PRIVACY GUIDE

December 2022| 3725-87736-004A

Poly Clariti Solution Components

Poly Clariti Core, Poly Clariti Edge, Poly Clariti Relay, Poly Clariti App and Poly Clariti Roster, Workflow Lite, and Poly Clariti SDK

Contents

Before You Begin

This document provides security and privacy-related information regarding Poly Clariti solution components, including:

- Poly Clariti Core
- Poly Clariti Edge
- Poly Clariti Relay
- Poly Workflow Lite
- Poly Clariti App (Mobile and Web)
- Poly Clariti Roster
- Poly Clariti SDK

It also describes the security features and access controls in Poly's processing of personally identifiable information or personal data and customer data in connection with the running of the Poly Clariti solution components, as well as the location and transfer of personal and other customer data.

Getting Help and Related Documentation

For information about installing, configuring, and administering Poly Clariti products, see the Poly Clariti Support Page.

The following types of documents are available on the support page:

- Getting Started Guide
- Server Replacement Migration Guide
- Administrator Guide
- Release Notes
- Privacy Guide
- End-User License Agreement
- System API documentation
- Offer of Open Source Software
- Whitepapers

For information about security issues, see Poly Clariti Security and Privacy White Paper.

Poly and Partner Resources

To find all Poly partner solutions, see Strategic Global Partner Solutions.

The Poly Community

The Poly Community gives you access to the latest developer and support information. Participate in discussion forums to share ideas and solve problems with your colleagues. To register with the Poly Community, simply create a Poly online account. When logged in, you can access Poly support personnel and participate in developer and support forums to find the latest information on hardware, software, and partner solutions topics.

Security-Related Options

This section provides information on security-related options for Poly Clariti Core, Poly Clariti Edge, Poly Clariti Relay, and Poly Clariti Workflow Lite, along with the video endpoint and roster applications (Poly Clariti App and Poly Clariti Roster).

Feature Summary

This section lists the feature summary of Poly Clariti Core, Poly Clariti Edge, Poly Clariti Relay, Poly Clariti App (Mobile and Web), Poly Clariti Workflow Lite, Poly Clariti Roster, and Poly Clariti SDK.

Note: From 2022, Poly ends the support for WebRTC that is used by Poly Web Suite.

Poly Clariti Core and Poly Clariti Edge

Poly Clariti Core and Poly Clariti Edge are a feature-rich video conferencing platform and server. At a high level, Poly Clariti Core and Poly Clariti Edge provide the following set of features:

- Call server (SIP, H.323)
- Conference management (SVC and AVC support)
- Virtual meeting rooms (VMRs)
- Bridge virtualization
- Firewall/NAT traversal

- High Availability (HA) and geographic redundancy
- SBC media relay
- STUN, TURN
- Reverse proxy (HTTPS, HTTP, XMPP, LDAP)
- REST APIs for all administrative functions
- HTML5 browser-based management interface (system web interface)
- Extensive dial plan capabilities
- Multiple dial plans based on signaling protocol, port, or transport
- Support for Poly and third-party endpoints
- Integrations with other systems (Skype for Business, Microsoft Exchange, Microsoft Active Directory, Poly Clariti Manager, Poly RealPresence Collaboration Server (RMX), Poly ContentConnect, Poly RealConnect with Microsoft Teams, Zoom, Cisco Webex)
- Registration policy
- Access lists
- Device authentication
- Port range settings
- Certificate management
- Extensive monitoring and reporting
- Remote syslog and SNMP
- Custom security settings
- Management and signaling cipher selection
- Login policy
- Back up and restore
- Troubleshooting utilities

You can install Poly Clariti Core and Poly Clariti Edge on a virtual machine (VMWare, Hyper-V, KVM), on an appliance (COTS – Dell Servers), or in a private cloud environment (AWS, Azure). You can set Poly Clariti Core on LAN side, and Poly Clariti Edge in a DMZ, or both in DMZ.

You can deploy Poly Clariti Core and Poly Clariti Edge in various network configurations. Here are some examples:

- Poly Clariti Edge communicating with Poly Clariti Core

- Two Poly Clariti Edge systems peered across a firewall communicating with Poly Clariti Core
- Two Poly Clariti Edge systems in a VPN tunnel communicating with Poly Clariti Core

Customers who use a cloud VaaS service, like Poly RealConnect for Microsoft Teams or Zoom, may require Poly Clariti Edge for increased security, for firewall/NAT traversal from enterprises to the cloud service, and for internet bandwidth preservation.

Poly Clariti Relay

Poly Clariti Relay is a headless MCU-media component managed and controlled by Poly Clariti Core. It maintains the media management for ongoing Poly EVO (SVC) based calls passing through Poly Clariti Core. At a high level, it does the following:

- Manages the media streams between the endpoints, delivering audio, video, and content between them
- Supports mixing of multiple audio streams into a cohesive single audio stream for all conference participants
- Supports transcoding of supported audio codecs between participants
- Provides video switching and other related video delivery features for all participants

Poly Clariti Workflow Lite

Poly Clariti Workflow Lite is a reliable and scalable video collaboration infrastructure solution comprised of two key feature sets in the Poly Clariti solution.

- Poly Easy Schedule App for Outlook. Scheduling plug-in for Microsoft Outlook used to simplify scheduling Poly Clariti conferences.
- Poly One Touch Dial App. Enables click-to-join on supported video endpoints that synchronize with Exchange.

Poly Clariti App Web and Poly Clariti Roster

Deployed inside Poly Clariti Core and Poly Clariti Edge are two web-based applications: Poly Clariti App Web and Poly Clariti Roster. You can access these web applications using a Google Chrome, Safari, or Microsoft Edge browser to provide the following functionality:

- Poly Clariti App Web is the web version of Poly Clariti App. It’s a simple endpoint client that can participate in audio or video conferences when using Poly Clariti Core and Poly Clariti Relay. It also provides in-conference messaging/chat, voting, and current participant display (roster).
- Poly Clariti Roster is a simplified version of Poly Clariti App Web that only provides the roster functionality, conference participant display, and controls for a currently running conference.

Poly Clariti App Mobile

The Poly Clariti App Mobile is the mobile version of Poly Clariti App, available in v1.2 release and later. It's a software-based video client that allows the user to join a video conference from an iOS or Android device.

Poly Clariti App Mobile is a simple endpoint client that can participate in audio/video conferences when using Poly Clariti Core and Poly Clariti Relay. It also provides in-conference messaging/chat, voting, and current participant display (roster).

Poly Clariti SDK

The Poly Clariti SDK is a software-based framework that facilitates the building of Poly Clariti focused software clients. The SDK supports the following environments: MacOS, Windows, iOS, and Android.

Poly Clariti SDK supports the building simple endpoint clients that can participate in audio/video conferences when using Poly Clariti Core and Poly Clariti Relay. It provides the foundation such that those applications can provide in-conference messaging/chat, voting, and current participant display (roster).

Operating System

The Oracle Linux 8.5 operating system running the Poly Clariti Relay, Poly Clariti Core, Poly Clariti Edge, and Poly Clariti Workflow Lite 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 several industry-leading security and vulnerability scan tools, as well as manual testing.

Security Settings

The Poly Clariti Core and Poly Clariti Edge software may reside within the customer enterprise network and/or in the DMZ. It communicates and responds to other devices and services on the network using specific ports (as configured by the customer).

