Approved for External Audiences

HP Device as a Service (DaaS)

Analytics and Proactive Management Service Definition

Contents

HP DaaS Analytics and Proactive Management Service Definition

Service Description

As part of HP DaaS, the analytics and proactive management capability provided by HP places comprehensive data, reports and insights at the customer's fingertips. HP 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 Experts. These highly trained Service Experts then use HP's multi-device, multi-OS analytics and endpoint management platform to manage devices and applications 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 (APM) features and functionality differ based on the HP DaaS plan selected - Standard, Enhanced or Premium. Analytics and Proactive Management does not include any form of onsite "break-fix" support OR any onsite support Service Level Agreement (SLA), however, these can be purchased separately and included in the HP DaaS contract.

The Onboarding Process

Prior to creating an HP Analytics and Proactive Management account, the customer purchases an HP DaaS license key from their reseller or from HP.

Standard Plan

1. An HP Service Expert and/or partner (if applicable) to schedule a customer conference call(s) to:
   - Review the customer on-boarding experience and expectations.
   - Exchange point of contact information, including to designate user(s) for the Analytics and Proactive Management portal.
   - Discuss and document customer network environment.
   - Complete the written agreement for the customer to give partner access to reports (if applicable).
   - Collect details on the customer's Azure Active Directory (AAD) implementation.
   - Schedule a call for the device enrollment steps based on the agreed upon deployment schedule.
2. Once all these items are documented and agreed to, an HP Service Expert will create the customer account and add partner (if applicable) as a report admin.
3. The HP Service Expert will email the customer with the following information and/or partner:
   - Account information
   - Device enrollment instructions
   - Report Admin details
   - Support contact information
4. Deployment Kick Off Call – An HP Service Expert will meet with customer and/or partner (if applicable) to start device enrollment and help with any issues.
   - HP to validate that customer has access to the Analytics and Proactive Management dashboard.
   - HP to reconfirm to customer the instructions on how to get help from within the Analytics and Proactive Management dashboard.
   - HP will show the customer how to navigate the site and pull reports.
5. Validation that the customer can independently complete the deployment.
6. Customer completes device enrollment, based on customer preference and confirms with the HP Service Expert that the initial deployment is complete.

Enhanced and Premium Plans

Prior to creating an HP Analytics and Proactive Management account, the customer purchases an HP DaaS license key from their reseller or from HP.

Phase 1: Information Gathering

1. The HP Service Expert will work with the Account Delivery Manager and/or partner (if applicable), to schedule a customer conference call(s) to:
   - Review the customer on-boarding experience and expectations.
   - Exchange point of contact information.
   - Discuss and document customer network environment.
   - Discuss how customer uses devices and what they are trying to accomplish.
   - Develop customer configuration and deployment plan including schedule and requested start date.
   - Explain and provide written agreement for HP to give partner access to reports (if applicable).
   - Outline automated parts replacement process.
   - Discuss Apple Device Enrollment Program (DEP) for existing installed base (if applicable).
   - Discuss Azure Active Directory (AAD) (if applicable).
   - Collect a CSV file containing end user names and emails (or serial numbers).

Phase 2: HP Recommendations and Account Creation

2. HP Service Expert meets with customer and Account Delivery Manager and/or partner (if applicable) to provide recommendations on how to proceed based on the specific customer use cases and customer environment. HP recommends a configuration designed to try to be the best fit for the customer. This is an iterative process. Once the customer agrees on the configuration, then HP can create the customer account in Analytics and Proactive Management and schedule a call for the device enrollment steps based on the agreed upon deployment schedule.
3. An HP Service Expert will create the customer account in Analytics and Proactive Management.
4. The HP Service Expert will add the partner as a report admin (if applicable).
5. The HP Service Expert will email the customer with the following information, copy Account Delivery Manager and/or partner (if applicable):
   - Account information
   - Device enrollment instructions
   - Report Admin details
   - Support contact information

Phase 3: Deployment

6. Deployment Kick Off Call – the HP Service Expert will meet with the customer and Account Delivery Manager and/or partner (if applicable) to start device enrollment and help with any issues.
   - HP will validate that customer has access to the Analytics and Proactive Management dashboard.
   - HP will reconfirm the instructions with the customer on how to get help from within the Analytics and Proactive Management dashboard.
   - HP will show the customer how to navigate the site and pull reports.
7. Validate that the configuration HP delivered meets customer's expectations and that the customer is autonomous to complete the deployment on their own.
8. The customer completes device enrollment, based on customer preference and confirms with HP that the deployment is complete.

Roles and Responsibilities

HP Service Expert

The HP Service Expert's primary responsibilities include:

- Create the HP DaaS Analytics and Proactive Management account in response to the input from the HP account rep or customer
- Add or remove managed users and devices
- Track users and devices
- Request and default application deployment and updates
- Remove requested apps from the customer's Device App Catalog
- Monitor devices and notify customer when a device health issue is detected. Also, provide optimization and diagnostic tools to resolve health issues
- Generate and send requested reports
- Provide optimization and diagnostic tools for end users
- Troubleshoot installation and connectivity issues
- Assist customer and answering service related questions
- Help ensure compliance with application licensing requirements
- Attempt to remotely locate or erase data from a missing or stolen device

Customer IT Administrator

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

- Establish an HP DaaS account, working with their partner or HP account rep
- Install the Analytics and Proactive management software onto their DaaS managed devices
- Request add or remove managed users and devices
- Request application deployment or removal
- Review hardware, software and other reports and taking action as necessary
- Troubleshoot and perform triage for common end-user support issues before escalating to HP support
- Roll back OS updates in customer environment in case of failure
- Request device location or data erase on a device reported missing or stolen
- Ensure compliance with software application licensing requirements
- Renew, change or cancel the HP DaaS account

  Note: Authorized personnel could include a partner if the customer pre-approves a specific individual within the partner organization to have access to the customer's Analytics and Proactive Management account.

HP Account Delivery Manager

The objective of an HP Account Delivery Manager (if applicable), is to help ensure HP is meeting its contract goals and be a proactive, trusted customer advisor.

