Poly RealAccess™ Analytics
Introduction
This white paper addresses security and privacy related information regarding Poly RealAccess™ Analytics.

This paper also describes the security features and access controls in 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 RealAccess product, and the location and transfers of personal and other customer data. Poly will use such data in a manner consistent with the Poly Privacy Policy, and this white paper which may be updated from time to time. This white paper is supplemental to the Poly Privacy Policy. The most current version of this white paper will be available on Poly’s website.

Overview
Poly RealAccess provides a subscribing customer access to a dedicated web portal, which includes a broad range of on-demand monitoring and management of video conferencing services, along with in-depth reporting capabilities. Reports are based on data (including certain personal data of customer as described below) collected from a customer’s Poly RealPresence Platform and automatically uploaded to the cloud-based RealAccess portal using a data extraction agent installed on the customer’s premises.

Security at Poly
Security is always a critical consideration for all Poly products and services. 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 Poly has established and implemented best-practice information security processes.


Secure Software Development Life Cycle
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 initial design. Architecture reviews, code reviews, internal penetration testing and attack surface analysis are performed to verify the implementation.

The S-SDLC implemented by Poly also includes a significant emphasis on risk analysis and vulnerability management. To increase the security posture of 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
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, Poly considers the right to data protection with due regard.

**Security by Design**
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 Poly uses – both on-premises and in the cloud as well as to the development, delivery and support of Poly products, cloud services and managed services.

The foundational principles which serve as the basis of 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. 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 Poly to minimize any impact on the services provided to the customers. All changes implemented for the Poly RealAccess product 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**
Poly does not access any customer’s data except as required to enable the features provided by the service.

The RealAccess product collects and processes logs containing:
- Device data (includes information like type of device, device name and installed software version)
- Call and conference data (includes call connection information like IP addresses or phone numbers and some other caller personal data like user ID, or caller name).

If you are an individual user and the purchase of RealAccess 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 RealAccess service is to:
- Enable asset management – View your devices and manage importance information like software versions of device data.
- Perform data analytics – Better understand utilization, capacity, and performance.

Personal data is processed for display and reporting purposes only.
<table>
<thead>
<tr>
<th>Source of Personal Data</th>
<th>Categories of PI Processed</th>
<th>Business Purpose for Processing</th>
<th>Disclosed to the following Service Providers</th>
</tr>
</thead>
</table>
| Administrative user and customer operator profiles | • Name  
• Email address  
• Password (hashed)  
• Organization name  
• SIP URI  
• System name  
• System owner  
• Domain name  
• IP address  
• MAC address  
• Gatekeeper address  
• E164 address  
• H323 ID | • Authenticate and authorize administrative access to the service  
• Deliver the service  
• Reporting  
• Usage/activity | Azure |
| Call participant personal data | • Name  
• Email address  
• Phone number  
• Organization name  
• Display name  
• SIP URI  
• IP address  
• Dial string | • 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 | Azure |
| Device information | • Device name  
• IP address  
• Geolocation  
• MAC address  
• Time zone  
• Serial number | • Diagnose technical issues  
• Respond to customer support requests  
• Serial number for entitlement | Azure |
| Usage information | • Activity logs  
• Call detail records | • Understand how the service is used  
• Diagnose technical issues  
• Capacity forecasts  
• Keep track of KPIs | Azure |
How Customer Data is Stored and Protected
The RealAccess database server is in a SSAE 16 Type II certified data center in the United States that runs dedicated databases and application servers. When the RealAccess database server receives data from the customer, it is verified for integrity, processed, and saved in the database.

Poly may change the location of the RealAccess database server and details of any such change shall be set forth in the latest copy of this white paper available on Poly’s website.

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

Data Portability
RealAccess customer admins and users who have access to the portal can download all customer data from the RealAccess portal.

Data Deletion and Retention
All information collected from the customer is stored in the multi-tenant database with email domain information configured as the access control mechanism. Nothing is transmitted outside of RealAccess. All data is self-contained in the database in the data center.

Poly may retain customer data for as long as needed to provide the customer with any Poly cloud services for which they have subscribed and for product improvement purposes. When a customer makes a request for deletion to privacy@poly.com, Poly will delete the requested data within 30 days, unless the data is required to be retained to provide the service to customer. 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.

RealAccess Software Agent
The agent is an instance operation as a virtual machine. The agent’s Operating System (OS) has been hardened with the latest security patches, best practices for software configurations, and the removal of unnecessary services. Additionally, the OS security has been verified using several industry-leading security and vulnerability scan tools, as well as manual testing.

The agent may reside in the customer’s DMZ if required, with access to the cloud and the RealPresence Platform component(s) on the customer’s RealPresence video network.

