HP DaaS Analytics and Proactive Management
Data Management FAQ

This document answers the most commonly asked questions related to HP Device as a Service (HP DaaS) Analytics and Proactive Management's data collection, transmission, storage, retention and disposal of data.

Contents

HP DaaS Analytics and Proactive Management - Data Management FAQ

Cloud Technology/Data Centers

Q: What cloud technology and data centers are leveraged by the HP DaaS platform?

A: The HP DaaS platform is hosted on Amazon Web Services (AWS), a scalable computing infrastructure and recognized leader in cloud hosting.

HP maintains data centers in the United States (AWS-OR) and Frankfurt, Germany (AWS-DE). Data for customers located in EMEA countries can be hosted in the Frankfurt data center. Data for customers in all other countries can be hosted in Oregon in the U.S. All data within a single customer "tenant" is hosted in a single data center, although customers who wish to have separate tenants in different data centers to host data for different business units may request this option.

By partnering with AWS, the service inherits a cloud infrastructure that has been architected to be one of the most flexible and secure cloud computing environments available today.

To learn more about AWS security, visit https://aws.amazon.com/security/.

Q: What are the roles of each data center with respect to tasks and customers?

A: The United States and German data centers can be used to differentiate customers from different regions. EU-based customers may prefer to use the German data center, while the U.S. data center manages customers from all other countries. Having the two data centers, allows the HP DaaS Analytics and Proactive Management service to localize personal data within each of the regions.

Data analytics for HP DaaS Analytics and Proactive Management services is performed in the United States Analytics data center. For data protection purposes, all personal data is de-identified prior to transmission to and storage in the U.S. data center.

Q: How does the data flow between the device and various HP DaaS Analytics and Proactive Management components?

A: Data flow follows this process:

1. After an account is created, the HP DaaS customer enrolls on the cloud-based HP DaaS Analytics and Proactive Management portal, which is hosted in U.S. and German regional data centers.
2. Analytics and Proactive Management software is then pushed to customer's devices to enroll individual devices to be managed by Analytics and Proactive Management from either the U.S. and German regional data center.
3. The cloud-based HP DaaS Analytics and Proactive Management portal and the Analytics and Proactive Management software on the devices captures and sends data to the U.S. and German regional data centers.
4. Personal data maintained in the German data center is de-identified prior to transmission to the U.S. Analytics data center where it will be leveraged for analytics purposes.
5. HP DaaS Analytics and Proactive Management uses the cloud-based portal to provide its functionality—device management as well as analytical services (such as fleet health monitors, actionable reports, incidents, and alerts) by combining de-identified analytic data from the U.S. Analytics data center with personal data and information from the regional data centers.

Data Collection

Q: What data does the HP DaaS Analytics and Proactive Management service collect and how is it used?

A: The "types" of data collected by HP DaaS Analytics and Proactive Management service are either provided by the customer directly or collected automatically from HP DaaS Analytics and Proactive Management portal and the Analytics and Proactive Management software on the devices.

HP DaaS Analytics and Proactive Management collects the following data to execute contract services:

Purpose of Data Collection	Data Collected	Description of data collected
Account management	Account data	Information such as how a customer purchases or signs up for HP DaaS Analytics and Proactive Management, support history with respect to incidents generated by the HP DaaS Analytics and Proactive Manager, and anything else relating to the HP DaaS Analytics and Proactive Management account to perform transaction services like account management.
Ensure HP DaaS Analytics and Proactive Management software and services works properly	Application data	Analytics and Proactive Management software versions, installation status, data sharing choices and update details.
Account setup and entitlement validation	Contact data	Personal and/or business contact data including first name, last name, mailing address, telephone number, fax number, email address and other similar contact information for HP DaaS Analytics and Proactive Management account setup and validation, services entitlement and e-mail notifications around incidents and services.
Deliver proactive IT service maintenance and management, and customer-centric reports/dashboards	Device data	Basic hardware information related to device: computer, operating system, amount of memory, region, language, time zone, model number, first start date, age of device, device manufacture date, browser version, computer manufacturer, warranty status, unique device identifiers and additional technical information that varies by product.
		Hardware components such as battery, disk, BIOS, HP SureStart, display and graphics, plug and play devices and drivers, driver errors and driver crashes, memory, real-time clock, processor, system slots, environment variables, thermals, operating system, network interface, operating system and third-party patches, anti-virus and firewall status and applications, windows device security profile, and device management profiles and their status.
		Software applications installed on devices. Note: We do not scan or collect the content of any file or information that might be displayed by an application.
		Performance data: Battery, disk, CPU, memory and thermal utilization.
		Software application utilization with respect to frequency and time of usage, and impact of software utilization on hardware performance data (battery, disk, CPU, memory and thermal usage).
		Network utilization data: network transmission rates from the device.