Poly Clariti Relay software may reside within the customer enterprise network. It communicates only to Poly Clariti Core over an encrypted web socket or to endpoints signaled through Poly Clariti Core using encrypted web sockets and UDP RTP/SRTP on specific ports.

Poly Clariti Workflow Lite software should reside within the customer enterprise network. It communicates to Poly Clariti Core over an HTTPS connection, Active Directory, and Exchange.

When communicating with any device, service, and/or the system web interface, you can configure Poly Clariti Core and Poly Clariti Edge to use encrypted communication as well as the nature of that encryption (for example, protocols or ciphers). Poly Clariti Core and Poly Clariti Edge provide fine-grained security settings in its user interface so that customers can further harden security of Poly Clariti Core and Poly Clariti Edge as required for their environments.

The following are some of the options Poly Clariti Core Poly Clariti Edge and Poly Clariti Workflow Lite provide that the user can enable or disable:

- Console access
- SSH access
- Unencrypted connections to Active Directory, MCUs, and Exchange server
- Port level configuration for mutual TLS authentication
- Third-party applications to receive SIP RFC 4575 conference events
- Allow system to boot from a USB flash drive or optical drive
- Require endpoints to be provisioned for LDAP and XMPP access
- Allow LDAP access for non-TLS connections through access proxy
- Skip validation of certificates for inbound connections
- Allow forwarding of IPv6 ICMP destination unreachable messages
- Allow IPv6 CIMP echo reply messages to multicast addresses
- Ignore SIP *critical* privacy flag
- SSL 3.0
- TLS 1.0
- TLS 1.1
- TLS 1.2
- Use FIPS or non-FIPS cryptography modes
- Skip validation of certificates received while making outbound connections
- Refuse TLS connections with DHS key less than a specified size

In addition to these options, the user can select or deselect a wide variety of specific ciphers for management and signaling traffic for encrypted network connections.

Poly Clariti Relay offers fewer configuration options, being mostly stateless and more singularly focused.

However, the following options can be enabled or disabled:

- Console access
- SSH access
- Skip validation of certificates for inbound connections
- Use FIPS or non-FIPS cryptography modes

- Refuse TLS connections with DHS key less than a specified size

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

Poly Clariti Core and Poly Clariti Edge use certificates in the following ways:

- Poly Clariti Core and Poly Clariti Edge present certificates to the remote end. For example:
  - When a user logs in to the Poly Clariti Core, Poly Clariti Edge, or Poly Clariti Workflow Lite system web interface, Poly Clariti Core, Poly Clariti Edge, and Poly Clariti Workflow Lite offer a certificate to identify itself to the browser (client). The certificate must have been signed by a certificate authority, and the browser must be configured to trust that certificate authority. If trust can't be established, most browsers allow connection anyway and display a dialog to the user requesting permission.
  - When Poly Clariti Core, Poly Clariti Edge, or Poly Clariti Workflow Lite connect to a Microsoft Active Directory server, they may present a certificate to the server to identify themselves. If an Active Directory is configured to require a client certificate (for specific configuration information, please see the *Poly Clariti Core and Poly Clariti Edge Administrator Guide*), Poly Clariti Core and Poly Clariti Edge offer the same SSL server certificate that they offer to browsers connecting to the system web interface. Active Directory must be configured to trust the certificate authority, or it rejects the certificate, and the connection fails.
  - When Poly Clariti Core, Poly Clariti Edge, or Poly Clariti Workflow Lite connect to a Microsoft Exchange server (if the calendaring service is enabled), they may present a certificate to the server to identify themselves. Unless the **Allow unencrypted calendar notifications from Exchange server** security option is enabled, Poly Clariti Core, Poly Clariti Edge, and Poly Clariti Workflow Lite offer the same SSL server certificate that they offer to browsers connecting to the system management interface. Configure the Microsoft Exchange server to trust the certificate authority. Otherwise, **Microsoft Exchange Server** > **Integration status** remains **Subscription pending** indefinitely, Poly Clariti Core and Poly Clariti Edge system don't receive calendar notifications, and incoming meeting request messages are only processed approximately every 4 minutes.
- Poly Clariti Core and Poly Clariti Edge can validate the certificates of remote devices (mTLS - mutual TLS). For example:

- When Poly Clariti Core and Poly Clariti Edge connect to a Poly MCU configured for secure communications, a certificate may be used to identify the MCU (server) to Poly Clariti Core and Poly Clariti Edge (client). You can configure this option in Poly Clariti Core and Poly Clariti Edge.
- When performing call signaling requiring TLS, Poly Clariti Core and Poly Clariti Edge presents a certificate to the connecting client (one-way TLS). If the **Require mutual authentication (validation of client certificates) SIP Settings** option is enabled, both ends validate each other's certificates (mutual TLS).

Poly Clariti Relay uses certificates in the following ways:

- Poly Clariti Relay presents certificates to the remote end. For example:
  - When Poly Clariti Core and Poly Clariti Edge connect to the Poly Clariti Relay for API connections.
  - When an EVO endpoint connects to the signaling port on the Poly Clariti Relay.
- Poly Clariti Relay can validate the certificates of remote devices (mTLS - mutual TLS) for any inbound connection. Uncheck the box for **Security Settings > Skip validation of certificates for inbound connections** to enable mutual TLS.

Access Control Lists

Poly Clariti Core and Poly Clariti Edge provide the ability to configure access control lists (ACLs) for blocking incoming traffic (H.323 and SIP only).

Based on the configured criteria of ACLs, Poly Clariti Core and Poly Clariti Edge either processes the traffic or blocks 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 Poly Clariti Core and Poly Clariti Edge (edge or combo configuration).

Device, Call, and Conference Security

Poly Clariti Core and Poly Clariti Edge provide several security-related features for call signaling and conference management that the user can enable or disable:

- Device authentication (SIP, H.323, and EVO)
- Device registration policy
- Access lists (ACLs)
- Conference and chairperson passcode for virtual meeting rooms (VMRs)
- Support for media encryption
- Allow calls to inactive endpoints
- Allow calls from unregistered endpoints in territory
- Allow calls from unregistered endpoints out of territory

- Allow offerless INVITE to endpoints for SIP
- Accept H.323 neighbor requests only from specified external gatekeepers
- Dynamically block list signaling from hyperactive endpoints
- Remove inactive shared registrations after a specified number of days
- Authentication for SIP peer traffic
- TLS connection for SIP
- SIP traffic to/from authorized domains
- Authentication for external H.323 gatekeeper traffic
- Secure web sockets (WSS only for EVO)

Poly Clariti Core and Poly Clariti Edge 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, H.323, management, API access, media traversal, SIP, system ephemeral, TURN, and EVO.

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

Poly Clariti Relay provides the following security-related features:

- Support for media encryption
- Secure web sockets (WSS only for EVO signaling)

Encryption Protocols

The following table lists the encryption protocols used by Poly Clariti Core and Poly Clariti Edge.

