WHITE PAPER

Polycom® Cloud Service Security White Paper

Introduction

The Polycom® Cloud Service solution lets customers quickly, easily, and securely share documents in meetings from their existing cloud storage service, such as Microsoft Office 365, via the Polycom® Pano™ room device and Polycom® Pano™ App.

Security is a critical consideration in the deployment of any network-connected device, and even more so for enterprise integration with a cloud-hosted service. The Polycom Cloud Service and Polycom Pano have emphasized solution security at every stage, from conception to delivery. Polycom places the highest priority on securely operating the service in the Microsoft Azure public cloud to provide customers with a secure collaboration environment. This white paper is intended to inform customers how data is secured for this solution and offer some recommendations for secure deployment.

Secure software development life cycle

The threat landscape for software products continues to dramatically change. Polycom has responded by adopting a Secure Software Development Life Cycle (S-SDLC), incorporating an emphasis on security throughout our product development processes. Every phase of Polycom Cloud Service development has stressed security—from initial design requirements and scoping through architecture reviews, the development of product features, to internal penetration testing and attack surface analysis.

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 continuous commitment to information security practices and controls, it explicitly includes the product development process. In addition, this certification is an important foundation for adopting other security standards and frameworks as we go to market with existing and new solutions.

Product security at Polycom is managed through the Polycom Security Office (PSO), which oversees secure software development standards and guidelines. The *Polycom Product Security Standards* are derived from NIST Special Publication 800-53 and ISO/IEC 27001:2013.

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. Existing industry standards and practices around cloud security have also been incorporated into cloud requirements, including the Cloud Security Alliance's Cloud Controls Matrix (CCM v3.01) and Consensus Assessments Initiative Questionnaire (CAIQ v3.01).

The S-SDLC implemented by Polycom also includes a significant emphasis on risk analysis and testing, using external guidelines such as the Open Web Application Security Project (OWASP) Top 10. We have analyzed the overall attack surface of the Polycom Cloud Service and Polycom Pano and systematically incorporated layered defenses, the principle of least privilege, and whenever possible, disabled or restricted access to system services nonessential to standard operation. Additional testing, in the form of standards-based Static Application Security Testing and internal penetration testing, is also a cornerstone of our S-SDLC.

Cryptographic security

Cryptography is one of the first and most visible considerations when it comes to system and network security. Secure cryptographic protocols, cipher suites, and implementations are core requirements in today's threat landscape, and Polycom has placed a strong emphasis on cryptographic security.

The Polycom Cloud Service provides encryption of all data moving in and out of the cloud. Content arrives at our cloud servers encrypted—files, annotations, and room names are encrypted from the Polycom Pano and Polycom Pano App before sending them to the cloud. Likewise, all information sent from the cloud (document filenames, rendered cloud document image data, room names, user names, etc.) is encrypted before being sent to the Polycom Pano and Polycom Pano App. Azure Storage Service Encryption is leveraged to provide an additional layer of protection for data at rest in the cloud.

We use HTTP Secure (HTTPS) to encrypt data in transit between Polycom Pano systems and our servers. Although the Polycom Pano responds to HTTP requests on port 80, the web server on this port is simply a convenience that redirects all activity to an encrypted connection over port 443.

Transport Layer Security (TLS) between components of the Polycom Cloud Service is mutual for all connections. Protocol version 1.2 (TLS 1.2) is preferred for connections, and versions prior to TLS 1.1 are disabled. TLS compression and client-initiated renegotiation also are disabled. Where 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 Advanced Encryption Standard (AES-128 and AES-256) cipher suites.

Polycom requirements for cryptographic ciphers include:

