SECURITY AND PRIVACY WHITE PAPER

Poly One Touch Dial Cloud Service

Part 3725-87726-001

Version 08

March 2024

Introduction

This white paper addresses security and privacy-related information regarding the Poly One Touch Dial (OTD) Cloud Service.

This paper also describes the security features and access controls in HP | Poly's processing of personally identifiable information or personal data ("personal data") and customer data in connection with the provisioning and delivery of the OTD service, and the location and transfers of personal and other customer data. HP | Poly will use such data in a manner consistent with the HP Privacy Statement, and this white paper which may be updated from time to time. This white paper is supplemental to the HP Privacy Statement. The most current version of this white paper will be available on HP | Poly's website.

The OTD 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 OTD service can be used as a standalone service, or it is often paired with the Poly RealConnect 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 OTD service. HP | Poly Global Services also offers the Poly One Touch Dial App, which is a software application that is installed as a web service on customer premises.

Security at HP | Poly

Security is always a critical consideration for all HP | Poly products and services. HP | Poly's Information Security Management System (ISMS) has achieved ISO 27001:2013 certification. ISO/IEC 27001 is the most widely accepted international standard for information security best practices and you can be reassured that HP | Poly has established and implemented best-practice information security processes.

Product security at HP | Poly is managed through the HP Cybersecurity team, which oversees secure software development standards and guidelines. The HP | 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 with industry-approved methods for adhering to the HP | Poly Product Security Standards.

Secure Software Development Life Cycle

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

The S-SDLC implemented by HP | Poly also includes a significant emphasis on risk analysis and vulnerability management. To increase the security posture of HP | 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.

Standards-based Static Application Security Testing (SAST) and patch management are cornerstones of our S-SDLC.

Privacy by Design

HP | 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 exercise any rights they may have.

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, HP | Poly considers the right to data protection with due regard.

Security by Design

HP | Poly follows Security by Design principles throughout our product creation and delivery lifecycle which includes considerations for confidentiality, integrity (data and systems) and availability. These extend to all systems that HP | Poly uses – both on-premises and in the cloud as well as to the development, delivery, and support of HP | Poly products, cloud services and managed services.

The foundational principles which serve as the basis of HP | Poly's security practices include:

1. Security is required, not optional
2. Secure by default, Secure by design
3. Defense-in-depth
4. Understand and assess vulnerabilities and threats
5. Security testing and validation
6. Manage, monitor, and maintain security posture
7. End-to-end security: full lifecycle protection

Security Testing

Both static and dynamic vulnerability scanning as well as penetration testing are regularly performed for production releases and against our internal corporate network by both internal and external test teams.

Cloud systems are managed by HP | Poly and are updated as needed. Patches are evaluated and applied in a timely fashion based on perceived risk as indicated by CVSSv3 scores.

Change Management

A formal change management process is followed by all teams at HP | Poly to minimize any impact on the services provided to the customers. All changes implemented for the Poly One Touch Dial Cloud Service go through vigorous quality assurance testing where all functional and security requirements are verified. Once Quality Assurance 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. 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.

Data Processing

HP | Poly does not access any customer's data except as required to enable the features provided by the service. If someone is an individual user and the purchase of the Poly One Touch Dial Cloud Service has been made by their employer as the customer, all the privacy information relating to personal data in this white paper is subject to their employer's privacy policies as controller of such personal data.

Purpose of Processing

The primary purpose of processing information by the Poly 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.

Source of Personal Data	Categories of PI Processed	Business Purpose of Processing	Disclosed to the following Service Providers
Account Information	• Service account email address • Username and password • Customer account ID • Calendar event time zone	• Reading calendar information • Display of calendar to device association • Deliver the service • Internal analysis and reporting • Troubleshooting • Performance analytics	Azure
Device Information	• Device ID • IP address	• Push calendar to video conferencing endpoint • Help customer diagnose technical issues	Azure

Request Caching
A caching layer is utilized by Poly One Touch Dial Cloud Service when retrieving calendar events from Office 365, Exchange, or Google.

