

NOVEMBER 2020

# Guide to Hardening Windows 10

For Administrators, Developers and Office Workers

# TABLE OF CONTENTS

<b>Introduction .....</b>	<b>4</b>
Prerequisites .....	4
User roles.....	4
<b>EFI (BIOS) Configuration .....</b>	<b>5</b>
To be enabled: .....	5
To be disabled:.....	5
<b>Windows Defender Firewall .....</b>	<b>6</b>
Enable logging of dropped packets.....	6
Disable enforcement of local rules and disable notifications.....	7
Block outbound connections by default.....	8
Secure potentially vulnerable protocols.....	9
Add exceptions to basic services, like Windows Update and Microsoft Defender.....	9
Test Microsoft Defender connectivity and Windows Update.....	15
Create new rules based on the use case.....	16
<b>Logging.....</b>	<b>17</b>
Configure Advanced Audit Policy .....	17
Enable PowerShell logging.....	20
<b>Application Allowlisting .....</b>	<b>22</b>
Enable AppLocker .....	22
Switching the Application Identity service to automatic startup using group policy .....	22
Switching the Application Identity service to automatic startup locally .....	22
Importing default rules .....	22
Hardening AppLocker .....	24
Enabling AppLocker in audit mode.....	26
Switching AppLocker to enforcing mode.....	27
<b>Protecting credentials.....</b>	<b>28</b>
Enable Credential Guard .....	28
Protect lsass.exe (for system incompatible with Credential Guard).....	29
Prevent brute force of credentials .....	30
Delete BitLocker encryption keys after X unsuccessful attempts .....	30
<b>Improving the detection &amp; security of Microsoft Defender .....</b>	<b>31</b>
Enforcing a more aggressive cloud detection .....	31
Block the execution of files deemed unreputable by Microsoft Defender.....	31
Enable detection of potentially unwanted programs (PUPs).....	32
Enforce system-wide SmartScreen filter.....	33

# TABLE OF CONTENTS

Prevent SmartScreen bypasses .....	33
<b>Mitigating Execution and Persistence Techniques.....</b>	<b>34</b>
Blocking persistence through WMI .....	34
Blocking code execution through WMI and PSEXec.....	34
Block svchost.exe code injection .....	35
Protecting kernel memory and blocking vulnerable drivers .....	35
Preventing boot of a system with malicious drivers.....	37
Block code injection into sensitive processes.....	37
Remove debug permission from administrators.....	39
Restrict execution capabilities of malware spread via Office documents .....	39
Blocking obfuscated scripts.....	40
Allow execution of only signed PowerShell scripts.....	41
Block executable files downloaded via JavaScript or VBScript .....	41
Block executable files originating from mail clients or webmail .....	42
<b>Encryption &amp; Physical Attacks.....</b>	<b>43</b>
Hardening BitLocker against DMA attacks .....	43
Use of 256-bit AES for operating system drives and fixed data drives .....	44
Use of 256-bit AES in XTS mode for removable data drives.....	44
Enforcing Full encryption type.....	45
Enable stronger authentication for BitLocker .....	46
Protection against BadUSB attacks .....	48
Prevent code execution from removable drives .....	48
Enable BitLocker .....	49
<b>Conclusion .....</b>	<b>50</b>

# INTRODUCTION

Windows 10 is the most widely used desktop operating system in enterprise environment. It features extensive security policies, allowing in-depth configuration of each security subsystem. To ensure secure computing, administrators must take in consideration all the threats the enterprise might face and deploy appropriate policies. This often includes strict firewall and AppLocker rules.

With the rapid pace of Windows 10 feature updates, the recommended security policies change very often, and security guides should change accordingly.

This paper will provide an in-depth guide to hardening Windows 10, including configuration of BitLocker, AppLocker, and Windows Firewall. For each security policy or recommendation, impact to security and usability is assessed, along with a MITRE ATT&CK technique mitigated by the policy.

Some of the security policies mentioned require additional configuration by administrators based on a specific use cases, a set of deployed software and a network environment. We do not recommend home users to deploy the policies.

## Prerequisites

- Computer running Windows 10 Enterprise/Education, version 20H1 / 20H2 (most of these settings will apply to older versions of Windows 10 or lower SKUs, but compatibility is not guaranteed).
- TPM module.

## User roles

Not all policies are suitable for all types of users. For this reason, we will be analyzing the suitability of each policy for two types of users depending on their role:

**Administrator/Developer** – Uses an administrator account, launches a lot of software, and connects different accessories and hardware.

**Office Worker** – Uses a standard account and the set of their software is limited. Office Workers do not change hardware and accessories without the assistance of the IT department.

# EFI (BIOS) Configuration

Many of the modern Windows 10 features rely on hardware and firmware support, therefore it is necessary to properly configure the system's EFI.

Due to major differences between EFI configuration interfaces of various manufacturers, we cannot provide exact steps. Some of the below mentioned options will feature a different name or will be missing entirely on some systems.

## To be enabled:

- Secure boot
- Intel Boot Guard
- Intel VT-x \ Intel VT-D \ AMD-V \ IOMMU \ virtualization support
- Execute Disable Bit
- BIOS administrator password
- TPM module (on systems with both hardware and firmware option is hardware preferred)
- Device Guard
- DMA Protection

## To be disabled:

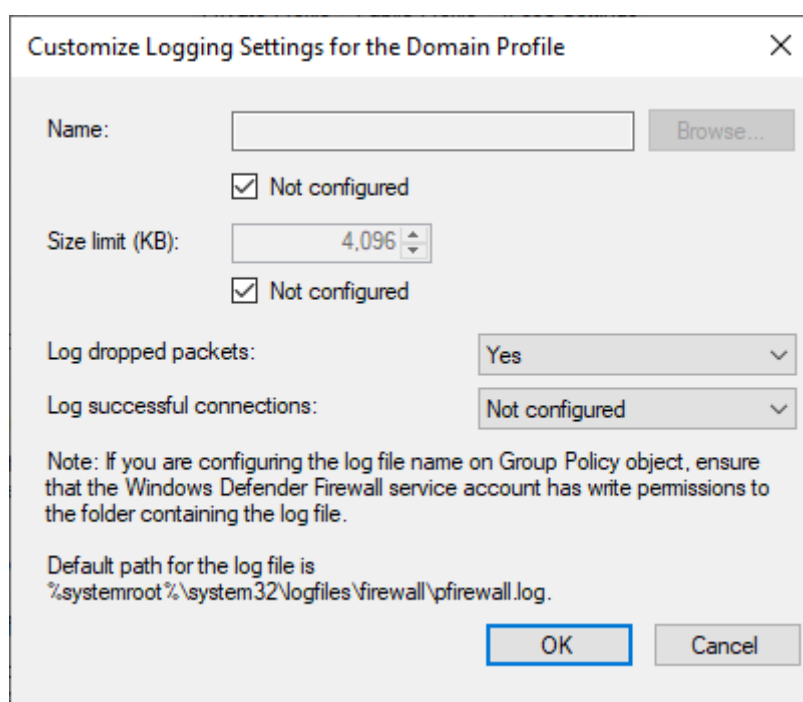
- Compatibility Support Mode (CSM) support

# Windows Defender Firewall

## Enable logging of dropped packets

**Policy path:** *Computer Configuration\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security.*

Right-click on *Windows Defender Firewall with Advanced Security* and select *Properties*. Under *Logging*, select *Customize* and enable *Log dropped packets*.



*Screenshot 1. Enabling logging of dropped packets.*

Repeat the process for all the network profiles – Domain Profile, Private Profile, and Public Profile.

The default location for log file is: `%systemroot%\system32\LogFiles\Firewall\pfirewall.log` and the default size limit is 4,096KB. The location and log limit can be changed by right-clicking on *Windows Defender Firewall with Advanced Security* and selecting *Properties*. Under *Logging*, uncheck *Not configured* for both name and/or size limit and choose custom values. Make sure the location is accessible by all clients and is not user writable.

**Effects:** Locally added rules will not be enforced, and no notification will be display for a blocked incoming connection.

**Suitable for:** Everyone.

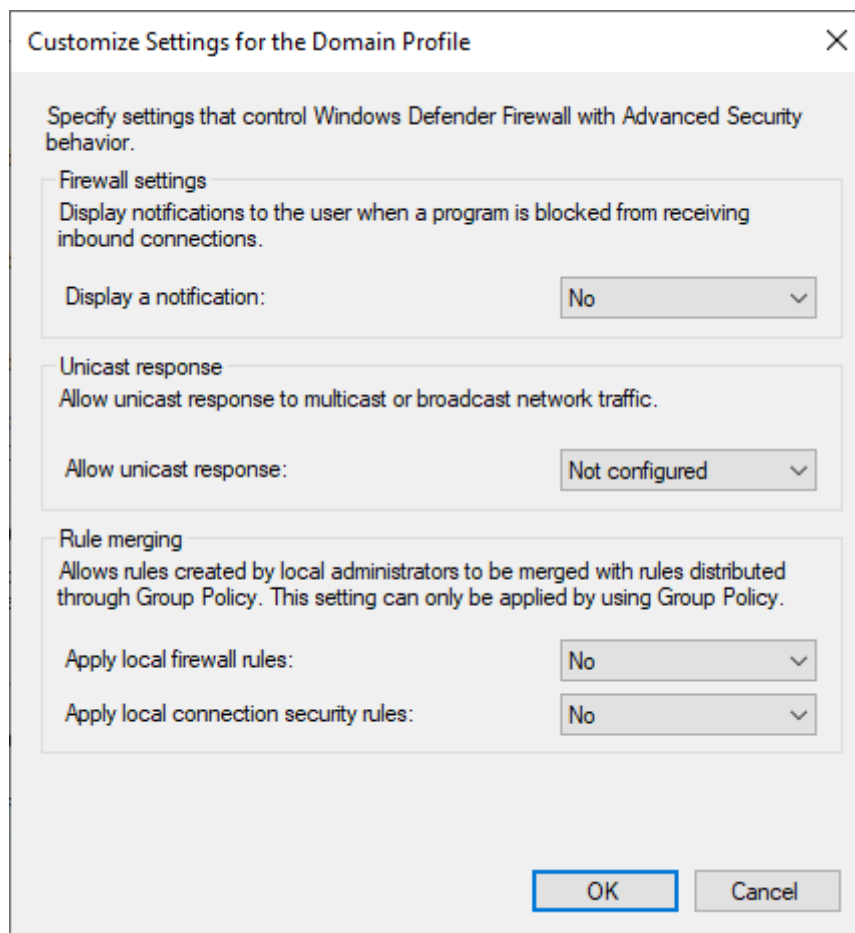
# Windows Defender Firewall

## Disable enforcement of local rules and disable notifications

**Policy path:** *Computer Configuration|Windows Settings|Security Settings|Windows Defender Firewall with Advanced Security|Windows Defender Firewall with Advanced Security.*

Right-click on *Windows Defender Firewall with Advanced Security* and select *Properties*. Under *Settings*, select *Customize* and disable the following settings:

- *Display a notification*
- *Apply local firewall rules*
- *Apply local connection security rules*



*Screenshot 2. Disabling notifications and enforcement of local rules.*

Repeat the process for all three network profiles – *Domain Profile*, *Private Profile*, and *Public Profile*.

