HP DaaS Proactive Management
Enhanced and Premium Plans for Intune | Service Fact Sheet

HP Baseline:

The following table describes the baseline parameters and settings applied on devices enrolled in HP DaaS Enhanced and Premium Plans for Intune supported by Proactive Management. Please consult with your onboarding Program Manager if changes are required.

See the HP DaaS Proactive Management Service Definitions for Operating System requirements.

Feature	Description	Supported OS
Locate Device	The device must be a corporate-owned iOS device, enrolled through the device enrollment program, and be in supervised mode. Before you use this action, be sure the device is in lost mode.	iOS (Supervisor Mode)
Remote Lock	The Remote lock device action locks the device. To unlock the device, the device owner enters their passcode. You can remotely lock devices that have a PIN or password set. Devices that don't have a PIN or password can't be remotely locked.	iOS and Android
Factory Reset	Wipes all user accounts, data, MDM policies, and settings. Resets the operating system to its default state and settings.	Windows 10, iOS and Android
Remove company data	The Remove company data action removes managed app data (where applicable), settings, and email profiles that were assigned by using Intune. The device will be removed from Intune management. This happens the next time the device checks in and receives the remote Remove company data action. Remove company data leaves the user's personal data on the device.	Windows 10, iOS, Android and macOS

Software Updates Windows 10 update Rings		
Parameter	Description	Setting
Servicing channel	Set channel to receive updates	Semi-Annual Channel
Microsoft Product Updates	Choose to scan for app updates from Microsoft Update	Allow
Windows drivers	Choose to exclude Windows Update drivers during updates	Allow
Automatic update behavior	Manage Automatic Updates behavior to scan, download and install updates	Auto Install and restart at maintenance time

Windows Enrollment

Microsoft Hello for Business

Parameter	Description	Setting
Configure Windows Hello for Business	Not Configured will honor the configuration done on the client. Multi-Factor Authentication through Microsoft is a prerequisite if Windows Hello for Business is enabled.	Not Configured
Use a Trusted Platform Module (TPM)	A Trusted Platform Module (TPM) provides an additional layer of data security. If set to required, only devices with an accessible TPM can provision Windows Hello for Business	Required (If Hello is enabled)
Minimum PIN length	Minimum PIN length must be between 4 and 127	8 (if Hello is enabled)
Allow Biometric authentication	If Allowed, Windows Hello for Business can authenticate using gestures, such as face and fingerprint. Users must still configure PIN in case of failure.	Yes (If Hello is enabled)

Devices

Device Clean-Up Rules

Set your Intune device cleanup rules to delete Intune MDM enrolled devices that appear inactive, stale, or unresponsive. Intune applies cleanup rules immediately and continuously so that your device records remain current.

Parameter	Description	Setting
Delete Device based on Last Check-in	When set to yes, Intune deletes devices based on the custom number of days specified (90-270). When set to no, Intune deletes all devices not checked in after 270 days	Yes
Delete Devices that have not checked in after this many days?	Custom Number of days (90-270)	90

Device Compliance Policy

Windows 10 Compliance Profile

Device Health

Parameter	Description	Setting
Require BitLocker	Require BitLocker to be enabled on the device (Not Supported on Windows 10 Professional)	Require

System Security		
Parameter	Description	Setting
Firewall	Require firewall to be on and monitoring	Require
Antivirus	Require any Antivirus solution registered with Windows Security Center to be on and monitoring	Require
AntiSpyWare	Require any AntiSpyWare solution registered with Windows Security Center to be on and monitoring	Require
Windows Defender Antimalware	Require the Windows Defender service to be enabled.	Require
Windows Defender Antimalware signature up-to-date	Require the Windows Defender signature to be up-to-date	Require
Real-time protection	Require real-time protection prompts for known malware detection	Require
Actions for noncompliance		
Parameter	Description	Setting
Mark Device noncompliant	One block item makes the device noncompliant	Mark Device noncompliant
Scheduled (days of noncompliant)	Specifies the number of days after noncompliance after which this action should be triggered for the user's device	0

Device Configuration Policy
Windows 10 and Later
End Point Protection Profile
Windows Encryption
BitLocker base settings (OS Drive Only)

