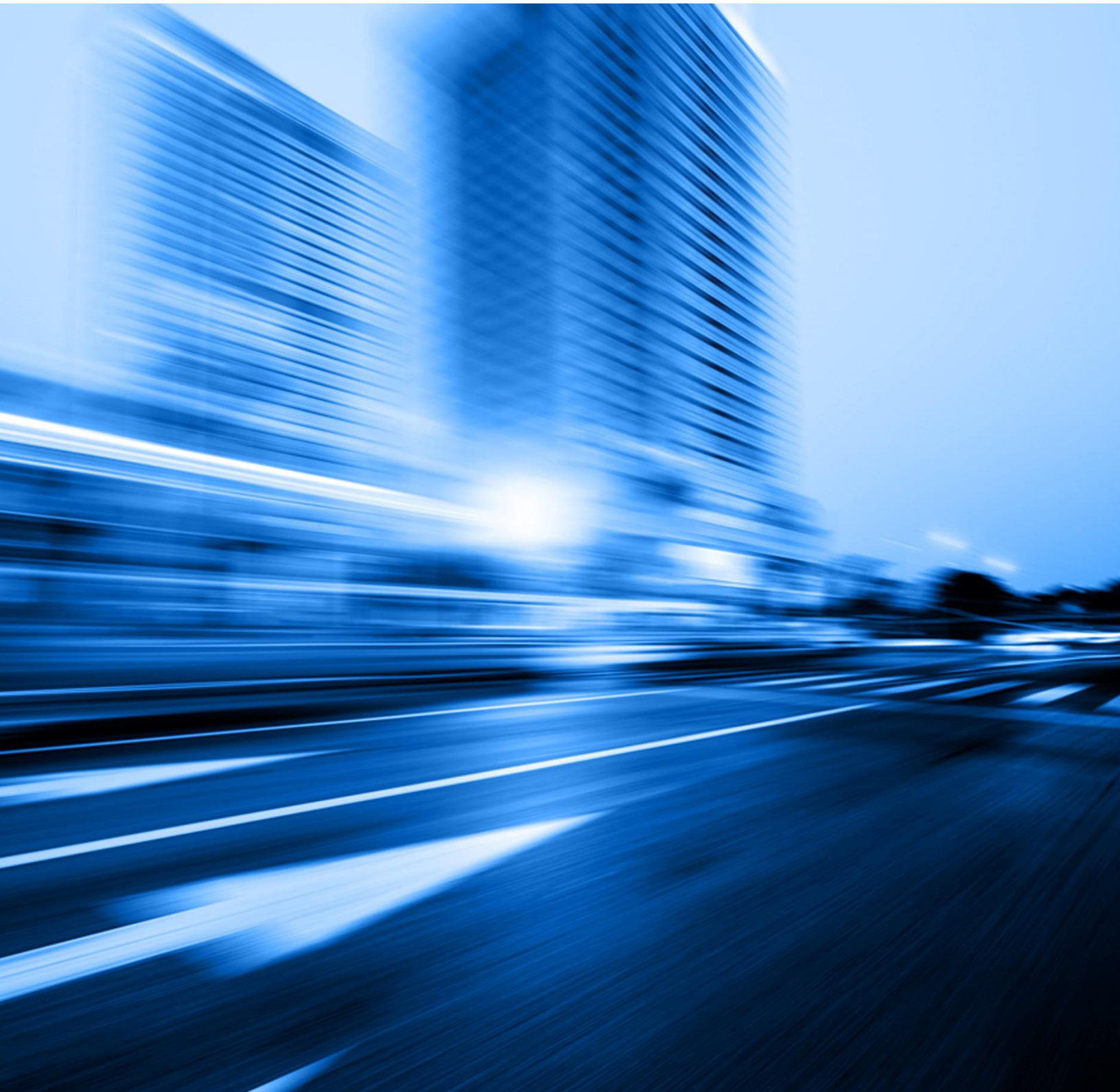
Adaptiva Endpoint Health: Health Checks List



Introduction

For Enterprise IT organizations who are dissatisfied with the time and effort it takes to keep endpoints secure and up-to-date, Adaptiva offers Endpoint Health.

