SECURITY AND PRIVACY WHITE PAPER

Polycom RealPresence DMA

Part 3725-86312-001

Version 01

July 2019

INTRODUCTION

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

OVERVIEW

RealPresence DMA is a feature-rich video conferencing platform and server.

RealPresence 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).

RealPresence DMA systems can be deployed in a variety of network configurations.

The CentOS operating system running the RealPresence 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 POLY

Security is always a critical consideration for any product. Polycom was awarded ISO/IEC 27001:2013 certification for our Information Security Management System (ISMS). ISO/IEC 27001 is the most widely accepted international standard for information security best practices and a tangible measure by which existing and potential customers can be reassured that Poly has established and implemented best-practice information security processes. ISO/IEC 27001:2013 certification not only reinforces our commitment to information security best practices and controls, but it explicitly includes the product development process.

Product security at Poly is managed through the Poly Security Office (PSO), which oversees secure software development standards and guidelines. The Poly Product Security Standards align with NIST Special Publication 800-53, ISO/IEC 27001:2013 and OWASP for application security.

Guidelines, standards, and policies are implemented to provide our developers industry-approved methods for adhering to the Poly Product Security Standards.

SECURE SOFTWARE DEVELOPMENT LIFE CYCLE

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

The S-SDLC implemented by Poly also includes a significant emphasis on risk analysis and vulnerability management. To increase the security posture of Poly products, a defense-in-depth model is systematically incorporated through layered defenses. The principle of least privilege is always followed. Access is disabled or restricted to system services nonessential to standard operation. Additional testing, in the form of standards-based Static Application Security Testing and patch management, is a cornerstone of our S-SDLC.

PRIVACY BY DESIGN

Poly implements internal policies and measures based on perceived risks which meet the principles of data protection by design and data protection by default. Such measures consist of minimizing the processing of personal data, anonymizing personal

data as soon as possible, transparently documenting the functions, and processing of personal data and providing features which enable the data subject to monitor the data processing while also enabling the data controller to create and improve security features. When developing, designing, selecting, and using applications, services and products that are based on the processing of personal data or Poly considers the right to data protection with due regard to making sure that data controllers and processors can fulfill their data protection obligations.

SECURITY SETTINGS

The 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 RealPresence DMA to use encrypted communication. RealPresence DMA provides fine-grained security settings in its user interface so that customers can harden security of RealPresence DMA as required.

RealPresence 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.

RealPresence DMA provides certificate management capabilities which enable the user to load new certificates for use by the system. RealPresence 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)

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 RealPresence 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 RealPresence DMA system (edge or combo configuration).

DEVICE, CALL, AND CONFERENCE SECURITY

RealPresence DMA provides different security features for call signaling and conference management that the user can enable or disable from RealPresence DMA web GUI.

PORT RANGES

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

MANAGEMENT ACCESS

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

For additional security, the user can enable management access settings and provide the list of IP-addresses of machines that can access the web GUI or the REST APIs of the RealPresence DMA system.

As RealPresence 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

RealPresence DMA has extensive reporting capability and provides the user with both system level and call/conference level reports.

DATA PROCESSING

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.

RealPresence 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 you are an individual user and the purchase of RealPresence DMA has been made by your employer as the customer, all the privacy information relating to personal data in this white paper is subject to your employer's privacy policies as the controller of such personal data.

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

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

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 • E164 address • H.323 ID	• 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 • Capacity forecasts • Keep track of KPIs
Device information	• Device name • IP address • MAC address • Serial number	
Analytics/Usage information	• Activity logs • Call detail records	

PURPOSE OF PROCESSING

Analytics/send usage data

To continually improve the product, Poly collects data to understand how customers use the RealPresence DMA system. By collecting this data, Poly can identify system level utilization and the combined use of RealPresence DMA system features. This data informs Poly which features are important and actually used on your system. Poly uses this information to help guide future development and testing. Your 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 RealPresence 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 Poly collection point (customerusagedatacollection.polycom.com). There is no access by any customer or others to view the data received at the collection point. The raw data is viewable only by Poly as well as by the system administrators of each RealPresence 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 RealPresence 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. 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. The RealPresence 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 Poly in the *analytics.json* log file available for download through the management web GUI.

HOW CUSTOMER DATA IS STORED AND PROTECTED

Poly does not upload any personal data. Analytics excludes all information that identifies individual people or an individual's habits. For example, user names, 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, user names, and passwords are not uploaded. Customer-specific data is pseudonymized. Analytics only stores 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 white paper available on Poly's GDPR 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 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.

THIRD-PARTY PROVIDERS (SUB-PROCESSORS)

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.

DATA DELETION AND RETENTION

Poly may retain customer data for as long as needed to provide the customer support for the RealPresence DMA product. 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.

CHANGE MANAGEMENT

A formal change management process is followed by all teams at Poly. All changes implemented to RealPresence DMA go through vigorous QA testing where all functional and security requirements are verified.

SECURITY INCIDENT RESPONSE

The Poly Security Office (PSO) promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. You can contact the PSO directly at informationsecurity@poly.com

The PSO team works proactively with customers, independent security researchers, consultants, industry organizations, and other suppliers to identify possible security issues with Poly products and networks. Poly security advisories and bulletins can be found at the Poly Security Center.

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 RealPresence DMA configuration and capabilities. To access those guides and other information about RealPresence DMA, please visit our support site.

DISCLAIMER:

This document is provided for informational purposes only and does not convey any legal rights to any intellectual property in any Poly product. You may copy and use this paper for your internal reference purposes only. POLY MAKES NO WARRANTIES, EXPRESS OR IMPLIED OR STATUTORY AS TO THE INFORMATION IN THIS WHITE PAPER. THIS WHITE PAPER IS PROVIDED "AS IS" AND MAY BE UPDATED BY POLY FROM TIME TO TIME.