Account Delivery Manager's primary responsibilities can include:

- Account transition and setup
- Business reviews
- Account planning
- Business Collaboration

- Fleet management
- Contract administration
- Services and 3rd party management
- Internal HP deliverables
- Customer specific requests

Partner

The partner (if applicable) is responsible for the following tasks:

- Ensure the HP Analytics and Proactive Management Care Pack is registered.
- Schedule and host meetings with HP and customer as needed.
- If applicable, provide business insights and expert analysis for customer environment leveraging Analytics and Proactive Management reports.
- Assist customer with device enrollment as needed.

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 DaaS 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 Click this link then select **Personal Data Rights** at the bottom of the webpage.	• Describes personal data rights for users located in selected countries
HP Privacy Statement Click this link then select **Privacy** at the bottom of the webpage.	• 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

Service Expert availability and languages supported:

HP DaaS Analytics and Proactive Management Support Structure								
	May 2017	May 2017	May 2017	Feb 2018	Feb 2018	Feb 2018	May 2017	May 2017
Language Supported	US, Canada	UK, IR	France	GE, AT, CH, Lu	China	Japan	India	AU, NZ, MY, PH, SG
Coverage (excluding holidays)	12/5 hrs/day	10/5 hrs/day	10/5 hrs/day	10/5 hrs/day	24/7 hrs/day	12/7 hrs/day	24/7 hrs/day	24/7 hrs/day
Operating Hours	6AM-6PM MST, M-F	8 a.m.-6 p.m. CET, M-F			24/7	8AM-8PM CST	24/7	
Language Supported	English	English,	French	German	English, Chinese	Japanese	English	English
Support routes	Email, chat	Email, chat	Email, chat	Email, chat	Email, chat	Email, chat	Email, chat	Email, chat
Email add	ManagedServices@hp.com	ManagedServices_EMEA@hp.com	ManagedServices_EMEA@hp.com	ManagedServices_EMEA@hp.com	Managedservices_CHINA@hp.com	Managedservices_JAPAN@hp.com	ManagedServices_APJ_India@hp.com	ManagedServices_APJ@hp.com

Note: Primary Support is available via email. Outbound chat and Call back are available as needed.

System Requirements

Windows PC operating systems

Desktops or notebooks from any major vendor running Windows 7 Service Pack 1 (SP1), Windows 8.1 or Windows 10.

Supported browsers:

- Google Chrome for Windows: Version 63.0 or higher
- Internet Explorer for Windows: Version 11 or higher (Windows 7 SP1 or 8.1 only)
- Firefox for Windows: Version 57.0 or higher
- Microsoft Edge for Windows: 40.0 or higher (Note: Your PC does not need to be manufactured by HP.)

Mobile device operating systems

- iOS 10 or higher
- Android 4.4 or higher (Note: Your mobile device does not need to be manufactured by HP.)

Mobile device browsers

- Chrome on Android: 63 or higher
- Safari on iOS 10 or higher

Network requirements

An Internet connection is required for communications between the managed device and the cloud management service.

To check for updates to the system requirements list for HP DaaS Analytics and Proactive Management, please see the following web page: https://www.hpdaas.com/requirements.

Data Centers

The HP DaaS Analytics and Proactive Management platform is hosted on Amazon Web Services (AWS), a scalable computing infrastructure.

The HP DaaS Analytics and Proactive Management platform maintains data centers in Oregon, United States (AWS-OR) and Frankfurt, Germany (AWS-DE). The United States and German data centers can be used to differentiate customers from different regions and act as regional data centers. EU-based customers may prefer to use the German regional data center, while customers from all other countries may prefer to use the U.S. regional data center. Having the two data centers, allows HP DaaS Analytics and Proactive Management to localize personal data within each of the regions. All data within a single customer "tenant" is hosted in a single regional 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.

Data analytics for HP DaaS Analytics and Proactive Management services are performed in the United States Analytics data center. For data protection purposes, all personal data is de-identified and cannot be tied to an individual, prior to transmission and storage in the U.S. Analytics data center.

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. 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.
2. 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.
3. 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. All databases and unstructured storage in the U.S. Analytics data center will be encrypted in H1 2018.
4. 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.

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

For more information on HP DaaS Analytics and Proactive Management's data collection, transmission, storage, retention and disposal of data, refer to HP DaaS Analytics and Proactive Management Data Management FAQ.

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

Service Level Objectives

Event type	Initial Response	Service Level Objective (*)
On-boarding kick-off	HP Onboarding team first contact with customer	Two days to two weeks from registration in HP Systems
Email from customer to HP DaaS Support mail node.	Acknowledgement of email receipt	Email sent within 2 business hours local time
Proactive Incidents		
Critical	Email notification with Incident details (one email per notification)	Email sent within 4 business hours local time
High	Periodic report sent over email	Default Frequency: every business day
Medium	Periodic report sent over email	Default Frequency: Monthly *Customer can request weekly or bi-monthly reports.*
Low	Periodic reports sent over email	Default Frequency: Monthly *Customer can request weekly or bi-monthly reports.*

(*) These Service Level Objectives only cover HP Inc. lead time to engage with the customer and notify the customer of particular DaaS devices conditions. Issues resolution is not covered by the above Service Level Agreement.

HP DaaS Standard Plan

1. Azure Active Directory identity integration: Enable access to HP Analytics and Proactive Management using the customer's Azure Active Directory logon credentials.
   - Supported operating systems: See web browser system requirements above for details.
   - Customer responsibilities:
     - Provide Azure Active Directory import credentials (only required if user import is requested)
   - HP responsibilities:
     - Import Azure Active Directory users upon customer request
2. Device performance CPU monitoring: to determine if a device has a high CPU utilization consistently over the last 30 days.
   - Supported operating systems: Windows PC 7 SP1, or 8.1 and above.
   - Customer responsibilities: Review the device utilization report and consider upgrading to a higher performance device.
   - HP responsibilities: HP will provide a monitoring tool to detect and notify when there is a device health issue.
3. Device performance memory monitoring: to determine if a device consistently has a high memory utilization, over the last 30 days.
   - Supported operating systems: Windows PC 7 SP1, or 8.1 and above.
   - Customer responsibilities: Review the device utilization report and consider upgrading the memory of the device or the device to meet the user's needs.
   - HP responsibilities: HP will provide a monitoring tool to detect and notify when there is a device health issue.
4. End-user info: Ability to quickly search and view user's information such as name, email, and the user's devices.
   - Supported operating systems: All supported OS (iOS, Windows and Android).
   - Customer responsibilities: Review hardware, software inventory and other reports and act as needed.
   - HP responsibilities: HP will provide a tool to track users and devices.

