SECURITY AND PRIVACY WHITE PAPER

Poly RealConnect

Part 3725-85375-001

Version 12

March 2024

Introduction

This white paper addresses security and privacy-related information regarding Poly RealConnect for Office 365 and Teams.

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 Poly RealConnect 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.

Poly RealConnect for Office 365 is a certified video interoperability solution for Office 365 and Skype for Business. Poly 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 Poly RealConnect Service is integrated into the Skype and Teams meeting workflow making it easy and intuitive to schedule a video interop call.

Security at HP | Poly

Security is always a critical consideration for a cloud-based service such as Poly RealConnect. 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 process. 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 & 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 RealConnect 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. The video stream is transcoded by HP | Poly in the HP | Poly cloud before it is passed to Teams. HP | Poly has no access to the video stream, and it is not used for any other purpose.

If you are an individual user and the purchase of Poly RealConnect has been made by your employer as the customer, all 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.

Poly RealConnect for Teams receives details from Microsoft about your online meeting when you join that meeting using our service, including, but not limited to, meeting subject, meeting scheduled time, meeting organizer, and meeting participants. HP | Poly only uses the returned meeting's URI so as to join the meeting, and ignores the rest, but this information is still logged and remains in our system (in an encoded format that is non-human-readable) for a period of 30 days. In addition to the online meeting details, HP | Poly receives real-time updates from Microsoft about Teams participants for the joined meeting, which includes participant names. Participant names are only used by HP | Poly to be displayed on-screen as part of the normal meeting experience but are also logged and remain in our system for a period of 30 days. For the sole purpose of troubleshooting customer issues, HP | Poly also exchanges unique but potentially correlatable identifiers with Microsoft. Some troubleshooting identifiers may be logged for longer than 30 days.

For details related to how Poly One Touch Dial processes customer data (including calendar/meeting details), please see the *Security and Privacy White Paper for Poly One Touch Dial* here.

NOTE: No RTP media is ever captured without a direct customer request. If requested, the media is only manually captured on a per-call basis and in a separate dedicated deployment used only for diagnostic purposes.

Source of Personal Data	Categories of PI Processed	Business Purpose for Processing	Disclosed to the following Service Providers
Service user information	• Display name • Email address • Edge network IP address (e.g., router, Session Border Controller, gatekeeper, or SIP Proxy) • Video stream	• Authenticate and authorize administrative access to the service • Deliver the service • Internal analysis and reporting • Licensing • Transcoding (video stream is not otherwise processed)	Azure
Device Identifier Information	• Device name • IP address (e.g., router, Session Border Controller, gatekeeper, or SIP Proxy)	• Help customer diagnose technical issues • IP addresses are used to connect video endpoints to the Skype for Business or Teams service	Azure
Calendar and meeting information	• Meeting subject • Meeting scheduled time • Meeting organizer • Meeting participant name • Microsoft unique identifiers	• Joining meetings • On-screen name display • Troubleshooting customer issues	Azure

Purpose of Processing

Poly 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 correctly. Some data elements are additionally used to perform internal analysis and reporting.

How Customer Data is Stored and Protected

Poly RealConnect for Office 365 and Teams stores customer data in Azure CosmosDB. Data is encrypted at rest using AES 256.

To learn about how encryption is applied, please visit the following link here.

The Poly RealConnect database server is in an SSAE 16 Type II certified data center that runs dedicated databases and application servers. When the Poly RealConnect database server receives data from the customer, it is verified for integrity, processed, and saved in the database.

We route calls to the nearest Azure data center based on ping latency. So generally, if the customer is US-based, their calls will land in US data centers. If a call were routed outside the US due to data center outage or capacity problem, call data may temporarily reside in the Netherlands or Australia for 30 days. Long-term storage of call information is US-based. The license data that HP | Poly holds (PII is the email contact who ordered the license) will be held in the US and the Netherlands. We also persist RealConnect call information records and service metrics in the Azure datacenter in the Central US.

We leverage the following Azure data centers:

- South Central US
- East US 2
- Central US 2
- West US 2
- Northern Europe (Ireland)
- Western Europe (The Netherlands)
- Germany West Central
- Australia Southeast

HP | Poly may change the location of the Poly RealConnect 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 Poly RealConnect 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 Poly RealConnect is blocked.

