Windows 10 Accelerator Program Health Checks

Introduction

The Adaptiva Windows 10 Accelerator Program is a stress-free, cost-effective way to deploy Windows 10 at unparalleled speed and massive scale.

Save	Speed	Secure
Infrastructure and administration costs	OS deployment by automating tasks	Windows 10 endpoints during and post deployment

To deliver these benefits, Adaptiva has curated best-in-class technology, tools, and training from Microsoft, the SCCM community, and our own technical team. This unique approach provides a complete, end-to-end ecosystem to help you plan and test, deploy, and maintain Windows 10 in your organization.

Adaptiva Client Health is an endpoint health and security engine that improves IT efficiency and response rates by automatically checking a device's health, diagnosing any problems, and fixing issues…instantly. The Windows 10 Accelerator Program includes a new version of Client Health specifically designed for Windows 10. Adaptiva Client Health for Windows 10 includes over a dozen new health checks unique to Windows 10. The following pages list the health checks included as part of the program.

Client Health for Windows 10: Health Check List

Windows 10 Only

Health Checks	Supports Remediation	Description	Impact
Windows 10 - Credential Guard Active	Yes	Verifies: That Credential Guard is enabled and active on the machine. If Credential Guard is not enabled, remediation will enable it.	Improves security by enabling Credential Guard to protect the organization by isolating and hardening key system and user secrets against compromise.
Windows 10 - Device Guard & Credential Guard Active	Yes	Verifies: That both Device Guard and Credential Guard are enabled and active on the machine. If Device Guard and Credential Guard are not enabled, remediation will enable them.	Improves security by enabling Device Guard and Credential Guard to harden a computer system against malware and further protect the organization by isolating and hardening key system and user secrets against compromise.
Windows 10 - Device Guard & Credential Guard Capable	No	Verifies: That the device has all prerequisites and is capable of supporting both Device Guard and Credential Guard.	Helps improve security by determining whether or not the endpoint can run Device Guard and Credential Guard features.

Health Checks	Supports Remediation	Description	Impact
Windows 10 - Device Guard HVCI Active	Yes	Verifies: That Device Guard/HVCI is enabled and active on the machine. If Device Guard is not enabled remediation will enable it.	Improves security by enabling Device Guard, which will harden a computer system against malware.
Windows 10 - DG-CG - DMA Protection	No	Verifies: That Direct Memory Access Protection is available.	Helps improve security by determining whether DMA Protection, which is desirable for Device Guard/Credential Guard security, is available.
Windows 10 - DG-CG - NX Protection	No	Verifies: That No-Execute (NX) Protection is available.	Helps improve security by determining whether No-Execute (NX) Protection, which is desirable for Device Guard/Credential Guard security, is available.
Windows 10 - DG-CG - OS Architecture	No	Verifies: That the Operating System is 64-bit.	Helps improve security by determining whether the system is running the 64-bit version of the OS, as 64-bit virtualization is required for Device Guard/Credential Guard.

Health Checks	Supports Remediation	Description	Impact
Windows 10 - DG-CG - OS SKU	No	Verifies: That the Operating System is a valid SKU. Supported SKUs for Device Guard/ Credential Guard include Enterprise, Server, Education and IoT.	Helps improve security by determining whether the version of Windows on an endpoint is capable of running Device Guard/ Credential Guard.
Windows 10 - DG-CG - Secure Boot State	No	Verifies: That Secure Boot is enabled on the device.	Helps improve security by determining whether Secure Boot, which is a requirement for Device Guard/ Credential Guard, is running.
Windows 10 - DG-CG - Secure MOR	No	Verifies: That Secure Memory Overwrite Request (MOR) Protection is available.	Helps improve security by determining whether MOR protection, an advanced security feature desirable for Device Guard/ Credential Guard security, is available on the endpoint.
Windows 10 - DG-CG - SLAT Supported CPU	No	Verifies: That the installed CPU supports the Second-level address translation feature.	Helps improve security by determining whether Second-level address translation, an advanced security feature desirable for Device Guard/ Credential Guard security, is supported by the hardware.

