Approved for External Audiences

HP Device as a Service (DaaS)

HP Confidential and Proprietary Information. May be shared with HP partners and customers in part or in total, subject to NDA in place between the parties. HP disclaims any and all liability in connection with the information contained herein. To be used for informational purposes only.

Proactive Management with HP TechPulse for Microsoft Intune

Service Definition

September 2018

Contents

1. Service Overview

1.1 HP DaaS Overview

HP Device as a Service (DaaS) is a modern service model that simplifies how organizations equip their employees with the right hardware, support, and lifecycle services. Our goal is to improve end user productivity and security while providing customers and IT with performance, agility, and cost predictability.

As part of HP DaaS, Proactive Management with HP TechPulse provides multi-OS device management services, comprehensive insights, and reports for devices. HP offers three plans: Standard, Enhanced, and Premium. Standard is designed for customers who want to manage and secure their own endpoints but want to leverage the unique insights and reports from HP TechPulse to do this more effectively and with greater visibility to issues that are impacting end-user productivity. Enhanced and Premium packages include multi-OS device management and security policy enforcement by specialized, HP Service Experts. HP Service Experts are trained and certified in unified, multi-OS endpoint management technology and will assist IT in delivering proactive security, support, and device management. Please note that 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.

HP TechPulse is the HP analytics and machine learning platform that provides rich insights at OS level while also providing detailed insights and recommendations at the individual device/user level. HP TechPulse uses machine learning, preconfigured logic, and contextual data to deliver device, application, and usage insights which help customers optimize IT spending, resources and perhaps most importantly, end user productivity and security. Customers can view dashboards of their environment and reports for all enrolled devices, including non-HP devices1. The HP DaaS Proactive Management and TechPulse platform is cloud-based and offers flexibility and scalability for customers who have mobile users and multiple device and OS types at multiple locations. HP TechPulse analytics and reporting gives customers that "single pane of glass," holistic view of their multi-OS devices through an intuitive dashboard.

HP DaaS Plans at a glance

	Standard Plan Self-Managed	Enhanced Plan HP Managed	Premium Plan HP Managed
Devices	• HP desktops, notebooks, and workstations • HP Retail Systems: HP Engage, HP RP9, MP9, ElitePOS[2]	√	√
Hardware Support	• Next business day repair/replace response	Standard plan plus: • Accidental Damage Protection[3] • Defective Media Retention	√
Customer Success Management	N/A	Account Delivery Manager for onboarding and regular service check-ins[4]	√
Proactive Management with HP TechPulse	HP TechPulse:	All in the Standard Plan plus:	All in the Enhanced Plan plus:

[1] Managed device types include Windows devices from HP and other manufactures, Android, and Apple iOS and macOS devices. iOS devices are not covered in the Standard plan. See complete system requirements at https://www.hpdaas.com/requirements

[2] Available through HP DaaS via custom agreements in the United States only.

[3] Accidental Damage Protection is available in selected countries. Please check with your HP Representative.

[4] Additional service/purchase required.

	Standard Plan Self-Managed	Enhanced Plan HP Managed	Premium Plan HP Managed
	• Windows, Android, and MacOS analytics • Hardware, software, BIOS inventory • Device and component health • CPU, hard disk and software utilization • Predictive reports • Hardware and OS health incidents • Mobility factor report • Device replacement guide	• Security analytics from HP TechPulse • iOS analytics Performed by HP Service Experts: • Security policies and enforcement • Windows OS patch management • Data protection on missing devices • Automatic parts replacement on HP devices • Security incidents and reports • Remote assistance	• Advanced software analytics from HP TechPulse HP Service Experts perform: • Application deployment • Mobile app whitelisting and blacklisting • Windows Information Protection policies • Local account password recovery on Windows devices • Wi-Fi provisioning
Lifecycle Services	Services, for all phases of the asset lifecycle, delivered by HP or our partners with a one-stop quote and agreement		
Financial Services	• Device as a Service (DaaS) plans include options from HP Financial Services with 12, 24, 36, 48, or 60-month terms.[5] • Fleet Flexibility options[6] include the ability to flex the number of devices up or down with 36 or 48-month terms		

1.2 HP Proactive Management for Microsoft Intune service option

HP DaaS leverages industry leading, cloud-based UEM/EMM solutions to effectively and securely manage multi-OS device environments at scale. Using EMM, HP deploys policies recommended by industry security experts and designed for companies who want to modernize their workplace using cloud-based technology.

HP supports leading UEM/EMM providers and will utilize the best EMM technology partner most suitable for the customer's environment and goals. HP can either include and price VMWare Workspace One licenses as a part of our DaaS Enhanced and Premium plans or leverage a customer's Intune licenses if available as a part of their Windows 10 licensing agreement.

The customer license and infrastructure prerequisites for the Microsoft Intune option are described in next section.

[5] 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.

[6] The DaaS Fleet Flexibility offer allowing customers to flex up at 5 – 10% or flex down at 5, 10, and 15% increments is available by HP DaaS deals supported by HPEFS. Additional requirements may apply. See your HP representative for more information.

2. Prerequisites

HP Proactive Management service has some dependencies on systems, network, and some important customer information.

2.1 System requirements

To enable HP Proactive Management service on your covered devices, systems need to meet following requirements:

Category	Requirements
HP DaaS Proactive Management Enhanced and Premium Plan for Microsoft Intune[7]	• Windows 10 • Android v4.4 and up • iOS 10.0 and up • MacOS 10.12 and up
Browser requirements for HP DaaS portal	Windows PC web browsers • Google Chrome for Windows: Version 68.0 or higher • Internet Explorer for Windows: Version 11 or higher (Windows 7 SP1 or 8.1 only) • Firefox for Windows: Version 61.0 or higher • Microsoft Edge for Windows: 40.0 or higher Mobile OS browsers • Chrome on Android: 68 or higher • Safari on iOS 10 or higher • Safari on MacOS 10.12 or higher
Supported HP Retail Point of Sale (RPOS) systems	Retail Point of Sale Devices[8] [9] • HP RP9 G1 Model 9015, 9018, 9115, 9118 • HP MP9 G4 • HP RP5 Model 5810 • HP Engage One (includes former ElitePOS Model 141,143,145) • HP Engage Flex Pro • HP Engage Flex Pro-C • HP Engage Go

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

2.2 Network requirements

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

[7] To manage Apple devices, an APNS certificate must be installed within the Microsoft Intune and be renewed yearly.
[8] Systems running Windows 10 Professional and Windows 10 IoT only
[9] Supported for HP DaaS Proactive Management analytics only. Not supported by Intune MDM.