**Effects:** Locally added rules will not be enforced, and no notification will be display for a blocked incoming connection.

**Suitable for:** Everyone.

# Windows Defender Firewall

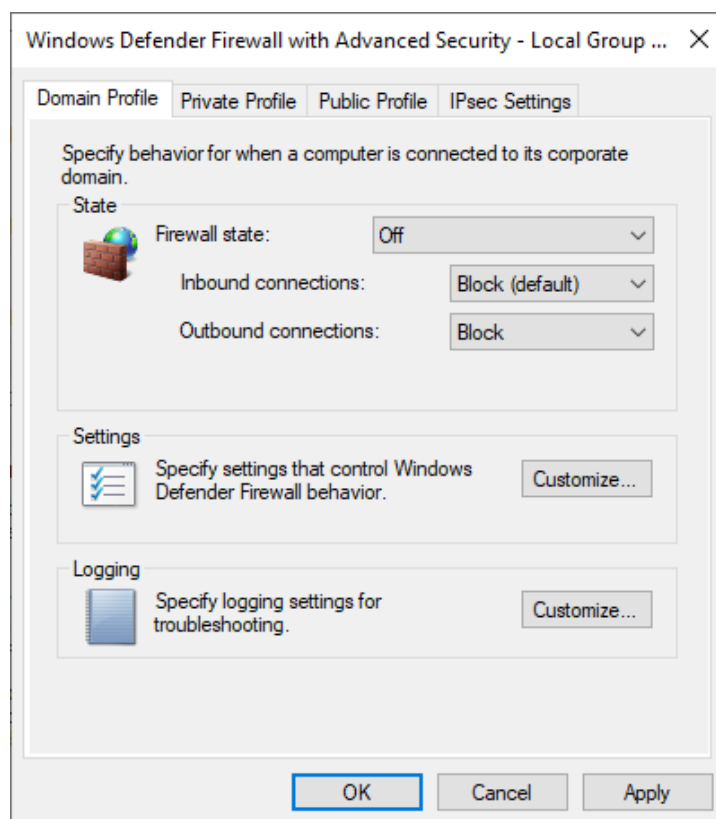
## Block outbound connections by default

Outbound connections are allowed by default. To achieve higher security, outbound connections can be blocked.

Keep in mind that blocking outbound connection will require extensive configuration and testing. Not even basic Windows services and built-in browsers will be able to connect without a manually created ruleset.

**Policy path:** *Computer Configuration\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security.*

Right-click on *Windows Defender Firewall with Advanced Security* and select *Properties*. Set *Firewall State* to *on*, set *Inbound connection* to *Block (Default)* and *Outbound connections* to *Block*.



*Screenshot 3. Blocking outbound connections by default.*

Repeat the process for all three network profiles – *Domain Profile*, *Private Profile*, and *Public Profile*.

**Effects:** Outbound connections will be blocked by default, unless explicitly allowlisted. Inbound connections are already blocked by default.

**Suitable for:** Office Workers.



# Windows Defender Firewall

## Secure potentially vulnerable protocols

Potentially vulnerable protocols include Server Message Block (SMB), Remote Desktop Protocol (RDP), Windows Remote Management (WinRM) and Network Basic Input/Output System (NetBIOS).

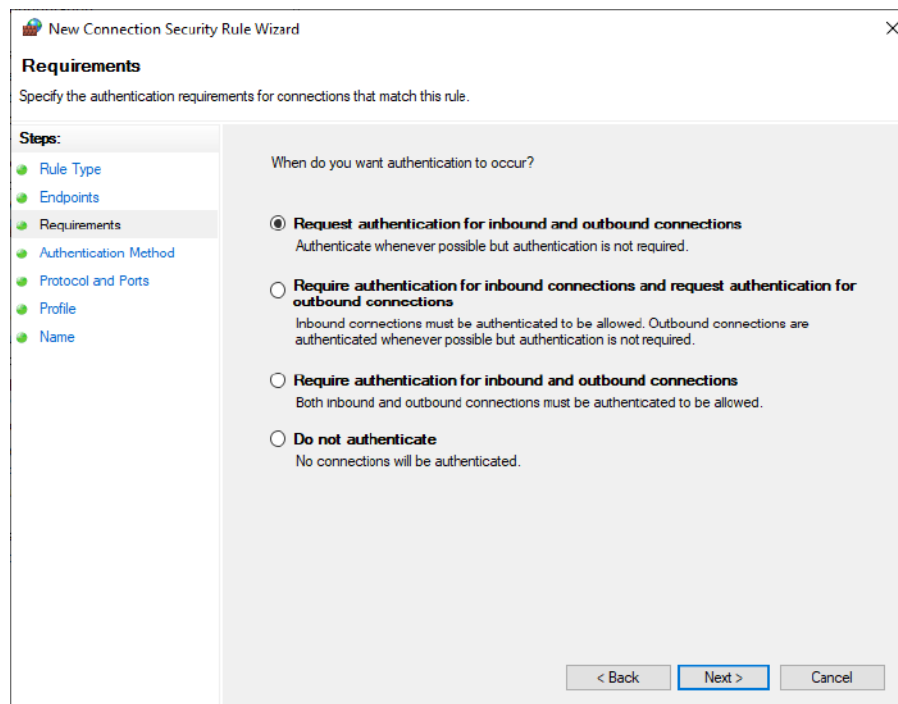
You can either restrict some ports to only select IP addresses or require an authenticated IPsec tunnel.

IPsec connection requirements can be configured by creating a connection security rule:

**Policy path:** *Computer Configuration\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security.*

Right-click on *Connection Security Rules* and select *New Rule...* Choose *Custom* rule type. In the next step, configure IP addresses for both endpoints or select *Any IP address*, if the rule should apply to all endpoints or if IP addresses are dynamically assigned.

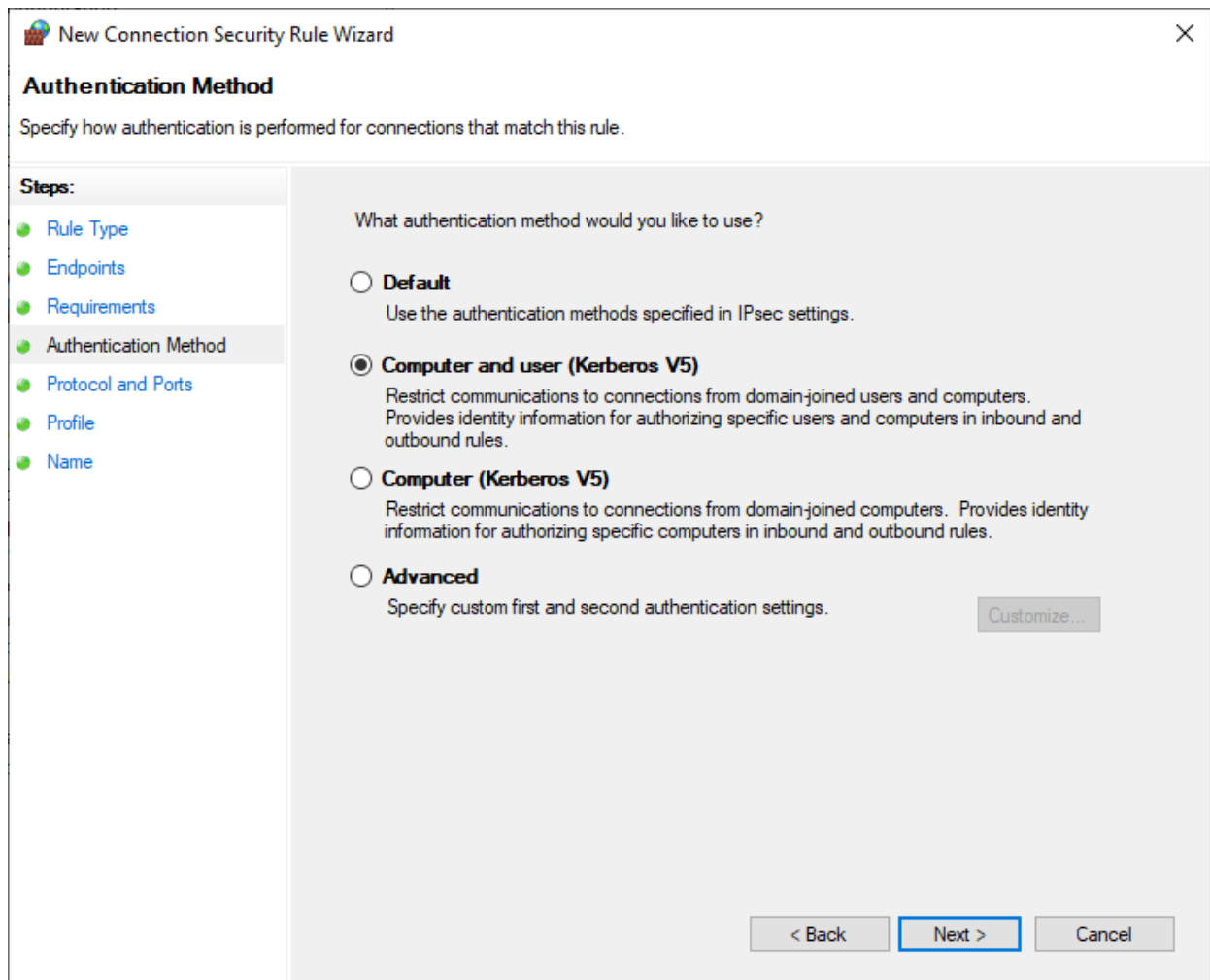
In the requirements section, you can either choose *Request authentication for inbound and outbound connections* or *Require authentication for inbound and outbound connections*. The former will allow unauthenticated connections while the latter will drop unauthenticated connections. Both options are viable for security purposes, as security requirements will be configured further by an inbound connection rule.