Purpose of Data Collection	Data Collected	Description of data collected
Deliver Proactive service maintenance and management of devices by pinpointing the location of a missing device	Location data	Geolocation data to enable location-based services. This feature is turned off by default for all customers and an option is provided for customers to enable or disable location-based services in HP DaaS Analytics and Proactive Management.
Authentication and authorization of user access to HP DaaS Analytics and Proactive Management accounts and services	Security credentials	User IDs, passwords, password hints, and similar security information required for authentication authorizes users for access to HP DaaS Analytics and Proactive Management accounts and services.

Q: What types of data is not collected by HP DaaS Analytics and Proactive Management?

A: HP DaaS Analytics and Proactive Management does not collect the following types of data:

- Demographic information (with the exception of country or language preferences)
- Financial account information, credit or debit card numbers, credit records, or payment data
- Social media or web browsing information
- Government-issues identifier such as social security, social insurance number, or Government ID
- Health information
- Sensitive data such as ethnic origin, political beliefs, trade union membership, health data, sexual orientation, and genetic data

Security

Q: What security measures are used by HP DaaS Analytics and Proactive Management to protect personal data?

A: When capturing, transmitting and storing data, HP DaaS Analytics and Proactive Management uses a variety of security technologies and procedures to help protect your personal data from unauthorized access, use, or disclosure. This includes:

1. Data stored in the U.S. and German regional data centers:
   - The databases that contain personal data located in U.S. and German regional data centers are encrypted.
   - Security credentials data (like HP DaaS Analytics and Proactive Management account passwords) are encrypted in these regional data centers using HP DaaS Analytics and Proactive Management application level encryption and SHA256 hashing.
   - Contact data (i.e. personal and/or business contact data including a customer and/or user's first name, last name, mailing address, telephone number, fax number, email address and other similar contact information for HP DaaS Analytics and Proactive Management accounts) are stored in clear text in both the U.S. and German regional data centers.
   - Location data (i.e. real-time geolocation of the device captured by HP DaaS Analytics and Proactive Management) is encrypted using HP DaaS Analytics and Proactive Management application level encryption and SHA256 hashing.
2. Data stored in the U.S. Analytics data center: Device, Application and Location data is de-identified and cannot be tied to an individual prior to being transmitted and stored in the U.S. Analytics data center.

Data Transmission and Storage

Q: What data types are transmitted and stored by HP DaaS Analytics and Proactive Management in the different data centers?

A: The following data types are transmitted and stored in the different data centers:

Data Category	U.S. Regional Data Center (for non-European based customers)	German Regional Data Center (for European based customers)	U.S. Analytics Data Center (for all customers)
Account data	Yes	Yes	No
Application data	Yes	Yes	Yes
Contact data	Yes	Yes	No
Device data	Yes	Yes	Yes
Location data	Yes	Yes	Yes
Security credentials data	Yes	Yes	No

Q: What data can a customer opt-out from sharing with HP DaaS Analytics and Proactive Management service?

A: The following table provides opt-out information:

Data Category	Opt-Out	Additional comments
Account data	No	
Application data	No	
Contact data	See Additional comments	A customer's first name, last name, e-mail and country information are mandatory information for a customer to provide. Mailing address and telephone number are optional.
Device data	No	
Location data	Yes	
Security Credentials data	No	

Q: What are the sources and methodology of data capture by HP DaaS Analytics and Proactive Management?

A: The sources and methodology of data capture include:

Data Category	Source	Methodology
Account data	Cloud-based HP DaaS Analytics and Proactive Management portal	The data is provided by customer, to be entered either by a HP DaaS Analytics and Proactive Management support specialist or directly by the customer in cloud-based HP DaaS Analytics and Proactive Management portal.
Application data	Cloud-based HP DaaS Analytics and Proactive Management portal and software	Automatic
Contact data	Cloud-based HP DaaS Analytics and Proactive Management portal	The data is provided by customer, to be entered either by a HP DaaS Analytics and Proactive Management support specialist or directly by the customer in cloud-based HP DaaS Analytics and Proactive Management portal.
Device data	Analytics and Proactive Management software	Automatic
Location data	Real-time geolocation of the device is captured by Analytics and Proactive Management software	Automatic
Security Credentials data	Cloud-based HP DaaS Analytics and Proactive Management portal	The data is entered by the customer in the cloud-based HP DaaS Analytics and Proactive Management portal.

Q: What location data is captured, transmitted and stored by HP DaaS Analytics and Proactive Management?

A: Customer address data

- In HP DaaS Analytics and Proactive Management, an HP DaaS customer using the cloud-based HP DaaS Analytics and Proactive Management portal can enter their address information to indicate either the customer's address. For example: country, city, postal code, street address, etc.
- This information is entered manually by the customer in the cloud-based HP DaaS portal.
- This is information is not mandatory.
- This information is transmitted to and stored in the U.S. or German regional data centers only.

Operating system country data

- The operating system locale of the devices enrolled in HP DaaS Analytics and Proactive Management.
- This is automatically captured from the device using HP DaaS Analytics and Proactive Management software on the device.
- This information is transmitted to and stored in U.S. and German Regional data centers and U.S. Analytics data center.