2.3 Prerequisites within Customer IT Environment

Deployment of HP Proactive Management services using the customer's existing Intune license require the following prerequisites:

License Requirements

The customer must have one of following subscriptions or license from Microsoft:

- Microsoft365 (M365) E3
- Microsoft365 (M365) E5
- Enterprise Mobility + Security (EM+S) E3
- Enterprise Mobility + Security (EM+S) E5
- Azure Active Directory Premium (P1 or P2) and Intune full version

Note: If you plan on using Windows 10 Enterprise Edition, you will require specifically the M365 E3/E5 SKU for appropriate Windows Enterprise licensing
If you are not sure if your license work for this solution, please check with your HP sales representative.

Prerequisites on other technical implementations

The following technical components are required to be in place prior to the onboarding of HP Proactive Management. Alternatively, HP Professional Services can be contracted on a project-based capacity for prerequisite tasks outlined here:

- Customer Active Directory Remediation using IDFix (i.e. the on-premise Active Directory objects must be synchronized with Azure Active Directory)
- Azure AD Connect Server and Database design, install & configuration
- (Optional) ADFS Federation Server design, install and configuration including WAP (Proxy)
- Customer Domain suffix registered with Azure AD for tenant Auto-Discovery (required for Sign-on) *https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/domains-manage
- CNAME Registration in customer DNS for Windows 10 enrollment https://docs.microsoft.com/en-us/intune/windows-enroll#simplify-windows-enrollment-without-azure-ad-premium
- Configure Windows 10 Auto-enrollment in Azure AD Premium https://docs.microsoft.com/en-us/intune/windows-enroll#simplify-windows-enrollment-without-azure-ad-premium
- Determine the source of truth for User Assignment Groups; Active Directory or Azure Active Directory
- Apple Push Notification Certificate (APNS) if enrolling Apple devices.

Additional system requirements for Microsoft Intune can be found on the Microsoft web site at this location: https://docs.microsoft.com/en-us/intune/supported-devices-browsers,[10]

2.4 Prerequisites for Onboarding

Onboarding is the process of transitioning all customer devices covered under the DaaS plan into HP Proactive Management using the HP TechPulse solution. The following information and activities are required to proceed with the onboarding project. The responsibility to provide the required information to the Onboarding Program Manager falls to the customer, the HP Account Manager, and/or the reseller/partner:

- Customer primary contact (name, email, phone, and location information). NOTE: This should be the IT contact for the customer or partner who will be working with HP to deploy the software agent to the devices.
- Customer company address
- Customer User Principal Name (UPN) (Example:bob.smith@mycompanyname123.com)

[10] Note: HP does not support management of Windows 7 or 8.1 devices as part of its HP DaaS managed service for Microsoft Intune.

- (Enhanced and Premium Plan) Customer device list to be managed by HP Proactive Management. Device model and serial number are needed when we enroll the devices into Workspace ONE. A template will be provided during the onboarding process.
- Active Directory DNS domain name (for example: hp.com)
- Customer list of report admins
- Implemented firewall and proxy settings
- Install and run the Proactive Management network assessment tool.

More details can be found in Customer Onboarding.

3. Roles and Responsibilities

3.1 Primary Service roles and personas

Depending on the HP DaaS Proactive Management plan and options purchased, different personas may come into play. The task responsibilities for the respective plans are outlined in more detail under each plan's description.

Onboarding Program Manager	HP Service Expert	Customer IT Device Administrator
The Onboarding Program Manager assumes some, or all, of the following responsibilities, depending on the needs of each account: • Gather and consolidate the required customer environment information, and the specific needs of the customer to accurately enroll the HP DaaS devices. • Develop and implement the onboarding project plan. • Communicate progress to the customer, HP, and partner (if applicable) throughout the onboarding process. • Complete the onboarding process promptly. • Reduce deployment time while mitigating transition risks. • Verify a successful implementation. • Transition customer support for the HP DaaS Proactive Management capability to Service Experts.	The HP Service Expert's primary responsibilities include: • Create the HP DaaS Proactive Management account. • Add or remove HP DaaS Proactive Management console users. • Deploy Intune device policies and customer applications per customer request. • Remove requested apps from the customer's Device App Catalog. • Monitor device incidents in Proactive Management portal and notify customer when a device health issue is detected. Also, provide optimization and diagnostic tools to resolve health issues • Provide requested reports. • Troubleshoot installation and connectivity issues. • Coordinate Windows update deployments and changes to Windows update installation policy in coordination with the customer. • Assist customer and provide answers to service related questions. • Help ensure compliance with HP DaaS Proactive Management subscription requirements. • Attempt to remotely locate or erase data from a missing or stolen device[11]	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 Proactive Management software onto their DaaS managed devices. • Request to add or remove managed users and devices. • Request application deployment or removal • Test updates throughout the Windows 10 update life cycle, including application user acceptance with the updates. Also, communicate change requests with HP Service Expert team to enable them to adjust the updates rollout and associated ring settings. • Review hardware, software, and other reports and respond 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 a failure. • Request device lock 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:** Personnel authorized to access the Proactive Management console include a partner if the customer pre-approves a specific individual within the partner organization to have access to the customer's Proactive Management account.

[11] iOS devices only, running in Supervisor Mode

3.2 Other HP DaaS Proactive Management personas

HP Account Delivery Manager(ADM)[12]	Partner
HP Account Delivery Managers (ADM) may be included in some plans or can be added to an existing HP DaaS Proactive Management contract for an additional charge. Customers who purchase HP DaaS Proactive Management through their preferred partner will sometimes designate their partner to have access to the HP DaaS Proactive Management portal and to also serve as the primary point of contact for incident notifications in coordination with HP Service Experts. 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. The ADMs primary responsibilities can include: • Account transition and setup • Business reviews • Account planning • Business Collaboration • Contract administration • Services and third-party management • Socialize new Service features with the customer • Internal HP deliverables • Customer-specific requests	The customer's reseller or IT services partner, at the customer's discretion, may take on some or all the customer's responsibilities within the Proactive Management plan. In addition to that option, partners (if applicable) can be responsible for the following tasks: • Ensure the HP 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 Proactive Management reports. • If applicable, perform customer point of contact or other duties, if so designated by the end customer. • Assist customer with device enrollment or troubleshooting as needed. • Socialize new Service features with the customer

