SECURITY AND PRIVACY WHITE PAPER

# Poly Touch Controller

Part 3725-88834-001

Version 2

July 2024

## Introduction

This white paper addresses security and privacy related information for the Poly Touch Controller.

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 Touch Controller, 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. You may also subscribe to receive notifications when this paper is updated from the website.

HP | Poly delivers a secure touch controller platform, whether operating as an endpoint controller in a room, or as a stand-alone scheduling device (usually deployed outside the room). HP | Poly designs these touch room controllers/schedulers to work in demanding high-security environments while still being simple and user friendly. The Poly Touch Controller (TC) employs a host of customizable layers and best practices, all working in tandem, to achieve industry leading security. For more detailed information, please see the Touch Controller Admin Guide.

## Security at HP | Poly

Security is always a critical consideration for products such as Poly Touch Controller. 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 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 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 Touch Controller 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 is the processor of customer data while the customer is the data controller.

The TC itself only retains basic device and application information over time (i.e. processor utilization, memory statistics, software versions, model, serial number, etc.). It does not track or store call use nor any personally identifying information from its use outside of the configuration values required for its features as applicable. All internal logging masks out any sensitive transient information like passwords and other sensitive information.

### Lens Data

Lens is a cloud service offering from HP | Poly, which provides a bevy of administrative and analytical features for many different HP devices (endpoints, cameras, phones, touch panels, speakers, etc.). If the TC is enrolled/integrated with Lens (either explicitly itself or as a result of being paired to an endpoint that is) configuration and usage data may be periodically sent to the Lens cloud service for a variety of provided features, including but not limited to: anonymous usage statistics, device inventory lists, device health alerts, provisioning/configuration, remote administration, and more... See https://lens.poly.com, along with the terms of service and privacy statement links for more details.

If someone is an individual user, and the purchase of Poly Touch Controller 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.

| Source from Where PI Collected | Categories of PI Collected | Business Purpose for Collection | Disclosed to the following Service Providers |
|---|---|---|---|
| • Device Administrator and user information | • First/Last Name<br>• User ID<br>• Email address<br>• Password (hashed)<br>• Organization name<br>• Tenant ID | • Authenticate and authorize administrative access to the service<br>• Deliver the service<br>• Reporting<br>• Usage/activity | Auth0, Azure, AWS |
| • Device Identifier and Network data | • Device ID<br>• Device name<br>• MAC address (for both primary device and paired/ unpaired IP peripherals)<br>• Serial number<br>• Software version<br>• IPv4/v6 address<br>• MAC address<br>• Display name<br>• System name<br>• System owner<br>• Domain name<br>• Log files<br>• Device geolocation data including time zone<br>• Network identifiers<br>• Network type<br>• Bluetooth addresses<br>• Device status<br>• Device configuration records | • Understand how devices are being used in a customer environment<br>• Help customer diagnose technical issues<br>• Collect analytics to improve the technical performance of the customer's UC service<br>• Provide details in support of room or devices issues that require support<br>• Serial number for entitlement | Azure, AWS |

**Purpose of Processing**

The primary purpose of processing information with Poly Lens service is to:

- Enable inventory management—View your devices and manage important information like software versions and device data.
- Perform data analytics—Better understand utilization, performance, and call quality.

NOTE: Personal data is processed for display and reporting purposes only.

**How Customer Data is Stored and Protected**

The TC contains limited data involving only configuration of it and its services. Any usage data that may be transmitted to the Lens service, if configured, is not preserved. All configuration data is stored in secure internal storage, inside the sealed access Android OS, and is only accessible via administrative authenticated interfaces (administrative UIs and REST APIs).

### Data Deletion and Retention

Resetting a TC device (reset administrative menu/API function and/or “Pinhole” reset + reboot) will completely clear out all internal configuration, logging, and any other stored information from the device. A reset will make the TC device’s data state as it was when first purchased. After reset, it will remain on the currently installed version of software instead of reverting to an earlier software release.

Any data sent to Lens is removable via provided Lens mechanisms (please see Lens help and administrative guides for details).

HP | Poly may retain customer data for as long as needed to provide the customer with any HP | Poly 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

The TC employes standard AES-256 cipher suites as well as hash strengths including SHA-256, SHA-384, and SHA-512 for all its networking protocols, APIs, and administrative interfaces.

