SECURITY AND PRIVACY WHITE PAPER

# Polycom RealPresence DMA

Part 3725-86312-001

Version 05

March 2024

**Introduction**
This white paper addresses security and privacy related information for Polycom RealPresence DMA. It also describes the security features and access controls in HP | Poly's processing of personally identifiable information or personal data ("personal data") and customer data in connection with the running of the DMA product, as well as the location and transfer of personal and other customer data. HP | Poly uses such data in a manner consistent with the HP Privacy Statement and this white paper (as may be updated from time to time). This white paper is supplemental to the HP Privacy Statement. The most current version of this white paper will be available on HP | Poly's website.

**Overview**
Polycom RealPresence DMA is a feature-rich video conferencing platform and server. DMA can be installed either on a virtual machine (VMWare or Hyper-V) or on an appliance (COTS – Dell Servers). It can be configured as Core (LAN), Edge (in DMZ), or Combo (Core & Edge in DMZ). DMA systems can be deployed in a variety of network configurations.

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

Product security at HP | Poly is managed through the HP Cybersecurity team, which oversees secure software development standards and guidelines.

The HP | Poly Product Security Standards align with NIST Special Publication 800-53, ISO/IEC 27001:2013, and OWASP for application security. Guidelines, standards, and policies are implemented to provide our developers with industry approved methods for adhering to the HP | Poly Product Security Standards.

**Secure Software Development Life Cycle**
HP | Poly follows a secure software development life cycle (S-SDLC) with an emphasis on security throughout the product development processes. Every phase of development process ensures security by establishing security requirements alongside functional requirements as part of initial design. Architecture reviews, code reviews, internal penetration testing and attack surface analysis are performed to verify the implementation.

The S-SDLC implemented by HP | Poly also includes a significant emphasis on risk analysis and vulnerability management. To increase the security posture of HP | Poly products, a defense-in-depth model is systematically incorporated through layered defenses. The principle of least privilege is always followed. Access is disabled or restricted to system services nonessential to standard operation.

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

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

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

**Security by Design**

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

The foundational principles which serve as the basis of HP | Poly's security practices include:

1. Security is required, not optional
2. Secure by default, Secure by design
3. Defense-in-depth
4. Understand and assess vulnerabilities and threats
5. Security testing and validation
6. Manage, monitor, and maintain security posture
7. End-to-end security: full lifecycle protection

**Security Testing**

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

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

**Change Management**

A formal change management process is followed by all teams at HP | Poly to minimize any impact on the services provided to the customers. All changes implemented for the Polycom RealPresence DMA 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.

**Security Settings**

The Polycom RealPresence DMA 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). When communicating with any device, service, and/or the management interface, you can configure DMA to use encrypted communication. DMA provides fine-grained security settings in its user interface so that customers can harden the security of DMA as required. DMA 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.

**Certificates**

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

Polycom RealPresence DMA provides certificate management capabilities which enable the user to load new certificates for use by the system. DMA also supports Online Certificate Status Protocol (OCSP) for obtaining the revocation status of an X.509 certificate presented to the system.

**Access Control Lists (ACLs)**

Polycom RealPresence DMA provides the ability to configure Access Control Lists (ACLs) for blocking incoming traffic (H.323 and SIP). Based on the configured criteria of ACLs, the DMA 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 the DMA system (edge or combo configuration).

**Device, Call, and Conference Security**
Polycom RealPresence DMA provides different security features for call signaling and conference management that the user can enable or disable from the DMA web GUI.

**Port Ranges**
Polycom RealPresence DMA enables 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 WebRTC.

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

**Management Access**
Polycom RealPresence DMA is 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 DMA 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, users can view specific pages.

The administrator 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 administrator 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 DMA system.

As DMA runs 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.

**Reporting**
Polycom RealPresence DMA has extensive reporting capabilities and provides the user with both system level and call/conference level reports.