3.3 Enhanced Plan for Microsoft Intune – Roles and responsibilities

HP Service Expert	Customer IT Device Administrator
The HP Service Expert's primary responsibilities include: • Create the HP DaaS Proactive Management account • Grant user account access to enable the customer's IT device management team to access the HP DaaS Proactive Management analytics portal • Create or remove users based on customer request from HP DaaS Proactive Management. • Provide documentation and guidance to deploy the analytics agent for supported platforms • Provide the device PIN information used to support mass enrollment of devices • Help ensure compliance with HP DaaS Proactive Management application licensing requirements • Deploy the HP DaaS Proactive Management software agent to Intune-managed Windows 10 and Android devices	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 • Link Intune to HP Proactive Management account following instructions provide by HP • Create an Intune Service Admin account for HP to manage the devices for customer • Install the Proactive Management software onto their DaaS-managed devices to enroll them in the reporting and analytics service • Ensure compliance with the total device count covered under the HP DaaS Proactive Management plan • Request creation ore removal of Report Administrator accounts in the reporting portal as needed • Troubleshoot and resolve end-user support issues • Log on to the HP DaaS Proactive Management console to view dashboards, reports, and incidents • Review and respond to reported device health incidents • Manage changes, renewals, or cancellation of the HP DaaS account subscription • Maintain responsibility for activation and termination of Subscribers for the Microsoft Services via Active Directory or Azure AD group membership

[12] Some countries may include a similar role called Customer Success Manager (CSM).

HP Service Expert	Customer IT Device Administrator
• Provide service monitoring and coordinate escalated troubleshooting and assistance with Microsoft • Configure scheduled reports which list other devices which may require remediation • Provide and coordinate HP Service Expert L2 and L3 support with Customer's service desk • Configure device policies per customer request. HP will configure default policies for managed devices. Alternately, HP can, upon customer request, create and deploy custom policies • Configure device encryption policies on managed devices (iOS, Android) • Set BitLocker encryption policies for managed Windows devices • Investigate Incidents detected by the HP Proactive Management system, notify customers of any new incidents which require action on their behalf, or undertake corrective action and report to Customer, as appropriate • Support Intune Tenant management, provided Customer has designated HP as Partner of Record • Provide customer with notification of service upgrades which will impact the use of the Proactive Management service	• Promote the Services within the organization and provide User training regarding the Services • Maintain a current maintenance and support agreement with Microsoft for related Microsoft-licensed products • When a problem is identified to associate with Microsoft product, file a case at Microsoft through customer's support channel and keep HP updated on the progress • Provide service desk support for Azure Active Directory sync services • Provide QA devices and other resources needed to validate the deployment • Provide service desk support for Active Directory Federation Services (If in scope) • Provide service desk support the ability to interact with HP Service Expert Level 2 and 3 support team as necessary • Manage and update the customer's certificate infrastructure, and update certificates owned by the customer which are pending expiration. Also, provide certificates to HP or into the Intune console as needed for specific service configuration • Maintain financial responsibility for all licensing associated with hardware and software required for HP to provide the Services • Perform upgrades of service-dependent components (ADFS, etc.) located at the customer premises/site • Notify HP of planned and unplanned system changes which impact the managed device infrastructure. • Configure application access capabilities (single sign-on options (SSO), provisioning) in relevant third-party Applications • Installation and configuration of on-premise (within client datacenter) components used to provide connectivity between client datacenter and the cloud-based management environment • Ensure managed client devices are enrolled in Intune • Alert HP Account Delivery Manager or HP Service Expert of new users or devices to which the Proactive Management client needs to be deployed

3.4 Premium Plan for Microsoft Intune – Roles and responsibilities

HP Service Expert	Customer IT Device Administrator
In addition to the responsibilities covered in the Enhanced Plan, the HP Service Expert is responsible for the following tasks: • Deploy applications to groups of users and devices as per customer request. - Configure QA deployment ring for app deployment tests. - Capture information needed to manage application deployment in Intune. - Collaborate with customer to define an appropriate application deployment schedule in accordance with the customer's change control policies and other business requirements. - Perform test of application deployment to QA devices prior to production rollout. - Select and assign any app store apps (Google Play, Store for Business, Apple app store) as specified in customer requirements. - Upload and assign non-store MSI application installer binaries for Windows 10 line-of-business applications. - Specify command line options or application configuration options per customer direction. - Assign applications to devices/users to QA deployment ring based on customer requirements. - If no issues are found during QA, update deployment will proceed automatically to additional rings. • Apply application whitelist or blacklist policies to control usage on corporate-owned devices. • Configure Information Protection policies for Windows devices to restrict company data access to unsanctioned applications.	In addition to the responsibilities covered in the Enhanced Plan, the customer is responsible for the following tasks: • Maintain responsibility for the lifecycle management of all Application certificates and Application licenses required for deployment of mobile software Applications pursuant to the Application Publishing option specified below. • Provides any configuration data (key-value pairs) for AppConfig-compliant apps. • Create and maintain a Microsoft Store for Business account as needed for deployment of Windows applications. • If using Apple VPP, create the VPP Account and provide details to HP as needed to support Service. (https://www.apple.com/business/vpp/). – Provide installer binaries for any non-store apps (IPA, APK, EXE, MSI): o IPA files must be signed with customer enterprise certificate. o EXE/MSI installers must include silent install, uninstall, and any additional command line option instructions. - Acquire and maintain software licenses for deployment to users/devices and ensure ongoing license compliance. - Specify applications to be deployed, as well as their device and/or user assignments. - Review applications after deployment to QA devices to confirm deployment settings are correct prior to production rollout. • Notify HP of any specific application whitelist or blacklist entries which are needed for a specific user/device. • Notify HP of application and/or data rules needed to configure Information Protection policies.

4. Customer Onboarding

Onboarding is the process of bringing all customer devices covered under an HP DaaS plan into the Proactive Management with HP TechPulse solution. This is critical for HP to deliver the service successfully. HP TechPulse can monitor and track the devices, collect data, and generate reports and actionable insights, once the customer has been successfully onboarded, and all DaaS devices have been enrolled. This data collection is required for HP Service Experts to manage the customer devices in both the Enhanced and the Premium DaaS plans.

4.1. Onboarding Program Management

If the customer selects an HP DaaS Enhanced or Premium plan, an HP Onboarding Program Manager will be assigned to manage the onboarding process for the account. Once the service is registered, the Onboarding Program Manager will manage the onboarding project from kick off to completion and is responsible for the successful onboarding of the account. Please refer to the Roles and Responsibilities section for more details about the scope of the Onboarding Program Manager role.

