Endpoint Security

Attack surface reduction

MDE-AppGuard-Active

Name	Value
Basics	
Name	MDE-AppGuard-Active
Description	
Platform supported	Windows 10 and later
Category	Attack surface reduction
Policy type	App and browser isolation
Scope tags	Default

Table 1. Basics - MDE-AppGuard-Active

Name	Value	Recommended
App and browser isolation		
Turn on Application Guard	Enabled for Edge	notConfigured
Clipboard behavior (Microsoft Edge only)	Block copy and paste between PC and browser	notConfigured
Allow camera and microphone access (Microsoft Edge only)	Not configured	
Block external content from non-enterprise approved sites (Microsoft Edge only)	Not configured	False
Collect logs for events that occur within an Application Guard session	Yes	False
Allow user-generated browser data to be saved (Microsoft Edge only)	Not configured	False
Enable hardware graphics acceleration (Microsoft Edge only)	Not configured	False

Allow users to download files onto the host (Microsoft Edge only)	Not configured	False
Application Guard allow use of Root Certificate Authorities from the user's device	Not configured	
Application Guard allow print to local printers	Not configured	False
Application Guard allow print to network printers	Not configured	False
Application Guard allow print to PDF	Not configured	False
Application Guard allow print to XPS	Not configured	False
Windows network isolation policy	Not configured	@{enterpriseNetworkDomainNames=System.Object[]; enterpriseInternalProxyServers=System.Object[]; enterpriseIPRangesAreAuthoritative=False; enterpriseProxyServers=System.Object[]; enterpriseProxyServersAreAuthoritative=False; neutralDomainResources=System.Object[]; enterpriseCloudResources=System.Object[]; enterpriseIPRanges=System.Object[]}

Table 2. Settings - MDE-AppGuard-Active

Group	Filter	Filter mode
Included Groups		
Autopilot-Devices	None	None

Table 3. Assignments - MDE-AppGuard-Active

MDE-Web Protection-Active

Name	Value
Basics	
Name	MDE-Web Protection-Active
Description	
Platform supported	Windows 10 and later
Category	Attack surface reduction
Policy type	Web protection (Microsoft Edge Legacy)
Scope tags	Default

Table 4. Basics - MDE-Web Protection-Active

Name	Value	Recommended
Web Protection (Microsoft Edge Legacy)		
Enable network protection	Enable	notConfigured

Require SmartScreen for Microsoft Edge Legacy	Yes	False
Block malicious site access	Yes	False
Block unverified file download	Yes	False

Table 5. Settings - MDE-Web Protection-Active

Group	Filter	Filter mode
Included Groups		
Autopilot-Devices	None	None

Table 6. Assignments - MDE-Web Protection-Active

Disk encryption

Bitlocker Policy

Name	Value
Basics	
Name	Bitlocker Policy
Description	
Platform supported	Windows 10 and later
Category	Disk encryption
Policy type	BitLocker
Scope tags	Default

Table 7. Basics - Bitlocker Policy

Name	Value	Recommended
BitLocker - Base Settings		
Enable Full disk or Used Space only encryption for OS and fixed data drives	Yes	False
Require storage cards to be encrypted (mobile only)	Yes	False
Hide prompt about third-party encryption	Yes	False
Allow standard users to enable encryption during Autopilot	Yes	False
Configure client-driven recovery password rotation	Enable rotation on Azure AD-joined devices	notConfigured
BitLocker - Fixed Drive Settings		
BitLocker fixed drive policy	Configure	@{encryptionMethod=; requireEncryptionForWriteAccess=False; recoveryOptions=}

Fixed drive recovery	Configure	
Recovery key file creation	Blocked	
Configure BitLocker recovery package	Password only	
Require device to back up recovery information to Azure AD	Yes	
Recovery password creation	Required	
Hide recovery options during BitLocker setup	Yes	
Enable BitLocker after recovery information to store	Yes	
Block the use of certificate-based data recovery agent (DRA)	Not configured	
Block write access to fixed data-drives not protected by BitLocker	Yes	
Configure encryption method for fixed data-drives	AES 256bit XTS	
BitLocker - OS Drive Settings		
BitLocker system drive policy	Configure	@{encryptionMethod=; startupAuthenticationRequired=False; startupAuthenticationTpmUsage=; startupAuthenticationTpmKeyUsage=; startupAuthenticationTpmPinUsage=; startupAuthenticationTpmPinAndKeyUsage=; startupAuthenticationBlockWithoutTpmChip=False; minimumPinLength=; recoveryOptions=; prebootRecoveryEnableMessageAndUrl=False; prebootRecoveryMessage=; prebootRecoveryUrl=}
Startup authentication required	Not configured	
Configure encryption method for Operating System drives	AES 256bit XTS	
BitLocker - Removable Drive Settings		
BitLocker removable drive policy	Configure	@{encryptionMethod=; requireEncryptionForWriteAccess=False; blockCrossOrganizationWriteAccess=False}

Configure encryption method for removable data-drives	AES 256bit CBC	
Block write access to removable data-drives not protected by BitLocker	Yes	
Block write access to devices configured in another organization	Yes	

Table 8. Settings - Bitlocker Policy

Group	Filter	Filter mode
Included Groups		
Autopilot-Devices	None	None

Table 9. Assignments - Bitlocker Policy

Security baselines

Edge Baseline

Name	Value
Basics	
Name	Edge Baseline
Description	
Platform supported	Windows 10 and later
Category	Security baselines
Policy type	Microsoft Edge baseline
Scope tags	Default

Table 10. Basics - Edge Baseline

Name	Value	Recommended
Microsoft Edge		
Supported authentication schemes	Enabled	
Supported authentication schemes	NTLM Negotiate	
Default Adobe Flash setting	Enabled	
Default Adobe Flash setting	Block the Adobe Flash plugin	
Control which extensions cannot be installed	Enabled	
Extension IDs the user should be prevented from installing (or * for all)	*	*
Allow user-level native messaging hosts (installed without admin permissions)	Disabled	

Enable saving passwords to the password manager	Disabled	
Prevent bypassing Microsoft Defender SmartScreen prompts for sites	Enabled	
Prevent bypassing of Microsoft Defender SmartScreen warnings about downloads	Enabled	
Enable site isolation for every site	Enabled	
Configure Microsoft Defender SmartScreen	Enabled	
Configure Microsoft Defender SmartScreen to block potentially unwanted apps	Enabled	
Allow users to proceed from the SSL warning page	Disabled	
Minimum SSL version enabled	Enabled	
Minimum SSL version enabled	TLS 1.2	
Allow certificates signed using SHA-1 when issued by local trust anchors (deprecated)	Disabled	

Table 11. Settings - Edge Baseline

Group	Filter	Filter mode
Included Groups		
Autopilot-Devices	None	None

Table 12. Assignments - Edge Baseline

Security baselines

Windows 10 Security Baseline

Name	Value
Basics	
Name	Windows 10 Security Baseline
Description	
Platform supported	Windows 10 and later
Category	Security baselines
Policy type	MDM Security Baseline for Windows 10 and later for November 2021
Scope tags	Default

Table 13. Basics - Windows 10 Security Baseline

Name	Value	Recommended
Above Lock		
Voice activate apps from locked screen	Disabled	

Block display of toast notifications	Yes	
App Runtime		
Microsoft accounts optional for Windows Store apps	Enabled	
Application management		
Block app installations with elevated privileges	Yes	
Block user control over installations	Yes	
Block game DVR (desktop only)	Yes	
Audit		
Account Logon Audit Credential Validation (Device)	Success and Failure	
Account Logon Audit Kerberos Authentication Service (Device)	None	
Account Logon Logoff Audit Account Lockout (Device)	Failure	
Account Logon Logoff Audit Group Membership (Device)	Success	
Account Logon Logoff Audit Logon (Device)	Success and Failure	
Audit Other Logon Logoff Events (Device)	Success and Failure	
Audit Special Logon (Device)	Success	
Audit Security Group Management (Device)	Success	
Audit User Account Management (Device)	Success and Failure	
Detailed Tracking Audit PNP Activity (Device)	Success	
Detailed Tracking Audit Process Creation (Device)	Success	
Object Access Audit Detailed File Share (Device)	Failure	
Audit File Share Access (Device)	Success and Failure	
Object Access Audit Other Object Access Events (Device)	Success and Failure	

Object Access Audit Removable Storage (Device)	Success and Failure	
Audit Authentication Policy Change (Device)	Success	
Policy Change Audit MPSSVC Rule Level Policy Change (Device)	Success and Failure	
Policy Change Audit Other Policy Change Events (Device)	Failure	
Audit Changes to Audit Policy (Device)	Success	
Privilege Use Audit Sensitive Privilege Use (Device)	Success and Failure	
System Audit Other System Events (Device)	Success and Failure	
System Audit Security State Change (Device)	Success	
Audit Security System Extension (Device)	Success	
System Audit System Integrity (Device)	Success and Failure	
Auto Play		
Auto play default auto run behavior	Do not execute	
Auto play mode	Disabled	
Block auto play for non-volume devices	Enabled	
BitLocker		
BitLocker removable drive policy	Not configured	@{requireEncryptionForWriteAccess=True}
Browser		
Block Password Manager	Yes	
Require SmartScreen for Microsoft Edge Legacy	Yes	
Block malicious site access	Yes	
Block unverified file download	Yes	
Prevent user from overriding certificate errors	Yes	
Connectivity		
Configure secure access to UNC paths	Configure Windows to only allow access to the specified UNC paths	@{$implementationId=deviceConfiguration--hardenedUncPathEnabled; hardenedUncPaths=System.Object[]}

	after fulfilling additional security requirements	
Hardened UNC path list	Require mutual authentication;Require integrity;*\SYSVOL Require mutual authentication;Require integrity;*\NETLOGON	
Block downloading of print drivers over HTTP	Enabled	
Block Internet download for web publishing and online ordering wizards	Enabled	
Credentials Delegation		
Remote host delegation of non-exportable credentials	Enabled	
Credentials UI		
Enumerate administrators	Disabled	
Data Protection		
Block direct memory access	Enabled	
Device Guard		
Virtualization based security	Enable VBS with secure boot	
Enable virtualization based security	Yes	
Launch system guard	Enabled	
Turn on Credential Guard	Enable with UEFI lock	
Device Installation		
Block hardware device installation by setup classes	Yes	
Remove matching hardware devices	Yes	
Block list	{d48179be-ec20-11d1-b6b8-00c04fa372a7}	
Device Lock		
Require password	Yes	
Required password	Alphanumeric	
Password expiration (days)	60	
Password minimum character set count	3	
Prevent reuse of previous passwords	24	

Minimum password length	8	
Number of sign-in failures before wiping device	10	
Block simple passwords	Yes	
Password minimum age in days	1	
Prevent use of camera	Enabled	
Prevent slide show	Enabled	
DMA Guard		
Enumeration of external devices incompatible with Kernel DMA Protection	Block all	
Event Log Service		
Application log maximum file size in KB	32768	
System log maximum file size in KB	32768	
Security log maximum file size in KB	196608	
Experience		
Block Windows Spotlight	Not configured	True
File Explorer		
Block data execution prevention	Disabled	
Block heap termination on corruption	Disabled	
Firewall		
Firewall profile domain	Configure	
Inbound connections blocked	Yes	
Outbound connections required	Yes	
Inbound notifications blocked	Yes	
Firewall enabled	Allowed	
Firewall profile private	Configure	
Inbound connections blocked	Yes	
Outbound connections required	Yes	
Inbound notifications blocked	Yes	
Firewall enabled	Allowed	
Firewall profile public	Configure	

Inbound connections blocked	Yes	
Outbound connections required	Yes	
Inbound notifications blocked	Yes	
Firewall enabled	Allowed	
Connection security rules from group policy not merged	Yes	
Policy rules from group policy not merged	Yes	
Internet Explorer		
Internet Explorer encryption support	TLS v1.1 TLS v1.2	
Internet Explorer prevent managing smart screen filter	Enable	
Internet Explorer restricted zone script Active X controls marked safe for scripting	Disable	
Internet Explorer restricted zone file downloads	Disable	
Internet Explorer certificate address mismatch warning	Enabled	
Internet Explorer enhanced protected mode	Enabled	
Internet Explorer fallback to SSL3	No sites	
Internet Explorer software when signature is invalid	Disabled	
Internet Explorer check server certificate revocation	Enabled	
Internet Explorer check signatures on downloaded programs	Enabled	
Internet Explorer processes consistent MIME handling	Enabled	
Internet Explorer bypass smart screen warnings	Disabled	
Internet Explorer bypass smart screen	Disabled	

warnings about uncommon files		
Internet Explorer crash detection	Disabled	
Internet Explorer download enclosures	Disabled	
Internet Explorer ignore certificate errors	Disabled	
Internet Explorer disable processes in enhanced protected mode	Enabled	
Internet Explorer security settings check	Enabled	
Internet Explorer Active X controls in protected mode	Disabled	
Internet Explorer users adding sites	Disabled	
Internet Explorer users changing policies	Disabled	
Internet Explorer block outdated Active X controls	Enabled	
Internet Explorer include all network paths	Disabled	
Internet Explorer internet zone access to data sources	Disable	
Internet Explorer internet zone automatic prompt for file downloads	Disabled	
Internet Explorer internet zone copy and paste via script	Disable	
Internet Explorer internet zone drag and drop or copy and paste files	Disable	
Internet Explorer internet zone less privileged sites	Disable	
Internet Explorer internet zone loading of XAML files	Disable	
Internet Explorer internet zone .NET Framework reliant components	Disable	

Internet Explorer internet zone allow only approved domains to use ActiveX controls	Enabled	
Internet Explorer internet zone allow only approved domains to use tdc ActiveX controls	Enabled	
Internet Explorer internet zone scripting of web browser controls	Disabled	
Internet Explorer internet zone script initiated windows	Disabled	
Internet Explorer internet zone scriptlets	Disable	
Internet Explorer internet zone smart screen	Enabled	
Internet Explorer internet zone updates to status bar via script	Disabled	
Internet Explorer internet zone user data persistence	Disabled	
Internet Explorer internet zone allow VBscript to run	Disable	
Internet Explorer internet zone do not run antimalware against ActiveX controls	Disabled	
Internet Explorer internet zone download signed ActiveX controls	Disable	
Internet Explorer internet zone download unsigned ActiveX controls	Disable	
Internet Explorer internet zone cross site scripting filter	Enabled	
Internet Explorer internet zone drag content from different domains across windows	Disabled	
Internet Explorer internet zone drag	Disabled	

content from different domains within windows		
Internet Explorer internet zone protected mode	Enable	
Internet Explorer internet zone include local path when uploading files to server	Disabled	
Internet Explorer internet zone initialize and script Active X controls not marked as safe	Disable	
Internet Explorer internet zone java permissions	Disable java	
Internet Explorer internet zone launch applications and files in an iframe	Disable	
Internet Explorer internet zone logon options	Prompt	
Internet Explorer internet zone navigate windows and frames across different domains	Disable	
Internet Explorer internet zone run .NET Framework reliant components signed with Authenticode	Disable	
Internet Explorer internet zone security warning for potentially unsafe files	Prompt	
Internet Explorer internet zone popup blocker	Enable	
Internet Explorer intranet zone do not run antimalware against Active X controls	Disabled	
Internet Explorer intranet zone initialize and script Active X	Disable	

controls not marked as safe		
Internet Explorer intranet zone java permissions	High safety	
Internet Explorer local machine zone do not run antimalware against Active X controls	Disabled	
Internet Explorer local machine zone java permissions	Disable java	
Internet Explorer locked down internet zone smart screen	Enabled	
Internet Explorer locked down intranet zone java permissions	Disable java	
Internet Explorer locked down local machine zone java permissions	Disable java	
Internet Explorer locked down restricted zone smart screen	Enabled	
Internet Explorer locked down restricted zone java permissions	Disable java	
Internet Explorer locked down trusted zone java permissions	Disable java	
Internet Explorer processes MIME sniffing safety feature	Enabled	
Internet Explorer processes MK protocol security restriction	Enabled	
Internet Explorer processes notification bar	Enabled	
Internet Explorer prevent per user installation of Active X controls	Enabled	
Internet Explorer processes protection from zone elevation	Enabled	
Internet Explorer remove run this time button for outdated Active X controls	Enabled	

Internet Explorer processes restrict Active X install	Enabled	
Internet Explorer restricted zone access to data sources	Disable	
Internet Explorer restricted zone active scripting	Disable	
Internet Explorer restricted zone automatic prompt for file downloads	Disabled	
Internet Explorer restricted zone binary and script behaviors	Disable	
Internet Explorer restricted zone copy and paste via script	Disable	
Internet Explorer restricted zone drag and drop or copy and paste files	Disable	
Internet Explorer restricted zone less privileged sites	Disable	
Internet Explorer restricted zone loading of XAML files	Disable	
Internet Explorer restricted zone meta refresh	Disabled	
Internet Explorer restricted zone .NET Framework reliant components	Disable	
Internet Explorer restricted zone allow only approved domains to use Active X controls	Enabled	
Internet Explorer restricted zone allow only approved domains to use tdc Active X controls	Enabled	
Internet Explorer restricted zone scripting of web browser controls	Disabled	

Internet Explorer restricted zone script initiated windows	Disabled	
Internet Explorer restricted zone scriptlets	Disabled	
Internet Explorer restricted zone smart screen	Enabled	
Internet Explorer restricted zone updates to status bar via script	Disabled	
Internet Explorer restricted zone user data persistence	Disabled	
Internet Explorer restricted zone allow vbscript to run	Disable	
Internet Explorer restricted zone do not run antimalware against Active X controls	Disabled	
Internet Explorer restricted zone download signed Active X controls	Disable	
Internet Explorer restricted zone download unsigned Active X controls	Disable	
Internet Explorer restricted zone cross site scripting filter	Enabled	
Internet Explorer restricted zone drag content from different domains across windows	Disabled	
Internet Explorer restricted zone drag content from different domains within windows	Disabled	
Internet Explorer restricted zone include local path when uploading files to server	Disabled	
Internet Explorer restricted zone initialize and script Active X	Disable	

controls not marked as safe		
Internet Explorer restricted zone java permissions	Disable java	
Internet Explorer restricted zone launch applications and files in an iFrame	Disable	
Internet Explorer restricted zone logon options	Anonymous	
Internet Explorer restricted zone navigate windows and frames across different domains	Disable	
Internet Explorer restricted zone run Active X controls and plugins	Disable	
Internet Explorer restricted zone run .NET Framework reliant components signed with Authenticode	Disable	
Internet Explorer restricted zone scripting of java applets	Disable	
Internet Explorer restricted zone security warning for potentially unsafe files	Disable	
Internet Explorer restricted zone protected mode	Enable	
Internet Explorer restricted zone popup blocker	Enable	
Internet Explorer processes restrict file download	Enabled	
Internet Explorer processes scripted window security restrictions	Enabled	
Internet Explorer security zones use only machine settings	Enabled	

Internet Explorer use Active X installer service	Enabled	
Internet Explorer trusted zone do not run antimalware against Active X controls	Disabled	
Internet Explorer trusted zone initialize and script Active X controls not marked as safe	Disable	
Internet Explorer trusted zone java permissions	High safety	
Internet Explorer auto complete	Disabled	
Local Policies Security Options		
Block remote logon with blank password	Yes	
Minutes of lock screen inactivity until screen saver activates	15	
Smart card removal behavior	Lock workstation	
Require client to always digitally sign communications	Yes	
Prevent clients from sending unencrypted passwords to third party SMB servers	Yes	
Require server digitally signing communications always	Yes	
Prevent anonymous enumeration of SAM accounts	Yes	
Block anonymous enumeration of SAM accounts and shares	Yes	
Restrict anonymous access to named pipes and shares	Yes	
Allow remote calls to security accounts manager	O:BAG:BAD:(A;;RC;;;BA)	
Prevent storing LAN manager hash value on next password change	Yes	

Authentication level	Send NTLMv2 response only. Refuse LM and NTLM	
Minimum session security for NTLM SSP based clients	Require NTLM V2 and 128 bit encryption	
Minimum session security for NTLM SSP based servers	Require NTLM V2 and 128 bit encryption	
Administrator elevation prompt behavior	Prompt for consent on the secure desktop	
Standard user elevation prompt behavior	Automatically deny elevation requests	
Detect application installations and prompt for elevation	Yes	
Only allow UI access applications for secure locations	Yes	
Require admin approval mode for administrators	Yes	
Use admin approval mode	Yes	
Virtualize file and registry write failures to per user locations	Yes	
Microsoft Defender		
Block Adobe Reader from creating child processes	Not configured	enable
Block Office communication apps from creating child processes	Not configured	enable
Enter how often (0-24 hours) to check for security intelligence updates	4	
Scan type	Quick scan	
Defender schedule scan day	Everyday	
Scheduled scan start time	Not configured	
Cloud-delivered protection level	Not configured	
Scan network files	Not configured	True
Turn on real-time protection	Not configured	True

Scan scripts that are used in Microsoft browsers	Not configured	True
Scan archive files	Not configured	True
Turn on behavior monitoring	Not configured	True
Turn on cloud-delivered protection	Not configured	True
Scan incoming email messages	Not configured	True
Scan removable drives during full scan	Not configured	True
Block Office applications from injecting code into other processes	Not configured	block
Block Office applications from creating executable content	Not configured	block
Block all Office applications from creating child processes	Not configured	block
Block Win32 API calls from Office macro	Not configured	block
Block execution of potentially obfuscated scripts (js/vbs/ps)	Not configured	block
Block JavaScript or VBScript from launching downloaded executable content	Not configured	block
Block executable content download from email and webmail clients	Not configured	block
Block credential stealing from the Windows local security authority subsystem (lsass.exe)	Not configured	enable
Defender potentially unwanted app action	Block	
Block untrusted and unsigned processes that run from USB	Not configured	block
Enable network protection	Not configured	enable
Defender sample submission consent	Send safe samples automatically	
MS Security Guide		

SMB v1 client driver start configuration	Disable driver	
Apply UAC restrictions to local accounts on network logon	Enabled	
Structured exception handling overwrite protection	Enabled	
SMB v1 server	Disabled	
Digest authentication	Disabled	
MSS Legacy		
Network IPv6 source routing protection level	Highest protection	
Network IP source routing protection level	Highest protection	
Network ignore NetBIOS name release requests except from WINS servers	Enabled	
Network ICMP redirects override OSPF generated routes	Disabled	
Power		
Require password on wake while on battery	Enabled	
Require password on wake while plugged in	Enabled	
Standby states when sleeping while on battery	Disabled	
Standby states when sleeping while plugged in	Disabled	
Remote Assistance		
Remote Assistance solicited	Disable Remote Assistance	
Remote Desktop Services		
Remote desktop services client connection encryption level	High	
Block drive redirection	Enabled	
Block password saving	Enabled	
Prompt for password upon connection	Enabled	
Secure RPC communication	Enabled	
Remote Management		
Block client digest authentication	Enabled	

Block storing run as credentials	Enabled	
Client basic authentication	Disabled	
Basic authentication	Disabled	
Client unencrypted traffic	Disabled	
Unencrypted traffic	Disabled	
Remote Procedure Call		
RPC unauthenticated client options	Authenticated	
Search		
Disable indexing encrypted items	Yes	
Smart Screen		
Turn on Windows SmartScreen	Yes	
Block users from ignoring SmartScreen warnings	Yes	
System		
System boot start driver initialization	Good unknown and bad critical	
Wi-Fi		
Block Automatically connecting to Wi-Fi hotspots	Yes	
Block Internet sharing	Yes	
Windows Connection Manager		
Block connection to non-domain networks	Enabled	
Windows Ink Workspace		
Ink Workspace	Enabled	
Windows PowerShell		
PowerShell script block logging	Enabled	