Endpoint Health is a health and security engine that automatically identifies & repairs endpoint issues instantly. It is the fastest and most automated way to keep your endpoints secure and up-to-date.

Unlike competitive alternatives that simply provide visibility into security issues, Endpoint Health proactively monitors the health of endpoints, troubleshoots issues, and then automatically resolves them without the need for manual efforts.

Endpoint Health comes pre-packaged with dozens of health checks as well as a WorkFlow Designer tool that companies can use to visually create their own custom health checks without writing a single line of code. This document provides a list and brief description of over 100 health checks that are included in Endpoint Health.

Health Check	Remediates?	Description	Impact
ConfigMgr Client Configuration Checks		Ensure that Microsoft ConfigMgr client endpoints are configured correctly	
ConfigMgr Client -Cache Available Space	Yes	Checks and Remediates: The specified amount of space is available in the client cache	The ConfigMgr client can only hold a finite amount of data and the cache size is set to a fixed MB limit. When the cache gets full and/or there isn't enough room to download a piece of content to it, then the installation will fail. This check ensures that the cache has a required amount of space, which is useful to ensure that there's always room for a large deployment.
ConfigMgr Client -Cache Location	Yes	Checks and Remediates: The client cache location is correctly set	Allows for standardization of ConfigMgr cache location and prevents the end-user from changing it.
ConfigMgr Client - Orphaned Cache Folders	Yes	Checks whether there are any folders in the ccmcache that the ConfigMgr client is not aware of.	Orphaned cache folders become unmanaged by the ConfigMgr client so do not get cleaned up or utilized when needed for installation. This causes duplication of content and wasted disk space.

Health Check	Remediates?	Description	Impact
ConfigMgr Client –Site Assignment	Yes	Checks and Remediates: The client is assigned to the specified site	In multi–site hierarchies, when clients move around, are shipped or relocate to a different office, or are installed incorrectly, they can point to an incorrect site. This would result management by the wrong server not appropriate to their location. This check ensures clients are always pointing to their correct, local site.
ConfigMgr Client –Site Auto Discovery	No	Verifies: Site auto discovery is working on the client	If the client is unable to automatically discover a site, this may indicate other issues such as boundary configuration or a local client problem. This check allows for administrators to identify these systems and problems before the effects are reported by the end user.
ConfigMgr Client – Download Provider	No	Checks whether the specified Alternate ContentProvider is registered as the download provider.	Incorrect or missing download provider information can lead to content coming from an undesired source.
ConfigMgr Client Health Checks		Check and resolve issues related to the Microsoft ConfigMgr client	
ConfigMgr Client –Cache Size	Yes	Checks and Remediates: The client cache size is set to desired value, or more	By default, the ConfigMgr client cache size is set to 5120MB. If content that is larger than this needs to be downloaded, there will not be enough room in the cache and the download job will fail. This health check allows for a desired size to be set. Then, if the cache size is not large enough, it will get corrected.
ConfigMgr Client –CCM Folders	Yes	Checks and Remediates: There is no file named CCM in the Windows system32 folder, and there is no file named CCMSETUP in the Windows system32 folder	This can be used by administrators to tidy up legacy or incorrectly placed ConfigMgr installation and setup folders. These folders can be confusing and can result in misinformation if, for example, they still contain configuration data or log files from a previous installation.