4.2. Onboarding process overview

The onboarding process can be broken down into five phases and are explained in the following sections:

- Phase 1 - Registration
- Phase 2 - Information gathering
- Phase 3 - HP Recommendations and Account Creation
- Phase 4 – Deployment
- Phase 5 – Transition to Ongoing Management

4.3. Phase 1 - Registration

Registration of HP DaaS Proactive Management is a requirement. Once the service is properly registered HP can create the account and onboard the customer. The HP DaaS support team needs the basic information and the proper authorization to begin onboarding customer devices into HP DaaS. Currently, HP DaaS Proactive Management for Intune is offered through a contractual model only, and an Account Delivery Manager (ADM) is usually included as part of the contract. Under that model the Account Delivery Manager will coordinate with the customer, or partner if applicable, to have the service registered. If there is no Account Delivery Manager included in the contract, either the HP Account Manager or Sales Representative, or the partner will serve as the Account Delivery Manager.

4.4. Phase 2 - Information Gathering

Once the service is registered in phase 1, an HP Onboarding Program Manager will be assigned. For Premium and Enhanced plans, HP recommends inclusion of an HP Account Delivery Manager (ADM) to manage the service quality. The HP Onboarding Program Manager will work with the ADM to schedule customer conference calls to review the service offer. If an ADM is not included in the service plan, the HP Onboarding Program Manager will work with the account manager (if it is sold as HP Direct), or partners (if it is sold through channel), on this phase. This phase consists of the following steps:

- Review the customer onboarding experience and set expectations.
- Exchange contact information.
- Discuss and document the customer's network environment.
- Discuss how the customer uses devices and what they are trying to accomplish.
- Develop a customer configuration and deployment plan, schedule and requested start date.
- Review the automated parts replacement process.
- Review Apple Device Enrollment Program (DEP) for existing install base if applicable.
- Validate customer pre-requisites outlined in Section 2: Prerequisites.
- Verify group assignment for application licenses and device policies which the customer wants HP to enforce.
- Ensure appropriate permissions are delegated for HP Proactive Management Tenant linking required for Intune Service administration.

4.5. Phase 3 - HP recommendations and account creation

HP will analyze the data and work on the recommendations once all the required information has been gathered.

Within two weeks of the information gathering call, the HP Onboarding Program Manager will schedule a conference call with the customer (and partner if needed) to provide recommendations on how to proceed based on specific customer use cases, and the customer environment. HP will recommend the configurations most suited to the customer's needs. This is an iterative process.

- Once the customer and HP agree on the solution, HP will create the customer account in the HP DaaS platform.
- HP will add the partner (if applicable) as a report admin if authorized by customer.
- Then, HP will schedule a call to initiate the device enrollment steps based on the agreed upon deployment schedule.
- The HP Service Expert emails the Customer with the following information, copying the partner if applicable.
  - Account information
  - Enterprise Mobile Management software integration instruction
  - Device enrollment instructions
  - Report Admin details
  - Support contact information
- After receiving the welcome email, customer need to confirm the access to HP Proactive Management Portal and accept the T&Cs.
- Customer IT Admin needs to link Intune and HP Proactive Management tenant following instruction from HP included in the welcome email
- Customer needs to create an account with the Intune Service Admin role for HP so that HP can manage the devices for customer during the service contract.
- Customer needs to notify HP when the above is done, so we can move to next phase.

4.6. Phase 4 – Deployment

- Deployment Kick Off Call: HP Onboarding Program Manager will meet with the customer and partner (if applicable) to start device enrollment, and to help resolve any issues.
  - HP will validate that customer has access to the HP DaaS platform dashboard
  - HP will notify the customer on how to get help within the HP DaaS platform.
  - HP will show the customer how to navigate the site and pull reports.
- HP will validate the link between HP Proactive Management tenant and Intune is functional.
- HP will apply the customer configuration settings based on the agreed-to policy spreadsheet
- HP will assign HP Proactive Management client user groups in Intune for deployment
- HP will conduct stage testing with limited devices and inform the customer when complete.
- Customer will perform a User Acceptance Test (UAT) and confirm the configuration delivered by HP meets the customer's expectations
- The customer and/or partner (if applicable) move to broad deployment of device enrollments.

4.7. Phase 5 – Transition to Ongoing Support and Management

During this phase, the HP Onboarding Program Manager and customer will agree on the deployment plan for the remaining devices. The Onboarding Program Manager will also:

- Generate initial reports and explain the usefulness of each.
- Demonstrate the HP TechPulse portal's functionality.
- Outline how HP Proactive Management related service requests or incidents should be submitted.

Next, the HP Onboarding Program Manager will obtain customer sign off on the acceptance document and verify customer satisfaction with the services, as delivered at that point in time. This is a required step in the onboarding process signifying that the account can be transitioned to the next phase of Ongoing Support and Management.

Accounts are chosen at random to participate in our service quality survey. The survey is optional; but customer participation would be greatly appreciated. HP values your feedback and uses that information to improve the onboarding process. Ongoing Support and Management.

5. Ongoing Support and Management

Once the onboarding project is signed off by the customer, the service moves to the Ongoing Support and Management phase for Enhanced and Premium plans. HP Service Experts will monitor and manage devices for the customer throughout the contract term.

HP's service delivery methodology capitalizes on the wide knowledge base that HP has built over the years, as well as best practices from Information Technology Infrastructure Library (ITIL®) 2011 framework. The Service Experts are geographically dispersed to provide a world-class customer experience.

The team provides the following services on an ongoing basis:

5.1 Operation Optimization

Leveraging HP's unique TechPulse technology, HP Service Experts monitor all devices and help customers optimize their operations.

- HP Service Experts monitor incidents and alerts and help identify issues and provide recommendations. When needed, HP Service Experts can provide remote diagnosis with LogMeIn or other tools.
- HP Service Experts review hardware failure incidents and notify the customer whether the device is eligible for replacement under their DaaS plan.
- HP TechPulse can predict failures on some key component such as hard drive and battery. HP Service Experts will work with customer to have those components replaced before the failure occurs to minimize the impact to customer's productivity.

Other services include improving report accuracy, analyzing Service Level Target (SLT) performance, adjusting thresholds (e.g. turning off incidents on firewall if it is not used in the company) within HP TechPulse based on the customer environment.

5.2 Customer Support

For any problems related to HP Proactive Management, such as report accuracy or login issues, an HP Service Expert will be available to the customer for the service contract term. HP Service Experts will work with HP Internal L2 and L3 teams to resolve the issues when needed. If a 3rd party vendor product outside of HP DaaS is identified as the cause impacting HP Proactive Management services, HP Service Experts will assist the customer in opening a case through their customer support channel by providing logs or other diagnostics.