Table 14. Settings - Windows 10 Security Baseline

Group	Filter	Filter mode
Included Groups		
Autopilot-Devices	None	None

Table 15. Assignments - Windows 10 Security Baseline

Device configuration

Settings Catalog

AdditionalSecurity

Name	Value
Basics	
Name	AdditionalSecurity
Description	Additional Security Policies to meet CIS guidelines
Profile type	Settings catalog
Platform supported	Windows 10 and later
Scope tags	Default

Table 16. Basics - AdditionalSecurity

Name	Value
Above Lock	
Allow Cortana Above Lock	Block
Administrative Templates	
MSS (Legacy)	
MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)	Disabled
MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds	Enabled
KeepAliveTime (Device)	300000 or 5 minutes (recommended)
MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)	Disabled
MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)	Enabled
MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)	Enabled
ScreenSaverGracePeriod (Device)	5
MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)	Enabled
TcpMaxDataRetransmissions (Device)	3
MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)	Enabled
TcpMaxDataRetransmissions (Device)	3
MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning	Enabled
WarningLevel (Device)	90%
Network Connections	
Prohibit installation and configuration of Network Bridge on your DNS domain network	Enabled
Require domain users to elevate when setting a network's location	Enabled
Turn off notifications when a connection has only limited or no connectivity (User)	Enabled
Windows Connect Now	

Configuration of wireless settings using Windows Connect Now	Disabled
Prohibit access of the Windows Connect Now wizards	Enabled
Windows Connection Manager	
Minimize the number of simultaneous connections to the Internet or a Windows Domain	Enabled
Minimize Policy Options (Device)	3 = Prevent Wi-Fi when on Ethernet
Printers	
Allow Print Spooler to accept client connections	Disabled
Point and Print Restrictions	Enabled
Enter fully qualified server names separated by semicolons (Device)	
Users can only point and print to machines in their forest (Device)	False
Users can only point and print to these servers: (Device)	False
When installing drivers for a new connection: (Device)	Show warning and elevation prompt
When updating drivers for an existing connection: (Device)	Show warning and elevation prompt
Audit Process Creation	
Include command line in process creation events	Enabled
Device Installation	
Prevent device metadata retrieval from the Internet	Enabled
Internet Communication settings	
Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com	Enabled
Turn off printing over HTTP	Enabled
Turn off Registration if URL connection is referring to Microsoft.com	Enabled
Turn off Search Companion content file updates	Enabled
Turn off the "Order Prints" picture task	Enabled
Turn off the "Publish to Web" task for files and folders	Enabled
Turn off the Windows Messenger Customer Experience Improvement Program	Enabled
Turn off Windows Customer Experience Improvement Program	Enabled
Turn off Windows Error Reporting	Enabled
Kerberos	
Support device authentication using certificate	Enabled
Device authentication behavior using certificate: (Device)	Automatic
System	

Prevent access to registry editing tools (User)	Enabled
Disable regedit from running silently? (User)	Yes
Prevent access to the command prompt (User)	Enabled
Disable the command prompt script processing also? (User)	No
App runtime	
Block launching Universal Windows apps with Windows Runtime API access from hosted content.	Disabled
Credential User Interface	
Do not display the password reveal button	Enabled
Application	
Control Event Log behavior when the log file reaches its maximum size	Disabled
Security	
Control Event Log behavior when the log file reaches its maximum size	Disabled
Setup	
Control Event Log behavior when the log file reaches its maximum size	Disabled
System	
Control Event Log behavior when the log file reaches its maximum size	Disabled
Device and Resource Redirection	
Do not allow COM port redirection	Enabled
Do not allow LPT port redirection	Enabled
Do not allow supported Plug and Play device redirection	Enabled
Auditing	
Audit Authorization Policy Change	Success
System Audit I Psec Driver	Success+ Failure
Authentication	
Enable Fast First Sign In	Disabled. Do not auto-connect new non-admin Azure AD accounts to pre-configured local accounts
Experience	
Allow Cortana	Block
Allow Device Discovery	Block
Allow Manual MDM Unenrollment	Block
Do Not Show Feedback Notifications	Feedback notifications are disabled.
Local Policies Security Options	
Accounts Enable Guest Account Status	Disable
Accounts Rename Guest Account	Visitors
Devices Allowed To Format And Eject Removable Media	0
Devices Prevent Users From Installing Printer Drivers When Connecting To Shared Printers	Disable
Interactive Logon Do Not Display Last Signed In	Enabled (username will not be shown)
Interactive Logon Do Not Require CTRLALTDEL	Disabled

Microsoft App Store	
Allow Developer Unlock	Explicit deny.
Allow Game DVR	Block
Microsoft Edge	
Allow users to proceed from the HTTPS warning page	Disabled
Block third party cookies	Enabled
Hide the First-run experience and splash screen	Enabled
Security	
Allow Add Provisioning Package	Block
Allow Remove Provisioning Package	Block
System Services	
Configure Xbox Accessory Management Service Startup Mode	Disabled
Configure Xbox Live Auth Manager Service Startup Mode	Disabled
Configure Xbox Live Game Save Service Startup Mode	Disabled
Configure Xbox Live Networking Service Startup Mode	Disabled
Windows Logon	
Enable First Logon Animation	Enabled
Wireless Display	
Require Pin For Pairing	All pairings will require PIN

Table 17. Settings - AdditionalSecurity

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 18. Assignments - AdditionalSecurity

Browser Homepage

Name	Value
Basics	
Name	Browser Homepage
Description	Browser settings
Profile type	Settings catalog
Platform supported	Windows 10 and later
Scope tags	Default

Table 19. Basics - Browser Homepage

Name	Value
Browser	
Configure Home Button	Show home button and load the Start page
Home Pages	https://deployintune.com
Set Home Button URL	https://deployintune.com

Set New Tab Page URL	https://deployintune.com
Microsoft Edge	
Startup, home page and new tab page	
Action to take on startup	Enabled
Action to take on startup (Device)	Open a new tab
Configure the home page URL	Enabled
Home page URL (Device)	https://deployintune.com
Configure the Microsoft Edge new tab page experience	Enabled
New tab page experience (Device)	Microsoft News feed experience
Configure the new tab page URL	Enabled
New tab page URL (Device)	https://deployintune.com
Set the new tab page as the home page	Enabled
Show Home button on toolbar	Enabled
Sites to open when the browser starts	Enabled
Sites to open when the browser starts (Device)	https://deployintune.com

Table 20. Settings - Browser Homepage

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 21. Assignments - Browser Homepage

LAPS Config

Name	Value
Basics	
Name	LAPS Config
Description	Uses lapsadmin created via custom OMA-URI policy
Profile type	Settings catalog
Category	Account protection
Policy type	Local admin password solution (Windows LAPS)
Platform supported	Windows 10 and later
Scope tags	Default

Table 22. Basics - LAPS Config

Name	Value
Backup Directory	Backup the password to Azure AD only
Password Age Days	30
Administrator Account Name	lapsadmin
Password Complexity	Large letters + small letters + numbers + special characters
Password Length	20
Post Authentication Actions	Reset password: upon expiry of the grace period, the managed account password will be reset.

Table 23. Settings - LAPS Config

Group	Filter	Filter mode
Included Groups		
All devices	None	None

Table 24. Assignments - LAPS Config

MDE-ASR Rules

Name	Value
Basics	
Name	MDE-ASR Rules
Description	Defender Attack Surface Reduction Rules
Profile type	Settings catalog
Category	Attack surface reduction
Policy type	Attack Surface Reduction Rules
Platform supported	Windows 10 and later
Scope tags	Default

Table 25. Basics - MDE-ASR Rules

Name	Value
Defender	
Attack Surface Reduction Rules	
Block Adobe Reader from creating child processes	Block
Block process creations originating from PSExec and WMI commands	Block
Block execution of potentially obfuscated scripts	Block
Block persistence through WMI event subscription	Block
Block Win32 API calls from Office macros	Block
Block Office applications from creating executable content	Block
Block credential stealing from the Windows local security authority subsystem	Block
Block executable files from running unless they meet a prevalence, age, or trusted list criterion	Block
Block JavaScript or VBScript from launching downloaded executable content	Block
Block Office communication application from creating child processes	Block
Block Office applications from injecting code into other processes	Block
Block all Office applications from creating child processes	Block
Block untrusted and unsigned processes that run from USB	Block
Use advanced protection against ransomware	Block

Block executable content from email client and webmail	Block
Block abuse of exploited vulnerable signed drivers (Device)	Block
Enable Controlled Folder Access	Audit Mode

Table 26. Settings - MDE-ASR Rules

Group	Filter	Filter mode
Included Groups		
Autopilot-Devices	None	None

Table 27. Assignments - MDE-ASR Rules

MDE-AV-Active

Name	Value
Basics	
Name	MDE-AV-Active
Description	Defender for Endpoint Settings
Profile type	Settings catalog
Category	Antivirus
Policy type	Microsoft Defender Antivirus
Platform supported	Windows 10 and later
Scope tags	Default

Table 28. Basics - MDE-AV-Active

Name	Value
Defender	
Allow Archive Scanning	Allowed. Scans the archive files.
Allow Behavior Monitoring	Allowed. Turns on real-time behavior monitoring.
Allow Cloud Protection	Allowed. Turns on Cloud Protection.
Allow Email Scanning	Allowed. Turns on email scanning.
Allow Full Scan On Mapped Network Drives	Allowed. Scans mapped network drives.
Allow Full Scan Removable Drive Scanning	Allowed. Scans removable drives.
[Deprecated] Allow Intrusion Prevention System	Allowed.
Allow scanning of all downloaded files and attachments	Allowed.
Allow Realtime Monitoring	Allowed. Turns on and runs the real-time monitoring service.
Allow Scanning Network Files	Allowed. Scans network files.
Allow Script Scanning	Allowed.
Allow User UI Access	Allowed. Lets users access UI.
Check For Signatures Before Running Scan	Enabled
Cloud Block Level	High Plus
Enable Network Protection	Enabled (block mode)
Real Time Scan Direction	Monitor all files (bi-directional).
Disable Local Admin Merge	Disable Local Admin Merge
Allow On Access Protection	Allowed.

Threat Severity Default Action	
Remediation action for Severe threats	Remove. Removes files from system.
Remediation action for Moderate severity threats	Quarantine. Moves files to quarantine.
Remediation action for Low severity threats	Clean. Service tries to recover files and try to disinfect.
Remediation action for High severity threats	Remove. Removes files from system.

Table 29. Settings - MDE-AV-Active

Group	Filter	Filter mode
Included Groups		
Autopilot-Devices	None	None

Table 30. Assignments - MDE-AV-Active

MDE-AV-Global Exclusions

Name	Value
Basics	
Name	MDE-AV-Global Exclusions
Description	Defender for Endpoint Exclusions list, add as appropriate
Profile type	Settings catalog
Category	Antivirus
Policy type	Microsoft Defender Antivirus exclusions
Platform supported	Windows 10 and later
Scope tags	Default

Table 31. Basics - MDE-AV-Global Exclusions

Name	Value
Defender	
Excluded Paths	C:\dontusethis\

Table 32. Settings - MDE-AV-Global Exclusions

Group	Filter	Filter mode
Included Groups		
Autopilot-Devices	None	None

Table 33. Assignments - MDE-AV-Global Exclusions

MDE-DeviceControl

Name	Value
Basics	
Name	MDE-DeviceControl
Description	Device Control Rules
Profile type	Settings catalog
Category	Attack surface reduction
Policy type	Device Control
Platform supported	Windows 10 and later
Scope tags	Default

Table 34. Basics - MDE-DeviceControl

Name	Value
Administrative Templates	
Device Installation Restrictions	
Apply layered order of evaluation for Allow and Prevent device installation policies across all device match criteria	Enabled
Bluetooth	
Allow Advertising	Block
Allow Prepairing	Block
Allow Prompted Proximal Connections	Block
Data Protection	
Allow Direct Memory Access	Block

Table 35. Settings - MDE-DeviceControl

Group	Filter	Filter mode
Included Groups		
Autopilot-Devices	None	None

Table 36. Assignments - MDE-DeviceControl

MDE-FW-Active

Name	Value
Basics	
Name	MDE-FW-Active
Description	Turns on Windows Firewall
Profile type	Settings catalog
Category	Firewall
Policy type	Windows Firewall
Platform supported	Windows 10 and later
Scope tags	Default

Table 37. Basics - MDE-FW-Active

Name	Value
Auditing	
Object Access Audit Filtering Platform Connection	Success+ Failure
Object Access Audit Filtering Platform Packet Drop	Success+ Failure
Firewall	
Enable Domain Network Firewall	True
Allow Local Policy Merge	False
Enable Private Network Firewall	True
Allow Local Policy Merge	False
Allow Local Ipsec Policy Merge	False
Auth Apps Allow User Pref Merge	False
Enable Public Network Firewall	True
Allow Local Policy Merge	False

Global Ports Allow User Pref Merge	False
Allow Local Ipsec Policy Merge	False

Table 38. Settings - MDE-FW-Active

Group	Filter	Filter mode
Included Groups		
Autopilot-Devices	None	None

Table 39. Assignments - MDE-FW-Active

MDE-Targeted-TamperPro

Name	Value
Basics	
Name	MDE-Targeted-TamperPro
Description	Highly recommended: Turn it on globally in security.microsoft.com. Tamper protection allows MDE to defend itself against modern Defense Evasion techniques. It should not break anything in Active or Passive Mode MDE deployments. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-tamper-protection-microsoft-365-defender
Profile type	Settings catalog
Category	Antivirus
Policy type	Windows Security Experience
Platform supported	Windows 10 and later
Scope tags	Default

Table 40. Basics - MDE-Targeted-TamperPro

Name	Value
Defender	
TamperProtection (Device)	On
Windows Defender Security Center	
Disable Family UI	(Enable) The users cannot see the display of the family options area in Windows Defender Security Center.

Table 41. Settings - MDE-Targeted-TamperPro

Group	Filter	Filter mode
Included Groups		
Autopilot-Devices	None	None

Table 42. Assignments - MDE-Targeted-TamperPro

Office Settings- User

Name	Value
Basics	
Name	Office Settings - User

Description	Automatic activation of M365 Apps Exchange Login using primary SMTP
Profile type	Settings catalog
Platform supported	Windows 10 and later
Scope tags	Default

Table 43. Basics - Office Settings - User

Name	Value
Microsoft Office 2016	
Subscription Activation	
Automatically activate Office with federated organization credentials (User)	Enabled
Microsoft Outlook 2016	
Exchange	
Automatically configure profile based on Active Directory Primary SMTP address (User)	Enabled

Table 44. Settings - Office Settings - User

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 45. Assignments - Office Settings - User

Office-BroadRing

Name	Value
Basics	
Name	Office-BroadRing
Description	Sets Office Updates to Semi Annual Channel
Profile type	Settings catalog
Platform supported	Windows 10 and later
Scope tags	Default

Table 46. Basics - Office-BroadRing

Name	Value
Microsoft Office 2016 (Machine)	
Updates	
Enable Automatic Updates	Enabled
Update Channel (Deprecated)	Disabled
Update Channel	Enabled
Channel Name: (Device)	Monthly Enterprise Channel

Table 47. Settings - Office-BroadRing

Office-BroadRing

Name	Value
Basics	
Name	Office-BroadRing
Description	Sets Office Updates to Semi Annual Channel

Profile type	Settings catalog
Platform supported	Windows 10 and later
Scope tags	Default

Table 48. Basics - Office-BroadRing

Name	Value
Microsoft Office 2016 (Machine)	
Updates	
Enable Automatic Updates	Enabled
Update Channel (Deprecated)	Disabled
Update Channel	Enabled
Channel Name: (Device)	Monthly Enterprise Channel

Table 49. Settings - Office-BroadRing

Office-PilotRing

Name	Value
Basics	
Name	Office-PilotRing
Description	Sets Office Updates to Monthly Channel
Profile type	Settings catalog
Platform supported	Windows 10 and later
Scope tags	Default

Table 50. Basics - Office-PilotRing

Name	Value
Microsoft Office 2016 (Machine)	
Updates	
Enable Automatic Updates	Enabled
Update Channel (Deprecated)	Enabled
Channel Name: (Device) (Deprecated)	Monthly Channel
Update Channel	Enabled
Channel Name: (Device)	Monthly Enterprise Channel

Table 51. Settings - Office-PilotRing

Office-PilotRing

Name	Value
Basics	
Name	Office-PilotRing
Description	Sets Office Updates to Monthly Channel
Profile type	Settings catalog
Platform supported	Windows 10 and later
Scope tags	Default

Table 52. Basics - Office-PilotRing

Name	Value
Microsoft Office 2016 (Machine)	
Updates	

Enable Automatic Updates	Enabled
Update Channel (Deprecated)	Enabled
Channel Name: (Device) (Deprecated)	Monthly Channel
Update Channel	Enabled
Channel Name: (Device)	Monthly Enterprise Channel

Table 53. Settings - Office-PilotRing

Office-PreviewRing

Name	Value
Basics	
Name	Office-PreviewRing
Description	Sets Office Updates to Insider Fast Channel
Profile type	Settings catalog
Platform supported	Windows 10 and later
Scope tags	Default

Table 54. Basics - Office-PreviewRing

Name	Value
Microsoft Office 2016 (Machine)	
Updates	
Enable Automatic Updates	Enabled
Update Channel (Deprecated)	Enabled
Channel Name: (Device) (Deprecated)	Insider Fast
Update Channel	Enabled
Channel Name: (Device)	Current Channel

Table 55. Settings - Office-PreviewRing

Office-VIPRing

Name	Value
Basics	
Name	Office-VIPRing
Description	Sets Office Updates to Semi Annual Channel (Targeted)
Profile type	Settings catalog
Platform supported	Windows 10 and later
Scope tags	Default

Table 56. Basics - Office-VIPRing

Name	Value
Microsoft Office 2016 (Machine)	
Updates	
Enable Automatic Updates	Enabled
Update Channel (Deprecated)	Enabled
Channel Name: (Device) (Deprecated)	Semi-Annual Channel (Targeted)
Update Channel	Enabled
Channel Name: (Device)	Semi-Annual Enterprise Channel

Table 57. Settings - Office-VIPRing

OneDrive Config

Name	Value
Basics	
Name	OneDrive Config
Description	Enabled KFM, Files on Demand, Silent sign-in and excludes lnk files from synchronising
Profile type	Settings catalog
Platform supported	Windows 10 and later
Scope tags	Default

Table 58. Basics - OneDrive Config

Name	Value
OneDrive	
Exclude specific kinds of files from being uploaded	Enabled
Keywords: (Device)	*.lnk
Hide the "Deleted files are removed everywhere" reminder	Enabled
Prevent users from redirecting their Windows known folders to their PC	Enabled
Silently move Windows known folders to OneDrive	Enabled
Show notification to users after folders have been redirected: (Device)	No
Tenant ID: (Device)	065f849d-bc53-4b5a-bae3-c5793f9239c1
Silently sign in users to the OneDrive sync app with their Windows credentials	Enabled
Use OneDrive Files On-Demand	Enabled

Table 59. Settings - OneDrive Config

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 60. Assignments - OneDrive Config

StoreSettings

Name	Value
Basics	
Name	StoreSettings
Description	Store for Business Restrictions
Profile type	Settings catalog
Platform supported	Windows 10 and later
Scope tags	Default

Table 61. Basics - StoreSettings

Name	Value

Microsoft App Store	
Require Private Store Only	Only Private store is enabled.

Table 62. Settings - StoreSettings

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 63. Assignments - StoreSettings

Windows 11 Start Menu

Name	Value
Basics	
Name	Windows 11 Start Menu
Description	Configures Windows 11 Taskbar and Start Menu
Profile type	Settings catalog
Platform supported	Windows 10 and later
Scope tags	Default

Table 64. Basics - Windows 11 Start Menu

Name	Value
Experience	
Configure Chat Icon	Disabled
Start	
Configure Start Pins (Windows Insiders only)	{ "pinnedList": [{ "desktopAppId": "MSEdge" }, { "desktopAppId": "Microsoft.Office.EXCEL.EXE.15" }, { "desktopAppId": "Microsoft.Office.POWERPNT.EXE.15" }, { "desktopAppId": "Microsoft.Office.OUTLOOK.EXE.15" }, { "desktopAppId": "Microsoft.Office.ONENOTE.EXE.15" }, { "desktopAppId": "Microsoft.Office.com.squirrel.Teams.Teams" }, { "packagedAppId": "Microsoft.CompanyPortal_8wekyb3d8bbwe!App" }, { "desktopAppId": "Microsoft.Office.WINWORD.EXE.15" }, { "packagedAppId": "Microsoft.WindowsStore_8wekyb3d8bbwe!App" }, { "desktopAppId": "Microsoft.Windows.Explorer" }] }
No Pinning To Taskbar	Enabled
Start Layout	<?xml version="1.0" encoding="utf-8"?> <LayoutModificationTemplate xmlns="http://schemas.microsoft.com/Start/2014/LayoutModification" xmlns:defaultlayout="http://schemas.microsoft.com/Start/2014/FullDefaultLayout" xmlns:start="http://schemas.microsoft.com/Start/2014/StartLayout" xmlns:taskbar="http://schemas.microsoft.com/Start/2014/TaskbarLayout" Version="1"> <CustomTaskbarLayoutCollection PinListPlacement="Replace"> <defaultlayout:TaskbarLayout> <taskbar:TaskbarPinList> <taskbar:DesktopApp DesktopApplicationID="Microsoft.Windows.Explorer"/> <taskbar:DesktopApp

	DesktopApplicationID="Microsoft.Office.OUTLOOK.EXE.15"/> <taskbar:DesktopApp DesktopApplicationID="MSEdge"/> </taskbar:TaskbarPinList> </defaultlayout:TaskbarLayout> </CustomTaskbarLayoutCollection> </LayoutModificationTemplate>

Table 65. Settings - Windows 11 Start Menu

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 66. Assignments - Windows 11 Start Menu

Windows Health Monitoring

Name	Value
Basics	
Name	Windows Health Monitoring
Description	Contains the monitoring settings that are needed for Update Compliance Workspace, and Windows Autopatch. Note - for organisation that are not using Update Compliance, or Autopatch, this policy can be ignored.
Profile type	Settings catalog
Platform supported	Windows 10 and later
Scope tags	Default

Table 67. Basics - Windows Health Monitoring

Name	Value
Administrative Templates	
Data Collection and Preview Builds	
Configure the Commercial ID	Disabled
Device Health Monitoring	
Allow Device Health Monitoring	The DeviceHealthMonitoring connection is enabled.
System	
Allow Commercial Data Pipeline	Disabled.
Allow device name to be sent in Windows diagnostic data	Allowed.
Allow Telemetry	Full
Allow Update Compliance Processing	Enabled
Configure Telemetry Opt In Change Notification	Disable telemetry change notifications.
Configure Telemetry Opt In Settings Ux	Disable Telemetry opt-in Settings.