Poly Clariti Core and Poly Clariti Edge Encryption Protocols

Application	Security Function	Description	Encryption Protocol
System passwords	Confidentiality Integrity	/etc/shadow	N/A
Poly Clariti Core and Poly Clariti Edge passwords	Confidentiality Integrity	Application passwords stored in database	N/A
SIPS	Confidentiality Integrity Authentication	SIP signaling (DiffieHellman key exchange)	TLS (NSS) SSLv3 TLS v1.0, v1.1, v1.2

HTTPS/WSS	Confidentiality Integrity Authentication	Web admin traffic REST API (DiffieHellman key exchange), or EVO signaling web sockets	TLS (NSS) SSLv3 TLS v1.0, v1.1, v1.2
Gatekeeper	Authentication Confidentiality	H.323 signaling	H.235 authentication
Data Encryption	Confidentiality Integrity	Licensing	N/A
Data Encryption	Confidentiality Integrity	Licensing Digital signatures: License Key	N/A
Data Encryption	Signature	Licensing Digital signatures: Cer8com's ECDSA	OpenSSL
Data Encryption	Signature	Licensing Digital signatures: OpenSSL's core cryptography library	OpenSSL
Data Encryption	Confidentiality Integrity	Trusted Storage: OpenSSL's core cryptography library	OpenSSL
Data Encryption	Confidentiality Integrity	Node-to-node communication	Custom with AES-128
TURN signal	Authentication	Allows the setup of media channels for video conferencing calls for products that are present outside the core network, that is, on the external side of firewall/NAT devices	UDP/TCP, which carries MD5 hashed authentication data and message integrity is protected by SHA1
Access proxy	Confidentiality	Provides video conferencing products outside the firewall (external to the network) the ability to connect to HTTPS, LDAP, and XMPP servers located inside the core network over encrypted TLS channels	Same as SIP Signal (Active)

VC2 provisioning proxy	Confidentiality	Provides provisioning of parameters for SIP registrar/proxy and user access details to the video conferencing products over encrypted TLS channels	Same as SIP Signal (Active)
SSH	Authentication Confidentiality	Provides a remote control/ management interface over an encrypted SSH channel	SSH v2.0
Tunnel (Encryption mode is disabled in Russia release)	Authentication Confidentiality	Provides a dedicated connection between two OpenVPN-enabled devices, such as two Poly Clariti Core and Poly Clariti Edge systems, residing on either side of the firewall to minimize impacts to firewall policies and still provide connectivity for video conferencing products	AES-256, AES-128 UDP or TCP

Poly Clariti Relay uses TLS 1.2 for both the HTTPS/WSS Poly EVO web socket signaling and management API connections. It supports AES-128 to AES-256 with DTLS key exchange for SRTP media encryption.

Poly Clariti App (Mobile and Web) and Poly Clariti Roster always use standard WebRTC browser mechanisms, which are HTTPS+TLS 1.2 for the secure web socket connections and AES-128 with DTLS-SRTP key exchanges for media encryption. There’s no way to disable the encryption for the web applications per WebRTC browser specifications.

Poly Clariti App (Mobile and Web) and Poly Clariti Roster only use the HTTPS/WSS configured ports on Poly Clariti Core to establish the Poly EVO signaling connections and the RTP ports configured on Poly Clariti Relay for the media. There may or may not be ephemeral ports the browsers themselves use on the local client machines to perform the WebRTC and media functions (signaling and SRTP media), but that is beyond the scope of this document.

Poly Clariti SDK uses TLS 1.2 for both the HTTPS and WSS Poly EVO web socket signaling. It supports AES-128 to AES-256 for SRTP/SRTCP media and control encryption.

Poly Clariti Workflow Lite Encryption Protocols

Application	Security Function	Description	Encryption Protocol
System passwords	Confidentiality Integrity	/etc/shadow	N/A

Poly Clariti Workflow Lite passwords	Confidentiality Integrity	Application passwords stored in database	N/A
HTTPS/WSS	Confidentiality Integrity Authentication	Web admin traffic REST API (DiffieHellman key exchange)	TLS (NSS) SSLv3 TLS v1.0, v1.1, v1.2
Data Encryption	Confidentiality Integrity	Licensing	N/A
Data Encryption	Confidentiality Integrity	Licensing Digital signatures: License Key	N/A
Data Encryption	Signature	Licensing Digital signatures: Cer8com's ECDSA	OpenSSL
Data Encryption	Signature	Licensing Digital signatures: OpenSSL's core cryptography library	OpenSSL
Data Encryption	Confidentiality Integrity	Trusted Storage: OpenSSL's core cryptography library	OpenSSL
Data Encryption	Confidentiality Integrity	Node-to-node communication	Custom with AES-128
SSH	Authentication Confidentiality	Provides a remote control/ management interface over an encrypted SSH channel	SSH v2.0

Management Access

Poly Clariti Core and Poly Clariti Edge are designed to use multiple network interfaces, which allow 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 Poly Clariti Core and Poly Clariti Edge system web interface 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, users can view specific pages.

The following table describes the user roles.

User Roles

Role	Description
Administrator	Responsible for the overall administration of the system. Can access all the management user interface pages except those reserved for auditors. Must be an enterprise user to see enterprise reports, enterprise users, and groups.
Auditor	Responsible for configuring and logging history record retention and managing logs. Can access all history reports.
Provisioner	Responsible for managing Conferencing User accounts. Can only create or modify users that have the Conferencing User role but can view all local users. Can view history reports. Must be an enterprise user to view all enterprise users.
Conferencing User	Provisioned with a conference room (virtual meeting room) or rooms and can host conferences. Can’t access the management user interface. Automatically present on all user accounts. Not listed under Available Roles or explicitly assigned.

The following additional capabilities are provided for the management of the local user accounts:

- Account lockout – Failed login threshold and window
- User account lockout duration
- Account inactivity
- Password aging
- Password complexity

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

For additional security, users can enable management access settings and provide the list of IP addresses of machines that can access the system web interface or the REST APIs of for Poly Clariti Core and Poly Clariti Edge.

As Poly Clariti Core and Poly Clariti Edge run the Linux operating system, users can change the Linux root (`root`) as well as remote (`dmaremote`) user passwords for console and SSH access if enabled.

Poly Clariti Relay uses a proprietary protocol over an authenticated secure web socket connection as its management interface. Once Poly Clariti Core connects to Poly Clariti Relay, settings for Poly Clariti Relay can be altered through the Poly Clariti Core system web interface. The authentication credentials for this connection can only be changed from the Poly Clariti Core, when the Poly Clariti Relay isn't in service.

Poly Clariti Relay also runs the Linux operating system, and users can likewise change the root and remote user passwords for the console and SSH access (if enabled) from either the Linux command line or from the User Management settings for the Poly Clariti Relay, when the Poly Clariti Relay isn't in service.

Reporting

Poly Clariti Core and Poly Clariti Edge have extensive reporting capability and provide the user with the following reports:

- Registration history
- Call history
- Conference history
- ACL denials
- Remote syslog
- Audit logs
- CDRs
- SNMP monitoring

All reporting for the Poly Clariti Relay is done via Poly Clariti Core except for application logs, which can be accessed through the Poly Clariti Core system web interface. No other reporting or data is stored on Poly Clariti Relay.

Ports Summary

The following table lists the default port settings that Poly Clariti Core and Poly Clariti Edge use for communication with other devices.

ICMP (ping) is useful between all private network devices and for public network diagnostics. If you have Poly Clariti Manager managing Poly Clariti Core and Poly Clariti Edge, then you must enable ICMP between the two servers.

