SECURITY AND PRIVACY WHITE PAPER

Unified Communications Software (UCS) and Poly Voice Software (PVOS) for Poly CCX, VVX, and Edge E Phone Series

Part 3725-85683-001

Version 11

March 2024

Introduction

This white paper addresses security and privacy-related information regarding Unified Communications Software (UCS) and Poly Voice Software (PVOS) for Poly CCX, VVX, and Edge E Series devices.

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 software for the CCX, VVX, and Edge E devices, including the location and transfers of personal and other customer data.

HP | Poly uses such data in a manner consistent with the HP Privacy Statement and this white paper (as 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.

UCS/PVOS is the telecommunications industry's most powerful and flexible SIP software for VoIP-enabled devices. HP | Poly's software and award-winning product design are compatible with the broadest range of call control platforms and support highly robust provisioning and device management solutions, employing the broadest SIP feature set.

Optional Integrations Available

Your device natively supports the optional integrations as listed below. Please note that no data is shared with any other party until your device is configured to do so. Please consult the administrative guide for more detailed information.

Optional configuration	Provisioning	Other Services
Poly Lens	Yes	Device Management, Analysis & Reporting
Zero Touch Provisioning (ZTP)	Yes	Basic provisioning and redirection
PDMS-SP (Polycom cloud service)	No (Basic provisioning supported)	Device Management & Monitoring, Analysis and Reporting
Poly RealPresence Resource Manager System (RPRM) (on customer premises)	Yes	Device Management & Monitoring

For security and privacy details related to these optional products and services, please refer here.

For security and privacy details related to the RealPresence Resource Manager System, please refer to the Privacy section of the Operations Guide for Poly RealPresence Resource Manager System.

CCX devices also support integration with certain third-party applications which may result in one of these applications processing personal data. Please carefully review all security and privacy information that is provided by the applicable vendor prior to using their applications with CCX.

Security at HP | Poly

Security is always a critical consideration for all HP | Poly products and services. 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.

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 CCX, VVX and Edge E Series 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 Collection
By default, no product usage data or identifiable personal data is sent to HP | Poly from Poly CCX, VVX, and Edge E Series devices. However, if certain settings are enabled, HP | Poly automatically collects and analyzes product usage data, device data, call detail records, and quality of service data from your CCX, VVX, and Edge E devices. Data collected will be used for the purposes identified in the table following this section. To enable data collection, please see the "Device Analytics Settings" section in the *Privacy Guide for Poly CCX Business Media Phones* and the *Privacy Guide for Poly VVX Business Media and IP Phones*.

If someone is an individual user of a CCX, VVX, or Edge E device, and their employer has purchased and configured the system on their behalf, 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.

Data Processing
By default, the following list provides some of the information that is processed and stored locally on Poly CCX, VVX, and Edge E Series devices:

- MAC address
- Serial number
- Line name
- IPv4/v6 addresses
- SIP username
- SIP URI
- SIP alias name
- PDMS-SP number
- Local contacts
- Admin and usernames
- Admin and user passwords
- Missed/Placed/Received Call lists
- Full Call detail record (CDR)
- System log files
- Directory entries
- Offset GMT

This information is used by the device to provide basic functionality, enable the REST API functionality, and to enhance the user experience by providing easy access to call history and frequently used contacts.

If someone elects to enable the use of the CCX, VVX, or Edge E devices with the optional Poly Lens cloud service, their device will send information to that system for the purposes of device management, intelligent insights, and cloud-based services. For details about this data processing, please refer to the Security and Privacy White Paper for Poly Lens located here.

If you elect to use the CCX, VVX, and Edge E devices with optional products or services such as RPRM, PDMS-SP or Poly Lens, you can find security and privacy details related to these optional products and services at HP | Poly's website located here.

Purpose of Processing
Information that is processed is used for enhancing the user experience, allowing configuration of settings required for proper delivery of services, and easy access to frequently used data.

Source from Where PI Collected	Categories of PI Collected	Business Purpose for Collection	Disclosed to the following Service Providers
Device Identifier Information	• MAC address (primary device and IP peripherals) • Bluetooth MAC address (mobile phone or headset) • Public Bluetooth name • Serial number • Device ID • Display name • System name • IP address • Device geolocation data including Time zone	• Internal research (product improvement, development, and analytics) • Activities to verify or maintain the quality (Product and Sales Engineering Support) • Detecting security incidents • Debugging • Mobile phone book access	Azure (Poly Lens) or AWS (PDMS-SP)
Device User Information	• SIP username • SIP URI • SIP alias name • Admin and usernames and passwords • Local contacts • Directory entries • System log files • Tenant ID • Site ID • Room ID • Org ID • DNS information • Network Identifiers • Email address • Obi number • PCS account code • PCS number	• Internal research (product improvement, development, and analytics) • Activities to verify or maintain the quality (Product and Sales Engineering Support) • Detecting security incidents • Debugging • Short-term, transient use (login) • Mobile phone book and call management (local use only – not sent to cloud)	Azure (Poly Lens) or AWS (PDMS-SP)
Local and Remote Call Participant Information	• Full Call detail record (CDR) • Call lists • Dial string number • Caller ID • Call ID • Participant names (local and remote)	• Internal research (product improvement, development, and analytics) • Activities to verify or maintain the quality (Product and Sales Engineering Support) • Detecting security incidents • Debugging • Short-term, transient use (login)	Azure (Poly Lens) or AWS (PDMS-SP)

When configured to use an optional Poly device management solution, the on-premises server or cloud service processes configuration files and their overrides to aid the management of the devices in a

given deployment. The server or cloud service may also process device network information, media statistics, and device asset information to aid in device analytics, which enables device performance validation and visibility into customer quality of experience and service performance.