Parameter	Description	Setting
Encrypted OS Drive (Windows 10 Business, Education & Enterprise Only)	To prompt users to enable device encryption (Not supported in Windows 10 Professional)	Required
Configure encryption methods (Windows 10 Business, Education & Enterprise Only)	BitLocker will use the default encryption method of XTS-AES 128-bit	Default
Additional authentication at startup	This setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This setting is applied when you turn on BitLocker.	Require
Compatible TPM Startup	This setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This setting is applied when you turn on BitLocker.	Require TPM
Compatible TPM startup PIN	The entry of a 6-digit to 20-digit personal identification number (PIN)	Allow startup PIN
Compatible TPM startup key	Can require insertion of a USB flash drive containing a start-up key	Allow startup key
Compatible TPM startup key and PIN	The entry of a 4-digit to 20-digit personal identification number (PIN) and require insertion of a USB flash drive containing a start-up key.	Allow startup PIN or startup key
Save BitLocker recovery information to Azure Active Directory	Enable BitLocker recovery information to Azure Active Directory	Enable
BitLocker recovery Information stored to Azure Active Directory	Configure what pieces of the BitLocker Information will be in the Azure Active Directory	Backup Recovery Passwords and Key Packages
Store recovery information in Azure Active Directory before enabling BitLocker	Prevent Users from Enabling BitLocker until all the recovery information has been stored in Azure Active Directory	Enable

Windows Defender Security Center		
Parameter	Description	Setting
Family Options	Provides easy access to managing your children's online experiences and the devices in your household.	Hide

Windows Defender Firewall Network settings Domain (workplace) network		
Parameter	Description	Setting
Windows Defender Firewall	If this value is disabled, the server MUST NOT block any network traffic, regardless of other policy settings	Enabled
Shielded	If this value is Blocked and Firewall is Enabled, the server MUST block all incoming traffic regardless of other policy settings.	Blocked

Private (discoverable) network		
Parameter	Description	Setting
Windows Defender Firewall	If this value is disabled, the server MUST NOT block any network traffic, regardless of other policy settings	Enabled
Shielded	If this value is Blocked and Firewall is Enabled, the server MUST block all incoming traffic regardless of other policy settings.	Blocked
Public (non-discoverable) network		
Parameter	Description	Setting
Windows Defender Firewall	If this value is disabled, the server MUST NOT block any network traffic, regardless of other policy settings	Enabled
Shielded	If this value is Blocked and Firewall is Enabled, the server MUST block all incoming traffic regardless of other policy settings.	Blocked

Device Restriction Profile		
Password		
Parameter	Description	Setting
Windows Hello device authentication	Allow the use of Windows Hello companion devices for authentication with Windows	Allow
Maximum minutes of inactivity until screen locks	Maximum minutes of inactivity until screen locks	15 Minutes
Number of sign-in failures before wiping device	For devices running Windows 10: If the device has BitLocker enabled, it's put into BitLocker recovery mode after sign-in fails the number of times that you specified. If the device is not BitLocker enabled, then this setting doesn't apply. For devices running Windows 10 Mobile: After sign-in fails the number of times you specify, the device is wiped.	10
Simple passwords	Specifies whether simple passwords such as “1111” or “1234” are allowed.	Block
Cloud and Storage		
Parameter	Description	Setting
Settings synchronization for Microsoft account	Block synchronization of Microsoft Account	Block
Reporting and Telemetry		
Parameter	Description	Setting
Allow Telemetry	Select Level of diagnostic data submission	Enhanced Level
Windows Defender Antivirus		
Parameter	Description	Setting
Real-time monitoring	Real-time monitoring	Enable
Behavior monitoring	Check for patterns of suspicious behavior	Enable
Network Inspection System (NIS)	Block malicious traffic detected by signature in the Network Inspection System	Enable
Scan all downloads	Scan all downloads	Enable
Scan scripts loaded in Microsoft web browsers	Scan scripts loaded in Microsoft web browsers	Enable
Signature update interval (in hours)	Signature update interval (in hours)	6
Monitor file and program activity	Monitor file and program activity	Monitoring Incoming Only
Days before deleting quarantined malware	Days to wait before deleting quarantined malware. 0-90, 0 means never delete	1
CPU usage limit during a scan	Maximum CPU % usage during a scan (50 is recommend by Microsoft) (0-100)	50
Scan archive files	Scan archive files	Enable
Scan incoming mail messages	Scan incoming mail messages	Enable

