Australian Government

Digital Transformation Agency

Intune Security Baselines – As-built as-configured

March 2020

dta

Contents

Overview

Purpose

The purpose of this as-built as-configured (ABAC) document is to detail the Intune Security Baselines deployed within the solution. These baselines align to the design decisions captured within the associated blueprint document. All settings captured within this ABAC were captured as of the time of writing.

Associated Documentation

The following table lists the documents that were referenced during the creation of this ABAC.

Table 1 Associated Documentation

Name	Version	Date
DTA – Blueprint Solution Overview	March	03/2020
DTA – Platform Design	March	03/2020
DTA – Workstation Design	March	03/2020
DTA – Office 365 Design	March	03/2020
DTA – Office 365 – ABAC	March	03/2020
DTA – Platform – ABAC	March	03/2020
DTA – Software Updates – ABAC	March	03/2020
DTA – Intune Applications – ABAC	March	03/2020
DTA – Intune Enrolment – ABAC	March	03/2020
DTA – Conditional Access Policies – ABAC	March	03/2020
DTA – Intune Compliance – ABAC	March	03/2020
DTA – Intune Configuration – ABAC	March	03/2020

Device Security Baselines

The following tables lists the device security baseline profiles deployed within the tenant. Security baselines are utilised to maintain a device security level congruent to the standards determined in the design documents.

ACSC1709Guidance-DefenderATPSecurityBaseline_Settings

Table 2 ACSC1709Guidance-DefenderATPSecurityBaseline details

Profile name	ACSC1709Guidance-DefenderATPSecurityBaseline
Current Baseline	June 2019 v1
Assigned	Yes

Table 3 ACSC1709Guidance-DefenderATPSecurityBaseline_Settings settings

Name	Value
Scan scripts loaded in Microsoft web browsers	True
Scan incoming mail messages	True
Office apps launch child process	block
Encrypt devices	True
Security association idle time before deletion	300
File Transfer Protocol	True
Defender sample submission consent	sendSafeSamplesAutomatically
Network Inspection System (NIS)	True
Signature update interval (in hours)	4
Script downloaded payload execution	block
Configure low CPU priority for scheduled scans	True
External content on enterprise sites	False
Defender block on access protection	True

Upload XML	<?xml version="1.0" encoding="UTF-8"?><MitigationPolicy><AppConfig Executable="ONEDRIVE.EXE"><DEP Enable="true" EmulateAtlThunks="false" /><ASLR Enable="true" ForceRelocateImages="true" /><ImageLoad BlockRemoteImageLoads="true" /><Payload EnableExportAddressFilter="true" EnableExportAddressFilterPlus="true" EnableImportAddressFilter="true" EnableRopStackPivot="true" EnableRopCallerCheck="true" EnableRopSimExec="true" /></AppConfig><AppConfig Executable="firefox.exe"><DEP Enable="true" EmulateAtlThunks="false" /><ASLR ForceRelocateImages="true" RequireInfo="false" BottomUp="true" HighEntropy="false" /></AppConfig><AppConfig Executable="fltldr.exe"><DEP Enable="true" EmulateAtlThunks="false" /><ImageLoad BlockRemoteImageLoads="true" /><ChildProcess DisallowChildProcessCreation="true" /><Payload EnableExportAddressFilter="true" EnableExportAddressFilterPlus="true" EnableImportAddressFilter="true" EnableRopStackPivot="true" EnableRopCallerCheck="true" EnableRopSimExec="true" /></AppConfig><AppConfig Executable="GROOVE.EXE"><DEP Enable="true" EmulateAtlThunks="false" /><ASLR Enable="true" ForceRelocateImages="true" /><ImageLoad BlockRemoteImageLoads="true" /><Payload EnableExportAddressFilter="true" EnableExportAddressFilterPlus="true" EnableImportAddressFilter="true" EnableRopStackPivot="true" EnableRopCallerCheck="true" EnableRopSimExec="true" /><ChildProcess DisallowChildProcessCreation="false" /></AppConfig><AppConfig Executable="Acrobat.exe"><DEP Enable="true" EmulateAtlThunks="false" /><ASLR ForceRelocateImages="true" RequireInfo="false" BottomUp="true" HighEntropy="false" /><Payload EnableExportAddressFilter="true" EnableExportAddressFilterPlus="true" EnableImportAddressFilter="true" EnableRopStackPivot="true" EnableRopCallerCheck="true" EnableRopSimExec="true" /></AppConfig><AppConfig Executable="AcroRd32.exe"><DEP Enable="true" EmulateAtlThunks="false" /><ASLR ForceRelocateImages="true" RequireInfo="false" BottomUp="true" HighEntropy="false" /><Payload EnableExportAddressFilter="true" EnableExportAddressFilterPlus="true" EnableImportAddressFilter="true" EnableRopStackPivot="true" EnableRopCallerCheck="true" EnableRopSimExec="true" /></AppConfig><AppConfig Executable="chrome.exe"><DEP Enable="true" EmulateAtlThunks="false" /></AppConfig><AppConfig Executable="EXCEL.EXE"><DEP Enable="true" EmulateAtlThunks="false" /><ASLR Enable="true" ForceRelocateImages="true" /><Payload EnableExportAddressFilter="true"

EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig Executable="iexplore.exe"><DEP
Enable="true" EmulateAtlThunks="false" /><ASLR
ForceRelocateImages="true" RequireInfo="false"
BottomUp="true" HighEntropy="false" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig
Executable="INFOPATH.EXE"><DEP Enable="true"
EmulateAtlThunks="false" /><ASLR Enable="true"
ForceRelocateImages="true" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig Executable="java.exe"><DEP
Enable="true" EmulateAtlThunks="false" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig Executable="javaw.exe"><DEP
Enable="true" EmulateAtlThunks="false" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig Executable="javaws.exe"><DEP
Enable="true" EmulateAtlThunks="false" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig Executable="LYNC.EXE"><DEP
Enable="true" EmulateAtlThunks="false" /><ASLR
Enable="true" ForceRelocateImages="true" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig
Executable="MSACCESS.EXE"><DEP Enable="true"
EmulateAtlThunks="false" /><ASLR Enable="true"
ForceRelocateImages="true" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig Executable="MSPUB.EXE"><DEP
Enable="true" EmulateAtlThunks="false" /><ASLR
Enable="true" ForceRelocateImages="true" /><Payload

EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig Executable="OIS.EXE"><DEP
Enable="true" EmulateAtlThunks="false" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig
Executable="OUTLOOK.EXE"><DEP Enable="true"
EmulateAtlThunks="false" /><ASLR Enable="true"
ForceRelocateImages="true" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig Executable="plugin-
container.exe"><DEP Enable="true" EmulateAtlThunks="false"
/><Payload EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig
Executable="POWERPNT.EXE"><DEP Enable="true"
EmulateAtlThunks="false" /><ASLR Enable="true"
ForceRelocateImages="true" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig
Executable="PPTVIEW.EXE"><DEP Enable="true"
EmulateAtlThunks="false" /><ASLR Enable="true"
ForceRelocateImages="true" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig Executable="VISIO.EXE"><DEP
Enable="true" EmulateAtlThunks="false" /><ASLR
Enable="true" ForceRelocateImages="true" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig
Executable="VPREVIEW.EXE"><DEP Enable="true"
EmulateAtlThunks="false" /><ASLR Enable="true"
ForceRelocateImages="true" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"

