SECURITY AND PRIVACY WHITE PAPER

# Poly Clariti

Part 3725-87602-001

Version 01

August 2021

**Introduction**

This white paper addresses security and privacy related information for the Poly Clariti solution which includes Poly Clariti Edge, Poly Clariti Core, Poly Clariti Relay, Poly Clariti App, and Poly Clariti Roster. Note that the Clariti solution also includes other components such as RealPresence Resource Manager, Poly Content Connect and RealPresence Collaboration Server (RMX). The security and privacy information for these components are not included in this whitepaper but can be found in the respective product documentation. This whitepaper 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 running of the Clariti Edge, Clariti Core, Clariti Relay, and Clariti App products, as well as the location and transfer 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**

Poly Clariti is simple, powerful, cloud-ready collaboration software for businesses of all sizes that promotes voice, video, content, and web collaboration and takes team work to a new level. It provides an ultramodern and feature-rich user experience and a high level of security and enhanced privacy for communications. Clariti, the future of private video solutions, is a reimagined collaboration and video conferencing solution built on top of Poly's legendary RealPresence Clariti video platform.

**Poly Clariti Edge and Poly Clariti Core**

Poly Clariti Edge and Poly Clariti Core provide a platform that delivers highly scalable and reliable call signaling (registrar and call server), conference control, and media firewall/NAT traversal. Clariti functionality significantly enhances the platform to include new Poly EVO signaling, Poly Clariti Relay management, signaling gateways between Poly SIP MRC and Poly EVO, roster control APIs, SVC cascading between Poly Clariti Relay, and RealPresence Collaboration Server (RMX) MCUs, and many other features. It also serves as the web server for the Poly Clariti App and Poly Clariti Roster applications.

**Poly Clariti Relay**

Poly Clariti Relay is a new, highly scalable, super-efficient, SVC-capable MCU that relays media streams to endpoints in a conference. It supports the new Poly EVO signaling as well as SVC cascading with existing RealPresence Collaboration Server (RMX) MCUs for interoperability with existing Poly and third-party endpoints.

**Poly Clariti App and Poly Clariti Roster**

Poly Clariti App and Poly Clariti Roster provide a new, modern, browser-based, collaboration client (using WebRTC and the new Poly EVO signaling) that provides a feature-rich user experience. Enjoy the high-quality video, audio and content sharing, roster control, chat, polling, hand raising, and many other features. Clariti App and Clariti Roster are packaged and deployed via Poly Clariti Core or Poly Clariti Edge.

Clariti Edge, Clariti Core and Clariti Relay can be installed either on a virtual machine (VMWare, Hyper-V, KVM), on an appliance (specific Dell Servers used for Clariti), or in cloud accounts (AWS, Azure). The Clariti Core and Clariti Edge can be configured as a Clariti Core system (LAN), a Clariti Edge (in DMZ), or as a combination (Clariti Core and Clariti Edge in DMZ). The Clariti Relay is typically only configured alongside a Clariti Core (LAN).

The CentOS operating system running the Clariti Edge and Clariti Core software has been hardened with the latest security patches, best practices for software configurations, and the removal of unnecessary services. Additionally, the OS security has been

verified using industry-leading security and vulnerability scan tools, as well as manual testing. The Oracle Linux operating system, on which the Clariti Relay runs, has been likewise hardened.

**Security at Poly**

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

Standards-based Static Application Security Testing (SAST) and patch management are cornerstones 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 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.

**Security by Design**

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 Poly uses – both on-premises and in the cloud as well as to the development, delivery and support of Poly products, cloud services and managed services.

The foundational principles which serve as the basis of 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.

**Security Settings**

The Poly Clariti Edge and Poly Clariti Core software may reside within the customer enterprise network and/or in their DMZ. It communicates and responds to other devices and services on the network using specific ports (as configured by the customer). When communicating with any device, service, and/or the management interface, you can configure Clariti Edge and Clariti Core to use encrypted communication. Clariti Edge and Clariti Core provide fine-grained security settings in its user interface so that customers can harden security of Clariti Edge, and Clariti Core as required.