Note that this table is intended as general guidance, and ports may vary depending on specific configurations and/or services used.

Poly Clariti Core and Poly Clariti Edge Inbound and Outbound Ports

Source IP	Source Port	Destination IP	Destination Port	Protocol	Direction	Poly Clariti Core and Poly Clariti Edge Configuration	Interface	Description
Any Public IP	Any	Access proxy services-public interface IP	389, 443, 5222, 9950 - 9999	TCP/UDP (either or both)	Inbound	Edge or Combo	Access proxy services-public	Access proxy ports depending on configured instances
Access proxy services-private interface IP	10000 – 13000	Any Private IP	Any	TCP/UDP (either or both)	Outbound	Edge or Combo	Access proxy services-private	Access proxy dynamic ports
Access proxy services-private interface IP	>1023	Poly Clariti Manager	389, 443, 5222	TCP	Outbound	Edge or Combo	Access proxy services-private	Access proxy (private) communication with Clariti Manager
Any Private IP	>1023	Media traversal services private interface IP	40002 – 50998	TCP/UDP	Inbound	Edge or Combo	Media traversal services-private	Media traversal (private) For a single-NIC deployment of a Poly Clariti Core and Poly Clariti Edge or combo system, media Poly Clariti Relay uses both public and private ports
Media traversal services private interface IP	40002 – 50998	Any Private IP	>1023	TCP/UDP	Outbound	Edge or Combo	Media traversal services-private	Media traversal (private) For a single-NIC deployment of a Poly Clariti Core and Poly Clariti Edge or combo system, media Poly Clariti Relay uses both public and private ports

Source IP	Source Port	Destination IP	Destination Port	Protocol	Direction	Poly Clariti Core and Poly Clariti Edge Configuration	Interface	Description
Any Public IP	>1023	Media traversal services public interface IP	23002 – 33998	TCP/UDP	Inbound	Edge or Combo	Media traversal services-public	Media traversal (public) For a single-NIC deployment of a Poly Clariti Core and Poly Clariti Edge or combo system, media Poly Clariti Relay uses both public and private ports
Media traversal services public interface IP	23002 – 33998	Any Public IP	>1023	TCP/UDP	Outbound	Edge or Combo	Media traversal services-public	Media traversal (public) For a single-NIC deployment of a Poly Clariti Core and Poly Clariti Edge or combo system, media Poly Clariti Relay uses both public and private ports
Any Public IP	>1023	TURN services public interface IP	60002 – 65535	UDP	Inbound	Edge or Combo	TURN services - public	TURN relay
TURN services public interface IP	60002 – 65535	Any Public IP	>1023	UDP	Outbound	Edge or Combo	TURN Services-public	TURN relay
Any Private IP	>1023	TURN services private interface IP	60002 – 65535	UDP	Inbound	Edge or Combo	TURN services-private	TURN relay
TURN services private interface IP	60002 – 65535	Any Private IP	>1023	UDP	Outbound	Edge or Combo	TURN Services-private	TURN relay
Any Public IP	>1023	TURN services public interface IP	3478	UDP	Inbound	Edge or Combo	TURN services-public	TURN
Any Private IP	>1023	TURN services private interface IP	3478	UDP	Inbound	Edge or Combo	TURN Services-private	TURN

Source IP	Source Port	Destination IP	Destination Port	Protocol	Direction	Poly Clariti Core and Poly Clariti Edge Configuration	Interface	Description
Any Public IP	>1023	Signaling services public interface IP	1719	UDP	Inbound	Edge or Combo	Signaling services-public	H.323 RAS
Any Private IP	>1023	Signaling services private interface IP	1719	UDP	Inbound	Edge, Core, or Combo	Signaling services-private	H.323 RAS
Signaling services public interface IP	1719, 52000 – 60000	Any Public IP	1719	UDP	Outbound	Edge or Combo	Signaling services-public	H.323 RAS
Signaling services private interface IP	1719, 52000 – 60000	Any Private IP	1719	UDP	Outbound	Edge, Core, or Combo	Signaling services-private	H.323 RAS
Any Public IP	Any	Signaling services public interface IP	1718	UDP	Inbound	Edge or Combo	Signaling services-public	Optional H.323 RAS; gatekeeper discovery (multi- and unicast)
Any Private IP	Any	Signaling services public interface IP	1718	UDP	Inbound	Edge, Core, or Combo	Signaling services-private	Optional H.323 RAS; gatekeeper discovery (multi- and unicast)
Any Public IP	>1023	Signaling services public interface IP	1720	TCP	Inbound	Edge or Combo	Signaling services-public	H.323, H.225
Any Private IP	>1023	Signaling services private interface IP	1720	TCP	Inbound	Edge, Core, or Combo	Signaling services-private	H.323, H.225
Signaling services public interface IP	52000 – 60000	Any Public IP	1720	TCP	Outbound	Edge or Combo	Signaling services-public	H.323, H.225
Signaling services private interface IP	52000 – 60000	Any Private IP	1720	TCP	Outbound	Edge, Core, or Combo	Signaling services-private	H.323, H.225
Signaling services public interface IP	35001 – 40000	Any Public IP	>1023	TCP	Outbound	Edge or Combo	Signaling services-public	H.323 dynamic ports (H.245)

Source IP	Source Port	Destination IP	Destination Port	Protocol	Direction	Poly Clariti Core and Poly Clariti Edge Configuration	Interface	Description
Signaling services private interface IP	35001 – 40000	Any Private IP	>1023	TCP	Outbound	Edge, Core, or Combo	Signaling services-private	H.323 dynamic ports (H.245)
Any Public IP	>1023	Signaling services public interface IP	35001 – 40000	TCP	Inbound	Edge or Combo	Signaling services-public	H.323 dynamic ports (H.245)
Any Private IP	>1023	Signaling services private interface IP	35001 – 40000	TCP	Inbound	Edge, Core, or Combo	Signaling services-private	H.323 dynamic ports (H.245)
Signaling services private interface IP	5060, 5061, 13001 – 23000	Any Private IP	>1023	TCP/UDP	Outbound	Edge, Core, or Combo	Signaling services-private	SIP outbound ports (private)
Signaling services public interface IP	5060, 5061, 13001 – 23000	Any Public IP	>1023	TCP/UDP	Outbound	Edge or Combo	Signaling services-public	SIP outbound ports (public)
Any Public IP	>1023	Signaling services public interface IP	5060	TCP/UDP	Inbound	Edge or Combo	Signaling services-public	SIP signaling (default); other ports can be configured in **SIP Settings**
Any Public IP	>1023	Signaling services public interface IP	5061	TCP	Inbound	Edge or Combo	Signaling services-public	SIP signaling TLS (default); other ports can be configured in **SIP Settings**
Any Private IP	>1023	Signaling services private interface IP	5060	TCP/UDP	Inbound	Edge, Core, or Combo	Signaling services-private	SIP signaling (default); other ports can be configured in **SIP Settings**
Any Private IP	>1023	Signaling services private interface IP	5061	TCP	Inbound	Edge, Core, or Combo	Signaling services-private	SIP signaling TLS (default); other ports can be configured in **SIP Settings**