	/></AppConfig><AppConfig Executable="WINWORD.EXE"><DEP Enable="true" EmulateAtlThunks="false" /><ASLR Enable="true" ForceRelocateImages="true" /><Payload EnableExportAddressFilter="true" EnableExportAddressFilterPlus="true" EnableImportAddressFilter="true" EnableRopStackPivot="true" EnableRopCallerCheck="true" EnableRopSimExec="true" /></AppConfig><AppConfig Executable="wmplayer.exe"><DEP Enable="true" EmulateAtlThunks="false" /><Payload EnableExportAddressFilter="false" EnableExportAddressFilterPlus="false" EnableImportAddressFilter="false" EnableRopStackPivot="true" EnableRopCallerCheck="true" EnableRopSimExec="true" /></AppConfig><AppConfig Executable="wordpad.exe"><DEP Enable="true" EmulateAtlThunks="false" /><Payload EnableExportAddressFilter="true" EnableExportAddressFilterPlus="true" EnableImportAddressFilter="true" EnableRopStackPivot="true" EnableRopCallerCheck="true" EnableRopSimExec="true" /></AppConfig></MitigationPolicy>
Prevent credential stealing	enable
Email content execution	block
Packet queuing	deviceDefault
Type of system scan to perform	quick
Scan all downloads	True
Adobe Reader launch in a child process	enable
Block execution of unverified files	True
Days before deleting quarantined malware	0
Network protection	enable
Scheduled scan start time	t2AM
Cloud-delivered protection	True
Defender potentially unwanted app action	block
Script obfuscated macro code	block
Scan removable drives during a full scan	True
Require SmartScreen for Microsoft Edge	True
Enumeration of external devices incompatible with Kernel DMA Protection	deviceDefault
Defender cloud extended timeout	50

Firewall profile domain	
Firewall profile public	
Scan archive files	True
Firewall profile private	
Application Guard	False
Defender system scan schedule	userDefined
Hardware device installation by device identifiers	
Block malicious site access	True
Block user editing of exploit protection interface	True
Behavior monitoring	True
BitLocker removable drive policy	
Block unverified file download	True
Scan files opened from network folders	True
Untrusted USB process	block
Office apps other process injection	block
Firewall pre shared key encoding method	uTF8
Office macro code allow Win32 imports	block
Configure Windows Hello for Business:	False
Encrypt storage card (mobile only)	True
Expedite telemetry reporting frequency	True
Block direct memory access	True
Defender cloud block level	high
BitLocker fixed drive policy	
Certificate revocation list verification	deviceDefault
Clipboard behavior	notConfigured
BitLocker system drive policy	
Sample sharing for all files	True
Folder protection	auditMode
Real-time monitoring	True
CPU usage limit during a scan	50

Office communication apps launch in a child process	enable
Scan mapped network drives during a full scan	True
Lowercase letters in PIN:	allowed
Block end-user access to Defender	True
Special characters in PIN:	allowed
Hardware device installation by setup classes	
Quick scan start time	t2AM
Require SmartScreen for apps and files	True
Windows network isolation policy	
Uppercase letters in PIN:	allowed
Office apps executable content creation or launch	block

ACSC1709Guidance-EdgeSecurityBaseline_Settings

Table 4 ACSC1709Guidance-EdgeSecurityBaseline_Settings details

Profile name	ACSC1709Guidance-EdgeSecurityBaseline
Current Baseline	October 2019 (Edge version 77 and later)
Assigned	Yes

Table 5 ACSC1709Guidance-EdgeSecurityBaseline_Settings settings

Name	Value
Prevent bypassing Microsoft Defender SmartScreen prompts for sites	enabled
Default Adobe Flash setting	2
Minimum SSL version enabled	tls1.2
Minimum SSL version enabled	enabled
Prevent bypassing of Microsoft Defender SmartScreen warnings about downloads	enabled
Allow users to proceed from the SSL warning page	disabled
Default Adobe Flash setting	enabled
Enable site isolation for every site	enabled

Supported authentication schemes	enabled
Enable saving passwords to the password manager	disabled
Control which extensions cannot be installed	enabled
Configure Microsoft Defender SmartScreen	enabled
Allow user-level native messaging hosts (installed without admin permissions)	disabled
Supported authentication schemes	
Extension IDs the user should be prevented from installing (or * for all)	