*Screenshot 4. Setting requirement to request authentication.*

The optimal authentication method is *Computer and user (Kerberos V5)* to also restrict connections based on user accounts. In the next two steps, specific ports and network profiles should be selected.

# Windows Defender Firewall



*Screenshot 5. Setting authentication method to Kerberos V5.*

# Windows Defender Firewall

The screenshot shows the 'New Connection Security Rule Wizard' window. The title bar reads 'New Connection Security Rule Wizard'. The main heading is 'Protocol and Ports'. Below it, the instruction says 'Specify the protocol and ports to which this rule applies.' On the left, a 'Steps' pane lists: Rule Type, Endpoints, Requirements, Authentication Method, Protocol and Ports (selected), Profile, and Name. The main area is titled 'To which ports and protocols does this rule apply?'. It contains the following fields: 'Protocol type' set to 'TCP', 'Protocol number' set to '6', 'Endpoint 1 port' set to 'Specific Ports' with a text box containing '3389' and an example '80, 445, 5000-5010', and 'Endpoint 2 port' set to 'All Ports' with an example '80, 445, 5000-5010'. At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

*Screenshot 6. Configuring the rule to apply to the default RDP port.*

The next step is be a creation of an inbound connection rule set to allow only secure connections. You can allow the use of null encapsulation mode for authenticity only or also require the encryption for integrity and confidentiality of the data. Keep in mind that encrypting the data will make any network-level inspection impossible.

**MITRE ATT&CK Technique ID:** T1190

**Effect on security:** IPsec authentication will be required for the configured network protocols.

**Effects on usability:** Connections that will fail to negotiate IPsec will fail.

**Suitable for:** Everyone.

# Windows Defender Firewall

## Add exceptions to basic services, like Windows Update and Microsoft Defender

With only default rules and outbound connection blocked, both Windows Update and Microsoft Defender will not work correctly. That would severely weaken security, as the system would receive no security updates, no definitions updates and cloud protection features.

To enable Windows Update, you need to add the following exceptions:

**Policy path:** *Computer Configuration\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Outbound Rules.*

Right-click on *Outbound Rules*, select *New Rule...* and *Custom*. Configure rules with the following options while leaving the rest at their default settings.

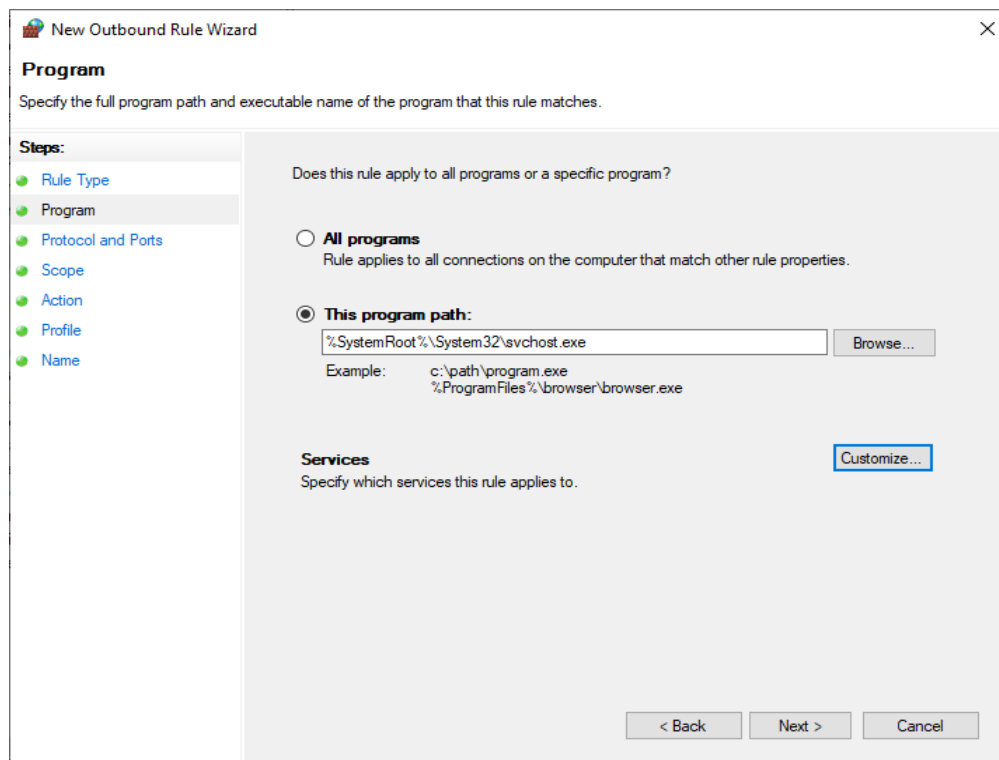
**Program path:** *%SystemRoot%\System32\svchost.exe.*

**Services:** *All services.*

**Protocol Type:** *TCP.*

**Ports:** *80, 443.*

**Action:** *Allow the connection.*



*Screenshot 7. Setting a rule for svchost.exe.*

# Windows Defender Firewall

Due to technical limitations of Windows, the exception must apply to all services in order to allow Windows Update. Ignore the security warning provided by Windows.

## To enable Microsoft Defender, add following rules:

**Program path:** *All programs.*

**Services:** *Applied to this service: Microsoft Defender Antivirus Network Inspection Service.*

**Protocol Type:** *TCP.*

**Action:** *Allow the connection.*

**Program path:** *All programs.*

**Services:** *Applied to this service: Microsoft Defender Antivirus Network Inspection Service.*

**Protocol Type:** *UDP.*

**Action:** *Allow the connection.*

**Program path:** *All programs.*

**Services:** *Applied to this service: Microsoft Defender Antivirus Service.*

**Protocol Type:** *TCP.*

**Action:** *Allow the connection.*

**Program path:** *All programs.*

**Services:** *Applied to this service: Microsoft Defender Antivirus Service.*

**Protocol Type:** *UDP.*

**Action:** *Allow the connection.*

**Program path:** *All programs.*

**Services:** *Applied to this service: Windows Defender Advanced Threat Protection Service.*

**Protocol Type:** *TCP.*

**Action:** *Allow the connection.*

# Windows Defender Firewall

**Program path:** *All programs.*

**Services:** *Applied to this service: Windows Defender Advanced Threat Protection Service.*

**Protocol Type:** *UDP.*

**Action:** *Allow the connection.*

Windows Defender path is often changing with software updates and therefore rules must be set for all programs.

**Program path:** *C:\windows\system32\smartscreen.exe.*

**Services:** *All services.*

**Protocol Type:** *TCP.*

**Action:** *Allow the connection.*

**Program path:** *C:\windows\system32\smartscreen.exe.*

**Services:** *All services.*

**Protocol Type:** *UDP.*

**Action:** *Allow the connection.*

## Enable DNS Client and Windows Time Service:

**Program path:** *C:\windows\system32\svchost.exe.*

**Services:** *DNS Client.*

**Protocol Type:** *TCP.*

**Action:** *Allow the connection.*

**Program path:** *C:\windows\system32\svchost.exe.*

**Services:** *DNS Client.*

**Protocol Type:** *UDP.*

**Action:** *Allow the connection.*

# Windows Defender Firewall

**Program path:** *C:\windows\system32\svchost.exe.*

**Services:** *Windows Time.*

**Protocol Type:** *UDP.*

**Remote port:** *123.*

**Action:** *Allow the connection.*

## Test Microsoft Defender connectivity and Windows Update

After setting exceptions, connectivity to Windows Update and Microsoft Defender needs to be verified.

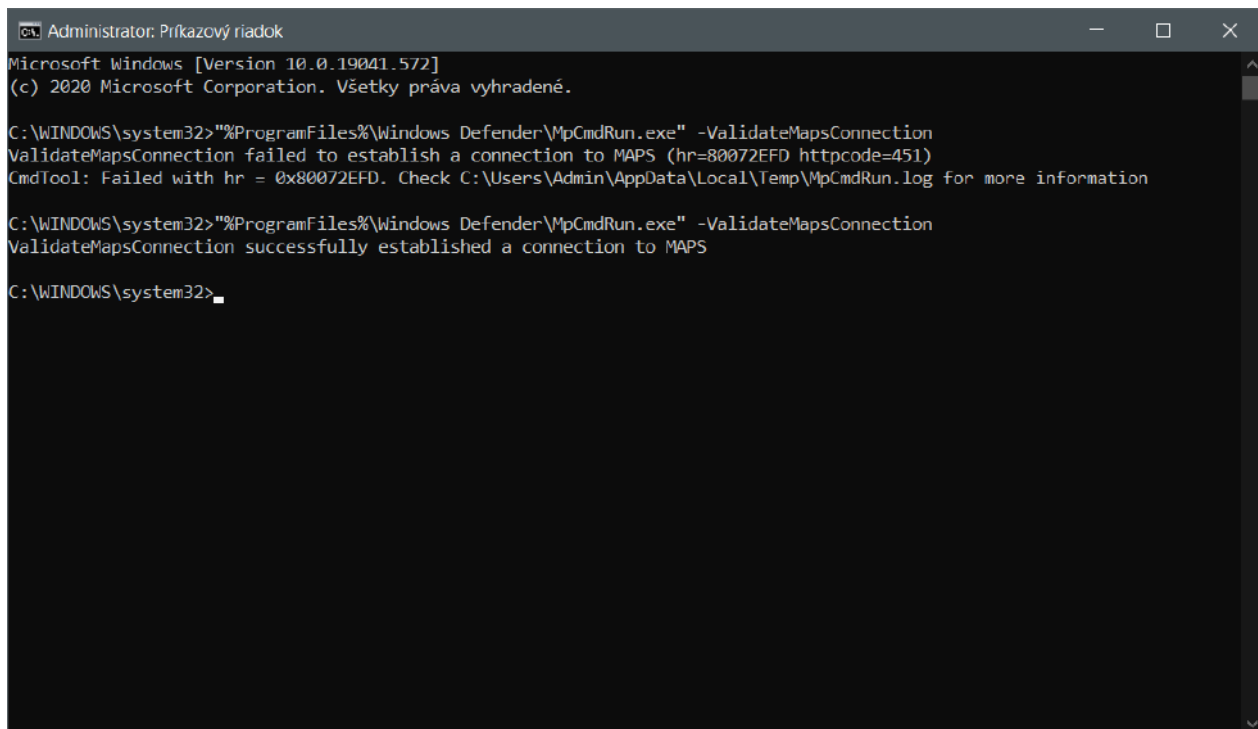
To verify Windows Update, try to check for updates and install new updates on a system with the policies configured.