Clariti Edge and Clariti Core provides several configurable security settings that the user can set to enabled or disabled.

The user can also configure a wide variety of specific ciphers for management and signaling traffic for TLS and FIPS connections.

In contrast, Poly Clariti Relay is a limited-feature-set product. It is headless, with no UI or administrative interface of its own. Its administrative functions are available only through the Clariti Core administrative interface using a properly authenticated Clariti Core user. It is a product with the singular purpose of managing active call media. As such, it has a narrow set of configurations and designs implementing security by default. For example, its proprietary administrative connection to a Clariti Core is always encrypted (TLS) and it always uses a limited and well-defined set of ports for media, which are only available after call signaling setup (from a Clariti Core). It offers no other access or services (SSH and console may be optionally enabled), and all other ports are closed (firewalled), making its potential attack surface extremely limited.

In a similar manner, the Poly Clariti App and Poly Clariti Roster, have few settings of their own. Encryption is their only method of communication, including media (SRTP). All other settings and concerns are delegated to the web-browser inside of which they run.

**Certificates**

Certificates are used between devices within the video conferencing environment (such as servers and endpoints) to authenticate the devices and to support encryption.

Poly Clariti Edge and Poly Clariti Core provide certificate management capabilities which enable the user to load new certificates for use by the system. Clariti Edge and Clariti Core also support Online Certificate Status Protocol (OCSP) for obtaining the revocation status of an X.509 certificate presented to the system.

**Access Control Lists (ACLs)**

Poly Clariti Edge and Poly Clariti Core provide the ability to configure Access Control Lists (ACLs) for blocking incoming traffic (H.323 and SIP). Based on the configured criteria of ACLs, Clariti Edge and Clariti Core either process the traffic or block traffic believed to be nefarious in nature. ACLs are meant to be specific to SIP and H.323 signaling and allow for dynamic determination of blocking. This can be as simple as blocking known attackers (the default ACL configuration) or as complex as blocking certain IP

addresses or allowing only provisioned endpoints to connect to the Clariti Edge and Clariti Core system (edge or combo configuration).

**Device, Call, and Conference Security**
Poly Clariti Edge and Poly Clariti Core provide different security features for call signaling and conference management that the user can enable or disable from the Clariti Edge and Clariti Core web GUI.

**Port Ranges**
Poly Clariti Edge and Poly Clariti Core enable the user to configure the port ranges that are used for all inbound and outbound network communication on any interface by different services like access proxy, Poly EVO, SIP, H.323, management, API access, media traversal, system ephemeral, TURN, and WebRTC.

For improved security, Clariti Edge and Clariti Core enable the user to specify which services (management, signaling, media traversal, access proxy, and TURN) run on specific network interfaces.

Poly Clariti Relay specifies the media port range it will use, and the 2 ports used for Poly EVO signaling and the administrative connection from a Clariti Core. No other ports are ever opened or are in use.

**Management Access**
Poly Clariti Edge and Poly Clariti Core are designed to use multiple network interfaces, which allows different services to run on different networks. For example, management traffic can be limited to the internal network to prevent possible intrusion from outside the local network.

For management access to the Clariti Edge and Clariti Core web GUI or REST APIs, local as well as Active Directory users are supported. Users are assigned specific roles like Administrator, Auditor, and Provisioner. Based on the role assigned, authenticated users can view specific pages.

The user can also control the number of active sessions, the active sessions per user, and the session timeout interval to the web GUI and REST API logins.

For additional security, the user can enable management access settings and provide the list of IP addresses of machines that can access the web GUI or the REST APIs of the Clariti Edge and Clariti Core systems.

Poly Clariti Relay is administered only through its encrypted administrative connection to a Clariti Core.

As Clariti Edge, Clariti Core, and Clariti Relay run the Linux operating system, users can change the Linux Root (root) as well as secure-shell remote user passwords for SSH and access if enabled.

**Reporting**
Poly Clariti Edge and Poly Clariti Core have extensive reporting capability and provide the user with both system level and call/conference level reports.