Source IP	Source Port	Destination IP	Destination Port	Protocol	Direction	Poly Clariti Core and Poly Clariti Edge Configuration	Interface	Description
Signaling services public interface IP	>1023	Customerusage datacollection. polycom.com	8443	TCP	Outbound	Edge, Core, or Combo	Signaling services-public	Signaling services (public) communication with Poly Analytics Service
Signaling services private interface IP	>1023	RealPresence ContentConnect	8443	TCP	Outbound	Core or Combo	Signaling services-private	Signaling services (private) communication with Poly ContentConnect
Signaling services private interface IP	>1023	RealPresence ContentConnect	5060, 5061	TCP	Outbound	Core or Combo	Signaling services-private	Signaling services (private) communication with Poly ContentConnect
RealPresence ContentConnect	>1023	Signaling services private interface IP	5060, 5061	TCP	Inbound	Core or Combo	Signaling services-private	Signaling services (private) communication with Poly ContentConnect
Other Poly Clariti Core and Poly Clariti Edge nodes Management services IPs	8989	Management services interface IP	8989	UDP	Inbound	Edge, Core, or Combo	Management services	Supercluster communication (core) HA communication (edge, core, or combo)
Management services interface IP	8989	Other Poly Clariti Core and Poly Clariti Edge nodes Management services IPs	8989	UDP	Outbound	Edge, Core, or Combo	Management services	Supercluster communication (core) HA communication (edge, core, or combo)
Management services interface IP	52000 – 60000	DNS Servers	53	TCP/UDP	Outbound	Edge, Core, or Combo	Management services	DNS queries.
Any Private IP	Any	Management services interface IP	80	TCP	Inbound	Edge, Core, or Combo	Management services	HTTP. Redirects to 8443 (HTTP access isn’t allowed)
Any Private IP	Any	Management services interface IP	8080	TCP	Inbound	Edge, Core, or Combo	Management services	HTTP. Redirects to 8443 (HTTP access isn’t allowed)

Source IP	Source Port	Destination IP	Destination Port	Protocol	Direction	Poly Clariti Core and Poly Clariti Edge Configuration	Interface	Description
								Used for uploading upgrade packages and backups; during upgrades, the progress page is served from this port
Any Private IP	Any	Management services interface IP	443	TCP	Inbound	Edge, Core, or Combo	Management services	HTTPS; redirects to 8443 Management interface access
Any Private IP	Any	Management services interface IP	8443	TCP	Inbound	Edge, Core, or Combo	Management services	Management/API
Management services interface IP	52000 – 60000	Any Private IP	8443	TCP	Outbound	Edge, Core, or Combo	Management services	Management/API
Management services interface IP	52000 – 60000	Active Directory Server	3268, 3269	TCP	Outbound	Edge, Core, or Combo	Management services	Active Directory integration Global Catalog
Management services interface IP	52000 – 60000	Active Directory server IP	389	TCP	Outbound	Edge, Core, or Combo	Management services	LDAP Active Directory Integration
Management services interface IP	52000 – 60000	Microsoft Active Directory Server IP	636	TCP	Outbound	Edge, Core, or Combo	Management services	Microsoft Active Directory integration
Management services interface IP	514, 52000 – 60000	Syslog server IP	514	UDP/TCP	Outbound	Edge, Core, or Combo	Management services	Log forwarding
Management services interface IP	123, 52000 – 60000	NTP Server IP	123	UDP	Outbound	Edge, Core, or Combo	Management services	NTP (private only); available only if an NTP server is specified in **Time Setting**s
Management services interface IP	52000 – 60000	Clariti Manager IP	3333, 9333	TCP	Outbound	Edge, Core, or Combo	Management services	Poly Clariti Manager licensing; licensing on Poly Core Edge is optional

Source IP	Source Port	Destination IP	Destination Port	Protocol	Direction	Poly Clariti Core and Poly Clariti Edge Configuration	Interface	Description
Any Private IP	Any	Management services interface IP	161	UDP	Inbound	Edge, Core, or Combo	Management services	SNMP (private only); default port; can be changed or disabled
Management services interface IP	162, 52000 – 60000	SNMP Trap Receiver IP	162	TCP/UDP	Outbound	Edge, Core, or Combo	Management services	SNMP notifications (Traps or Informs) Used if SNMP is enabled and configured to send notifications, or if system is monitored with Poly Clariti Manager
Any Private IP	>1023	Management services interface IP	22	TCP	Inbound	Edge, Core, or Combo	Management services	SSH (private only); only available if Linux console access is enabled
Management services interface IP	>1023	RealPresence Collaboration Server management IP	80, 8080, 443	TCP	Outbound	Core or Combo	Management services	Management services communication with RealPresence Collaboration Server
Poly ContentConnect IP	443	Management services interface IP	8443	TCP (TLS)	Inbound	Core or Combo	Management services	Poly ContentConnect communication
Management services interface IP	8443	Poly ContentConnect IP	443	TCP (TLS)	Outbound	Core or Combo	Management services	Poly ContentConnect communication
Res IP	>1023	Management services interface IP	4449	TCP	Inbound	Core or Combo	Management services	Legacy LDAP port for Poly CMA and Clariti Manager integration
Management services interface IP	5986, 52000 – 60000	Windows Active Directory server IP	5986	TCP (TLS)	Outbound	Core or Combo	Management services	WinRM 2.0 communication during Poly contact creation in Active Directory
Any Private IP	Any	Management services interface IP	53	TCP/UDP	Inbound	Core	Management services	DNS; only available if the embedded DNS server is enabled

You can configure Poly Clariti Core and Poly Clariti Edge in different ways with a variety of services enabled or disabled. Due to the configurable nature of Poly Clariti Core and Poly Clariti Edge, required ports may vary. The Poly Clariti Core and Poly Clariti Edge system web interface provides a list of all configured ports (**Service Config** > **System Port Ranges**). From the **System Port Ranges** page, a firewall administrator can determine which ports Poly Clariti Core and Poly Clariti Edge use for its configuration and for which services.

Poly Clariti Workflow Lite Inbound and Outbound Ports

Source IP	Source Port	Destination IP	Destination Port	Protocol	Direction	Interface	Description
Signaling services public interface IP	>1023	Customerusage datacollection. polycom.com	8443	TCP	Outbound	Signaling services- public	Signaling services (public) communication with Poly Analytics Service
Other Poly Clariti Core and Poly Clariti Edge nodes Management services IPs	8989	Management services interface IP	8989	UDP	Inbound	Management services	HA communication
Management services interface IP	8989	Other Poly Clariti Core and Poly Clariti Edge nodes Management services IPs	8989	UDP	Outbound	Management services	HA communication
Management services interface IP	52000 – 60000	DNS Servers	53	TCP/UDP	Outbound	Management services	DNS queries.
Any Private IP	Any	Management services interface IP	80	TCP	Inbound	Management services	HTTP. Redirects to 8443 (HTTP access isn't allowed)
Any Private IP	Any	Management services interface IP	8080	TCP	Inbound	Management services	HTTP. Redirects to 8443 (HTTP access isn't allowed) Used for uploading upgrade packages and backups; during upgrades, the progress page is served from this port
Any Private IP	Any	Management services interface IP	443	TCP	Inbound	Management services	HTTPS; redirects to 8443 Management interface access