**Data Processing**
Polycom RealPresence DMA does not access any customer's data except as required to enable the features provided by the application. As these systems are deployed in the customer's environment, it is the responsibility of the customer to protect data privacy.

DMA collects and processes 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 someone is an individual user and the purchase of DMA 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.

DMA provides the ability to delete the following data from the management web GUI:

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

| Source of Personal Data | Categories of PI Processed | Business Purpose of Processing | Disclosed to the Following Service Providers |
|---|---|---|---|
| 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 | None |
| Call participant personal data | • Name<br>• Email address (optional)<br>• Phone number<br>• Display name<br>• SIP URI<br>• IP address<br>• Dial string | • Deliver video service<br>• Keep track of KPIs | None |
| Device information | • Device name<br>• IP address<br>• MAC address<br>• Serial number | • Diagnose technical issues<br>• Respond to customer support requests<br>• Serial number for entitlement | None |
| Analytics/Usage information | • Activity logs<br>• Call detail records | • Conduct analytics and analysis to improve the technical performance of the service<br>• Capacity forecasts | AWS |

**Purpose of Processing**

*Analytics/Send Usage Data*
To continually improve the product, HP | Poly collects data to understand how customers use the Polycom RealPresence DMA system. By collecting this data, HP | Poly can identify system level utilization and the combined use of DMA system features. This data informs HP | Poly which features are important and actually used on your system. HP | 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 DMA system 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 HP | Poly collection point.

NOTE: The analytics proxy service runs in AWS. However, there is no UI interface to the analytics proxy service, and it is not possible to access via a normal web browser.

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 HP | Poly as well as by the system administrators of each DMA 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

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 the DMA system sends 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. HP | Poly's collection and use of this data complies with HP Privacy Statement.

The user can allow or disallow the automatic sending of usage data at any time. The DMA system requires 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 HP | Poly in the *analytics.json* log file available for download through the management web GUI.

**How Customer Data Is Stored and Protected**

HP | Poly does not upload any personal data. Analytics excludes all information that identifies individual people or an individual's habits. For example, usernames, device aliases, and certain description fields are not uploaded. Analytics does not upload data that could compromise the security of customer environments. For example, host names, internal IP addresses, usernames, and passwords are not uploaded. Customer-specific data is pseudonymized. Analytics only stores the HP | 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. HP | 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 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.

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

**Data Portability**

A data subject has the right to receive a copy of all personal data in a commonly used, machine-readable format. CDRs can be downloaded in CSV format. Log files can be downloaded in plain text format.

**Data Deletion and Retention**
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.

HP | Poly may retain customer data for as long as needed to provide the customer support for the Polycom RealPresence DMA product. When a customer makes a request for deletion at 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 be retained for HP | Poly's legitimate interests or if needed to provide the service to customer.

**Disaster Recovery and Business Continuity**
The Polycom RealPresence DMA is architected to provide high reliability, resiliency, and security. Analytics is hosted in AWS data centers in the United States. Normal low impact outage due to loss of power or connectivity is already handled by the cloud hosting provider — AWS. During a major crisis or disaster, service will be moved to a different region until the affected region is restored.

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 but are sometimes conducted more frequently when there are changes to our infrastructure that warrant new tests. 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 can contact them directly at informationsecurity@hp.com. The 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 at the HP Customer Support website.

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

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

Prior to engagement, suppliers that may process data on behalf of HP | Poly must undergo a privacy and security assessment. The assessment process is designed to identify deficiencies in privacy practices or security gaps and make recommendations for reduction of risk. Suppliers that cannot meet the security requirements are disqualified.

**Additional Resources**
The *RealPresence DMA Security and Privacy Guide, RealPresence DMA System Getting Started Guide,* and the *Polycom RealPresence DMA System Operations Guide* have in-depth details about Polycom RealPresence DMA configuration and capabilities. To access those guides and other information about DMA, 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 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.