Poly Clariti Relay has no reporting or data collection facilities of its own, and only retains incidental call meta-data in transient application logs.

**Data Processing**
Poly Clariti Edge and Poly Clariti Core do not access any customer’s data except as required to enable the features provided by each application. As these systems are deployed in the customer’s environment, it is the responsibility of the customer to protect data privacy.

NOTE: If the “Analytics/Send usage data” option is enabled, certain data will be sent to Poly and processed. Please see the section in this white paper titled “Purpose of Processing” for more details.

Clariti Edge, Clariti Core, and Poly Clariti Relay collect and process logs containing the following information:

- Device data (includes information such as type of device, device name, and installed software version)

- Call and conference data (includes call connection information such as IP addresses, phone numbers, and some other caller personal data like user ID or caller name)

Clariti Relay automatically deletes transient application logs. Clariti Edge and Clariti Core provide the ability to automatically or manually delete the following data from the management web GUI:

- Endpoint records (activity history)
- Log file archives
- Backup files

If someone is an individual user and the purchase of Clariti 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 the controller of such personal data.

**Purpose of Processing**

*Analytics/send usage data*

To continually improve the product, Poly optionally collects data to understand how customers use the Poly Clariti solution. By collecting this data, Poly can identify system level utilization and the combined use of Poly Clariti Edge and Poly Clariti Core system features. This data informs Poly which features are important and actually used on your system. Poly uses this information to help guide future development and testing.

The customer's decision to enable or not enable the sending of this data does not affect the availability of any documented system feature in any way. Enabling this feature does not affect the capacity or responsiveness of the Clariti Edge and Clariti Core systems to process calls and conferences, nor does it affect access to the management user interface or API interactions.

The system sends usage data once per hour over a secured (TLS) connection (port 8443) to a Poly collection point (here). There is no access by any customer or others to view the data received at the collection point. The raw data is viewable only by Poly as well as by the system administrators of each Clariti Edge and Clariti Core system (viewable JSON file). To avoid any impact to starting and ending calls and conferences, data is never sent between 5 minutes before the hour and 5 minutes after the hour.

The following types of data are reported:

- License information
- Hardware configuration
- System resource usage: CPU, RAM, disk, and database
- System configuration: number of servers and clusters
- Feature configuration: Enterprise directory integration, Skype for Business, dial rules, shared number dialing, hunt groups, registration policy, and device authentication, security settings
- Number of users, endpoints, sites, MCUs, external gatekeepers, SIP peers, and SBCs
- Registrations and call/conference statistics (CDRs, registration, and call history)

The administrator can disable or enable data collection. All data is anonymized before sending and is thus scrubbed of any identifying information— such as IP addresses, domains, names, etc.—before Clariti Edge and Clariti Core systems send usage data to the data collection point. System serial numbers and license information are sent without anonymization and may be used to help improve customer experiences. In total, less than 100KB of data per hour is collected and sent. Poly's collection and use of this data complies with the Poly Privacy Policy.

The user can allow or disallow the automatic sending of usage data at any time. Clariti Edge and Clariti Core systems require HTTPS port 8443 to be open to send usage data across the internet. The administrator can also view the system records data that has been sent and collected by Poly in the analytics.json log file available for download through the management web GUI. Poly Clariti Relay sends no data of its own.

The Poly Clariti App does provide an optional anonymous call survey at the end of each call. This survey, if submitted by the user/client/customer, only contains pertinent diagnostic information related to the previous call and the customer's manually entered rating (1-5) and an optional user's note. It contains no personally identifiable information. Its data is stored on systems accessible only by authorized Poly personal. It is used to help Poly development teams identify potential issues experienced by users. This feature can be disabled from the Clariti Edge and Clariti Core management web GUIs.