Source IP	Source Port	Destination IP	Destination Port	Protocol	Direction	Interface	Description
Any Private IP	Any	Management services interface IP	8443	TCP	Inbound	Management services	Management/API
Management services interface IP	52000 – 60000	Any Private IP	8443	TCP	Outbound	Management services	Management/API
Management services interface IP	52000 – 60000	Active Directory Server	3268, 3269	TCP	Outbound	Management services	Active Directory integration Global Catalog
Management services interface IP	52000 – 60000	Active Directory server IP	389	TCP	Outbound	Management services	LDAP Active Directory Integration
Management services interface IP	52000 – 60000	Microsoft Active Directory Server IP	636	TCP	Outbound	Management services	Microsoft Active Directory integration
Management services interface IP	514, 52000 – 60000	Syslog server IP	514	UDP/TCP	Outbound	Management services	Log forwarding
Management services interface IP	123, 52000 – 60000	NTP Server IP	123	UDP	Outbound	Management services	NTP (private only); available only if an NTP server is specified in **Time Settings**
Any Private IP	Any	Management services interface IP	161	UDP	Inbound	Management services	SNMP (private only); default port; can be changed or disabled
Management services interface IP	162, 52000 – 60000	SNMP Trap Receiver IP	162	TCP/UDP	Outbound	Management services	SNMP notifications (Traps or Informs) Used if SNMP is enabled and configured to send notifications, or if system is monitored with Poly Clariti Manager
Any Private IP	>1023	Management services interface IP	22	TCP	Inbound	Management services	SSH (private only); only available if Linux console access is enabled

Source IP	Source Port	Destination IP	Destination Port	Protocol	Direction	Interface	Description
Management services interface IP	>1023	RealPresence Collaboration Server management IP	80, 8080, 443	TCP	Outbound	Management services	Management services communication with RealPresence Collaboration Server
Poly ContentConnect IP	443	Management services interface IP	8443	TCP (TLS)	Inbound	Management services	Poly ContentConnect communication
Management services interface IP	8443	Poly ContentConnect IP	443	TCP (TLS)	Outbound	Management services	Poly ContentConnect communication
Any Private IP	Any	Management services interface IP	53	TCP/UDP	Inbound	Management services	DNS; only available if the embedded DNS server is enabled

Media Port Ranges and Security

Poly Clariti Edge and Poly Clariti Relay use several media ports to carry audio and video media traffic. The UDP media ports must be open on the firewall for all call signaling types (Poly EVO, SIP, H.323) and are necessary to carry RTP/SRTP/STUN/DTLS media traffic. Each call to a Poly Clariti Edge or Poly Clariti Relay uses one or more of the media ports.

Poly Clariti Edge and Poly Clariti Relay employ the latest firewall and security design technologies for the open media ports. Services that use the ports only allow traffic that has been negotiated by secure signaling and the traffic is constantly monitored while the ports are in use.

Centralizing all media traffic to a known set of devices (Poly Clariti Edge and Poly Clariti Relay), especially at the edge of a customer’s network (Poly Clariti Edge), allows corporate firewall administrators to employ strict and specific firewall rules for traffic to and from only these devices. By using only transparent and industry standard media protocols (RTP/SRTP/STUN/DTLS), no hidden traffic passes over the ports. This enables inspection of corporate firewall rules and network scanners and monitors to be seamlessly integrated into the Poly Clariti Edge and Poly Clariti Relay solution for even greater security assurance.

The overall design provides essential security confidence when using wider media port ranges and delivers the highest level of call quality.

A greater number of simultaneous calls requires more ports to be open, so decreasing the number of open ports may reduce the number of concurrent calls that can take place.

The following table provides an estimate on how to calculate required ports:

Calculations for the Number of Required Ports

Information Type	H.323 Dynamic Ports	SIP Dynamic Ports (public)	SIP Dynamic Ports (private)	Media Traversal Dynamic Ports (public) (edge or combo config)	Media Traversal Dynamic Ports (private) (edge or combo config)	Access Proxy (edge or combo config)	System Ephemeral
Ports used per call	3	3	3	10	10	N/A	N/A
Number of calls	X	X	X	X	X	N/A	N/A
Total ports required	3x	3x	3x	10x	10x	3000	3000

The following table lists the inbound and outbound ports for Poly Clariti Relay:

Poly Clariti Relay Inbound and Outbound Ports

Service	Relay Port	Destination IP	Destination Port	Protocol	Direction	Description
Management/API	Any Core Ephemeral	Relay	8443	HTTPS/WSS TLS 1.2	Inbound	Management/API connection from Poly Clariti Core to Poly Clariti Relay
Poly EVO Signaling	8090	Relay	8090	WSS TLS 1.2	Inbound	Poly EVO from endpoints
Media	10000 - 3000	Endpoint	Any	UDP (RTP, RTCP, SRTP, SRTCP)	Outbound	RTP media traffic outbound

Media*	10000 - 3000	Relay	Any	UDP (RTP, RTCP, SRTP, SRTCP)	Inbound	RTP media traffic inbound

* Media ports utilization:

- Total media ports used per SIP call = (Audio RTP/RTCP (2 ports) + People RTP/RTCP (2 ports) + Content(2 ports) RTP/RTCP + SCP. (2 ports) RTP/RTCP + BFCP (2 ports)) * 2 = 20
- Total media ports used per EVO call = 1
- Poly Clariti Relay reserves twice the number of media ports required for each SIP call (i.e. for each SIP call, 20 UDP ports for media are reserved). This is because the operating system doesn't release ports immediately when a call ends.
- Poly Clariti Relay reserves the higher number of media ports per call (that is, 20) assuming a worst case scenario of 100% SIP calls.

Poly Clariti App (Mobile and Web) and Poly Clariti Roster only use the HTTPS/WSS configured ports on Poly Clariti Core to establish the signaling connections and the RTP ports configured on Poly Clariti Relay for the media. There may or may not be ephemeral ports the browsers themselves use on the local client machines to perform the WebRTC functions (signaling and SRTP media), but that is beyond the scope of this document.

Poly Clariti SDK only uses the HTTPS/WSS configured ports on Poly Clariti Core to establish the Poly EVO signaling connections and the RTP ports configured on Poly Clariti Relay for the media.

Privacy-Related Options

This section provides information on privacy-related options for Poly Clariti Core, Poly Clariti Edge, and Poly Clariti Relay.

How to Turn Off Analytics or Send Usage Data

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, and names, before Poly Clariti Core and Poly Clariti Edge 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 100 KB of data per hour is collected and sent. Poly's collection and use of this data complies with *Poly's Privacy Policy*.

The user can allow or disallow the automatic sending of usage data at any time. Poly Clariti Core and Poly Clariti Edge require HTTPS port 8443 to be open to send usage data across the internet. Poly Clariti Relay doesn't require any open ports as it sends information through Poly Clariti Core. 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 system web interface.

Analytics exclude all information that identifies individual people or an individual's habits. For example, user names, device aliases, and certain description fields aren't uploaded. Analytics don't upload data that could compromise the security of customer environments. For example, host names, internal IP addresses, user names and passwords aren't uploaded. Customer-specific data is pseudonymized. Analytics only store the Poly serial number/ unique identifier, MAC address of the system running analytics, and the public internet IP address from where the data was sent.

The analytics data is 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 guide 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. 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 system web interface requires each user to be granted individual access.

Poly may share customer information with service providers, contractors, or other third parties to assist in providing and improving the service. All sharing of information is carried out consistent with the *Poly Privacy Policy*.