Health Check	Remediates?	Description	Impact
ConfigMgr Client –Duplicate GUID	No	Verifies: The client does not have a duplicate SMS GUID	If a machine shares a ConfigMgr GUID with another device, any and all deployments targeted at one will also target the other. It would also be impossible to directly target one device. This can cause a number of issues.
ConfigMgr Client – Management Point Location	No	Verifies: The client can correctly determine the location of the management point	If the client cannot determine its MP location, then it could indicate a boundary issue or a client problem. Admins could proactively identify and resolve these issues before the end user experiences any content issues as a result.
ConfigMgr Client – Provisioning Mode	Yes	Checks and Remediates: Cases where the Task Sequence Manager leaves software distribution disabled even after it has exited	If a machine is left in provisioning mode by mistake, then it will be unable to download software as the client will believe it's still running a task sequence.
ConfigMgr Client –Service Running	Yes	Checks and Remediates: The SCCM client agent service is running, and its start mode is set to automatic	If the ConfigMgr client agent service (ccmexec/SMS Agent Host) is not running, then the entire ConfigMgr capabilities are unavailable for that device: software deployment, Windows Updates (if managed by ConfigMgr), Operating System Deployment, etc.
ConfigMgr Client –Version	Yes	Checks and Remediates: The specified version or later of SCCM agent is installed	If the ConfigMgr client has not been auto–upgraded to the latest version, or is running a lower/incorrect version, that could either indicate a problem with the client or that the client may just not have upgraded yet. New features available in newer client versions would not be available until this happens.
ConfigMgr Client Installation Checks		Detect and resolve Microsoft ConfigMgr setup and installation issues	

Health Check	Remediates?	Description	Impact
CCMSetup –DiscoveryStatus MOF	Yes	Checks and Remediates: If the event logs contain entries indicating CCMSetup failed due to a DiscoveryStatus MOF compile issue; compiles the MOF automatically if so	This error would indicate a problem preventing the installation of the ConfigMgr client.
CCMSetup – StatusAgentProxy DLL	No	Detects if the event logs contain entries indicating CCMSetup failed due to a StatusAgentProxy DLL issue	This error would indicate a problem preventing the installation of the ConfigMgr client.
CCMSetup –Visual C++DLL	Yes	Checks and Remediates: If the size of the Visual C++DLL is incorrect, the correct DLL is copied from the specified path	This error would indicate a problem preventing the installation of the ConfigMgr client.
ConfigMgr Client –Installed	Yes	Checks and Remediates: The SCCM client agent is installed	Without the ConfigMgr client agent installed, the entire ConfigMgr capabilities are unavailable for that device: software deployment, Windows Updates (if managed by ConfigMgr), Operating System Deployment, etc.
ConfigMgr Client Status Checks		Detect and resolve Microsoft ConfigMgr client communication, reporting and download issues	
ConfigMgr Client Status – Hardware Inventory	Yes	Checks and Remediates: whether hardware inventory is working	Hardware inventory provides important inventory data used for system identification, asset knowledge and targeting, installed software data and dynamic query–based collection population. Without accurate data systems may get incorrectly targeted, and important knowledge about systems may be inaccurate or missing.
ConfigMgr Client Status – Heartbeat Discovery	Yes	Checks and Remediates: whether heartbeat discovery is working	Systems send heartbeat discovery data to inform the site that the client is healthy. If the system is healthy, but unable to send heartbeat data, it may be incorrectly assumed to be unhealthy, marked as inactive, or removed from ConfigMgr entirely.

Health Check	Remediates?	Description	Impact
ConfigMgr Client Status – ManagementPoint Ping	No	Checks and Remediates: The management point location can be detected, and management point can be pinged using ICMP echo	If the client cannot determine its MP location then it could indicate a boundary issue or a client problem. Admins could proactively identify and resolve these issues before the end user experiences any content issues as a result.
ConfigMgr Client Status – Package Ping	Yes	Checks and Remediates: whether package download is working or not	If packages cannot be downloaded, then end-users will not able to install software. Also, systems administrators will not be able to patch machines or deploy applications. The end-user experience would be severely compromised.
ConfigMgr Client Status – Policy Retrieval	Yes	Checks and Remediates: a recently updated policy can be downloaded successfully by the client	ConfigMgr works using policies, which control many things, including client settings, software, compliance, and Windows Update installation. If machines are unable to download and apply policies, then this will severely impact on the systems' management and on the end-user.
ConfigMgr Client Status – Software Distribution	Yes	Checks and Remediates: whether software distribution is working or not	If software distribution is not working, then end-users will not be able to install software. Systems administrators will not be able to patch machines or deploy applications. The end-user experience would be severely compromised.
ConfigMgr Client Status – Software Inventory	Yes	Checks and Remediates: whether software inventory is working or not	Software inventory can be used by administrators to report on devices that contain certain files. Without this information machines may be mistargeted, or intelligence information may be inaccurate.

