Approved for External Audiences

DaaS

Analytics and Proactive Management Service Definition

HP DaaS Analytics and Proactive Management Service Definition

Contents

HP DaaS Analytics and Proactive Management Service Definition

Purpose of Document

This document provides a detailed description of HP Device as a Service (DaaS) Analytics and Proactive Management. Its purpose is to educate interested parties on current service capabilities related to HP's device health analytics and fully managed unified endpoint management service.

Service Description

As part of HP DaaS, the device health analytics and proactive endpoint management provided by HP places comprehensive data, reports and insights at the customer's fingertips. DaaS, which is cloud-enabled for scale and flexibility, continually monitors the fleet and reports device problems, or potential problems, including hard disk drive and battery health, overheating and thermal issues, firewall and antivirus settings, and security compliance, for example, and alerts the HP Service Agents . These highly trained Service Agents then use HP's multi-device, multi-OS analytics and endpoint management platform to manage devices for customers allowing them to offload day-to-day IT management functions so that staff can focus on more strategic projects for the company.

HP DaaS Analytics and Proactive Management features and functionality differ based on the HP DaaS plan selected - Standard, Enhanced or Premium.

Features at a Glance

Standard Plan

- Analytics and Reports
  - Hardware and Software Inventory
  - Device Health
  - Security and Compliance Status
- End-user self-help

Self Service

Enhanced Plan

All in the Standard Plan plus:

- Proactive monitoring and management by HP Agents
  - Security Policies and Enforcement
  - Device Locate/Alarm/Lock/Erase
  - Automatic Parts Replacement*
  - Remote Assistance

*HP in Warranty products only

HP Managed Services

Premium Plan

All in the Enhanced Plan plus:

- Windows Information Protection
- Password Recovery
- Application Deployment
- 3rd Party and OS Patch Management
- Wi-Fi Provisioning

HP Managed Services

Note: Service options in plans may also vary by region or country.

HP DaaS Analytics and Proactive Management Features by HP DaaS Plan[1]

Features	Standard plan	Enhanced plan	Premium plan
Bulk device enrollment Support for rapid deployment via software distribution tools	✓	✓	✓
Inventory and health monitoring Device and application inventory as well as monitoring device health including battery, hard drive, CPU utilization, crashes, and blue screen errors	✓	✓	✓
Dashboard with analytics and reports View detailed device and software inventory, system health, and real-time incident notifications	✓	✓	✓
Security monitoring, alerts and self-healing Monitoring and alerts for devices that are non-compliant with company standards and self-healing when a Windows firewall or anti-virus is disabled	✓	✓	✓
End-user self-help Easy access to Windows system repair and diagnostic utilities for commonly encountered problems that also includes the ability to request remote assistance from the same interface	✓	✓	✓
Predicative analytics Cutting-edge analytics identify systems at risk for disk, battery, or full-system thermal failure so you can take action before a problem occurs		✓	✓
Device locate/alarm/ lock/wipe Find, alarm, lock, or erase a lost or stolen device keeping data secure		✓	✓
Security policy setting and enforcement Security policy settings and enforcement to ensure compliance		✓	✓
Automatic parts replacement HP will inform you and automatically replace battery or hard drives to ensure your fleet is running smoothly		✓	✓
Proactive service agent An experienced HP Service Agent does the monitoring and proactive management for you		✓	✓
Remote assistance HP Service Agents remotely connect to and troubleshoot Windows devices for you		✓	✓
Windows OS patch management Your HP Service Agents stays on top of Windows OS patch deployments		✓	✓
Windows information protection Enforces encryption policies for sensitive company documents on client devices			✓
Password recovery Reset a forgotten local machine user account password on Windows notebooks, PCs, and tablets			✓
Application deployment HP Service Agents will deploy applications as specified by the customer on their behalf to managed devices			✓
3rd party patch management HP Service Agents deliver security and software updates for Microsoft Windows and 3rd-party applications such as Java, Flash, and Adobe Acrobat			✓
Wi-Fi provisioning Grant and revoke access to a wireless network for managed devices without exposing credentials to users			✓

[1] Features may vary by operating system. Refer to Feature Details by Product Type later in this document.

The Onboarding Process

1. Prior to creating an HP Analytics and Proactive Management account, the customer purchases an HP DaaS license key from their reseller or from HP.
2. The Managed Services team creates the license key and sends it along with customer details to the HP Service Agent.
3. The HP Service Agent sends a Welcome email with contract information and questionnaire along with .csv files for iOS and Windows 10 to the customer's designated IT Admin for completion.
4. The Customer IT Admin completes the questionnaire, and if necessary, adds .csv files, agrees to Terms and Conditions, and returns them to the HP Service Agent via the email address provided.
5. The HP Service Agent creates the customer account and password, enters the license key, and completes any required customization which may inlcude creating reporting and admin accounts as well as importing customer-provided .csv files, if necessary.
6. The HP Service Agent creates unique device PIN codes when a device list (.csv) file is received.
7. The HP Service Agent emails the instructions and files for enrolling customer devices to the customer IT Admin.
8. The customer IT Admin then performs the steps required to enroll customer end-user devices.