This is a transient in-memory cache, and exclusively used for HTTP request caching.

HTTP request caching is considered best-practice for reducing server load on downstream calendaring providers and encouraged or even required by these providers. In addition, this caching layer allows OTD to continue to function in the event of short service disruptions from calendaring providers.

Calendar events will only be cached for short periods following the ETAG standard as specified in [RFC2616] and are automatically removed from the cache on expiration as specified in [RFC 7234]. The cache time is determined by the “Expires” header sent by Microsoft, not by OTD (as explained in RFC 7234).

Data Logging
Poly One Touch Dial Cloud Service utilizes a logging infrastructure for diagnosing problems, providing customer support, and maintaining service health.

Sensitive customer data, calendar events, or credentials are **never** logged.

As an additional precaution, all logging statements are passed through a sanitation function that strips all credentials, calendar events and access tokens from the statement. Access to logs is strictly controlled via Azure Active Directory using a Kibana IdP system as well as IP-whitelisting. Logging statements are purged within 90 days whenever possible. In the event of a service level problem in Azure, we may decide to preserve system level logs for a longer period to assist Microsoft Azure engineers in identifying the root problem. Service level logs are not customer-sensitive. They contain information such as memory usage, CPU utilization, server count and so on.

For customer support and troubleshooting, specific calendar event metadata is logged to assist support engineers with identifying relevant logging:

Customer Account ID
The customer’s OTD account ID.

Customer Account Domain
The domain of the customer’s organization (e.g., example.com).

Event ID
The ID of the event as assigned by the calendar provider. (e.g., O365 uses a random hash as the event ID)

User-Principal-Name (UPN) of Calendar Account
The username of the calendar account in which the event resides (e.g., EXAMPLE\room1account or room1@example.com).

Event Start Date/Time
When the event is scheduled to start.

Event Stop Date/Time
When the event is scheduled to end.

Event Time zone
The time zone in which the event will take place.

Event Reoccurrence
If the event part of a reoccurring series or a single event.

Event Language
The language in which the event is written.

Event Meeting Provider (if applicable)
The meeting provider if OTD finds one (e.g., Zoom, Teams, GoToMeeting)

Device ID
The ID of the device assigned by OTD which the event is being delivered to.

Device Type
The type/make/model of the device which the event is being delivered to.

Performance Analytics

To measure service availability (SLO), perform application performance monitoring (APM), determine future application scaling requirements, and understand customer usage patterns, Poly One Touch Dial Cloud Service collects analytics data.

Most data collected for analytics would be categorized as internal performance data. This includes statistics on run times of specific methods, processes, and HTTP response codes.

To provide insights on how customers use the system to inform future feature prioritization, and calculate system scaling requirements, some data is collected and stored in an ELK stack and access controlled using Azure Active Directory and IP-whitelisting:

Customer ID Hash
A SHA1 hash of the OTD customer ID

Calendar Provider
Aggregate the calendaring providers used by our customers (Office 365, Google, Exchange) to direct new integration features. This is stored as a map of the provider’s name to an event count (e.g., Zoom: 400, etc.)

Event Meeting Provider
Which meeting provider(s) customers are using most often (e.g., Zoom, Teams, etc.) to determine what additional providers should be added to the system.

Event ID
The ID of the event as assigned by the calendar provider. (e.g., O365 uses a random hash as the event ID)

Event Start and Stop Date/Time
Helps calculate upcoming scalability requirements of the system by compiling aggregation counts of upcoming events the system will need to handle.

Event Reoccurrence
Also used to calculate scalability requirements.

Event Language
The language in which the event is written to help improve OTD parsing engine.

Event Attendee Count
The number of participants for an event (how many accepted/declined)

Event Importance
The priority assigned to an event.

Device Type
Informs which types of devices are being connected to OTD to focus defect triage.

Similar to the way access to logging data is secured, access to analytics is strictly controlled via Azure Active Directory using a Kibana IdP system as well as IP-whitelisting.

How Customer Data is Stored and Protected

The Poly One Touch Dial Cloud Service stores customer data in Azure Cosmos DB. 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 here.