5. Hard Disk Health - Hard Disk Drive full: Monitor hard drives on managed notebooks and desktops, and to determine if the hard disk drive storage capacity is full, preventing the OS and/or software from being properly updated or patched.
   - Supported operating systems: Windows PC 7 SP1, or 8.1 and above.
   - Customer responsibilities: Review the Hardware Health report and work with end-users to ensure data is backed up and hard disk drive space is routinely cleaned up. If a user needs more storage capacity, consider addition of a second hard disk drive if the system supports it, or an upgrade to a higher capacity HDD.
   - HP responsibilities: Provide a monitoring tool to help detect and notify when there is a device health issue.
6. Hardware inventory report: Detailed information of hardware inventory of managed devices such as processor, hard disk drive and storage, graphics, and total memory in addition to the device serial number, model and manufacturer.
   - Supported operating systems: All supported OSs (iOS, Windows and Android).
   - Customer responsibilities: Review hardware inventory reports and act as needed.
   - HP responsibilities: HP will provide a tool which enables the customer to track users and devices.
7. Mass device enrollment: Simplifies large-scale enrollment of devices and users. Simultaneously enroll and provision many devices with a single PIN code.
   - Supported operating systems: Windows 7 SP1, Windows 8.1 or above.
   - Customer responsibilities: customer IT admins can perform push deployment installations of the HP Analytics and Proactive Management software through a login script (domain joined environments) or deploy the Analytics and Proactive Management software using their existing software distribution tool set (*e.g.*, SCCM).
   - HP responsibilities: HP will provide the companywide PIN and other device enrollment details needed for mass deployment. Analytics and Proactive Management user accounts can be created rapidly. Device(s) can be silently enrolled.
8. Non-reporting device: Report if a managed device has not connected to Analytics and Proactive Management for 7 days.
   - Supported operating systems: All supported OS (iOS, Windows and Android).
   - Customer responsibilities: Review the Non-reporting Devices report and identify the source of the issue in collaboration with the end user. If the device no longer needs to be managed by HP Analytics and Proactive Management tool, then the device can be removed.
   - HP responsibilities: HP will provide a tool to track users and devices, and which allows the customer to see devices which have not reported in to Analytics and Proactive Management.
9. Optimization and diagnostic tools for end-users: Ability for end-users to troubleshoot and resolve common issues instead of escalating to their company's support team.
   - Supported operating systems: Windows 7 SP1, Windows 8.1 or above.
   - Customer responsibilities: End-users will run a tool to optimize the device or resolve common issues on their own before contacting the support team.
   - HP responsibilities: Provide a utility on managed Windows devices which enables access to OS and device diagnostic tools locally on end-user devices.
10. OS and Software Health – blue screen errors: Reports blue screen errors.
    - Supported operating systems: Windows 7 SP1, Windows 8.1 or above.
    - Customer responsibilities: Review Blue Screen Errors report and work with end-user to try and identify the root cause. Where possible, try to fix OS-related crash issues to prevent future device downtime and/or data loss.
    - HP responsibilities: HP will provide a monitoring tool to detect and report when there is a device health issue.

11. Software Inventory: Enables the IT Administrator to view the operating system version and software applications installed on a managed device. This includes the ability to view when an app was last updated, the top app installed within your fleet, and a list of most recently installed/updated apps.
    - Supported operating systems: All supported OS (iOS, Windows and Android).
    - Customer responsibilities: Review Software Inventory and other reports and identify actionable details as needed.
    - HP responsibilities: HP will provide a tool to track users and devices.
12. Visual dashboard summary and detailed reports: View and extract fleet level intelligence with an advanced view of reports.
    - Supported operating systems: All supported OS (iOS, Windows and Android).
    - Customer responsibilities: Review hardware, software and other reports to gain actionable information on the device fleet.
    - HP responsibilities: HP will provide a tool to track users and devices.
13. Warranty tracking: View the warranty expiration dates for HP devices and use this information to proactively plan your hardware refresh cycles.
    - Supports HP devices.
    - Customer responsibilities: Review Hardware Warranty report and have knowledge regarding warranty for HP Hardware.
    - HP responsibilities: HP will provide a tool to track users and devices.

----------THE STANDARD PLAN FEATURES END HERE----------

HP DaaS Enhanced Plan

HP Service Experts will perform the following additional tasks for Enhanced service plan customers:

