SECURITY AND PRIVACY WHITE PAPER

Polycom® Device Management Service

Part 3725-85376-001

Version 1.1 September 2018

Introduction

This white paper addresses security and privacy related information regarding the Polycom® Device Management Service and describes the security features and access controls in Polycom's processing of personally identifiable information or personal data ("personal data") and customer data regarding the provisioning and delivery of the service, and the location and transfers of personal and other customer data used to provide this service. Polycom will use such data in a manner consistent with the *Polycom Privacy Policy* and this white paper (as may be updated from time to time). This white paper is supplemental to the *Polycom Privacy Policy*. The most current version of this white paper will be available on *Polycom's website*.

If you are an individual user and the purchase of Polycom Device Management Service has been made by your employer as the Customer, all the privacy information relating to personal data is subject to your employer's privacy policies as controller of such personal data.

The Polycom Device Management Service is a cloud-based device management service for Polycom Audio Endpoints (both personal and conference-based).

Security at Polycom

Security is always a critical consideration for any product whether it is network-connected a device or a cloud-based service such as Polycom Device Management Service. Polycom has been awarded ISO/IEC 27001:2013 certification for our Information Security Management System (ISMS). ISO/IEC 27001 is the most widely accepted international standard for information security best practices and a tangible measure by which existing and potential customers can be reassured that Polycom has established and implemented best-practice information security processes. ISO/IEC 27001:2013 certification not only reinforces our commitment to information security best practices and controls but it explicitly includes the product development process.

Product security at Polycom is managed through the Polycom Security Office (PSO), which oversees secure software development standards and guidelines. The Polycom *Product Security Standards* align with NIST Special Publication 800-53, ISO/IEC 27001:2013 and OWASP for application security.

Guidelines, standards and policies are implemented to provide our developers industry-approved methods for adhering to the Polycom Product Security Standards.

Secure software development life cycle

Polycom follows a secure software development life cycle (S-SDLC) with an emphasis on security throughout the product development processes. Every phase of development ensures security by establishing security requirements alongside functional requirements as part of initial design. Architecture reviews, code reviews, internal penetration testing and attack surface analysis are performed to verify the implementation.

The S-SDLC implemented by Polycom also includes a significant emphasis on risk analysis and vulnerability management. To increase the security posture of Polycom products, a defense-in-depth model is systematically incorporated through layered defenses. The principle of least privilege is always followed. Access is disabled or restricted to system services nonessential to standard operation. Additional testing, in the form of standards-based Static Application Security Testing and patch management is a cornerstone of our S-SDLC.

Change management

A formal change management process is followed by all teams at Polycom to minimize any impact on the services provided to customers. All changes implemented to the Polycom Device Management Service go through vigorous QA testing where all functional and security requirements are verified. Once QA approves the changes, the changes are pushed to a staging environment for UAT (User Acceptance Testing) testing. Only after final approval from stakeholders are changes implemented in production. All scheduled changes are applied during regularly scheduled maintenance periods. While emergency changes are processed on a much faster timeline, risk is evaluated, and approvals are obtained from stakeholders prior to application.

Privacy by design

Polycom implements internal policies and measures based on perceived risks which meet the principles of data protection by design and data protection by default. Such measures consist of minimizing the processing of personal data, anonymizing personal data as soon as possible, transparently documenting the functions and processing of personal data and providing features which enable the data subject to monitor the data processing while also enabling the data controller to create and improve security features.

When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfill their task,

Polycom considers the right to data protection with due regard to making sure that data controllers and processors can fulfill their data protection obligations.

User authentication

User authentication for the Polycom Device Management Service is provided by the Polycom Cloud Service, which offers two different methods. The first is to use the built-in "local" Polycom Cloud Service user accounts. Each Polycom Cloud Service customer gets at least one "local" account that is created when the customer activates their Polycom Cloud Service. These accounts use a user's email address as the user ID; the email address is verified via an email that contains an activation link, which, when followed, allows the user to configure a password for the account, at which time they can sign in. Users then can manage their passwords as needed, with the ability to reset their password if it is forgotten or change it at their discretion. All local passwords are stored in 1-way encrypted format using SHA256 hashing.