Poly Clariti App(Mobile and Web) provides an optional anonymous call survey at the end of each call. Should the user wish to submit, this 1-to-5 star quality rating plus an optional note is sent to Poly servers to help improve services. It contains no identifiable or trackable information if submitted.

Call Detail Report (CDR)

Poly Clariti Core and Poly Clariti Edge generate call detail records (CDRs) for all calls and conferences, which you can download.

After you unzip the download file, you can open the two `.csv` files it contains (one for calls and one for conferences) with Microsoft Excel or another spreadsheet application. The `.csv` files contain a line for each call or conference that ended during the selected time frame.

The `.zip` file also includes a text file that contains a single line specifying the following information:

- The number of calls in the call CDR file
- The number conferences in the conference CDR file
- The clusters whose calls and conferences are included in the CDR file
- The clusters whose calls and conferences are excluded from the CDR file because those clusters weren't reachable when the CDR export was generated

For more information, see *Export CDR Data* in the *Poly Clariti Core, Poly Clariti Edge and Poly Clariti Relay Administrator Guide available on Poly Support*.

Recent Call List

You can view the recent calls and conferences as well as the details on the Poly Clariti Core and Poly Clariti Edge system web interface.

The recent calls and conference list include the following information:

- Originator
- Dial string
- Destination
- Start Time
- End Time
- Ingress Cluster
- Call ID
- Conference Room ID

For more information, see *View Call History* in the *Poly Clariti Core, Poly Clariti Edge and Poly Clariti Relay Administrator Guide available on Poly Support*.

Local Administrator

Poly Clariti Core and Poly Clariti Edge system administrators are responsible for the installation and ongoing maintenance of the system.

The administrator should be familiar with the following configurations, tasks, and operations:

- Installing licenses when the system is first installed and when additional call capacity is added.
- Monitoring system health and performing the recommended regular maintenance.
- Using the system tools provided to aid with system and network diagnostics, monitoring, and troubleshooting. Should the need arise, Poly Global Services personnel may ask you to run these tools.
- Upgrading the system when upgrades/patches are made available.

At installation, the default local administrator login ID and password are set. Poly strongly recommends changing the default password from the system web interface. Additional user logins with administrative privileges can be created.

Likewise, Poly Clariti Relay has a single administrative user, which Poly Clariti Core uses to establish a connection. Changing the administrative account can only be accomplished from the Poly Clariti Core when the Poly Clariti Relay in not in service.

Active Directory Integration

Poly Clariti Core and Poly Clariti Edge support integration with an Active Directory server. This simplifies the task of deploying conferencing to a large organization. All Poly Clariti Core and Poly Clariti Edge access to the Active Directory server is read-only and minimally impacts the directory performance.

Active Directory integration automatically makes the enterprise users (directory members) Conferencing Users in Poly Clariti Core and Poly Clariti Edge, and it can assign each of them a conference room (virtual meeting room, or VMR). The conference room IDs are typically generated from the enterprise users' phone numbers. Creating conference rooms for enterprise users is optional. You can integrate with Active Directory to load user and group information into Poly Clariti Core and Poly Clariti Edge without giving all users the ability to host conferences. You can manually add conference rooms for selected users at any time.

You can assign Poly Clariti Core and Poly Clariti Edge roles to an enterprise group, applying the roles to all members of the group and enabling them to log in to Poly Clariti Core and Poly Clariti Edge system web interface with their standard network user names and passwords.

Enterprise groups can have their own conference templates that provide a custom conferencing experience. They can also have their own MCU pool order, which preferentially routes conferences to certain MCUs.

Once Poly Clariti Core and Poly Clariti Edge are integrated with Active Directory, they read the directory information nightly, so that user and group information is updated automatically as people join and leave the organization. The systems cache certain data from an Active Directory. In a superclustered system, one cluster is responsible for updating the cache, which is shared with all the clusters.

Between updates, clusters access the directory only to authenticate passwords (for instance, for the system web interface login); all other user information (such as user search results) comes from the cache. You can manually update the cache at any time.

Downloading Logs

The Poly Clariti Core and Poly Clariti Edge system web interface provides the administrator the ability to download system log files. The administrator can download active logs, individual logs, and archived logs. Current Poly Clariti Relay logs may also be downloaded through the Poly Clariti Core system web interface. The administrator can view the download history of log files and delete log archives.

For more information, see *Download Logs* in the *Poly Clariti Core, Poly Clariti Edge and Poly Clariti Relay Administrator Guide available on Poly Support.*

How Data Subject Rights Are Supported

The following information shows how data subject rights are supported.

Right to Access

A data subject has the right to view and/or obtain a copy of all personal data for a specific data subject. Personal data about specific participants in conferences can be viewed or downloaded via the CDR.

A copy of any personal data made available to Poly when working with Poly support is available by requesting it from your Poly support representative.

For more information, see *Export CDR Data* in the *Poly Clariti Core, Poly Clariti Edge and Poly Clariti Relay Administrator Guide available on Poly Support*.

Right to Be Informed

What Personal Data Is Collected?

Data Collection Within Poly Clariti Core and Poly Clariti Edge

Poly Clariti Core and Poly Clariti Edge don't access any customer data except as required to enable the features provided by the applications. As these systems are deployed in the customer's environment, it's the responsibility of the customer to protect data privacy.

Poly Clariti Core and Poly Clariti Edge 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)

If you're an individual user and the purchase of Poly Clariti Core and Poly Clariti Edge has been made by your employer as the customer, all the privacy information relating to personal data in this guide is subject to your employer's privacy policies as the controller of such personal data.

Data Collection Within Poly Clariti Relay

Data collection and storage within Poly Clariti Relay is intentionally kept to a minimum. The product is designed to be mostly stateless except for some basic network and administrative security configurations. Once a call or conference ends, the only data incidentally retained on Poly Clariti Relay is basic call metadata inside of application logs, which are automatically removed after a short period of time. These logs are only accessible via the secure administrative interface on Poly Clariti Core or via the secure shell/console (if enabled).

Data Collection Within Poly Clariti App(Mobile and Web) and Poly Clariti Roster

Data collection and storage within Poly Clariti App and Poly Clariti Roster is also intentionally kept to a minimum. The product is designed to keep a minimum set of information necessary to deliver the video service and diagnose technical issues.

Data Collection Within Poly Clariti SDK

Data collection and storage within Poly Clariti SDK is intentionally kept to a minimum. The SDK framework is designed to keep a minimum set of information necessary to deliver the video service and diagnose technical issues.

How Is Personal Data Used?

