Feature updates for Windows 10 and later

Feature Updates

Windows 11 22H2

Name	Value
Basics	
Name	Windows 11 22H2
Description	
Policy type	Feature updates for Windows 10 and later
Created	01 July 2023 17:21:14
Last modified	01 July 2023 17:21:14
Scope tags	Default

Table 1. Basics - Windows 11 22H2

Name	Value
Deployment settings	
Feature update to deploy	Windows 11, version 22H2
Rollout options	

Table 2. Settings - Windows 11 22H2

Group
Included Groups
Autopilot-Devices

Table 3. Assignments - Windows 11 22H2

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
Last modified	01 July 2023 16:43:55
Scope tags	Default

Table 4. Basics - MDE-AppGuard-Active

Name	Value
App and browser isolation	
Turn on Application Guard	Not configured

Application Guard allow use of Root Certificate Authorities from the user's device	Not configured
Application Guard allow print to local printers	Not configured
Application Guard allow print to network printers	Not configured
Application Guard allow print to PDF	Not configured
Application Guard allow print to XPS	Not configured
Windows network isolation policy	Not configured

Table 5. Settings - MDE-AppGuard-Active

Group
Included Groups
Autopilot-Devices

Table 6. 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)
Last modified	01 July 2023 16:43:55
Scope tags	Default

Table 7. Basics - MDE-Web Protection-Active

Name	Value
Web Protection (Microsoft Edge Legacy)	
Enable network protection	Not configured
Require SmartScreen for Microsoft Edge Legacy	Not configured
Block malicious site access	Not configured
Block unverified file download	Not configured

Table 8. Settings - MDE-Web Protection-Active

Group
Included Groups
Autopilot-Devices

Table 9. 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
Last modified	01 July 2023 16:43:56
Scope tags	Default

Table 10. Basics - Bitlocker Policy

Name	Value
BitLocker - Base Settings	
Enable Full disk or Used Space only encryption for OS and fixed data drives	Not configured
Require storage cards to be encrypted (mobile only)	Not configured
Hide prompt about third-party encryption	Not configured
Configure client-driven recovery password rotation	Not configured
BitLocker - Fixed Drive Settings	
BitLocker fixed drive policy	Not configured
BitLocker - OS Drive Settings	
BitLocker system drive policy	Not configured
BitLocker - Removable Drive Settings	
BitLocker removable drive policy	Not configured

Table 11. Settings - Bitlocker Policy

Group
Included Groups
Autopilot-Devices

Table 12. 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
Last modified	01 July 2023 16:43:54
Scope tags	Default

Table 13. Basics - Edge Baseline

Name	Value
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 14. Settings - Edge Baseline

Group
Included Groups
Autopilot-Devices

Table 15. 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
Last modified	01 July 2023 16:43:55
Scope tags	Default

Table 16. Basics - Windows 10 Security Baseline

Name	Value
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	Configure
Block write access to removable data-drives not protected by BitLocker	Yes
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 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	Yes
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 warnings about uncommon files	Disabled
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 content from different domains within windows	Disabled
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 controls not marked as safe	Disable
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 controls not marked as safe	Disable
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	Enable
Block Office communication apps from creating child processes	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	Yes
Turn on real-time protection	Yes
Scan scripts that are used in Microsoft browsers	Yes
Scan archive files	Yes
Turn on behavior monitoring	Yes
Turn on cloud-delivered protection	Yes
Scan incoming email messages	Yes
Scan removable drives during full scan	Yes
Block Office applications from injecting code into other processes	Block
Block Office applications from creating executable content	Block
Block all Office applications from creating child processes	Block
Block Win32 API calls from Office macro	Block
Block execution of potentially obfuscated scripts (js/vbs/ps)	Block
Block JavaScript or VBScript from launching downloaded executable content	Block
Block executable content download from email and webmail clients	Block
Block credential stealing from the Windows local security authority subsystem (lsass.exe)	Enable
Defender potentially unwanted app action	Block
Block untrusted and unsigned processes that run from USB	Block
Enable network protection	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 17. Settings - Windows 10 Security Baseline

Group
Included Groups
Autopilot-Devices

Table 18. Assignments - Windows 10 Security Baseline

Endpoint analytics

Health Scripts

Remediate Store Icon

Name	Value
Basics	
Name	Remediate Store Icon
Description	Remove Windows Store from Taskbar
Created	01 July 2023 16:44:02
Last modified	01 July 2023 16:44:02
Version	1
Scope tags	Default

Table 19. Basics - Remediate Store Icon

Name	Value
Script settings	
Detection script	Yes
Remediation script	Yes
Run this script using the logged-on credentials	Yes
Enforce script signature check	No
Run script in 64-bit PowerShell	Yes