ACSC1709Guidance-MDMSecurity_Settings

Table 6 ACSC1709Guidance-MDMSecurity_Settings details

Profile name	ACSC1709Guidance-MDMSecurity
Current Baseline	May 2019
Assigned	Yes

Table 7 ACSC1709Guidance-MDMSecurity_Settings settings

Name	Value
RPC unauthenticated client options	authenticated
Password minimum character set count	3
Internet Explorer restricted zone updates to status bar via script	disabled
Internet Explorer internet zone drag and drop or copy and paste files	disable
Block user control over installations	True
Number of sign-in failures before wiping device	10
Internet Explorer restricted zone .NET Framework reliant components	disable
Scan incoming mail messages	True
Office apps launch child process	block
Internet Explorer local machine zone do not run antimalware against Active X controls	disabled

Internet Explorer internet zone access to data sources	disable
Internet Explorer restricted zone drag content from different domains within windows	disabled
Defender sample submission consent	sendSafeSamplesAutomatically
Restrict anonymous access to named pipes and shares	True
Minimum session security for NTLM SSP based servers	ntlmV2And128BitEncryption
Internet Explorer certificate address mismatch warning	enabled
Internet Explorer restricted zone less privileged sites	disable
Block display of toast notifications	True
Internet Explorer restricted zone automatic prompt for file downloads	disabled
Signature update interval (in hours)	4
Internet Explorer internet zone .NET Framework reliant components	disable
Block storing run as credentials	enabled
Internet Explorer internet zone allow only approved domains to use tdc ActiveX controls	enabled
Internet Explorer restricted zone script initiated windows	disabled
Apply UAC restrictions to local accounts on network logon	enabled
Internet Explorer internet zone include local path when uploading files to server	disabled
Internet Explorer disable processes in enhanced protected mode	enabled
Minutes of lock screen inactivity until screen saver activates	15
Internet Explorer ignore certificate errors	disabled
Prevent use of camera	enabled
Internet Explorer internet zone loading of XAML files	disable
Script downloaded payload execution	block

Internet Explorer internet zone automatic prompt for file downloads	disabled
Auto play default auto run behavior	doNotExecute
Internet Explorer restricted zone security warning for potentially unsafe files	disable
Require password on wake while plugged in	enabled
Internet Explorer internet zone cross site scripting filter	enabled
Network IP source routing protection level	highestProtection
Internet Explorer fallback to SSL3	noSites
Internet Explorer encryption support	
Require client to always digitally sign communications	True
Password expiration (days)	60