Health Checks	Supports Remediation	Description	Impact
Windows 10 - DG-CG - SMM Protection	No	Verifies: That System Management Mode (SMM) Protection is available.	Helps improve security by determining whether (SMM) Protection, an advanced security feature desirable for Device Guard/ Credential Guard security, is available.
Windows 10 - DG-CG - TPM Version	No	Verifies: That the system has a valid TPM and that it is at least version 2.0.	Helps improve security by determining whether the version TPM allows the utilization of Device Guard/Credential Guard.
Windows 10 - DG-CG - Virtualization Firmware	No	Verifies: That virtualization firmware is present and available. This includes Intel Virtualization Technology, Intel VT-x, AMD-V, Virtualization Extensions or similar. Virtualization firmware is a requirement for Device Guard/ Credential Guard.	Helps improve security by determining whether the virtualization firmware required for Device Guard/Credential Guard is present and available.
Windows 10 - DG-CG - Win10 Build Version	No	Verifies: That the version of Windows 10 running is Redstone X or higher.	Helps improve security by determining whether the version of Windows, supports advanced security features for Device Guard/Credential Guard that were made available in the release of version 1511.

Health Checks	Supports Remediation	Description	Impact
Windows 10 - Last OS Install Date-Time	No	Verifies: That the last time the device had an OS install/reinstall was more than X days ago.	Improves end-user experience by ensuring that end-users that have just been disrupted for an install are prioritized last for another install.
Windows 10 - Microsoft Edge Version	No	Verifies: That the installed version of Microsoft Edge meets requirements.	Ensures secure browsing via Microsoft Edge by determining if the installed version of Edge meet requirements.
Windows 10 - Minimum Hardware Requirements	No	Verifies: That the device has the minimum required hardware specification for supporting Windows 10. Defaults are set to Microsoft hardware recommendations but can be adjusted at design time or runtime to reflect specific business requirements for upgrade.	Supports Windows 10 deployment by allowing for automatic determination of Windows 10 hardware compatibility to ensure smooth upgrades.
Windows 10 - Unified Extensible Firmware Interface (UEFI)	No	Verifies: That the device is running the Unified Extensible Firmware Interface (UEFI) required for Secure Boot and Device Guard/Credential Guard. These security features are not supported on legacy BIOS.	Helps improve security by determining hardware readiness for advanced security features such as Secure Boot, Device Guard, and Credential Guard.

Windows 10, 8.1, 8, and 7

Health Checks	Supports Remediation	Description	Impact
OS - Admin Share Available	Yes	Verifies: The admin$ share is published on the client	The Admin$ share is used for administrative connectivity to the device. This allows administrators to be able to connect and manage the file system remotely. Some applications also depend on this share being accessible.
Adaptiva Client - Version	No	Verifies: Whether adaptiva client version is equal to desired adaptiva client version	Many product improvements, enhancements, bug fixes, and new features have been added to later versions of the Adaptiva Client. This check will check whether the client is at the latest version and can be used for reporting and targeting purposes.
OS - Computer Naming Convention	No	Detects whether the computer naming convention matches the specified regular expression	Used for reporting purposes to identify machines that have been named incorrectly and not according to corporate naming standards. These devices could then be renamed appropriately.

Health Checks	Supports Remediation	Description	Impact
OS - File Associations	Yes	Verifies: That a list of file extensions are present and match. Corrects any that are incorrect and adds any that are missing	Useful for enforcing file-extensions, use cases include association of files to corporate-preferred applications rather than Windows native, commercially licensable, or undesired alternative applications.
OS - Logon Server correct	No	Detects whether the current Logon Server matches the desired name	An incorrect or geographically different logon server could indicate a misconfiguration centrally that would need to be addressed. An incorrect remote logon server could introduce problems such as slow logon or the inability to access certain resources.
OS - Remote Desktop Settings	Yes	Verifies: Remote Desktop, Remote Assistance and Secure connection (Network Level Authentication) and sets if any are incorrect	Allows for central management of device RDP settings. This allows for administrators to be able to remotely connect to and manage devices.