14. Azure Active Directory identity integration: Enable UEM policy management based on end user Azure AD identity.
    - Supported operating systems: See web browser system requirements above for details.
    - Customer responsibilities:
        - Perform AAD link configuration steps
        - Provide AAD base domain name to HP Service Expert
        - Provide the AAD "SAML Single Sign-On Service URL" to the HP Service Expert
        - Add and assign users to AirWatch in the Azure Portal and providing the user list to HP Service Expert
    - HP responsibilities:
        - Import Azure AD user upon customer request
        - AirWatch configuration steps
        - Provide "Sign on URL" to customer
        - Provide "Identifier" to customer
        - Add users to AirWatch
15. Smart Battery Health – advance failure notification: Get notified in advance when a managed HP manufactured computer battery needs replacement soon.
    - Supports HP devices.
    - Customer responsibilities: Review Battery Replacement Report being addressed by Service Experts. If needed, assist HP Service Experts on some issues which can only be addressed by customer or end-user action (e.g. non- reporting devices, battery replacement).
    - HP responsibilities: HP Service Experts will proactively manage end-users' device battery health issues. HP will collaborate with the customer to ship a replacement part if a device is under warranty or is similarly covered under contract terms.
16. Smart Battery Health - not detected: If not detected, an incident will be generated.
    - Supports HP devices.
    - Customer responsibilities: Review the device health report and replace field replaceable parts.
    - HP responsibilities: HP will provide a monitoring tool to detect and notify the customer if it appears the battery has been removed from the device.
17. Bring Your Own Device (BYOD) Policy: Allows the user to designate their managed device as either company owned or employee-owned/personal (BYOD). Certain administrative functions are limited on devices designated at personally-owned. Some restricted functions include: Software Inventory, Find Device, and Wipe Device
    - Supported operating systems: All supported OS (iOS, Windows and Android).
    - Customer responsibilities: Review report and inform HP Service Experts if any device is incorrectly set as BYOD and needs to be designated as company-owned.
    - HP responsibilities: HP Service Experts will collaborate with the customer IT Administrator to help ensure managed devices are properly configured.
18. Multi tenancy access: The HP Proactive Support team has the ability to efficiently manage multiple customers from the same management console/dashboard.
    - Supported operating systems: All supported OS (iOS, Windows and Android).
    - Customer responsibilities: Review reports and track progress of device health issues being addressed by the HP Service Experts. If needed, assist HP Service Experts on issues which require action on the part of the customer or end-user (e.g.: non-reporting devices, battery replacements).
    - HP responsibilities: HP Service Experts will leverage a secure, integrated, single sign on solution to efficiently and proactively review and address device health issues. Each customer's data is separated logically and physically from that of other customers.

19. Remote Assistance: The HP Proactive Services Support team has the ability to remotely assist end-users using web based tools to chat with and/or initiate remote control sessions with end-user devices.
    - Supported operating systems: Windows 7 SP1, Windows 8.1 or above.
    - Customer responsibilities: End-users who receive an alert from the HP Service Expert can initiate a chat or remote-control session with the end-user to diagnose and troubleshoot device health issues. The user has option to decline or accept the chat or remote controls request to the device.
    - HP responsibilities: HP Service Experts can remotely assist an end-user on device health related issues as needed.
20. Group assignment of users and devices: Quickly apply security policies to group of devices or deploy apps to groups of users.
    - Supported operating systems: All supported OS (Windows iOS and Android)
    - Customer responsibilities: Provide instructions to the HP Service Expert on group and policy definitions for the respective groups.
    - HP responsibilities: HP Service Experts work will define the user and device groups as per the customer IT Administrator's instructions.
21. Hard Disk Health – advance failure notification: Monitor hard drives on managed notebooks and desktops, and generate incidents if a drive has stability issues and needs replacement.
    - Supported operating systems: Windows 7 SP1, Windows 8.1 or above.
    - HP responsibilities: HP Service Experts proactively manage end-users' device health issues. If HP predicts an imminent hard disk failure within 30 days or if a hard disk failure has occurred, HP will collaborate with the customer according to HP's break/fix process to ship a replacement part if the device is qualified for DaaS automatic parts replacement or is similarly covered under the service contract terms.
    - Customer responsibilities: Respond to HP Service Experts for any automatic parts replacement services, including confirming shipping address and other information. Follow the automatic parts replacement process.
22. Hardware inventory - HDD change: Monitor hardware configuration and generate an incident if the hard drive has been replaced with another.
    - Supported operating systems: All supported OS (iOS, Windows and Android).
    - Customer responsibilities: Review the incident and work with the end-user to confirm the hard disk change was approved.
    - HP responsibilities: HP will provide a tool which enables the customer to track users and devices.
23. Hardware inventory - total memory changed: Monitor total memory and generate an incident if the total memory has been changed from a previous state.
    - Supported operating systems: All supported OS (iOS, Windows and Android).
    - Customer responsibilities: Review the incident and confirm with the end-user the memory change was approved.
    - HP responsibilities: HP will provide a tool which enables the customer to track users and devices.
24. Hardware health - Thermal alerts: Detect if a system is running hotter than normal, especially for a given HP model, and may require hardware maintenance.
    - Supported operating systems: Windows 7 SP1, Windows 8.1 or above.
    - Customer responsibilities: Review report and track progress of device health issues being addressed by HP Service Experts. If needed, assist HP Service Experts for issues which can only be addressed by onsite action by the customer IT Administrator or end-user (e.g. ensure the device is stationed in a location with proper airflow, clean dust off the fan and internal other components).
    - HP responsibilities: HP Service Experts will proactively manage end-users' device health issues and notify the customer if there are devices which require maintenance for thermal problems.

25. Non-reporting device: Generate an incident if a managed device has not connected to Analytics and Proactive Management for 7 days.
    - Supported operating systems: All supported OS (iOS, Windows and Android).
    - Customer responsibilities: Review the Non-reporting Devices report and identify the source of the issue in collaboration with the end user. If the device no longer needs to be managed by HP Analytics and Proactive Management tool, then the device can be removed.
    - HP responsibilities: HP will provide a tool to track users and devices, and which allows the customer to see devices which have not reported in to Analytics and Proactive Management.
26. Security – Antivirus: Monitor and generate incident if antivirus software has been disabled.
    - Supported operating systems: Windows 7 SP1, Windows 8.1 or above.
    - Customer responsibilities: Review report and validate with end user to confirm ensure device virus protection software is always enabled.
    - HP responsibilities: HP will provide a monitoring tool to detect devices where antivirus software is not detected or disabled on a managed Windows device.
27. Security – Firewall: Monitor and generate incident if software firewall has been disabled.
    - Supported operating systems: Windows 7 SP1, Windows 8.1 or above.
    - Customer responsibilities: Review report and work with end-user to ensure device firewall protection software is always enabled.
    - HP responsibilities: HP will provide a monitoring tool to detect and notify when active firewall software is not detected on a managed Windows device.
28. OS and Software Health – unexpected and/or blue screen errors: Monitor and generate incident if the system has an unexpected OS crash or abnormal shutdown event. For blue screen errors, an error code and link to Microsoft KB article will be provided, if available.
    - Supported operating systems: Windows 7 SP1, Windows 8.1 or above.
    - Customer responsibilities: Review Blue Screen Errors – Top Errors and/or Blue Screen Errors – Top Devices reports and work with end-user to try and identify the root cause. Where possible, try to fix OS-related crash issues to prevent future device downtime and/or data loss.
    - HP responsibilities: HP will provide a monitoring tool to detect and notify when there is a device health issue.
29. Incident management system: The incident management system reports detected issues into a problem tracking system. HP Service Experts use the same problem tracking system to identify issues and recommend resolution options. The incident system tracks issue priority, type, details, comments and resolution details. The incident management system also links incidents to the affected device to enable rapid problem diagnostics.
    - Supported operating systems: All supported OS (Windows, iOS and Android).
    - Customer responsibilities: Review report and track progress of device health issues being addressed by HP Service Experts. If needed, assist HP Service Experts where an issue can only be addressed onsite by the customer IT Administrator or end-user (example: non-reporting device, battery replacement).
    - HP responsibilities: HP Service Experts proactively manage end-users' device health issues from a central dashboard. The team will collaborate with the customer to provide resolution options for the customer to act upon.
30. Lost device - Wipe Device Data: Remove data from a managed mobile device, notebook, or desktop PC. Devices will be reset to factory default settings.