Table 20. Settings - Remediate Store Icon

Detection script

```
##We're looping through the verbs so it's going to be easier to count
$pinned = 0
##Loop through verbs for the store app
$apps = ((New-Object -Com Shell.Application).NameSpace('shell:::{4234d49b-0245-4df3-b780-3893943456e1}').Items() | Where-Object { $_.Name -eq "Microsoft Store" }).verbs()
foreach ($app in $apps) {
    ##Is Unpin an option?
if ($app.Name -eq "Unpin from tas&kbar") {
    ##Yep, increment the counter
$pinned++
}
}

#Has it been found?
if ($pinned -gt 0) {
Write-Warning "Store has been pinned"
exit 1
}
else {
write-host "Not pinned"
exit 0
}
```

Table 21. Detection script - Remediate Store Icon

Remediation script

```

$apps = ((New-Object -Com Shell.Application).NameSpace('shell:::{4234d49b-0245-4df3-b780-3893943456e1}').Items())
```

```
foreach ($app in $apps) {
$appname = $app.Name
if ($appname -like "*store*") {
$finalname = $app.Name
}
}

((New-Object -Com Shell.Application).NameSpace('shell:::{4234d49b-0245-4df3-
b780-3893943456e1}').Items() | ?{$_.Name -eq $finalname}).Verbs() |
?{$_.Name.replace('&','') -match 'Unpin from taskbar'} | %{$_.DoIt(); $exec =
$true}
```

Table 22. Remediation script - Remediate Store Icon

Group
Included Groups
Intune-Users

Table 23. Assignments - Remediate Store Icon

Update rings for Windows 10 and later

Update Policies

Broad Ring

Name	Value
Basics	
Name	Broad Ring
Description	
Platform supported	Windows 10 and later
Profile type	Software Updates
Created	01 July 2023 19:02:49
Last modified	01 July 2023 19:02:49
Version	1
Scope tags	Default

Table 24. 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	Enable
Select pre-release 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	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 25. Settings - Broad Ring

Group
Included Groups
Intune-Users
Excluded Groups
Intune-Preview-Users
Intune-Pilot-Users
Intune-VIP-Users

Table 26. Assignments - Broad Ring

iOS Update Policy

Name	Value
Basics	
Name	iOS Update Policy
Description	
Platform supported	iOS/iPadOS
Profile type	iOS Update policy
Created	01 July 2023 16:43:05
Last modified	01 July 2023 16:43:05
Version	1
Scope tags	Default

Table 27. 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 28. Settings - iOS Update Policy

Group
Included Groups
Intune-Users

Table 29. Assignments - iOS Update Policy

Pilot Ring

Name	Value
Basics	
Name	Pilot Ring
Description	
Platform supported	Windows 10 and later
Profile type	Software Updates
Created	01 July 2023 17:29:58
Last modified	01 July 2023 17:29:58
Version	1
Scope tags	Default

Table 30. Basics - Pilot Ring

Name	Value
Settings	
Update settings	
Microsoft product updates	Allow
Windows drivers	Allow
Quality update deferral period (days)	5
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	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 31. Settings - Pilot Ring

Group
Included Groups
Intune-Pilot-Users

Table 32. Assignments - Pilot Ring

Preview Ring

Name	Value
Basics	
Name	Preview Ring

Description	
Platform supported	Windows 10 and later
Profile type	Software Updates
Created	01 July 2023 17:30:29
Last modified	01 July 2023 17:30:29
Version	1
Scope tags	Default

Table 33. 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	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 34. Settings - Preview Ring

Group
Included Groups
Intune-Preview-Users

Table 35. Assignments - Preview Ring

VIP Ring

Name	Value
Basics	
Name	VIP Ring
Description	
Platform supported	Windows 10 and later
Profile type	Software Updates

Created	01 July 2023 17:31:13
Last modified	01 July 2023 17:31:13
Version	1
Scope tags	Default

Table 36. Basics - VIP Ring

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	Enable
Select pre-release channel	
User experience settings	
Automatic update behavior	Notify download
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 37. Settings - VIP Ring

Group
Included Groups
Intune-VIP-Users

Table 38. Assignments - VIP Ring

Scripts

Scripts (PowerShell)

Defender for Endpoint Active-Tag

Name	Value
Basics	
Name	Defender for Endpoint Active-Tag
Description	
Profile type	PowerShell script
Created	01 July 2023 19:03:08
Last modified	01 July 2023 19:03:08
Scope tags	Default