To verify Microsoft Defender connectivity to the cloud architecture, run the following command in an elevated cmd:

```
"%ProgramFiles%\Windows Defender\MpCmdRun.exe" -ValidateMapsConnection
```

Expected output is:

*ValidateMapsConnection successfully established a connection to MAPS.*



```
Administrator: Příkazový řádek
Microsoft Windows [Version 10.0.19041.572]
(c) 2020 Microsoft Corporation. Všetky práva vyhrazené.

C:\WINDOWS\system32>"%ProgramFiles%\Windows Defender\MpCmdRun.exe" -ValidateMapsConnection
ValidateMapsConnection failed to establish a connection to MAPS (hr=80072EFD httpcode=451)
CmdTool: Failed with hr = 0x80072EFD. Check C:\Users\Admin\AppData\Local\Temp\MpCmdRun.log for more information

C:\WINDOWS\system32>"%ProgramFiles%\Windows Defender\MpCmdRun.exe" -ValidateMapsConnection
ValidateMapsConnection successfully established a connection to MAPS

C:\WINDOWS\system32>
```

*Screenshot 8. Testing Microsoft Defender connectivity with both error and success as outputs.*

# Windows Defender Firewall

Other features, such as SmartScreen, can be verified using the [Microsoft Defender demo scenarios](#).

## Create new rules based on the use case

Based on the use case of the system, individual rules for each Windows service and for each application need to be created.

Keep in mind the order in which firewall rules are evaluated.

1. Allow if secure
2. Block
3. Allow

Assess the default Windows Defender Firewall rules. Some rules, such as exceptions for Wi-Fi Direct or AllJoyn are not needed for most workstations. Any default rules that do not match the use case of the system should be disabled.

3<sup>rd</sup> party software can help simplify the process. For example, Windows Firewall Control by Malwarebytes supports audit mode, which will automatically create rules for any outbound network connection. It also supports one-click rule creation of blocked connections.



# Logging

## Configure Advanced Audit Policy

Advanced Audit Policy provide an in-depth way to manage auditing of Windows. Correct configuration of audit policies is crucial, as simply enabling logging for each group will generate too much noise.

Do not enable both Advanced Audit Policy and audit groups located in *Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy*.

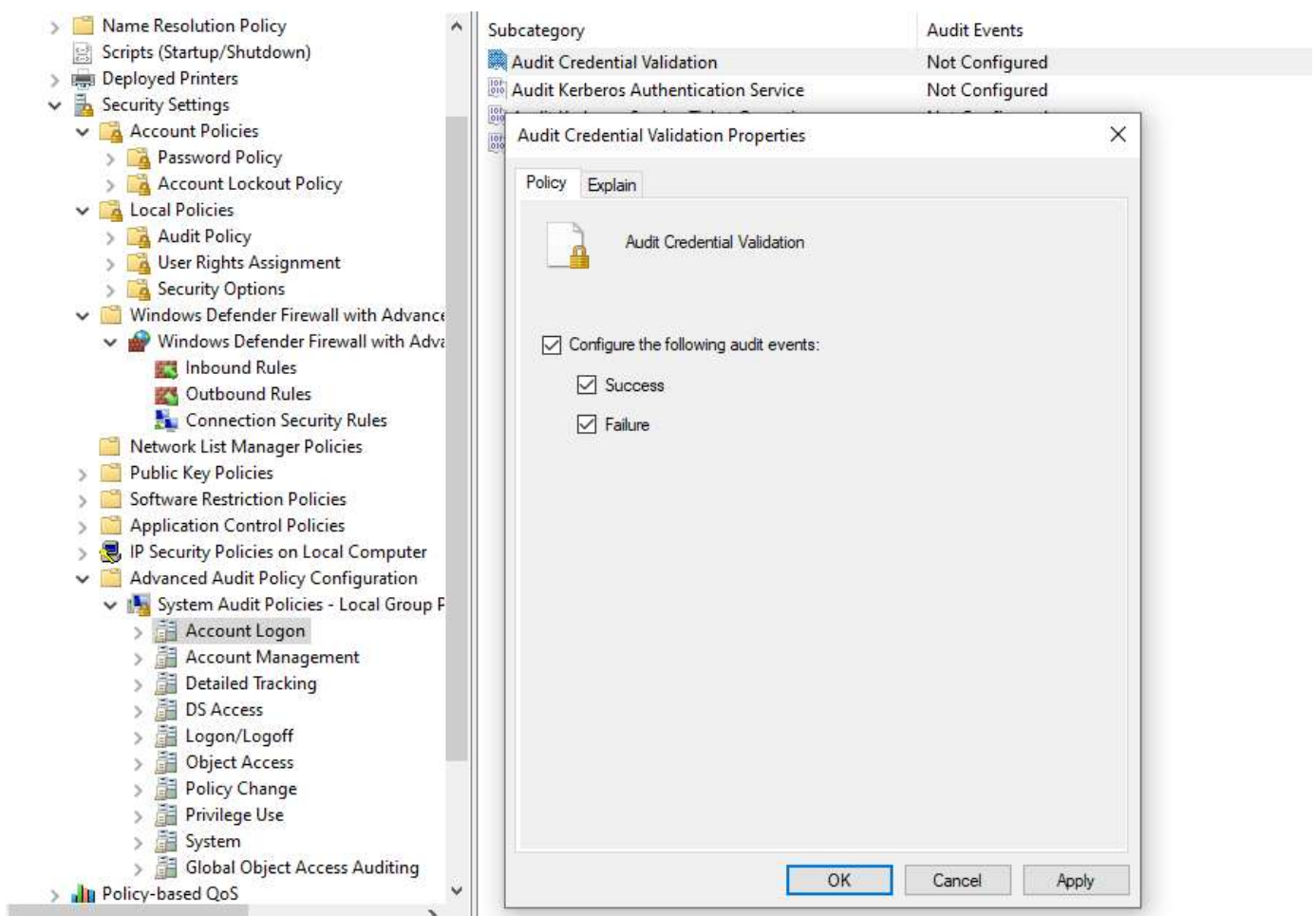
The following policies are recommended:

**Policy path:** *Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies – Local Group Policy Object\Account Logon.*

**Policy name:** *Audit Credential Validation.*

**Recommended settings:** *Enabled.*

Select: *Success* and *Failure*



*Screenshot 9. Enabling auditing of credential events.*

# Logging

**Policy path:** *Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies – Local Group Policy Object\Account Management.*

**Policy name:** *Audit Computer Account Management.*

**Recommended settings:** *Enabled.*

Select: *Success* and *Failure*

**Policy name:** *Audit Other Account Management Events.*

**Recommended settings:** *Enabled.*

Select: *Success* and *Failure*

**Policy name:** *Audit Security Group Management.*

**Recommended settings:** *Enabled.*

Select: *Success* and *Failure*

**Policy name:** *Audit User Account Management.*

**Recommended settings:** *Enabled.*

Select: *Success* and *Failure*

**Policy path:** *Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies – Local Group Policy Object\Detailed Tracking.*

**Policy name:** *Process Creation.*

**Recommended settings:** *Enabled.*

Select: *Success* and *Failure*

**Policy name:** *Audit PNP Activity.*

**Recommended settings:** *Enabled.*

Select: *Success* and *Failure*

**Policy path:** *Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies – Local Group Policy Object\Logon/Logoff.*

**Policy name:** *Audit Account Lockout.*

**Recommended settings:** *Enabled.*

Select: *Success* and *Failure*

**Policy name:** *Audit Logon.*

# Logging

**Recommended settings:** *Enabled*

Select: *Success* and *Failure*

**Policy name:** *Audit Special Logon.*

**Recommended settings:** *Enabled.*

Select: *Success* and *Failure*

**Policy path:** *Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies – Local Group Policy Object\Privilege Use.*

**Policy name:** *Audit Sensitive Privilege Use.*

**Recommended settings:** *Enabled.*

Select: *Success*

**Policy path:** *Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies – Local Group Policy Object\System.*

**Policy name:** *Audit IPsec Driver.*

**Recommended settings:** *Enabled.*

Select: *Success* and *Failure*

**Policy name:** *Audit Security System Extension.*

**Recommended settings:** *Enabled.*

Select: *Success* and *Failure*

**Policy path:** *Computer Configuration\Administrative Templates\System\Audit Process Creation.*

**Policy name:** *Include command line in process creation events.*

**Recommended settings:** *Enabled.*

**Effect on security:** Logons, account actions, process creations, account lockouts, connected devices, use of sensitive permissions and various system events will be logged.

**Effects on usability:** A huge increase in log amount.

**Suitable for:** Everyone.

# Logging

## Enable PowerShell logging

PowerShell features extensive logging capabilities. PowerShell can log executed commands, command invocations and full, de-obfuscated blocks of code. It can also capture all inputs and outputs of the PowerShell console and timestamps for each command.

Since PowerShell is used very often by malware, auditing can help with threat hunting, incident response and forensics.