Table 68. Settings - Windows Health Monitoring

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 69. Assignments - Windows Health Monitoring

Templates

Base Android Config

Name	Value
Basics	
Name	Base Android Config
Description	Sets Android security baseline to secure mobile devices
Platform supported	Android Enterprise
Profile type	Device restrictions
Version	1
Scope tags	Default

Table 70. Basics - Base Android Config

Name	Value
General	
Fully managed, dedicated, and corporate-owned work profile devices	
Screen capture (work profile-level)	Block
Camera (work profile-level)	Not configured
Date and Time changes	Block
Roaming data services	Not configured
Wi-Fi access point configuration	Not configured
Bluetooth configuration	Not configured
Tethering and access to hotspots	Block
USB file transfer	Block
External media	Block
Beam data using NFC (work profile-level)	Block
Microphone adjustment	Not configured
Factory reset protection emails	Not configured
System update	Automatic
Fully managed and dedicated devices	
Volume changes	Not configured
Factory reset	Block
Status bar	Not configured
Wi-Fi setting changes	Not configured
USB storage	Not configured
Network escape hatch	Not configured
Notification windows	Not configured
Skip first use hints	Enable
Corporate-owned work profile devices	
Contact sharing via Bluetooth (work profile-level)	Block
Search work contacts and display work contact caller-id in personal profile.	Block
Copy and paste between work and personal profiles.	Allow
Data sharing between work and personal profiles.	Block all sharing between profiles

System security	
Fully managed, dedicated, and corporate-owned work profile devices	
Threat scan on apps	Require
Common Criteria mode	Not configured
Device experience	
Fully managed and dedicated devices	
Enrollment profile type	Fully managed
Configure Microsoft Launcher on your fully managed devices.	
Make Microsoft Launcher the default launcher	Enable
Configure custom wallpaper	Not configured
Enable launcher feed	Not configured
Dock presence	Not configured
Allow user to change dock presence	Not configured
Search bar placement	Not configured
Device password	
Fully managed, dedicated, and corporate-owned work profile devices	
Required password type	Numeric
Minimum password length	4
Number of days until password expires	180
Number of passwords required before user can reuse a password	3
Number of sign-in failures before wiping device	6
Disabled lock screen features	Secure camera (fully managed or dedicated) ;Text entry in notifications (fully managed or dedicated);Unredacted notifications
Required unlock frequency	Device default
Fully managed and dedicated devices	
Disable lock screen	Not configured
Power Settings	
Fully managed, dedicated, and corporate-owned work profile devices	
Time to lock screen (work profile-level)	1 Minute
Fully managed and dedicated devices	
Screen on while device plugged in	
Users and Accounts	
Fully managed, dedicated, and corporate-owned work profile devices	
Add new users	Block
User can configure credentials (work profile-level)	Block
Fully managed and dedicated devices	
User removal	Block
Personal Google accounts	Block
Dedicated devices	
Account changes	Block
Applications	
Fully managed, dedicated, and corporate-owned work profile devices	
Allow installation from unknown sources	Not configured
App auto-updates (work profile-level)	Always
Allow access to all apps in Google Play store	Not configured

Connectivity	
Fully managed, dedicated, and corporate-owned work profile devices	
Always-on VPN (work profile-level)	Not configured
Lockdown mode	Not configured
Fully managed and dedicated devices	
Recommended global proxy	Not configured
Work profile password	
Corporate-owned work profile devices	
Required password type	Numeric
Minimum password length	4
Number of days until password expires	180
Number of passwords required before user can reuse a password	3
Number of sign-in failures before wiping device	6
Required unlock frequency	Device default
Personal profile	
Corporate-owned work profile devices	
Camera	Not configured
Screen capture	Block
Allow users to enable app installation from unknown sources in the personal profile	Not configured
Type of restricted apps list	Not configured

Table 71. Settings - Base Android Config

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 72. Assignments - Base Android Config

Baseline Device Restrictions

Name	Value
Basics	
Name	Baseline Device Restrictions
Description	Sets iOS Security Baseline device restrictions for both iPad and iPhone
Platform supported	iOS/iPadOS
Profile type	Device restrictions
Version	1
Scope tags	Default

Table 73. Basics - Baseline Device Restrictions

Name	Value
App Store, Doc Viewing, Gaming	
All enrollment types	
Block viewing corporate documents in unmanaged apps	Yes

Allow unmanaged apps to read from managed contacts accounts	Not configured
Treat AirDrop as an unmanaged destination	Yes
Block viewing non-corporate documents in corporate apps	Yes
Allow copy/paste to be affected by managed open-in	Yes
Device enrollment and automated device enrollment	
Require iTunes Store password for all purchases	Not configured
Block in-app purchases	Yes
Block download of explicit sexual content in Apple Books	Yes
Allow managed apps to write contacts to unmanaged contacts accounts	Not configured
Ratings region	No region configured
Automated device enrollment	
Block App store	Yes
Block installing apps using App Store	Not configured
Block automatic app downloads	Not configured
Block playback of explicit music, podcast, and iTunes U	Yes
Block adding Game Center friends	Yes
Block Game Center	Yes
Block multiplayer gaming in the Game Center	Yes
Block access to network drive in Files app	Yes
Autonomous Single App Mode	
Automated device enrollment	
App name	
Built-in apps	
All enrollment types	
Block Siri	Not configured
Block Siri while device is locked	Yes
Require Safari fraud warnings	Yes
Device enrollment and automated device enrollment	
Block internet search results from Spotlight	Yes
Safari cookies	Not configured
Block Safari JavaScript	Not configured
Block Safari pop-ups	Yes
Block Siri for dictation	Not configured
Block Siri for translation	Not configured
Automated device enrollment	
Block camera	Not configured
Block FaceTime	Not configured
Require Siri profanity filter	Not configured
Block user-generated content in Siri	Not configured
Block Apple News	Yes
Block Apple Books	Yes
Block iMessage	Not configured

Block Podcasts	Yes
Music service	Yes
Block iTunes Radio	Yes
Block iTunes store	Yes
Block Find My iPhone	Not configured
Block Find My Friends	Yes
Block user modification to the Find My Friends settings	Yes
Block removal of system apps from device	Yes
Block Safari	Not configured
Block Safari Autofill	Not configured
Cloud and Storage	
All enrollment types	
Force encrypted backup	Yes
Block managed apps from storing data in iCloud	Yes
Block backup of enterprise books	Not configured
Block notes and highlights sync for enterprise books	Not configured
Device enrollment and automated device enrollment	
Block iCloud Photos sync	Yes
Block iCloud Photo Library	Yes
Block My Photo Stream	Yes
Block Handoff	Yes
Automated device enrollment	
Block iCloud backup	Yes
Block iCloud document and data sync	Yes
Block iCloud Keychain sync	Yes
Block iCloud Private Relay	Yes
Connected devices	
All enrollment types	
Force Apple Watch wrist detection	Yes
Device enrollment and automated device enrollment	
Require AirPlay outgoing requests pairing password	Not configured
Block Apple Watch auto unlock	Not configured
Automated device enrollment	
Block AirDrop	Yes
Block pairing with Apple Watch	Not configured
Block modifying Bluetooth settings	Not configured
Block pairing with non-Configurator hosts	Yes
Block AirPrint	Not configured
Block storage of AirPrint credentials in Keychain	Block
Require AirPrint to destinations with trusted certificates	Not configured
Block iBeacon discovery of AirPrint printers	Not configured
Block setting up new nearby devices	Yes
Block access to USB drive in Files app	Yes

Disable near-field communication (NFC)	Not configured
Allow users to boot devices into recovery mode with unpaired devices	Not configured
Domains	
Unmarked email domains	
Unmarked email domains	
Managed Safari web domains	
Web Domain URL	
Safari password domains	
Domain URL	
General	
All enrollment types	
Block sending diagnostic and usage data to Apple	Yes
Block screenshots and screen recording	Yes
Device enrollment and automated device enrollment	
Block untrusted TLS certificates	Yes
Block over-the-air PKI updates	Not configured
Force limited ad tracking	Yes
Block trusting new enterprise app authors	Yes
Limit Apple personalized advertising	Yes
Automated device enrollment	
Block modification of diagnostics settings	Not configured
Block remote AirPlay, view screen by Classroom app, and screen sharing	Not configured
Allow Classroom app to perform AirPlay and view screen without prompting	Not configured
Block modification of account settings	Yes
Block Screen Time	Yes
Block users from erasing all content and settings on device	Yes
Block modification of device name	Yes
Block modification of notifications settings	Not configured
Block modification of Wallpaper	Not configured
Block configuration profile changes	Yes
Allow activation lock	Not configured
Block removing apps	Yes
Block app clips	Not configured
Allow USB accessories while device is locked	Yes
Force automatic date and time	Yes
Require teacher permission to leave Classroom app unmanaged classes	Not configured
Allow Classroom to lock to an app and lock the device without prompting	Not configured
Allow students to automatically join Classroom classes without prompting	Not configured
Block VPN creation	Yes
Block modification of eSIM settings	Yes
Defer software updates	Not configured
Delay default visibility of software updates	

Keyboard and dictionary	
Automated device enrollment	
Block word definition lookup	Not configured
Block predictive keyboards	Not configured
Block auto-correction	Not configured
Block spell check	Not configured
Block keyboard shortcuts	Not configured
Block dictation	Not configured
Block QuickPath	Not configured
Locked Screen Experience	
All enrollment types	
Block Control Center access in lock screen	Yes
Block Notification Center access in lock screen	Yes
Block Today view in lock screen	Yes
Device enrollment and automated device enrollment	
Block Wallet notifications in lock screen	Yes
Password	
All enrollment types	
Require password	Yes
Device enrollment and automated device enrollment	
Block simple passwords	Yes
Required password type	Alphanumeric
Number of non-alphanumeric characters in password	Not configured
Minimum password length	6
Number of sign-in failures before wiping device	6
Maximum minutes after screen lock before password is required	Immediately
Maximum minutes of inactivity until screen locks	2 minutes
Password expiration (days)	180
Prevent reuse of previous passwords	3
Block Touch ID and Face ID unlock	Not configured
Automated device enrollment	
Block passcode modification	Not configured
Block modification of Touch ID fingerprints and Face ID faces	Not configured
Block password AutoFill	Yes
Block password proximity requests	Yes
Block password sharing	Yes
Require Touch ID or Face ID authentication for AutoFill of password or credit card information	Yes
Restricted Apps	
Device enrollment and automated device enrollment	
Type of restricted apps list	Not configured
Apps list	
Shared iPad	
Automated device enrollment	

Block Shared iPad temporary sessions	Not configured
Show or Hide Apps	
Automated device enrollment	
Type of apps list	Not configured
Apps list	
Wireless	
Device enrollment and automated device enrollment	
Block data roaming	Not configured
Block global background fetch while roaming	Not configured
Block voice dialing while device is locked	Not configured
Block voice roaming	Not configured
Block personal hotspot	Not configured
Add managed iOS apps that should not be allowed to use any cellular data.	
Block use of cellular data	Not configured
Block use of cellular data when roaming	
Block use of cellular data when roaming	Not configured
Automated device enrollment	
Block changes to app cellular data usage settings	Not configured
Block changes to cellular plan settings	Yes
Block modification of personal hotspot	Yes
Require joining Wi-Fi networks only using configuration profiles	Not configured
Require Wi-Fi always on	Not configured
Require devices to use Wi-Fi networks set up via configuration profiles	Not configured

Table 74. Settings - Baseline Device Restrictions

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 75. Assignments - Baseline Device Restrictions

Baseline iOS Features

Name	Value
Basics	
Name	Baseline iOS Features
Description	Sets the lock screen message on iOS devices
Platform supported	iOS/iPadOS
Profile type	Device features
Version	1
Scope tags	Default

Table 76. Basics - Baseline iOS Features

Name	Value
AirPrint	
All enrollment types	
AirPrint destinations	

App Notifications	
Automated device enrollment	
App notifications	
Lock Screen Message	
Automated device enrollment	
"If Lost, Return to..." Message	If Lost, please return to X
Asset tag information	
Single sign-on	
Device enrollment and automated device enrollment	
Azure AD username attribute	Not configured
Credential renewal certificate	

Table 77. Settings - Baseline iOS Features

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 78. Assignments - Baseline iOS Features

Intune data collection policy

Name	Value
Basics	
Name	Intune data collection policy
Description	Enable Data Analytics
Platform supported	Windows 10 and later
Version	1
Scope tags	Default

Table 79. Basics - Intune data collection policy

Name	Value
Health monitoring	
Health monitoring	Enable
Scope	Endpoint analytics;Windows updates

Table 80. Settings - Intune data collection policy

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 81. Assignments - Intune data collection policy

iOS device restriction to block Game Center

Name	Value
Basics	
Name	iOS device restriction to block Game Center
Description	
Platform supported	iOS/iPadOS
Profile type	Device restrictions

Version	1
Scope tags	Default

Table 82. Basics - iOS device restriction to block Game Center

Name	Value
App Store, Doc Viewing, Gaming	
All enrollment types	
Block viewing corporate documents in unmanaged apps	Not configured
Allow unmanaged apps to read from managed contacts accounts	Not configured
Treat AirDrop as an unmanaged destination	Not configured
Block viewing non-corporate documents in corporate apps	Not configured
Allow copy/paste to be affected by managed open-in	Not configured
Device enrollment and automated device enrollment	
Require iTunes Store password for all purchases	Not configured
Block in-app purchases	Not configured
Block download of explicit sexual content in Apple Books	Not configured
Allow managed apps to write contacts to unmanaged contacts accounts	Not configured
Ratings region	No region configured
Automated device enrollment	
Block App store	Not configured
Block installing apps using App Store	Not configured
Block automatic app downloads	Not configured
Block playback of explicit music, podcast, and iTunes U	Not configured
Block adding Game Center friends	Not configured
Block Game Center	Not configured
Block multiplayer gaming in the Game Center	Not configured
Block access to network drive in Files app	Not configured
Autonomous Single App Mode	
Automated device enrollment	
App name	
Built-in apps	
All enrollment types	
Block Siri	Not configured
Block Siri while device is locked	Not configured
Require Safari fraud warnings	Not configured
Device enrollment and automated device enrollment	
Block internet search results from Spotlight	Not configured
Safari cookies	Not configured
Block Safari JavaScript	Not configured
Block Safari pop-ups	Not configured
Block Siri for dictation	Not configured
Block Siri for translation	Not configured

Automated device enrollment	
Block camera	Not configured
Block FaceTime	Not configured
Require Siri profanity filter	Not configured
Block user-generated content in Siri	Not configured
Block Apple News	Not configured
Block Apple Books	Not configured
Block iMessage	Not configured
Block Podcasts	Not configured
Music service	Not configured
Block iTunes Radio	Not configured
Block iTunes store	Not configured
Block Find My iPhone	Not configured
Block Find My Friends	Not configured
Block user modification to the Find My Friends settings	Not configured
Block removal of system apps from device	Not configured
Block Safari	Not configured
Block Safari Autofill	Not configured
Cloud and Storage	
All enrollment types	
Force encrypted backup	Not configured
Block managed apps from storing data in iCloud	Not configured
Block backup of enterprise books	Not configured
Block notes and highlights sync for enterprise books	Not configured
Device enrollment and automated device enrollment	
Block iCloud Photos sync	Not configured
Block iCloud Photo Library	Not configured
Block My Photo Stream	Not configured
Block Handoff	Not configured
Automated device enrollment	
Block iCloud backup	Not configured
Block iCloud document and data sync	Not configured
Block iCloud Keychain sync	Not configured
Block iCloud Private Relay	Not configured
Connected devices	
All enrollment types	
Force Apple Watch wrist detection	Not configured
Device enrollment and automated device enrollment	
Require AirPlay outgoing requests pairing password	Not configured
Block Apple Watch auto unlock	Not configured
Automated device enrollment	
Block AirDrop	Not configured
Block pairing with Apple Watch	Not configured
Block modifying Bluetooth settings	Not configured
Block pairing with non-Configurator hosts	Not configured

Block AirPrint	Not configured
Block storage of AirPrint credentials in Keychain	Not configured
Require AirPrint to destinations with trusted certificates	Not configured
Block iBeacon discovery of AirPrint printers	Not configured
Block setting up new nearby devices	Not configured
Block access to USB drive in Files app	Not configured
Disable near-field communication (NFC)	Not configured
Allow users to boot devices into recovery mode with unpaired devices	Not configured
Domains	
Unmarked email domains	
Unmarked email domains	
Managed Safari web domains	
Web Domain URL	
Safari password domains	
Domain URL	
General	
All enrollment types	
Block sending diagnostic and usage data to Apple	Not configured
Block screenshots and screen recording	Not configured
Device enrollment and automated device enrollment	
Block untrusted TLS certificates	Not configured
Block over-the-air PKI updates	Not configured
Force limited ad tracking	Not configured
Block trusting new enterprise app authors	Not configured
Limit Apple personalized advertising	Not configured
Automated device enrollment	
Block modification of diagnostics settings	Not configured
Block remote AirPlay, view screen by Classroom app, and screen sharing	Not configured
Allow Classroom app to perform AirPlay and view screen without prompting	Not configured
Block modification of account settings	Not configured
Block Screen Time	Not configured
Block users from erasing all content and settings on device	Not configured
Block modification of device name	Not configured
Block modification of notifications settings	Not configured
Block modification of Wallpaper	Not configured
Block configuration profile changes	Not configured
Allow activation lock	Not configured
Block removing apps	Not configured
Block app clips	Not configured
Allow USB accessories while device is locked	Not configured
Force automatic date and time	Not configured
Require teacher permission to leave Classroom app unmanaged classes	Not configured

Allow Classroom to lock to an app and lock the device without prompting	Not configured
Allow students to automatically join Classroom classes without prompting	Not configured
Block VPN creation	Not configured
Block modification of eSIM settings	Not configured
Defer software updates	Not configured
Delay default visibility of software updates	
Keyboard and dictionary	
Automated device enrollment	
Block word definition lookup	Not configured
Block predictive keyboards	Not configured
Block auto-correction	Not configured
Block spell check	Not configured
Block keyboard shortcuts	Not configured
Block dictation	Not configured
Block QuickPath	Not configured
Locked Screen Experience	
All enrollment types	
Block Control Center access in lock screen	Not configured
Block Notification Center access in lock screen	Not configured
Block Today view in lock screen	Not configured
Device enrollment and automated device enrollment	
Block Wallet notifications in lock screen	Not configured
Password	
All enrollment types	
Require password	Not configured
Device enrollment and automated device enrollment	
Block simple passwords	Not configured
Required password type	Device default
Number of non-alphanumeric characters in password	Not configured
Minimum password length	
Number of sign-in failures before wiping device	
Maximum minutes after screen lock before password is required	Not configured
Maximum minutes of inactivity until screen locks	Not configured
Password expiration (days)	
Prevent reuse of previous passwords	
Block Touch ID and Face ID unlock	Not configured
Automated device enrollment	
Block passcode modification	Not configured
Block modification of Touch ID fingerprints and Face ID faces	Not configured
Block password AutoFill	Not configured
Block password proximity requests	Not configured
Block password sharing	Not configured

Require Touch ID or Face ID authentication for AutoFill of password or credit card information	Not configured
Restricted Apps	
Device enrollment and automated device enrollment	
Type of restricted apps list	Not configured
Apps list	
Shared iPad	
Automated device enrollment	
Block Shared iPad temporary sessions	Not configured
Show or Hide Apps	
Automated device enrollment	
Type of apps list	Not configured
Apps list	
Wireless	
Device enrollment and automated device enrollment	
Block data roaming	Not configured
Block global background fetch while roaming	Not configured
Block voice dialing while device is locked	Not configured
Block voice roaming	Not configured
Block personal hotspot	Not configured
Add managed iOS apps that should not be allowed to use any cellular data.	
Block use of cellular data	Not configured
Block use of cellular data when roaming	
Block use of cellular data when roaming	Not configured
Automated device enrollment	
Block changes to app cellular data usage settings	Not configured
Block changes to cellular plan settings	Not configured
Block modification of personal hotspot	Not configured
Require joining Wi-Fi networks only using configuration profiles	Not configured
Require Wi-Fi always on	Not configured
Require devices to use Wi-Fi networks set up via configuration profiles	Not configured

Table 83. Settings - iOS device restriction to block Game Center

Group	Filter	Filter mode
Included Groups		
sg-Sales and Marketing	None	None

Table 84. Assignments - iOS device restriction to block Game Center

macOS Features

Name	Value
Basics	
Name	macOS Features
Description	Sets macOS login options
Platform supported	macOS

Profile type	Device features
Version	1
Scope tags	Default

Table 85. Basics - macOS Features

Name	Value
AirPrint	
All enrollment types	
AirPrint destinations	
Associated domains	
User approved and automated device enrollment	
Associated domains	
Content caching	
All enrollment types	
Enable content caching	Not configured
Type of content to cache	All content
Maximum cache size	
Cache location	
Port	
Block internet connection and cache content sharing	Not configured
Enable internet connection sharing	Not configured
Enable cache to log client details	Not configured
Always keep content from the cache, even when the system needs disk space for other apps	Not configured
Show status alerts	Not configured
Prevent the device from sleeping while caching is turned on	Not configured
Devices to cache	Not configured
Custom public IP addresses	
Share content with other caches	Not configured
Parent IP addresses	
Parent selection policy	Not configured
Login items	
All enrollment types	
Add the files, folders, and custom apps that will launch at login	
Login window	
Window Layout	
Show additional information in the menu bar	Yes
Banner	MAC Test
Require username and password text fields	Not configured
Hide local users	Yes
Hide mobile accounts	Yes
Show network users	Not configured
Hide computer's administrators	Not configured
Show other users	Not configured
Login screen power settings	

Hide shut down button	Not configured
Hide restart button	Not configured
Hide sleep button	Not configured
Other	
Disable user login from Console	Not configured
Apple Menu	
Disable Shut Down while logged in	Not configured
Disable Restart while logged in	Not configured
Disable Power Off while logged in	Not configured
Disable Log Out while logged in	Not configured
Disable Lock Screen while logged in	Not configured

Table 86. Settings - macOS Features

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 87. Assignments - macOS Features

macOS Protection

Name	Value
Basics	
Name	macOS Protection
Description	Enabled Firewall, Filevault and Gatekeeper
Platform supported	macOS
Profile type	Endpoint protection
Version	1
Scope tags	Default

Table 88. Basics - macOS Protection

Name	Value
FileVault	
Enable Full Disk Encryption using XTS-AES 128 with FileVault 2.	
Enable FileVault	Yes
Escrow location description of personal recovery key	It's on Intune
Personal recovery key rotation	Not configured
Hide recovery key	Not configured
Disable prompt at sign out	Not configured
Firewall	
Enable Firewall	Yes
Block all incoming connections	Not configured
Apps allowed	
App lists	
Apps blocked	
App lists	
Enable stealth mode	Not configured
Gatekeeper	
Allow apps downloaded from these locations	Mac App Store and identified developers

Do not allow user to override Gatekeeper	Not configured

Table 89. Settings - macOS Protection

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 90. Assignments - macOS Protection

macOS Restrictions

Name	Value
Basics	
Name	macOS Restrictions
Description	macOS Security Baseline Settings
Platform supported	macOS
Profile type	Device restrictions
Version	1
Scope tags	Default

Table 91. Basics - macOS Restrictions

Name	Value
App Store, Doc Viewing, Gaming	
Automated device enrollment	
Block adding Game Center friends	Yes
Block Game Center	Yes
Block multiplayer gaming in the Game Center	Yes
Built-in apps	
All enrollment types	
Block Safari AutoFill	Not configured
Block use of camera	Not configured
Block Apple Music	Yes
Block spotlight suggestions	Yes
Block file transfer using Finder or iTunes	Not configured
Cloud and Storage	
All enrollment types	
Block iCloud Keychain sync	Yes
Block iCloud desktop and documents sync	Yes
Block iCloud document and data sync	Yes
Block iCloud Mail backup	Yes
Block iCloud Contact Backup	Yes
Block iCloud Calendar Backup	Yes
Block iCloud Reminder Backup	Yes
Block iCloud Bookmark Backup	Yes
Block iCloud Notes Backup	Yes
Block iCloud Photos backup	Yes
Block Handoff	Yes
User approved and automated device enrollment	
Block iCloud Private Relay	Yes
Connected devices	

All enrollment types	
Block AirDrop	Yes
Block Apple Watch auto unlock	Yes
Domains	
All enrollment types	
Unmarked email domains	
General	
All enrollment types	
Block look up	Not configured
Block dictation	Not configured
Block content caching	Not configured
Block screenshots and screen recording	Not configured
Automated device enrollment	
Disable AirPlay, view screen by Classroom app, and screen sharing	Not configured
Allow Classroom app to perform AirPlay and view screen without prompting	Not configured
Require teacher permission to leave Classroom app unmanaged classes	Not configured
Allow Classroom to lock the device without prompting	Not configured
Students can automatically join Classroom class without prompting	Not configured
Block modification of wallpaper	Yes
Block users from erasing all content and settings on device	Not configured
Allow activation lock	Not configured
Password	
All enrollment types	
Require password	Yes
Required password type	Alphanumeric
Number of non-alphanumeric characters in password	2
Minimum password length	
Block simple passwords	Yes
Maximum minutes after screen lock before password is required	Immediately
Maximum minutes of inactivity until screen locks	5 minutes
Password expiration (days)	
Prevent reuse of previous passwords	
Maximum allowed sign-in attempts	
Block user from modifying passcode	Not configured
Block Touch ID to unlock device	Not configured
Timeout (hours of inactivity)	
Block password AutoFill	Not configured
Block password proximity requests	Yes
Block password sharing	Yes
Privacy preferences	

