SECURITY AND PRIVACY WHITE PAPER

Poly Remote Managed Infrastructure Services Overview

Part 3725-86321-001

Version 07

March 2024

Introduction

This white paper addresses security and privacy related information regarding Poly Remote Managed Infrastructure Services for Poly Unified Communications and Collaboration (UC&C) infrastructure which are **not** hosted by HP | Poly. This white paper describes the security features and access controls applied to HP | Poly's processing of personally identifiable information or personal data ("personal data") and customer data in connection with the provisioning and delivery of the Managed Services, and the location and transfers of personal and other customer data. HP | Poly will use such data in a manner consistent with the HP Privacy Statement and this white paper (which may be updated from time to time). This white paper is supplemental to the HP Privacy Statement. The most current version of this white paper is available on HP | Poly's website.

The following Managed Services are discussed in this white paper:

Remote Monitoring and Management Services

- Remote Monitoring and Management On-Premises (RMM)
- Remote Monitoring and Management for Service Providers (RMM SP)
- Hybrid Hosted for Enterprise (HHfE)
- Remote Monitoring and Management for Cloud Infrastructure

Overview of Remote Managed Services

There are four (4) options for this type of service as listed above. Each Remote Managed Service is designed to provide a remote management and monitoring solution for Poly Unified Communications and Collaboration infrastructure implemented in a non-HP | Poly environment. The customer provides all network systems and supporting infrastructure, so security considerations will need to be configured in the customer's and/or their service provider's environment.

HP | Poly will provide a secure Managed Services environment consisting of the appropriate systems to provide the supporting services for the DMZ, user authentication, and secure customer connections. Each solution is created using at least one logically separate DMZ to host the monitoring and management systems. IP addressing (RFC 1918) is provided by the customer making the DMZ a virtual extension of the customer's network. The customer must ensure that there are no IP conflicts on their network.

The monitoring and management systems consist of a jump server, a monitoring probe, and file storage dedicated to the engagement. This DMZ is external to the Managed Service environment and is connected to the customer via IPSec VPN.

VPN for Remote Monitoring and Management Service

An IPsec VPN across the Internet is used to connect the customer environment to the Managed Services DMZ for remote monitoring and management. The DMZ contains the monitoring and management servers and is external to the customer environment.

The IP address space used by the servers is typically provided by the customer for convenience in routing across the customer's network. The customer should budget 50Mbps internet bandwidth for this VPN. If multiple VPNs are used, each VPN is dedicated to access from a specific DMZ with a unique set of IP addresses. Redundant VPNs between one DMZ and the customer's infrastructure require custom development and are not part of the standard RMM service. On the HP | Poly side, each VPN will terminate at the HP | Poly core data center judged to provide connectivity with the least network latency.

At the customer's option the IPSec VPN may be terminated directly on the customer's network equipment or on a VPN appliance provided by HP | Poly. If the latter option is selected, the customer is responsible to provide public internet access, customer network access, power, cooling, and space for the VPN appliance. The VPN appliance requires a public IP address for the VPN peer address. This address can be directly on the appliance or can be routed via 1-to-1 NAT to a private address on the appliance, whichever best fits the customer's network environment. All traffic traversing the VPN is protected by encryption. The DMZ is encapsulated by firewall security zones. No unnecessary network ports are opened between zones. Externally, all traffic between the DMZ and the customer will traverse the IPsec VPN. Internally, monitoring information is sent to the monitoring database within the Managed Services environment, to generate alerts and dashboards for the Customer Management Center (CMC) technical support team.

HP | Poly's preferred IPSec VPN parameters are shown in this table:

IKE/ISAKMP Parameters (Phase I)	Values
Mode	Main
IKE Version	1
IKE Encryption / Encryption Algorithm:	AES-256
Pre-Shared Key:	TBD
Authentication Algorithm:	SHA-2 (256)
DH-Group:	Group 2
Security Association Lifetime (Seconds):	86400

IPSEC Parameters (Phase II)	Values
Protocol	ESP
IPSEC Encryption Algorithm:	AES-256
Authentication Algorithm:	SHA-2 (256/128)
Perfect-Forward Secrecy (PFS):	Yes
PFS Keys DH-Group:	Group 2
Security Association Lifetime (Seconds):	7200

These are the parameters that will be used if the VPN terminates on an appliance provided by HP | Poly. If the customer elects to terminate the VPN on its own network equipment, parameter values will be negotiated between HP | Poly and the customer. But the above are strongly recommended for the security of customer and HP | Poly.