The second method is to federate the Polycom Cloud Service to the customer's enterprise authentication service. Polycom Cloud Service supports federation via OAuth 2.0 to both Microsoft Office 365/Azure AD and to Microsoft Active Directory (via Active Directory Federation Services 3.0). This allows users to use their enterprise user account credentials when signing in to the Polycom Cloud Service, entering them only into the federated authentication provider's own sign-in page and enjoying whatever level of Single Sign On (SSO) integration has been configured in their organization. The Polycom Cloud Service then receives access tokens from the authentication provider that grant it limited and controlled access to resources owned by a user.

Note:

- Access tokens are not stored by the cloud service—they are discarded after being used to obtain basic user profile information (user email address, user display name).
- Access tokens have limited lifetimes controlled by the authentication provider.

Role-Based Access Control (RBAC) allows the Polycom cloud service administrator to tailor access control to each user based on their specific access needs. For Polycom Device Management Service specifically, both a 'Device Admin' and 'Device Operator' role can be selected for users—the former provides full access to device management functions; the latter provides a 'viewing-only' access level. See the Polycom Cloud Service Administration Guide for more details on user roles.

Cryptographic security

Polycom Device Management Service uses secure communication channels for all connections between its cloud services and the devices it manages.

Summary

Polycom Cloud Service Administration Portal

- HTTPS (443) using TLS 1.1, TLS 1.2
  - Compression: disabled
  - RFC 5746 renegotiation
    - » Client-initiated: disabled
  - Ciphers
    - » AES 128/256 (CBC, GCM)
    - » Key Exchange: DHE 2048, ECDHE 256
    - » SHA, SHA256, SHA384 hashing

Polycom Device Management Service Portal

- HTTPS (443) using TLS 1.2
  - Compression: disabled
  - RFC 5746 renegotiation
    - » Client-initiated: disabled
  - Ciphers
    - » AES 128/256
    - » Key Exchange: ECDHE 256
    - » SHA, SHA256, SHA384 hashing

Polycom Cloud Relay to Polycom Cloud Service

- HTTPS (443) using TLS 1.1, TLS 1.2
  - Compression: disabled
  - RFC 5746 renegotiation
    - » Client-initiated: disabled
  - Ciphers
    - » AES 128/256 (CBC, GCM)
    - » Key Exchange: DHE 2048, ECDHE 256
    - » SHA, SHA256, SHA384 hashing

Polycom Cloud Relay Device Connections (to local on-premise devices)

- HTTPS (443) using 1.1, 1.2
  - Compression: disabled
  - RFC 5746 renegotiation
    - » Client-initiated: disabled
  - Ciphers
    - » AES 128/256 (CBC, GCM), Camellia 128/256 (CBC)
    - » Key Exchange: ECDHE 256, RSA
    - » SHA, SHA256, SHA384 hashing

TLS cipher suites and modules implemented in the Polycom Cloud Service are open (i.e., publicly disclosed) and have been peer reviewed. Cryptographic libraries are current and regularly updated.

Disaster recovery

Polycom Device Management Service is architected to provide high reliability, resiliency and security. The service is hosted within the Microsoft Azure cloud to leverage the scalability, availability, and redundancy offered within such an environment.

All customer data is backed up daily. Access controls are implemented for authorized users and data security policies are followed for all backup data. No physical transport of backup media occurs. The backup data, both at rest and while in transit, is encrypted using AES 256.

Data processing

The Device Management Service collects and processes data related to the provisioning, configuration and management of supported devices, including:

- Site names, descriptions and locations
- Site device counts
- Device names and group lists
- Device-configuration profiles
- Device software updates

Additionally, with Polycom Cloud Relay deployed:

- Line registration status and URI
- Call status
- Device uptime and last reboot time
- Scheduled tasks

Purpose of processing

The primary purposes of processing information by the Device Management Service are to:

Manage site provisioning—Sites are a collection of customer-defined networks that can be configured for management and deployment of devices.

Enable device provisioning—View your devices and manage important information like software versions and device configurations.

Personal data is processed only as it is relevant to the configuration and provisioning of audio devices.

Personal Data Category	Type of Personal Data	Purpose of Processing
Administrative user profile	• Name • Email address • Password • Organization name	• Authenticate and authorize administrative access to the service
Device information	• Device name • Device public IP • Device private IP • MAC address • SIP URI • SIP user • Far site name • Far site number	• Configuration of devices • Monitoring of devices (only available when deployed with Cloud Relay)

How customer data is stored and protected

The Polycom Device Management Service is hosted in the Microsoft Azure Cloud, in a data center located in the United States region of the Americas geography. Polycom has implemented technical and physical controls designed to prevent unauthorized access to, or disclosure of customer content. In addition, we have systems, procedures and policies in place to prevent unauthorized access to customer data and content by Polycom employees.