| Source of Personal Data | Categories of PI Processed | Business Purpose for Processing | Disclosed to the following Service Providers |
|---|---|---|---|
| Analytics/Send usage data information (only data sent to and processed by Poly) | • Activity logs<br>• Call detail records<br>• Serial number/Unique identifier<br>• MAC address | • Troubleshooting customer issues<br>• Product improvement | AWS (Poly tenant) |
| Administrative user and customer operator profiles | • Name<br>• Email address (optional)<br>• Password (hashed)<br>• SIP URI<br>• System name<br>• System owner<br>• IP address<br>• MAC address<br>• E164 address<br>• H.323 ID | • Authenticate and authorize administrative access to the service<br>• Deliver video service<br>• Reporting<br>• Usage/activity | N/A |
| Call participant personal data | • Name/User ID<br>• Email address (optional)<br>• Phone number<br>• Display name<br>• SIP URI<br>• IP address<br>• Dial string | • Deliver video service<br>• Diagnose technical issues<br>• Conduct analytics and analysis to improve the technical performance of the service<br>• Respond to customer support requests<br>• Serial number for entitlement<br>• Capacity forecasts<br>• Keep track of KPIs | N/A |

| | | | |
|---|---|---|---|
| Device information | • Device name<br>• IP address<br>• MAC address<br>• Serial number | • Deliver video service<br>• Diagnose technical issues<br>• Conduct analytics and analysis to improve the technical performance of the service<br>• Respond to customer support requests<br>• Serial number for entitlement<br>• Capacity forecasts<br>• Keep track of KPIs | N/A |

**How Customer Data is Stored and Protected**
Customer data such as usernames, device aliases, and certain description fields are not uploaded by the analytics service. Additionally, host names, internal IP addresses, usernames, and passwords are not uploaded. Other customer-specific data is pseudonymized. The analytics software only stores the Poly serial number/unique identifier and interface MAC values are reported with the hardware profile data of each system running analytics.

The analytics data is securely transmitted to an AWS service in the Poly tenant over an encrypted connection and stored in Amazon Web Services (AWS). Currently, we use data centers in the United States only. Poly may change the location of the analytics 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.

All information collected is stored in a database with email domain information configured as the access control mechanism. Nothing is transmitted outside of the analytics server. All data is self-contained in the database in the data center.

Only approved Poly staff are allowed direct access to the data based on the principles of need-to-know and least privilege. An email is sent out to approved Poly staff for incident response. Read-only access to view the data is controlled through an interface that requires a Poly-credentialed user to be logged into the Poly network. Access to the Poly internal-only analytics web interface requires each user to be granted individual access.

The anonymous call survey results from Clariti App are stored encrypted in SurveyMonkey and only accessed by authorized Poly personnel. For more details see:
https://www.surveymonkey.com/mp/privacy/

**Data Portability**
CDRs can be downloaded in CSV format. Log files can be downloaded in plain text format.

**Data Deletion and Retention**
Poly may retain customer data for as long as needed to provide the customer with any Poly 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 the requested data within 30 days, unless the data is required to be retained to provide the service to customer. 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**
Depending on customer settings, Poly Clariti Core, Poly Clariti Edge, and Poly Clariti Relay support TLS 1.2 (or can be configured with lesser if desired) for all HTTPS based communications (web UI and REST interfaces) with 128-bit and 256-bit AES ciphers along with 2048+ bit or equivalent key exchanges using RSA, DH, or ECDH exchange algorithms. The SHA-256 and SHA-384 cryptographic hashes are also employed.

System backup and upgrade files themselves are protected with AES-256 encryption. Control of specific ciphers for particular purposes (e.g., signaling vs. management interfaces), as well as detailed password policies, and other security configurations are available via the management web GUI.

**Password Management**
Strong passwords are supported. All configuration settings and password management details are located in the administrator's guide.

**API**
All APIs are encrypted over TLS (REST) and authenticated against the internal, and modifiable, credentials.

**Disaster Recovery and Business Continuity**
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. Poly tests disaster recovery processes and procedures on an annual basis. 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 Poly Security Office (PSO) promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. Please 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**
The *Poly Clariti Security and Privacy Guide, Poly Clariti Edge/Core System Getting Started Guide* and the *Poly Clariti Edge/Core System Operations Guide* have in-depth details about Clariti Edge/Core configuration and capabilities. To access those guides and other information about Poly Clariti, please visit our support site.

**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.