field.
5. Click **Submit**.

Your account is activated and you are redirected to the main **Sign In** screen.

6. Enter your email address in the **Email Address** field and click **Continue**.
7. When the **Sign In** screen reappears, do one of the following:
 - Enter your password in the **Password field** and click **Sign in**.
 - Click a listed authentication provider and sign in with it.
8. If you're a guest user of another organization, you can select that organization on the **Select Organization** screen when it appears.

Edit a User Account

You can edit the properties of a Polycom Cloud Services user account.

Procedure

1. In the Polycom Cloud Services portal, go to **Administration > Users**.
2. Click **Refresh** to refresh the list manually.
3. Click the user's name that you want to edit.
4. In the user account configuration section, configure the required fields for the user, and do one of the following:
 - Click **Save** to save the changes, then click **>** to close the configuration tab.
 - Click **Cancel** to cancel the changes.

The user receives different notification email messages depending on the **Sign In Account** type changes you make, as follows:

- If you changed the account type to **Enterprise and Local**, the user receives a welcome email with an activation link to begin activating the Polycom Cloud Services local account.
- If you changed the account type to **Enterprise Only**, the user receives a deactivation email indicating the Polycom Cloud Services local account has been deactivated.

Delete a User Account

You can delete a user account.

Procedure

1. In the Polycom Cloud Services portal, go to **Administration > Users**.
2. Click the user you want to delete.
3. Click **Delete**.

When you delete a user's account, the user receives an email notification of the account deletion.

- Deleting your organization user's account, the user can't access all organizations.
- Deleting a guest user's account, the user can't access your organization, but the user still can sign into other tenants.

Related Concepts

[Right to Erasure](#) on page 13

Update Your Profile

You can update your profile from the account menu.

Procedure

1. In the Polycom Cloud Services portal, click the account menu.


2. Select **My Profile** to view your email address, and user name.
3. Optional: Change your `First Name` and `Last Name` if needed.

Related Concepts

[Right to Access](#) on page 12

[Right to Rectification](#) on page 14

Account Management

You must have the **Enterprise Admin** role assigned to your user account to access the **Account Management**  functions.

You can update your current Polycom Cloud Services account name or copy your account ID.


Related Concepts

[Right to Access](#) on page 12

Copy Your Current Account ID

You may need to provide your current account ID when you report a Polycom Cloud Services issue. You can copy it from your account information in the Polycom Cloud Services portal.


Procedure

1. In the Polycom Cloud Services portal, go to **Administration > Account Management > Account Information**.
2. Click **Copy to Clipboard**  to copy the string next to **Account ID**.
3. Paste the string into a text file and save it to your local system.


Edit Your Current Account Name

You can edit your account name in the Polycom Cloud Services portal.

Procedure

1. In the Polycom Cloud Services portal, go to **Administration > Account Management > Account Information**.
2. Click **Edit** .
3. Edit your current account name and click **Save**.

View Activity Logs

Activity Logs  is where you can view previous operations performed by you or other users.

You must have the **User Admin** user role to view previous operations performed by all users. Without **User Admin** user role, you can only view your own previous operations.

Note: The Polycom Cloud Services portal clears activity logs if logs are older than 7 days.

You can identify user activities that may cause Polycom Cloud Services issues, then report the activities and your organization account ID to your Polycom support representatives for further investigation.

Procedure

1. In the Polycom Cloud Services portal, go to **Administration > Activity Logs**.
2. Click **Refresh** to refresh the list manually.

Related Concepts

[Right to Access](#) on page 12

Managing Device Profiles

A user whose Polycom Cloud Service user account has been granted the “Device Admin” role can view, add, edit or delete device profiles and information through the Polycom Cloud Service web portal under the Polycom Device Management Service for Enterprises **Device Monitor** screen.

A user whose Polycom Cloud Service user account has been granted the “Device Operator” role can view device profiles and information through the Polycom Cloud Service web portal under the Polycom Device Management Service for Enterprises **Device Monitor** screen.

Bulk Edit Devices

You can bulk edit devices by exporting the device list, which includes the updated attributes in the auto-generated profiles (if any), to a CSV file.

You can export only the user-imported profiles (named with `MAC_Address_csv_profile` or `serial_number_CSV_profile`) from the device. You cannot export other manually associated user-defined profiles when exporting the device.

Once you update the data by editing the CSV file, import the CSV file to update the device data.

Format:

```
mac_address, serial_number, endpoint_name, endpoint_type, endpoint_group,
reg.[1-5].address, reg.[1-5].displayname, reg.[1-5].auth.userId, reg.
[1-5].auth.password, [any attribute name]
```

Note: The MAC address or serial number is the unique identifier of a device. The service treats a changed MAC address or serial number as a new device instead of an update to the old one.

Procedure

1. In the Polycom Device Management Service for Enterprise portal, go to **Device Monitor**.
2. Click **Export Devices**.
3. Select a separator.
4. Click **Export and Download** to download the CSV file.
5. Open the CSV file and edit the device information as needed.
6. Reimport the updated CSV file.