Health Check	Remediates?	Description	Impact
ConfigMgr Client Status – Status Message Submission	Yes	Checks and Remediates: whether status messages are being reported	Status messages are used for reporting to determine things such as download and installation state and various other factors. Without this, the information shown in reports and queries would be inaccurate.
DCOM Checks		Ensure networked computers are enabled for remote connection	
DCOM –Remote Connection Enabled	Yes	Checks and Remediates: Whether remote connection is enabled or not	Allows system administrators to ensure that DCOM Rermote Connectivity is available on all desired devices.
Instant Inventory Checks		Return instant inventory details from clients for reporting purposes	
Instant Inventory –Disk Space	No	Returns any machines that have below the specified amount of available disk space	Shows within seconds any device in the target collection or group that has under a specified amount of disk space. Useful for cleanup exercises, reporting or replacement PC targeting.
Instant Inventory –File Contains Text	No	Returns any machines that have the specified text in a specified file	Useful for searching text–based files such as log files, ini files, configuration files, etc., for a specific string of text. This can be used for intelligence purposes, finding machines with a specific config, or for troubleshooting— finding devices with a specific/partial error string.
Instant Inventory –File Exists	No	Returns any machines that have a specified file	Will return within seconds any devices with a specific file. Could be used for finding infected machines, or just devices that have an installed app, etc.
Instant Inventory –Folder Exists	No	Returns any machines that have a specified folder	Will return within seconds any devices with a specific folder. Useful for system identification purposes.

Health Check	Remediates?	Description	Impact
Instant Inventory –Process Running	No	Returns any machines that have a specified process running	Could be useful for identifying infected machines, machines running a certain prohibited application, finding devices that are using licenses from a pooled license application, etc.
Instant Inventory –Service Started	No	Returns any machines that have a specified service that is in the started state	Can be used for finding systems that have a service running that should not be running.
Instant Inventory –Service Stopped	No	Returns any machines that have a specified service that is in the stopped state	Can be used for finding systems that should have a service running but do not.
IP Address Scope Checks		Ensure client endpoints have a valid IP address	
IP –Permitted Scope	No	Verifies: Client's IP address is within the specified permitted IP address scopes	Could be used by network teams to identify machines that are active within a certain IP address range and to take action —if they should or should not be in there.
IP –Prohibited Scope	No	Verifies: Client's IP address is not within the specified prohibited IP address scopes	Could be used by network teams to identify machines that are active within a certain IP address range and to take action —if they should or should not be in there.
Network		Ensure clients have properly configured network and communication settings	
Network –DNS Settings	Yes	Checks and Remediates: If the Primary DNS suffix, Sync Domain with Membership, the Primary DNS Domain, the NIC DNS Domain and Enable Dynamic DNS Registration settings are set correctly; sets to the desired state if incorrect	En masse, real–time configuration of DNS settings. Ensures that machines are correctly registered with the DNS server and that they can communicate out and be communicated with.
Network –Hosts file entries present	Yes	Checks and Remediates: If the hosts file contains the specified entries; if any specified hosts entry is not present, it is appended	Hosts file entries are useful for endpoints that need to communicate with other devices that are not present on their local DNS server.

Health Check	Remediates?	Description	Impact
Network – DNS Name Resolution	Yes	Checks whether the local hostname resolves to the correct IP address in DNS.	Outdated or incorrect name resolution can cause to numerous application issues that rely on accurate name resolution.
Operating System Health Checks		Ensure endpoint user operating systems are configured correctly	
(Lanman) Server –Service Running	Yes	Checks and Remediates: The lanmanserver service is running, and its start mode is set to automatic	The Server/LANMANServer service is responsible for numerous file and communication purposes on the client. Without this service running, file shares, remote access to certain resources, and other services will be unavailable. This health check ensures that it is running, and the service start mode is set properly.
OS –Admin Share Available	Yes	Checks and Remediates: 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.
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.
Remote Registry Service Running (OS Specific)	Yes	Checks and Remediates: The Remote Registry 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.
OS –Clear windows print queues	No (Action)	Clears the Windows printer queues	Performs an action to clear the print queues, useful for resolving many printer–related issues or stopping a bad print–job.