5.3 Fulfill Customer's Service Request

Other Service requests can be requested by customers via email to the Service Experts team. Depending on the DaaS plan selected, frequent service requests include:

- Add or remove devices
- Add/remove/change access
- Device encryption
- Lock or wipe data on missing devices
- Mobile application deployment
- Mobile app whitelisting and blacklisting
- Mobile device security policy
- Windows machine local password recovery
- Microsoft update and patch management
- Create smart groups
- Wi-Fi provisioning

6. Terms of Service

The terms of service are contained in several documents. All documents should be reviewed to confirm understanding of the HP DaaS Proactive Management's terms governing product use rights, data security and privacy, and confidentiality (non-disclosure).

Document	
HP DaaS Terms and Conditions	• 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
End User License Agreement	• Governs the use of the software agent we store on devices
• Service Level Agreement	• Governs service uptime and availability • Describes service credit amounts • Describes claim eligibility and process
HP DaaS Data Security white paper	• Describes data handling and security controls for HP DaaS Proactive Management analytics data.

7. HP Proactive Management Data Centers

The HP DaaS Proactive Management platform is hosted on Amazon Web Services (AWS).

The HP DaaS Proactive Management platform maintains data centers in Oregon, United States (AWS-OR) and Frankfurt, Germany (AWS-DE). Data for customers located in EU countries can be hosted in the German data center while data for customers in all other countries can be hosted in the U.S. data center. 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. Having the two data centers allows the HP DaaS Proactive Management service to leverage cloud servers in the respective region.

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

Identity management for HP DaaS Proactive Management services is performed in two geographically dispersed locations on Amazon Web Services within United States. HP DaaS Proactive Management uses a unified identity management ecosystem for all HP customers across all HP applications. This unified identity management primarily stores all the core data needed for an identity to authenticate (e.g. first name, last name, email address, country of residence, mailing address, phone number, password, locale, and credential recovery methods, if needed). The exact location of these data centers cannot be disclosed due to security reasons.

For more information on HP DaaS Proactive Management's data collection, transmission, storage, retention and disposal of data, please contact HP for the HP DaaS 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 website.

8. Service Level Objectives

If the customer purchases an Enhanced or Premium plan, HP Service Experts will manage the DaaS devices for the customer. The tables below provide Service Expert availability by country or region. Note that the HP DaaS Standard plan is a self-managed model, and the customer will manage all devices by utilizing HP TechPulse.

Americas Region

Country	United States	Argentina Chile Colombia Mexico Peru Puerto Rico	Brazil	Rest of AMS
Coverage (Hours/ Days per week, excluding holidays)	12 / 5	11 /5		12 / 5
Operating Hours	6AM-6PM MST	7AM – 6PM (GMT-5)		6AM-6PM MST
	Mon-Fri	Mon-Fri		Mon-Fri
Language Supported	English	Spanish, English	English	English
Support routes	Email, outbound chat[13]			
Support Email address	HPDaaS_AMS@hp.com	HPDaaS_LA@hp.com	HPDaaS_LA@hp.com	HPDaaS_AMS@hp.com

EMEA Region

Country	United Kingdom Ireland	France	Germany Austria Switzerland Luxembourg	Rest of EMEA
Coverage (Hours/ Days per week, excluding holidays)	10 / 5			
Operating Hours	8 AM - 6PM CET			
	Mon-Fri			
Language Supported	English	French, English	German, English	English
Support routes	Email, outbound chat[14]			
Support Email address	HPDaaS_EMEA@hp.com			

[13] Primary Service and Support are available via email. Outbound chat and call back is available as needed.

[14] Primary Service and Support are available via email. Outbound chat and call back is available as needed

APJ Region

Country	China	Japan	India	Australia New Zealand Malaysia Philippines Singapore	Rest of APJ
Coverage (Hours/ Days per week, excluding holidays)	24 / 7	12 / 7	24 / 7	24 / 7	24 / 7
Operating Hours	24/7	9AM-9PM Japan Standard Time	24/7		
Language Supported	Chinese, English	Japanese, English	English	English	English
Support routes	Email, outbound chat[15]				
Support Email address	HPDaaaS_CHINA@hp.com	HPDaaaS_JAPAN@hp.com	HPDaaaS_INDIA@hp.com	HPDaaaS_APJ@hp.com	HPDaaaS_APJ@hp.com

When HP is contacted, depending on the nature of the request, below is the service level objective:

Event type	Initial Response	Service Level Objective[16]
On-boarding kick-off	HP onboarding team first contact with customer	Within two weeks
Email from customer to HP DaaS Support mail node.	Acknowledgement of email receipt	2 business hours local time
Proactive Incidents - Critical	Periodic report sent over email	Default Frequency: every business day
Proactive Incidents - Medium	Periodic report sent over email	Default Frequency: Weekly
Proactive Incidents - Low	Periodic reports sent over email	Default Frequency: Monthly

[15] Primary Service and Support are available via email. Outbound chat and call back is available as needed

[16] These Service Level Objectives only cover HP Inc. lead time to engage with the customer and notify the customer of DaaS devices' conditions. Issues resolution is not covered by the above Service Level Agreement.

The chart below shows the Service Level Objectives (SLO) when contacting HP for support. These objectives are based upon the nature of the event:

Category	Type of incidents	Priority
Account	License Expiration	Critical
Hardware Health	Battery not detected	Critical
Hardware Health	Battery Predictive Failure	Critical
Hardware Health	HDD Predictive Failure	Critical
Hardware Health	HDD SMART Event Failure	Critical
Hardware Health	System Error – Thermal	Critical
Hardware Health	HDD Storage Capacity Full	Medium
OS Health	CPU High Utilization	Medium
OS Health	Memory High Utilization	Medium
Security	Antivirus	Medium
Security	Firewall	Medium
Security	Heartbeat failure	Medium
OS Health	BSOD	Low
OS Health	Unexpected Crash/Reboot	Low
Hardware Change	HDD Change	Low
Hardware Change	Memory Change	Low
Hardware Health	Battery Degradation	Low
Hardware Health	HDD Degradation	Low

