



SECURITY AND PRIVACY WHITE PAPER

# Polycom Device Management Service for Enterprise

Part 3725-85376-001

Version 1.1

September 2018

## SECURITY AND PRIVACY WHITE PAPER FOR DEVICE MANAGEMENT SERVICE FOR ENTERPRISE

### INTRODUCTION

This white paper addresses security and privacy related information for Polycom Device Management Service for Enterprise (PDMS-E). It also describes the security features and access controls in Poly's processing of personally identifiable information or personal data ("personal data") and customer data in connection with the running of the RealPresence DMA product, as well as the location and transfer of personal and other customer data. Poly uses such data in a manner consistent with the [Poly Privacy Policy](#) and this white paper (as may be updated from time to time). This white paper is supplemental to the [Poly 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 POLY

Security is always a critical consideration for any product whether it is a network-connected device or a cloud-based service such as Polycom Device Management Service. Polycom aligns with ISO/IEC 27001:2013 practices 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 Poly 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 Poly is managed through the Poly Security Office (PSO), which oversees secure

software development standards and guidelines. The Poly 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 Poly Product Security Standards.

### SECURE SOFTWARE DEVELOPMENT LIFE CYCLE

Poly follows a Secure Software Development Life Cycle (S-SDLC) with an emphasis on security throughout the product development process. Every phase of the development process 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 Poly also includes a significant emphasis on risk analysis and vulnerability management. To increase the security posture of Poly 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.

### PRIVACY BY DESIGN

Poly 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.

## SECURITY AND PRIVACY WHITE PAPER FOR DEVICE MANAGEMENT SERVICE FOR ENTERPRISE

When developing, designing, selecting, and using applications, services and products that are based on the processing of personal data or Poly 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 levels. 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 TLS 1.1, TLS 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 device, 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 importance 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
<b>Administrative user profile</b>	<ul style="list-style-type: none"> <li>• Name</li> <li>• Email address</li> <li>• Password</li> <li>• Organization name</li> </ul>	<ul style="list-style-type: none"> <li>• Authenticate and authorize administrative access to the service</li> </ul>

<b>Device information</b>	<ul style="list-style-type: none"> <li>• Device name</li> <li>• Device public IP</li> <li>• Device private IP</li> <li>• MAC address</li> <li>• SIP URI</li> <li>• SIP user</li> <li>• Far site name</li> <li>• Far site number</li> </ul>	<ul style="list-style-type: none"> <li>• Configuration of devices</li> <li>• Monitoring of devices (only available when deployed with Cloud Relay)</li> </ul>
---------------------------	--	---

**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 America geography. Poly 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.

Poly 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 [Poly’s website](#).

For transferring personal data of EU customers to the US, Poly 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 for 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/>.

Poly has implemented technical and physical control 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 Poly employees.

**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.

**THIRD-PARTY PROVIDERS (SUB-PROCESSORS)**

Poly 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 [Poly Privacy Policy](#).

**DATA DELETION AND RETENTION**

Poly may retain customer data for as long as needed to provide the customer support for the Polycom Device Management Service product. After a customer’s subscription terminates or expires, Poly will delete personal data within one

year of termination or expiration of the service. When a customer makes a request for deletion, Poly will delete the requested data within 30 days, unless the data is required to be retained for Poly's legitimate interests or if needed to provide the service to the customer. Poly 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.

### CHANGE MANAGEMENT

A formal change management process is followed by all teams at Poly 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). 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.

### SECURITY INCIDENT RESPONSE

The Poly Security Office (PSO) promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. You can contact the PSO directly at [informationsecurity@poly.com](mailto:informationsecurity@poly.com)

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

Poly security advisories and bulletins can be found at the [Poly Security Center](#).

### ADDITIONAL RESOURCES

To learn more about the Polycom Device Management Service, please visit our [website](#).

### DISCLAIMER:

This document is provided for informational purposes only and does not convey any legal rights to any intellectual property in any Poly product. You may copy and use this paper for your internal reference purposes only. POLY 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 POLY FROM TIME TO TIME.