31. Supported operating systems: All supported OS (Windows 10, iOS and Android).
    - Customer responsibilities: The customer IT Administrator or end-user informs the HP Service Expert. HP will then send a remote erase command to the device.
    - HP responsibilities: The HP Service Expert will verify the user identity and then send the remote command as requested.
32. Lost device - Find Device: Pinpoint the location of a missing device on an online map. 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 or personal devices (within the cloud-based HP DaaS Analytics and Proactive Management portal).
    - Supported operating systems: All supported OS (Windows 10, iOS and Android).
    - Customer responsibilities: The customer IT Administrator or end-user informs the HP Service Expert. HP will then send a remote command to the device. If the customer has user privacy concern the customer IT Administrator may request that the HP team disable this feature.
    - HP responsibilities: HP Service Experts will verify the user identity and then send the remote command as requested. HP will then inform the customer of the last known location of the device. The customer IT Administrator may request that the feature be disabled, at which point the HP team member will configure the Find feature to be disabled for all devices. The Find command is also disabled for designated personal-owned devices.
33. Lost device - Lock Device: Perform a screen lock (PIN block) or Windows logoff on a managed device if it is reported lost or stolen.
    - Supported operating systems: All supported OS (iOS and Android).
    - Customer responsibilities: The customer IT Administrator or end-user informs the HP Service Expert. HP will then send a remote command to the device.
    - HP responsibilities: HP Service Experts will verify the user identity and then send the remote lock command as requested.
34. Microsoft Patch Management: HP Analytics and Proactive Management leverages modern management techniques to deliver update management via third party Unified Endpoint Management tools. This approach allows configuration and control of Windows Update.

    Service Flow:
    - HP Service Expert and Account Delivery Manager (if applicable) captures configuration information from company IT to specify Service Options (below), including deployment rings
    - HP Service Expert will configure policies in the Unified Endpoint Management tool as specified
    - HP Service Expert will configure a QA ring containing devices and/or users specified by customer
    - HP Service Expert will assign devices/user to rings based on Customer requirements
    - If no issues are found during QA, update deployment will proceed automatically to additional rings
    - If issues are found by customer in QA ring
        - HP Service Expert will pause deployment to remaining rings
        - Customer will provide relevant data to HP Service Expert or Account Delivery Manager (if applicable)
        - HP Service Expert will report issue to Microsoft and/or appropriate vendor
    - Customer will contact Account Delivery Manager or HP Service Expert to make changes to Update policy

HP Responsibilities:

- Gather requirements from customer
- Create necessary rings and update profiles based on customer specifications
- Assign device and/or users to rings/profiles based on customer specifications
- Pause updates in response to customer report of update issue
- Report issues with updates to Microsoft and/or third-party vendor
- Resume update policy after issue resolution

Customer Responsibilities:

- Communicate configuration requirements to HP Service Experts, including deployment ring structure, timing, and options
- Provide user or device assignment to deployment rings
- Maintain QA ring (indicative hardware, image, software, etc.)
- Perform QA on updates deployed to the QA ring
- Report issues encountered to HP Account Delivery Manager or HP Service Expert
- Communicate any policy changes to HP Account Delivery Manager or HP Service Expert
- Alert HP Account Delivery Manager or HP Service Expert of new users or devices

35. Mobile Device Security Policy: Apply custom security levels to tablets and mobile devices or apply custom mobile security profiles to Windows 10 PCs.
    - Supported operating systems: All supported OS (Windows, iOS and Android).
    - Customer responsibilities: Communicate with the HP team to define the security management policy for various device groups.
    - HP responsibilities: HP Service Experts will configure or adjust security management policies as requested by the customer.
36. Windows Firewall Policy: Monitor the Microsoft Windows firewall service on Windows PCs. For third party firewalls, the HP Analytics and Proactive Management system will monitor and alert if the firewall has been disabled by an end-user.
    - Supported operating systems: Windows 7 SP1, Windows 8.1 or above.
    - Customer responsibilities: Communicate with the HP team to define the firewall management policy.
    - HP responsibilities: HP Service Experts will configure or adjust firewall management settings based on the customer's preferences.
37. Windows Virus Protection Policy: Detect whether antivirus software has been enabled on a Windows device. In addition, the system will monitor the status of third party virus protection software, and generate an incident if it has been disabled by the end-user.
    - Supported operating systems: Windows 7 SP1, Windows 8.1 or above.
    - Customer responsibilities: Communicate with the HP team to define the virus protection management policy.
    - HP responsibilities: HP Service Experts will configure or adjust virus protection policy based on the customer's preferences.
38. Automatic parts replacement: Based on the predictive alerts for hard disk & battery issues, HP will dispatch replacement parts for covered HP manufactured devices to the customer site.
    - Supported operating systems: Windows 7 SP1, Windows 8.1 or above.
    - Customer responsibilities: Collaborate with the HP team to define the replacement dispatch process, including key contacts and shipping information.
    - HP responsibilities: HP Service Experts will respond to replacement requests based on the customer's preferences.