**MITRE ATT&CK Technique ID:** T1059.001.

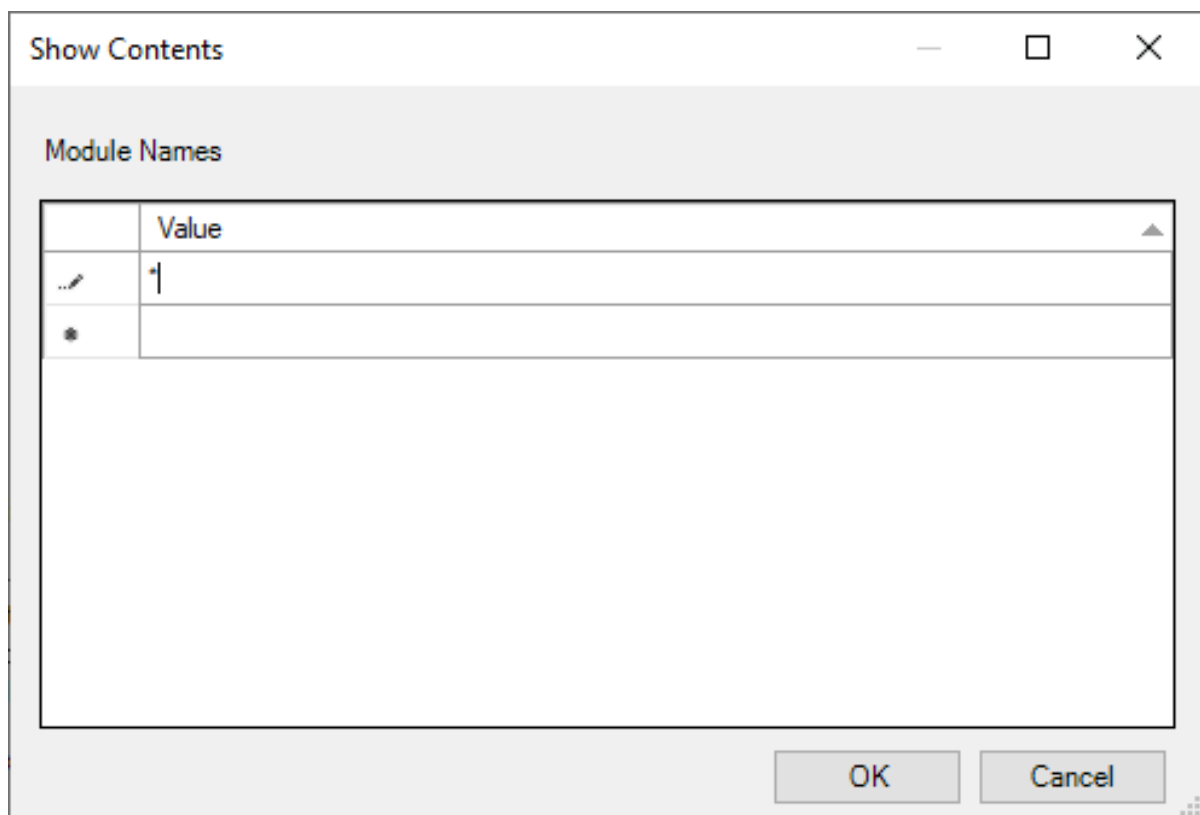
**Policy path:** *Administrative Templates\Windows Components\Windows PowerShell.*

**Policy name:** *Turn on Module Logging.*

**Recommended settings:** *Enabled.*

*Module Names: Add the following module name (to log all modules):*

Value
*



*Screenshot 10. Enabling logging of all modules.*

# Logging

**Policy name:** *Turn on PowerShell Script Block Logging.*

**Recommended settings:** *Enabled.*

Uncheck: *Log script block invocation start | stop events.*

**Policy name:** *Turn on PowerShell Transcription.*

**Recommended settings:** *Enabled.*

Transcript output directory: Choose a write-only, shared network path

Check: *Include invocation headers.*

**Effect on security:** PowerShell commands, input/outputs of the console, and code as PowerShell engine sees it, are logged.

**Effects on usability:** In some cases, huge number of logs are generated.

**Suitable for:** Everyone.

# Application Allowlisting

## Enable AppLocker

Even the most advanced anti-malware solution cannot block all the malware, thus it is best to allow only the necessary applications based on an allowlist. AppLocker, built into all enterprise versions of Windows 10, can block the execution of non-allowlisted apps, packed apps, scripts, and libraries.

To enable AppLocker, the Application Identity service must be enabled. The service is not running by default, so it must be switched to automatic startup. This can be done either via Group Policy, or manually on the host.

## Switching the Application Identity service to automatic startup using group policy

**Policy path:** *Computer Configuration|Windows Settings|Security Settings|System Services.*

**Policy name:** *Application Identity.*

Configure the service to automatic start.

## Switching the Application Identity service to automatic startup locally

Enter in an elevated command prompt:

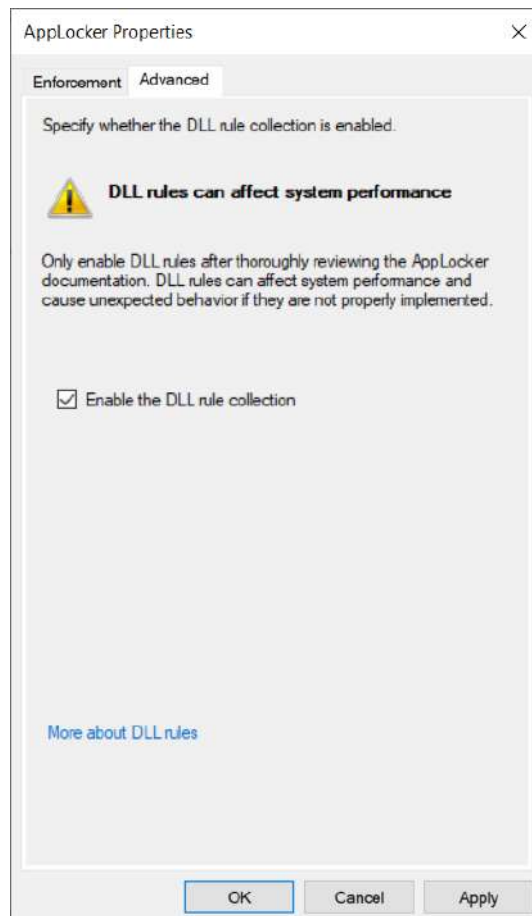
```
sc.exe config appidsvc start= auto
```

## Importing default rules

**Policy path:** *Computer Configuration|Windows Settings|Security Settings|Application Control Policies|AppLocker.*

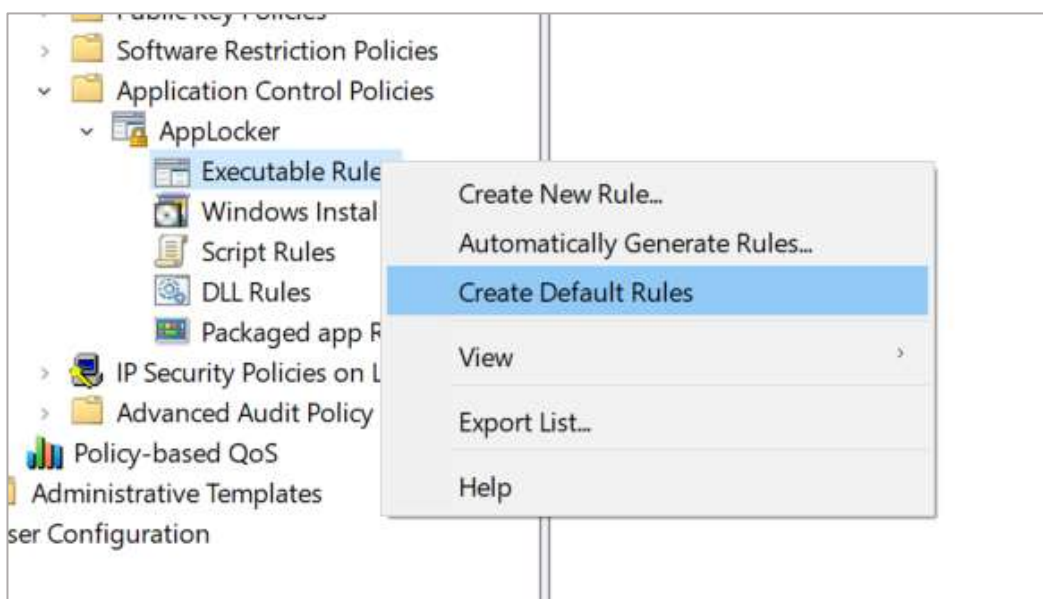
Right-click on *AppLocker*, select *Properties*, select *Advanced*, and check *Enable the DLL rule collection*.

# Application Allowlisting



*Screenshot 11. Enabling DLL rule collection in AppLocker.*

Right-click on *Executable Rules* and select *Create Default Rules*. Repeat the process for *Windows Installer Rules*, *Script Rules*, *DLL Rules*, *Packaged app Rules*.



*Screenshot 12. Creation of default rules.*



# Application Allowlisting

## Hardening AppLocker

Default AppLocker rules can be bypassed easily. Therefore, it is necessary to improve the default rules.

The following rule changes need to be implemented to prevent bypasses:

- Delete the default rule: *(Default Rule) All digitally signed Windows Installer files* rule in *Windows Installer Rules*.
- Delete the default rule: *(Default Rule) All signed packaged apps*.
- Right-click on *Packed app Rules*, select *Automatically Generate Rules...* and generate automatic rules for all packed apps installed in your golden image.