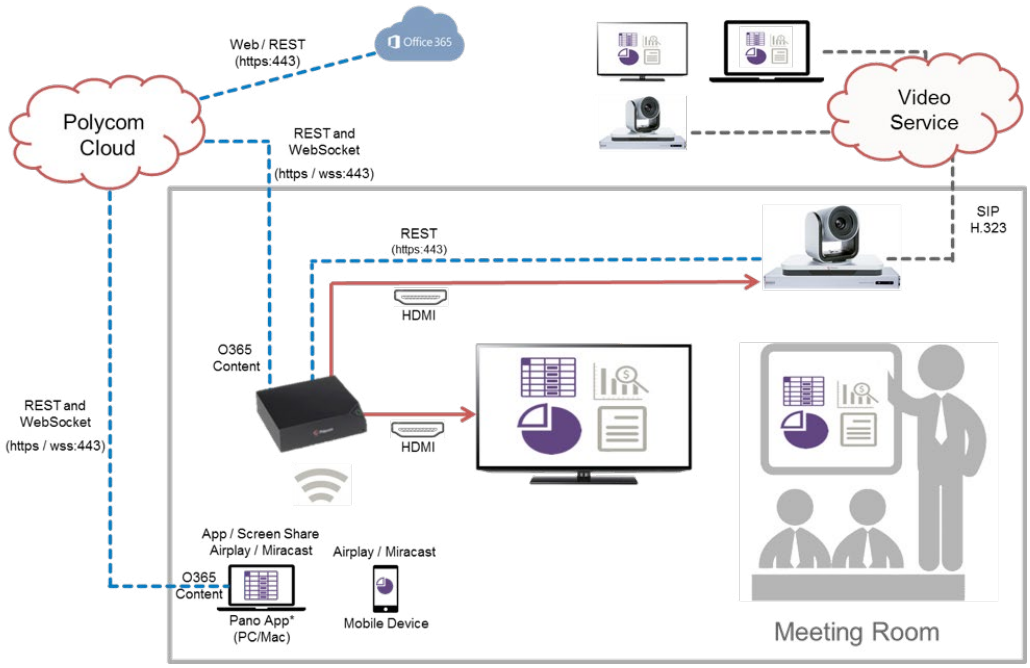
- Greater than or equal to 128-bit keys for symmetric ciphers.
- Greater than or equal to 2048-bit keys for asymmetric ciphers and Diffie-Hellman key exchange algorithms.
- Greater than or equal to 256-bit curves for Elliptic Curve Cryptography (ECC).

All Polycom software executable images and install packages/bundles are digitally signed using only an approved Extended Validation (EV) Class 3 certificate issued by a trusted public Certificate Authority (CA). This assures customers that they are using only authentic Polycom software.

Authentication

The Polycom Cloud Service solution integrates enterprise authentication providers and document storage services via the OAuth 2.0 standard, which is the authentication standard behind the ubiquitous “Sign In with Facebook” or “Sign In with Google” options found across the web.

Using OAuth 2.0, the Polycom Cloud Service securely integrates with enterprise authentication providers so that users are authenticated without having to re-enter their credentials (users enter their credentials only on the authentication provider’s sign-in page). The Polycom Cloud Service receives access tokens from the authentication provider that grant limited and controlled access to resources.



Single sign-on (SSO) authentication within the Polycom Cloud Service environment:

- Access tokens are not stored by the cloud service—they are discarded after basic user profile information (e.g., user email address, user display name) is obtained.
- Access tokens have limited lifetimes that are controlled by the authentication provider.
- Tokens are cached in the cloud service until the user signs out of it (tokens are refreshed as needed during this time) and are not sent to the Polycom Pano App application or distributed anywhere outside the cloud service.
- Users can enable access to their cloud storage service within the Polycom Pano App. If a user does this, the Polycom Cloud Service (via OAuth 2.0) enables browsing of the user’s documents when they sign in to the cloud service.
- Access is granted by access tokens that have limited lifetimes that are controlled by the cloud storage service’s authorization provider; not the Polycom Cloud Service.
- The Polycom Cloud Service supports the following authentication providers:
  - Microsoft Active Directory Federation Services (AD FS) 3.0 via OAuth 2.0
  - Microsoft Office 365 (Azure AD) via OAuth 2.0

- The Polycom Cloud Service supports the following cloud storage service integrations:
  - Microsoft OneDrive for Business (Azure AD via OAuth2)

Secure web access

Polycom Pano connects to the cloud via standard HTTPS connections that are mutually authenticated by the Polycom Pano system and Polycom Cloud Service:

- Polycom Pano systems are shipped with a Polycom device identity certificate issued by a trusted internal Polycom CA. This certificate uses RSA 2048-bit keys and is authenticated by the Polycom Cloud Service before a connection is accepted.
- Similarly, the Polycom Cloud Service uses a service identity certificate issued by a trusted public CA. This certificate is authenticated by the Polycom Pano system before completing a connection to the cloud service.

Polycom Pano App uses only standard HTTPS connections to communicate with the Polycom Cloud Service. Signing in is done only via the integrated enterprise authentication provider(s), and OAuth 2.0 accomplishes this without ever exposing the user credentials to either the Pano App or Polycom Cloud Service.

Administrative access to individual Polycom Pano devices is provided through a web interface, while all devices in a customer organization can be accessed through the Polycom Cloud Service Administration Portal. Passwords for these administrator accounts can be changed. Once their tasks are complete, administrators can explicitly sign out of the interface (sessions eventually time out due to inactivity).

Web application security is provided throughout the solution with the implementation of Strict Transport Security. All cookies are flagged as secure with maximal restrictions, which also apply to cross-origin resource sharing (CORS). Additional standard headers and methods are implemented and tested to defend against cross-site request forgery (CSRF) and cross-site scripting (XSS).