HP Service Experts will perform the following additional tasks for Enhanced service plan customers:

- Maintain and update device and user groups:
  - Manage user groups.
  - Manage device groups.
- Monitor and respond to incidents:
  - Monitor incidents.
  - Notify the customer IT Administrator when incidents are detected.
- Order replacement parts (HP devices and Apple DaaS devices only):
  - Review hardware failure incidents and notify the customer whether the device is eligible for replacement under their DaaS plan.
  - If the customer agrees to the part replacement, open request in HP ticketing system for warranted devices.
- Act on the customer's behalf:
  - Use HP Analytics and Proactive Management to locate a missing or lost device upon customer request.
  - Use HP Analytics and Proactive Management to erase a missing or lost device upon customer request.
  - Use HP Analytics and Proactive Management to lock a missing or lost device upon customer request.
  - Monitor thermal failure incidents and advise customer how to improve thermal background, or open a replacement request ticket if needed.
  - Monitor Windows firewall state and set enforcement policy for Windows Firewall.
- Provide insights and reports
  - Monitor the device fleet status and inform the IT Administrator of non-compliant devices or other situations where additional action is required.
  - Provide reports, graphs and charts to IT Administrator upon request.
- Provide customer support
  - Monitor and respond to customer support requests (through the customer IT Administrator).
  - Assist the customer IT Administrator remotely using standard tools as needed.
  - Notify the customer IT Administrator customer of incidents or system degradation which require attention.
  - Monitor and resolve customer's account manager/representative (ADM/PDM/TTM) support requests.
  - Call customer directly as needed, or upon callback request, to resolve issues or to communicate information not supported through email (e.g. security-related and user identification).

---------- THE ENHANCED SERVICE PLAN FEATURES END HERE ----------

HP DaaS Premium Plan

HP Service Experts will perform the following additional tasks for Premium service plan customers:

39. Apple Device Enrollment Program (DEP): Over-The-Air (OTA) enrollment and enforcement of Mobile Device Management (MDM) persistency through the Apple DEP framework
    - Supported operating systems: iOS
    - Customer responsibilities:
        - Create and maintain a DEP account with Apple
        - Link the customer DEP to the HP DaaS endpoint management tool that is used in Analytics and Proactive Management and grant access to HP to manage DEP MDM settings
    - HP responsibilities:
        - Provide the HP DaaS endpoint management tool to configure and enforce DEP settings
40. Apple Push Notification service (APNS) certificate: To manage Apple devices, an APNS certificate must be installed within the HP DaaS endpoint management tool and be renewed yearly.
    - Supported operating systems: iOS.
    - Customer responsibilities: If Apple DEP feature is used, the customer should also create the APNS certificate. If the Apple DEP feature is not used within the HP DaaS endpoint management tool, the customer can choose to manage APNS certificate, including yearly renewal, or allow the HP team to manage this as part of the service.
    - HP responsibilities:
        - Provide the HP DaaS endpoint management tool to manage iOS devices. The system will notify when the APNS certificate needs to be renewed - 30, 10 and 5 days in advance. If not renewed, all iOS devices will no longer be managed. HP will manage the APNS certificate if Apple DEP is not used, or upon customer request. However, it is recommended that the customer manage the APNS certificate for their organization.
41. Wi-Fi Provisioning: Assign and configure WiFi settings to devices without providing end-users the Wifi SSID password. This enables traveling users to gain access to different office locations seamlessly, and at the same time ensure the wifi password remains confidential.
    - Supported operating systems: All supported operating systems (Windows iOS and Android).
    - Customer responsibilities: Collaborate with HP Service Experts to provide access points which end-users should have access to. Inform HP if there is a change to the password or Wi-Fi network assignments for managed device groups.
    - HP responsibilities: HP Service Experts will configure and provision Wi-Fi network settings as requested by the customer.
42. Windows Information Protection (WIP): Protect against accidental data leakage due to device loss with policy-based access controls.
    - Supported operating systems: Windows 10.
    - Customer responsibilities: Collaborate with the HP Service Experts to define the WIP management policy and verify the settings are correctly configured.
    - HP responsibilities: HP Service Experts will configure or adjust the WIP management policy as requested by the customer on specified devices.
43. End-user password “spare key”: The password recovery feature (aka “spare key”) enables an end-user to login to their machine local account if it is not locked out by answering a series of personal questions. To use the feature, the account must not be locked out. Also, Active Directory is not supported by this feature.
    - Supported operating systems: Windows 7 SP1, or Windows 8.1 or above.
    - Customer responsibilities: The customer IT Administrator must request activation of this feature for it to be enabled. Once activated, the end users configure the spare key questions and answers. When they are unable to log on, they can use the password recovery feature to login.
    - HP responsibilities: HP will activate the feature upon customer request.

44. OS & software health - Required apps not installed: An incident will be generated if a mandatory app has not been installed on a targeted device.
    - Supported operating systems: Windows, iOS and Android.
    - Customer responsibilities: Review the report and assist end-users to complete installation of the required apps.
    - HP responsibilities: HP will provide a tool to distribute software to end-users' devices. Legacy Windows PC applications (MSI and EXE and similar installer) apps will be automatically installed if they are marked as required. On other operating systems the user will be prompted to confirm installation of the deployed apps.
45. Software distribution – Deployment or publishing of customer specified or provided application to Windows or Mobile Devices.

    The software distribution service supports:

    - Public (App Store, Google Play, Windows Store) free applications for iOS, Android, and Windows 10.
    - Public paid applications via Apple VPP, and Windows Store for Business for iOS, and Windows 10.
    - Win32 applications packaged as MSI packages with silent command line options for Windows 7 and Windows 10.
    - Android and iOS line-of-business applications packaged as IPA (iOS) or APK (Android) with appropriate enterprise signatures.
    - Web-based applications.

    Application deployment service does not support:

    - AppV or other application virtualization or streaming; however, streaming client can be deployed if it is available as specified above.
    - File sharing, synchronization or related content management functions related to application data.