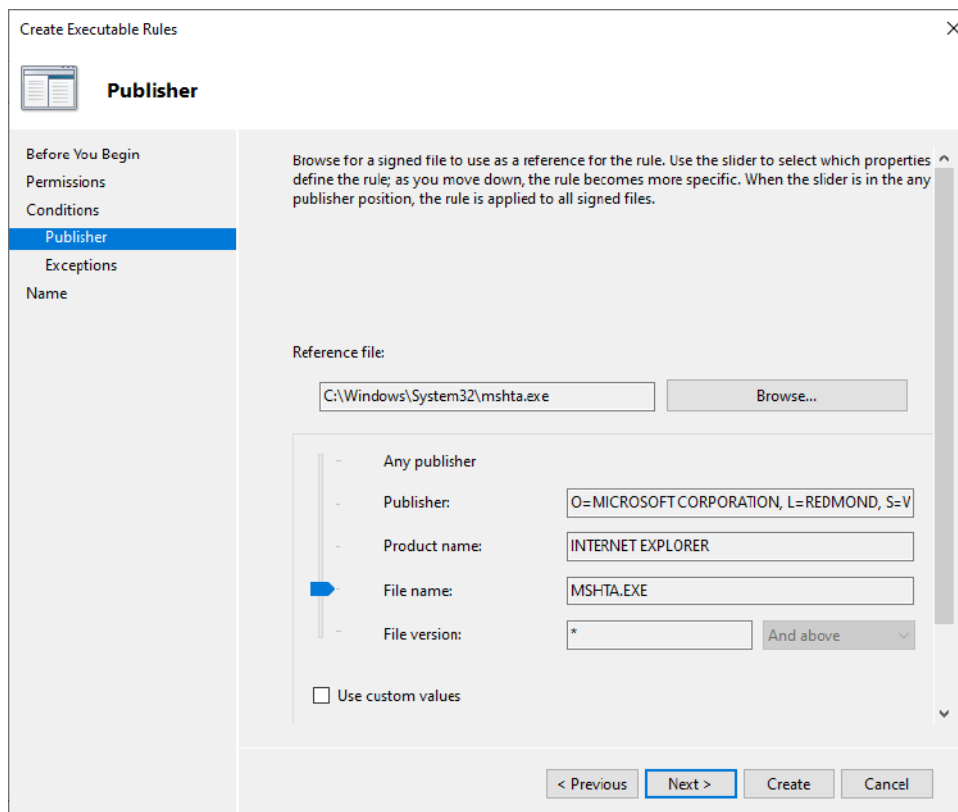
Block the executables and libraries [recommended by Microsoft](#), as they are known to provide AppLocker bypass capabilities:

- *addinprocess.exe*
- *addinprocess32.exe*
- *addinutil.exe*
- *aspnet\_compiler.exe*
- *bash.exe*
- *bginfo.exe*
- *cdb.exe*
- *csi.exe*
- *dbgghost.exe*
- *dbgsvc.exe*
- *dnx.exe*
- *dotnet.exe*
- *fsi.exe*
- *fsiAnyCpu.exe*
- *infdefaultinstall.exe*
- *kd.exe*
- *kill.exe*
- *lxssmanager.dll*
- *lxrun.exe*
- *Microsoft.Build.dll*
- *Microsoft.Build.Framework.dll*
- *Microsoft.Workflow.Compiler.exe*
- *msbuild.exe2*
- *msbuild.dll*
- *mshta.exe*
- *ntkd.exe*
- *ntsd.exe*
- *powershellcustomhost.exe*
- *rcsi.exe*
- *runscripthelper.exe*
- *texttransform.exe*
- *visualuiaverifynative.exe*
- *system.management.automation.dll*
- *wfc.exe*
- *windbg.exe*
- *wmic.exe*
- *wsl.exe*
- *wslconfig.exe*
- *wslhost.exe*

An executable or a library can be blocked by creating a new rule, using *Create New Rule...* option, selecting *Deny* action and specifying an user group, selecting *Publisher* condition, choosing a file and moving slider to the *File name:* option.



# Application Allowlisting



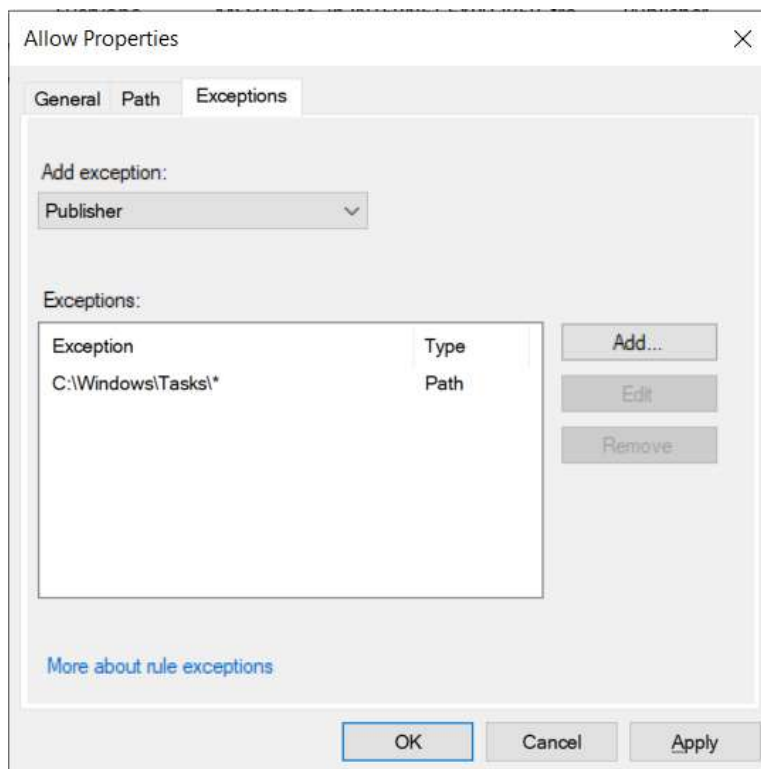
*Screenshot 13. Example of a rule blocking mshta.exe.*

In addition to the blocklist provided by Microsoft, it is recommended to create exceptions to the default rules for the following user-writable paths:

Path
C:\Windows\Tasks\*
C:\Windows\Temp\*
C:\Windows\tracing\*
C:\Windows\System32\Com\dmp\*
C:\Windows\System32\FxsTmp\*
C:\Windows\SysWow64\Com\dmp\*
C:\Windows\SysWow64\FxsTmp\*
C:\Windows\System32\spool\drivers\color\*
C:\Windows\System32\spool\PRINTERS\*
C:\Windows\System32\spool\SERVERS\*
C:\Windows\System32\Microsoft\Crypto\RSA\MachineKeys\*
C:\Windows\System32\tasks_migrated\microsoft\windows\pla\system
C:\Windows\SysWow64\Tasks\microsoft\Windows\pla\system*

An exception to the default executable rule can be created by right clicking at the *All files located in the Windows folder*, selecting *Properties*, selecting *Exceptions*, and adding an exception based on *Path*. Repeat the same process for *Script Rules* and *Windows Installer Rules*.

# Application Allowlisting



*Screenshot 14. Example of an exception to the default rule.*

Some third-party applications tend to create user writable locations in *%ProgramFiles%*. Each installed application needs to be examined whether they do not create a possible bypass.

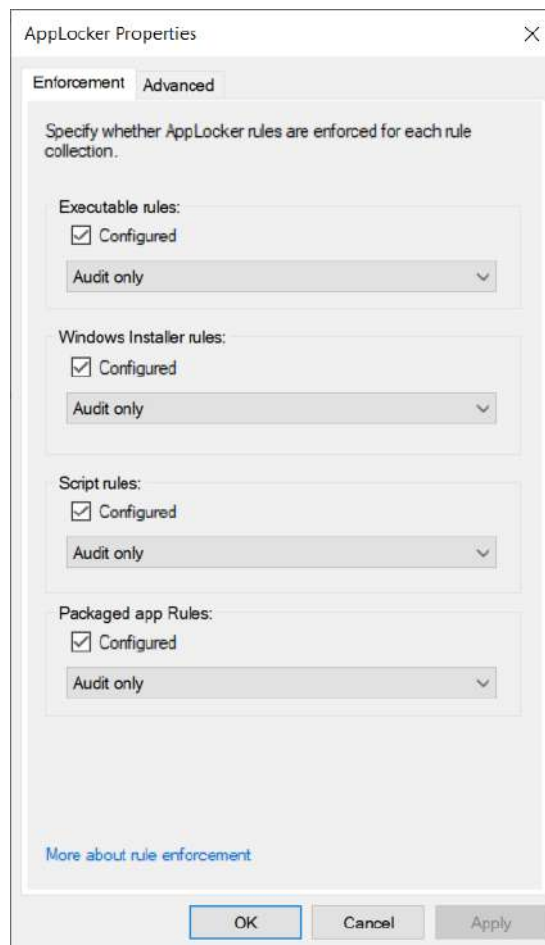
## Enabling AppLocker in audit mode

After rule configuration, it is strongly recommended to enable AppLocker in audit mode to test the policies. Bad policies can cause various issues, ranging from applications not launching to system instability. AppLocker in audit mode will not enforce the rules but will create an event each time a rule is triggered.

To enable AppLocker in audit mode, right-click on AppLocker, select *Properties*, enable *Executable rules*, *Windows Installer rules*, *Script rules*, *Packaged app Rules*, *DLL rules* and select *Audit only* for each.

AppLocker will generate events to the Event Viewer under *Application and Services Logs\Microsoft\Windows\AppLocker*.

# Application Allowlisting



*Screenshot 15. Enabling AppLocker in audit mode.*

## Switching AppLocker to enforcing mode

To enable AppLocker in enforcing mode, right-click on AppLocker, select *Properties*, enable *Executable rules*, *Windows Installer rules*, *Script rules*, *Packaged app Rules*, *DLL rules* and select *Enforce rules* for each. AppLocker will log and block any violations.

Staged rollout is recommended when deploying AppLocker to limit the scope of potential issues.

**MITRE ATT&CK Technique ID:** T1204.001, T1055.001, T1059

**Suitable for:** Office workers

# Protecting Credentials

## Enable Credential Guard

Credential Guard protects secrets by isolating them using Hyper-V. Credential Guard can prevent post-exploitation tools as Mimikatz from obtaining credentials.

There are additional hardware requirements for this feature:

- Intel VT-D\AMD-Vi and SLAT support
- At least Kaby Lake or Zen 2 based CPU for best performance
- TPM 2.0 for best security
- Compatible firmware
- Compatible drivers

To verify the system's drivers, you can use the Device Guard and Credential Guard hardware readiness tool.

Credential Guard with UEFI lock can be disabled by following [the Microsoft guide](#).

**MITRE ATT&CK Technique ID:** T1003.

**Policy path:** *Computer Configuration\Administrative Templates\System\Device Guard.*

**Policy name:** *Turn On Virtualization Based Security.*

**Recommended settings:** *Enabled.*

Select Platform Security Level: "*Secure Boot*" on PCs without DMA Protection, otherwise "*Secure Boot and DMA Protection*".

Credential Guard Configuration: "*Enabled with UEFI Lock*".