Related Concepts

[Right to Access](#) on page 12

[Right to Data Portability](#) on page 13

Related Tasks

[Download Activity Logs](#) on page 10

Adding Devices

Add devices to the PDMS-E service based on your deployment's needs.

You can add devices to the Polycom Device Management Service for Enterprise by one of the following options:

- Add devices automatically: Devices that connect to your tenant for provisioning that haven't already been added automatically show up on the **Device Monitor** page.
- Add a device manually: You can stage single device for configuration prior to network deployment.
- Bulk add devices: Import a CSV file to stage devices in bulk for configuration prior to network deployment.

Adding Devices Automatically

The service adds devices to the Polycom Device Management Service for Enterprise automatically based on associations.

Automatically added devices retrieve configuration from the **Global**, **Default Device Group**, **Device Mode**, and **Site** associations.

Add a Device Manually

You can manually add a device on the **Device Monitor** page.

Procedure

1. In the Polycom Device Management Service for Enterprise portal, go to **Device Monitor** and click **Add**.
2. Select the device type and model that you want to add in the **Device Type** and the **Device Model** drop-down lists.
3. Specify the MAC address for audio device or specify the serial number for other devices such as Polycom Studio.
4. Enter a device name in the **Device Name** field.
5. (Optional) In the **Device Group Association** column, select the device group to associate with and click **Apply**.
6. (Optional) In the **Configuration Profile Association** column, select the configuration profile to associate with and click **Apply**.
7. Click **Save**.
8. (Optional) Schedule a task to apply the selected configuration profiles to the device.

Edit a Device

You can update the device name, private IP address, and description using the PDMS-E portal.

Procedure

1. In the Polycom Device Management Service for Enterprise portal, go to **Device Monitor**.
2. Click a device name (hyperlink).
3. In the **Summary** tab, edit the device name, private IP address, and description.
4. Click **Update**.

Related Concepts


[Right to Rectification](#) on page 14

Delete a Device

You can manually delete devices.

After you delete a device that registers to Polycom Cloud registration, the registration is also deleted.

Procedure

1. In the Polycom Device Management Service for Enterprise portal, go to **Device Monitor**.
2. Select a device.
3. Click **Delete** .
4. Click **OK** to confirm.

Related Concepts

[Right to Erasure](#) on page 13

Download Activity Logs

The Polycom Device Management Service for Enterprise saves the administrator operations logs.

The service provides activity logs for adding, editing, deleting, and other operations in a weekly log file. The system retains up to four weeks worth of logs.

Procedure

1. Click **Username > Download Activity Log**.
2. Specify the date for the log that you want to download.
3. Click **Download**.

The logs for the week of the specified date download. For example, if today is Friday and you select today, the log file from Monday to Friday downloads. If you select Monday, the same log file downloads.

Related Concepts

[Right to Data Portability](#) on page 13

Related Tasks

[Bulk Edit Devices](#) on page 8

Saving Log Files to an External Server

If you want to collect device log files on an external server, you can include the `LOG_FILE_DIRECTORY` attribute in a configuration profile to be deployed to the devices.

You can specify a FTP server or HTTP server address. The Polycom Device Management Service for Enterprise sends the device log files to the specified server.

You send logs to an HTTP, HTTPS, FTP, FTPS, or TFTP server by providing the full string value for the server in the `LOG_FILE_DIRECTORY` attribute.

For example:

```
[protocol]://[user]:[password]@[server address]/[path]
```

- Where `[protocol]` may be:
 - HTTP
 - HTTPS
 - FTP

- FTPS
- TFTP
- Where [`Server address`] may be either IP or FQDN Host.
- [`Path`] is optional and environment dependent.
- The variable `$mac_address` can be included. For example: `http://user:password@1.2.3.4/${mac_address}`
`${mac_address}` is included in a path. When deployed, the service replaces the value with the phone's MAC address.

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 Access

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

- A user whose Polycom Cloud Service user account has been granted the “User Admin” role can:
 - View other user account information.
 - View Polycom Cloud Service activity logs for past 7 days.
- Any Polycom Cloud Service user can:
 - View their own user profile information.
 - View their own activity logs for the past 7 days.
- A user whose Polycom Cloud Service user account has been granted either the “Device Admin” or “Device Operator” role can view device profiles and information through the Polycom Cloud Service web portal under the Polycom Device Management Service for Enterprises **Device Monitor** screen.
- A Polycom Cloud Service account which has been granted the Polycom Device Management Service for Enterprises “Device Admin” role can download device information via the Polycom Cloud Service web portal.
- 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 Concepts

[Account Management](#) on page 7

Related Tasks

[Update Your Profile](#) on page 6

[View Activity Logs](#) on page 7

[Bulk Edit Devices](#) on page 8

Right to Be Informed

What personal data is collected?

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

How is personal data is used?

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

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. See the [How admin can be informed of any security anomalies \(including data breach\)](#) table in this topic.