The OTD service database server is in an SSAE 16 Type II certified data center in the United States, the Netherlands or Australia that runs dedicated databases and application servers. When the OTD service database server receives data from the customer, it is verified for integrity, processed, and saved in the database.

HP | Poly may change the location of the OTD service database server and details of any such change shall be set forth in the latest copy of this white paper available on HP | Poly's website.

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

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

Data Deletion and Retention

All information collected from the customer is stored in the database with the tenant information configured as the access control mechanism. Nothing is transmitted outside of the Poly One Touch Dial Cloud Service. All data is self-contained in the database in the data center.

HP | Poly may retain customer data for as long as needed to provide the customer with any HP | Poly cloud services for which they have subscribed and for product improvement purposes. When a customer makes a request for deletion to HP's Chief Privacy and Data Protection Officer form, HP | Poly will delete the requested data within 30 days, unless the data is required to be retained to provide the service to customer. HP | Poly may "anonymize" personal data in lieu of deletion. In cases where anonymization occurs, the 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.

Secure Deployment

The Poly One Touch Dial Cloud Service supports two deployment topologies. In support of HP | Poly endpoints, Exchange Web Services is used to provide the calendar to the endpoint. For third-party endpoints, the Poly 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 Poly 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 AMPQ message bus. Subsequent delivery of calendar events from Poly Cloud Relay to the endpoint is over the customer's internal network.

The OTD 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 are encrypted using TLS.

All traffic transported between the OTD service and Microsoft O365, Microsoft Exchange on-premises, and Google as calendar providers is always encrypted.

Server Access and Data Security

All customer data sent to HP | Poly is encrypted both at rest and in transit using strong cryptography including AES-256 and TLS up to v1.2.

All customer data sent to HP | Poly is backed up daily in digital form using the Azure data factory. 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.

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. For details, see here.

Cryptographic Security

All communication with the Poly One Touch Dial Cloud Service 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 OTD 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.

Access Controls and Permissions

To access calendaring data, customers must integrate Poly One Touch Dial Cloud Service to their calendar system. OTD uses OAuth applications to request the necessary permissions to authenticate users and connect to the calendar. The OTD service will request the minimum set of permissions required for read-only calendar access for the room account.

This prevents OTD from having broad access to calendar accounts across the customer's organization and allows customers to use fine-grained access controls to whitelist specific accounts for OTD.

Poly One Touch Dial Portal

This application is simply used for authentication when accessing the administration portal (https://otd.plcm.vc) for the Poly One Touch Dial (OTD) service.

A Microsoft permissions request will appear when signing into the OTD portal for the first time and must be approved to access the portal.

Required Permissions:

- Sign you in and read your profile
  - Allows you to sign-in to the app with your organizational account and let the app read

your profile. It also allows the app to read basic company information.
- Maintain access to the data you have specified
  - Allows the app to see and update the data you gave it access to, even when you are not currently using the app. This does not give the app any additional permissions.

Note: The “Consent on behalf of your organization” option is not required. It will only be presented when the approving user is also an administrator in the Microsoft 365 tenant, but admin consent is not needed unless other users in the tenant who might also be setup as administrators in the One Touch Dial Portal are not able to approve application requests themselves.

Poly One Touch Dial Service
This application is used by the One Touch Dial Service to access calendar data stored in Exchange Online mailboxes. A user account assigned the Global Admin role in the Microsoft 365 tenant will need to be used to approve this application.

There are two different sets of permissions that this application can request access to which depends on which calendar integration option is selected in the OTD administration portal: either as an Application or with a Service Account. In either approach the application is limited to read access of only the Calendar folder to any mailboxes which it is permitted to access. The scope of which mailboxes can be accessed can be controlled by the Microsoft tenant.

Either option can be used to limit permissions to the same set of defined mailboxes, but via different steps. The Application model is currently recommended as the configuration and management is simpler than the Service Account model. The Application model also supports environments where Exchange Online resource mailboxes are enabled for both accounts which created directly online and accounts which were originally synchronized from an on-premises Active Directory environment.

