SECURITY AND PRIVACY WHITE PAPER

Polycom RealConnect Service (RealConnect for Office 365 and RealConnect for Teams)

Part 3725-85375-001

Revision C March 2019 © 2019 Polycom, Inc. All rights reserved

Introduction

This white paper addresses security and privacy related information regarding Polycom RealConnect for Office 365 and Teams. It also describes the security features and access controls in Polycom's processing of PII (personally identifiable information or personal data) including customer data in connection with the provisioning and delivery of Polycom RealConnect Service, and the location and transfers of those data. Polycom will use data in a manner consistent with the *Polycom Privacy Policy*. 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*.

Polycom RealConnect for Office 365 is a certified video interoperability solution for Office 365 and Skype for Business. Polycom RealConnect for Teams is a certified video interoperability solution for Microsoft Teams. These services allow standard-based devices, such as Polycom and Cisco video endpoints, to join either a Skype for Business meeting or a Microsoft Teams meeting. The Polycom RealConnect Service is integrated into the Skype and Teams meeting workflow making it easy and intuitive to schedule a video interop call.

Security at Polycom

Security is always a critical consideration for any product whether it is a network-connected device or a cloud-based service such as Polycom RealConnect for Office 365 and Teams.

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 lifecycle

Polycom follows a secure software development lifecycle (S-SDLC) with an emphasis on security throughout the product development processes. Every phase of 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 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 the customers. All changes deployed to Polycom RealConnect 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, changes are 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 applying any changes in production.

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.

Revision C March 2019 © 2019 Polycom, Inc. All rights reserved

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 are able to fulfill their data protection obligations.

User authentication

Polycom RealConnect for Office 365 and Teams supports integration of enterprise authentication providers via the OAuth2 standard.

With OAuth2, Polycom RealConnect for Office 365 and Teams can securely integrate with enterprise authentication providers and thereby authenticate enterprise users without ever having access to their credentials. Users enter credentials only into the authentication provider's own sign-in page. Polycom RealConnect Service then receives access tokens from the authentication provider that grants 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
- The cloud service supports the following authentication providers:
  - Microsoft Active Directory Federation Services 3.0 via OAuth2
  - Microsoft Office 365 (Azure AD) via OAuth2

Disaster recovery

The Polycom RealConnect Service is architected to provide high reliability, resiliency and security. The entire service is hosted on multiple geographically distributed Microsoft Azure data centers. Normal low impact outage due to loss of power or connectivity is already handled by the cloud hosting provider—Microsoft Azure.

During a major crisis or disaster, service will be moved to a different region until the affected region is restored.

Cryptographic security

All communication with the Polycom RealConnect for Office 365 and Teams web portal is encrypted over an HTTPS connection that uses TLS 1.2 with 128 or 256-bit encryption and a 2048-bit key exchange mechanism. Cryptographic cipher suites and modules implemented in the Polycom RealConnect Service are open (i.e., publicly disclosed) and have been peer reviewed. Cryptographic libraries are current, regularly updated and leverage the Advanced Encryption Standard (AES-128 and AES-256) cipher suites. Hash strengths supported include SHA-256 and SHA-384.

Polycom RealConnect for Office 365 and Teams ensures that your communications are secure and does not record or capture video or audio streams. Media transported between Polycom RealConnect for Office 365 and Teams cloud and the customer's endpoint is encrypted at the customer's option. Please note that some video endpoints may need additional licenses for an encryption option.

All traffic transported between Polycom RealConnect Service and Microsoft is always encrypted.

Data processing

Polycom does not access any customer's data except as required to enable the features provided by the service. If you are an individual user and the purchase of Polycom RealConnect for Office 365 and Teams has been made by your employer as the customer, all of the privacy information relating to personal data in this white paper is subject to your employer's privacy policies as controller of such personal data.

Personal Data Category	Type of Personal Data	Purpose of Processing
Service user information	• Display name • Email address • IP address	• Display identity to other users • Authentication and authorization
Device information	• Device name • IP address	• Diagnose technical issues • IP addresses are used to connect video endpoints to the Skype for Business or Teams service

 © 2019 Polycom, Inc. All rights reserved

Purpose of processing

Polycom RealConnect for Office 365 and Teams collects data to enable users to have a seamless video and content collaboration experience in Skype for Business or Teams calls, regardless of the video device they use to join. Data is collected for internal services to operate. Some data elements are additionally used to perform internal analysis and reporting.

How customer data is stored and protected

The Polycom RealConnect for Office 365 and Teams stores customer data in Azure CosmosDB. Data is encrypted at rest using AES 256. Data may reside in the United States, the Netherlands or Australia. To learn about how encryption is applied, please visit the following link: *https://docs.microsoft.com/en-us/azure/cosmos-db/database-encryption-at-rest*

Polycom may change the location of the RealConnect Service database server and 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 E.U. customers to the U.S., Polycom uses an Intragroup Data Transfer Agreement incorporating the E.U. Standard Contractual Clauses as the transfer mechanism.

Customer data is backed up daily using Azure data factory. Access is restricted to control access only to authorized users and data security policies are followed for all backup data. No physical transport of backup media occurs. The backup data in transit is encrypted using AES 256.

Server access and data security

Polycom RealConnect Service is hosted in Microsoft Azure. Only authorized staff members with proper access permissions have access to the production servers. For details, see *https://azure.microsoft.com/en-us/blog/azure-layered-approach-to-physical-security/*

Polycom has also 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.

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 the customer the Polycom RealConnect for Office 365 and Teams 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 (e.g., name, site information and IP address) with randomly generated alphanumeric characters.

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 Polycom RealConnect Service, please visit our *website*.

Revision C March 2019 © 2019 Polycom, Inc. All rights reserved

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

© 2019 Polycom, Inc. All rights reserved. All Polycom® names and marks associated with Polycom products are trademarks or service marks of Polycom, Inc. and are registered or common law marks in the United States and 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.

38141-0319