Responsibilities

HP Service Agent

The HP Service Agent's primary responsibilities include:

- Creating the HP DaaS Analytics and Proactive Management account in response to the input form from the HP account rep
- Adding or removing managed users and devices
- Tracking users and devices
- Deploying the requested applications
- Deploying default applications
- Rolling back OS updates in customer environment in case of failure[2]
- Updating customer applications[2]
- Monitoring devices and notifying customer when a device health issue is detected
- Generating and sending application usage and installed hardware reports
- Providing optimization and diagnostic tools for end users
- Troubleshooting installation and connectivity issues
- Assisting customer and answering product related questions
- Ensuring compliance with application licensing requirements[2]
- Removing apps[3] from the customers' Device App Catalog as necessary
- Attempting to remotely locate or erase data from a missing or stolen device[2]

[2] Upon request only.
[3] Customer should provide all the App dependency components such as Runtime environment platform, APIs, SDKs and Plug-ins/Drivers

Customer IT Administrator

The customer's designated IT Admin is responsible for the following tasks:

- Establishing an HP DaaS account, working with their HP account rep
- Installing the agent onto their DaaS managed devices
- Adding or removing managed users and devices
- Requesting application deployment or removal
- Reviewing hardware, software and other reports and taking action as necessary
- Troubleshooting and resolving common end-user support issues before of escalating to HP support
- Requesting device location or data erase on a device reported missing or stolen
- Ensuring compliance with software application licensing requirements[2]
- Renewing, changing or cancelling the HP DaaS account

Terms of Service

The terms that apply to the service are contained in several documents. All documents should be consulted to arrive at a comprehensive understanding of HP DaaS Analytics and Proactive Management's terms governing product use rights, data security and privacy, and confidentiality (non-disclosure).

Document	Relevance
HP Managed Services Terms and Conditions Click this link then select **Terms and Conditions** at the bottom of the webpage.	• Governs product use rights • Describes termination, addition/removal of users • Describes data usage, data privacy, data storage terms
HP Personal Data Rights Notice	• Describes personal data rights for users located in selected countries
HP Privacy Statement	• Describes collection and use of customer information • Describes collection and use of information about customer computer • Describes transfer of data
Service Level Agreement Click this link then select **Service Level Agreement** at the bottom of the webpage.	• Governs service uptime and availability • Describes service credit amounts • Describes claim eligibility and process

Availability

Locations

HP DaaS is currently available in the following locations:

North America	Europe	Asia
• Canada • US	• UK • Ireland • France	• Australia • New Zealand • India • Malaysia • Philippines • Singapore

Service Agent availability and languages supported

HP DaaS Support Structure				
Location	HP New Mexico Rio Rancho Supports: US, Canada	HP Tunisia Tunis Supports UK, IR	HP Tunisia Tunis Supports France	HP India, Bangalore Supports AU, NZ, IN, MY, PH, SG
Coverage (hours/days /excluding holidays)	12/5	10/5	10/5	24/7
Operating Hours	6 a.m.-6 p.m. MST, M-F	8 a.m.-6 p.m. CET, M-F	8 a.m.-6 p.m. CET, M-F	24/7
Language Supported	English	English	French	English
Note: Support is available via email as well as outbound chat and call back services.				

System Requirements

	PCs	Tablets	Smartphones
Operating Systems	Desktops, notebooks, workstations from any major vendor running: • Windows 7 Service 1 (SP1) • Windows 8.1 or higher	• iOS 10 or higher • Android 4.4 or higher • Windows 8.1 or higher (x86 or Intel platforms	• iOS 10 or higher • Android 4.4 or higher • Windows 10 Mobile
Browsers	• Google Chrome for Windows version 60.0 or higher • Internet Explorer for Windows version 11 or higher • Firefox for Windows version 55.0 or higher • Microsoft Edge for Windows version 40 or higher	• Chrome on Android version 60.0 or higher • Safari on iOS 10 or higher • Microsoft Edge for Windows latest version	• Chrome on Android version 60.0 or higher • Safari on iOS 10 or higher • Microsoft Edge on Windows 10 Mobile (Continuum recommended)
	Click here for requirement updates.		

Data Centers

HP DaaS Analytics and Proactive Management is hosted by Amazon Web Services (AWS), a scalable computing capacity and recognized leader in cloud hosting. Customer and device data are stored in AWS data centers that are geographically distributed to provide redundancy. By collaborating with AWS, HP analytics and management platform inherits a cloud infrastructure that has been architected to be one of the most flexible and secure cloud computing environments available today.