Health Check	Remediates?	Description	Impact
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.
OS –Delete Temp Folder Contents	No (Action)	Deletes all content from Temp folders	Allows for reclamation of disk space, removing potentially harmful files, and general housekeeping.
OS –File Associations	Yes	Checks and Remediates: 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 –Remote Desktop Settings	Yes	Checks and Remediates: Remote Desktop, Remote Assistance and Secure connection (Network Level Authentication) and sets if any are incorrect	Allows for central managementof device RDP settings. This allows for administrators to be able to remotely connect to and manage devices.
OS –Run Key Entries	Yes	Checks and Remediates: 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 can be present in the run key, which protects systems from harmful software execution.
OS –Screen Saver Settings	Yes	Checks and Remediates: 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 managementof screensaver settings. Could be used by organizations to enforce a corporate–branded screensaver.
OS –Security Group presence	Yes	Checks and Remediates: 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.

Health Check	Remediates?	Description	Impact
OS –Windows Explorer Settings	Yes	Checks and Remediates: The following –Show Hidden Files, Show Protected System Files, Hide File Extensions for Known File Types, CompressedFiles 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 –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.
PowerShell Health Checks		Ensure desired PowerShell scripting and remote management settings are configured correctly	
PowerShell –WinRM	Yes	Checks and Remediates: That WinRM is enabled or disabled on the machine. If in an incorrect state, changes it accordingly	WinRM is Windows Remote Management and allows for PowerShell to perform various commands on remote systems. This allows administrators to ensure that WinRM is either enabled or disabled.
PowerShell –Set PowerShell Execution Policy	Yes	Checks and Remediates: The PowerShell execution policy. Choose between Restricted, All Signed, Remote Signed, Unrestricted, Bypass or Undefined Sets to the desired state if incorrect	This controls the PowerShell script execution policy to determine whether scripts can be run and, if they can, whether they need to be digitally signed.
Security Health Checks		Ensures client endpoint user access is configured correctly	

Health Check	Remediates?	Description	Impact
Security –User Access Control (UAC) Enabled	Yes	Checks and Remediates: If UAC is enabled; performed only on Windows 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.
Security –BitLocker Drive Encryption	Yes	Checks and Remediates: If BitLocker drive encryption is enabled for either the OS Drive, All Drives or a Specific drive; enables if it is not already enabled (encrypts)	BitLocker ensures that content on a disk cannot be accessed if the device is lost, stolen, or simply powered off and the drive inserted into another device. This check will ensure that drive encryption is turned on and will perform the encryption if not.
Security – Bad Rabbit Immunisation	Yes	Checks for signs of infection and performs immunization against future attack.	Bad Rabbit ransomware can cause irrevocable damage to systems, immunizing against attack prevents data loss and downtime.
Security – WannaCry Infection Detection Health Check	No	Checks for systems that have already been infected by WannaCry by searching all hard disk drives for files with the extension ".WNCRY", conducting a comprehensive evaluation of Indicators of Compromise (IOC) for this exploit.	The WannaCry ransomware can cause irrevocable damage to systems, fast and efficient detection and prevention of the spread of the outbreak prevents data loss and downtime.