For RMM for Cloud Infrastructure, the VPN appliance option is not applicable and VPN tunnel will be required to terminate on Azure Native VPN Gateway in the customer's Azure tenant.

Recommended minimum parameters for Azure VPN Setup:

Parameters	Values
VPN Type	Route-based
VPN SKU	VpnGw1
Connection type	Site-to-Site (IPSEC)
Pre-Shared Key:	TBD

Remote Monitoring and Management On-Premises

For the RMM service, the call platform is owned by the customer and is physically located in the customer's space. HP | Poly will only retain ownership of the products provided in support of the managed services.

The RMM service is based around Poly RealPresence infrastructure hosted in the customer environment. An IPsec VPN is used to connect the customer environment to the managed services DMZ for remote monitoring and management.

Remote Monitoring and Management for Service Providers

The RMM SP service is designed to provide an RMM solution for service providers to rebrand as their own and sell into customer environments. HP | Poly will only retain ownership of the products provided in support of the Managed Services. Each service provider solution is created using a logically separate DMZ to host the service provider's customers. A DMZ is created for the service provider, but that environment is shared across the service provider's customers as is the monitoring instance. Since the customer or service provider provides all network systems and supporting infrastructure, security considerations will need to be configured in their own environments.

The DMZ is created for the service provider and is shared by all service provider customers. IP addresses that reach into the customer's network is assigned from the subnet provided by the service provider during onboarding. NAT may be necessary to avoid IP conflicts. NAT IP addresses are provided by the service provider.

Service providers are provided non-branded service reporting, to be shared with their customers, using their template.

Hybrid Hosted for Enterprise

The HHfE service is designed to provide RealPresence Platform (RPP) services to customers requiring a video solution hosted within their own or a service provider's environment without a capital purchase. These solutions include all RPP hardware, services, and maintenance as part of the service. HP | Poly retains ownership of all provided service components. The RMM access is provided via VPN.

Since the customer provides all network systems and supporting infrastructure, security considerations will need to be configured in the customer's environment. HP | Poly creates a separate DMZ to provide the RMM services for each customer.

The RPP functionality and hardware installed in the customer specified location is provided by HP | Poly, and ownership is retained by HP | Poly. All servers required to run RPP applications are supplied and configured by HP | Poly. The customer owns the environment and the responsibility to secure it.

Remote Monitoring and Management for Cloud Infrastructure

For the RMM service, the call platform is owned by the customer and is deployed in the customer's Azure tenant space. HP | Poly will only retain ownership of the products provided in support of the Managed Services. HP | Poly will only require access to the applications it manages; the ownership and responsibility for the underlying cloud infrastructure will remain with the customer.

The RMM service is based around HP | Poly RealPresence infrastructure hosted in the customer Azure environment. An IPsec VPN is used to connect the customer environment to the managed services DMZ for remote monitoring and management.

Security at HP | Poly

Poly Remote Managed Infrastructure Services utilize the ITIL framework.

Security is always a critical consideration for all HP | Poly products and services. HP | Poly's Information Security Management System (ISMS) has achieved ISO 27001:2013 certification. ISO/IEC 27001 is the most widely accepted international standard for information security best practices and you can be reassured that HP | Poly has established and implemented best-practice information security processes.

Product security at HP | Poly is managed through the HP Cybersecurity team which oversees secure software development standards and guidelines. The HP | Poly Product Security Standards align with NIST Special Publication 800-53, ISO/IEC 27001:2013, and OWASP for application security. Guidelines, standards, and policies are implemented to provide our developers with industry approved methods for adhering to the HP | Poly Product Security Standards.

Privacy by Design

HP | Poly implements internal policies and measures based on perceived risks which meet the principles of data protection by design and data protection by default. Such measures consist of minimizing the processing of personal data, anonymizing personal data as soon as possible, transparently documenting the functions, and processing of personal data and providing features which enable the data subject to exercise any rights they may have.

When developing, designing, selecting, and using applications, services and products that are based on the processing of personal data or process personal data to fulfill their task, HP | Poly considers the right to data protection with due regard.

Security by Design

HP | Poly follows Security by Design principles throughout our product creation and delivery lifecycle which includes considerations for confidentiality, integrity (data and systems), and availability. These extend to all systems that HP | Poly uses – both on-premises and in the cloud as well as to the development, delivery, and support of HP | Poly products, cloud services and managed services.