    Service Flow:
    - HP Service Expert or Account Delivery Manager (if applicable)) captures configuration information fromcompany IT to specify Service Options (below).
    - Customer will provide any necessary application or logo binaries in MSI packages.
    - Customer enrolls in iOS VPP if necessary (optional).
    - Customer provides VPP token and VPP options to HP Account Delivery Manager (optional).
    - Customer enables the HP DaaS endpoint management tool in Windows Store for Business (optional).
    - HP Service Expert configures app policies in HP's 3rd party Unified Endpoint Management tool as specified in configuration requirements:
        - HP Service Expert will upload application binaries for line-of-business applications.
        - HP Service Expert will specify command line options or application configuration options per requirements.
        - HP Service Expert will upload VPP token and configure VPP options if specified.
    - HP Service Expert will assign devices/user to rings based on customer requirements.
    - If no issues are found during QA, update deployment will proceed automatically to additional rings.
    - If issues are found by customer in QA ring:
        - HP Service Expert will pause deployment to remaining rings.
        - Customer will provide relevant data to HP Service Expert.
        - HP Service Expert will report issue to Microsoft and/or appropriate vendor.
    - Customer will contact HP Service Expert to make changes to update policy.

HP Responsibilities:

- Gather requirements from customer.
- Upload VPP token and enter VPP information in HP's 3rd party Unified Endpoint Management tool.
- Create user/device groups to facilitate staged deployment:
  - Deploys to QA group before deploying to mass population.
  - Holds deployment until customer indicates UAT success.
- For each requested application:
  - Create application in catalog per customer requirements.
  - Assign deployment option and group per requirements.
- Pause deployment in response to customer report of update issue.
- Resume deployment policy after issue resolution.

Customer Responsibilities:

- Provide list of applications and application details.
- Provides binaries for any non-store apps (IPA, APK, EXE, MSI):
  - IPA files must be signed with customer enterprise certificate.
  - EXE/MSI installers must include silent install, uninstall, and any additional command line options.
  - Customer is responsible for licensing software and ensuring license compliance.
- Provides any configuration data (key-value pairs) for AppConfig-compliant apps.
- If using Apple VPP,
  - Creates VPP Account (http://www.apple.com/business/vpp/).
  - Provides VPP details to HP Service Expert or Account Delivery Manager.
- If using Windows Store for Business, customer associates Microsoft Store for Business Account with the Analytics and Proactive Management tool as specified by the HP Service Expert.
- Provides QA devices and other resources.
- Performs QA on deployed applications:
  - Provides UAT pass/fail.
  - Reports deployment-related issues to HP Service Expert.
  - Provides functional/integration triage and reporting to individual ISV.
- Report issues encountered to HP Service Expert.
- Communicate any policy changes to HP Service Expert.
- Alert HP Service Expert of new users, devices, or applications.

46. App blacklist/whitelist management: HP Service Experts will implement and enforce policies to allow (whitelist) or deny (blacklist) use of applications on managed devices.
    - Supported operating systems: iOS and Android.
    - Customer responsibilities: Provide the list of applications to be allowed or blocked on managed devices.
    - HP responsibilities: The HP Service Experts will configure and provision the app whitelist/blacklist policies as requested by the customer.
47. HP Service Experts will implement and manage Microsoft OS and Microsoft Application Software Patch Deployment policies via Windows Update:
    - Supported operating systems: Windows 7 SP1, Windows 8.1 or above.
    - Customer responsibilities: Provide information to the HP team as needed to device the Windows Update settings policy.
    - HP responsibilities: Configure or adjust Windows Update management policy to device groups per customer request.

HP Service Experts will perform the following additional tasks for Premium service plan customers:

- All Enhanced service plan tasks are supported, plus:
- Device enrollment
  - Over-the-Air (OTA) enrollment and enforcement of the HP DaaS endpoint management tool for Apple devices.
- Customer Support contact options:
  - Monitor and respond to end user help requests (through the customer IT Administrator).
  - Assist the IT Administrator and end user using chat and remote control as needed.
  - Notify the customer IT Administrator of incidents or system degradation which require attention.
  - Monitor and resolve customer's account manager/representative (ADM/PDM/TTM) support requests.
  - Call customer directly as needed, or upon callback request, to resolve issues or to communicate information not supported through email (e.g. security-related and user identification).
  - Track, prioritize, and manage incidents from the HP Analytics and Proactive Management dashboard.
  - View and update device details.
  - HP Service Experts personnel will use a remote-control session to help resolve Windows PC end user device issues.
- Windows Update settings management for Windows PC devices:
  - Define the operating system update policy (monitor or enforce).
  - Define the software update policy for both Microsoft Windows OS and Microsoft application software.
- Application deployment:
  - Create and provision app packages from mobile OS app stores - Windows, Apple, and Google Play.
  - Assign and deploy legacy Windows PC apps (.MSI installer type) to managed devices.
  - Monitor incidents for required applications that do not complete the installation successfully. Some assistance may be required by the customer IT Administrator to resolve installation issues for some end user devices.
- Wi-Fi provisioning:
  - Configure Wi-Fi settings and enable devices to auto-connect to a network without disclosing the SSID password to the end user.
- Mobile device management (MDM):
  - Apply custom security polices to managed devices.