Upload XML	<?xml version="1.0" encoding="UTF-8"?><MitigationPolicy><AppConfig Executable="ONEDRIVE.EXE"><DEP Enable="true" EmulateAtlThunks="false" /><ASLR Enable="true" ForceRelocateImages="true" /><ImageLoad BlockRemoteImageLoads="true" /><Payload EnableExportAddressFilter="true" EnableExportAddressFilterPlus="true" EnableImportAddressFilter="true" EnableRopStackPivot="true" EnableRopCallerCheck="true" EnableRopSimExec="true" /></AppConfig><AppConfig Executable="firefox.exe"><DEP Enable="true" EmulateAtlThunks="false" /><ASLR ForceRelocateImages="true" RequireInfo="false" BottomUp="true" HighEntropy="false" /></AppConfig><AppConfig Executable="fltldr.exe"><DEP Enable="true" EmulateAtlThunks="false" /><ImageLoad BlockRemoteImageLoads="true" /><ChildProcess DisallowChildProcessCreation="true" /><Payload EnableExportAddressFilter="true" EnableExportAddressFilterPlus="true" EnableImportAddressFilter="true" EnableRopStackPivot="true" EnableRopCallerCheck="true" EnableRopSimExec="true" /></AppConfig><AppConfig Executable="GROOVE.EXE"><DEP Enable="true" EmulateAtlThunks="false" /><ASLR Enable="true" ForceRelocateImages="true" /><ImageLoad BlockRemoteImageLoads="true" /><Payload EnableExportAddressFilter="true" EnableExportAddressFilterPlus="true" EnableImportAddressFilter="true" EnableRopStackPivot="true" EnableRopCallerCheck="true" EnableRopSimExec="true" /><ChildProcess DisallowChildProcessCreation="false" /></AppConfig><AppConfig Executable="Acrobat.exe"><DEP Enable="true" EmulateAtlThunks="false" /><ASLR ForceRelocateImages="true" RequireInfo="false" BottomUp="true" HighEntropy="false" /><Payload EnableExportAddressFilter="true" EnableExportAddressFilterPlus="true" EnableImportAddressFilter="true" EnableRopStackPivot="true" EnableRopCallerCheck="true" EnableRopSimExec="true" /></AppConfig><AppConfig Executable="AcroRd32.exe"><DEP Enable="true" EmulateAtlThunks="false" /><ASLR ForceRelocateImages="true" RequireInfo="false" BottomUp="true" HighEntropy="false" /><Payload EnableExportAddressFilter="true" EnableExportAddressFilterPlus="true" EnableImportAddressFilter="true" EnableRopStackPivot="true" EnableRopCallerCheck="true" EnableRopSimExec="true" /></AppConfig><AppConfig Executable="chrome.exe"><DEP Enable="true" EmulateAtlThunks="false" /></AppConfig><AppConfig Executable="EXCEL.EXE"><DEP Enable="true" EmulateAtlThunks="false" /><ASLR Enable="true" ForceRelocateImages="true" /><Payload EnableExportAddressFilter="true"

EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig Executable="iexplore.exe"><DEP
Enable="true" EmulateAtlThunks="false" /><ASLR
ForceRelocateImages="true" RequireInfo="false"
BottomUp="true" HighEntropy="false" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig
Executable="INFOPATH.EXE"><DEP Enable="true"
EmulateAtlThunks="false" /><ASLR Enable="true"
ForceRelocateImages="true" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig Executable="java.exe"><DEP
Enable="true" EmulateAtlThunks="false" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig Executable="javaw.exe"><DEP
Enable="true" EmulateAtlThunks="false" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig Executable="javaws.exe"><DEP
Enable="true" EmulateAtlThunks="false" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig Executable="LYNC.EXE"><DEP
Enable="true" EmulateAtlThunks="false" /><ASLR
Enable="true" ForceRelocateImages="true" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig
Executable="MSACCESS.EXE"><DEP Enable="true"
EmulateAtlThunks="false" /><ASLR Enable="true"
ForceRelocateImages="true" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig Executable="MSPUB.EXE"><DEP
Enable="true" EmulateAtlThunks="false" /><ASLR
Enable="true" ForceRelocateImages="true" /><Payload

EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig Executable="OIS.EXE"><DEP
Enable="true" EmulateAtlThunks="false" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig
Executable="OUTLOOK.EXE"><DEP Enable="true"
EmulateAtlThunks="false" /><ASLR Enable="true"
ForceRelocateImages="true" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig Executable="plugin-
container.exe"><DEP Enable="true" EmulateAtlThunks="false"
/><Payload EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig
Executable="POWERPNT.EXE"><DEP Enable="true"
EmulateAtlThunks="false" /><ASLR Enable="true"
ForceRelocateImages="true" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig
Executable="PPTVIEW.EXE"><DEP Enable="true"
EmulateAtlThunks="false" /><ASLR Enable="true"
ForceRelocateImages="true" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig Executable="VISIO.EXE"><DEP
Enable="true" EmulateAtlThunks="false" /><ASLR
Enable="true" ForceRelocateImages="true" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"
/></AppConfig><AppConfig
Executable="VPREVIEW.EXE"><DEP Enable="true"
EmulateAtlThunks="false" /><ASLR Enable="true"
ForceRelocateImages="true" /><Payload
EnableExportAddressFilter="true"
EnableExportAddressFilterPlus="true"
EnableImportAddressFilter="true" EnableRopStackPivot="true"
EnableRopCallerCheck="true" EnableRopSimExec="true"

