SECURITY AND PRIVACY WHITE PAPER

Polycom RealAccess™ Analytics

Part 3725-85367-001

Version 1.3

September 2018

INTRODUCTION

This white paper addresses security and privacy related information for Polycom RealAccess™ Analytics. It 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 Polycom RealAccess product, and the location and transfers of personal and other customer data. Poly uses such data in a manner consistent with the Poly Privacy Policy and this white paper (as 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

Polycom 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 Polycom 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 any product. Poly aligns with ISO/IEC 27001:2013 practices 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 Poly has established and implemented best-practice information security processes. ISO/IEC 27001:2013 not only reinforces our commitment to information security best practices and controls, but it explicitly includes the product development process.

Product security at Poly is managed through the Poly Security Office (PSO), which oversees secure software development standards and guidelines. The 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 industry-approved methods for adhering to the Poly Product Security Standards.

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. Additional testing, in the form of standards-based Static Application Security Testing and patch management, is a cornerstone 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 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, Poly considers the right to data protection with due regard to making sure that data controllers and processors can fulfill their data protection obligations.

REALACCESS SOFTWARE AGENT

The agent is an instance operation as a virtual machine. The agents Operating System (OS) has been hardened with the latest security patches, best practices for software configurations, and he 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 stored data collected from the RealPresence Platform in any shape or form (cache or storage) in the agent.

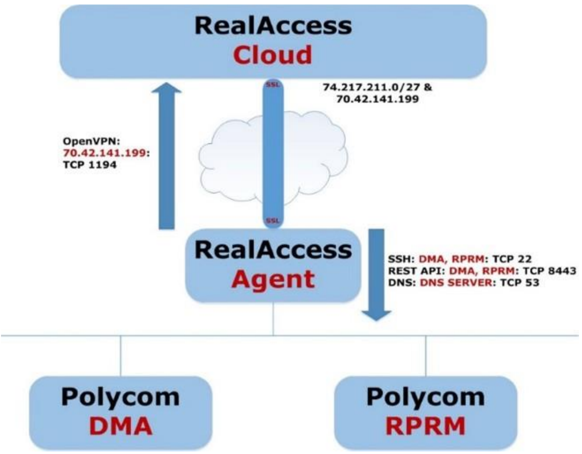
The next step in the data delivery process is to transport and deposit customer data to the RealAccess data store, located in an SSAE 16 Type II certified data center in California. All communication between the RealAccess agent and data store is via an OpenVPN tunnel. Any attempt to monitor the link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

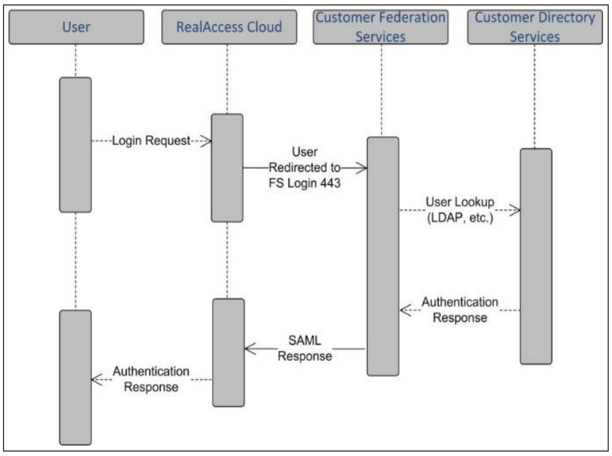


USER AUTHENTICATION:

User authentication for RealAccess can be performed in two ways. The simplest is to use the authorized customer domain. Members of the domain can user 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 authentication 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.

RealAccess SSO message flow



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.

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).

DISASTER RECOVERY AND BUSINESS CONTINUITY

There is a disaster recovery strategy in place and policy in effect. Business recovery and contingency plans are reviewed and tested on an annual basis but are sometimes conducted more frequently when there are changes to our infrastructure that warrant new tests.

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

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.

SERVER ACCESS AND DATA SECURITY

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.

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.

Personal Data Category	Type of Personal Data	Purpose of Processing
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
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 • Serial number for entitlement • Capacity forecasts • Keep track of KPIs
Device information	• Device name • IP address • Geolocation • MAC address • Time zone • Serial number	
Usage information	• Activity logs • Call detail records	

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.

For a detailed listing of the specific data elements processed, please contact your Poly representative to request the companion non-public white paper for this product.

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.

The RealAccess 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 RealAccess is blocked.

DATA PORTABILITY

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

THIRD-PARTY PROVIDERS (SUB-PROCESSORS)

Poly 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 Poly Privacy Policy.

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 the RealAccess service. After a customer's subscription terminates or expires, Poly will delete personal data within one year of termination or expiration of the service. When a customer makes a request for deletion (privacy@poly.com), Poly will delete the requested data 30 days, unless the data is required to be retained for Poly's legitimate interests or if needed to provide the service to customer. Poly 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, and IP address) with randomly generated alphanumeric characters.

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 to Polycom RealConnect for Office 365 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 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.

SECURITY INCIDENT RESPONSE

The Poly Security Office (PSO) promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. You can 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 at the Poly Security Center.

ADDITIONAL RESOURCES

To learn more about Polycom RealAccess Analytics, please visit our 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.