Health Check	Remediates?	Description	Impact
Security – WannaCry Vulnerability Assessment Health Check	Yes	Checks for systems that are vulnerable to the WannaCry attack evaluating whether the correct patches and system updates have been applied to the system. If a machine contains none of the specified patches, it is vulnerable to attack by WannaCry.	The WannaCry ransomware can cause irrevocable damage to systems, fast and efficient detection and prevention of the spread of the outbreak prevents data loss and downtime.
System –Secure Boot	No	Detects whether Secure boot is enabled or disabled	Secure boot prevents the machine booting into an unauthorized boot environment, this check can be used to report on devices that have this setting enabled or disabled.
Software Health Checks		Performs various checks relating to software issues	
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	Checks and Remediates: 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.
System Performance Health Checks		Maintain system performance for end users	
System –Free Disk Space	No	Verifies: The % free space on disk drives	This check allows admins to report on devices that fall under a certain percentage of free disk space. They could then use this information to target hardware replacements, disk cleanup, or other remediation.

Health Check	Remediates?	Description	Impact
System –Defrag drive	No (Action)	Runs the disk defragmentation tool to reorganize and optimize the disk	Disk defragmentation is useful for spindle disks as it is used to move data together on the disk so that less movement of the read head is required. This improves disk read/write speeds and improves system performance.
System –Run Check Disk	No (Action)	Schedules a ChkDsk to run on the next reboot	ChkDsk verifies the integrity of the disk. It will look for any bad sectors and attempt repair. This health check allows for administrators to schedule this action on next reboot to proactively check the disk or to repair a reported unhealthy disk.
System –Run Disk Cleanup	No (Action)	Runs the disk cleanup utility to remove unneeded files and reclaim lost disk space	Disk cleanup utility will remove things such as temporary Internet files, temporary Windows files, unused applications and system utilities, etc.. It can be used to reclaim disk space if the system is getting low on space.
System –Trigger System Restore	No (Action)	Triggers a System Restore task so systems can be restored to a specific point in time	Allows for remote system restore point creation, allowing administrators to trigger a restore point on demand.
System – Disk Cleanup	Yes	Checks whether systems have under a certain percentage of free disk space.	Machines running out of space is a concern to lots of IT administrators and they need a way of reclaiming space without compromising any data that the user may be storing in unknown locations.
System – Reboot Required	No	Checks whether a reboot is required for up to four primary reboot reasons (Windows Update Installation, Windows Component Installation, File Rename Operations, SCCM Reboot Pending)	A pending reboot can cause application issues and can prevent the installation of security updates that are waiting on the previous installation and subsequent reboot.
System – Up Time	No	Checks whether the system has been online for longer than the specified number of days	Systems that have been online without a reboot for long periods of time are more likely to suffer from health issues resulting from previous installation, configuration or general file system/registry changes.

Health Check	Remediates?	Description	Impact
Windows Update Agent Health Checks		Ensure the successful distribution of updates and hotfixes released for Microsoft products	
WUA –Service Missing	Yes	Checks and Remediates: Whether WSUS service is present on the machine or not	If the Windows Update Agent service is not present or not running, then it would not be possible to patch the machine with Windows Updates either through WSUS or through ConfigMgr. This can compromise machine security, compliance and application functionality.
WUA –Service Running	Yes	Checks and Remediates: The wuauserv service is running, and its start mode is set to desired type	If the Windows Update Agent service is not present or not running, then it would not be possible to patch the machine with Windows Updates either through WSUS or through ConfigMgr. This could compromise machine security, compliance and application functionality.
WUA –Version	Yes	Checks and Remediates: The WSUS client version is current	Improvements, bug fixes, and the ability to patch certain software can only be attained using later versions of the update agent. This check will ensure that the version installed on devices is current and up–to–date.
Windows Update – Auto Update GPO	No	Checks whether the group policy settings for Windows Update configuration are set correctly.	Devices with incorrect or missing group policy configuration may not know for example, which server to contact for updates or they may be contacting an incorrect (legacy, retired, wrong region) server.
Windows Update – Last Scan Cycle	Yes	Checks when the machine last run the software update scan cycle.	The scan cycle pulls down and compares the latest WSUS catalogue with the installed updates on the system. If the scan hasn't run recently, the clients would not be aware of any new applicable updates.