**Effect on security:** Lsass will run in a hypervisor, thus preventing dumping of credentials.

**Effects on usability:** Hyper-V will be enabled, which might cause issues with other virtualization software, such as VirtualBox or VMWare. Might cause system instability, 3<sup>rd</sup> party device issues and performance issues. UEFI Lock will prevent the disabling of HVCI without user interaction (remotely).

**Suitable for:** Office Workers.

# Protecting Credentials

## Protect lsass.exe (for system incompatible with Credential Guard)

In some cases, enabling Credential Guard is not an option. Since Credential Guard is using Hyper-V to isolate the credential subsystem. Hardware support is required and might cause issues with other hypervisors.

For such systems, a less effective mitigation is available. The policy will prevent access to lsass.exe from other processes.

**MITRE ATT&CK Technique ID:** T1003.

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction.*

**Policy name:** *Configure Attack Surface Reduction rules.*

**Recommended settings:** *Enabled.*

Show...: Add the following rule ID and its value;

ID	Value
9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2	1

**Effect on security:** Block access to lsass.exe for 3<sup>rd</sup> party processes.

**Effects on usability:** Might produce security errors for processes enumerating lsass.exe, such as Chromium update processes. However, it should not have any other negative effect other than producing log entries.

**Suitable for:** Everyone.

# Protecting Credentials

## Prevent brute force of credentials

Windows can block login after X unsuccessful logins. It can protect logins via UAC, lock screen and RDP. You can specify the lockout duration, with the default being 30 minutes.

**MITRE ATT&CK Technique ID:** T1110.

**Policy path:** *Windows Settings|Security Settings|Account Policies|Account Lockout Policy.*

**Policy name:** *Account lockout threshold.*

**Recommended settings:** 15 (or a custom number).

**Effect on security:** After 15 unsuccessful login attempts, login will be blocked for 30 minutes.

**Effects on usability:** Users might get locked out.

**Suitable for:** Everyone.



The screenshot shows the 'Account Lockout Policy' settings in Windows. It is a table with two columns: 'Policy' and 'Security Setting'. The 'Policy' column lists three settings: 'Account lockout duration', 'Account lockout threshold', and 'Reset account lockout counter after'. The 'Security Setting' column shows the corresponding values: '30 minutes', '15 invalid logon attempts', and '30 minutes'.

Policy	Security Setting
Account lockout duration	30 minutes
Account lockout threshold	15 invalid logon attempts
Reset account lockout counter after	30 minutes

*Screenshot 16. Lockout after 15 unsuccessful login attempts, reset duration left at the default settings.*

## Delete BitLocker encryption keys after X unsuccessful attempts

For computers with sensitive data, deleting encryption keys after X unsuccessful attempts is necessary to protect against credential stuffing / brute force.

**MITRE ATT&CK Technique ID:** T1110.

**Policy path:** *Windows Settings|Security Settings|Local Policies|Security Options.*

**Policy name:** *Interactive logon: Machine account lockout threshold.*

**Recommended settings:** 15.

**Effect on security:** After 15 unsuccessful login attempts, encryption keys will get wiped and only way of recovery will be via the BitLocker recovery.

**Effects on usability:** Users might get locked out.

**Suitable for:** Everyone.

# Improving the Detection & Security of Microsoft Defender

## Enforcing a more aggressive cloud detection

The threshold, at which a file is considered dangerous can be lowered and the time spend analyzing the file in cloud can be increased. While false detection rate will get slightly higher, so will the detection rate.

**MITRE ATT&CK Technique ID:** T1204.002.

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender Antivirus\MpEngine.*

**Policy name:** *Select cloud protection level.*

**Recommended settings:** *Enabled.*

*Select cloud blocking level: High.*

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender Antivirus\MpEngine.*

**Policy name:** *Configure extended cloud check.*

**Recommended settings:** *Enabled.*

*Specify the extended cloud check time in seconds: 20.*

**Effect on security:** Detection of unknown malware samples will improve.

**Effects on usability:** False detection rate will get higher. Launch delay of suspicious software (software without reputation) will increase from ~10 seconds to ~30 seconds.

**Suitable for:** Everyone.

## Block the execution of files deemed unrepeatable by Microsoft Defender

Microsoft Defender calculates reputation based on various factors: signatures, prevalence, cloud analysis... This policy blocks execution of files without a proper reputation. Local files, such as locally compiled executables are usually allowed to run.

**MITRE ATT&CK Technique ID:** T1204.002.

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction.*

**Policy name:** *Configure Attack Surface Reduction rules.*

**Recommended settings:** *Enabled.*



# Improving the Detection & Security of Microsoft Defender

Show...: Add the following rule IDs and their values;

ID	Value
01443614-cd74-433a-b99e-2ecdc07bfc25	1
c1db55ab-c21a-4637-bb3f-a12568109d35	1

**Effect on security:** Block files seemed unreputable by Microsoft Defender.

**Effects on usability:** Often blocks less popular software or new versions of even popular software.

**Suitable for:** Office workers.

## Enable detection of potentially unwanted programs (PUPs)

PUPs not only often serve ads, but also can introduce security vulnerabilities. It is best to block all types of unwanted programs.

Detection of PUPs is disabled by default and can be enabled via a policy.

**MITRE ATT&CK Technique ID:** T1204.002.

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender Antivirus.*

**Policy name:** *Configure detection for potentially unwanted applications.*

**Recommended settings:** *Enabled.*

*Block.*

**Effect on security:** Microsoft Defender will detect and block PUPs.

**Effects on usability:** Some installers containing PUPs might get blocked.

**Suitable for:** Everyone.



# Improving the Detection & Security of Microsoft Defender

## Enforce system-wide SmartScreen filter

SmartScreen filter is a feature which blocks sites with phishing, scams, malware, or exploits. By default, it is enabled for both versions of Microsoft Edge and for Internet Explorer. It is possible to enforce the filter system-wide, including for 3<sup>rd</sup> party browsers and 3<sup>rd</sup> party apps.

**MITRE ATT&CK Technique ID:** T1204.001.

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender Exploit Guard\Network Protection.*

**Policy name:** *Prevent users and apps from accessing dangerous websites.*

**Recommended settings:** Enabled.

*Block.*

**Effect on security:** Sites deemed dangerous will be blocked system-wide.

**Effects on usability:** Unlike SmartScreen in Microsoft Edge or Internet Explorer, there is no bypass option with the system wide SmartScreen. However, the false positive rate is low.

**Suitable for:** Everyone.

## Prevent SmartScreen bypasses

SmartScreen filter can block suspicious files with the option to bypass. This policy disabled the bypass option.

**MITRE ATT&CK Technique ID:** T1204.002.

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender SmartScreen\Explorer.*

**Policy name:** *Configure Windows Defender SmartScreen.*

**Recommended settings:** *Enabled.*

*Pick one of the following settings: Warn and prevent bypass.*

**Effect on security:** SmartScreen filter in Windows Explorer cannot be bypasses.

**Effects on usability:** SmartScreen filter can sometimes block legitimate files and users will be unable to bypass the filter. It is not recommended to enable this setting for computers without a reliable Internet connection, as no connection to SmartScreen server might prevent users from running some apps.

**Suitable for:** Office workers.

# Mitigating Execution and Persistence Techniques

## Blocking persistence through WMI

Abusing WMI event subscriptions is a common persistence technique used by malware.

**MITRE ATT&CK Technique ID:** T1546.003.

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction.*

**Policy name:** *Configure Attack Surface Reduction rules.*

**Recommended settings:** *Enabled.*

Show...: Add the following rule ID and its value;

ID	Value
e6db77e5-3df2-4cf1-b95a-636979351e5b	1

**Effect on security:** Blocks executing code via WMI events.

**Effects on usability:** Some system management software utilizing WMI might be affected.

**Suitable for:** Everyone.

## Blocking code execution through WMI and PSEXEC

WMI and PSEXEC can be abused to run code via remote commands. It is commonly abused by malware and APT groups for lateral movement.

**MITRE ATT&CK Technique ID:** T1569.002.

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction.*

**Policy name:** *Configure Attack Surface Reduction rules.*

**Recommended settings:** *Enabled.*

Show...: Add the following rule ID and its value;

ID	Value
d1e49aac-8f56-4280-b9ba-993a6d77406c	1

**Effect on security:** Blocks process creation via PSEXEC and WMI.

**Effects on usability:** Software utilizing PSEXEC might have compatibility issues.

**Suitable for:** Everyone.

# Mitigating Execution and Persistence Techniques

## Block svchost.exe code injection

Injection into svchost.exe is commonly abused by malware. The policy enables Code Integrity Guard (CIG) and Arbitrary Code Guard (ACG) for svchost.exe.

**MITRE ATT&CK Technique ID:** A subset of T1055.

**Policy path:** *Computer Configuration\Administrative Templates\System\Service Control Manager\Security Settings.*

**Policy name:** *Enable svchost.exe mitigation options.*

**Recommended settings:** *Enabled.*

**Effect on security:** Only Microsoft signed binaries can be loaded into svchost.exe and no new malicious code can be dynamically loaded into svchost.exe memory.

**Effects on usability:** Compatibility issues with various software.

**Suitable for:** Everyone.

## Protecting kernel memory and blocking vulnerable drivers

Kernel-level attacks are one of the more advanced techniques, but they allow for a complete bypass of all security policies. Using Hyper-V and modern hardware, Windows 10 can verify that all kernel code is signed by Microsoft and protect the kernel from dynamic code injection.

In addition to protecting the kernel, Windows 10 can block vulnerable drivers based on a blocklist by Microsoft.

There are additional hardware requirements for this feature:

- Intel VT-D\AMD-Vi and SLAT support
- At least Kaby Lake or Zen 2 based CPU for best performance
- TPM 2.0 for best security
- Compatible firmware
- Compatible drivers

To verify the system's drivers, you can use the Device Guard and Credential Guard hardware readiness tool.

Device Guard with UEFI lock can be disabled by following [the Microsoft guide](#).