Poly Clariti Core and Poly Clariti Edge Personal Data Processing

Personal Data Category	Type of Personal Data	Purpose of Processing
Administrative user and customer operator profiles	Name Email address (optional) Password (hashed) SIP URI System name System owner IP address MAC address	Authenticate and authorize administrative access to the service Deliver video service Reporting Usage/activity
Call participant personal data	Name Email address (optional) Phone number Display name SIP URI IP address Dial string	Deliver video service Diagnose technical issues Conduct analytics and analysis to improve the technical performance of the service Respond to customer support requests Serial number for entitlement

Device information	Device name IP address MAC address Serial number	Deliver video service Diagnose technical issues Conduct analytics and analysis to improve the technical performance of the service Respond to customer support requests Serial number for entitlement
Usage information	Activity logs Call detail records	Deliver video service Diagnose technical issues Conduct analytics and analysis to improve the technical performance of the service Respond to customer support requests Serial number for entitlement

Poly Clariti App (Mobile and Web) and Poly Clariti Roster Personal Data Processing

Personal Data Category	Type of Personal Data	Purpose of Processing
Call participant personal data	User name Display name	Deliver video service Diagnose technical issues

Poly Clariti Mobile App (Web and Mobile) Personal Data Processing

Personal Data Category	Type of Personal Data	Purpose of Processing
Call participant personal data	User name Display name IP Address Activity Logs	Deliver video service Diagnose technical issues

Poly Clariti SDK Personal Data Processing

Personal Data Category	Type of Personal Data	Purpose of Processing
Call participant personal data	User name Display name IP Address Activity Logs	Deliver video service Diagnose technical issues

How Long Is Personal Data Kept?

Poly may retain customer data for as long as needed to provide the customer support for the Poly Clariti Core and Poly Clariti Edge product. Normally, analytics have a five-year retention policy. When a customer makes a request for deletion (`privacy@poly.com`), Poly will delete the requested data within 30 days, unless the data is required to be retained for Poly's legitimate interests or if needed to provide the service to customer.

Is Personal Data Shared with Any Third Parties and If So, Who?

Personal Data Sharing Within Poly Clariti Core, Poly Clariti Edge, and Poly Clariti Relay

To continually improve the product, Poly collects data to understand how customers use Poly Clariti Core, Poly Clariti Edge, and Poly Clariti Relay.

By collecting this data, Poly can identify system level utilization and the combined use of Poly Clariti Core and Poly Clariti Edge features. This data informs Poly which features are important and are actually used on your system. Poly uses this information to help guide future development and testing. Your decision to enable or not enable the sending of this data doesn't affect the availability of any documented system feature in any way. Enabling this feature doesn't affect the capacity or responsiveness of Poly Clariti Core and Poly Clariti Edge to process calls and conferences, nor does it affect access to the system web interface or API interactions.

The system sends usage data once per hour over a secured (TLS) connection (port 8443) to a Poly collection point (`customerusagedatacollection.Poly.com`). There's no access by any customer or others to view the data received at the collection point. The raw data is viewable only by Poly and the system administrators of each Poly Clariti Core and Poly Clariti Edge 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
- Number of users, endpoints, sites, MCUs, external gatekeepers, SIP peers, and SBCs
- Registrations and call/conference statistics (CDRs, registration, and call history)
- Security settings

How Can a Data Subject Be Notified of a Data Breach?

Data subjects have a right to be notified when their data has been processed without authorization. Contact your system administrator for the most appropriate method to receive this information.

Right to Data Portability

A data subject has the right to receive a copy of all personal data in a commonly-used, machine-readable format.

Data Portability within Poly Clariti Core, Poly Clariti Edge and Poly Clariti Relay

Poly Clariti Core and Poly Clariti Edge system administrators can:

- Download CDRs in `.csv` format.
- Download log files in plain-text format.

For more information, see *Export CDR Data* and *Download Logs* in the *Poly Clariti Core, Poly Clariti Edge and Poly Clariti Relay Administrator Guide available on Poly Support*.

Data Portability within Poly Clariti App (Mobile and Web) and Poly Clariti Roster

Poly Clariti App (Mobile and Web) and Poly Clariti Roster users can download log files in plain-text format**.**

Data Portability within Poly Clariti SDK

Poly Clariti SDK users can download log files in plain-text format.

For more information, see *Download Logs* in the *Poly Clariti App User Guide* available on *Poly Support*.

Right to Erasure

A data subject has the right to remove all his or her own personal data.

Poly may retain customer data for as long as needed to provide the customer support for the Poly Clariti Core and Poly Clariti Edge product. Normally, analytics have a five-year retention policy. When a customer makes a request for deletion (`privacy@poly.com`), Poly will delete the requested data within

30 days, unless the data is required to be retained for Poly's legitimate interests or if needed to provide the service to customer.

For more information, see How Personal Data Is Deleted.

Right to Rectification

A data subject has the right to make corrections to inaccurate or incomplete personal data. Personal data specific to device configuration can be edited or updated by the device administrator.

Personal data about specific participants in conferences can't be edited or updated because the information derives from the device of origin.

Poly doesn't manipulate data made available during the support process, so any rectification of inaccuracies of personal data must be performed by customers directly.

Right to Object to Processing

Not applicable.

Right to Restrict Processing

Not applicable.

Purposes of Processing Personal Data

See the *Purposes of Processing* section in the *Security and Privacy White Paper for Clariti*.

How Administrators Are Informed of Any Security Anomalies

Poly Clariti Core and Poly Clariti Edge provide the ability to send system logs to a remote syslog server. Customers may choose to use third-party solutions to analyze the logs for anomalies.

The system administrator can also download the system log archive from the system web interface to review any anomalies. The system log archive also contains detailed logs with transactional information for who, what and when any system changes are made.

For Poly Clariti Relay, the system administrator can download the application logs for anomalies analysis. As Poly Clariti Relay has an administrative interface within Poly Clariti Core and Poly Clariti Edge, Poly Clariti Core and Poly Clariti Edge logs contain transactional information about system changes on Poly Clariti Relay. There's an alerting interface to notify Poly Clariti Core and Poly Clariti Edge of alerts on Poly Clariti Relay.

How Personal Data Is Deleted

The Poly Clariti Core, Poly Clariti Edge, and Poly Clariti Relay systems automatically purge system logs periodically. However, the system administrator can also manually delete the following data from the Poly Clariti Core and Poly Clariti Edge system web interface:

- Poly Clariti Core and Poly Clariti Edge log archive
- Poly Clariti Core and Poly Clariti Edge backup archive
- Endpoint history

This table lists how personal data is deleted within Poly Clariti Core, Poly Clariti Edge, and Poly Clariti Relay.

Data type	***Steps to delete***	***Deletion method***
Log archive	Refer to *Purge Records* in the *Poly Clariti Core, Poly Clariti Edge and Poly Clariti Relay Administrator Guide available on Poly Support.*	Simple delete from database
Backup archive	Refer to *Purge Records* in the *Poly Clariti Core, Poly Clariti Edge and Poly Clariti Relay Administrator Guide available on Poly Support.*	Simple delete from database
Endpoint history	Refer to *Purge Records* in the *Poly Clariti Core, Poly Clariti Edge and Poly Clariti Relay Administrator Guide available on Poly Support.*	Simple delete from database

For more information, see *Purge Records* in the *Poly Clariti Core, Poly Clariti Edge and Poly Clariti Relay Administrator Guide available on Poly Support*.

This table lists how personal data is deleted within Poly Clariti App Mobile and the Poly Clariti SDK.

Application	***Deletion Method***
Poly Clariti App Mobile	Delete the Poly Clariti App Mobile application from the mobile device.

Application	*Deletion Method*
Poly Clariti SDK (iOS/Android)	Delete the application that builds upon the Poly Clariti SDK from the mobile device.
Poly Clariti SDK (MacOS/Windows)	Delete the activity logs from the file system. **Note**: The location of the Poly Clariti SDK logs on MacOS and Windows is specified by the application that builds upon the SDK.

DISCLAIMER