User approved and automated device enrollment	
Apps and processes	
Restricted Apps	
All enrollment types	
Type of restricted apps list	Prohibited apps
Apps list	com.apple.calculator;Calculator;

Table 92. Settings - macOS Restrictions

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 93. Assignments - macOS Restrictions

MDE-iOS-Supervised-ControlFilter

Name	Value
Basics	
Name	MDE-iOS-Supervised-ControlFilter
Description	Configures Defender for Endpoint on iOS devices
Platform supported	iOS/iPadOS
Profile type	Custom
Version	1
Scope tags	Default

Table 94. Basics - MDE-iOS-Supervised-ControlFilter

Name	Value
Custom Configuration Profile	
Custom configuration profile name	MDE-iOS-Supervised
Configuration profile file	Microsoft_Defender_for_Endpoint_Control_Filter_Zerotouch.mobileconfig

Table 95. Settings - MDE-iOS-Supervised-ControlFilter

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 96. Assignments - MDE-iOS-Supervised-ControlFilter

Start-Menu-W10

Name	Value
Basics	
Name	Start-Menu-W10
Description	Windows 10 Start Menu Office Apps, Teams, Edge, Company Portal and Store pinned to start Outlook, Explorer and Edge pinned to taskbar

Platform supported	Windows 10 and later
Profile type	Device restrictions
Version	1
Scope tags	Default

Table 97. Basics - Start-Menu-W10

Name	Value
App Store	
App store (mobile only)	Not configured
Auto-update apps from store	Not configured
Trusted app installation	Not configured
Developer unlock	Not configured
Shared user app data	Not configured
Use private store only	Not configured
Store originated app launch	Not configured
Install app data on system volume	Not configured
Install apps on system drive	Not configured
Game DVR (desktop only)	Not configured
Apps from store only	Not Configured
User control over installations	Not configured
Install apps with elevated privileges	Not configured
Startup apps	
Cellular and connectivity	
Cellular data channel	Not configured
Data roaming	Not configured
VPN over the cellular network	Not configured
VPN roaming over the	Not configured

cellular network	
Connected devices service	Not configured
NFC	Not configured
Wi-Fi	Not configured
Automatically connect to Wi-Fi hotspots	Not configured
Manual Wi-Fi configuration	Not configured
Wi-Fi scan interval (mobile only)	
Bluetooth	
Bluetooth	Not configured
Bluetooth discoverability	Not configured
Bluetooth pre-pairing	Not configured
Bluetooth advertising	Not configured
Bluetooth proximal connections	Not configured
Bluetooth allowed services	
Cloud and Storage	
Microsoft account	Not configured
Non-Microsoft account	Not configured
Settings synchronization for Microsoft account	Not configured
Microsoft Account sign-in assistant	Not configured
Cloud Printer	
Printer discovery URL	
Printer access authority URL	
Azure native client app GUID	
Print service resource URI	

Maximum printers to query(Mobile only)	
Printer discovery service resource URI	
Control Panel and Settings	
Settings app	Not configured
System	Not configured
Power and sleep settings modification (desktop only)	Not configured
Devices	Not configured
Network and Internet	Not configured
Personalization	Not configured
Apps	Not configured
Accounts	Not configured
Time and Language	Not configured
System Time modification	Not configured
Region settings modification (desktop only)	Not configured
Language settings modification (desktop only)	Not configured
Gaming	Not configured
Ease of Access	Not configured
Privacy	Not configured
Update and Security	Not configured
Display	
Turn on GDI scaling for apps.	
Turn off GDI scaling for apps.	
General	

Screen capture (mobile only)	Not configured
Copy and paste (mobile only)	Not configured
Manual unenrollment	Not configured
Manual root certificate installation (mobile only)	Not configured
Camera	Not configured
OneDrive file sync	Not configured
Removable storage	Not configured
Geolocation	Not configured
Internet sharing	Not configured
Phone reset	Not configured
USB connection	Not configured
AntiTheft mode (mobile only)	Not configured
Cortana	Not configured
Voice recording (mobile only)	Not configured
Device name modification (mobile only)	Not configured
Add provisioning packages	Not configured
Remove provisioning packages	Not configured
Device discovery	Not configured
Task Switcher (mobile only)	Not configured
SIM card error dialog (mobile only)	Not configured
Ink Workspace	Not configured
Autopilot Reset	Not configured
Require users to connect to network	Not configured

during device setup	
Direct Memory Access	Not configured
End processes from Task Manager	Not configured
Locked Screen Experience	
Action center notifications (mobile only)	Not configured
Locked screen picture URL (Desktop only)	
User configurable screen timeout (mobile only)	Not configured
Cortana on locked screen (Desktop only)	Not configured
Toast notifications on locked screen	Not configured
Screen timeout (mobile only)	
Voice activate apps from locked screen	Not configured
Messaging	
Message sync (mobile only)	Not configured
MMS (mobile only)	Not configured
RCS (mobile only)	Not configured
Microsoft Edge Legacy (Version 45 and earlier)	
Use Microsoft Edge kiosk mode	No
Start experience	
Start Microsoft Edge with	Start pages in local app settings
Allow user to change Start pages	No

Allow web content on new Tab page	Yes
New Tab URL	
Allow Users to change Home button	No
Show First Run Experience page (Mobile only)	Yes
First Run Experience URL list location	
Allow pop-ups	Yes
Send intranet traffic to Internet Explorer	No
Enterprise mode site list location (Desktop only)	
Message when opening sites in Internet Explorer	Don't show message
Allow Microsoft compatibility list	Yes
Preload Start pages and new Tab page	Yes
Prelaunch Start pages and new Tab page	Yes
Favorites and search	
Show Favorites bar	On Start and new Tab pages
Allow changes to favorites	Yes
Favorites List	
Sync favorites between Microsoft browsers (Desktop only)	No

Default search engine	Not configured
Show search suggestions	Yes
Privacy and security	
Allow InPrivate browsing	Yes
Save browsing history	Yes
Clear browsing data on exit (Desktop only)	No
Sync browser settings between user's devices	Allow
Allow Password Manager	Yes
Cookies	Allow
Allow Autofill in forms	Yes
Send do-not-track headers	No
Show WebRTC localhost IP address	Yes
Allow live tile data collection	Yes
User can override certificate errors	Yes
Additional	
Allow Microsoft Edge browser (Mobile only)	Yes
Allow address bar dropdown	Yes
Allow full screen mode	Yes
Allow printing	Yes
Allow about flags page	Yes
Allow developer tools	Yes
Allow JavaScript	Yes

User can install extensions	Yes
Allow sideloading of developer extensions	Yes
Required extensions	
Network proxy	
Automatically detect proxy settings	Not configured
Use proxy script	Allow
Setup script address URL	
Use manual proxy server	Not configured
Address	
Port number	
Proxy exceptions	
Bypass proxy server for local address	Not configured
Password	
Password	Not configured
Required password type	Not configured
Minimum password length	
Number of sign-in failures before wiping device	
Maximum minutes of inactivity until screen locks	Not configured
Password expiration (days)	
Prevent reuse of previous passwords	
Require password when device returns from	Not configured

idle state (Mobile and Holographic)	
Simple passwords	Not configured
Automatic encryption during AADJ	Not configured
Federal Information Processing Standard (FIPS) policy	Not configured
Windows Hello device authentication	Not configured
Preferred Azure AD tenant domain	
Per-app privacy exceptions	
Exceptions	
Personalization	
Desktop background picture URL (Desktop only)	
Printer	
Printers	
Default printer	
Add new printers	Not configured
Privacy	
Privacy experience	Not configured
Input personalization	Not configured
Automatic acceptance of the pairing and privacy user consent prompts	Not configured
Publish user activities	Not configured
Local activities only	Not configured
Projection	
User input from wireless	Not configured

display receivers	
Projection to this PC	Not configured
Require PIN for pairing	Not configured
Reporting and Telemetry	
Share usage data	Not configured
Send Microsoft Edge browsing data to Microsoft 365 Analytics	Not configured
Telemetry proxy server	
Search	
Safe Search (mobile only)	User defined
Display web results in search	Not configured
Diacritics	Not configured
Automatic language detection	Not configured
Search location	Not configured
Indexer backoff	Not configured
Removable drive indexing	Not configured
Low disk space indexing	Not configured
Remote queries	Not configured
Start	
Start menu layout	<LayoutModificationTemplate xmlns:defaultlayout="http://schemas.microsoft.com/Start/2014/FullDefaultLayout" xmlns:start="http://schemas.microsoft.com/Start/2014/StartLayout" Version="1" xmlns="http://schemas.microsoft.com/Start/2014/LayoutModification" xmlns:taskbar="http://schemas.microsoft.com/Start/2014/TaskbarLayout"> <LayoutOptions StartTileGroupCellWidth="6" /> <DefaultLayoutOverride LayoutCustomizationRestrictionType="OnlySpecifiedGroups"> <StartLayoutCollection> <defaultlayout:StartLayout GroupCellWidth="6"> <start:Group Name="">

	<start:DesktopApplicationTile Size="2x2" Column="4" Row="0" DesktopApplicationID="Microsoft.Office.EXCEL.EXE.15" /> <start:DesktopApplicationTile Size="2x2" Column="2" Row="2" DesktopApplicationID="Microsoft.Office.POWERPNT.EXE.15" /> <start:DesktopApplicationTile Size="2x2" Column="0" Row="4" DesktopApplicationID="MSEdge" /> <start:DesktopApplicationTile Size="2x2" Column="0" Row="0" DesktopApplicationID="Microsoft.Office.OUTLOOK.EXE.15" /> <start:DesktopApplicationTile Size="2x2" Column="2" Row="4" DesktopApplicationID="Microsoft.Office.ONENOTE.EXE.15" /> <start:DesktopApplicationTile Size="2x2" Column="4" Row="4" DesktopApplicationID="com.squirrel.Teams.Teams" /> <start:DesktopApplicationTile Size="2x2" Column="2" Row="0" DesktopApplicationID="Microsoft.Office.WINWORD.EXE.15" /> <start:Tile Size="2x2" Column="0" Row="2" AppUserModelID="Microsoft.CompanyPortal_8wekyb3d8bbwe!App" /> <start:Tile Size="2x2" Column="4" Row="2" AppUserModelID="Microsoft.WindowsStore_8wekyb3d8bbwe!App" /> </start:Group> </defaultlayout:StartLayout> </StartLayoutCollection> </DefaultLayoutOverride> <CustomTaskbarLayoutCollection PinListPlacement="Replace"> <defaultlayout:TaskbarLayout> <taskbar:TaskbarPinList> <taskbar:DesktopApp DesktopApplicationID="Microsoft.Windows.Explorer"/> <taskbar:DesktopApp DesktopApplicationID="Microsoft.Office.OUTLOOK.EXE.15"/> <taskbar:DesktopApp DesktopApplicationID="MSEdge"/> </taskbar:TaskbarPinList> </defaultlayout:TaskbarLayout> </CustomTaskbarLayoutCollection> </LayoutModificationTemplate>
Pin websites to tiles in Start menu	
Unpin apps from task bar	Not configured
Fast user switching	Not configured
Most used apps	Not configured
Recently added apps	Not configured
Start screen mode	User defined
Recently opened items in Jump Lists	Not configured
App list	User defined
Power button	Not configured

User Tile	Not configured
Lock	Not configured
Sign out	Not configured
Shut Down	Not configured
Sleep	Not configured
Hibernate	Not configured
Switch Account	Not configured
Restart Options	Not configured
Documents on Start	Not configured
Downloads on Start	Not configured
File Explorer on Start	Not configured
HomeGroup on Start	Not configured
Music on Start	Not configured
Network on Start	Not configured
Personal folder on Start	Not configured
Pictures on Start	Not configured
Settings on Start	Not configured
Videos on Start	Not configured
Microsoft Defender SmartScreen	
SmartScreen for Microsoft Edge Legacy	Not configured
Malicious site access	Not configured
Unverified file download	Not configured
Windows Spotlight	
Windows Spotlight	Not configured
Windows Spotlight on lock screen	Not configured
Third-party suggestions in Windows Spotlight	Not configured
Consumer Features	Not configured
Windows Tips	Not configured

Windows Spotlight in action center	Not configured
Windows Spotlight personalization	Not configured
Windows welcome experience	Not configured
Apps suggestions in Ink workspace	Not configured
Microsoft Defender Antivirus	
Real-time monitoring	Not configured
Behavior monitoring	Not configured
Network Inspection System (NIS)	Not configured
Scan all downloads	Not configured
Configure low CPU priority for scheduled scans	Not configured
Catch-up quick scan	Not configured
Catch-up full scan	Not configured
Scan scripts loaded in Microsoft web browsers	Not configured
End-user access to Defender	Not configured
Security intelligence update interval (in hours)	Not configured
Monitor file and program activity	Not configured
Days before deleting quarantined malware	

CPU usage limit during a scan	
Scan archive file	Not configured
Scan incoming mail messages	Not configured
Scan removable drives during a full scan	Not configured
Scan mapped network drives during a full scan	Not configured
Scan files opened from network folders	Not configured
Cloud-delivered protection	Not configured
File Blocking Level	Not configured
Time extension for file scanning by the cloud	
Prompt users before sample submission	Not configured
Time to perform a daily quick scan	Not configured
Type of system scan to perform	Not configured
Detect potentially unwanted applications	Not configured
On Access Protection	Not configured
Actions on detected malware threats	Not configured
Microsoft Defender Antivirus Exclusions	
Files and folders to	

exclude from scans and real-time protection	
File extensions to exclude from scans and real-time protection	
Processes to exclude from scans and real-time protection	
Power Settings	
Battery	
Battery level to turn Energy Saver on	
Lid close (mobile only)	Not configured
Power button	Not configured
Sleep button	Not configured
Hybrid sleep	Not configured
Plugged In	
Battery level to turn Energy Saver on	
Lid close (mobile only)	Not configured
Power button	Not configured
Sleep button	Not configured
Hybrid sleep	Not configured

Table 98. Settings - Start-Menu-W10

Rule	Property	Value
Don't assign profile if	OS version	10.0.22000.100 to 10.0.22999.999

Table 99. Applicability Rules - Start-Menu-W10

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 100. Assignments - Start-Menu-W10

WDAC

Name	Value
Basics	
Name	WDAC

Description	WDAC Microsoft Rules Sets PS to restricted mode
Platform supported	Windows 10 and later
Profile type	Custom
Platform	Windows 10 and later
Scope tags	Default

Table 101. Basics - WDAC

Name	Value
OMA-URI Settings	
WDAC	
Name	WDAC
Description	
OMA-URI	./Vendor/MSFT/ApplicationControl/Policies/E39A37BC-41DA-4461-8D80-031640DC938F/Policy
Data type	Base64 (file)
Value	BwAAALw3muPaQWFEjYADFkDck4/k9wcuTBkgTbfJb0SmxaI0BASckAEAAAAEAAAAEgAAAAIA AAAAAAAAAAAKAEAAAAAMAAAAAQorBgEEAYI3TAMBAQAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAgAAACIAAABSAGUAZgByAGUAcwBoAFAAbwBsAGkAYwB5AC4AZQB4AGUAAAAAAAA AAAABiSgAACgAAAAAAAQAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAEAAAAFAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABAAAABg AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAcAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAAAAIAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAABAAAADAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAQAAAA4AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAE AAAAKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABAAAABAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAUAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAAAAGAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAABAAAABwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAQAAAAgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAAAAM AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABAAAADgAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAAAAD8nt49zKCRhrLTv5tziiBQyxp VTaLcrbVfP3LuF3ITeAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAgAAAA9vcXpDrZq93Izv3eHFBUYlNefRMH5jD5VEotFP6L8m4AAAAAAAAAAAAAAAAAqAAA

	ATQBpAGMAcgBvAHMAbwBmAHQAIABDAG8AcgBwAG8AcgBhAHQAaQBvAG4AAAAAAAAAA AAAAAAAAAABAAAAAwAAAAEAAAAKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAgAAAA8AAAAQAAAAgwAAAAAAAAAMgAAACAAAAAAAAAAAAAAAAAQA AAAAAAAACAAAAAAAAAAMAAAAAAAAABAAAAAAAAAAFAAAAAAAAAAYAAAAAAAAABwAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAwAAAAAAAADIAAA AoAAAAIAAAAAAAAAAkAAAAAAAAACgAAAAAAAALAAAAAAAAAAwAAAAAAAADQAAAAA AAAAOAAAAAAAAA8AAAAAAAAEAAAAAAAAAARAAAAAAAAAAAAAADAAAAAAAAAEA AAACAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAMAAAAUAAAAQQBsAGwA SABvAHMAdABJAGQAcwAAAAATAAAAHsAMAA0ADYAOABDADAAOAA1AC0AQwBBADUAQ gAtADEAMQBEADAALQBBAEYAMAA4AC0AMAAwADYAMAA5ADcAOQA3AEYAMABFADAAfQA AAAAALAAAAEUAbgB0AGUAcgBwAHIAaQBzAGUARABlAGYAaQBuAGUAZABDAGwAcwBJAGQ AAAAAAAAAAAABAAAAFAAAAFAAbwBsAGkAYwB5AEkAbgBmAG8AAAAAABYAAABJAG4AZgB vAHIAbQBhAHQAaQBvAG4AAAAAAAAABAAAAEkAZAAAAAAAAwAAABAAAAAxADIAMAAyAD IAMAAyADIAAAAAABQAAABQAG8AbABpAGMAeQBJAG4AZgBvAAAAAAAWAAAASQBuAGYA bwByAG0AYQB0AGkAbwBuAAAAAAAAAAgAAABOAGEAbQBlAAAAAAADAAAAMAAAAEQAZQ BmAGEAdQBsAHQATQBpAGMAcgBvAHMAbwBmAHQARQBuAGYAbwByAGMAZQBkAAAAAA ADAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAUAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAABgAAALw3muPaQWFEjYADFkDck4+8N5rj2kFhRI 2AAxZA3JOPAAAAAAcAAABiAAAAJQBPAFMARABSAEkAVgBFACUAXABQAHIAbwBnAHIAYQBt ACAARgBpAGwAZQBzAFwAYgBhAGMAawB1AHAALQByAGUAcwB0AG8AcgBlAFwAYgBhAGM AawB1AHAALgBiAGEAdAAAAAAAAABqAAAAJQBPAFMARABSAEkAVgBFACUAXABQAHIAbwBn AHIAYQBtACAARgBpAGwAZQBzAFwAYgBhAGMAawB1AHAALQByAGUAcwB0AG8AcgBlAFwAT gBFAFcAcgBlAHMAdABvAHIAZQAuAGIAYQB0AAAAAAAAAHAAAAAlAE8AUwBEAFIASQBWAE UAJQBcAFAAcgBvAGcAcgBhAG0AIABGAGkAbABlAHMAXABiAGEAYwBrAHUAcAAtAHIAZQBzA HQAbwByAGUAXAByAHUAbgAtAGkAbgB2AGkAcwBpAGIAbABlAC4AdgBiAHMAAAAAAAAAA AAAAAAACAAAAA==

Table 102. Settings - WDAC

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 103. Assignments - WDAC

Win10-DeviceConfig-Restrictions

Name	Value
Basics	
Name	Win10-DeviceConfig-Restrictions
Description	
Platform supported	Windows 10 and later
Profile type	Device restrictions
Version	1
Scope tags	Default

Table 104. Basics - Win10-DeviceConfig-Restrictions

Name	Value
App Store	
App store (mobile only)	Not configured
Auto-update apps from store	Not configured
Trusted app installation	Not configured
Developer unlock	Not configured
Shared user app data	Not configured
Use private store only	Not configured
Store originated app launch	Not configured
Install app data on system volume	Not configured
Install apps on system drive	Not configured
Game DVR (desktop only)	Not configured
Apps from store only	Not Configured
User control over installations	Not configured
Install apps with elevated privileges	Not configured
Startup apps	
Cellular and connectivity	
Data roaming	Not configured
VPN over the cellular network	Not configured
VPN roaming over the cellular network	Not configured
Connected devices service	Not configured
NFC	Not configured
Wi-Fi	Not configured
Automatically connect to Wi-Fi hotspots	Not configured
Manual Wi-Fi configuration	Not configured
Wi-Fi scan interval (mobile only)	
Bluetooth	
Bluetooth	Not configured
Bluetooth discoverability	Not configured
Bluetooth pre-pairing	Not configured
Bluetooth advertising	Not configured
Bluetooth proximal connections	Not configured
Bluetooth allowed services	
Cloud and Storage	
Microsoft account	Not configured
Non-Microsoft account	Not configured
Settings synchronization for Microsoft account	Not configured
Microsoft Account sign-in assistant	Not configured
Cloud Printer	
Printer discovery URL	
Printer access authority URL	
Azure native client app GUID	
Print service resource URI	
Maximum printers to query(Mobile only)	
Printer discovery service resource URI	
Control Panel and Settings	
Settings app	Not configured
System	Not configured

Power and sleep settings modification (desktop only)	Not configured
Devices	Not configured
Network and Internet	Not configured
Personalization	Not configured
Apps	Not configured
Accounts	Not configured
Time and Language	Not configured
System Time modification	Not configured
Region settings modification (desktop only)	Not configured
Language settings modification (desktop only)	Not configured
Gaming	Not configured
Ease of Access	Not configured
Privacy	Not configured
Update and Security	Not configured
Display	
Turn on GDI scaling for apps.	
Turn off GDI scaling for apps.	
General	
Screen capture (mobile only)	Not configured
Copy and paste (mobile only)	Not configured
Manual unenrollment	Not configured
Manual root certificate installation (mobile only)	Not configured
Camera	Not configured
OneDrive file sync	Not configured
Removable storage	Not configured
Geolocation	Not configured
Internet sharing	Not configured
Phone reset	Not configured
USB connection	Not configured
AntiTheft mode (mobile only)	Not configured
Cortana	Not configured
Voice recording (mobile only)	Not configured
Device name modification (mobile only)	Not configured
Add provisioning packages	Not configured
Remove provisioning packages	Not configured
Device discovery	Not configured
Task Switcher (mobile only)	Not configured
SIM card error dialog (mobile only)	Not configured
Ink Workspace	Not configured
Autopilot Reset	Not configured
Require users to connect to network during device setup	Not configured
Direct Memory Access	Not configured
End processes from Task Manager	Not configured
Locked Screen Experience	
Action center notifications (mobile only)	Not configured

Locked screen picture URL (Desktop only)	
User configurable screen timeout (mobile only)	Not configured
Cortana on locked screen (Desktop only)	Not configured
Toast notifications on locked screen	Not configured
Screen timeout (mobile only)	
Voice activate apps from locked screen	Not configured
Messaging	
Message sync (mobile only)	Not configured
MMS (mobile only)	Not configured
RCS (mobile only)	Not configured
Microsoft Edge Legacy (Version 45 and earlier)	
Use Microsoft Edge kiosk mode	No
Start experience	
Start Microsoft Edge with	Start pages in local app settings
Allow user to change Start pages	No
Allow web content on new Tab page	Yes
New Tab URL	
Allow Users to change Home button	No
Show First Run Experience page (Mobile only)	Yes
First Run Experience URL list location	
Allow pop-ups	Yes
Send intranet traffic to Internet Explorer	No
Enterprise mode site list location (Desktop only)	
Message when opening sites in Internet Explorer	Don't show message
Allow Microsoft compatibility list	Yes
Preload Start pages and new Tab page	Yes
Prelaunch Start pages and new Tab page	Yes
Favorites and search	
Show Favorites bar	On Start and new Tab pages
Allow changes to favorites	Yes
Favorites List	
Sync favorites between Microsoft browsers (Desktop only)	No
Default search engine	Not configured
Show search suggestions	Yes
Privacy and security	
Allow InPrivate browsing	Yes
Save browsing history	Yes
Clear browsing data on exit (Desktop only)	No
Sync browser settings between user's devices	Allow
Allow Password Manager	Yes
Cookies	Allow
Allow Autofill in forms	Yes
Send do-not-track headers	No
Show WebRTC localhost IP address	Yes
Allow live tile data collection	Yes