	/></AppConfig><AppConfig Executable="WINWORD.EXE"><DEP Enable="true" EmulateAtlThunks="false" /><ASLR Enable="true" ForceRelocateImages="true" /><Payload EnableExportAddressFilter="true" EnableExportAddressFilterPlus="true" EnableImportAddressFilter="true" EnableRopStackPivot="true" EnableRopCallerCheck="true" EnableRopSimExec="true" /></AppConfig><AppConfig Executable="wmplayer.exe"><DEP Enable="true" EmulateAtlThunks="false" /><Payload EnableExportAddressFilter="false" EnableExportAddressFilterPlus="false" EnableImportAddressFilter="false" EnableRopStackPivot="true" EnableRopCallerCheck="true" EnableRopSimExec="true" /></AppConfig><AppConfig Executable="wordpad.exe"><DEP Enable="true" EmulateAtlThunks="false" /><Payload EnableExportAddressFilter="true" EnableExportAddressFilterPlus="true" EnableImportAddressFilter="true" EnableRopStackPivot="true" EnableRopCallerCheck="true" EnableRopSimExec="true" /></AppConfig></MitigationPolicy>
Internet Explorer locked down internet zone smart screen	enabled
Block password saving	enabled
Authentication level	lmNtlmV2AndNotLmOrNtm
Ink Workspace	enabled
Internet Explorer restricted zone launch applications and files in an iFrame	disable
Disable indexing encrypted items	True
System boot start driver initialization	goodAndUnknown
Block Internet sharing	True
Prevent clients from sending unencrypted passwords to third party SMB servers	True
Prevent credential stealing	enable
Email content execution	block
Internet Explorer bypass smart screen warnings about uncommon files	disabled
Internet Explorer internet zone popup blocker	enable
Internet Explorer processes consistent MIME handling	enabled

Microsoft accounts optional for Windows Store apps	enabled
Standby states when sleeping while on battery	disabled
Adobe Reader launch in a child process	enable
Secure RPC communication	enabled
Block execution of unverified files	True
Internet Explorer restricted zone java permissions	disableJava
Block connection to non-domain networks	enabled
Internet Explorer Active X controls in protected mode	disabled
Internet Explorer restricted zone loading of XAML files	disable
Internet Explorer processes scripted window security restrictions	enabled
Network protection	enable
Internet Explorer restricted zone run Active X controls and plugins	disable
Internet Explorer restricted zone script Active X controls marked safe for scripting	disable
Require server digitally signing communications always	True
Administrator elevation prompt behavior	promptForCredentialsOnTheSecureDesktop
SMB v1 client driver start configuration	disableDriver
Internet Explorer restricted zone logon options	anonymous
Block drive redirection	enabled
Defender schedule scan day	noScheduledScan
Block Internet download for web publishing and online ordering wizards	enabled
Block MSI app installations with elevated privileges	True
Internet Explorer trusted zone initialize and script Active X controls not marked as safe	disable
SMB v1 server	disabled
Cloud-delivered protection	True

Block Automatically connecting to Wi-Fi hotspots	True
Auto play mode	disabled
Defender potentially unwanted app action	block
Credential Guard	enableWithUEFILock
Internet Explorer check server certificate revocation	enabled
Internet Explorer internet zone less privileged sites	disable
Required password	alphanumeric
Security log maximum file size in KB	196608
Internet Explorer restricted zone file downloads	disable
Configure secure access to UNC paths	
Block data execution prevention	disabled
Internet Explorer internet zone run .NET Framework reliant components signed with Authenticode	disable
Script obfuscated macro code	block
Internet Explorer prevent per user installation of Active X controls	enabled
Scan removable drives during a full scan	True
Require SmartScreen for Microsoft Edge	True
Minimum session security for NTLM SSP based clients	ntlmV2And128BitEncryption
Enumeration of external devices incompatible with Kernel DMA Protection	blockAll
Internet Explorer prevent managing smart screen filter	enable
Internet Explorer processes MIME sniffing safety feature	enabled
Internet Explorer restricted zone download signed Active X controls	disable
Virtualization based security	withoutDMA
Internet Explorer auto complete	disabled
Smart card removal behavior	lockWorkstation