Health Checks	Supports Remediation	Description	Impact
OS - Run Key Entries	Yes	Verifies: Both the x86 and x64 Run Key entries are in an allowed list. Removes any that are not	Run key entries are a popular way for viruses or malicious code to execute on system startup. This check ensures that only the items in the allowed list are allowed to be present in the run key, which protects systems from harmful software execution.
OS - Screen Saver Settings	Yes	Verifies: For each user, whether the screen saver is configured, whether it's set to password protected, the timeout and the path. If any are incorrect, they are corrected	Allows for central management of screensaver settings. Could be used by organizations to enforce a corporate-branded screensaver.
OS - Security Group presence	Yes	Verifies: Local group membership for a specified local group to ensure that a specified member exists. If it does not exist, it is added	Can be used in place of group policy preferences to ensure that a specific local group—such as the Local Administrators, Power Users or Remote Access groups—have the specified user or group as a member.
OS - Version	No	Verifies: The client operating system version is one of the desired versions	Used for OS identification purposes and to report on machines that are running outdated, unsupported or externally-installed operating systems.

Health Checks	Supports Remediation	Description	Impact
OS - Windows Explorer Settings	Yes	The following - Show Hidden Files, Show Protected System Files, Hide File Extensions for Known File Types, Compressed Files in a different color, Show Run on Start Menu, Hide Empty Drives. Corrects any that are incorrect	Useful for enforcing or initially setting explorer settings without restricting the user from changing them later, such as through group policy.
OS - Windows licensing compliance	No	Detects the current Windows licensing state	This is useful for administrators to detect machines that are not licensed for Windows. This could indicate a problem with KMS, or machines using a MAK key rather than a KMS key, machines that are running a home edition or non-corporate installation, etc.
OS - Clear windows print queues	Yes	Clears the Windows printer queues	Performs an action to clear the print queues, useful for resolving many printer-related issues or stopping a bad printjob.
OS - Delete Temp Folder Contents	No	Deletes all content from Temp folders	Allows for reclamation of disk space, removing potentially harmful files, and general housekeeping.

Health Checks	Supports Remediation	Description	Impact
Remote Registry Service Running (OS Specific)	Yes	Verifies: The RemoteRegistry service is running based on operating system, and its start mode is set to desired type	Remote registry allows administrators to remotely access and manage a client's registry. It is therefore important that this service is running and the service start mode is set correctly.
Security - User Access Control (UAC) Enabled	Yes	Verifies: If UAC is enabled: performed only on Vista or later operating systems	User Account Control prevents actions that would normally require administrator access from making changes to the system by presenting a user dialogue box that has to be manually accepted. This check ensures that this setting is enabled.
Security - User Local Admin	No	Detects whether the currently logged on user is a local administrator.	Useful for reporting purposes to identify systems where the user is an administrator of their machine. Administrative access allows full control over the system and system resources and could be used for malicious purposes if someone were to gain access to the machine.

Health Checks	Supports Remediation	Description	Impact
Software - Illegal Software installed	No	Detects whether any software specified in a named list of either software titles or software GUIDs is installed	Lots of organizations will maintain a list of prohibited software, such as torrent applications, games, illegal, or inappropriate software, etc. This health check will scan the machine for any named or partial-matching titles and can be used for reporting purposes or for targeted, enforced software removal.
Software - Internet Explorer Home Page	Yes	Verifies: Whether the Internet Explorer home page is set correctly, and if not sets it.	Can be used by administrators for enforcing a particular home page or list of home pages.

Learn More

The Windows 10 Accelerator Program is the fastest and most complete deployment solution available to enterprises. OneSite runs on millions of devices in the largest companies in the world, and has been successfully deploying Windows 10 at massive scale since 2015. The program covers everything from initial training for IT through every aspect of planning, deployment, security, and ongoing maintenance.

To learn more about the Windows 10 Accelerator Program, **ask for a demo** customized to your unique needs.

3005 112th Ave NE
Suite 250
Bellevue, WA

+1 (425) 823-4500
info@adaptiva.com
adaptiva.com

@adaptiva
/adaptiva
/company/adaptiva