There is a service on the agent that uses device-specific credentials to make API calls on specific ports to access data from sources such as call servers (Polycom RealPresence Distributed Media Application™ (DMA)), and scheduling and provisioning servers (Polycom RealPresence Resource Manager). While accessing these devices, all credentials are encrypted via HTTPS tunnel using TLS with 256-bit encryption.

The agent does not store data collected from the RealPresence Platform in any shape or form (cache or storage) in the agent.

The next step in the data delivery process is to transport and deposit customer data to the RealAccess data store, located in an SSAE 16 Type II certified data center in California. All communication between the RealAccess agent and data store is via an OpenVPN tunnel. Any attempt to monitor the link between the agent and data center servers will only show encrypted packets instead of cleartext.
SECURITY AND PRIVACY WHITE PAPER FOR POLY REALACCESS ANALYTICS

information.

All maintenance activities, OS patching, code updates, and NTP time synchronization for the agent are handled via this OpenVPN tunnel from the data center. All OS patches, updates or other necessary hot fixes will be performed on a regular basis as needed.

Secure Deployment
The RealAccess agent gathers data from various RealPresence Platform sources and transports it to the RealAccess data store. The following information and architecture diagram provide an overview of the secure deployment configuration:

- Secure and bi-directional tunnel
  - Open VPN/SSL
  - All packets are encrypted
  - The tunnel is encrypted
- RealAccess software agent
  - Deployed on virtual server (in your environment)
- Supported virtual machine formats
  - VMware
  - KVM
  - Xen
  - HyperV

User Authentication
User authentication for RealAccess can be performed in two ways. The simplest is to use the authorized customer domain. Members of the domain can use their email address to register at the self-sign-in portal. The system will send a verification email to the email address provided for the user to authenticate and choose a password.

The alternative is to use the RealAccess portal authentication service, which supports Active Directory Federation Services (ADFS). Please see the diagram below. With this method, the portal is configured for single sign-on (SSO) and integrated with the customer’s active directory via SAML. The user will use their enterprise network credentials to log in to the portal.

With the ADFS method, the user first logs in to the portal with their enterprise network credential. The request is forwarded on a secure https connection that uses TLS1.2 with 256-bit encryption to the customer federation services, which look up to the user. The response is then passed to the portal with an allow/deny message.
Cryptographic Security
All communication with the RealAccess portal web servers and client browsers is over a standard secure SSL connection that encrypts all requests and responses. This is achieved with an HTTPS connection that uses TLS1.2 with a 256-bit encryption layer using SSL using certificates. This connection is encrypted and authentication using AES_128GCM with ECDH as the key exchange mechanism.

Transport Layer Security (TLS) between components of the Polycom RealAccess is mutual for all connections. Protocol version 1.2 (TLS1.2) is preferred for connections, and versions prior to TLS 1.1 are disabled. TLS compression and client-initiated renegotiation also are disabled. When implemented, secure server renegotiation is compliant with RFC 5746. The data is encrypted as it is written to the database where it remains encrypted at rest stored in the database.

Cryptographic cipher suites and modules implemented in the Polycom Cloud Service are open (i.e. publicly disclosed) and have been peer reviewed. Cryptographic libraries are current, regularly updated, and leverage the Advance Encryption Standard (AES-128 and AES-256) cipher suites. Hash strengths supported include SHA-256, SHA-384 and SHA-512.

Poly requirements for cryptographic ciphers include:
- Greater than or equal to 128-bit keys for symmetric ciphers.
- Greater than or equal to 2048-bit keys for asymmetric ciphers and Diffie-Hellman key exchange algorithms.
- Greater than or equal to 256-bit curves for Elliptic Curve Cryptographic (ECC).

Server Access and Data Security
The RealAccess database and application servers reside in a secure data center behind a fully patched firewall that is also managed. Access for any services not required by RealAccess is blocked. Only authorized staff members have access based on the principles of least privilege and need to know. The servers are not directly accessible from outside the data center.

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

All 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.

Disaster Recovery and Business Continuity
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. 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.

Backups are automated, encrypted and securely stored. Services are architected for High Availability (HA). The failover Azure data center depends on the type of disaster.

Security Incident Response
The Poly Security Office (PSO) promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. You may contact the PSO directly at informationsecurity@poly.com
The PSO team works proactively with customers, independent security researchers, consultants, industry organizations and other suppliers to identify possible security issues with Poly products and networks. Poly security advisories and bulletins can be found on the Poly Security Center.

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

The subprocessor list here identifies Poly’s authorized subprocessors and includes their name, purpose, location and website. For questions, please contact privacy@poly.com.

Prior to engagement, suppliers that may process data on behalf of 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 RealAccess™ Analytics, 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 Poly product. You may copy and use this paper for your internal reference purposes only. 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 POLY FROM TIME TO TIME. To review the most current version of this white paper, please visit our website.