Content sharing

With the Polycom Pano App, users can share a document from their cloud storage service folder to a Polycom Pano system. This does NOT involve the transmission of the document itself to the Polycom Pano system or Polycom Pano App. The document is opened in the cloud and only rendered on the Polycom Pano system.

Depending on the document type, the rendering is performed either natively within the cloud storage service (never leaving the user's document folder), or is copied temporarily into the Polycom Cloud Service and rendered there (for document types that cannot be rendered directly by the cloud storage service). In either case, all artifacts of the document shared within the cloud service are destroyed at the end of the sharing session.

- Document types rendered natively by OneDrive for Business:
  - Microsoft Word (including Rich Text Format)
  - Microsoft Excel
  - Microsoft PowerPoint
  - Microsoft OneNote
- Document types rendered by the Polycom Cloud Service:
  - Text (.txt)
  - Image (.jpeg, .png, .gif, .webp)
  - Adobe® PDF

Data processed

Polycom limits access to customer data except as required to enable the features provided by the cloud service. Due to the nature of the service, Polycom stores only the following user information.

Customer data stored:

The following information is stored on a customer's cloud tenant account:

- Device Information including:
  - Device and room names, IP addresses, MAC addresses, and serial numbers
- Microsoft Tenant Information including:
  - Tenant domain, name, GUID, and email (global IT admin)
- Authentication Provider and/or Document Services configuration (if enabled) including:
  - Name, Client ID, Client Secret, Tenant, and Tenant ID

The following data may be saved in the local configuration of the Polycom Pano system and Polycom Pano App and may be logged to help with troubleshooting, analysis, and enhancing the customer's service:

- Document filenames
- Device and room names, IP addresses, MAC addresses, and serial numbers
- DNS server addresses (if configured in Pano)
- Pairing configuration with Polycom RealPresence® Group Series (if configured in Pano) including:
  - Group Series system IP address and administrator name and password
- Platform details (for Pano App) including:
  - OS version, manufacturer, model, language, CPU, GPU, memory

Customer data transmitted:

The following information is transmitted in conjunction with content sharing and annotating functions:

- Rendered cloud document image data
- Annotated documents

Secure deployment

The following information may provide security conscious administrators of the Polycom Cloud Service and Polycom Pano systems additional guidance concerning the secure deployment of the solution. Each deployment needs to find the appropriate balance of security between convenience and features.

General guidance

- Restrict physical access to Polycom Pano hardware components as much as possible.
- Place Polycom Pano systems behind a network firewall. The only port required for communication between Polycom Pano or Polycom Pano App and the Polycom Cloud Service is 443.
- Restrict access to the Polycom Pano system administration web interface and Polycom Cloud Service Administration Portal.
- Adopt complex password requirements for the Polycom Pano system administration web interface and Polycom Cloud Service Administration Portal. Secure access to these passwords, too.

Secure Polycom Pano deployment

- Rename the Polycom Pano system web interface access account from *admin* to a less obvious alternative.
- Polycom Pano logs are accessible via system web access. Although no highly sensitive personally identifying information (PII) or passwords are logged, log access may constitute restricted information disclosure. This can be mitigated by limiting access to the system administration web interface.
- An HDMI connection provides the most secure means of local content sharing.
- Although Miracast® and Airplay® are secure protocols, additional protection for content sharing may be provided by disabling wireless features in environments that do not require (or explicitly disallow) it.
- Likewise, Bluetooth may be disabled. Note, however, that if the Polycom Pano system is registered to the cloud, then it can be found by room name; if it is not, then IP address is the only connection mechanism possible if Bluetooth is disabled.
- A Security Code is enabled by default for content sharing and is a recommended setting. The Security Code automatically cycles from one session to the next.

Secure cloud service deployment

- To ensure timely and unattended system updates, Polycom Pano devices must be configured to automatically download and enable updates from the Polycom Cloud Service.
- Polycom Pano App users who are signed into the Polycom Cloud Service can search and see the room name of Polycom Pano systems registered with a customer's Polycom Cloud Service. If the disclosure of room names is considered privileged or a security risk, use a different naming convention for Polycom Pano systems other than room names.
- Polycom Pano systems that are decommissioned or otherwise removed from service should be deleted from the list of registered entries in the Device Management interface of the Polycom Cloud Service Administration Portal.

Polycom Labs features

Polycom occasionally releases features to provide early access to an area of new innovation and capability within the Polycom solution ecosystem. Polycom Labs features are fully tested and supported and can be used and evaluated in production environments.

The following Polycom Labs feature is included in Polycom Pano version 1.0:

- Polycom Cloud Service Content Sharing: With the Polycom Pano App, users can securely share documents during a meeting from their cloud storage service (e.g., OneDrive for Business) to a Polycom Pano system registered with the Polycom Cloud Service.

Resources

To learn more about Polycom Pano and Polycom Pano App, please visit our site.