User can override certificate errors	Yes
Additional	
Allow Microsoft Edge browser (Mobile only)	Yes
Allow address bar dropdown	Yes
Allow full screen mode	Yes
Allow printing	Yes
Allow about flags page	Yes
Allow developer tools	Yes
Allow JavaScript	Yes
User can install extensions	Yes
Allow sideloading of developer extensions	Yes
Required extensions	
Network proxy	
Automatically detect proxy settings	Not configured
Use proxy script	Allow
Setup script address URL	
Use manual proxy server	Not configured
Address	
Port number	
Proxy exceptions	
Bypass proxy server for local address	Not configured
Password	
Password	Not configured
Required password type	Not configured
Minimum password length	
Number of sign-in failures before wiping device	
Maximum minutes of inactivity until screen locks	Not configured
Password expiration (days)	
Prevent reuse of previous passwords	
Require password when device returns from idle state (Mobile and Holographic)	Not configured
Simple passwords	Not configured
Automatic encryption during AADJ	Not configured
Federal Information Processing Standard (FIPS) policy	Not configured
Windows Hello device authentication	Not configured
Preferred Azure AD tenant domain	
Per-app privacy exceptions	
Exceptions	
Personalization	
Desktop background picture URL (Desktop only)	
Printer	
Printers	
Default printer	
Add new printers	Not configured
Privacy	

Privacy experience	Not configured
Input personalization	Not configured
Automatic acceptance of the pairing and privacy user consent prompts	Not configured
Publish user activities	Not configured
Local activities only	Not configured
Projection	
User input from wireless display receivers	Not configured
Projection to this PC	Not configured
Require PIN for pairing	Not configured
Reporting and Telemetry	
Share usage data	Not configured
Send Microsoft Edge browsing data to Microsoft 365 Analytics	Not configured
Telemetry proxy server	
Search	
Safe Search (mobile only)	User defined
Display web results in search	Not configured
Diacritics	Not configured
Automatic language detection	Not configured
Search location	Not configured
Indexer backoff	Not configured
Removable drive indexing	Not configured
Low disk space indexing	Not configured
Remote queries	Not configured
Start	
Start menu layout	
Pin websites to tiles in Start menu	
Unpin apps from task bar	Not configured
Fast user switching	Not configured
Most used apps	Not configured
Recently added apps	Not configured
Start screen mode	User defined
Recently opened items in Jump Lists	Not configured
App list	User defined
Power button	Not configured
User Tile	Not configured
Lock	Not configured
Sign out	Not configured
Shut Down	Not configured
Sleep	Not configured
Hibernate	Not configured
Switch Account	Not configured
Restart Options	Not configured
Documents on Start	Not configured
Downloads on Start	Not configured
File Explorer on Start	Not configured
HomeGroup on Start	Not configured
Music on Start	Not configured

Network on Start	Not configured
Personal folder on Start	Not configured
Pictures on Start	Not configured
Settings on Start	Not configured
Videos on Start	Not configured
Microsoft Defender SmartScreen	
SmartScreen for Microsoft Edge Legacy	Not configured
Malicious site access	Not configured
Unverified file download	Not configured
Windows Spotlight	
Windows Spotlight	Not configured
Windows Spotlight on lock screen	Not configured
Third-party suggestions in Windows Spotlight	Not configured
Consumer Features	Not configured
Windows Tips	Not configured
Windows Spotlight in action center	Not configured
Windows Spotlight personalization	Not configured
Windows welcome experience	Not configured
Apps suggestions in Ink workspace	Not configured
Microsoft Defender Antivirus	
Real-time monitoring	Not configured
Behavior monitoring	Not configured
Network Inspection System (NIS)	Not configured
Scan all downloads	Not configured
Configure low CPU priority for scheduled scans	Not configured
Catch-up quick scan	Not configured
Catch-up full scan	Not configured
Scan scripts loaded in Microsoft web browsers	Not configured
End-user access to Defender	Not configured
Security intelligence update interval (in hours)	Not configured
Monitor file and program activity	Not configured
Days before deleting quarantined malware	
CPU usage limit during a scan	
Scan archive file	Not configured
Scan incoming mail messages	Not configured
Scan removable drives during a full scan	Not configured
Scan mapped network drives during a full scan	Not configured
Scan files opened from network folders	Not configured
Cloud-delivered protection	Not configured
File Blocking Level	Not configured
Time extension for file scanning by the cloud	
Prompt users before sample submission	Not configured
Time to perform a daily quick scan	Not configured
Type of system scan to perform	Not configured
Detect potentially unwanted applications	Not configured
On Access Protection	Not configured
Actions on detected malware threats	Not configured
Microsoft Defender Antivirus Exclusions	

Files and folders to exclude from scans and real-time protection	
File extensions to exclude from scans and real-time protection	
Processes to exclude from scans and real-time protection	
Power Settings	
Battery	
Battery level to turn Energy Saver on	
Lid close (mobile only)	Not configured
Power button	Not configured
Sleep button	Not configured
Hybrid sleep	Not configured
Plugged In	
Battery level to turn Energy Saver on	
Lid close (mobile only)	Not configured
Power button	Not configured
Sleep button	Not configured
Hybrid sleep	Not configured

Table 105. Settings - Win10-DeviceConfig-Restrictions

Group	Filter	Filter mode
Included Groups		
All users	None	None
All devices	None	None

Table 106. Assignments - Win10-DeviceConfig-Restrictions

WindowsDeliveryOptimization

Name	Value
Basics	
Name	WindowsDeliveryOptimization
Description	Configure Branch Cache for Windows
Platform supported	Windows 10 and later
Profile type	Delivery Optimization
Version	1
Scope tags	Default

Table 107. Basics - WindowsDeliveryOptimization

Name	Value
Delivery Optimization	
Download mode	HTTP blended with peering behind same NAT (1)
Restrict Peer Selection	Subnet mask
Bandwidth	
Bandwidth optimization type	Percentage
Maximum foreground download bandwidth (in %)	70

Maximum background download bandwidth (in %)	25
Delay background HTTP download (in seconds)	60
Delay foreground HTTP download (in seconds)	60
Caching	
Minimum RAM required for peer caching (in GB)	4
Minimum disk size required for peer caching (in GB)	32
Minimum content file size for peer caching (in MB)	10
Minimum battery level required to upload (in %)	40
Modify cache drive	
Maximum cache age (in days)	7
Maximum cache size type	Percentage
Maximum cache size (in %)	20
VPN peer caching	Enabled
Local Server Caching	
Cache server host names	
Delay foreground download Cache Server fallback (in seconds)	0
Delay background download Cache Server fallback (in seconds)	0

Table 108. Settings - WindowsDeliveryOptimization

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 109. Assignments - WindowsDeliveryOptimization

Windows-ESP

Name	Value
Basics	
Name	Windows-ESP
Description	Custom ESP Settings
Platform supported	Windows 10 and later
Profile type	Custom
Platform	Windows 10 and later
Scope tags	Default

Table 110. Basics - Windows-ESP

Name	Value
OMA-URI Settings	
UserESP	
Name	UserESP
Description	

OMA-URI	./Device/Vendor/MSFT/DMClient/Provider/MS DM Server/FirstSyncStatus/SkipUserStatusPage
Data type	Boolean
Value	True

Table 111. Settings - Windows-ESP

Group	Filter	Filter mode
Included Groups		
Autopilot-devices	None	None

Table 112. Assignments - Windows-ESP

Windows-LAPS-User

Name	Value
Basics	
Name	Windows-LAPS-User
Description	Creates a new user to be used with LAPS
Platform supported	Windows 10 and later
Profile type	Custom
Platform	Windows 10 and later
Scope tags	Default

Table 113. Basics - Windows-LAPS-User

Name	Value
OMA-URI Settings	
Create-User	
Name	Create-User
Description	Create lapsadmin and set password
OMA-URI	./Device/Vendor/MSFT/Accounts/Users/lapsadmin/Password
Data type	String
Value	%JGy8ld2_^]2h%yy-n0o
Add-to-group	
Name	Add-to-group
Description	Add to admins
OMA-URI	./Device/Vendor/MSFT/Accounts/Users/lapsadmin/LocalUserGroup
Data type	Integer
Value	2

Table 114. Settings - Windows-LAPS-User

Group	Filter	Filter mode
Included Groups		
All devices	None	None

Table 115. Assignments - Windows-LAPS-User

Winget Custom Policy

Name	Value
Basics	
Name	Winget Custom Policy

Description	All Current Winget Settings
Platform supported	Windows 10 and later
Profile type	Custom
Platform	Windows 10 and later
Scope tags	Default

Table 116. Basics - Winget Custom Policy

Name	Value
OMA-URI Settings	
Enable Default Source	
Name	Enable Default Source
Description	Enabled
OMA-URI	./Device/Vendor/MSFT/Policy/Config/DesktopAppInstaller/EnableDefaultSource
Data type	String
Value	UEdWdVlXSnNaV1F2UGc9PQ==
Enable Local Manifest Files	
Name	Enable Local Manifest Files
Description	Enabled
OMA-URI	./Device/Vendor/MSFT/Policy/Config/DesktopAppInstaller/EnableLocalManifestFiles
Data type	String
Value	UEdWdVlXSnNaV1F2UGc9PQ==
Enable Hash Override	
Name	Enable Hash Override
Description	Enabled
OMA-URI	./Device/Vendor/MSFT/Policy/Config/DesktopAppInstaller/EnableHashOverride
Data type	String
Value	UEdWdVlXSnNaV1F2UGc9PQ==
Enable Microsoft Store Source	
Name	Enable Microsoft Store Source
Description	Enabled
OMA-URI	./Device/Vendor/MSFT/Policy/Config/DesktopAppInstaller/EnableMicrosoftStoreSource
Data type	String
Value	UEdWdVlXSnNaV1F2UGc9PQ==
Enable MS App Installer Protocol	
Name	Enable MS App Installer Protocol
Description	Enabled

OMA-URI	./Device/Vendor/MSFT/Policy/Config/DesktopAppInstaller/EnableMSAppInstallerProtocol
Data type	String
Value	UEdWdVlXSnNaV1F2UGc9PQ==
Enable Settings	
Name	Enable Settings
Description	Enabled
OMA-URI	./Device/Vendor/MSFT/Policy/Config/DesktopAppInstaller/EnableSettings
Data type	String
Value	UEdScGMyRmliR1ZrTHo0PQ==
Enable Experimental Features	
Name	Enable Experimental Features
Description	Disabled
OMA-URI	./Device/Vendor/MSFT/Policy/Config/DesktopAppInstaller/EnableExperimentalFeatures
Data type	String
Value	UEdScGMyRmliR1ZrTHo0PQ==
Enable App Installer	
Name	Enable App Installer
Description	Enabled
OMA-URI	./Device/Vendor/MSFT/Policy/Config/DesktopAppInstaller/EnableAppInstaller
Data type	String
Value	UEdWdVlXSnNaV1F2UGc9PQ==
EnableBypassCertificatePinningForMicrosoftStore	
Name	EnableBypassCertificatePinningForMicrosoftStore
Description	Enabled
OMA-URI	./Device/Vendor/MSFT/Policy/Config/DesktopAppInstaller/EnableBypassCertificatePinningForMicrosoftStore <enabled/>
Data type	String
Value	UEdWdVlXSnNaV1F2UGc9PQ==
EnableLocalArchiveMalwareScanOverride	
Name	EnableLocalArchiveMalwareScanOverride
Description	Disabled
OMA-URI	./Device/Vendor/MSFT/Policy/Config/DesktopAppInstaller/EnableLocalArchiveMalwareScanOverride
Data type	String
Value	UEM5a2FYTmhZbXhsWkQ0PQ==

Table 117. Settings - Winget Custom Policy

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 118. Assignments - Winget Custom Policy

Enrollment restrictions

Enrollment Restrictions

All users and all devices

Name	Value
Basics	
Name	All users and all devices
Description	This is the default Device Type Restriction applied with the lowest priority to all users regardless of group membership.
Profile type	Enrollment device platform restrictions
Platform	All Platforms

Table 119. Basics - All users and all devices

Name	Value
Platform settings	
Android enterprise	
Type	Android enterprise
Platform	Allow
versions	
Personally owned	Block
Device manufacturer	
Android device administrator	
Type	Android device administrator
Platform	Block
versions	
Personally owned	Allow
Device manufacturer	Restriction not supported
iOS/iPadOS	
Type	iOS/iPadOS
Platform	Allow
versions	
Personally owned	Allow
Device manufacturer	Restriction not supported
macOS	
Type	macOS
Platform	Allow
versions	Restriction not supported
Personally owned	Block
Device manufacturer	Restriction not supported
Windows	

Type	Windows
Platform	Allow
versions	
Personally owned	Block
Device manufacturer	Restriction not supported

Table 120. Settings - All users and all devices

Group	Filter	Filter mode
Included Groups		
All devices	None	None

Table 121. Assignments - All users and all devices

All users and all devices

Name	Value
Basics	
Name	All users and all devices
Description	This is the default Device Limit Restriction applied with the lowest priority to all users regardless of group membership.

Table 122. Basics - All users and all devices

Name	Value
Device limit	
Device limit	15
Priority	0

Table 123. Settings - All users and all devices

Group	Filter	Filter mode
Included Groups		
All devices	None	None

Table 124. Assignments - All users and all devices

Update rings for Windows 10 and later

Update Policies

Broad Ring

Name	Value
Basics	
Name	Broad Ring
Description	Semi Annual Channel
Platform supported	Windows 10 and later
Profile type	Software Updates
Version	1
Scope tags	Default

Table 125. Basics - Broad Ring

Name	Value

Settings	
Update settings	
Microsoft product updates	Allow
Windows drivers	Allow
Quality update deferral period (days)	10
Feature update deferral period (days)	0
Upgrade Windows 10 devices to Latest Windows 11 release	Yes
Set feature update uninstall period (2 - 60 days)	10
Enable pre-release builds	Not configured
User experience settings	
Automatic update behavior	Auto install at maintenance time
Active hours start	6 AM
Active hours end	6 PM
Restart checks	Allow
Option to pause Windows updates	Disable
Option to check for Windows updates	Enable
Change notification update level	Use the default Windows Update notifications
Use deadline settings	Allow
Deadline for feature updates	10
Deadline for quality updates	10
Grace period	5
Auto reboot before deadline	Yes

Table 126. Settings - Broad Ring

iOS Update Policy

Name	Value
Basics	
Name	iOS Update Policy
Description	
Platform supported	iOS/iPadOS
Profile type	iOS Update policy
Version	1
Scope tags	Default

Table 127. Basics - iOS Update Policy

Name	Value
Settings	
Update to install	Install iOS/iPadOS (Selected version is no longer supported)
Schedule type	Update at next check-in
Time window	

Table 128. Settings - iOS Update Policy

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 129. Assignments - iOS Update Policy

Pilot Ring

Name	Value
Basics	
Name	Pilot Ring
Description	Insider Slow
Platform supported	Windows 10 and later
Profile type	Software Updates
Version	1
Scope tags	Default

Table 130. Basics - Pilot Ring

Name	Value
Settings	
Update settings	
Microsoft product updates	Allow
Windows drivers	Allow
Quality update deferral period (days)	0
Feature update deferral period (days)	0
Upgrade Windows 10 devices to Latest Windows 11 release	No
Set feature update uninstall period (2 - 60 days)	10
Enable pre-release builds	Enable
Select pre-release channel	Beta Channel
User experience settings	
Automatic update behavior	Auto install at maintenance time
Active hours start	8 AM
Active hours end	5 PM
Restart checks	Allow
Option to pause Windows updates	Disable
Option to check for Windows updates	Enable
Change notification update level	Use the default Windows Update notifications
Use deadline settings	Allow
Deadline for feature updates	10
Deadline for quality updates	10
Grace period	5
Auto reboot before deadline	Yes

Table 131. Settings - Pilot Ring

Preview Ring

Name	Value
Basics	
Name	Preview Ring
Description	Insider Fast
Platform supported	Windows 10 and later

Profile type	Software Updates
Version	1
Scope tags	Default

Table 132. Basics - Preview Ring

Name	Value
Settings	
Update settings	
Microsoft product updates	Allow
Windows drivers	Allow
Quality update deferral period (days)	7
Feature update deferral period (days)	0
Upgrade Windows 10 devices to Latest Windows 11 release	No
Set feature update uninstall period (2 - 60 days)	10
Enable pre-release builds	Enable
Select pre-release channel	Windows Insider - Release Preview
User experience settings	
Automatic update behavior	Auto install at maintenance time
Active hours start	8 AM
Active hours end	5 PM
Restart checks	Allow
Option to pause Windows updates	Disable
Option to check for Windows updates	Enable
Change notification update level	Use the default Windows Update notifications
Use deadline settings	Allow
Deadline for feature updates	10
Deadline for quality updates	10
Grace period	5
Auto reboot before deadline	Yes

Table 133. Settings - Preview Ring

VIP Channel

Name	Value
Basics	
Name	VIP Channel
Description	Semi Annual with Deferral
Platform supported	Windows 10 and later
Profile type	Software Updates
Version	1
Scope tags	Default

Table 134. Basics - VIP Channel

Name	Value
Settings	
Update settings	
Microsoft product updates	Allow

Windows drivers	Allow
Quality update deferral period (days)	30
Feature update deferral period (days)	180
Upgrade Windows 10 devices to Latest Windows 11 release	No
Set feature update uninstall period (2 - 60 days)	60
Enable pre-release builds	Not configured
User experience settings	
Automatic update behavior	Auto install at maintenance time
Active hours start	8 AM
Active hours end	5 PM
Restart checks	Allow
Option to pause Windows updates	Enable
Option to check for Windows updates	Enable
Change notification update level	Use the default Windows Update notifications
Use deadline settings	Not configured
Deadline for feature updates	
Deadline for quality updates	
Grace period	

Table 135. Settings - VIP Channel

Scripts

Scripts (PowerShell)

Backup Script

Name	Value
Basics	
Name	Backup Script
Description	Configures Backup Script scheduled task
Profile type	PowerShell script
Scope tags	Default

Table 136. Basics - Backup Script

Name	Value
Script settings	
PowerShell script	userbackup.ps1
Run this script using the logged on credentials	No
Enforce script signature check	No
Run script in 64 bit PowerShell Host	Yes

Table 137. Settings - Backup Script

userbackup.ps1

```
$DirectoryToCreate = $env:ProgramFiles+"\backup-restore"
if (-not (Test-Path -LiteralPath $DirectoryToCreate)) {

    try {
        New-Item -Path $DirectoryToCreate -ItemType Directory -ErrorAction Stop
| Out-Null #-Force
```

```
    }
    catch {
        Write-Error -Message "Unable to create directory '$DirectoryToCreate'.
Error was: $_" -ErrorAction Stop
    }
    "Successfully created directory '$DirectoryToCreate'."

}
else {
    "Directory already existed"
}

##Download Backup Script
$backupurl="https://raw.githubusercontent.com/andrew-s-
taylor/public/main/Batch%20Scripts/backup.bat"
$backupscript = $DirectoryToCreate+"\backup.bat"
Invoke-WebRequest -Uri $backupurl -OutFile $backupscript -UseBasicParsing

##Download Restore Script
$restoreurl="https://raw.githubusercontent.com/andrew-s-
taylor/public/main/Batch%20Scripts/NEWrestore.bat"
$restorescript = $DirectoryToCreate+"\restore.bat"
Invoke-WebRequest -Uri $restoreurl -OutFile $restorescript -UseBasicParsing

##Download Silent Launch Script
$content = @"
Set WshShell = CreateObject("WScript.Shell")
WshShell.RUN "cmd /c c:\PROGRA~1\backup-restore\backup.bat", 0
"@

$launchscript = $DirectoryToCreate+"\run-invisible.vbs"
$content | Out-File $launchscript -UseBasicParsing



##Create scheduled task
# Create a new task action
$taskAction = New-ScheduledTaskAction -Execute 'C:\Program Files\backup-
restore\run-invisible.vbs'

##Create Trigger (login)
$taskTrigger = New-ScheduledTaskTrigger -AtLogOn

# Register the new PowerShell scheduled task

#Name it
$taskName = "UserBackup"

#Describe it
$description = "Backs up User profile to OneDrive"

# Register it
Register-ScheduledTask `
    -TaskName $taskName `
    -Action $taskAction `
    -Trigger $taskTrigger `
    -Description $description
```

Table 138. PowerShell script - Backup Script

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 139. Assignments - Backup Script

Device Configuration Script

Name	Value
Basics	
Name	Device Configuration Script
Description	Configures Baseline Device Settings
Profile type	PowerShell script
Scope tags	Default

Table 140. Basics - Device Configuration Script

Name	Value
Script settings	
PowerShell script	device-config.ps1
Run this script using the logged on credentials	No
Enforce script signature check	No
Run script in 64 bit PowerShell Host	Yes