Table 39. Basics - Defender for Endpoint 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 40. Settings - Defender for Endpoint 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 41. PowerShell script - Defender for Endpoint Active-Tag

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
Created	01 July 2023 19:03:09
Last modified	01 July 2023 19:03:09
Scope tags	Default

Table 42. 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 43. 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 44. PowerShell script - Disable running or installing downloaded software with invalid signature

Remove Bloat

Name	Value
Basics	
Name	Remove Bloat
Description	Removes bloat from Win10 machine
Profile type	PowerShell script
Created	01 July 2023 19:03:08
Last modified	01 July 2023 19:03:08
Scope tags	Default

Table 45. 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 46. 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 47. PowerShell script - 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
Created	01 July 2023 19:03:09
Last modified	01 July 2023 19:03:09
Scope tags	Default

Table 48. 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 49. 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 50. PowerShell script - Require domain users to elevate when setting a network's location

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...
Created	01 July 2023 16:43:33
Last modified	01 July 2023 16:43:33
Scope tags	Default

Table 51. 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 52. 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 53. Assignments - Company Portal

Edge

Name	Value
Basics	
Name	Edge
Description	Edge
App type	Microsoft Edge (Windows 10 and later)
Created	01 July 2023 16:44:05
Last modified	01 July 2023 17:08:50
Scope tags	Default

Table 54. Basics - Edge

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

App suite configuration	
	Stable

Table 55. Settings - Edge

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

Table 56. Assignments - Edge

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
Created	01 July 2023 19:03:21
Last modified	01 July 2023 19:03:21
Version	"cc00ed29-0000-0c00-0000-64a06a690000"
Scope tags	Default

Table 57. 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 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 Condeco 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 Field Service Mobile Microsoft Invoicing Microsoft Edge Power Automate Azure Information Protection Microsoft Launcher Microsoft Lists Microsoft Kaizala Power Apps Microsoft Excel Skype for Business Microsoft 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	
Data protection	
<b>Data Transfer</b>	
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	
<b>Encryption</b>	
Encrypt org data	Require
Encrypt org data on enrolled devices	Require
<b>Functionality</b>	
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	
<b>Functionality</b>	
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	
<b>Functionality</b>	
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 58. Settings - 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
Created	01 July 2023 19:03:23
Last modified	01 July 2023 19:03:23
Version	"cc00242a-0000-0c00-0000-64a06a6b0000"
Scope tags	Default

Table 59. 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 AssetScan For Intune Appian for Intune BlueJeans Video Conferencing Diligent Boards Box for EMM iAnnotate for Intune / O365 Breezy for Intune Comfy F2 Manager - Intune F2 Touch Intune CellTrust SL2™ for Intune Cisco Jabber for Intune Webex for Intune Condeco 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 ZERØ - email for attorneys Zero for Intune Incorta (BestBuy) Omnipresence Go CAPTOR ISEC7 Mobile Exchange Delegate ISEC7 Mobile Exchange Delegate for Intune Klaxoon for Intune

	Leap Work for Intune Nexis Newsdesk™ Mobile Lexmark Mobile Print Intune LumApps for Intune M-Files for Intune MangoApps, Work from Anywhere My Portal By MangoApps Senses Meetings by Decisions MentorcliQ Cortana Field Service Mobile Microsoft Dynamics 365 Microsoft Invoicing Microsoft Dynamics 365 for phones Field Service (Dynamics 365) Dynamics 365 Sales Skype for Business Microsoft Kaizala Microsoft Power Apps Microsoft Edge Microsoft 365 Admin Microsoft Excel Microsoft Outlook Microsoft PowerPoint Microsoft Word Microsoft Lens Microsoft 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 Visio Viewer 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	
Data protection	
<b>Data Transfer</b>	
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
<b>Encryption</b>	
Encrypt org data	Require
<b>Functionality</b>	
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	
<b>Functionality</b>	
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	
<b>Functionality</b>	
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 60. Settings - 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
Created	01 July 2023 16:43:24
Last modified	01 July 2023 16:43:24
Scope tags	Default

Table 61. 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 62. Settings - Autopilot Profile

Group
Included Groups
Autopilot-Devices

Table 63. Assignments - Autopilot Profile

Enrollment Status Page

AutoPilot Enrollment

Name	Value
Basics	
Name	AutoPilot Enrollment
Description	Custom Enrollment Status
Policy type	Enrollment Status Page
Created	01 July 2023 16:48:26
Last modified	01 July 2023 17:07:54
Version	2
Scope tags	Default