Data is secured at several levels, providing server authentication, data encryption, and data integrity. Because the Transport Layer Security (TLS) protocol is implemented beneath the application layer, it is a passive security mechanism that does not rely on additional steps or procedures from the user. This allows client applications and their users to have little or no knowledge of secure communications and still be better protected from attackers.

These features help secure data from incidental corruption and from malicious attack, and are intended to avoid common web-based threats. In addition to the encryption for network communication between the agent and the server, HP encrypts some of the "data at rest" (data stored in our server database). The user's login email and password are also encrypted through the TLS protocol upon logging in.

For detailed information on physical and environmental security, AWS access and network security, please read the AWS Overview of Security Processes whitepaper. For more information about the security regulations and standards with which AWS complies, see the AWS Compliance webpage.

For more information on HP DaaS data security, refer to the HP DaaS Security Whitepaper.

Feature Details by Product Type

Windows PCs and Tablets

- Bring Your Own Device (BYOD) Policy - Limits management capabilities for employee owned devices
- Bulk Device Enrollment - Enable large-scale enrollment of devices and users
- Lock Device - Perform a screen lock (PIN block) or Windows logoff on a managed device if it is reported lost or stolen
- Find Device - Pinpoint the location of a missing device on an online map
- Erase Device Data - Remove data from a managed mobile device, notebook, or desktop PC
- Firewall Policy - Monitor and enable the Microsoft Windows firewall service on Windows PCs
- Groups - Quickly apply policies to groups of users and/or devices
- Hard Disk Health - Monitor hard drives on managed notebooks and desktops. Get notified if a drive is full, needs replacement or has been changed to a different drive
- Microsoft Patch Management - Monitor operating system update status and apply patches. And monitors patch the status and identifies missing patches and installation success or failure
- Mobile Application Deployment - Create, distribute, and manage curated bundles of mobile applications from the Windows App Store. "Get Notified" is a required app that is not installed on a device
- Microsoft Windows Application Deployment - Create, distribute, and manage curated bundles desktop applications in the MSI or .exe file types to managed Windows devices. Get notified is a required app is not installed on a device
- Mobile Device Security Policy - Apply custom security levels to tablets and mobile devices
- Windows Information Protection - Protect against accidental data leakage by enforcing encryption and application access controls
- Password Recovery - Reset a forgotten machine local user account password on Windows notebooks PCs and tablets
- Remote Alarm - Sound an alarm to locate a nearby missing Windows or Android mobile device
- Remote Assistance - Sound an alarm to locate a nearby missing Windows or Android mobile device
- Smart Battery Health Monitor - Monitor battery charge capacity and wear on managed notebooks and tablets. Get notified when a battery is not detected or needs a replacement
- Software Inventory - Automatically discover and track which applications are installed across all your managed devices
- Thermal Monitoring and Alert - Get notified when a system needs maintenance due to a heat-related issue

- Third Party Software Patch Management - Monitor application versions and apply patches for a wide range of popular software applications. Also, view the status of all managed patches identifying missing patches and successful or failed installations
- User and Device Inventory - Provide a list of monitored PCs, mobile devices and users, as well as detailed device information such as available space, memory, OS version and other details
- Virus Protection Policy - Detect whether antivirus software has been enabled on a Windows device. If not, automatically enable and monitor Microsoft Windows Defender or Microsoft Security Essentials
- Warranty Tracking - Know the warranty expiration dates for HP devices. Proactively plan your hardware refresh cycles
- Wi-Fi Provisioning - Grant and revoke access to a wireless network for managed devices without exposing network passwords or credentials to users
- System Performance Monitoring - Get notified when CPU or memory is consistently running at a high percentage level, which may indicate a system problem or need for upgrade
- OS Crash Monitoring - Monitor OS for unexpected system crashes and blue screen events and generate an incident when these are detected
- Self-help Tool - Ability for end-users to troubleshoot and resolve common issues instead of escalating to the support team
- End user Help Request - Ability for end-users to request help from within the device. Each request is formally tracked by the HP Service Agent. Service Agents can immediately view the full hardware & software inventory, and identify root causes such as component failure, missing patches, outdated drivers or bios
- Non-reporting Device Monitoring - Get alerted if a managed device has not communicated with the management server for more than one week
- Azure Active Directory Federation- Ability to provision users and enable customer logon using Azure AD login credentials
- Visual and Detailed Reports - View and extract fleet level intelligence with advanced analytics and reports on security compliance, missing mandatory apps, and more