Parameter	Description	Setting
Cloud-delivered protection	Send the Microsoft Active Protection Service telemetry to allow detection of suspicious activity	Enable
File Blocking Level	Specify the level of cloud-delivered protection. • Not configured - uses the default Windows Defender Antivirus blocking level and provides strong detection without increasing the risk of detecting legitimate files. • High - applies a strong level of detection • High + - uses the High level and applies additional protection measures (may impact client performance) • Zero tolerance - blocks all unknown executables While unlikely, setting to High may cause some legitimate files to be detected. Microsoft recommends you set this to the default level (Not configured)	High
Time extension for file scanning by the cloud	Specify the maximum amount of time that Windows Defender Antivirus should block a file while waiting for a result from the cloud. The base amount is 10 seconds – any additional time specified here (up to 50 seconds) will be added to those 10 seconds. This amount is a theoretical maximum-in most cases the scan will take less time than the maximum.	20
Prompt users before sample submission	Send telemetry to Microsoft Active Protection Service for detection of suspicious activity.	Send all data without prompting
Time to perform a daily quick scan	Time of day to perform a daily quick scan	12PM
Type of system scan to perform	Type of system scan to perform	Full Scan
Day scheduled	Day scheduled for system scan	Friday
Time scheduled	Time scheduled for system scan	4PM
Schedule scan day	Select the day Windows Defender should run	Everyday
Actions on detected malware threats	Allow to specify any valid threat levels and the corresponding default action to take.	Enable
Low severity	Low severity	Quarantine
Moderate severity	Moderate severity	Quarantine
High severity	High severity	Clean
Severe severity	Severe severity	Clean

Windows Defender Antivirus Exclusions		
Parameter	Description	Setting
Files and Folders to exclude from scans and real-time protection	Files and Folders to exclude from scans and real-time protection	%windir%\SoftwareDistribution\Datastore\Datastore.edb %windir%\SoftwareDistribution\Logs\Edb*.jrs %windir%\SoftwareDistribution\Logs\Edb.chk %windir%\SoftwareDistribution\Logs\Tmp.edb %windir%\Security\Database\
Windows Defender SmartScreen		
Parameter	Description	Setting
SmartScreen for apps and files	Enable SmartScreen for file executions and running apps	Enable

Other Device Profiles (Not Defined)		
Profiles	Description	Setting
Wi-Fi	If you interested in this Parameter, you will need to discuss with your Onboarding Program Manager. https://docs.microsoft.com/en-us/intune/wi-fi-settings-configure	Customer Provided Settings
VPN	If you interested in this Parameter, you will need to discuss with your Onboarding Program Manager. https://docs.microsoft.com/en-us/intune/vpn-settings-configure	Customer Provided Settings
Advanced Threat Protection (ATP)	If you interested in this Parameter, you will need to discuss with your Onboarding Program Manager.	Customer Provided Settings

Apple IOS Policies Device Compliance Policy System Security		
Require a password to unlock mobile devices.	This setting specifies whether to require users to enter a password before access is granted to information on their mobile devices.	Require
Device Configuration Policy Device Restriction Password		
Parameter	Description	Setting
Password	Require password to access device	Require
Simple passwords	Block simple password sequences, such as 1234 or 1111	Blocked
Minimum password length	Minimum number of digits or characters in password. (4-14)	6
Number of sign-in failures before wiping device	Number of consecutive times an incorrect password can be entered before device is wiped of all data. (1-11)	Never
Maximum minutes after screen lock before password is required	Maximum minutes after screen lock before password is required. Immediately recommended. Ignored by device if new time is longer than what's currently set on device	15
Maximum minutes of inactivity until screen locks	Maximum minutes of inactivity until screen locks. Ignored by device if new time is longer than what's currently set on device. If set to Immediately, devices will use the minimum possible value per device.	10

Apple IOS Policies Device Compliance Policy System Security		
Require a password to unlock mobile devices.	This setting specifies whether to require users to enter a password before access is granted to information on their mobile devices.	Require