Web interfaces and REST APIs use HTTPS connections that utilize TLS 1.2 with a 256-bit encryption layer using SSL and certificates.

Cryptographic cipher suites and modules implemented and used in the TC are open (publicly disclosed) and have been peer reviewed. Cryptographic libraries are current, regularly updated, and leverage the Advanced Encryption Standard.

### Authentication

Administrative users may authenticate for TC configuration, and other administrative functions, on the TC embedded UI as well as the web UI and REST APIs. The administrative user employs basic user ID and password credentials, authenticated internally to the device. The password credentials are stored using standard irreversible salted hashing on the TC device, to be authenticated against.

### API

All configuration functions, whether in the embedded Android UI or in the administrative web UI, or via the REST APIs are protected behind administrative credentials. The only settings on the TC available outside of this protection are user functions like brightness, dark vs. light-mode, etc. For the web-based methods, once the POST form-based web authentication is performed, a time-limited token-based session allows access to the functions/settings. A similar time-limited administrative session is used for the embedded UI. Once expired, re-login and re-authentication is necessary to access these settings again.

For the web-based access methods, a modern embedded webserver carries requests to an interpreted API layer for parsing and processing. This layer translates the web-requests into internal commands and settings. This translation architecture prevents injection, as well as many other types, of attacks.

Note: In later TC versions, REST/UI HTTPS based access may be fully disabled for operation in high-security environments.

All APIs are encrypted over TLS.

### Server Access and Data Security

Access to the TC is restricted to the provided on-screen embedded UI, the administrative web-UI, and administrative REST APIs. Otherwise, the Android platform the TC uses is sealed to external admittance, preventing access to any configuration data therein except by the authenticated aforementioned means. All passwords, and any like sensitive information, is stored either in a 1-way hashed form or is encrypted with AES at rest.

### Security of the Android Platform

The first security layer the TC uses is a locked-down, access restricted, Android Platform for its base operating system.

This Android OS provides these security layers, which the TC takes full advantage of:

- **Linux Kernel -** the TC utilizes a Linux kernel which uses process isolation, a strict permissions model, secure IPC, hardened FIPS certified cryptographic system, and pluggable security modules (LSMs) and many other features to deliver secure computing.

- **SELinux with Strict Policy** – the TC uses a Linux Kernel Security Module (LSM), first developed by the NSA (USA's National Security Aency) that adds even tighter controls of permissions and access restrictions internal to the OS.

- **Read-Only Software Partitions** - Internal OS and HP | Poly software are flashed to device partitions that are then mounted read-only, preventing later malicious modification and corruption.

- **Android Verify Boot** - Any unauthorized change to OS files or applications will result in bootup failure. Only signed and authorized changes, like a verified upgrade, are permitted. This further ensures the integrity of the installed software.

- **Isolated Android Runtime** - Most TC applications and services run inside the secure Android Runtime sandbox, isolating them from the rest of the OS and from each other. The ART also implements strict permissions controls, limiting applications to only specified resources and operations on the device.

FIPS certified libraries, app-signing, and other low-level security features make the Android Platform the perfect base on which to build the security-conscious Poly Touch Controller.

For more information on Android security see:

- Android Security Overview

- What is SELinux?

- Overview of Linux Kernel Security Features

For more detailed description of these security layers, please see the Touch Controller Admin Guide.

### Signed Update Packages and Limited Upload

To limit the TC's attack surface and make it more hardened the TC is designed with the following features:

- The TC will only accept image update packages cryptographically signed and verified from HP | Poly. The TC accepts no other source of full system updates.

- All base TC software from HP | Poly is also included in this signed image, with the specific applications/services themselves also signed and validated.

- The only third-party applications allowed on the TC are those made by specifically supported partners, who employ HP | Poly evaluated integrations to operate with the TC hardware and update only their specific applications.

- The only other external software able to be run on the TC is external room-control and external customer application webpages, if these features are enabled, which are strictly client-side Javascript run inside isolated Android Web-View containers.

- No installation of other applications/services, or modifications, are possible to the TC product and as such the vector for any infection of malicious software is all but eliminated.