HP Proactive Management Incident Priority

9. HP Proactive Management Features and Services Scope

9.1. Reports by DaaS Proactive Management Plan and Platform

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

Reports	Enhanced Plan HP Managed	Premium Plan HP Managed	Windows 10	Windows 7	Android	MacOS	iOS[17]
Blue screen errors	✓	✓	✓	✓			
Device utilization	✓	✓	✓	✓			
Hardware health[18],[19]	✓	✓	✓	✓	✓	✓	✓
Hardware inventory	✓	✓	✓	✓	✓	✓	✓
HP hardware warranty	✓	✓	✓	✓			
BIOS inventory	✓	✓	✓	✓			
Non-reporting devices	✓	✓	✓	✓	✓	✓	✓
Software inventory	✓	✓	✓	✓	✓	✓	✓
Battery replacement[20]	✓	✓	✓	✓			
Disk replacement[21]	✓	✓	✓	✓			
Thermal grading	✓	✓	✓	✓			
Disk capacity planning	✓	✓	✓	✓	✓	✓	✓
Mobility Factor[22]	✓	✓	✓	✓	✓	✓	
Device health replacement guide [23]	✓	✓	✓	✓			
Security compliance	✓	✓	✓[24]		✓	✓	✓
Application catalog compliance		✓	✓[25]		✓	✓	✓
Software errors		✓	✓	✓			

[17] Requires Enhanced or Premium plan coverage and for device to be enrolled in Microsoft Intune.
[18] Only hard disk space monitoring available for IOS devices
[19] Only battery health, disk health, thermal health and hard disk space monitoring available for MAC devices. Only battery health, disk health, and hard disk space monitoring available for Android devices.
[20] Only shows devices that are classified with device type as Notebook in Proactive Management Report is available for both HP devices and non-HP devices, replacement depends on vendor's service coverage,
[21] Only includes devices that are classified as Desktop and Notebook in Proactive Management. Report is available for both HP and non-HP devices, replacement depends on vendor's service coverage.
[22] Geolocation services must be enabled on the device.
[23] Only hard disk space monitoring available for IOS devices
[24] Windows 10 only
[25] Windows 10 only

9.2. HP Proactive Management Enhanced Plan for Microsoft Intune

The HP Proactive Management Enhanced plan includes an option for customers who have invested in Microsoft Intune. HP Service Experts will perform device policy and application management tasks using Microsoft Intune for customer devices on behalf of the customer. (Note: The customer must provide the appropriate Intune licenses. Licenses are not provided by HP).

In addition, HP Service Experts monitor devices and applications on the customer's behalf and will respond as needed when problems are detected in the environment.

The HP DaaS Proactive Management Enhanced plan for Microsoft Intune includes all functions and features associated with HP DaaS Proactive Management Standard plan, plus a unified endpoint management service provided by HP Service Experts. HP Service Experts manage multiple-OS devices and Windows updates and policy settings on behalf of customers to help reduce the customer's IT workload.

1. **HP DaaS Proactive Management client –** HP DaaS Proactive Management uses client software agents to collect data on device inventory and to monitor the health of the device hardware and applications. The Windows and MacOS client software can be downloaded directly from https://www.hpdaas.com/software and deployed to end user devices. For Android systems, users can download the HP DaaS client for Android from the Google Play store.
2. **Bulk deployment support for HP DaaS Proactive Management client for Windows –** The HP DaaS Proactive Management client installer is designed to be deployed *en masse* using the customer's existing software deployment framework (Microsoft SCCM, login scripts, etc.). Customers can leverage a range of silent installation and deployment options to quickly and efficiently enroll their devices in Proactive Management, and command line options exist to silently install the software using the customer's application deployment systems.
3. **Hardware, BIOS, and software inventory reports.** Collect and view detailed device and software inventory, including BIOS version, installed applications, processor, memory, and a wide range of other details.
4. **Device Warranty reports.** View reports showing HP device warranty status.
5. **Hard disk, battery, and thermal health reports.** Monitor and detect the state of the hard disk drive, battery, and thermal health profile of the device. HP DaaS Proactive Management with TechPulse has both reactive and predictive health analysis capabilities. Examples include: disk SMART monitoring errors, disk read/write issues, devices which are operating at an unsafe temperature, which may indicate hardware failure, and disks or batteries at risk of failure based on load and behavioral characteristics. If problems are discovered, they will be available in the hardware health reports and an incident will be generated in the console, which the customer can then view and act upon.

   The Types of incidents related to device health include:
   - Hardware failure (thermal, hard disk errors, or battery degradation) – These issues may indicate a device component has experienced a failure and may need to be replaced. Note that incidents may vary by operating system.
   - Proactive hardware issue – HP DaaS Proactive Management can detect device components which are at risk of failure, even if they have not previously generated errors.
   - Non-reporting devices – A device has not communicated with HP DaaS in the past 30 days.
6. **Device hardware utilization, mobility factor, and device storage capacity planning and replacement guide reports.** HP DaaS Proactive Management includes reports on processor, memory, and disk utilization to help guide device replacement decisions. This helps customers better plan for and prioritize device hardware upgrades and replacements, making it easier to identify the device most appropriate for the end user.
7. **End user accessible tools –** The HP DaaS client for Windows includes a quick access icon in the Windows system tray (right-hand section of the Windows Taskbar). When users encounter problems on their devices with core Windows features (hard disk, display, sound, network connectivity, etc.), they can use this tool to access several Windows troubleshooting utilities.

8. **HP DaaS portal –** The HP DaaS web portal, located at https://www.hpdaas.com, is the central hub for all device analytics and reports. Using the portal, customer IT device managers can view detailed information on enrolled devices, including:
   - Device hardware inventory
   - Device software inventory
   - HP device warranty status
   - Incidents which have been detected on the device
   - Interactive, company-level dashboards with details-level drilldown. The product dashboard shows the aggregate health status of managed devices. Health information includes OS version, listing of incident types as a percentage, etc.
9. **Support for company-owned and personally-owned (aka "BYOD") device policies –** Allows the user to designate their managed device as either company-owned or employee-owned/personal (BYOD). Certain Proactive Management data collection functions are limited on devices designated at personally-owned. Some restricted functions include the collection of device software inventory and device location information.
10. **Multi-tenant views support for partners** – Multi-tenancy support allows HP partners who have multiple customers to use a single logon to access the HP DaaS portal to view incidents or run reports for different customers. This enables them to more rapidly identify and respond to incidents, enabling faster resolution of customer issues.
11. **Mass deployment of HP DaaS Proactive Management client by HP Service Experts** – HP will deploy the Proactive Management client software to Intune-managed devices to simplify the customer's deployment experience. For HP DaaS devices which are not managed by Microsoft Intune or which are not supported (e.g. Windows 7), the customer is responsible for deploying the Proactive Management client software onto the managed devices.
12. **Incident Monitoring -** This system reports detected issues into the HP Proactive Management portal. HP Service Experts use the same problem tracking system to diagnose, identify issues and provide recommendations to customers. The incident system tracks issue priority, type, details, comments, and resolution details. The incident management system also links incidents to the affected device inventory, the HP Warranty system, and the Proactive Management incident history to enable more rapid analysis of the issue.