Real-time device location data

- The real-time geolocation location of the device (i.e. latitude and longitude of the device)
- This data is captured only if a HP DaaS customer enables location-based services from the cloud-based HP DaaS Analytics and Proactive Management portal for its fleet of devices in Analytics and Proactive Management.
- This data is captured from the device using HP DaaS Analytics and Proactive Management software on the device.
- The location-based services to track geolocation of devices by HP DaaS Analytics and Proactive Management is turned off by default for all customers and an option is provided for customers to enable or disable location-based services in cloud-based HP DaaS Analytics and Proactive Management portal. Even in case of location-based services turned on, HP DaaS Analytics and Proactive Management does not allow for collection of device location data for any devices classified as employee-owned of personal devices (within the cloud-based HP DaaS Analytics and Proactive Management portal).
- This data is transmitted to and stored in U.S. and German regional data centers. Personal data associated with Location data (i.e. real-time geolocation of the device captured by HP DaaS Analytics and Proactive Management to be leveraged for analytics) is de-identified prior to being transmitted and stored in the U.S. Analytics data center.

Asset tracking location data

- HP DaaS Analytics and Proactive Management allows customers to enter the location address of an asset using the cloud-based HP DaaS Analytics and Proactive Management portal. This is not the real-time device location data, but rather a label to identify a physical location of the asset. For example, Building 1, Floor 2.
- This information is entered manually by the customer in the cloud-based HP DaaS Analytics and Proactive Management portal.This information is transmitted to and stored in U.S. or German regional data centers and U.S. Analytics data center.

Q: How does HP DaaS Analytics and Proactive Management handle any personal data in Device Data present in the Environment Variables?

A: Environment variables may contain personal names in some of the variable values. Analytics and Proactive Management reads the logged-on Windows user name from the device, and if it is present in the environment variable values, it will remove these before transmitting and storing in U.S. Analytics data center.

However, if a user has provided a user name in the environment variable value that is not the logged-on Windows user name, then the service will not be able to remove this before transmitting and storing the environment variable value in the U.S. Analytics data center.

For example, if a user name is John Boe, and the logged-on windows user is jboe, and one of the environment variable value's is C:\Users\jboe\Documents, then APM will send and store this data as C:\Users\username\Documents. However, if the environment variable value's is C:\Users\john\Documents, then Analytics and Proactive Management will send and store this data as C:\Users\john\Documents in the U.S. Analytics data center.

Q: How does HP DaaS Analytics and Proactive Management handle any personal data in the Device Data present in Windows Event Logs?

A: Windows event logs from devices may contain personal data. Because of the volume and variety of the data, it is very difficult to understand, remove and/or sanitize all personal data from Windows event logs data that is transmitted to and stored in the U.S. Analytics data center. Analytics and Proactive Management does not leverage any personal data from Windows event logs in its analysis or output.

Data Protection

Q: Is data transmitted over public networks encrypted using TLS 1.1 or greater, IPsec or other industry standard strong encryption technologies?

A: HP DaaS Analytics and Proactive Management leverages TLS 1.2 to transmit data between device and the U.S and German regional data centers and the U.S Analytics data center.

Q: Is data (in databases, logs, configuration files, backup media, etc.) stored securely?

A: All databases in the U.S. and German regional data centers that store personal data are encrypted.

All databases and unstructured storage in the U.S. Analytics data center will be encrypted in H1 2018.

Q: Is personal data (in databases, logs, configuration files, backup media, etc.) stored in clear-text format

A: All databases in the U.S. and German regional data centers that store personal data are encrypted.

Additionally, in the U.S. and German regional data centers, HP DaaS Analytics and Proactive Management also provides application level encryption and SHA256 hashing for security credentials data like account passwords and real-time device location data.

Contact data (for personal and/or business including a customer's and/or user's first name, last name, mailing address, telephone number, fax number, email address etc., for DaaS Analytics and Proactive Management accounts) are stored in clear text in the U.S. and German regional data centers.

Q: Is data securely disposed of when no longer needed

A: All data in U.S. and German regional data centers is deleted permanently within thirty days after customer inactivation from HP DaaS Analytics and Proactive Management service.

Data in U.S. Analytics data center is deleted after five years from the date of data creation (**Note:** Any data to be leveraged for analytics is removed of personal data prior to transmission and storage in U.S. Analytics data center.)

Q: How is access to data restricted?

A: All the data collected and stored in U.S. and German regional data centers and in the U.S. Analytics data center is secured by Amazon Web Services (AWS) through IAM roles, authenticated users, and bucket policies.

Q: Does HP DaaS Analytics and Proactive Management share its data with its HP suppliers, and if so, does it include personal and anonymized information?

A: Yes, HP DaaS Analytics and Proactive Management shares performance data (disk, CPU, memory) with some of HP's key suppliers for the performance optimization of HP products. HP only provides aggregated and anonymous data without any reference to any HP DaaS Analytics and Proactive Management customer.

Q: Does HP DaaS provide separate, dedicated database(s) for customers' exclusive use of their data?

A: No.

Q: Is customer data and information co-hosted with the data from other organizations or companies on the same physical server(s)

A: Yes.

4AA7-2191ENW, February 8, 2018