SECURITY AND PRIVACY WHITE PAPER

Polycom® OBiTALK

Part 3725-85377-001

Version 1.1 September 2018

Introduction

This white paper addresses security and privacy related information regarding Polycom® OBiTALK. 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 service and delivery of the service, and the location and transfer personal and other customer 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 OBiTALK is an online portal for managing Polycom phones and analog telephone adapters. The portal provides an easy way to add, configure and check the status of the devices. It also provides the following key functionalities:

- Add, delete or manage Polycom phones and ATAs
- View overall status of devices
- Setup wizards for configuring voice services like Google Voice or other VoIP service providers
- Subscribe to additional services such as ObiExtras or Extended Product Warranty
- Quick access to product FAQs, the OBiTALK Community Forum and other documentation

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 OBiTALK. 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 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 (SAST) 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 implemented to Polycom OBiTALK 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.

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 OBiTALK provides HTTP basic authentication using a username and password. The data is transported using HTTPS over TLS.

Disaster recovery

The Polycom OBiTALK Service is architected to provide high reliability, resiliency and security. The entire service is hosted in Amazon Web Services (AWS) to leverage the scalability and redundancy offered by such an environment. Normal low impact outage due to loss of power or connectivity is handled by the cloud hosting provider—AWS. 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 OBiTALK web portal is over a standard secure SSL connection that encrypts all requests and responses. Transport Layer Security (TLS) between components of OBiTALK is mutual for all connections. Protocol version TLS 1.2 is preferred for a secure connection. TLS compression and client initiated renegotiation also are disabled. Where implemented, secure server renegotiation is compliant with RFC 5746.

Cryptographic cipher suites and modules implemented in the OBiTALK 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, SHA-384 and SHA-512

Data processing

The OBiTALK Service collects and processes logs containing:

- Device data (includes information like type of device, device name, phone numbers and installed software version)
- Call data (includes call connection information like IP addresses, and other caller personal data like userID, or caller name).

If you are an individual user and the purchase of OBiTALK 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
Call participant device information AND managed device info	• Device name • IP address • Geolocation • MAC address • Time zone	• Understand how the service is used • Diagnose technical issues • Conduct analytics and analysis to improve the technical performance of the service • Respond to customer support requests

Purpose of processing

The primary purposes of processing information by OBiTALK are to:

Enable asset management—View your device information, manage important information like software versions and device data, and to collect and process device and call statistics.

Perform data analytics—Better understand utilization, capacity and performance. Personal data is processed for display and reporting purposes only.

How customer data is stored and protected

The OBiTALK service is run on distributed Amazon AWS servers that run dedicated databases and application servers that reside in the United States. When the OBiTALK database server receives data from the customer, it is verified for integrity, processed, and saved in the database.

The OBiTALK database and application servers reside in the data center behind a fully patched firewall. Access for any services not required by OBiTALK is blocked.

Polycom may change the location of the OBiTALK 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 EU Customers to the US, Polycom uses an Intragroup Data Transfer Agreement incorporating the EU Standard Contractual Clauses as the transfer mechanism.

Server access and security

Polycom OBiTALK is hosted in the Amazon cloud. Only authorized staff members with proper access permissions have access to the production servers.

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

Customer data is backed up daily. 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, both at rest and while in transit, is encrypted using AES 256.

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*.

If you subscribe to the optional feature ObiExtras or purchase an extended warranty, you will be redirected to Amazon directly to complete your purchase. Polycom does not collect or process your payment information.

Data deletion & retention

All information collected from the customer is stored in the multi-tenant database, in AWS.

Polycom may retain customer data for as long as needed to provide the customer the OBiTALK 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.

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 OBiTALK, please visit our *site*.

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

Polycom®