### Secure Networking, Open Ports, Link-Local-Networks, and SCEP

The TC only uses secure and encrypted network communications, using only a handful of known network ports. In addition to this basic security tenet, it also supports 802.1x for port-based network access and SCEP (Simple Certificate Enrollment Protocol) for auto-provisioning of secure certificates. In some configuations it also supports isolated link-local networks (LLN) for total network isolation.

**For any of the capabilities listed here, please refer to the administration guides for a particular version of the TC for details of use and applicability.*

### User Certificates

The TC supports installation of user defined certificates, which are used for all in and outbound secure connections as well as 802.1x network features. At this time, up-to 3K-bit, SHA-256, and RSA certificates are supported.

### Outbound Web-Proxy

The TC supports configuration and use of customer-provided web-proxies for all outbound external web connections. These connections may be from specific partner applications (e.g., Teams, Zoom, Ring Central, Google, etc.) or may be from HP | Poly services (e.g., checking for software updates or provisioning). Web-Proxy is supported by all HP | Poly endpoint paired TCs and is supported by TCs running in “stand-alone” mode in later versions.

### 802.1x

Authentication may be done either by configured/provisioned credentials on the TC and/or via trusted certificates. This mechanism is enforced by low-level networking infrastructue (switches and routers) to prevent unauthorized devices from any communiation/interfearance with authorized ones.

The TC fully supports operating in an 802.1x environment with a variety of configuration options. See the 802.1X Specification for more information on 802.1x.

### Open Ports

For detailed port information for the Touch Controller, please see the Touch Controller Admin Guide.

### Link Local Network

In specific deployments like PC-based MTRoW (MS Teams Room on Windows), the TC supports being deployed using an isolated private-to-the-room network. This private link-local-network (LLN) completely prevents network access to and from the TC except by the devices in the room (device it is paired with and other TCs), eliminating any external attack vectors to it. This type of deployment also has an administratively simplified auto-configuration “plug-n-play” feature as a benefit for use.

### SCEP – Simple Certificate Enrollment Protocol

The TC supports configurations to use SCEP to automate the installation of customer certificates for use. These certificates will be used for any outbound connections, for the web-based administrative UI, REST APIs, and for 802.1x features. See the RFC8894 Specification for more information.

### Communicating to Paired Devices

When a TC is paired to another device in the room (PC or Android Endpoint) to function as its 'controller', one of two protocols will be used. For detailed port information for the Touch Controller, please see the Touch Controller Admin Guide.

### RDCP – Room Device Communication Protocol

RDCP is used when communicating with mostly PC based solutions (e.g., MTRoW, Zoom Room on Windows, etc.). This protocol utilizes a UDP multicast packet (port 4077) for simple discovery should the devices be on the same LLN or LAN segment, and a TCP channel (port 50777) with encrypted payload packets of a proprietary communication/control protocol.

- To setup a pairing connection, the devices use a HP | Poly proprietary protocol over a standard TCP network connection.
- The initial TCP connection between the TC and room devices (using port 5077 TCP) is authenticated, and initially encrypted, using multiple HP | Poly manufactured cryptographic keys.
- The next step in pairing is to perform several Elliptic-Curve-Diffie-Hellman key exchanges, using a FIPS certified 512-bit curve.
- These ECDH keys shall then be used to encrypt separately and uniquely the transmit and receive payloads between the devices (i.e. A -> B uses Key1, B -> A uses Key2) using AES-256 for the life of that TCP connection (i.e. new TCP connections always get new TX and RX keys).
- Once the pairing connection is successfully setup between the devices, a proprietary set of messages is exchanged over this multi-encrypted connection.

### Modular Room (MR) Communication Protocol

MR is used when communicating with room endpoints/codecs (e.g., x30, x52, x70, G7500, etc.). This protocol utilizes a UDP multicast discovery packet (port 2000), should the devices be on the same LLN or LAN segment, and a standard TLS network channel (port 18888) for a proprietary communication/control protocol.

- To setup a pairing connection, the devices use a mutually authenticating TLS 1.2 connection which uses a HP | Poly manufactured certificate for mTLS authentication. This TLS channel is configured to use various high security ciphers and key exchanges such as ECDHE-RSA-AES256-GCM-SHA384.
- Once the pairing connection is successfully setup between the devices, a proprietary set of messages are exchanged over the TLS connection.

### Disaster Recovery and Business Continuity

Multiple redundant touch-controllers are allowed for all room deployments.

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 Touch Controller, 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.