Device Configuration Policy Device Restriction Password		
Parameter	Description	Setting
Password	Require password to access device	Require
Simple passwords	Block simple password sequences, such as 1234 or 1111	Blocked
Minimum password length	Minimum number of digits or characters in password. (4-14)	6
Number of sign-in failures before wiping device	Number of consecutive times an incorrect password can be entered before device is wiped of all data. (1-11)	Never
Maximum minutes after screen lock before password is required	Maximum minutes after screen lock before password is required. Immediately recommended. Ignored by device if new time is longer than what's currently set on device	15
Maximum minutes of inactivity until screen locks	Maximum minutes of inactivity until screen locks. Ignored by device if new time is longer than what's currently set on device. If set to Immediately, devices will use the minimum possible value per device.	10

OTHER Device Profiles (Not Defined)		
Profiles	Description	Setting
Wi-Fi	If you interested in this Parameter, you will need to discuss with your Onboarding Program Manager. https://docs.microsoft.com/en-us/intune/wi-fi-settings-configure	Customer Provided Settings
VPN	If you interested in this Parameter, you will need to discuss with your Onboarding Program Manager. https://docs.microsoft.com/en-us/intune/vpn-settings-configure	Customer Provided Settings

Android Policies

Device Compliance Policy

Android

System Security

Parameter	Description	Setting
Require a password to unlock mobile devices.	This setting specifies whether to require users to enter a password before access is granted to information on their mobile devices. Recommended value: Require	Require
Minimum password length	Specifies the Minimum number of digits or characters in password. (4-16)	6
Required password type	Specifies whether passwords can be comprised only of numeric characters, or whether they must contain other than numbers	At least Numeric
Maximum minutes of inactivity before password is required	Maximum length of time without user input after which the mobile device screen is locked. Recommended value:15 min	15
Encryption of data storage on device	Require encryption of data storage on device	Require

Device Configuration Policy

Device Restriction

Password

Parameter	Description	Setting
Password	Require users to enter a password before access is granted to information on their mobile devices.	Require
Minimum password length	Minimum number of digits or characters in password. (4-16)	6
Maximum minutes of inactivity until screen locks	Maximum length of time without user input after which the mobile device screen is locked.	15
Number of sign-in failures before wiping device	Number of consecutive times an incorrect password can be entered before device is wiped of all data. (4-11)	10
Encryption	Require encryption on device Not all devices support encryption. You must also: • Enable 'Require password' • Specify 'Password quality' of 'At least numeric' • Set 'Minimum password length' of at least 4, to correctly report complinace for this setting.	Require

Other Device Profiles (Not Defined)

Profiles	Description	Setting
Wi-Fi	If you interested in this Parameter, you will need to discuss with your Onboarding Program Manager. https://docs.microsoft.com/en-us/intune/wi-fi-settings-configure	Customer Provided Settings
VPN	If you interested in this Parameter, you will need to discuss with your Onboarding Program Manager. https://docs.microsoft.com/en-us/intune/vpn-settings-configure	Customer Provided Settings

Andriod Enterprise Policies

Device Compliance Policy

Android Enterprise

System Security

Parameter	Description	Setting
Require a password to unlock mobile devices.	This setting specifies whether to require users to enter a password before access is granted to information on their mobile devices.	Require
Minimum password length	Specifies the Minimum number of digits or characters in password. (4-16)	6
Required password type	Specifies whether passwords can be comprised only of numeric characters, or whether they must contain other than numbers	At least Numeric
Maximum minutes of inactivity before password is required	Maximum length of time without user input after which the mobile device screen is locked.	15
Encryption of data storage on device	Require encryption of data storage on device	Require

Device Configuration Policy

Android Enterprise

Device Restriction

Password

Parameter	Description	Setting
Password	Require users to enter a password before access is granted to information on their mobile devices.	Require
Minimum password length	Minimum number of digits or characters in password. (4-16)	6
Maximum minutes of inactivity until screen locks	Maximum length of time without user input after which the mobile device screen is locked.	10
Number of sign-in failures before wiping device	Number of consecutive times an incorrect password can be entered before device is wiped of all data. (4-11)	10

OTHER Device Profiles (Not Defined)

Profiles	Description	Setting
Wi-Fi	If you interested in this Parameter, you will need to discuss with your Onboarding Program Manager. https://docs.microsoft.com/en-us/intune/wi-fi-settings-configure	Customer Provided Settings
VPN	If you interested in this Parameter, you will need to discuss with your Onboarding Program Manager. https://docs.microsoft.com/en-us/intune/vpn-settings-configure	Customer Provided Settings