    As part of this service, HP Service Experts will:

   - Monitor and respond to customer support requests (through the customer IT Administrator).
   - Assist the customer IT Administrator remotely using standard tools (LogMeIn) as needed.
   - Notify the customer IT Administrator when incidents are detected.
   - Order replacement parts (HP devices only) of hard drive or battery proactively based on failure prediction.
   - Review hardware failure incidents and notify the customer whether the device is eligible for replacement under their DaaS plan.
   - Monitor the incident system and inform customers whenever issues are detected. If detected, the Service Expert will issue guidance to the customer to address specific issues. For example, if a device thermal issue is detected, the Expert may offer suggestions to improve thermal operating background for the device or open a device replacement request ticket if needed.
   - Monitor and resolve customer's account manager/representative (ADM/PDM/TTM) support requests.
   - Call customer directly as needed or upon call-back request to resolve issues or to communicate information not supported through email (e.g. security-related and user identification).
13. **Security compliance policy definition and enforcement –** HP Service Experts will provision and enforce security policies for managed devices using Microsoft Intune. Examples include:
   - Device terms of use popups and notifications
   - Mobile device PIN and passcode restrictions
   - Enforcement of device storage encryption
   - Configure rules to block access for devices not configured in accordance with policy – e.g. rooted (aka "jailbroken") devices

14. **Microsoft Windows 10 and Microsoft applications software updates**- HP Proactive Management leverages modern management techniques to deliver update management. This approach allows configuration and control of Windows Update settings. An HP Service Expert and Account Delivery Manager (if applicable) will:
    - Capture configuration information from company IT to specify Service Options (below), including deployment rings
    - Gather update settings requirements from customer. HP will also offer basic update profile guidance, based on recommended best practices, which the customer may adopt or request customization of.
    - Configure update deployment policies in Intune as specified and configure Windows Update profile settings as agreed upon with the customer. This includes the following task elements:
    - Create necessary rings and update profiles based on customer specifications
    - Configure a QA ring containing devices and/or users specified by customer
    - Assign devices/user to rings based on Customer requirements
    - Communicate the introduction of new Semi-Annual channel releases by Microsoft to the customer
    - Test the semi-annual channel release against the baseline Proactive Management enhanced/premium Service
    - Confirm the customer's completion of application testing for the semi-annual channel release by the customer to validate mission critical app compatibility and adjust or delay the deployment strategy in response to the customer's findings
    - Work with the customer's change control procedures to deploy updates for UATT and Broad Ring deployments
    - Pause updates in response to customer request
    - Report issues with Windows updates rollout to Microsoft
    - Resume update policy after issue resolution
    - Provide details on profile configuration to the customer
    - If no issues are found by the customer during QA, update deployment will proceed automatically to additional rings
    - If issues are reported by the customer regarding an update deployed to the QA ring, then:
        - An HP Service Expert will pause deployment to remaining rings
        - The Customer will provide relevant data to HP Service Expert or Account Delivery Manager (if applicable)
        - An HP Service Expert will report the issue to Microsoft and/or appropriate vendor
        - The Customer will contact Account Delivery Manager or HP Service Expert to make changes to Update policy.

    In addition, the customer will:
    - 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
    - Roll back any updates on devices where issues were encountered
    - Communicate any policy changes to HP Account Delivery Manager or HP Service Expert
    - The customer may opt to receive notifications on newly-released security updates, from Microsoft at https://profile.microsoft.com/RegSysProfileCenter/wizardnp.aspx?wizid=5a2a311b-5189-4c9b-9f1a-d5e913a26c2e&lcid=1033&culture=en-us&dir=LTR
15. **Lost Device Protection: Device Lock** – HP Service Experts will remotely issue a command to reset the device PIN code to lock users out of a missing or stolen device in response to the customer request.[26]

[26] The target device must be connected to the Internet to receive the command.

16. Lost Device Protection: Device Wipe – HP Service Experts will remotely issue a command to erase data (Corporate data erase or device factory reset) from a missing or stolen device in response to the customer request.[27]

17. Remote diagnostic and resolution assistance - The HP Proactive Service Expert team can remotely assist end-users using web-based tools (LogMeIn) to chat with and/or initiate remote control sessions with end-user devices.
18. Device hardware change monitoring - HP DaaS Proactive Management can detect changes to the installed hard disk, or system memory, which may be due to device repair, theft or other events.
19. Automatic parts replacement - Based on the predictive alerts for hard disk, thermal, and battery issues, HP will dispatch replacement parts for covered HP manufactured devices to the customer site, in accordance with the device warranty.

9.3. HP Proactive Management Premium Plan for Microsoft Intune

The HP DaaS Proactive Management Premium Plan for customers with Microsoft Intune expands upon the Enhanced service capabilities and extends the HP unified endpoint management service to include device application deployment and app policy. This includes all functions and features associated with HP DaaS Proactive Management Enhanced plan, plus:

1. Mobile Application deployment - The application delivery service covers multiple functions, including:
   - Automatic push or on-demand install through the enterprise app store
   - Group-based assignment leveraging AD groups or Azure AD Groups
   - Automatic or on-demand store app updates
   - Application removal from the enterprise app store or updates to end user or device application assignments

   Applications can be deployed to both Intune MDM-managed devices, or to users on unmanaged devices using mobile application management. The application delivery service supports:

   - Public App Store apps – Free apps from Google Play, Windows Store, or the Apple app store
   - Public paid applications via Apple VPP, and Windows Store for Business.
   - Windows 10 application package types including APPX, MSIX, or MSI. Win32 applications (MSI packaged) with slient command line options applications must be self-contained which do not require a task sequence, pre or post scripts, and no dependency checks (HP recommends to test package is self-contained by using command prompt *msiexec* to install).
   - Android and iOS line-of-business applications packaged as IPA (iOS) or APK (Android) with appropriate enterprise signatures.
   - Web-based application URL shortcuts.

   The application deployment capability does not support:

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

   Application deployment task flow:
   - HP Service Expert or Account Delivery Manager (if applicable) captures configuration information from company IT to specify Service Options (below).
   - Customer will provide any necessary application or logo binaries in MSI packages.
   - Customer enrolls in iOS VPP (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).