Table 64. 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	All

Table 65. Settings - AutoPilot Enrollment

Group
Included Groups
Autopilot-Devices

Table 66. Assignments - AutoPilot Enrollment

Device configuration

Settings Catalog

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
Created	01 July 2023 16:43:08
Last modified	01 July 2023 16:43:08
Scope tags	Default

Table 67. Basics - MDE-ASR Rules

Name	Value
Defender	
Attack Surface Reduction Rules	
Block Adobe Reader from creating child processes	Block

Block execution of potentially obfuscated scripts	Block
Block Win32 API calls from Office macros	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 all Office applications from creating child processes	Block
Block untrusted and unsigned processes that run from USB	Block
Block process creations originating from PSExec and WMI commands	Block
Block persistence through WMI event subscription	Block
Block Office applications from creating executable content	Block
Block Office applications from injecting code into other processes	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 68. Settings - MDE-ASR Rules

Group
Included Groups
Autopilot-Devices

Table 69. 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
Created	01 July 2023 16:43:08
Last modified	01 July 2023 16:43:08
Scope tags	Default

Table 70. 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 High severity threats	Remove. Removes files from system.
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.

Table 71. Settings - MDE-AV-Active

Group
Included Groups
Autopilot-Devices

Table 72. Assignments - MDE-AV-Active

MDE-EP-Active

Name	Value
Basics	
Name	MDE-EP-Active
Description	Exploit Protection Rules
Profile type	Settings catalog
Category	Attack surface reduction
Policy type	Exploit Protection

Platform supported	Windows 10 and later
Created	01 July 2023 16:43:09
Last modified	01 July 2023 16:43:09
Scope tags	Default

Table 73. Basics - MDE-EP-Active

Name	Value

Table 74. Settings - MDE-EP-Active

MDE-FW-Active

Name	Value
Basics	
Name	MDE-FW-Active
Description	Turns on Windows Firewall
Profile type	Settings catalog
Category	Firewall
Policy type	Microsoft Defender Firewall
Platform supported	Windows 10 and later
Created	01 July 2023 16:43:09
Last modified	01 July 2023 16:43:09
Scope tags	Default

Table 75. 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 76. Settings - MDE-FW-Active

Group
Included Groups
Autopilot-Devices

Table 77. 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
Created	01 July 2023 16:43:09
Last modified	01 July 2023 16:43:09
Scope tags	Default

Table 78. 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 79. Settings - MDE-Targeted-TamperPro

Group
Included Groups
Autopilot-Devices

Table 80. 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
Created	01 July 2023 19:03:00
Last modified	01 July 2023 19:03:00

Scope tags	Default

Table 81. 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 82. Settings - Office Settings - User

Group
Included Groups
Intune-Users

Table 83. 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
Created	01 July 2023 19:03:01
Last modified	01 July 2023 19:03:01
Scope tags	Default

Table 84. 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 85. 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

Created	01 July 2023 19:03:01
Last modified	01 July 2023 19:03:01
Scope tags	Default

Table 86. 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 87. 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
Created	01 July 2023 19:03:02
Last modified	01 July 2023 19:03:02
Scope tags	Default

Table 88. 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 89. 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
Created	01 July 2023 19:03:02
Last modified	01 July 2023 19:03:02

Scope tags	Default

Table 90. 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 91. Settings - Office-VIPRing

StoreSettings

Name	Value
Basics	
Name	StoreSettings
Description	Store for Business Restrictions
Profile type	Settings catalog
Platform supported	Windows 10 and later
Created	01 July 2023 19:03:03
Last modified	01 July 2023 19:03:03
Scope tags	Default

Table 92. Basics - StoreSettings

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

Table 93. Settings - StoreSettings

Group
Included Groups
Intune-Users

Table 94. 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
Created	01 July 2023 19:03:03
Last modified	01 July 2023 19:03:03
Scope tags	Default

Table 95. Basics - Windows 11 Start Menu

Name	Value
Experience	
Configure Chat Icon	Disabled
Start	

Configure Start Pins	{
	"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 96. Settings - Windows 11 Start Menu

Group
Included Groups
Intune-Users

Table 97. 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
Created	01 July 2023 19:03:04
Last modified	01 July 2023 19:03:04
Scope tags	Default

Table 98. 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 99. Settings - Windows Health Monitoring

Group
Included Groups
Intune-Users

Table 100. 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
Created	01 July 2023 19:02:46
Last modified	01 July 2023 19:02:46
Version	1
Scope tags	Default

Table 101. 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 102. Settings - Base Android Config

Group
Included Groups
Intune-Users

Table 103. 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
Created	01 July 2023 19:02:47
Last modified	01 July 2023 19:02:47
Version	1
Scope tags	Default

Table 104. 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	Yes
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 105. Settings - Baseline Device Restrictions

