SECURITY AND PRIVACY WHITE PAPER

Polycom® One Touch Dial (Cloud Service)

Part 3725-85485-001

Version 1.0 September 2018 © 2018 Polycom, Inc. All rights reserved
Introduction
This white paper addresses security- and privacy-related information regarding the Polycom® One Touch Dial cloud service. This white paper describes the security features and access controls in Polycom’s processing of personally identifiable information or personal data (“personal data”) and customer data in connection with the provisioning and delivery of the Polycom One Touch Dial cloud service, and the location and transfers of personal and other customer data. Polycom will use such data in a manner consistent with the Polycom Privacy Policy and this white paper (as updated from time to time). This white paper is supplemental to the Polycom Privacy Policy. The most current version of this paper will be available on the Polycom website.

The Polycom One Touch Dial cloud service enables an endpoint device to join a meeting by simply clicking a “join” button on the device without the need to dial a potentially long string of digits or a URL. The Polycom One Touch Dial cloud service can be used as a standalone service or it is often paired with Polycom® RealConnect™ for Office 365 cloud service or other third-party conference hosting services—providing the convenience of simplifying how an endpoint joins a meeting.

Note: This white paper only addresses the Polycom One Touch Dial cloud service. Polycom Global Services also offers the Polycom One Touch Dial App, which is a software application that is installed as a web service on customer premises. More information about the Polycom One Touch Dial App may be found here.

Security at Polycom
Security is a critical consideration in the deployment of any network-connected device, and even more so for enterprise integration with a cloud-based service such as Polycom One Touch Dial.

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.


Guidelines for the implementation of specific security technologies—such as cryptographic controls related to ciphers, protocols, storage and web services—are intended 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 customers. All changes implemented to the Polycom One Touch Dial cloud service go through vigorous QA testing where all functional and security requirements are verified. Once QA approves the changes, they are pushed to a staging environment for user acceptance testing (UAT). 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 fulfil data controllers’ and processors’ tasks, Polycom considers the right to data protection with due regard to making sure that they are able to fulfil their data protection obligations.

Secure deployment
The Polycom One Touch Dial cloud service supports two deployment topologies. In support of Polycom endpoints, Exchange Web Services is used to provide the calendar to the endpoint. For third-party endpoints, the Polycom Cloud Relay is deployed on-premises to push calendar events to the endpoint through the endpoint’s native API.

Calendar connections over Exchange Web Services support TLS v1.2. Older versions of TLS are available to support legacy endpoint models. Consult the Administrator’s Guide for detailed information about configuration options.

For customers that have opted to deploy Polycom Cloud Relay, communication of calendar events from the service to the on-premises virtual appliance is encrypted using TLS v1.2 and delivered over an AMQP message bus. Subsequent delivery of calendar events from Polycom Cloud Relay to the endpoint is over the customer’s internal network.

The Polycom One Touch Dial cloud service ensures that your communications are secure and does not record or capture calendar events. As stated above, calendar events that are transported between the service and the customer’s endpoint is encrypted using TLS.

All traffic transported between the Polycom One Touch Dial cloud service and Microsoft O365, Microsoft Exchange on-premises and Google as calendar providers is always encrypted.

User authentication
The Polycom One Touch Dial cloud service supports the integration of enterprise authentication providers via the OAuth2 standard.

With OAuth2, the Polycom One Touch Dial cloud service 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. The Polycom One Touch Dial cloud service then receives access tokens from the authentication provider that grant it limited and controlled access to resources owned by a user.

- Access tokens are not stored by the cloud service—They are discarded after being used to obtain basic user profile information (e.g., user email address, user display name).
- Access tokens have limited lifetimes controlled by the authentication provider.
- Refresh tokens are cached for continued calendar access on behalf of the calendar owner in order to provide ongoing updates to the video endpoint device.
- The cloud service supports the following authentication providers:
  - Microsoft Active Directory Federation Services 3.0 via OAuth2
  - Microsoft Office 365 (Azure AD) via OAuth2
  - Google via OAuth2

Cryptographic security
All communication with the Polycom One Touch Dial cloud service web portal is encrypted over an HTTPS connection that uses TLS v1.2 with 128 or 256-bit encryption using a 1024-bit or 2048-bit key exchange mechanism. Cryptographic cipher suites and modules implemented in the Polycom One Touch Dial cloud 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, SHA-256 and SHA-384.

Disaster recovery
The Polycom One Touch Dial cloud service is architected to provide high reliability, resiliency and security. Each session is completely transient.

The service is hosted on multiple, geographically distributed Microsoft Azure datacenters, see: https://azure.microsoft.com/en-us/blog/azure-layered-approach-to-physical-security/.
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 the Polycom One Touch Dial cloud service 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.

Purpose of processing
The primary purposes of processing information by the Polycom One Touch Dial cloud service is to enable an endpoint device to join a meeting by simply clicking a “join” button on the device without the need to dial a potentially long string of digits or a URL. Additional processing of information is for logging and diagnostic purposes and security adjudication.

The full complement of information collected is company confidential but is available under a signed NDA agreement. Contact your Polycom representative for more details.

Personal data collected is listed in the table below:

<table>
<thead>
<tr>
<th>Personal data category</th>
<th>Type of personal data</th>
<th>Purpose of processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account configuration</td>
<td>• Email address</td>
<td>• Reading calendar • Display of calendar to device association • Diagnose technical issues</td>
</tr>
<tr>
<td>Device configuration</td>
<td>• Username/password • IP address</td>
<td>• Pushing calendar to video teleconferencing endpoint • Diagnose technical issues</td>
</tr>
</tbody>
</table>

How customer data is stored and protected
All customer data is stored within the datacenters on which the service is deployed in an encrypted form at rest using 256-bit AES encryption.

Customer data is backed up daily in digital form. 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.

Customer data will be anonymized upon customer request at the end of a subscription. The anonymization process includes and is not limited to searching and sanitizing all customer-specific data (e.g., name, site information, IP address) with randomly generated alphanumeric characters.

Data resides in the United States. Polycom may change the location of the Polycom One Touch Dial cloud service database servers.

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.

Data deletion & retention
Polycom will only retain customer data for as long as needed to provide that customer the Polycom One Touch Dial cloud 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 business purposes 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, IP address) with randomly generated alphanumeric characters.

Server access and data security
The Polycom One Touch Dial cloud service is hosted on 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 also 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.
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.

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 One Touch Dial cloud service, please visit our website.