[27] The target device must be connected to the Internet to receive the command.

- 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 to the MDM infrastructure.
  - HP Service Expert will specify command line options or application configuration options per requirements.
  - HP Service Expert will deploy application initially to test device to validate deployment settings are correct.
  - Customer will review the deployed application to confirm deployment was successful and correct prior to approval of broad deployment.
  - HP Service Expert will coordinate the final production application deployment schedule with the customer, in accordance with the customer's change control policy.
- HP Service Expert will select and deploy store apps as needed.
- HP Service Expert will assign devices/user to deployment groups or rings based on customer requirements.

2. Support for Microsoft Intune MDM enrollment using Apple Device Enrollment Program (DEP) – To support out of box enrollment and enforcement of mobile device management (MDM) persistency, HP supports use of the Apple Device Enrollment Program (DEP) framework.
3. Device WIFI provisioning – HP Service Experts will use Microsoft Intune to provision WiFi, WLAN and VPN profiles, etc. per customer request.
4. Windows Information Protection (WIP) - HP Service Experts can help protect against accidental data leakage due to device loss with policy. Information protection policies enforce on-device encryption of application data and can be used to restrict copy and print function, or which applications can decrypt and open files from a protected data location.
5. Windows machine local password recovery - 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. Note: Active Directory is not supported by this feature. Only Windows machine local accounts are supported.
6. Mobile app blacklist/whitelist management - HP Service Experts will implement and enforce policies to allow (whitelist) or deny (blacklist) use of applications on managed devices.
7. Configure device "kiosk" mode – HP Service experts can configure Android and iOS mobile devices to run in kiosk n mode[28] or lock a Windows 10 desktop view to control which apps are able to run on the device.

[28] Requires supervisor mode.

9.4. Feature and managed service by plan and by OS type

Feature	Description	DaaS Plan for Microsoft Intune		Operating System				
		Enhanced	Premium	Win10	Win7	iOS	Android	Mac OS
Bring Your Own Device (BYOD) Policy	Limit Proactive Management data collection capabilities for employee owned devices.	✓	✓	✓	✓	✓	✓	✓
Mass Device Enrollment	Enables large-scale enrollment of devices and users for Proactive Management client[29]. Automated processes enable multiple devices to be configured and associated with the end user's account.	✓	✓	✓	✓	✓	✓[30]	✓
Lost Device Protection: Lock Device[31]	HP Service Experts can perform a screen lock (PIN reset) on a managed device if it is reported lost or stolen.	✓	✓			✓	✓	
Lost Device Protection: Wipe Device Data [32]	HP Service Experts can remotely issue a device Wipe command to reset the device (erase all data) or perform a corporate data erase from a managed mobile device, notebook, or desktop PC.	✓	✓	✓		✓	✓	
Lost Device Protection: Find device	HP Service Experts can attempt to locate the approximate location of a missing or lost device on a map.	✓	✓	✓		✓	✓[33]	
Firewall Policy	Generates reports on the state of the Microsoft Windows firewall service on Windows PCs, and enforce Defender using Microsoft Intune.	✓	✓	✓	✓	Report only		
Groups-based policy management	HP Service Experts can quickly apply policies to groups of users and/or devices.	✓	✓	✓	✓	✓	✓	✓
Hard Disk Health Monitoring	Monitors hard drives on notebooks and desktops. Get notified if a disk drive needs replacement or if the disk has been replaced or removed.	✓	✓	✓	✓	✓[34]		
Microsoft Updates Management	HP Service Experts can configure Windows Update settings on PC device.	✓	✓	✓				
Mobile Device Security Policy	HP Service Experts can apply custom security levels to managed devices using Microsoft Intune.	✓	✓	✓	✓	✓	✓	✓

[29] Bulk enrollment for iOS and MacOS devices applies to Intune MDM enrollment using Apple DEP

[30] Requires Apple DEP account.

[31] The target device must be connected to the Internet to receive the command. iOS devices must be in Supervisor mode.

[32] The target device must be connected to the Internet to receive the command. iOS devices must be in Supervisor mode.

[33] The target device must be connected to the Internet to receive the command. iOS devices must be in Supervisor mode.

[34] Available storage only

Feature	Description	DaaS Plan for Microsoft Intune		Operating System				
		Enhanced	Premium	Win10	Win7	iOS	Android	Mac OS
Incident Management	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 intelligence in multi-OS environments 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).	✓	✓			✓		✓
Device Encryption Enforcement	HP Service Experts can enforce encryption policy on managed devices.	✓	✓	✓		✓[35]	✓	✓
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	Identify 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.	✓	✓	✓	✓			
Device Inventory	View a list of managed PCs, and mobile devices, plus detailed device information such as available space, memory, OS version, and other details.	✓	✓	✓	✓	✓	✓	✓
Virus Protection Policy	Detect whether antivirus software is enabled on a Windows device. Customers can run security compliance reports to quantify gaps in coverage.	✓	✓	✓				
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.		✓	✓		✓	✓	✓

[35] Apple iOS enforces encryption automatically, if a passcode is set on the device. However, HP can enforce passcodes, and encryption using Microsoft Intune.

Feature	Description	DaaS Plan for Microsoft Intune		Operating System				
		Enhanced	Premium	Win10	Win7	iOS	Android	Mac OS
Device Utilization Report	Generate reports showing devices whose CPU and/or memory usage is consistently high, usually indicating poor user experience.	✓	✓	✓	✓			
OS Crash Monitoring	Generate reports to identify device OS crashes, and error information.	✓	✓	✓	✓			
Easy-access for Windows self-help tools	Provides easy access to diagnostic tools, enabling end-users to troubleshoot and resolve common issues instead of escalating to the customer's internal help desk.	✓	✓	✓	✓			
Non-reporting Device Monitoring	Get alerted if a managed device has not communicated with the management server for more than 7 days.	✓	✓	✓	✓	✓	✓	✓
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.		✓			✓	✓	✓
Microsoft Windows® Application Deployment	HP Service Experts can create, distribute, and manage curated bundles desktop applications to managed Windows devices. View reports to identify devices which do not have assigned apps installed.		✓	✓				
Machine local Password Recovery	End users can reset a forgotten machine local user account password on Windows notebooks PCs and tablets.		✓	✓	✓			
Mobile App Whitelisting and Blacklisting	HP Service Experts can control which apps can run on the device based on customer guidance.		✓	✓	✓	✓	✓	✓

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.

4AA7-3714ENW – September 18, 2018