Table 141. Settings - Device Configuration Script

device-config.ps1

```
    #requires -version 2
    <#
    .SYNOPSIS
      Sets all config for a new build

    .DESCRIPTION
      Sets the following:
      Configured MS OneDrive
      Allows Printer installs
      Disable FastBoot
      Set OneDrive Known Folder Move
      Configures background image


    .INPUTS
     $regpath - The full registry path
     $regname - The name of the key
     $regvalue - The value of the key
     $regtype - either STRING or DWORD

    .OUTPUTS
      Log file stored in C:\Windows\Temp\build-device.log>

    .NOTES
      Version:        1.0
      Author:         Andrew Taylor
      Creation Date:  11/08/2022
      Purpose/Change: Initial script development

    .EXAMPLE
```

```
      addregkey($path, "Test", "1", "DWORD")
    #>

    #-----------------------------------------------------------[Initialisations]-
-----------------------------------------------------------

    #Set Error Action to Silently Continue
    $ErrorActionPreference = "SilentlyContinue"


    #-----------------------------------------------------------[Declarations]---
-----------------------------------------------------------

    #Script Version
    $sScriptVersion = "1.0"

    #Log File Info
    $sLogPath = "C:\Windows\Temp\build-device.log"

    #-----------------------------------------------------------[Configurables]--
-----------------------------------------------------------
    ################################################### SET THESE FOR EACH CLIENT
################################################


    ##No special characters
    $clientname = "DeployIntune"


    ###################### DO NOT EDIT BELOW HERE WITHOUT COMMENTING AND GIT
CHANGE#################################################
    #-----------------------------------------------------------[Functions]-----
-----------------------------------------------------------

    start-transcript -path $sLogPath



    #-----------------------------------------------------------[Execution]-----
-----------------------------------------------------------

    ## Configure OneDrive
    write-host "Configuring OneDrive"
    $registryPath = "HKLM:\SOFTWARE\Policies\Microsoft\OneDrive"
    $Name = "SilentAccountConfig"
    $value = "1"
    $Type = "DWORD"
    IF(!(Test-Path $registryPath))
    {
    New-Item -Path $registryPath -Force | Out-Null
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}
    ELSE {
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}

    $registryPath = "HKLM:\SOFTWARE\Policies\Microsoft\OneDrive"
    $Name = "FilesOnDemandEnabled"
    $value = "1"
```

```
    $Type = "DWORD"
    IF(!(Test-Path $registryPath))
    {
    New-Item -Path $registryPath -Force | Out-Null
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}
    ELSE {
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}
    #--------------------------------------------------------------------------
----------------------------------------------------


    ## Allow Printer Installs

    write-host "Configuring Printers"
    $registryPath =
"HKLM:\Software\Policies\Microsoft\Windows\DriverInstall\Restrictions"
    $Name = "AllowUserDeviceClasses"
    $value = "1"
    $Type = "DWORD"
    IF(!(Test-Path $registryPath))
    {
    New-Item -Path $registryPath -Force | Out-Null
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}
    ELSE {
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}


    $registryPath =
"HKLM:\Software\Policies\Microsoft\Windows\DriverInstall\Restrictions\AllowUserD
eviceClasses"
    $Name = "{4658ee7e-f050-11d1-b6bd-00c04fa372a7}"
    $value = ""
    $Type = "String"
    IF(!(Test-Path $registryPath))
    {
    New-Item -Path $registryPath -Force | Out-Null
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}
    ELSE {
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}


    $registryPath =
"HKLM:\Software\Policies\Microsoft\Windows\DriverInstall\Restrictions\AllowUserD
eviceClasses"
    $Name = "{4d36e979-e325-11ce-bfc1-08002be10318}"
    $value = ""
    $Type = "String"
    IF(!(Test-Path $registryPath))
    {
    New-Item -Path $registryPath -Force | Out-Null
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}
    ELSE {
```

```
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}

    #------------------------------------------------------------------------
----------------------------------------------------


    ## Disable FastBoot
    write-host "Disable FastBoot"
    $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Control\Session
Manager\Power"
    $Name = "HiberbootEnabled"
    $value = "0"
    $Type = "DWORD"
    IF(!(Test-Path $registryPath))
    {
    New-Item -Path $registryPath -Force | Out-Null
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}
    ELSE {
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}

    #------------------------------------------------------------------------
----------------------------------------------------

    #------------------------------------------------------------------------
----------------------------------------------------
    ###Additional Security Keys

    ## Set Login Cache to One
    write-host "Configuring Cached Count"
    $registryPath = "HKLM:\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon"
    $Name = "CachedLogonsCount"
    $value = "1"
    $Type = "string"
    IF(!(Test-Path $registryPath))
    {
    New-Item -Path $registryPath -Force | Out-Null
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}
    ELSE {
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}


    ## Set DLLSearch to value of 1
    write-host "Configuring DLL Search"
    $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager"
    $Name = "CWDIllegalInDllSearch"
    $value = "1"
    $Type = "DWORD"
    IF(!(Test-Path $registryPath))
    {
    New-Item -Path $registryPath -Force | Out-Null
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}
    ELSE {
```

```
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}

    ## Enable Cert Padding Check for Wintrust 64-bit key
    write-host "Enable Cert Padding Check for Wintrust 64-bit key"
    $registryPath = "HKLM:\Software\Microsoft\Cryptography\Wintrust\Config"
    $Name = "EnableCertPaddingCheck"
    $value = "1"
    $Type = "DWORD"
    IF(!(Test-Path $registryPath))
    {
    New-Item -Path $registryPath -Force | Out-Null
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}
    ELSE {
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}

    ## Enable Cert Padding Check for Wintrust 32-bit key
    write-host "Enable Cert Padding Check for Wintrust 32-bit key"
    $registryPath =
"HKLM:\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config"
    $Name = "EnableCertPaddingCheck"
    $value = "1"
    $Type = "DWORD"
    IF(!(Test-Path $registryPath))
    {
    New-Item -Path $registryPath -Force | Out-Null
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}
    ELSE {
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}

    #-------------------------------------------------------------------------
-------------------------------------------------------


    ##Add Build Reg Keys
    write-host "Adding Reg Keys"
    $registryPath = "HKLM:\Software\BuildDetails"

    $CurrentComputerName = (Get-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName").ComputerName
    $major = (Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows
NT\CurrentVersion").CurrentMajorVersionNumber
    $version = (Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows
NT\CurrentVersion").ReleaseId
    $build = (Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows
NT\CurrentVersion").CurrentBuildNumber
    $release = (Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows
NT\CurrentVersion").UBR
    $edition = (Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows
NT\CurrentVersion").EditionID
    $installationtype = (Get-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion").InstallationType
    $productname = (Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows
NT\CurrentVersion").ProductName
```

```
    $fullversion = $major + ".0." + $build + "." + $release
    $fulledition = $productname + " " + $edition


    $Name1 = "WinVersion"
    $value1 = $fullversion
    $Name2 = "OS"
    $value2 = $fulledition
    $Name4 = "Client"
    $value4 = $clientname
    $Name6 = "DatePCBuilt"
    $value6 = get-date
    $Name7 = "Serial"
    $serial = Get-WmiObject win32_bios
    $value7 = $serial.SerialNumber
    $Name8 = "PCName"
    $value8 = $CurrentComputerName


    IF(!(Test-Path $registryPath))

      {

        New-Item -Path $registryPath -Force | Out-Null

        New-ItemProperty -Path $registryPath -Name $Name1 -Value $value1 -
PropertyType String -Force | Out-Null
        New-ItemProperty -Path $registryPath -Name $Name2 -Value $value2 -
PropertyType String -Force | Out-Null
        New-ItemProperty -Path $registryPath -Name $Name4 -Value $value4 -
PropertyType String -Force | Out-Null
        New-ItemProperty -Path $registryPath -Name $Name6 -Value $value6 -
PropertyType String -Force | Out-Null
        New-ItemProperty -Path $registryPath -Name $Name7 -Value $value7 -
PropertyType String -Force | Out-Null
        New-ItemProperty -Path $registryPath -Name $Name8 -Value $value8 -
PropertyType String -Force | Out-Null
        }

     ELSE {

        New-ItemProperty -Path $registryPath -Name $Name1 -Value $value1 -
PropertyType String -Force | Out-Null
        New-ItemProperty -Path $registryPath -Name $Name2 -Value $value2 -
PropertyType String -Force | Out-Null
        New-ItemProperty -Path $registryPath -Name $Name4 -Value $value4 -
PropertyType String -Force | Out-Null
        New-ItemProperty -Path $registryPath -Name $Name6 -Value $value6 -
PropertyType String -Force | Out-Null
        New-ItemProperty -Path $registryPath -Name $Name7 -Value $value7 -
PropertyType String -Force | Out-Null
        New-ItemProperty -Path $registryPath -Name $Name8 -Value $value8 -
PropertyType String -Force | Out-Null

        }
```

```
    #-------------------------------------------------------------------------
-----------------------------------------------------

    ##Set Background
    ##Include File Extension:


    write-host "Download Desktop Images"
    #Open the folder en Windows Explorer under
C:\Users\USERNAME\AppData\Roaming\CustomerXXXX

###############################################################################
########
    $path = [Environment]::GetFolderPath('ApplicationData') + "\" + $clientname

    If(!(test-path $path))
    {
          New-Item -ItemType Directory -Force -Path $path
    }

###############################################################################
########

    $newpath = "c:\Windows\Web\Wallpaper"

    #Save the bas64 to image file

###############################################################################
########
    $bytes = [System.Convert]::FromBase64String("IMG BASE 64 HERE")
    $file = "C:\Windows\Web\wallpaper\custombackground.jpg"

    [System.IO.File]::WriteAllBytes($file, $bytes)


###############################################################################
########


    write-host "Set Lockscreen"

    $registryPath = "HKLM:\SOFTWARE\Policies\Microsoft\Windows\Personalization"
    $img =  "C:\Windows\Web\Wallpaper\custombackground.jpg"
    $Name = "LockScreenImage"
    $value = "1"
    $Type = "String"
    IF(!(Test-Path $registryPath))
    {
    New-Item -Path $registryPath -Force | Out-Null
    New-ItemProperty -Path $registryPath -Name $Name -Value $img `
    -PropertyType $Type -Force | Out-Null}
    ELSE {
    New-ItemProperty -Path $registryPath -Name $Name -Value $img `
    -PropertyType $Type -Force | Out-Null}
    $RegKeyPath =
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\PersonalizationCSP"
    $DesktopPath = "DesktopImagePath"
    $DesktopStatus = "DesktopImageStatus"
    $DesktopUrl = "DesktopImageUrl"
```

```
    $StatusValue = "1"

    New-ItemProperty -Path $RegKeyPath -Name $DesktopStatus -Value $StatusValue
-PropertyType DWORD -Force
    New-ItemProperty -Path $RegKeyPath -Name $DesktopPath -Value $img -
PropertyType STRING -Force
    New-ItemProperty -Path $RegKeyPath -Name $DesktopUrl -Value $img -
PropertyType STRING -Force

    #-------------------------------------------------------------------------
-----------------------------------------------------

    ## Stop Logging
    stop-transcript
```

Table 142. PowerShell script - Device Configuration Script

Group	Filter	Filter mode
Included Groups		
Autopilot-Devices	None	None

Table 143. Assignments - Device Configuration Script

Disable running or installing downloaded software with invalid signature

Name	Value
Basics	
Name	Disable running or installing downloaded software with invalid signature
Description	
Profile type	PowerShell script
Scope tags	Default

Table 144. Basics - Disable running or installing downloaded software with invalid signature

Name	Value
Script settings	
PowerShell script	Disablerunningdownloadedsoftwarewithinvalidsignature.ps1
Run this script using the logged on credentials	No
Enforce script signature check	No
Run script in 64 bit PowerShell Host	No

Table 145. Settings - Disable running or installing downloaded software with invalid signature

Disablerunningdownloadedsoftwarewithinvalidsignature.ps1

```
$registryPath = "HKLM:SOFTWARE\Policies\Microsoft\Internet Explorer\Download"

$Name = "RunInvalidSignatures"
$value = "0"

IF(!(Test-Path $registryPath))

  {
    New-Item -Path $registryPath -Force | Out-Null
```

```
    New-ItemProperty -Path $registryPath -Name $name -Value $value -
PropertyType String -Force | Out-Null}

 ELSE {
    New-ItemProperty -Path $registryPath -Name $name -Value $value -
PropertyType string -Force | Out-Null}
```

Table 146. PowerShell script - Disable running or installing downloaded software with invalid signature

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 147. Assignments - Disable running or installing downloaded software with invalid signature

MDE-Active-Tag

Name	Value
Basics	
Name	MDE-Active-Tag
Description	
Profile type	PowerShell script
Scope tags	Default

Table 148. Basics - MDE-Active-Tag

Name	Value
Script settings	
PowerShell script	MDE-Active-Tag.ps1
Run this script using the logged on credentials	No
Enforce script signature check	No
Run script in 64 bit PowerShell Host	No

Table 149. Settings - MDE-Active-Tag

MDE-Active-Tag.ps1

```
$registryPath = "HKLM:SOFTWARE\Policies\Microsoft\Windows Advanced Threat
Protection\DeviceTagging"

$Name = "Group"
$value = "MDE-Active"

IF(!(Test-Path $registryPath))

  {
    New-Item -Path $registryPath -Force | Out-Null
    New-ItemProperty -Path $registryPath -Name $name -Value $value -
PropertyType String -Force | Out-Null}

 ELSE {
    New-ItemProperty -Path $registryPath -Name $name -Value $value -
PropertyType string -Force | Out-Null}
```

Table 150. PowerShell script - MDE-Active-Tag

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 151. Assignments - MDE-Active-Tag

MDE-Advanced

Name	Value
Basics	
Name	MDE-Advanced
Description	
Profile type	PowerShell script
Scope tags	Default

Table 152. Basics - MDE-Advanced

Name	Value
Script settings	
PowerShell script	MDE-Advanced.ps1
Run this script using the logged on credentials	No
Enforce script signature check	No
Run script in 64 bit PowerShell Host	No

Table 153. Settings - MDE-Advanced

MDE-Advanced.ps1

```
#Advanced Settings
Set-MpPreference -DisableTlsParsing $False
Set-MpPreference -AllowSwitchToAsyncInspection $true
Set-MpPreference -DisableBlockAtFirstSeen $False
Set-MpPreference -EnableDnsSinkhole $true
Set-MpPreference -EnableFileHashComputation $true
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name
"RunAsPPL" -Value 1 -Force
```

Table 154. PowerShell script - MDE-Advanced

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 155. Assignments - MDE-Advanced

MDE-WDCG-Remote

Name	Value
Basics	
Name	MDE-WDCG-Remote
Description	
Profile type	PowerShell script
Scope tags	Default

Table 156. Basics - MDE-WDCG-Remote

Name	Value
Script settings	
PowerShell script	DefenderRemoteCredentialGuard.ps1

Run this script using the logged on credentials	No
Enforce script signature check	No
Run script in 64 bit PowerShell Host	No

Table 157. Settings - MDE-WDCG-Remote

DefenderRemoteCredentialGuard.ps1

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v DisableRestrictedAdmin /d
0 /t REG_DWORD
```

Table 158. PowerShell script - MDE-WDCG-Remote

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 159. Assignments - MDE-WDCG-Remote

Remove Bloat

Name	Value
Basics	
Name	Remove Bloat
Description	Removes bloat from Win10 machine
Profile type	PowerShell script
Scope tags	Default

Table 160. Basics - Remove Bloat

Name	Value
Script settings	
PowerShell script	RemoveBloat.ps1
Run this script using the logged on credentials	No
Enforce script signature check	No
Run script in 64 bit PowerShell Host	Yes

Table 161. Settings - Remove Bloat

RemoveBloat.ps1

```
$DebloatFolder = "C:\ProgramData\Debloat"
If (Test-Path $DebloatFolder) {
    Write-Output "$DebloatFolder exists. Skipping."
}
Else {
    Write-Output "The folder '$DebloatFolder' doesn't exist. This folder will
be used for storing logs created after the script runs. Creating now."
    Start-Sleep 1
    New-Item -Path "$DebloatFolder" -ItemType Directory
    Write-Output "The folder $DebloatFolder was successfully created."
}

$templateFilePath = "C:\ProgramData\Debloat\removebloat.ps1"

Invoke-WebRequest `
-Uri "https://raw.githubusercontent.com/andrew-s-taylor/public/main/De-
Bloat/RemoveBloat.ps1" `
-OutFile $templateFilePath `
-UseBasicParsing `
```

```
-Headers @{"Cache-Control"="no-cache"}

invoke-expression -Command $templateFilePath
```

Table 162. PowerShell script - Remove Bloat

Group	Filter	Filter mode
Included Groups		
Autopilot-Devices	None	None

Table 163. Assignments - Remove Bloat

Require domain users to elevate when setting a network's location

Name	Value
Basics	
Name	Require domain users to elevate when setting a network's location
Description	
Profile type	PowerShell script
Scope tags	Default

Table 164. Basics - Require domain users to elevate when setting a network's location

Name	Value
Script settings	
PowerShell script	RequireAdminforNetworkChange.ps1
Run this script using the logged on credentials	No
Enforce script signature check	No
Run script in 64 bit PowerShell Host	No

Table 165. Settings - Require domain users to elevate when setting a network's location

RequireAdminforNetworkChange.ps1
`Set-Itemproperty "hklm:\SOFTWARE\Policies\Microsoft\Windows\Network Connections" -Name "NC_StdDomainUserSetLocation" -Value 1`

Table 166. PowerShell script - Require domain users to elevate when setting a network's location

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 167. Assignments - Require domain users to elevate when setting a network's location

User Configuration Script

Name	Value
Basics	
Name	User Configuration Script
Description	Configures Baseline User Settings
Profile type	PowerShell script
Scope tags	Default

Table 168. Basics - User Configuration Script

Name	Value

Script settings	
PowerShell script	user-config.ps1
Run this script using the logged on credentials	Yes
Enforce script signature check	No
Run script in 64 bit PowerShell Host	Yes

Table 169. Settings - User Configuration Script

user-config.ps1

```
    #requires -version 2
    <#
    .SYNOPSIS
      Configures User Settings

    .DESCRIPTION
      Configures:
      ADAL for OneDrive
      Unpins MS Store
      Sets background



    .INPUTS
     $regpath - The full registry path
     $regname - The name of the key
     $regvalue - The value of the key
     $regtype - either STRING or DWORD

    .OUTPUTS
      Log file stored in C:\Windows\Temp\build-user.log>

    .NOTES
      Version:        1.0
      Author:         Andrew S Taylor
      Creation Date:  11/08/2022
      Purpose/Change: Initial script development

    .EXAMPLE
      addregkey($path, "Test", "1", "DWORD")
    #>

    #-----------------------------------------------------------
[Initialisations]-------------------------------------------------------------

    #Set Error Action to Silently Continue
    $ErrorActionPreference = "SilentlyContinue"


    #-----------------------------------------------------------[Declarations]--
-----------------------------------------------------------

    #Script Version
    $sScriptVersion = "1.0"

    #Log File Info
    $sLogPath = "C:\Windows\Temp\build-user.log"

    #-----------------------------------------------------------[Configurables]-
-----------------------------------------------------------
```

```
    ######################## DO NOT EDIT BELOW HERE WITHOUT COMMENTING AND GIT
CHANGE#################################################

    ##-----------------------------------------------------------[Functions]---
-------------------------------------------------------

    Start-Transcript -Path $sLogPath

    #-----------------------------------------------------------[Execution]----
-------------------------------------------------------


    ## Enable OneDrive ADAL
    write-host "Enable ADAL"
    $registryPath = "HKCU:\SOFTWARE\Microsoft\OneDrive"
    $Name = "EnableADAL"
    $value = "1"
    $Type = "DWORD"
    IF(!(Test-Path $registryPath))
    {
    New-Item -Path $registryPath -Force | Out-Null
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}
    ELSE {
    New-ItemProperty -Path $registryPath -Name $Name -Value $value `
    -PropertyType $Type -Force | Out-Null}


    #-----------------------------------------------------------------------------
-------------------------------------------------------

    ##Set Desktop Background
    write-host "Setting Background"
    Set-ItemProperty -path 'HKCU:\Control Panel\Desktop\' -name wallpaper -
value "c:\Windows\Web\Wallpaper\custombackground.jpg"

    rundll32.exe user32.dll, UpdatePerUserSystemParameters

    #-----------------------------------------------------------------------------
-------------------------------------------------------

