SECURITY AND PRIVACY WHITE PAPER

Plantronics Manager Pro

Part 3725-86204-001

Version 09

March 2024

Introduction

This white paper addresses security and privacy-related information regarding Plantronics Manager Pro.

This paper 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 provisioning and delivery of Manager Pro, 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 will be available on HP | Poly's website.

Manager Pro is an internet-based subscription service (i.e., Software as a Service—SaaS) powered by Amazon Web Services (AWS), which provides the ability to manage, monitor, and configure a variety of Plantronics and Poly audio devices.

It supports managing headsets, configuring policy, viewing policy compliance status, locking settings, managing by user groups (LDAP/manual), IT troubleshooting, and analysis reporting of assets, usage, conversation, and acoustics.

Note: Although Manager Pro is powered by AWS and used with Plantronics Hub, the scope of this white paper is limited to Manager Pro. Please see AWS security details here.

Security at HP | Poly

Security is always a critical consideration for a cloud-based service such as Plantronics Manager Pro. 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.

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 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 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 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 the 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 & 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.

Cloud systems are managed by HP | Poly and are updated as needed. 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 Plantronics Manager Pro 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

HP | Poly does not access any customer's data except as required to enable the features provided by the service. If someone is an individual user and the purchase of the Plantronics Manager Pro has been made by their employer as the customer, all of 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. Personal data collected and the purposes for which it is collected are listed in the table below.

Purpose of Processing

In general, the data collected by Plantronics Manager Pro is directly related to the level of subscription. For example, if you are not subscribed to the Call Quality and Analytics Suite, then the data required to populate these reports will not be collected.

While using Plantronics' mobile apps, it is requested to collect location information for the purpose of enabling features in the Plantronics Hub for Android/iOS mobile app such as the BackTrack™ feature.

PLEASE NOTE: The ability to pseudonymize network username, end user display name, computer hostname, and domain was added as of

Source of Personal Data	Categories of PI Processed	Business Purpose for Processing	Disclosed to the following Service Providers
Tenant information	• First/last name • Email address • Access events (login/logout)	• Authenticate and authorize tenant administrative access to the service • Deliver the service • These events can be monitored by Poly at an individual (customer) level or in aggregate for understanding administrative behaviors.	AWS
Plantronics Hub for Desktop in a Plantronics Manager Pro environment (version 3.9 and higher)	• Client instance ID • System ID	Poly-assigned identifiers for ensuring a system and an instance of Hub can be associated to a user.	AWS
	• Network username • End user display name • Computer hostname • Computer domain	Associates a unique user to a device and the device to a system. Note: These data elements are pseudonymized by default beginning in version 3.13.	
	• LDAP user attributes including LDAP group membership, username, account name, city, company, country, department, department number, division, employee type, office, state, zip code, display name, telephone number, street address, and title	LDAP attributes are entirely under the control of the administrator. These LDAP attributes are completely optional and are not collected by default. Your company may choose to enable these attributes in the Plantronics Hub collection criteria.	
	• Plantronics device information including model ID, product ID, serial number	Required for proper update selection, troubleshooting, and reporting.	
Plantronics Hub for Desktop in a Plantronics Manager Pro environment (prior to version 3.9)	• End user email • Local IP address • Network IP address	Versions of Hub prior to 3.9 may send these pieces of data. Plantronics Manager Pro does not keep or store this information. Update to the latest version to ensure this data is not sent.	AWS
	• Call ID	Required for Radio Link Quality report (Data sent only with subscription of Call Quality and Analytics Suite or better).	
Plantronics Hub for Mobile in a Plantronics Manager Pro environment	• Client instance ID	Poly-assigned identifiers for ensuring an instance of Hub can be associated to a user	AWS
	• Network username • Mobile device hostname and domain	Associates a unique user to a device and the device to a system. Note: These data elements are pseudonymized by default beginning in version 3.13.	
	• Plantronics device information: model ID, product ID, serial number (IMEI)	Required for proper update selection, troubleshooting, and reporting	

version 3.13. It is only enabled by default for new tenants. Tenants that were created prior to 3.13 will need to enable the feature manually.

Versions of Hub prior to 3.13 do not support this functionality so in that case the pseudonymization is only performed on the server side.

How Customer Data is Stored and Protected

All customer data is stored within the AWS data centers on which the service is deployed using hardware-based AWS EBS volume encryption with Advanced Encryption Standard (AES-256) for data at rest.

Customer data is automatically backed up nightly in digital form. Normal access controls of authorized users and data security policies are followed for all backup data. No physical backup media is used.

All identifiable customer data is stored solely within the Plantronics Manager Pro system where the tenant resides. Tenant-specific MySQL data are stored in separate DB schemas. Mongo (NoSQL) documents are stored with tenant-specific IDs.