Data Portability

Call detail record data can be exported from the report portal in either .CSV or JSON formats.

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 Poly RealConnect. 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.

Cryptographic Security

All communication with the Poly RealConnect for Office 365 and Teams web portal (webapp.plcm.vc) is encrypted over an HTTPS connection that uses TLS 1.2 with 128 or 256-bit encryption (based on the user's web browser configuration settings) and a 2048-bit key exchange mechanism. Cryptographic cipher suites and modules implemented in Poly RealConnect 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.

Poly 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 Poly RealConnect for Office 365 and Teams 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 Poly RealConnect and Microsoft is always encrypted.

Key Management

HP | Poly leverages the Azure key vault for key management (https://azure.microsoft.com/en-us/services/key-vault/) which is FIPS 140-2 Level 1 compliant. Keys are protected in transit using TLS 1.2 encryption. Access is controlled by AD User Principals (human) or Service Principals (applications) with individualized permissions granted based upon the principal of least privilege. The Application Service Principal has key usage privileges only. The HP | Poly DevOps team has key management privileges.

For Real-time Transport Protocol (RTP) media encryption, keys are generated on a per-call basis and are not retained. Encryption keys for data at rest are managed by the platform and are rotated per Microsoft internal guidelines.

NOTE: Endpoint call encryption for the service must be managed by the customer.

Password Management

No customer passwords are stored in RealConnect. RealConnect uses OAuth2 exclusively with Microsoft. Single Sign On (SSO) usage is controlled by the Customer's AD.

Access Controls

All access is remote, and all accounts are OAuth2 based. Shared accounts are not allowed. There are no local accounts that can be administered by the end user outside of O365/Graph API consent. All customer access can be restricted to the customer's enterprise directory. If using SSO integration, this will be controlled by the customer's Active Directory. The local users are manually managed by the customer's administrator.

Access is narrowed by only allowing RealConnect administrators or the support team based on the principles of need to know and least privilege. All access control changes for RealConnect administrators (i.e., HP | Poly staff) are configured in compliance with HP | Poly access control policies and procedures. RealConnect administrators (HP | Poly staff) are authenticated through the HP | Poly Active Directory with strong passwords enforced via VPN and in conjunction with an authenticator for MFA.

Authentication

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

With OAuth2, Poly 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. Poly RealConnect 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

Administration and Reporting

For administrative access to HP | Poly portals for RealConnect, HP | Poly uses Microsoft OAuth2 Graph API consent to authenticate admin users from the customer's Office 365 tenants for access to configuration and licensing.

A reporting portal allows administrators to view concurrent utilization and other factors such as summarized or detailed call reports. Reporting dashboards are available at https://rc-reports.plcm.vc

Security Monitoring and Logging

HP | Poly actively monitors the overall RealConnect service using automated and manual methods but does not actively monitor the service on a call-by-call basis unless a support case has been created with HP | Poly to troubleshoot specific issues. The RealConnect service leverages Azure Security Center with Windows Defender to monitor our internal components. It is possible to subscribe to service updates and incident alerts delivered by email from the service status webpage.

Our service logs and auditing are not available to our customers. However, customers are provided call info records as part of the reporting portal. UI access to the RealConnect enrollment portal https://webapp.plcm.vc uses Microsoft OAuth2 application flows which can be audited via Azure Active Directory (AAD) enterprise application logging which is typically available to customer's SIEM.

API

HP | Poly uses the Microsoft Graph API. In order to access Microsoft APIs for Teams meetings to enable standards-based SIP and H.323 calls to participate in Teams video conferences, administrators must consent to the terms and conditions for the "Poly RealConnect for Microsoft Teams" Azure Active Directory (AAD) Application. The following APIs are used:

- ***Access media streams in a call as an app***
  Allows the app to get direct access to media streams in a call, without a signed-in user.
- ***Join group calls and meetings as an app***
  Allows the app to join group calls and scheduled meetings in your organization, without a signed-in user. The app will be joined with the privileges of a directory user to meetings in your organization.
- ***Read online meeting details***
  Allows the app to read online meeting details in your organization, 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.

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.

Disaster Recovery and Business Continuity

The Poly RealConnect service is architected to provide high reliability, resiliency, and security. The entire service is hosted on multiple geographically distributed Microsoft Azure data centers in the United States, Europe, or Australia. 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. 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 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 RealConnect, 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.