    Stop-Transcript
```

Table 170. PowerShell script - User Configuration Script

Client apps

Applications

Company Portal

Name	Value
Basics	
Name	Company Portal
Description	Microsoft Intune helps organizations manage access to corporate apps, data, and resources. Company Portal is the app that lets you, as an

	employee of your company, securely access those resources. Before you can use this app, make sure your IT admin has...
Scope tags	Default

Table 171. Basics - Company Portal

Name	Value
App information	
Publisher	Microsoft Corporation
Package Identifier	9WZDNCRFJ3PZ
Package Identifier	UWP
Category	
Show this as a featured app in the Company Portal	No
Information URL	http://go.microsoft.com/fwlink/?LinkId=273866
Privacy URL	http://go.microsoft.com/fwlink/?LinkID=316999
Developer	Microsoft Corporation
Owner	
Notes	

Table 172. Settings - Company Portal

Group mode	Group	Settings	
Required			
Included	Intune-Users	Filter	None
		Filter mode	None
		Availability	As soon as possible
		Installation deadline	As soon as possible
		End user notifications	Show all toast notifications
		Restart grace period	Disabled

Table 173. Assignments - Company Portal

Edge- Assigned

Name	Value
Basics	
Name	Edge - Assigned
Description	Edge - Assigned
App type	Microsoft Edge (Windows 10 and later)
Scope tags	Default

Table 174. Basics - Edge - Assigned

Name	Value
App information	
Publisher	Microsoft
Category	
Show this as a featured app in the Company Portal	No
Privacy URL	

Developer	Microsoft
Owner	Microsoft
Notes	
App suite configuration	
	Stable

Table 175. Settings - Edge - Assigned

Group mode	Group	Settings	
Required			
Included	Intune-Users	Filter	None
		Filter mode	None

Table 176. Assignments - Edge - Assigned

Mac Edge- Assigned

Name	Value
Basics	
Name	Mac Edge - Assigned
Description	MacOS Edge - Assigned
App type	Microsoft Edge (macOS)
Scope tags	Default

Table 177. Basics - Mac Edge - Assigned

Name	Value
App information	
Publisher	Microsoft
Category	
Show this as a featured app in the Company Portal	No
Privacy URL	
Developer	Microsoft
Owner	Microsoft
Notes	

Table 178. Settings - Mac Edge - Assigned

Group mode	Group	Settings	
Required			
Included	Intune-Users	Filter	None
		Filter mode	None

Table 179. Assignments - Mac Edge - Assigned

Mac Office 365- Assigned

Name	Value
Basics	
Name	Mac Office 365 - Assigned
Description	MacOS Office 365 - Assigned
App type	Microsoft 365 Apps (macOS)

Scope tags	Default

Table 180. Basics - Mac Office 365 - Assigned

Name	Value
App information	
Publisher	Microsoft
Category	
Show this as a featured app in the Company Portal	No
Privacy URL	
Developer	Microsoft
Owner	Microsoft
Notes	

Table 181. Settings - Mac Office 365 - Assigned

Group mode	Group	Settings	
Required			
Included	Intune-Users	Filter	None
		Filter mode	None

Table 182. Assignments - Mac Office 365 - Assigned

Microsoft 365 Apps

Name	Value
Basics	
Name	Microsoft 365 Apps
Description	Microsoft 365 Apps
App type	Windows app (Win32)
Scope tags	Default

Table 183. Basics - Microsoft 365 Apps

Name	Value
App information	
Publisher	Microsoft
Category	
Show this as a featured app in the Company Portal	No
Developer	
Owner	
Notes	
Program	
Install command	setup.exe /configure Configuration.xml
Uninstall command	setup.exe /configure uninstall.xml
Install behavior	System
Device restart behavior	Determine behavior based on return codes
Return codes	0;Success 1707;Success 3010;Soft reboot

	1641;Hard reboot 1618;Retry
Requirements	
Operating system architecture	x86,x64
Minimum operating system	Windows 10 1607
Disk space required (MB)	
Physical memory required (MB)	
Minimum number of logical processors required	
Minimum CPU speed required (MHz)	
Additional requirement rules	
Detection rules	
Rules format	Manually configure detection rules
Detection rules	Rule type;Registry Key path;HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun Value name; Detection method;Key exists Associated with a 32-bit app on 64-bit clients;No
Dependencies	
Dependencies	
Supersedence	
Supersedence	

Table 184. Settings - Microsoft 365 Apps

Group mode	Group	Settings	
Required			
Included	All devices	Filter	None
		Filter mode	None
		Delivery optimization priority	Content download in Background
		Availability	As soon as possible
		Installation deadline	As soon as possible
		End user notifications	Show all toast notifications
		Restart grace period	Device restart grace period (minutes)=1440 Select when to display the restart countdown dialog box before the

			restart occurs (minutes)=15 Allow user to snooze the restart notification=Yes Select the snooze duration (minutes)=240

Table 185. Assignments - Microsoft 365 Apps

Microsoft To Do: Lists, Tasks & Reminders

Name	Value
Basics	
Name	Microsoft To Do: Lists, Tasks & Reminders
Description	Got something on your mind? Get Microsoft To Do. Whether you want to increase your productivity, decrease your stress levels, or just free up some mental space, Microsoft To Do makes it easy to plan your day and manage your life. With Microsoft To Do, y...
Scope tags	Default

Table 186. Basics - Microsoft To Do: Lists, Tasks & Reminders

Name	Value
App information	
Publisher	Microsoft Corporation
Package Identifier	9NBLGGH5R558
Package Identifier	UWP
Category	
Show this as a featured app in the Company Portal	No
Information URL	https://go.microsoft.com/fwlink/?linkid=2156338
Privacy URL	https://go.microsoft.com/fwlink/?LinkId=521839
Developer	Microsoft Corporation
Owner	
Notes	

Table 187. Settings - Microsoft To Do: Lists, Tasks & Reminders

Group mode	Group	Settings	
Required			
Included	Intune-Users	Filter	None
		Filter mode	None
		Availability	As soon as possible
		Installation deadline	As soon as possible
		End user notifications	Show all toast notifications
		Restart grace period	Disabled

Table 188. Assignments - Microsoft To Do: Lists, Tasks & Reminders

Microsoft-Project

Name	Value
Basics	
Name	Microsoft-Project
Description	Microsoft Project x64 Current Branch
App type	Windows app (Win32)
Scope tags	Default

Table 189. Basics - Microsoft-Project

Name	Value
App information	
Publisher	Microsoft
Category	
Show this as a featured app in the Company Portal	No
Developer	
Owner	
Notes	
Program	
Install command	ServiceUI.exe -Process:explorer.exe Deploy-Application.exe
Uninstall command	ServiceUI.exe -Process:explorer.exe Deploy-Application.exe -DeploymentType Uninstall
Install behavior	System
Device restart behavior	Determine behavior based on return codes
Return codes	0;Success 1707;Success 3010;Soft reboot 1641;Hard reboot 1618;Retry
Requirements	
Operating system architecture	x86,x64
Minimum operating system	Windows 10 1607
Disk space required (MB)	
Physical memory required (MB)	
Minimum number of logical processors required	
Minimum CPU speed required (MHz)	
Additional requirement rules	
Detection rules	
Rules format	Manually configure detection rules
Detection rules	Rule type;File Path;C:\Program Files\Microsoft Office\root\Office16 File or folder;winproj.exe Detection method;File or folder exists Associated with a 32-bit app on 64-bit clients;No

Dependencies	
Dependencies	
Supersedence	
Supersedence	

Table 190. Settings - Microsoft-Project

Group mode	Group	Settings	
Required			
Included	Project-Install	Filter	None
		Filter mode	None
		Delivery optimization priority	Content download in Background
		Availability	As soon as possible
		Installation deadline	As soon as possible
		End user notifications	Show all toast notifications
		Restart grace period	Device restart grace period (minutes)=1440 Select when to display the restart countdown dialog box before the restart occurs (minutes)=15 Allow user to snooze the restart notification=Yes Select the snooze duration (minutes)=240
Uninstall			
Included	Project-Uninstall	Filter	None
		Filter mode	None
		Delivery optimization priority	Content download in Background
		Availability	As soon as possible
		Installation deadline	As soon as possible
		End user notifications	Show all toast notifications
		Restart grace period	Device restart grace period (minutes)=1440 Select when to display the restart countdown dialog box before the

			restart occurs (minutes)=15 Allow user to snooze the restart notification=Yes Select the snooze duration (minutes)=240

Table 191. Assignments - Microsoft-Project

Microsoft-Visio

Name	Value
Basics	
Name	Microsoft-Visio
Description	Microsoft Visio x64 Current Branch
App type	Windows app (Win32)
Scope tags	Default

Table 192. Basics - Microsoft-Visio

Name	Value
App information	
Publisher	Microsoft
Category	
Show this as a featured app in the Company Portal	No
Developer	
Owner	
Notes	
Program	
Install command	ServiceUI.exe -Process:explorer.exe Deploy-Application.exe
Uninstall command	ServiceUI.exe -Process:explorer.exe Deploy-Application.exe -DeploymentType Uninstall
Install behavior	System
Device restart behavior	Determine behavior based on return codes
Return codes	0;Success 1707;Success 3010;Soft reboot 1641;Hard reboot 1618;Retry
Requirements	
Operating system architecture	x86,x64
Minimum operating system	Windows 10 1607
Disk space required (MB)	
Physical memory required (MB)	
Minimum number of logical processors required	
Minimum CPU speed required (MHz)	

Additional requirement rules	
Detection rules	
Rules format	Manually configure detection rules
Detection rules	Rule type;File Path;C:\Program Files\Microsoft Office\root\Office16 File or folder;visio.exe Detection method;File or folder exists Associated with a 32-bit app on 64-bit clients;No
Dependencies	
Dependencies	
Supersedence	
Supersedence	

Table 193. Settings - Microsoft-Visio

Group mode	Group	Settings	
Required			
Included	Visio-Install	Filter	None
		Filter mode	None
		Delivery optimization priority	Content download in Background
		Availability	As soon as possible
		Installation deadline	As soon as possible
		End user notifications	Show all toast notifications
		Restart grace period	Device restart grace period (minutes)=1440 Select when to display the restart countdown dialog box before the restart occurs (minutes)=15 Allow user to snooze the restart notification=Yes Select the snooze duration (minutes)=240
Uninstall			
Included	Visio-Uninstall	Filter	None
		Filter mode	None
		Delivery optimization priority	Content download in Background
		Availability	As soon as possible
		Installation deadline	As soon as possible
		End user notifications	Show all toast notifications

		Restart grace period	Device restart grace period (minutes)=1440 Select when to display the restart countdown dialog box before the restart occurs (minutes)=15 Allow user to snooze the restart notification=Yes Select the snooze duration (minutes)=240

Table 194. Assignments - Microsoft-Visio

Windows Terminal Preview

Name	Value
Basics	
Name	Windows Terminal Preview
Description	This is the preview build of the Windows Terminal, which contains the latest features as they are developed. The Windows Terminal is a modern, fast, efficient, powerful, and productive terminal application for users of command-line tools and shells like Co...
Scope tags	Default

Table 195. Basics - Windows Terminal Preview

Name	Value
App information	
Publisher	Microsoft Corporation
Package Identifier	9N8G5RFZ9XK3
Package Identifier	UWP
Category	
Show this as a featured app in the Company Portal	No
Information URL	https://github.com/microsoft/terminal/issues
Privacy URL	https://privacy.microsoft.com/en-us/privacystatement
Developer	Microsoft Corporation
Owner	
Notes	

Table 196. Settings - Windows Terminal Preview

Group mode	Group	Settings	
Required			
Included	Intune-Users	Filter	None
		Filter mode	None

		Availability	As soon as possible
		Installation deadline	As soon as possible
		End user notifications	Show all toast notifications
		Restart grace period	Disabled

Table 197. Assignments - Windows Terminal Preview

App protection policy

App Protection

Android-App-Protection

Name	Value
Basics	
Name	Android-App-Protection
Description	Protects Android Company apps on un-managed devices
Policy type	App protection policy
Platform supported	Android
Version	"6112bbf5-0000-0c00-0000-65a7ebc90000"
Scope tags	Default

Table 198. Basics - Android-App-Protection

Name	Value
Apps	
Management type	Target to all app types
Public apps	MyQ Roger: OCR scanner PDF Dialpad Achievers Adobe Acrobat Reader FleetSafer Akumina EXP Appian for Intune Space Connect BlueJeans Video Conferencing Box Comfy F2 Touch Intune CellTrust SL2™ for Intune Cisco Jabber for Intune Webex for Intune Citrix ShareFile for Intune Hey DAN for Intune Condeco Dooray! for Intune ArcGIS Indoors for Intune FactSet Fuze Mobile for Intune Meetio Global Relay

	Groupdolists Hearsay Relate for Intune HowNow ixArma 6 CAPTOR ISEC7 MED for Intune Leap Work for Intune Nexis Newsdesk™ Mobile LumApps for Intune Meetings by Decisions MentorcliQ M-Files for Intune Cortana Microsoft Dynamics 365 for phones Field Service (Dynamics 365) Dynamics 365 Sales Microsoft Dynamics 365 for tablets Microsoft Invoicing Microsoft Edge Power Automate Azure Information Protection Microsoft Launcher Microsoft Lists Microsoft Loop Microsoft Kaizala Power Apps Microsoft Excel Skype for Business Microsoft 365 (Office) Microsoft Office [HL] Microsoft Office [ROW] Microsoft Lens Microsoft OneNote Microsoft Outlook Microsoft PowerPoint Microsoft Word Microsoft Planner Microsoft Power BI Dynamics 365 Remote Assist Microsoft Defender Endpoint Microsoft SharePoint Microsoft OneDrive Microsoft Stream Microsoft Teams Microsoft To-Do Microsoft Whiteboard Work Folders MultiLine for Intune MangoApps, Work from Anywhere Microsoft 365 Admin My Portal By MangoApps

	MURAL - Visual Collaboration MyITOps for Intune Nine Work for Intune Omnipresence Go PenPoint PrinterOn for Microsoft Qlik Sense Mobile RICOH Spaces RICOH Spaces V2 RingCentral for Intune Seismic ServiceNow® Agent - Intune Now® Mobile - Intune Notate for Intune Slack for Intune Tableau Mobile for Intune Varicent Vbrick Mobile Voltage SecureMail Viva Engage ArchXtract Confidential File Viewer myBLDNG Microsoft StaffHub Naso Mobile Board.Vision Re:Work Enterprise Idenprotect Go Zoom for Intune CiiMS GO
Custom apps	com.microsoft.rdc.android
Data protection	
Data Transfer	
Backup org data to Android backup services	Block
Send org data to other apps	Policy managed apps
Select apps to exempt	
Save copies of org data	Block
Allow user to save copies to selected services	Local Storage;OneDrive for Business;SharePoint
Transfer telecommunication data to	Any dialer app
Dialer App Package ID	
Dialer App Name	
Receive data from other apps	Policy managed apps
Open data into Org documents	Block
Allow users to open data from selected services	OneDrive for Business;SharePoint;Camera
Restrict cut, copy, and paste between other apps	Policy managed apps with paste in
Cut and copy character limit for any app	0
Screen capture and Google Assistant	Allow
Approved keyboards	Not required
Select keyboards to approve	

Encryption	
Encrypt org data	Require
Encrypt org data on enrolled devices	Require
Functionality	
Sync policy managed app data with native apps or add-ins	Allow
Printing org data	Allow
Restrict web content transfer with other apps	
Unmanaged Browser ID	
Unmanaged Browser Name	
Org data notifications	Allow
Access requirements	
Functionality	
PIN for access	Not required
PIN type	Numeric
Simple PIN	Allow
Select minimum PIN length	6
Fingerprint instead of PIN for access (Android 6.0+)	Allow
Override biometrics with PIN after timeout	Require
Timeout (minutes of inactivity)	30
Biometrics instead of PIN for access	Allow
PIN reset after number of days	Yes
Number of days	30
Select number of previous PIN values to maintain	0
App PIN when device PIN is set	Require
Work or school account credentials for access	Not required
Recheck the access requirements after (minutes of inactivity)	30
Conditional launch	
Functionality	
Conditional launch	Max PIN attempts;5;Reset PIN Offline grace period;720;Block access (minutes) Offline grace period;90;Wipe data (days) Jailbroken/rooted devices;;Block access

Table 199. Settings - Android-App-Protection

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 200. Assignments - Android-App-Protection

iOS-App-Protection

Name	Value
Basics	
Name	iOS-App-Protection

Description	Protects iOS Company apps on un-managed devices
Policy type	App protection policy
Platform supported	iOS/iPadOS
Scope tags	Default

Table 201. Basics - iOS-App-Protection

Name	Value
Apps	
Management type	Target to all app types
Public apps	LiquidText MyQ Roger: OCR scanner PDF MURAL - Visual Collaboration Space Connect Dialpad Achievers Adobe Acrobat Reader FleetSafer Akumina EXP AssetScan For Intune Appian for Intune BlueJeans Video Conferencing Diligent Boards Box for EMM iAnnotate for Intune / O365 Breezy for Intune BuddyBoard Comfy F2 Manager - Intune F2 Touch Intune CellTrust SL2™ for Intune Cisco Jabber for Intune Webex for Intune Hey DAN for Intune Condeco Dooray! for Intune Egnyte for Intune ArcGIS Indoors for Intune FactSet Fuze Mobile for Intune Meetio Global Relay Groupdolists EVALARM Dashflow for InTune iManage Work 10 For Intune ixArma 6 Zero for Intune Incorta (BestBuy) Omnipresence Go CAPTOR

	ISEC7 Mobile Exchange Delegate ISEC7 Mobile Exchange Delegate for Intune KeePassium for Intune Klaxoon for Intune Leap Work for Intune Nexis Newsdesk™ Mobile LumApps for Intune M-Files for Intune VerityRMS MangoApps, Work from Anywhere My Portal By MangoApps Senses Meetings by Decisions MentorcliQ Microsoft Azure Cortana Microsoft Dynamics 365 Microsoft Invoicing Microsoft Dynamics 365 for phones Field Service (Dynamics 365) Dynamics 365 Sales Microsoft Loop Skype for Business Microsoft Kaizala Microsoft Power Apps Microsoft Edge Microsoft 365 Admin Microsoft Excel Microsoft Outlook Microsoft PowerPoint Microsoft Word Microsoft Lens Microsoft 365 (Office) Microsoft OneNote Microsoft Planner Microsoft Power BI Power Automate Dynamics 365 Remote Assist Azure Information Protection Microsoft Defender Endpoint Microsoft SharePoint Microsoft StaffHub Microsoft OneDrive Microsoft Teams Microsoft Lists Microsoft Stream Microsoft To-Do Microsoft Whiteboard Work Folders MultiLine for Intune MyITOps for Intune

	PenPoint Board Papers Board Papers for Intune Team Papers for Intune PK Protect for Intune PrinterOn for Microsoft Qlik Sense Mobile Re:Work Enterprise RICOH Spaces RICOH Spaces V2 RingCentral for Intune Seismic ServiceNow® Agent - Intune Now® Mobile - Intune Notate for Intune Citrix ShareFile for Intune Slack for Intune Firstup - Intune Enterprise Files for Intune Mobile Work Orders Tableau Mobile for Intune Varicent Vbrick Mobile Vera for Intune Voltage Mail HowNow Secure Contacts Island Enterprise Browser ArchXtract Confidential File Viewer Box — Cloud Content Management iBabs For Intune myBLDNG Speaking Email Hearsay Relate for Intune Naso Mobile Board.Vision Board.Vision for iPad Idenprotect Go Zoom for Intune Viva Engage CiiMS GO
Custom apps	com.microsoft.rdc.ios
Data protection	
Data Transfer	
Backup org data to iTunes and iCloud backups	Block
Send org data to other apps	Policy managed apps
Select apps to exempt	Default;skype;app-settings;calshow;itms;itmss;itms-apps;itms-appss;itms-services;
Save copies of org data	Block

Allow user to save copies to selected services	Local Storage;OneDrive for Business;SharePoint
Transfer telecommunication data to	Any dialer app
Dialer App URL Scheme	
Receive data from other apps	Policy managed apps
Open data into Org documents	Block
Allow users to open data from selected services	OneDrive for Business;SharePoint;Camera
Restrict cut, copy, and paste between other apps	Policy managed apps with paste in
Cut and copy character limit for any app	0
Third party keyboards	Allow
Encryption	
Encrypt org data	Require
Functionality	
Sync policy managed app data with native apps or add-ins	Allow
Printing org data	Allow
Restrict web content transfer with other apps	
Unmanaged browser protocol	
Org data notifications	Allow
Access requirements	
Functionality	
PIN for access	Not required
PIN type	Numeric
Simple PIN	Allow
Select minimum PIN length	6
Fingerprint instead of PIN for access (Android 6.0+)	Allow
Override biometrics with PIN after timeout	Require
Timeout (minutes of inactivity)	30
Face ID instead of PIN for access (iOS 11+/iPadOS)	Allow
PIN reset after number of days	Yes
Number of days	30
Select number of previous PIN values to maintain	0
Work or school account credentials for access	Not required
Recheck the access requirements after (minutes of inactivity)	30
Conditional launch	
Functionality	
Conditional launch	Max PIN attempts;5;Reset PIN Offline grace period;720;Block access (minutes) Offline grace period;90;Wipe data (days) Jailbroken/rooted devices;;Block access

Table 202. Settings - iOS-App-Protection

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 203. Assignments - iOS-App-Protection

Windows enrollment

Autopilot

Autopilot Profile

Name	Value
Basics	
Name	Autopilot Profile
Description	OOBE Autopilot Profile
Profile type	Windows Autopilot deployment profiles
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC
Scope tags	Default

Table 204. Basics - Autopilot Profile

Name	Value
Out-of-box experience (OOBE)	
Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Language (Region)	English (United Kingdom)
Automatically configure keyboard	No
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow pre-provisioned deployment	Yes
Apply device name template	Yes
Enter a name	%SERIAL%

Table 205. Settings - Autopilot Profile

Enrollment Status Page

AutoPilot Enrollment

Name	Value
Basics	
Name	AutoPilot Enrollment
Description	Custom Enrollment Status
Policy type	Enrollment Status Page
Version	1
Scope tags	Default

Table 206. Basics - AutoPilot Enrollment

Name	Value
Settings	
Show app and profile configuration progress	Yes

Show an error when installation takes longer than specified number of minutes	120
Show custom message when time limit or error occurs	Yes
Error message	Enter your custom error here
Turn on log collection and diagnostics page for end users	Yes
Only show page to devices provisioned by out-of-box experience (OOBE)	Yes
Block device use until all apps and profiles are installed	Yes
Allow users to reset device if installation error occurs	Yes
Allow users to use device if installation error occurs	Yes
Block device use until required apps are installed if they are assigned to the user/device	Microsoft 365 Apps

Table 207. Settings - AutoPilot Enrollment

Group	Filter	Filter mode
Included Groups		
Autopilot-Devices	None	Exclude

Table 208. Assignments - AutoPilot Enrollment

Conditional access

Conditional access policies

Block anything not protected

Name	Value
Basics	
Name	Block anything not protected
Profile type	Conditional Access
Enable policy	Off

Table 209. Basics - Block anything not protected

Name	Value
Users and groups	
Include	
Include	All users
Exclude	
Users and groups	Azure BreakGlass Account
Cloud apps or actions	
Cloud apps	
Include	All cloud apps
Conditions	
Device platform	
Include	Android

	iOS Windows Phone macOS Linux
Filter for devices	
Exclude filtered devices from policy	device.deviceOwnership -eq "Company"
Grant	
Control access enforcement to block or grant access.	Grant access
Require device to be marked as compliant	Enabled
Require Microsoft Entra hybrid joined device	Enabled
Require app protection policy	Enabled
For multiple controls	Require one of the selected controls

Table 210. Settings - Block anything not protected

Block legacy authentication

Name	Value
Basics	
Name	Block legacy authentication
Profile type	Conditional Access
Enable policy	Off

Table 211. Basics - Block legacy authentication

Name	Value
Users and groups	
Include	
Include	All users
Exclude	
Users and groups	Azure BreakGlass Account
Cloud apps or actions	
Cloud apps	
Include	All cloud apps
Conditions	
Client apps	
Include	Exchange ActiveSync Other clients
Grant	
Control access enforcement to block or grant access.	Block access

Table 212. Settings - Block legacy authentication

Block Personal Windows without App

Name	Value
Basics	
Name	Block Personal Windows without App
Profile type	Conditional Access

Enable policy	Off

Table 213. Basics - Block Personal Windows without App

Name	Value
Users and groups	
Include	
Include	All users
Exclude	
Users and groups	Azure BreakGlass Account
Cloud apps or actions	
Cloud apps	
Include	All cloud apps
Conditions	
Device platform	
Include	Windows
Client apps	
Include	Exchange ActiveSync Mobile apps and desktop clients Other clients
Filter for devices	
Exclude filtered devices from policy	device.deviceOwnership -eq "Company"
Grant	
Control access enforcement to block or grant access.	Block access

Table 214. Settings - Block Personal Windows without App

Require App Protection for Mobile Devices

Name	Value
Basics	
Name	Require App Protection for Mobile Devices
Profile type	Conditional Access
Enable policy	Off
Created	17 January 2024 15:01:11

Table 215. Basics - Require App Protection for Mobile Devices

Name	Value
Users and groups	
Include	
Include	All users
Exclude	
Users and groups	Azure BreakGlass Account
Cloud apps or actions	
Cloud apps	
Include	All cloud apps
Conditions	
Device platform	
Include	Android

	iOS
Filter for devices	
Exclude filtered devices from policy	device.deviceOwnership -eq "Company"
Grant	
Control access enforcement to block or grant access.	Grant access
Require app protection policy	Enabled
For multiple controls	Require one of the selected controls

Table 216. Settings - Require App Protection for Mobile Devices

Require Device Compliance

Name	Value
Basics	
Name	Require Device Compliance
Profile type	Conditional Access
Enable policy	Off

Table 217. Basics - Require Device Compliance

Name	Value
Users and groups	
Include	
Include	All users
Exclude	
Users and groups	Azure BreakGlass Account
Cloud apps or actions	
Cloud apps	
Include	All cloud apps
Conditions	
Filter for devices	
Include filtered devices in policy	device.deviceOwnership -eq "Company"
Grant	
Control access enforcement to block or grant access.	Grant access
Require device to be marked as compliant	Enabled
Require Microsoft Entra hybrid joined device	Enabled
For multiple controls	Require one of the selected controls

Table 218. Settings - Require Device Compliance

Require MFA for Guests

Name	Value
Basics	
Name	Require MFA for Guests
Profile type	Conditional Access
Enable policy	Off

Table 219. Basics - Require MFA for Guests

Name	Value
Users and groups	
Include	
Include	Select users and groups
Exclude	
Users and groups	Azure BreakGlass Account
Cloud apps or actions	
Cloud apps	
Include	All cloud apps
Grant	
Control access enforcement to block or grant access.	Grant access
Require multifactor authentication	Enabled
For multiple controls	Require one of the selected controls

Table 220. Settings - Require MFA for Guests

Require multifactor authentication for admins

Name	Value
Basics	
Name	Require multifactor authentication for admins
Profile type	Conditional Access
Enable policy	Off

Table 221. Basics - Require multifactor authentication for admins

Name	Value
Users and groups	
Include	
Include	Select users and groups
Directory roles	62e90394-69f5-4237-9190-012177145e10 194ae4cb-b126-40b2-bd5b-6091b380977d f28a1f50-f6e7-4571-818b-6a12f2af6b6c 29232cdf-9323-42fd-ade2-1d097af3e4de b1be1c3e-b65d-4f19-8427-f6fa0d97feb9 729827e3-9c14-49f7-bb1b-9608f156bbb8 b0f54661-2d74-4c50-afa3-1ec803f12efe fe930be7-5e62-47db-91af-98c3a49a38b1 c4e39bd9-1100-46d3-8c65-fb160da0071f 9b895d92-2cd3-44c7-9d02-a6ac2d5ea5c3 158c047a-c907-4556-b7ef-446551a6b5f7 966707d0-3269-4727-9be2-8c3a10f19b9d 7be44c8a-adaf-4e2a-84d6-ab2649e08a13 e8611ab8-c189-46e8-94e1-60213ab1f814
Exclude	
Users and groups	Azure BreakGlass Account
Cloud apps or actions	
Cloud apps	
Include	All cloud apps

Grant	
Control access enforcement to block or grant access.	Grant access
Require multifactor authentication	Enabled
For multiple controls	Require one of the selected controls

Table 222. Settings - Require multifactor authentication for admins

Require multifactor authentication for all users

Name	Value
Basics	
Name	Require multifactor authentication for all users
Profile type	Conditional Access
Enable policy	Off

Table 223. Basics - Require multifactor authentication for all users

Name	Value
Users and groups	
Include	
Include	All users
Exclude	
Users and groups	Azure BreakGlass Account
Cloud apps or actions	
Cloud apps	
Include	All cloud apps
Grant	
Control access enforcement to block or grant access.	Grant access
Require multifactor authentication	Enabled
For multiple controls	Require one of the selected controls

Table 224. Settings - Require multifactor authentication for all users

Require Windows MAM

Name	Value
Basics	
Name	Require Windows MAM
Profile type	Conditional Access
Enable policy	Off

Table 225. Basics - Require Windows MAM

Name	Value
Users and groups	
Include	
Include	All users
Exclude	
Users and groups	Azure BreakGlass Account
Cloud apps or actions	

Cloud apps	
Include	All cloud apps
Conditions	
Device platform	
Include	Windows
Client apps	
Include	Browser
Filter for devices	
Exclude filtered devices from policy	device.deviceOwnership -eq "Company"
Grant	
Control access enforcement to block or grant access.	Grant access
Require app protection policy	Enabled
For multiple controls	Require one of the selected controls

Table 226. Settings - Require Windows MAM

Device compliance

Compliance Policies

Android Compliance

Name	Value
Basics	
Name	Android Compliance
Description	Requires threat level of medium or under, 4 digit expiring password and encryption
Platform supported	Android Enterprise
Profile type	Fully managed, dedicated, and corporate-owned work profile
Scope tags	Default

Table 227. Basics - Android Compliance

Name	Value
Device Health	
Require the device to be at or under the Device Threat Level	Medium
Device Properties	
Operating System Version	
Minimum OS version	
Maximum OS version	
Minimum security patch level	
System Security	
Require a password to unlock mobile devices	Require
Required password type	Numeric
Minimum password length	4
Maximum minutes of inactivity before password is required	1 minute
Number of days until password expires	90

Number of passwords required before user can reuse a password	3
Encryption	
Require encryption of data storage on device.	Require
Device Security	
Intune app runtime integrity	Require

Table 228. Settings - Android Compliance

Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	Immediately		

Table 229. Actions for noncompliance - Android Compliance

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 230. Assignments - Android Compliance

iOS Compliance

Name	Value
Basics	
Name	iOS Compliance
Description	Blocks Jailbroken devices, required threat level of medium or below. Blocks passwords and requires minimum 4 digit expiring password
Platform supported	iOS/iPadOS
Profile type	iOS compliance policy
Scope tags	Default

Table 231. Basics - iOS Compliance

Name	Value
Email	
Email	
Unable to set up email on the device	Not configured
Device Health	
Jailbroken devices	Block
Require the device to be at or under the Device Threat Level	Medium
Device Properties	
Operating System Version	
Minimum OS version	
Maximum OS version	
Minimum OS build version	
Maximum OS build version	
Microsoft Defender for Endpoint	
Microsoft Defender for Endpoint rules	

Require the device to be at or under the machine risk score:	Not configured
System Security	
Password	
Require a password to unlock mobile devices	Require
Device enrollment and automated device enrollment	
Simple passwords	Block
Minimum password length	4
Required password type	Numeric
Number of non-alphanumeric characters in password	Not configured
Maximum minutes after screen lock before password is required	Immediately
Maximum minutes of inactivity until screen locks	2 minutes
Password expiration (days)	180
Number of previous passwords to prevent reuse	3
Device Security	
Restricted apps	

Table 232. Settings - iOS Compliance

Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	Immediately		

Table 233. Actions for noncompliance - iOS Compliance

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 234. Assignments - iOS Compliance

macOS Compliance

Name	Value
Basics	
Name	macOS Compliance
Description	Required system integrity protection, encryption, firewall and restricted app install sources
Platform supported	macOS
Profile type	Mac compliance policy
Scope tags	Default

Table 235. Basics - macOS Compliance

Name	Value
Device Health	

Require system integrity protection	Require
Device Properties	
Operating System Version	
Minimum OS version	
Maximum OS version	
Minimum OS build version	
Maximum OS build version	
System Security	
Password	
Require a password to unlock devices.	Not configured
Simple passwords	Not configured
Minimum password length	
Password type	Device default
Number of non-alphanumeric characters in password	Not configured
Maximum minutes of inactivity before password is required	Not configured
Password expiration (days)	
Number of previous passwords to prevent reuse	
Encryption	
Require encryption of data storage on device.	Require
Device Security	
Firewall	Enable
Incoming connections	Not configured
Stealth Mode	Not configured
Gatekeeper	
Allow apps downloaded from these locations	Mac App Store and identified developers

Table 236. Settings - macOS Compliance

Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	Immediately		

Table 237. Actions for noncompliance - macOS Compliance

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 238. Assignments - macOS Compliance

Windows Compliance Policy

Name	Value
Basics	
Name	Windows Compliance Policy
Description	Custom Compliance policy
Platform supported	Windows 10 and later

Profile type	Windows 10 and later compliance policy
Scope tags	Default

Table 239. Basics - Windows Compliance Policy

Name	Value
Custom Compliance	
Custom compliance	Require
Select your discovery script	
Upload and validate the JSON file with your custom compliance settings	{ "Rules":[{ "SettingName":"UpdateStatus", "Operator":"IsEquals", "DataType":"String", "Operand":"True", "MoreInfoUrl":"https://support.microsoft.com/en-us/windows/windows-update-troubleshooter-19bc41ca-ad72-ae67-af3c-89ce169755dd", "RemediationStrings":[{ "Language":"en_US", "Title":"Missing Updates.", "Description": "Your machine is missing some recent critical updates." }] }, { "SettingName":"OSsupported", "Operator":"IsEquals", "DataType":"String", "Operand":"True", "MoreInfoUrl":"https://support.microsoft.com/en-us/windows/windows-update-troubleshooter-19bc41ca-ad72-ae67-af3c-89ce169755dd", "RemediationStrings":[{ "Language": "en_US", "Title": "Unsupported Operating System.", "Description": "Your operating system version is now out of support and requires updating" }] }, { "SettingName":"DomainFirewall", "Operator":"IsEquals",