---------- THE PREMIUM SERVICE PLAN FEATURES END HERE ----------

Feature and managed service by OS type

Feature	Description	Windows 10	Windows 7	iOS	Android	Mac OS X
Bring Your Own Device (BYOD) Policy	Limit management capabilities for employee owned devices.	✓	✓	✓	✓	✓
Bulk Device Enrollment	Enable large-scale enrollment of devices and users. Automated processes enable devices to be associated with the end user's account.	✓	✓	✓[1]	✓	
Lock Device	HP Service Experts can perform a screen lock (PIN reset) on a managed device if it is reported lost or stolen.			✓	✓	
Find Device[2]	HP Service Experts can help pinpoint the location of a missing device on an online map.	✓		✓	✓	
Wipe Device Data [2]	HP Service Experts can remove data from a managed mobile device, notebook, or desktop PC.	✓		✓	✓	
Firewall Policy	Monitor the Microsoft Windows firewall service on Windows PCs.	✓	✓			
Groups	HP Service Experts can quickly apply policies to groups of users and/or devices.	✓	✓	✓	✓	
Hard Disk Health	Monitor hard drives on notebooks and desktops. Get notified if a disk drive needs replacement or if the disk has been replaced or removed.	✓	✓			
Microsoft Patch Management	HP Service Experts can configure Windows Update settings on PC devices.	✓	✓			
Mobile Application Deployment	HP Service Experts can create, distribute, and manage curated bundles of mobile applications from the Windows App Store, Apple App Store and Google Play store to users.	✓		✓	✓	✓

[1] Requires Apple DEP account.
[2] Remote find, lock, and erase functionality requires the device to be powered on and have Internet access

Feature	Description	Windows 10	Windows 7	iOS	Android	Mac OS X
Microsoft Windows® Application Deployment	HP Service Experts can create, distribute, and manage curated bundles desktop applications to managed Windows devices. Get notified if a required app is not installed on a device.	✓				
Mobile Device Security Policy	HP Service Experts can apply custom security levels to managed devices.	✓	✓	✓	✓	✓
Password Recovery	End users can reset a forgotten machine local user account password on Windows notebooks PCs and tablets.	✓	✓			
Device Encryption	HP Service Experts can enforce encryption policy on managed devices.	✓	✓	[3]	✓	✓
App Whitelisting and Blacklisting	HP Service Experts can control which apps can run on the device.			✓	✓	
Remote Assistance	HP Service Experts can troubleshoot device issues using remote control technology.	✓	✓			
Smart Battery Health Monitor	Monitor battery charge capacity and wear. 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 Alerts	Get notified when an HP system needs maintenance due to a heat related issue.	✓	✓			
User and Device Inventory	View 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.	✓	✓	✓	✓	

[3] Apple iOS enforces encryption automatically.

Feature	Description	Windows 10	Windows 7	iOS	Android	Mac OS X
Virus Protection Policy	Detect whether antivirus software is enabled on a Windows device.	✓				
Warranty Tracking	View the warranty expiration dates for HP devices to proactively plan your hardware refresh cycles.	✓	✓			
Wi-Fi Provisioning	HP Service Experts can 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 Windows 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.	✓	✓			
Azure Active Directory Federation	Log on to the HP DaaS portal using Azure AD login credentials.	✓	✓	✓	✓	✓
Non-reporting Device Monitoring	Get alerted if a managed device has not communicated with the management server for more than 7 days.	✓	✓	✓	✓	

Feature	Description	Windows 10	Windows 7	iOS	Android	Mac OS X
Device Incidents	HP Service Experts monitor and receive notifications when actionable device incidents are detected.	✓	✓	✓	✓	
Dashboards and Reports	HP Service Experts and customer IT can view and extract fleet level intelligence with advanced dashboards and reports.	✓	✓	✓	✓	
Apple DEP	Over-The-Air (OTA) device enrollment and persistent enforcement of mobile device policies using Apple's Device Enrollment Program (DEP).			✓		✓

Reports by DaaS Plan and Platform

Customers can log on to view reports on the HP DaaS portal at hpdaas.com.

Features	Standard Plan Self-Service	Enhanced Plan HP Managed	Premium Plan HP Managed	Windows	Android	iOS
Blue Screen Errors [4]	✓	✓	✓	✓		
Device Utilization [4]	✓	✓	✓	✓		
Hardware Health Grade [4 5]	✓	✓	✓	✓	✓	✓
Hardware Health [5]	✓	✓	✓	✓	✓	✓
Hardware Inventory	✓	✓	✓	✓	✓	✓
Hardware Warranty [6]	✓	✓	✓	✓		
Non-Reporting Devices	✓	✓	✓	✓	✓	✓
Software Inventory	✓	✓	✓	✓	✓	✓
Battery Replacement [4 6]		✓	✓	✓		
Disk Replacement [4]		✓	✓	✓		
Thermal Grading [4]		✓	✓	✓		
Lost Device Protection		✓	✓	✓	✓	✓
Software Errors [4]			✓	✓		
Security Compliance			✓	✓	✓	✓

Note: Services are delivered by HP Service Experts in the Enhanced and Premium Plans

[4] Supports Windows PCs running Windows 7 Service Pack 1 or higher only
[5] Only hard disk space monitoring available for Android and iOS devices
[6] Supports HP devices only

Incidents Tracked by DaaS Plan and Platform

HP DaaS Analytics and Proactive Management includes a monitoring function. When problems or other conditions are detected which may require intervention, an incident is generated to trigger action by the HP Service Expert team. The Service Expert team will act to either remediate the issue, or notify the customer if action is required from them to move the issue to resolution.

Incident name	Standard	Enhanced	Premium	Windows 10	Windows 7	iOS	Android	Mac OSX
HP technology entitlement expiration		✓	✓	✓	✓	✓	✓	✓
Battery grade		✓	✓	✓	✓			
Battery missing		✓	✓	✓	✓			
Battery replacement [6]		✓	✓	✓	✓			
Blue screen errors		✓	✓	✓	✓			
Unexpected OS crashes		✓	✓	✓	✓			
Disk component changes		✓	✓	✓	✓			
Disk grade		✓	✓	✓	✓			
Disk smart event failure		✓	✓	✓	✓			
Disk storage full		✓	✓	✓	✓		✓	
Disk replacement		✓	✓	✓	✓			
High CPU utilization		✓	✓	✓	✓			
High memory utilization		✓	✓	✓	✓			
Thermal grading		✓	✓	✓	✓			
Memory changes		✓	✓	✓	✓			
Non-reporting devices		✓	✓	✓	✓	✓	✓	
Security Antivirus disabled		✓	✓	✓	✓			
Security – Firewall disabled		✓	✓	✓	✓			

HP DaaS plans and/or included components may vary by region or by Authorized HP DaaS Service Partner. Please contact your local HP Representative or Authorized DaaS Partner for specific details in your location.

HP services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product.

[6] Supports HP devices only