Windows 10 Mobile Smartphones

- Bring Your Own Device (BYOD) Policy - Limits management capabilities for employee owned devices
- USA and European Data Centers - Multiple data centers to support customers worldwide
- Lock Device - Perform a screen lock (PIN block) or Windows logoff on a managed device if it is reported lost or stolen
- Find Device - Pinpoint the location of a missing device on an online map
- Erase Device Data - Remove data from a managed mobile device, notebook, or desktop PC
- Groups - Quickly apply policies to groups of users and/or devices
- Mobile Device Security Policy - Apply custom security levels to tablets and mobile devices
- Windows Information Protection - Protect against accidental data leakage by enforcing encryption and application access controls
- Software Inventory - Automatically discover and track which applications are installed across all your managed devices
- User and Device Inventory - Provide a list of monitored PCs, mobile devices and users, as well as detailed device information such as available space, memory, OS version and other details

- Non-reporting Device Monitoring - Get alerted if a managed device has not communicated with the management server for more than one week
- Azure Active Directory Federation- Ability to provision users and enable customer logon using Azure AD login credentials
- Visual and Detailed Reports - View and extract fleet level intelligence with advanced analytics and reports on security compliance, missing mandatory apps, and more
- Mobile Application Deployment - Create, distribute, and manage curated bundles of mobile applications from the Windows App Store. "Get Notified" is a required app that is not installed on a device

iOS *Tablets and Smartphones*

- Bring Your Own Device (BYOD) Policy - Limits management capabilities for employee owned devices
- USA and European Data Centers - Multiple data centers to support customers worldwide
- Bulk Device Enrollment - Enable large-scale enrollment of devices and users
- Lock Device - Perform a screen lock (PIN block) or Windows logoff on a managed device if it is reported lost or stolen
- Find Device - Pinpoint the location of a missing device on an online map
- Erase Device Data - Remove data from a managed mobile device, notebook, or desktop PC
- Groups - Quickly apply policies to groups of users and/or devices
- Mobile Application Deployment - Create, distribute, and manage curated bundles of mobile applications from the Windows App Store. "Get Notified" is a required app that is not installed on a device
- Mobile Device Security Policy - Apply custom security levels to tablets and mobile devices
- Software Inventory - Automatically discover and track which applications are installed across all your managed devices
- User and Device Inventory - Provide a list of monitored PCs, mobile devices and users, as well as detailed device information such as available space, memory, OS version and other details
- Wi-Fi Provisioning - Grant and revoke access to a wireless network for managed devices without exposing network passwords or credentials to users
- End user Help Request - Ability for end-users to request help from within the device. Service Agents can immediately view the full hardware and software inventory, and identify root causes
- Non-reporting Device Monitoring - Get alerted if a managed device has not communicated with the management server for more than one week
- Azure Active Directory Federation- Ability to provision users and enable customer logon using Azure AD login credentials
- Visual and Detailed Reports - View and extract fleet level intelligence with advanced analytics and reports on security compliance, missing mandatory apps, and more
- Apple DEP – Over-the-Air (OTA) device enrollment and persistent enforcement of mobile device policies using Apple's Device Enrollment Program (DEP)

Tablets and Smartphones

- Bring Your Own Device (BYOD) Policy - Limits management capabilities for employee owned devices
- USA and European Data Centers - Multiple data centers to support customers worldwide
- Bulk Device Enrollment - Enable large-scale enrollment of devices and users
- Lock Device - Perform a screen lock (PIN block) or Windows logoff on a managed device if it is reported lost or stolen
- Find Device - Pinpoint the location of a missing device on an online map
- Erase Device Data - Remove data from a managed mobile device, notebook, or desktop PC
- Groups - Quickly apply policies to groups of users and/or devices
- Mobile Application Deployment - Create, distribute, and manage curated bundles of mobile applications from the Windows App Store. "Get Notified" is a required app that is not installed on a device
- Mobile Device Security Policy - Apply custom security levels to tablets and mobile devices
- Remote Alarm - Sound an alarm to locate a nearby missing Android mobile device
- Software Inventory - Automatically discover and track which applications are installed across all your managed devices
- User and Device Inventory - Provide a list of monitored PCs, mobile devices and users, as well as detailed device information such as available space, memory, OS version and other details
- Wi-Fi Provisioning - Grant and revoke access to a wireless network for managed devices without exposing network passwords or credentials to users
- End user Help Request - Ability for end-users to request help from within the device. Service Agents can immediately view the full hardware and software inventory, and identify root causes
- Non-reporting Device Monitoring - Get alerted if a managed device has not communicated with the management server for more than one week
- Azure Active Directory Federation- Ability to provision users and enable customer logon using Azure AD login credentials
- Visual and Detailed Reports - View and extract fleet level intelligence with advanced analytics and reports on security compliance, missing mandatory apps, and more

4AA7-1446ENW – October 24, 2017