Right to Data Portability

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

A user whose Polycom Cloud Service user account has been granted the “Device Admin” role can:

- Download device information via the Polycom Cloud Service web portal.
- Download activity log files in .txt format via the Polycom Cloud Service web portal.

Related Tasks

[Bulk Edit Devices](#) on page 8

[Download Activity Logs](#) on page 10

Right to Erasure

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

For details on how to erase customer personal data from the system, see the topic [How Personal Data Is Deleted](#) on page 17.

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

- A user whose Polycom Cloud Service user account has been granted the “User Admin” role can delete other user accounts.

Note: Deleting a user account from the Polycom Cloud Service portal does not terminate subscription to the Polycom Cloud Service service. This may only be done by contacting Polycom support.

- A user whose Polycom Cloud Service user account has been granted the “Device Admin” role can delete device profiles.
- Any personal data made available when working with Polycom support, specific to a support incident, is retained until the information is requested to be removed by the customer.

Related Concepts

[How Personal Data Is Deleted](#) on page 17

Related Tasks

[Delete a Device](#) on page 10

[Delete a User Account](#) on page 6

Right to Rectification

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

- A user whose Polycom Cloud Service user account has been granted the “User Admin” role can view and edit other user account information.
- All Polycom Cloud Service users can edit their user profile information.
- A user whose Polycom Cloud Service user account has been granted the “Device Admin” role can edit device profiles and information through the Polycom Cloud Service web portal.
- Polycom does not manipulate data made available during the support process, so any rectification of inaccuracies of personal data sent to Polycom support must be performed by the customer directly.

Related Concepts

[User Management](#) on page 3

Related Tasks

[Update Your Profile](#) on page 6

[Edit a Device](#) on page 9

Purposes of Processing Personal Data

See the *Purposes for processing personal data* table in the *Polycom Device Management Service for Enterprises Security and Privacy White Paper* [here](#).

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).

Security Anomaly Type	Where to Check	How to Request Information
Security related service and platform events	Polycom Device Management Service for Enterprises and Polycom Cloud Service security related service and platform alarms and alerts can only be viewed by Polycom support.	<ul style="list-style-type: none">▪ Please contact Polycom support to request information about security related events.▪ The activity logs can also provide an indication of a breach in the case of the misuse of an authorized user's account.

How Personal Data Is Deleted

This table lists how personal data is deleted.

Data Type	Steps to Delete	Deletion Method
Account information	<p>A user whose Polycom Cloud Service user account has been granted the “User Admin” role can delete other user accounts by following steps in the Polycom Cloud Service admin guide here.</p> <p>Note: Cloud Service portal does not terminate subscription to the Polycom Cloud Service service. This may only be done by contacting Polycom support.</p>	Manual - Simple delete
Device information	<p>A user whose Polycom Cloud Service user account has been granted the “Device Admin” role can delete device profiles through the Polycom Cloud Service web portal via the Polycom Device Management Service for Enterprises Device Monitor screen.</p>	Manual - Simple delete
Activity log files	<p>All Polycom Device Management Service for Enterprises activity log files are retained for 28 days after which they are automatically deleted by the system.</p> <p>All Polycom Cloud Service activity log files are retained for 7 days after which they are automatically deleted by the system.</p>	Automatic - Simple delete
Device log files	<p>All Polycom Device Management Service for Enterprises device log files are retained for 10 days after which they are automatically deleted by the system.</p> <p>This is not applicable for Polycom Cloud Service.</p>	Automatic - Simple delete

Data Type	Steps to Delete	Deletion Method
Troubleshooting log files	<p>This is not applicable for Polycom Device Management Service for Enterprises since all troubleshooting logs are sent to Polycom Cloud Service for storage.</p> <p>Once customer contract is terminated under normal terms and conditions, troubleshooting logs are deleted immediately with backups deleted in 30 days.</p>	Automatic - Simple delete
Data backups	<p>Customer personal data is automatically backed up daily.</p> <p>All Polycom Device Management Service for Enterprises backups are retained for 7 days after which they are automatically deleted by the system.</p> <p>All Polycom Cloud Service backups are retained for 30 days after which they are deleted by the system.</p>	Automatic - Simple delete

Related Concepts

[Right to Erasure](#) on page 13

Copyright© 2019, Polycom, Inc. All rights reserved. No part of this document may be reproduced, translated into another language or format, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc.

6001 America Center Drive
San Jose, CA 95002
USA

Trademarks Polycom®, the Polycom logo and the names and marks associated with Polycom products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries.



All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

End User License Agreement By installing, copying, or otherwise using this product, you acknowledge that you have read, understand and agree to be bound by the terms and conditions of the End User License Agreement for this product. The EULA for this product is available on the Polycom Support page for the product.

Patent Information The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

Open Source Software Used in this Product This product may contain open source software. You may receive the open source software from Polycom up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to Polycom of shipping or distributing the software to you. To receive software information, as well as the open source software code used in this product, contact Polycom by email at OpenSourceVideo@polycom.com (for video products) or OpenSourceVoice@polycom.com (for voice products).

Disclaimer While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

Limitation of Liability Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.

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.