Block anonymous enumeration of SAM accounts and shares	True
Internet Explorer internet zone allow VBscript to run	disable
Internet Explorer restricted zone allow only approved domains to use tdc Active X controls	enabled
Internet Explorer trusted zone do not run antimalware against Active X controls	disabled
Firewall profile domain	
Firewall profile public	
Scan archive files	True
Internet Explorer local machine zone java permissions	disableJava
Internet Explorer intranet zone do not run antimalware against Active X controls	disabled
Firewall profile private	
Block third-party suggestions in Windows Spotlight	True
Internet Explorer restricted zone scriptlets	disabled
Use enhanced anti-spoofing, when available:	True
Standby states when sleeping while plugged in	disabled
System log maximum file size in KB	65536
Internet Explorer processes notification bar	enabled
Internet Explorer internet zone download signed ActiveX controls	disable
Internet Explorer restricted zone smart screen	enabled
Internet Explorer remove run this time button for outdated Active X controls	enabled
Internet Explorer internet zone launch applications and files in an iframe	disable
Prompt for password upon connection	enabled
Minimum password length	8
Block remote logon with blank password	True
Internet Explorer restricted zone navigate windows and frames across different domains	disable

Digest authentication	disabled
Internet Explorer internet zone smart screen	enabled
Internet Explorer locked down trusted zone java permissions	disableJava
Internet Explorer check signatures on downloaded programs	enabled
Hardware device installation by device identifiers	
Block malicious site access	True
Internet Explorer restricted zone scripting of web browser controls	disabled
Internet Explorer restricted zone cross site scripting filter	enabled
Internet Explorer restricted zone binary and script behaviors	disable
Standard user elevation prompt behavior	promptForCredentialsOnTheSecureDesktop
Behavior monitoring	True
Require admin approval mode for administrators	True
BitLocker removable drive policy	
Remote desktop services client connection encryption level	high
Internet Explorer security settings check	enabled
Internet Explorer internet zone security warning for potentially unsafe files	prompt
Internet Explorer intranet zone java permissions	highSafety
Internet Explorer block outdated Active X controls	enabled
Internet Explorer restricted zone popup blocker	enable
Block unverified file download	True
Scan files opened from network folders	True
Untrusted USB process	block
Block Password Manager	True
Block consumer specific features	True

Application log maximum file size in KB	65536
Require password	True
Internet Explorer processes MK protocol security restriction	enabled
Remote host delegation of non-exportable credentials	enabled
Require password on wake while on battery	enabled
Prevent slide show	enabled
Block simple passwords	True
Office apps other process injection	block
Internet Explorer trusted zone java permissions	highSafety
Internet Explorer restricted zone scripting of java applets	disable
Internet Explorer locked down restricted zone java permissions	disableJava
Prevent anonymous enumeration of SAM accounts	True
Internet Explorer internet zone allow only approved domains to use ActiveX controls	enabled
Block Windows Spotlight	True
Internet Explorer include all network paths	disabled
Voice activate apps from locked screen	disabled
Allow remote calls to security accounts manager	O:BAG:BAD:(A;;RC;;;BA)
Internet Explorer internet zone protected mode	enable
Internet Explorer internet zone initialize and script Active X controls not marked as safe	disable
Basic authentication	disabled
Internet Explorer locked down restricted zone smart screen	enabled
Internet Explorer crash detection	disabled
Office macro code allow Win32 imports	block
Configure Windows Hello for Business:	False
Structured exception handling overwrite protection	enabled