The foundational principles which serve as the basis of HP | Poly's security practices include:
1. Security is required, not optional
2. Secure by default, Secure by design
3. Defense-in-depth
4. Understand and assess vulnerabilities and threats
5. Security testing and validation
6. Manage, monitor, and maintain security posture
7. End-to-end security: full lifecycle protection

Security Testing

Both static and dynamic vulnerability scanning as well as penetration testing are regularly performed for production releases and against our internal corporate network by both internal and external test teams.

Patches are evaluated and applied in a timely fashion based on perceived risk as indicated by CVSSv3 scores.

Change Management

Poly Remote Managed Infrastructure Services utilize the Information Technology Infrastructure Library (ITIL) framework. HP | Poly uses its own change management policies and procedures, aligned with ITIL, to document and review changes for viability and necessity.

A formal change management process is followed by all teams at HP | Poly to minimize any impact on the services provided to the customers. All changes implemented go through vigorous quality assurance testing where all functional and security requirements are verified. Once Quality Assurance approves the changes, the changes are pushed to a staging environment for UAT (User Acceptance Testing). Only after final approval from stakeholders, changes are implemented in production. While emergency changes are processed on a much faster timeline, risk is evaluated, and approvals are obtained from stakeholders prior to applying any changes in production.

Data Processing

System logs and call detail records can be collected by or sent to HP | Poly. These may contain names, emails, IP addresses, locations.

Customers who contact HP | Poly for technical support are asked to provide contact information.

If someone is an individual user and the purchase of a HP | Poly Managed Service has been made by their employer as the customer, all the privacy information relating to personal data in this white paper is subject to their employer's privacy policies as controller of such personal data.

Purpose of Processing

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

When configured to use an optional HP | Poly device management solution, the on-premises server or cloud service processes configuration files and their overrides to aid the management of the devices in a given deployment. The server or cloud service may also process device network information, media statistics and device asset information to aid in device analytics, which enables device performance validation and visibility into customer quality of experience and service performance.

How Customer Data Is Stored and Protected

Data backups are stored in an encrypted customer DMZ for 61 days. Reporting data is stored in an encrypted server in the HP | Poly IT environment for 2 months or the conclusion of the engagement. Technical support details are stored in HP | Poly CRMs and on sftp (temporarily held until 90 days after ticket is closed).

Source of Personal Data	Categories of PI Processed	Business Purpose for Processing	Disclosed to the following Service Providers
Support and reporting services	• Endpoint display name • User email address • User ID • User phone number • User address/location • Endpoint IP addresses	• Troubleshooting and support remediation • Provide required reporting for managed services	None
Configuration backups	• Display name • User email address • User ID • Phone number • Organization address/location	Ability to recover from system failure	None

HP | Poly may change the location of the HP | Poly Managed Service database server and details of any such change shall be set forth in the latest copy of this white paper available on HP | Poly's website.

For transferring personal data of EU customers to the US, HP | Poly uses an Intragroup Data Transfer Agreement incorporating the EU Standard Contractual Clauses as the transfer mechanism.

Data Deletion and Retention

All information collected from the customer is stored in the database with the tenant information configured as the access control mechanism.

Nothing is transmitted outside of HP | Poly Remote Managed Services for Poly UC&C infrastructure. All data is self-contained in the database in the data center.

For the set of usage data sent to HP | Poly, HP | Poly may retain customer data for as long as needed to provide the customer with any HP | Poly cloud services for which they have subscribed and for product improvement purposes. When a customer makes a request for deletion to HP's Chief Privacy and Data Protection Officer form, HP | Poly will delete the requested data within 30 days, unless the data is required to provide the service to customer. HP | Poly may "anonymize" personal data in lieu of deletion. The anonymization process is irreversible and includes but is not limited to searching and sanitizing all customer-specific data (e.g., name, site information and IP address) with randomly generated alphanumeric characters.

Secure Deployment

The RealPresence Platform (RPP) functionality and hardware is installed within the customer's environment. Ownership and environment responsibility is retained by the customer. The customer is responsible to procure and secure the public internet access and public IP addresses for the service to use.

Customer information obtained during onboarding is used to create the DMZ. Customer is able to monitor HP | Poly network traffic as it will only enter the customer's network using the subnet assigned.

The DMZ has the following specific functionality to support the service:

Monitoring uses a collector in each DMZ allowing for gathering of alert information (e.g., SNMP, API, Ping, etc.) from the customer and isolation of the internal Managed Services network. Externally, all traffic to the customer will traverse the IPsec VPN. Internally, monitoring information is sent to the monitoring database, within the Managed Services environment, to generate alerts and dashboards for the Customer Management Center (CMC) technical support team.