Health Check	Remediates?	Description	Impact
Windows Update – Metadata Version	Yes	Checks whether the software update metadata version on the client matches the current metadata version on the server	If the metadata version is out of date, then the client would not be aware of any new updates in later catalogue versions which would affect their overall compliance
Windows Update – Non–Compliant Assignments	No	Checks whether there are any ConfigMgr software update deployments that contain updates in a non–compliant state	If any updates that are part of a ConfigMgr software update assignment are not installed, then the system would be non–compliant for those updates.
Windows Update – Software Update Scan Errors	No	Checks whether any errors have been reported by the Software update scan agent and reports back up to the last 10 errors	Errors during the software update scan would mean that the system would be unable to determine the current health state for it's updates and would not be able to apply any new ones
WMI Health Checks		Detects and resolves client endpoint WMI issues	
WMI –ConfigMgr Client Namespaces	Yes	Checks and Remediates: Connectivity to WMI namespaces used by the SCCM client	ConfigMgr relies heavily on the Windows Management Instrumentation to function. This check ensures that the namespaces that ConfigMgr relies upon are present and can be connected to.
WMI –ExecMgr Connection Error	Yes	Checks and Remediates: Detects whether the SCCM client's execmgr log contains WMI connection errors	If the log contains connection errors, then that would indicate a potential WMI corruption, this check will automatically detect and remediate this issue.
WMI –In Path	Yes	Checks and Remediates: The system32\wbem folder is included in the path variable in the environment	If this folder is not included in the path, then calls to WMI that do not reference the full path will fail. This could cause applications and PowerShell scripts to fail, and create difficulty executing WMI from a command line.

Health Check	Remediates?	Description	Impact
WMI –Repository Integrity	Yes	Checks and Remediates: The integrity of the wmi repository	WMI is a fundamental component of Windows and is used to store and retrieve information about all aspects of the operating system. If WMI is broken, the service is not running, or the repository is corrupt then it can affect numerous system processes, including ConfigMgr.
WMI –Service Running	Yes	Checks and Remediates: The WinMgmt service is running, and its start mode is set to desired type	WMI is a fundamental component of Windows and is used to store and retrieve information about all aspects of the operating system. If WMI is broken, the service is not running, or the repository is corrupt then it can affect numerous system processes, including ConfigMgr.
WMI –Windows Server Updates Installed	Yes	Checks and Remediates: Proper hotfix installed on relevant Windows Server systems	This important hotfix is critical to WMI operability on Windows Server systems. This check ensures that the update is applied.
BITS Health Checks		Ensure file transfers are happening as expected	
BITS –Service Running	Yes	Checks and Remediates: The BITS service is running, and its start mode is set to desired type	BITS is used by ConfigMgr and other applications for data transfer.
BITS –Service Startup Failing	Yes	Checks and Remediates: Detects whether BITS startup is failing (it might be possible that BITS has become corrupted)	If BITS fails to start then corruption may have occurred and would need to be repaired.
BITS –Version	Yes	Checks and Remediates: Ensure SCCM Clients have a recent version of BITS	Improvements have been made to later versions of BITS.
Adaptiva Health Checks		Ensure you have the correct Adaptiva OneSite version running on all endpoints	

Health Check	Remediates?	Description	Impact
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.
Group Policy – Processing Errors		Ensure Group Policies are processed with no errors	
Group Policy – Processing Errors	No	Checks for any errors when attempting to process Group Policy	Group Policy is responsible for enforcing configuration and security settings on devices. If there are processing errors, then some important settings may be missing or incorrect
Windows 10 Health Checks			
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.
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.

Health Check	Remediates?	Description	Impact
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–bitversion of the OS, as 64–bitvirtualization is required for Device Guard/Credential Guard.
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 Check	Remediates?	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.
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.

Health Check	Remediates?	Description	Impact
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.

Contact Us

Request a Endpoint Health demo from Adaptiva to learn how your organization can start creating their own endpoint security health checks today.

Visit www.adaptiva.com/endpoint-health to learn more.

4010 Lake Washington Blvd
Suite 200
Kirkland,WA 98033

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

@adaptiva
/adaptiva
/company/adaptiva