Note: The Service Account model can only access user mailboxes configured using the same method as the service account was created.

Connect as Application:
With this approach, the app will request read access to calendar data in all mailboxes in the entire organization, but the scope of mailboxes the app is allowed to access can manually be limited by use of a custom mail-enabled security group. When using this approach, it is recommended to define a new Application Access Policy in Exchange Online prior to approving the application request to prevent even a brief period of access to all mailboxes in the organization.

A Microsoft permissions request will appear after selecting the Connect as Application option under the Office 365 Calendar Integration section of the OTD administration portal.

Required Permissions:
- Read calendars in all mailboxes
  - Allows the app to read events of all calendars without a signed-in user.
- Read directory data
  - Allows the app to read data in your organization's directory, such as users, groups, and apps, without a signed-in user.
- Sign-in and read user profile
  - Allows users to sign-in to the app and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.

Connect with Service Account:
This approach will request read access to only the mailboxes that a single user account has access to. That is defined by creating a dedicated service

account in the tenant which is then delegating rights for the desired mailboxes in the tenant. The app will use this service account when connecting to Exchange Online and thus be limited to reading calendar data in only the mailboxes accessible to that account.

A Microsoft permissions request will appear after selecting the Connect with Service Account option under the Office 365 Calendar Integration section of the OTD administration portal and providing the credentials of the desired service account.

Required Permissions:

- Sign you in and read your profile
  - Allows you to sign-in to the app with your organizational account and let the app read your profile. It also allows the app to read basic company information.
- Read your calendars
  - Allows the app to read events in your calendars.
- Read calendars you can access
  - Allows the app to read events in all calendars that you can access, including delegate and shared calendars.
- Maintain access to data you have specified
  - Allows the app to see and update the data you gave it access to, even when you are not currently using the app. This does not give the app any additional permissions.

If the admin wishes to further restrict what mailboxes OTD can access, an additional PowerShell command can be executed as outlined here: https://otd.plcm.vc/support/docs/calendars/office365-connect-as-application

The following scopes are requested by OTD for each calendar provider:

Microsoft Office 365:

- https://graph.microsoft.com/user.read
- https://graph.microsoft.com/calendars.read
- https://graph.microsoft.com/calendars.read.shared

Microsoft Exchange:

An exchange service account is configured by the customer with read-only access to select calendars. OTD provides documentation on how a service account can be configured with minimal access.

Google:

- https://www.googleapis.com/auth/userinfo.profile
- https://www.googleapis.com/auth/calendar.readonly

Authentication

The Poly One Touch Dial Cloud Service supports integration of enterprise authentication providers via the OAuth2 standard.

With OAuth2, the OTD 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. OTD 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
- 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

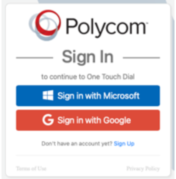
Credential Storage

There are some types of authentication data stored in the Poly One Touch Dial Cloud Service. This is required to enable ongoing access to calendaring data and authentication to customer devices. Data is stored in a Microsoft Azure Cosmos DB and is encrypted at rest using AES-256.

There are 3 distinct areas of authentication and authorization managed in OTD:

OTD User Account Credentials:

An OTD customer is given a user account. This account is required to sign in to the OTD interface, configure devices and integrate with calendaring providers.


Polycom

Sign In

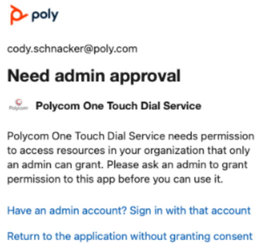
to continue to One Touch Dial

Authentication to OTD user accounts is handled by using SSO through Microsoft Office 365 or Google Suite. Therefore, OTD does **not** store user credentials for accounts.

Calendar Integration Credentials:

OTD must have ongoing access to customer calendaring accounts to consistently deliver events to devices.