Management is performed on a jump server. This serves as a bastion host for authorized users. No internet accessible HP | Poly systems directly access customer systems, except for operating system updates through a proxy. Management traffic (e.g., HTTPS, SSH, Telnet, Ping, etc.) is generated from the customer specific DMZ to systems covered under the Remote Management and Monitoring Service. Configuration backups of managed devices are taken monthly for recovery. Backups and support information (e.g., system logs, CDRs, network traces, etc.) are temporarily stored on the jump server. Backup information on jump servers is encrypted (see “Cryptographic security” section for details). Support information is to be removed from the DMZ immediately upon being moved to support systems.
HP | Poly uses its own change management policies and procedures, aligned with ITIL, to document and review changes for viability and necessity.

Server Access and Data Security

The customer or their service provider (depending on the agreement) is responsible for physical and data security for all systems in their environment up to the HP | Poly VPN connection at the edge of the network.

All backend and management servers created for the use of Managed Services follow hardened templates for deployment. Firewall ports are opened only as necessary, and changes are documented through change management.

Backend and management servers that are the foundation for the Managed Services network and DMZs are in secure data centers, with only authorized staff members having badged access. The access to the equipment for these systems is via secure and bidirectional tunnel.

Cryptographic Security

Managed Services Connections

- Certificates per HP | Poly asset used for administrative access
- Encryption algorithm: SHA-256
- Authentication algorithm: RSA
- IPsec VPN connection minimums
    - Encryption algorithm: AES-256
    - Authentication algorithm: SHA-2

Managed Services Data Storage Encryption

- Password storage
    - Encryption algorithm: AES-256
    - Local authentication: SHA-512
- Support ticket information
    - Encryption algorithm: AES-256
- Reporting server (BRMs)
    - Encryption algorithm: SHA-256
- Backup server (application backup data)
    - Encrypted by individual application (please see individual application Security White Paper for details)

Authentication

HP | Poly personnel use certificates on HP | Poly managed assets for their software VPN connection to the HP | Poly Managed Services network. From their HP | Poly device, administrators access the specific jump server using unique AD credentials. The Managed Services network has a separate active directory server for providing unique credentials and logging user activity on the jump server dedicated to the customer.
HP | Poly Managed Services personnel initially access
the customer’s managed devices using local administrator credentials provided during onboarding. These credentials are changed when HP | Poly Managed Services goes operational.

Managed device credentials are stored in an encrypted password manager which is assigned, managed, and logged per user.

Customer user access is provided requiring unique identifiers and passwords which must be changed per HP | Poly policy. Business Relationship Manager (BRM) can facilitate the request and will follow up on password changes. All customer user traffic will stay within the customer’s network.

Disaster Recovery and Business Continuity

Poly Remote Managed Infrastructure Services for Poly UC&C infrastructure are architected to provide high reliability, resiliency, and security.

HP | Poly has a Business Continuity and Disaster Recovery Plan reviewed and approved by management to ensure that we are appropriately prepared to respond to an unexpected disaster event. HP | Poly tests disaster recovery processes and procedures on an annual basis. We use the results of this testing process to evaluate our preparedness for disasters and to validate the completeness and accuracy of our policies and procedures.

Security Incident Response

The HP Cybersecurity team promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. You may contact them directly at informationsecurity@hp.com

The HP Cybersecurity team works proactively with customers, independent security researchers, consultants, industry organizations, and other suppliers to identify possible security issues with HP | Poly products and networks. HP | Poly security advisories and bulletins can be found on the HP Customer Support website.

Subprocessors

HP | Poly uses certain subprocessors to assist in providing our products and services. A subprocessor is a third-party data processor who, on behalf of HP | Poly, processes customer data. Prior to engaging a subprocessor, HP | Poly executes an agreement with the subprocessor that is in accordance with applicable data protection laws.

The subprocessor list here identifies HP | Poly's authorized subprocessors and includes their name, purpose, location, and website. For questions, please contact HP's Chief Privacy and Data Protection Officer form.

Additional Resources

To learn more about Poly Remote Managed Infrastructure Services, please visit our website.

Disclaimer

This white paper is provided for informational purposes only and does not convey any legal rights to any intellectual property in any HP | Poly product. You may copy and use this paper for your internal reference purposes only. HP | POLY MAKES NO WARRANTIES, EXPRESS OR IMPLIED OR STATUTORY AS TO THE INFORMATION IN THIS WHITE PAPER. THIS WHITE PAPER IS PROVIDED “AS IS” AND MAY BE UPDATED BY HP | POLY FROM TIME TO TIME. To review the most current version of this white paper, please visit our website.