Group
Included Groups
Intune-Users

Table 106. 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
Created	01 July 2023 19:02:48
Last modified	01 July 2023 19:02:48
Version	1
Scope tags	Default

Table 107. 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 108. Settings - Baseline iOS Features

Group
Included Groups
Intune-Users

Table 109. 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
Created	01 July 2023 19:02:50
Last modified	01 July 2023 19:02:50
Version	1
Scope tags	Default

Table 110. Basics - Intune data collection policy

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

Table 111. Settings - Intune data collection policy

Group
Included Groups
Intune-Users

Table 112. 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
Created	22 June 2023 19:18:48
Last modified	22 June 2023 19:18:48
Version	1
Scope tags	Default

Table 113. 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 114. Settings - iOS device restriction to block Game Center

Group
Included Groups
fd189654-22d3-4f98-bdc5-ff47290cbee9

Table 115. Assignments - iOS device restriction to block Game Center

macOS Protection

Name	Value
Basics	
Name	macOS Protection
Description	Enabled Firewall, Filevault and Gatekeeper
Platform supported	macOS
Profile type	Endpoint protection
Created	01 July 2023 19:02:52
Last modified	01 July 2023 19:02:52
Version	1
Scope tags	Default

Table 116. 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 117. Settings - macOS Protection

Group
Included Groups
Intune-Users

Table 118. Assignments - macOS Protection

macOS Restrictions

Name	Value
Basics	
Name	macOS Restrictions
Description	macOS Security Baseline Settings
Platform supported	macOS
Profile type	Device restrictions
Created	01 July 2023 19:02:52
Last modified	01 July 2023 19:02:52
Version	1
Scope tags	Default

Table 119. 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 120. Settings - macOS Restrictions

Group
Included Groups
Intune-Users

Table 121. Assignments - macOS Restrictions

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
Created	01 July 2023 19:02:54
Last modified	01 July 2023 19:02:54
Version	1

Scope tags	Default

Table 122. 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 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	Yes

developer extensions	
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	<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 123. Settings - Start-Menu-W10

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

Table 124. Applicability Rules - Start-Menu-W10

Group
Included Groups
Intune-Users

Table 125. Assignments - Start-Menu-W10

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
Created	01 July 2023 19:03:05
Last modified	01 July 2023 19:03:05
Version	1
Scope tags	Default

Table 126. Basics - Android Compliance

Name	Value
Device Health	
Require the device to be at or under the Device Threat Level	Medium
Google Play Protect	
SafetyNet device attestation	Check basic integrity
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 127. Settings - Android Compliance

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

Table 128. Actions for noncompliance - Android Compliance

Group
Included Groups

Intune-Users

Table 129. 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
Created	01 July 2023 19:03:04
Last modified	01 July 2023 19:03:04
Version	1
Scope tags	Default

Table 130. 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 131. Settings - iOS Compliance

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

Table 132. Actions for noncompliance - iOS Compliance

Group
Included Groups
Intune-Users

Table 133. 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
Created	01 July 2023 19:03:06
Last modified	01 July 2023 19:03:06
Version	1
Scope tags	Default

Table 134. 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 135. Settings - macOS Compliance

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

Table 136. Actions for noncompliance - macOS Compliance

Group
Included Groups
Intune-Users

Table 137. Assignments - macOS Compliance

Windows Essential Compliance

Name	Value
Basics	
Name	Windows Essential Compliance
Description	
Platform supported	Windows 10 and later
Profile type	Windows 10 and later compliance policy
Created	01 July 2023 19:03:06
Last modified	01 July 2023 19:03:06
Version	1
Scope tags	Default

Table 138. Basics - Windows Essential Compliance

Name	Value
Custom Compliance	
Custom compliance	Not configured

Device Health	
Windows Health Attestation Service evaluation rules	
Require BitLocker	Not configured
Require Secure Boot to be enabled on the device	Not configured
Require code integrity	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.	Require
Device Security	
Firewall	Require
Trusted Platform Module (TPM)	Require
Antivirus	Require
Antispyware	Require
Defender	
Microsoft Defender Antimalware	Require
Microsoft Defender Antimalware minimum version	
Microsoft Defender Antimalware security intelligence up-to-date	Require
Real-time protection	Require
Microsoft Defender for Endpoint	
Microsoft Defender for Endpoint rules	
Require the device to be at or under the machine risk score:	Medium

Table 139. Settings - Windows Essential Compliance

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

Table 140. Actions for noncompliance - Windows Essential Compliance

Group
Included Groups
Intune-Users

Table 141. Assignments - Windows Essential Compliance