Power shell shell script block logging	enabled
Internet Explorer internet zone java permissions	disableJava
Internet Explorer restricted zone active scripting	disable
Internet Explorer internet zone logon options	prompt
Internet Explorer restricted zone allow vbscript to run	disable
Network ignore NetBIOS name release requests except from WINS servers	enabled
Internet Explorer internet zone drag content from different domains across windows	disabled
Internet Explorer intranet zone initialize and script Active X controls not marked as safe	disable
Remote Assistance solicited	
Internet Explorer download enclosures	disabled
Internet Explorer restricted zone download unsigned Active X controls	disable
Internet Explorer internet zone drag content from different domains within windows	disabled
Internet Explorer processes restrict Active X install	enabled
Use admin approval mode	True
Password minimum age in days	1
Only allow UI access applications for secure locations	True
Block direct memory access	True
Defender cloud block level	notConfigured
Detect application installations and prompt for elevation	True
Internet Explorer internet zone scriptlets	disable
Internet Explorer restricted zone drag and drop or copy and paste files	disable
Internet Explorer software when signature is invalid	disabled
Block downloading of print drivers over HTTP	enabled

Internet Explorer restricted zone copy and paste via script	disable
Internet Explorer restricted zone drag content from different domains across windows	disabled
Internet Explorer users adding sites	disabled
Enable virtualization based security	True
Internet Explorer internet zone script initiated windows	disabled
Internet Explorer security zones use only machine settings	enabled
Prevent storing LAN manager hash value on next password change	True
Prevent certificate error overrides	True
Internet Explorer locked down local machine zone java permissions	disableJava
Internet Explorer restricted zone do not run antimalware against Active X controls	disabled
Internet Explorer restricted zone run .NET Framework reliant components signed with Authenticode	disable
Enumerate administrators	disabled
Internet Explorer restricted zone access to data sources	disable
Internet Explorer internet zone do not run antimalware against ActiveX controls	disabled
Internet Explorer internet zone copy and paste via script	disable
Internet Explorer use Active X installer service	enabled
Internet Explorer processes protection from zone elevation	enabled
Internet Explorer internet zone download unsigned ActiveX controls	disable
Internet Explorer internet zone navigate windows and frames across different domains	disable
Internet Explorer internet zone updates to status bar via script	disabled
Real-time monitoring	True

Internet Explorer restricted zone include local path when uploading files to server	disabled
Block client digest authentication	enabled
Office communication apps launch in a child process	enable
Internet Explorer processes restrict file download	enabled
Network IPv6 source routing protection level	highestProtection
Internet Explorer restricted zone allow only approved domains to use Active X controls	enabled
Virtualize file and registry write failures to per user locations	True
Block auto play for non-volume devices	enabled
Internet Explorer restricted zone initialize and script Active X controls not marked as safe	disable
Lowercase letters in PIN:	allowed
Special characters in PIN:	allowed
Hardware device installation by setup classes	
Block game DVR (desktop only)	True
Unencrypted traffic	disabled
Internet Explorer users changing policies	disabled
Internet Explorer restricted zone protected mode	enable
Internet Explorer internet zone user data persistence	disabled
Internet Explorer internet zone scripting of web browser controls	disabled
Require SmartScreen for apps and files	True
Minimum PIN length:	6
Internet Explorer restricted zone user data persistence	disabled
Network ICMP redirects override OSPF generated routes	disabled
Client unencrypted traffic	disabled
Internet Explorer locked down intranet zone java permissions	disableJava

Internet Explorer enhanced protected mode	enabled
Uppercase letters in PIN:	allowed
Internet Explorer bypass smart screen warnings	disabled
Prevent reuse of previous passwords	24
Internet Explorer restricted zone meta refresh	disabled
Client basic authentication	disabled
Office apps executable content creation or launch	block
Block heap termination on corruption	disabled
Launch system guard	enabled