```
        "DataType":"String",
        "Operand":"True",

"MoreInfoUrl":"https://support.microsoft.com/en-us/windows/turn-microsoft-defender-firewall-on-or-off-ec0844f7-aebd-0583-67fe-601ecf5d774f",
        "RemediationStrings":[
          {
            "Language": "en_US",
            "Title": "Domain Firewall is Off",
            "Description": "Your domain firewall is switched off, please re-enable."
          }
        ]
      },
      {
        "SettingName":"PrivateFirewall",
        "Operator":"IsEquals",
        "DataType":"String",
        "Operand":"True",

"MoreInfoUrl":"https://support.microsoft.com/en-us/windows/turn-microsoft-defender-firewall-on-or-off-ec0844f7-aebd-0583-67fe-601ecf5d774f",
        "RemediationStrings":[
          {
            "Language": "en_US",
            "Title": "Private Firewall is Off",
            "Description": "Your private firewall is switched off, please re-enable."
          }
        ]
      },
      {
        "SettingName":"PublicFirewall",
        "Operator":"IsEquals",
        "DataType":"String",
        "Operand":"True",

"MoreInfoUrl":"https://support.microsoft.com/en-us/windows/turn-microsoft-defender-firewall-on-or-off-ec0844f7-aebd-0583-67fe-601ecf5d774f",
        "RemediationStrings":[
          {
            "Language": "en_US",
            "Title": "Public Firewall is Off",
            "Description": "Your public firewall is switched off, please re-enable."
          }
        ]
      },
```

```
      {
        "SettingName":"AMEnabled",
        "Operator":"IsEquals",
        "DataType":"String",
        "Operand":"True",

"MoreInfoUrl":"https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963",
        "RemediationStrings":[
          {
            "Language": "en_US",
            "Title": "AntiMalwareScanner is Off",
            "Description": "Your anti-malware scanner is switched off, please re-enable."
          }
        ]
      },
      {
        "SettingName":"ASEnabled",
        "Operator":"IsEquals",
        "DataType":"String",
        "Operand":"True",

"MoreInfoUrl":"https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963",
        "RemediationStrings":[
          {
            "Language": "en_US",
            "Title": "AntiSpyware is Off",
            "Description": "Your anti-spyware scanner is switched off, please re-enable."
          }
        ]
      },
      {
        "SettingName":"AVEnabled",
        "Operator":"IsEquals",
        "DataType":"String",
        "Operand":"True",

"MoreInfoUrl":"https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963",
        "RemediationStrings":[
          {
            "Language": "en_US",
```

	"Title": "AntiVirus is Off", "Description": "Your anti-virus scanner is switched off, please re-enable." }] }, { "SettingName":"NISEnabled", "Operator":"IsEquals", "DataType":"String", "Operand":"True", "MoreInfoUrl":"https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-network-protection?view=o365-worldwide", "RemediationStrings":[{ "Language": "en_US", "Title": "Network Inspection Service is Off", "Description": "Your network inspection service is switched off, please re-enable." }] }, { "SettingName":"OPEnabled", "Operator":"IsEquals", "DataType":"String", "Operand":"True", "MoreInfoUrl":"https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963", "RemediationStrings":[{ "Language": "en_US", "Title": "On Access Protection is Off", "Description": "Your on access protection service is switched off, please re-enable." }] }, { "SettingName":"RPEEnabled", "Operator":"IsEquals", "DataType":"String", "Operand":"True",

	"MoreInfoUrl":"https://support.microsoft.com/en-us/windows/turn-off-defender-antivirus-protection-in-windows-security-99e6004f-c54c-8509-773c-a4d776b77960", "RemediationStrings":[{ "Language": "en_US", "Title": "RealTime Protection is Off", "Description": "Your realtime protection service is switched off, please re-enable." }] }, { "SettingName":"TPEEnabled", "Operator":"IsEquals", "DataType":"String", "Operand":"True", "MoreInfoUrl":"https://support.microsoft.com/en-us/windows/prevent-changes-to-security-settings-with-tamper-protection-31d51aaa-645d-408e-6ce7-8d7f8e593f87", "RemediationStrings":[{ "Language": "en_US", "Title": "Tamper Protection is Off", "Description": "Your tamper protection service is switched off, please re-enable." }] }, { "SettingName":"ASAge", "Operator":"IsEquals", "DataType":"String", "Operand":"True", "MoreInfoUrl":"https://support.microsoft.com/en-us/windows/update-windows-security-signatures-726d462d-b2a8-5bb2-8a9e-5d5871b06e05", "RemediationStrings":[{ "Language": "en_US", "Title": "AntiSpyware Out of Date", "Description": "Your antispyware is out of date, please update it." }] },

	{ "SettingName":"AVAge", "Operator":"IsEquals", "DataType":"String", "Operand":"True", "MoreInfoUrl":"https://support.microsoft.com/en-us/windows/update-windows-security-signatures-726d462d-b2a8-5bb2-8a9e-5d5871b06e05", "RemediationStrings":[{ "Language": "en_US", "Title": "Antivirus Out of Date", "Description": "Your antivirus is out of date, please update it." }] }, { "SettingName":"NISEAge", "Operator":"IsEquals", "DataType":"String", "Operand":"True", "MoreInfoUrl":"https://support.microsoft.com/en-us/windows/update-windows-security-signatures-726d462d-b2a8-5bb2-8a9e-5d5871b06e05", "RemediationStrings":[{ "Language": "en_US", "Title": "Network Inspection Out of Date", "Description": "Your network inspection service is out of date, please update it." }] }, { "SettingName":"SignatureOutOfDate", "Operator":"IsEquals", "DataType":"String", "Operand":"True", "MoreInfoUrl":"https://support.microsoft.com/en-us/windows/update-windows-security-signatures-726d462d-b2a8-5bb2-8a9e-5d5871b06e05", "RemediationStrings":[{ "Language": "en_US", "Title": "Signatures Out of Date",

```
            "Description": "Your antivirus signatures are out of date, please update them."
          }
        ]
      },
      {
        "SettingName":"QuickScanOverdue",
        "Operator":"IsEquals",
        "DataType":"String",
        "Operand":"False",

"MoreInfoUrl":"https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963",
        "RemediationStrings":[
          {
            "Language": "en_US",
            "Title": "Quick Scan Overdue",
            "Description": "Your machine needs a quick anti-virus scan."
          }
        ]
      },
      {
        "SettingName":"FullScanOverdue",
        "Operator":"IsEquals",
        "DataType":"String",
        "Operand":"False",

"MoreInfoUrl":"https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963",
        "RemediationStrings":[
          {
            "Language": "en_US",
            "Title": "Full Scan Overdue",
            "Description": "Your machine needs a full anti-virus scan."
          }
        ]
      },
      {
        "SettingName":"NoActiveMalware",
        "Operator":"IsEquals",
        "DataType":"String",
        "Operand":"True",

"MoreInfoUrl":"https://support.microsoft.com/en-us/windows/stay-protected-with-windows-
```

	security-2ae0363d-0ada-c064-8b56-6a39afb6a963", "RemediationStrings":[{ "Language": "en_US", "Title": "Active Malware Detected", "Description": "Active Malware detected, please remediate." }] }, { "SettingName":"TPMpresent", "Operator":"IsEquals", "DataType":"String", "Operand":"True", "MoreInfoUrl":"https://support.microsoft.com/en-us/windows/enable-tpm-2-0-on-your-pc-1fd5a332-360d-4f46-a1e7-ae6b0c90645c", "RemediationStrings":[{ "Language": "en_US", "Title": "No TPM Chip", "Description": "No TPM chip detected, please enable in BIOS." }] }, { "SettingName":"TPMactivated", "Operator":"IsEquals", "DataType":"String", "Operand":"True", "MoreInfoUrl":"https://support.microsoft.com/en-us/windows/enable-tpm-2-0-on-your-pc-1fd5a332-360d-4f46-a1e7-ae6b0c90645c", "RemediationStrings":[{ "Language": "en_US", "Title": "TPM not Activated", "Description": "TPM not activated, please activate." }] }, { "SettingName":"TPMenabled", "Operator":"IsEquals", "DataType":"String",

	"Operand":"True", "MoreInfoUrl":"https://support.microsoft.com/en-us/windows/enable-tpm-2-0-on-your-pc-1fd5a332-360d-4f46-a1e7-ae6b0c90645c", "RemediationStrings":[{ "Language": "en_US", "Title": "TPM not Enabled", "Description": "TPM not enabled, please enable." }] }, { "SettingName":"Bitlocker", "Operator":"IsEquals", "DataType":"String", "Operand":"True", "MoreInfoUrl":"https://support.microsoft.com/en-us/windows/turn-on-device-encryption-0c453637-bc88-5f74-5105-741561aae838", "RemediationStrings":[{ "Language": "en_US", "Title": "Unencrypted", "Description": "Your device is not fully encrypted, please encrypt." }] }] }
Device Health	
Windows 10 and 11	
BitLocker	Not configured
Secure Boot	Not configured
Code integrity	Not configured
Windows 11 only	
Early Launch AntiMalware	Not configured
Firmware Protection	Not configured
Memory Integrity Protection	Not configured
Memory Access Protection	Not configured
Virtualization-based Security	Not configured
Device Properties	
Operating System Version	
Minimum OS version	
Maximum OS version	
Minimum OS version for mobile devices	

Maximum OS version for mobile devices	
Valid operating system builds	
Configuration Manager Compliance	
Require device compliance from Configuration Manager	Not configured
System Security	
Password	
Require a password to unlock mobile devices	Not configured
Simple passwords	Not configured
Password type	Device default
Minimum password length	
Maximum minutes of inactivity before password is required	Not configured
Password expiration (days)	
Number of previous passwords to prevent reuse	
Require password when device returns from idle state (Mobile and Holographic)	Not configured
Encryption	
Require encryption of data storage on device.	Not configured
Device Security	
Firewall	Not configured
Trusted Platform Module (TPM)	Not configured
Antivirus	Not configured
Antispyware	Not configured
Defender	
Microsoft Defender Antimalware	Not configured
Microsoft Defender Antimalware minimum version	
Microsoft Defender Antimalware security intelligence up-to-date	Not configured
Real-time protection	Not configured
Microsoft Defender for Endpoint	
Microsoft Defender for Endpoint rules	
Require the device to be at or under the machine risk score:	Not configured

Table 240. Settings - Windows Compliance Policy

Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	Immediately		

Table 241. Actions for noncompliance - Windows Compliance Policy

Group	Filter	Filter mode
Included Groups		
Intune-Users	None	None

Table 242. Assignments - Windows Compliance Policy

Compliance Scripts

Custom Compliance Script

Name	Value
Basics	
Name	Custom Compliance Script
Description	Checks Machine has updated recently Checks OS is supported Checks OS is up to date Checks if all firewalls are enabled Checks if all AV is enabled Checks AV is updated Checks for active malware Checks for TPM Checks for Encryption
Profile type	Scripts (preview)
Scope tags	Default

Table 243. Basics - Custom Compliance Script

Name	Value
Settings	
Detection script	<# .SYNOPSIS .Custom Intune Compliance Policy .DESCRIPTION .Checks Machine has updated recently .Checks OS is supported .Checks OS is up to date .Checks if all firewalls are enabled .Checks if all AV is enabled .Checks AV is updated .Checks for active malware .INPUTS .OUTPUTS .NOTES Version: 1.0 Author: Andrew Taylor WWW: andrewstaylor.com Creation Date: 10/02/2023 Purpose/Change: Initial script development .EXAMPLE N/A #> ### When did we last check for updates?

	##Get the date [datetime]$dtToday = [datetime]::NOW $strCurrentMonth = $dtToday.Month.ToString() $strCurrentYear = $dtToday.Year.ToString() [datetime]$dtMonth = $strCurrentMonth + '/1/' + $strCurrentYear while ($dtMonth.DayofWeek -ne 'Tuesday') { $dtMonth = $dtMonth.AddDays(1) } $strPatchTuesday = $dtMonth.AddDays(7) $intOffSet = 7 if ([datetime]::NOW -lt $strPatchTuesday -or [datetime]::NOW -ge $strPatchTuesday.AddDays($intOffSet)) { $objUpdateSession = New-Object -ComObject Microsoft.Update.Session $objUpdateSearcher = $objUpdateSession.CreateupdateSearcher() $arrAvailableUpdates = @($objUpdateSearcher.Search("IsAssigned=1 and IsHidden=0 and IsInstalled=0").Updates) $strAvailableCumulativeUpdates = $arrAvailableUpdates \| Where-Object {$_.title -like "*cumulative*"} if ($strAvailableCumulativeUpdates -eq $null) { $strUpdateStatus = "True" } else { $strUpdateStatus = "False" } } else { $strUpdateStatus = "False" } [datetime]$Today = [datetime]::NOW $7daysago = $Today.AddDays(-7) ##Which OS ##Check if we are running Win10 or 11 $OSname = Get-WMIObject win32_operatingsystem \| select Caption if ($OSname -like "*Windows 10*") { $OSname = "Windows 10" }

```
if ($OSname -like "*Windows 11*") {
   $OSname = "Windows 11"
}

##Which OS Version?
##Check which version number
$OSVersion = (Get-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows
NT\CurrentVersion" -Name
DisplayVersion).DisplayVersion

if ($OSname -eq "Windows 11") {
##Windows 11
##Scrape the release information to find latest
supported versions
$url = "https://learn.microsoft.com/en-
us/windows/release-health/windows11-
release-information"
$content = (Invoke-WebRequest -Uri $url -
UseBasicParsing).content
[regex]$regex = "(?s)<tr class=.*?</tr>"
$tables =
$regex.matches($content).groups.value
$tables = $tables.replace("<td>","")
$tables = $tables.replace("</td>","")
$tables = $tables.replace('<td align="left">',"")
$tables = $tables.replace('<tr
class="highlight">',"")
$tables = $tables.replace("</tr>","")

##Add each found version for array
$availableversions = @()
foreach ($table in $tables) {
   [array]$toArray = $table.Split("`n") | Where-
Object {$_.Trim("")}
   $availableversions += ($toArray[0]).Trim()
}

##We want n-1 so grab the first two objects
$supportedversions = $availableversions |
select-object -first 2

##Check if we are supported
if ($OSVersion -in $supportedversions) {
   $OSsupported = "True"
}
else {
   $OSsupported = "False"
}
}
```

	if ($OSname -eq "Windows 10") { ##Windows 10 ##Scrape the release information to find latest supported versions $url = "https://learn.microsoft.com/en-us/windows/release-health/release-information" $content = (Invoke-WebRequest -Uri $url -UseBasicParsing).content [regex]$regex = "(?s)<tr class=.*?</tr>" $tables = $regex.matches($content).groups.value $tables = $tables.replace("<td>","") $tables = $tables.replace("</td>","") $tables = $tables.replace('<td align="left">',"") $tables = $tables.replace('<tr class="highlight">',"") $tables = $tables.replace("</tr>","") ##Add each found version for array $availableversions = @() foreach ($table in $tables) { [array]$toArray = $table.Split("`n") \| Where-Object {$_.Trim("")} $availableversions += ($toArray[0]).Trim() } ##We want n-1 so grab the first two objects $supportedversions = $availableversions \| select-object -first 2 ##Check if we are supported if ($OSVersion -in $supportedversions) { $OSsupported = "True" } else { $OSsupported = "False" } } ##Domain Firewall $domainfirewall= ((Get-NetFirewallProfile | select Name, Enabled | where-object Name -eq Domain | select Enabled).Enabled).ToString() ##Private Firewall $privatefirewall= ((Get-NetFirewallProfile | select Name, Enabled | where-object Name -eq Private | select Enabled).Enabled).ToString()

```
##Public Firewall
$publicfirewall= ((Get-NetFirewallProfile | select
Name, Enabled | where-object Name -eq Public
| select Enabled).Enabled).ToString()

##Antivirus
$allav = Get-MpComputerStatus

##AM Enabled
$amenabled =
($allav.AMServiceEnabled).ToString()

##AS Enabled
$asenabled =
($allav.AntispywareEnabled).ToString()

##AS Age
$asage =
$allav.AntispywareSignatureLastUpdated
if ($asage -lt $7daysago) {
   $asage = "False"
}
else {
   $asage = "True"
}


##AV Enabled
$avenabled =
($allav.AntivirusEnabled).ToString()

##AV Age
$avage = $allav.AntivirusSignatureLastUpdated
if ($avage -lt $7daysago) {
   $avage = "False"
}
else {
   $avage = "True"
}

##NISE Enabled
$niseenabled = ($allav.NISEnabled).ToString()

##NISE Age
$niseage = $allav.NISSignatureLastUpdated
if ($niseage -lt $7daysago) {
   $niseage = "False"
}
else {
```

```
    $niseage = "True"
}

##OP Enabled
$openabled =
($allav.OnAccessProtectionEnabled).ToString()

##RP Enabled
$rpenabled =
($allav.RealtimeProtectionEnabled).ToString()

##TP Enabled
$tpenabled =
($allav.IsTamperProtected).ToString()

##Quick Scan Overdue
$quickscanoverdue =
($allav.QuickScanOverdue).ToString()

##Full Scan Overdue
$fullscanoverdue =
($allav.FullScanOverdue).ToString()

##Signature out of date
$signatureoutofdate =
($allav.DefenderSignaturesOutOfDate).ToString()

##Active Malware
$noactivemalware = Get-MpThreatDetection
if ($null -eq $noactivemalware) {
    $noactivemalware = "True"
}
else {
    $noactivemalware = "False"
}

##Encrypted



##TPM
$TPMpresent = ((get-
tpm).TpmPresent).ToString()

##TPM Activated
$TPMactivated = ((get-
tpm).TPMactivated).ToString()

##TPM Enabled
$TPMenabled = ((get-
tpm).TPMenabled).ToString()
```

	##Bitlocker $bitlockerprotected = (get-bitlockervolume).ProtectionStatus $bitlockerencryption = (get-bitlockervolume).VolumeStatus if (($bitlockerprotected -eq "On") -and ($bitlockerencryption -eq "FullyEncrypted")) { $bitlocker = "True" } else { $bitlocker = "False" } $hash = @{ UpdateStatus = $strUpdateStatus OSsupported = $OSsupported DomainFirewall = $domainfirewall PrivateFirewall = $privatefirewall PublicFirewall = $publicfirewall AMEnabled = $amenabled ASEnabled = $asenabled ASAge = $asage AVEnabled = $avenabled AVAge = $avage NISEnabled = $niseenabled NISEAge = $niseage OPEnabled = $openabled RPEEnabled = $rpenabled TPEEnabled = $tpenabled QuickScanOverdue = $quickscanoverdue FullScanOverdue = $fullscanoverdue SignatureOutOfDate = $signatureoutofdate NoActiveMalware = $noactivemalware Bitlocker = $bitlocker TPMpresent = $TPMpresent TPMactivated = $TPMactivated TPMenabled = $TPMenabled } return $hash | ConvertTo-Json -Compress
Run this script using the logged on credentials	No
Enforce script signature check	No
Run script in 64 bit PowerShell Host	Yes

Table 244. Settings - Custom Compliance Script