SECURITY AND PRIVACY WHITE PAPER

Unified Communications Software for Poly CCX and Polycom VVX Series

Part 3725-85683-001

Version 03

June 2020

Introduction

This white paper addresses security and privacy related information regarding Unified Communications Software ("UCS") for Poly CCX and Polycom VVX series devices.

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 UCS for the Poly CCX and Polycom VVX series devices, including 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.

Unified Communications Software (UCS) is the telecommunications industry's most powerful and flexible SIP software for VoIP-enabled devices. Our UC 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

CCX and VVX series are capable of being configured to integrate with the following optional Poly products and services:

Optional configuration	Provisioning	Other Services
Poly Lens	Yes	Device Management, Analysis & Reporting
Zero Touch Provisioning (ZTP)	Yes	Not applicable
PDMS-E (cloud service)	Yes	Device Management & Monitoring
PDMS-SP (cloud service) (VVX only)	Yes (VVX only)	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 to 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.

Poly 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 Poly CCX.

Security at Poly

Security is always a critical consideration for any product which is a network-connected device such as the CCX and VVX series. Poly aligns with ISO/IEC 27001:2013 for our Information Security Management System (ISMS). ISO/IEC 27001 is the most widely accepted international standard for information security best practices, so customers are assured that Poly has established and implemented best-practice information security processes.

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 processes. 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.

Static Application Security Testing (SAST) and patch management are cornerstones of our S-SDLC.

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 CCX and VVX series go through vigorous quality assurance testing where all functional and security requirements are verified. Once Quality Assurance completes pre-beta testing and sign-off, beta testing is performed with selected customers to field validate the new software. Once beta testing is completed, a final Quality Assurance test is performed to validate the fixes for any issues raised during beta testing. Only after final approval from stakeholders are changes 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.

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.

Cryptographic Security

If CCX or VVX Series is 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.

Secure Deployment

For enterprise customers, CCX and VVX 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 and VVX Series devices is based on optional settings selected during local device setup or when provisioning is configured by the administrator. Please refer to the "Configuring Security Options" and "Recommended Security Settings for Provisioning" sections of the appropriate UC Software Administrator Guide for details on best practices for securely deploying the phones. Please refer to the "Privacy Guide for Poly CCX and Polycom VVX" for configuring privacy related options.

Authentication

User and administrator accounts can be authenticated either locally on the devices or via the customer's Active Directory. Users can access CCX or VVX Series devices using the phone's LCD menu display or the device's web interface. A separate password is required to be entered to access the administrator settings menu. Access to the device's web interface requires a username and 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).

Data Collection

By default, no product usage data or identifiable personal data is sent to Poly from CCX or VVX devices. However, if certain settings are enabled, Poly automatically collects and analyzes product usage data, device data, call detail records and quality of service data from your CCX and VVX series 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 and Polycom VVX".

If you are an individual user of a CCX or VVX series device, and your employer has purchased and configured the system on your behalf, all 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.

Data Processing

By default, the following list provides some of the information that is processed and stored locally on CCX and VVX series devices:

- MAC address
- Serial number
- Line name
- IPv4/v6 addresses
- SIP username
- SIP URI
- SIP alias name
- Obi 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 you elect to enable the use of the CCX and VVX series devices with the optional Poly Lens cloud service, your 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 and VVX series devices with optional products or services such as RPRM, PDMS-E or PDMS-SP, you can find security and privacy details related to these optional products and services at Poly's website located here.

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) • 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	Azure (Poly Lens) or AWS (PDMS-E, 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	• 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-E, PDMS-SP)

	• Obi number • PCS account code • PCS number		
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-E, PDMS-SP)

Purposes 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.

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.

Data Portability

By default, data is stored securely on the CCX or VVX Series device and is only accessible via the LCD menu or the device's web interface. However, you can retrieve the logs associated with your 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 of the "Privacy Guide for Poly CCX and Polycom VVX".

When a CCX or VVX Series device is configured to use an optional Poly device management solution (e.g. RPRM or PDMS-E), 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.

How Customer Data is Stored and Protected

VVX Series devices utilize full disk encryption to protect customer data. CCX Series devices are built based on the Android 9 AOSP in which File Based Encryption is supported and by default this feature is enabled. Hence, all the user created data is encrypted before writing onto the device using the 'encrypted key'. Please note that the 'encrypted key' is derived based on the user's device lock preference like PIN, password, or pattern on the lock screen.

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 .

Poly supports the use of encryption to protect configuration files and phone calls. For details, please see the Encryption section of the "Privacy Guide for Poly CCX and Polycom VVX".

For the set of usage data sent to 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 Poly database server receives data from the customer, it is verified for integrity, processed, and saved in the database.

Server Access and Data Security
All customer data sent to a Poly cloud service 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 Poly cloud 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.

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.

Data Deletion and Retention
For clearing of the contacts, there is an option presented to the user under the Basic settings in phone's LCD interface. A user can select this option to clear all the local contacts saved in the phone as well as the call lists and directory entries uploaded to the optional Poly device management solution (if used). Additionally, factory reset is available for resetting back to factory default values. For details, please see the "Right to Erasure" section in the "Privacy Guide for Poly CCX and Polycom VVX".

As stated above, the same also applies to all data stored on Poly CCX Series devices by third-party applications. This data will be deleted when the system is reset to factory settings. 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 the set of usage data sent to Poly, 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 all personal data within 30 days. Other unidentifiable data may continue to be processed.

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.

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 CCX and VVX 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 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.