How Customer Data is Stored and Protected

Poly VVX and Edge E Series devices are Linux based systems and utilize AES-256 to encrypt customer data including the file system, user data, and configuration files.

Poly CCX devices are built based on the Android Open-Source Project (AOSP) in which File Based Encryption (FBE) is in use. We utilize AES-256 to encrypt customer data including the file system, user data, and configuration files.

If the phone is configured to use an optional Poly device management solution or provisioning server, the local contacts file, the device logs, and the call log will be securely uploaded to the solution for backup. There is also a configurable option for the user to stop uploading of the local contacts and call lists through a menu item accessible from the phone's LCD interface.

HP | Poly supports the use of encryption to protect configuration files and phone calls. For details, please see the "Encryption" section in the *Privacy Guide for Poly CCX Business Media Phones* and the *Privacy Guide for Poly VVX Business Media and IP Phones*.

For the set of usage data sent to HP | Poly (if enabled), data is stored in a database server that is in an SSAE 16 Type II certified data center in the United States that runs dedicated databases and application servers. When the HP | Poly database server receives data from the customer, it is verified for integrity, processed, and saved in the database.

Data Portability

By default, data is stored securely on the Poly CCX, VVX, or Edge E Series devices and is only accessible via the LCD menu or the device's web interface. However, someone can retrieve the logs associated with their phone and some of its connected devices and copy application and boot logs to a USB device. For details, please see the "Right to Data Portability" section in the *Privacy Guide for Poly CCX Business Media Phones* and the *Privacy Guide for Poly VVX Business Media and IP Phones*.

When a CCX, VVX, or Edge E device is configured to use an optional Poly device management solution (e.g., RPRM or Poly Lens), certain information is uploaded using encrypted protocols to the server for backup and storage. This information can be retrieved by the administrator of a Poly device management solution upon request.

Data Deletion and Retention

All contact and call log data are deleted (but not overwritten) when the phone is reset to factory default settings.

As stated above, the same also applies to all data stored on the device by third-party applications. This data will be deleted when the system is reset to factory settings or when changing from one base profile to another. The rest of security-related aspects of third-party applications should be covered by each application's documentation available directly from the applicable vendor.

For additional details, please see the "How Personal Data is Deleted" section in the *Privacy Guide for Poly CCX Business Media Phones* and the *Privacy Guide for Poly VVX Business Media and IP Phones*.

For the set of usage data sent to HP | Poly, 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 provide the service to customer.

HP | 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.

Secure Deployment

For enterprise customers, Poly CCX, VVX, and Edge E Series devices are deployed and administered on-premises within the customer’s environment. For ITSPs, devices are deployed on-site but administered and provisioned from the cloud outside of the customer’s environment. Deployment options are available to support a variety of scenarios and work environments.

The security of CCX, VVX, and Edge E devices is based on optional settings selected during local device setup or when provisioning is configured by the administrator.

For configuring privacy related options, please see the *Privacy Guide for Poly CCX Business Media Phones* and the *Privacy Guide for Poly VVX Business Media and IP Phones*.

Server Access and Data Security

All customer data sent to the HP | Poly cloud 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 the HP | Poly cloud is backed up daily in digital form using the Azure or AWS backup processes. 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.

Cryptographic Security

If Poly CCX, VVX, or Edge E Series are configured to use an optional Poly device management solution, data transmitted can be encrypted by configuring the device to use TLS protocols as well as strong encryption ciphers for encrypting the packets transmitted over the network.

- Device to Poly Cloud Service
  - HTTPS (443) using TLS 1.1, TLS 1.2 Evaluating services on open TCP/UDP ports
    - Compression: disabled
    - RFC 5746 renegotiation
    - Client-initiated: disabled
    - Ciphers:
      - AES 128/256 (CBC, GCM)
      - Key Exchange: DHE 2048, ECDHE 256
      - SHA, SHA256, SHA384 hashing

  - Poly Cloud Service Device Connections (to local on-premises devices)
    - HTTPS (443) using TLS 1.1, TLS1.2
      - Compression: disabled
      - RFC 5746 renegotiation
      - Client-initiated: disabled
      - Ciphers:
        - AES 128/256 (CBC, GCM), Camellia 128/256 (CBC)
        - Key Exchange: ECDHE 256, RSA
        - SHA, SHA256, SHA384 hashing

For data at rest, please see the section “How Customer Data is Stored and Protected” later in this white paper.

Authentication

Administrator accounts can be authenticated locally on the devices. User accounts can be authenticated either

locally on the device or using the user's Active Directory when using Skype for Business. When Poly CCX devices are in Teams mode, authentication is handled by the Teams application and Microsoft authentication services. Users and administrators can access CCX, VVX, or Edge E Series devices using the phone's LCD menu display or the device's web interface. A password is required to be entered to access the administrator settings menu. Access to the device's web interface requires a password to be entered via a web browser. Accessing the device through the LCD menu requires an unlock PIN to be entered manually (when the phone lock feature is enabled).

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 CCX, VVX, and Edge E Series devices, 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 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.