When integrating to an Office 365 or Google calendar account, OTD utilizes an OAuth2 flow with the calendaring provider.


poly

cody.schnacker@poly.com

Need admin approval

Polycom One Touch Dial Service

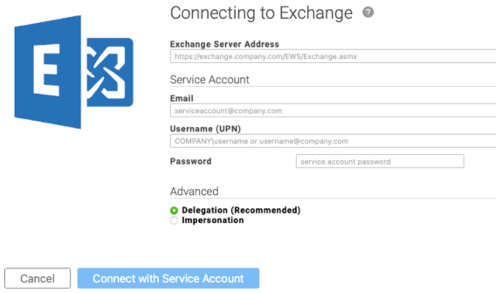
Polycom One Touch Dial Service needs permission to access resources in your organization that only an admin can grant. Please ask an admin to grant permission to this app before you can use it.

Have an admin account? Sign in with that account
Return to the application without granting consent

A user completes this grant flow using the provider's OAuth2 consent flow. If granted, the provider offers OTD a refresh token which can be used to obtain access to the calendaring data.

OTD does **not** store customer calendaring credentials for Office 365 or Google calendar integrations. OTD is only required to store the refresh token offered by the provider.

Exchange calendar accounts **do** require OTD to store credentials for ongoing service account access.


Connecting to Exchange

Exchange Server Address: https://exchange.company.com/EWS/Exchange.asmx

Service Account

Email: serviceaccount@company.com

Username (UPN): COMPANY\username or username@company.com

Password: service account password

Advanced

● Delegation (Recommended)
○ Impersonation

The Exchange server address, service account email, username and password are stored in OTD, encrypted at rest in Azure CosmosDB. The Exchange password is salted and encrypted using AES 256 GCM with the decryption key stored separately in an Azure Key Vault.

Device Authorization:

OTD must verify devices receiving calendar events are owned by the customer. To accomplish this, all interactions between the device and OTD must be authenticated.

When configuring devices, OTD will generate random credentials for each device which the customer will copy onto the device. This alleviates security concerns around password strength.

If the customer opts to use their own device credentials instead of the generated credentials OTD provides, they will be stored and encrypted using AES-256 GCM with the decryption key stored separately in an Azure Key Vault.

Disaster Recovery and Business Continuity

The Poly One Touch Dial Cloud Service is architected to provide high reliability, resiliency, and security. The service is hosted in multiple Microsoft Azure data centers in the United States. 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.

HP | Poly has a Business Continuity and Disaster Recovery Plan reviewed and approved by management to ensure that we are appropriately prepared to respond to an unexpected disaster event. HP | Poly tests disaster recovery processes and procedures on an annual basis but are sometimes conducted more frequently when there are changes to our infrastructure that warrant new tests. We use the results of this testing process to evaluate our preparedness for disasters, and to validate the completeness and accuracy of our policies and procedures.

Security Incident Response

The HP Cybersecurity team promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. You may contact them directly at informationsecurity@hp.com

The HP Cybersecurity team works proactively with customers, independent security researchers, consultants, industry organizations, and other suppliers to identify possible security issues with HP | Poly products and networks. HP | Poly security advisories and bulletins can be found on the HP Customer Support website

Subprocessors

HP | Poly uses certain subprocessors to assist in providing our products and services. A subprocessor is a third-party data processor who, on behalf of HP | Poly, processes customer data. Prior to engaging a subprocessor, HP | Poly executes an agreement with the subprocessor that is in accordance with applicable data protection laws.

The subprocessor list here identifies HP | Poly's authorized subprocessors and includes their name, purpose, location, and website. For questions, please contact HP's Chief Privacy and Data Protection Officer form.

Prior to engagement, suppliers that may process data on behalf of HP | Poly must undergo a privacy and security assessment. The assessment process is designed to identify deficiencies in privacy practices or security gaps and make recommendations for reduction of risk. Suppliers that cannot meet the security requirements are disqualified.

Additional Resources

To learn more about Poly One Touch Dial Cloud Service, visit our product website.

Disclaimer

This white paper is provided for informational purposes only and does not convey any legal rights to any intellectual property in any HP | Poly product. You may copy and use this paper for your internal reference purposes only. HP | 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 HP | POLY FROM TIME TO TIME. To review the most current version of this white paper, please visit our website.