Data center locations are determined based on customer location and may include USA, Ireland, and Australia.

Backups of identifiable customer data are stored in the same AWS region as where the tenant is hosted.

Pseudonymized data may be stored in an aggregated reporting data warehouse located in a Virtual Private Cloud in an AWS data center in the USA. This pseudonymized data may be used for product improvement and testing purposes.

NOTE: The use of third-party apps or APIs should be carefully considered as they may process data in or transfer data to different geographies.

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.

We use a combination of administrative, physical, and logical security safeguards and continue to work on features to keep your information safe. Customer data may be accessed by HP | Poly as required to support the service and access is limited to only those within the organization with the need to access data in order to support the service.

Data Portability

Certain data can be downloaded. For details, please see the Plantronics Manager Pro User Guide.

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. After a customer’s subscription terminates or expires, HP | Poly will delete customer data within 30 days of cancellation of services. All encryption keys are destroyed at time of deletion.

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 be retained to provide the service to customer.

Secure Deployment

Plantronics Manager Pro is an internet-based subscription service hosted entirely in AWS. The customer enterprise IT admin and user computers are required to make outbound connections to the Manager Pro tenant instance. All traffic transported between the customer's computers and Manager Pro is always encrypted. The customer admin is responsible for managing the Manager Pro tenant. The customer's administrator can access, view, and manage application audit logs for their tenant and run various reports if the reporting features are enabled but is not able to access any tenant data directly as it is stored in AWS using encryption for data at rest. Data can potentially be made visible via third-party partner apps but only if the customer has provided access.

From an HP | Poly administrative perspective, administrators are required to use strong password authentication and the HP | Poly Dev Ops team is required to use multi-factor authentication whenever logging into AWS to manage all deployments of the Manager Pro service. Certificate-based SSH is used to access AWS instances supporting Plantronics Manager. SSH certificates are rotated on a regular basis. Any remote access required by HP | Poly is directly into the AWS instance, not the customer's internal network.

Server Access and Data Security

Plantronics Manager Pro is hosted on AWS. Only authorized staff members with proper access permissions have access to the production servers.

HP | Poly also has implemented technical and physical controls designed to prevent unauthorized access to or disclosure of customer content. In addition, we have systems, procedures, and policies in place to prevent unauthorized access to customer data and content by HP | Poly employees.

Cryptographic Security

While processing all Plantronics Manager Pro data, industry-standard HTTPS over TLS 1.2 is used for data encryption in transit and hardware-based AWS EBS volume encryption with Advanced Encryption Standard (AES-256) for data at rest. To protect user passwords, the standard bcrypt algorithm is used to securely hash and salt passwords before being stored in a database.

Key Management

Encryption keys are managed by the AWS Key Management Service (KMS). There is no single super-user key capable of unlocking all data. Each individual region uses separate keys for live and backup data. Customers are not able to host, control, or maintain encryption keys themselves. For more details, please see here.

Password Management

Single Sign On accounts will follow their own corporate password policies. From an HP | Poly administrative perspective, HP | Poly admin accounts require strong password authentication. Local accounts on Plantronics Manager Pro must be configured manually by the customer IT administrator.

Authentication

Plantronics Manager Pro supports the integration of enterprise authentication providers via SAML 2.0. Once configured, Manager Pro can be accessed by selecting the single sign-on (SSO) button in the Manager Pro login dialog (service provider-initiated) or can be accessed by selecting Manager Pro from your list of identity provider applications (IDP-initiated). Both IDP-initiated SSO via SAML 2.0 and SP-initiated SSO are supported. Supported IDPs that have been tested and confirmed include Ping and ADFS. Other IDPs may work but have not been tested and therefore are not officially supported. Contact your HP | Poly account representative or your Plantronics reseller to request support for a specific IDP.

From an HP | Poly administrative perspective, HP | Poly administrators are required to use multi-factor authentication as well as strong passwords. However, two-factor authentication is not required or supported for customer use.

Disaster Recovery and Business Continuity

Plantronics Manager Pro is architected to provide high reliability, resiliency, and security. We test our backup and restore process at regular intervals.

Our infrastructure runs on fault-tolerant systems to protect the service from failures of individual servers or even entire data centers. The HP | Poly operations team tests disaster recovery measures regularly and an on-call team is ready to resolve any incidents in the event of such occurrence. Additionally, HP | Poly administrators manage and maintain the service under the Plantronics Manager Pro Standard Operating Guidelines.

Customer data is stored across multiple AWS availability zones within region-specific data centers.

When a system outage occurs, we will post notification on the Plantronics Manager Pro System Status page.

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.

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

To learn more about Plantronics Manager Pro, visit our product 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.