Polycom may change the location of the Device Management Service in the future; details of any such change shall be set forth in the latest copy of this white paper available on *Polycom's website*.

For transferring personal data of EU Customers to the US, Polycom uses an Intragroup Data Transfer Agreement incorporating the EU Standard Contractual Clauses as the transfer mechanism.

All customer data is stored within the data center(s) on which the service is deployed in an encrypted form at rest using 256-bit AES encryption.

All customer data is backed up daily. Normal access controls of authorized users and data security policies are followed for all backup data. No physical transport of backup media occurs. The backup data during rest and while in transit is encrypted using AES 256.

Server access and data security

Servers are in a secure data center, with only authorized staff members having access. The servers are not directly accessible from outside the data center—they are accessed only via a secured 'bastion' server, with only authorized Polycom Cloud Service personnel granted access to it.

Each customer's data resides in the data center in a multi-tenant system and is compartmentalized using access controls to provide data isolation between Polycom Device Management Service customers. All customer data is encrypted both at rest and in transit using strong cryptography including AES-256 and TLS up to v1.2.

For details on Microsoft Azure's underlying security mechanisms upon which the Polycom Device Management Service is built, see *https://azure.microsoft.com/en-us/blog/azure-layered-approach-to-physical-security/*

Polycom has implemented technical and physical controls designed to prevent unauthorized access to or disclosure of customer content or customer personal data. In addition, we have systems, procedures and policies in place to prevent unauthorized access to customer data and content by Polycom employees.

Third-party providers (sub-processors)

Polycom shares customer information with service providers, contractors, or other third parties to assist in providing and improving the service. All sharing of information is carried out consistent with the *Polycom Privacy Policy*.

Data deletion & retention

Polycom may retain customer data for as long as needed to provide that customer the Polycom Device Management Service. After a customer's subscription terminates or expires, Polycom will delete personal data within one year of termination or expiration of the service. When a Customer makes a request for deletion, Polycom will delete the requested data within 30 days, unless the data is required to be retained for Polycom's legitimate interests or if needed to provide the service to customer. Polycom may "anonymize" personal data in lieu of deletion. The anonymization process is irreversible and includes but is not limited to searching and sanitizing all customer-specific data (such as name, site information, and IP address) with randomly generated alphanumeric characters.

Data portability

Polycom Device Management Service administrators can download the following customer data from the PDMS Portal:

- Export user-defined configuration profiles.
- Export device lists and attributes as CSV files.

Security incident response

The Polycom Security Office (PSO) promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. You may contact the PSO directly at *informationsecurity@polycom.com*.

The PSO team works proactively with customers, independent security researchers, consultants, industry organizations and other suppliers to identify possible security issues with Polycom products and networks.

Polycom security advisories and bulletins can be found on the *Polycom Security Center*.

Additional resources

To learn more about the Polycom Device Management Service, please visit our *website*.

DISCLAIMER

This white paper is provided for informational purposes only, and does not convey any legal rights to any intellectual property in any Polycom product. You may copy and use this paper for your internal reference purposes only. POLYCOM MAKES NO WARRANTIES, EXPRESS OR IMPLIED OR STATUTORY AS TO THE INFORMATION IN THIS WHITE PAPER. THIS WHITE PAPER IS PROVIDED "AS IS" AND MAY BE UPDATED BY POLYCOM FROM TIME TO TIME. To review the most current version of this white paper, please visit our *website*.

About Polycom

Polycom helps organizations unleash the power of human collaboration. More than 400,000 companies and institutions worldwide defy distance with video, voice and content solutions from Polycom. Polycom and its global partner ecosystem provide flexible collaboration solutions for any environment that deliver the best user experience and unmatched investment protection.

Polycom, Inc.
1.800.POLYCOM
www.polycom.com

Polycom Asia Pacific Pte Ltd
+65 6389 9200
www.polycom.asia

Polycom EMEA
+44 (0)1753 723282
www.polycom.co.uk

35840-0918