**MITRE ATT&CK Technique ID:** T1398.

**Policy path:** *Computer Configuration\Administrative Templates\System\Device Guard.*

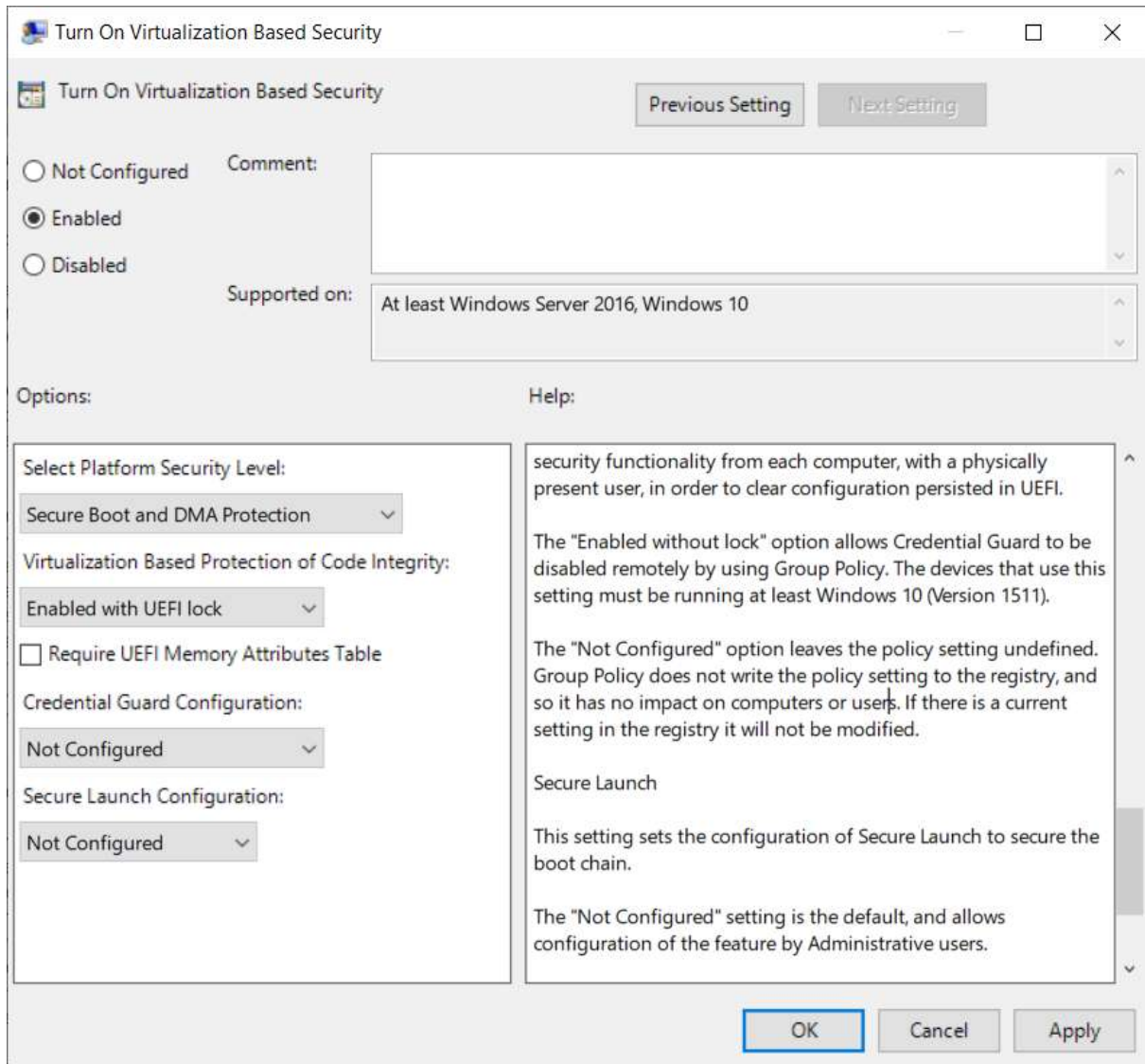
**Policy name:** *Turn On Virtualization Based Security.*

**Recommended settings:** *Enabled.*

# Mitigating Execution and Persistence Techniques

Select Platform Security Level: "*Secure Boot*" on PCs without DMA Protection, otherwise "*Secure Boot and DMA Protection*".

Virtualization Based Protection of Code Integrity: "*Enabled Without UEFI Lock*".



*Screenshot 17. Enabling VBS.*

**Effect on security:** Only Microsoft signed kernel code will run. No dynamically injected kernel code will run. Vulnerable drivers might be blocked.

**Effects on usability:** Hyper-V will be enabled, which might cause issues with other virtualization software, such as VirtualBox or VMWare. Might cause system instability, 3<sup>rd</sup> party device issues and performance issues.

**Suitable for:** Office Workers.

# Mitigating Execution and Persistence Techniques

## Preventing boot of a system with malicious drivers

Early Launch Anti-Malware (ELAM) is a security feature which helps Microsoft Defender (and 3<sup>rd</sup> party security software with ELAM support) to detect and block malware initialized at startup. By default, ELAM is configured to allow known bad drivers, that are required for system startup.

By enabling a Windows policy, we can prevent boot of a system with such malicious drivers.

**MITRE ATT&CK Technique ID:** T1542.

**Policy path:** *Computer Configuration\Administrative Templates\System\Early Launch Antimalware.*

**Policy name:** *Boot-Start Driver Initialization Policy.*

**Recommended settings:** *Enabled.*

*Choose the boot-start drivers that can be initialized: Good and unknown.*

**Effect on security:** Known malicious drivers will not be initialized at startup.

**Effects on usability:** In rare cases, a compromised system might now boot.

**Suitable for:** Everyone.

## Block code injection into sensitive processes

A successor to EMET, Microsoft Defender Exploit Guard, can block code injection into specified processes. This technique is used by malware to steal credentials, or display ads.

It is best practice to block code injection for all processes, that handle sensitive data. Common examples are browsers, password managers and OpenVPN GUI.

This policy can be configured using XML files. The example xml configuration below sets code injection protection for all major browsers and keepass.exe. While the example configuration is suitable for most enterprises, we recommend extending the scope for other sensitive processes used by employees. Make sure the XML file is readable by all hosts and write protected.

# Mitigating Execution and Persistence Techniques

```
<?xml version="1.0" encoding="UTF-8"?>
<MitigationPolicy>
  <AppConfig Executable="chrome.exe">
    <ExtensionPoints DisableExtensionPoints="true"
      OverrideExtensionPoint="false"><\ExtensionPoints>
    <\AppConfig>
  <AppConfig Executable="iexplore.exe">
    <ExtensionPoints DisableExtensionPoints="true"
      OverrideExtensionPoint="false"><\ExtensionPoints>
    <\AppConfig>
  <AppConfig Executable="firefox.exe">
    <ExtensionPoints DisableExtensionPoints="true"
      OverrideExtensionPoint="false"><\ExtensionPoints>
    <\AppConfig>
  <AppConfig Executable="msedge.exe">
    <ExtensionPoints DisableExtensionPoints="true"
      OverrideExtensionPoint="false"><\ExtensionPoints>
    <\AppConfig>
  <AppConfig Executable="keepass.exe">
    <ExtensionPoints DisableExtensionPoints="true"
      OverrideExtensionPoint="false"><\ExtensionPoints>
    <\AppConfig>
<\MitigationPolicy>
```

**MITRE ATT&CK Technique ID:** A subset of T1055.

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender Exploit Guard\Exploit Protection.*

**Policy name:** *Use a common set of exploit protection settings.*

**Recommended settings:** *Enabled.*

Type the location of the mitigation settings configuration XML file:  
Enter the XML file location.

**Effect on security:** Blocks common types of code injection into processes.

**Effects on usability:** Software that utilizes code injection, such as various security solutions, might not be compatible with this policy.

**Suitable for:** Everyone.



# Mitigating Execution and Persistence Techniques

## Remove debug permission from administrators

Debug permission is used by malware to dump credentials and as an anti-debugging measure. By removing the debug permission from administrators, we can deny debugging even from a malware with elevated privileges.

**MITRE ATT&CK Technique ID:** T1003.

**Policy path:** *Windows Settings|Security Settings|Local Policies|User Rights Assignment.*

**Policy name:** *Debug programs.*

**Recommended settings:** *<Blank>* (Remove Administrators from the list).

**Effect on security:** Applications will no longer be able to attach debugger.

**Effects on usability:** Might affect some IDEs.

**Suitable for:** Office Workers.

## Restrict execution capabilities of malware spread via Office documents

Office documents with macros and ActiveX are often used to distribute malware. Windows can block potentially exploitable capabilities, such as Win32 API calls for Office macros or spawning child processes.

**MITRE ATT&CK Technique ID:** T1059.005.

**Policy path:** *Computer Configuration|Administrative Templates|Windows Components|Microsoft Defender Antivirus|Microsoft Defender Exploit Guard|Attack Surface Reduction.*

**Policy name:** *Configure Attack Surface Reduction rules.*

**Recommended settings:** *Enabled.*

Show...: Add the following rule IDs and their value;

ID	Value
D4F940AB-401B-4EFC-AADC-AD5F3C50688A	1
92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B	1
3B576869-A4EC-4529-8536-B80A7769E899	1
75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84	1
26190899-1602-49e8-8b27-eb1d0a1ce869	1

**Effect on security:** Microsoft Word, Excel, PowerPoint, Access, OneNote, and Outlook will not be able to spawn child processes. Microsoft Office apps will not be able to save

# Mitigating Execution and Persistence Techniques

executable files on disk. Microsoft Office apps will not be able to inject code into other processes. Office macros will not be able to call Win32 API.

**Effects on usability:** Office apps will work normally, but some macros, ActiveX and addons might be affected.

**Suitable for:** Everyone.

## Blocking obfuscated scripts

Antimalware Scan Interface (AMSI) allows Windows to block potentially obfuscated scripts, including scripts that download their core functionality from remote hosts.

**MITRE ATT&CK Technique ID:** A subset of T1027.

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction.*

**Policy name:** *Configure Attack Surface Reduction rules.*

**Recommended settings:** *Enabled.*

Show...: Add the following rule ID and its value;

ID	Value
5BEB7EFE-FD9A-4556-801D-275E5FFC04CC	1

**Effect on security:** Obfuscated scripts will be prevented from running.

**Effects on usability:** Although very rare, some legitimate scripts might be considered as obfuscated by Microsoft Defender.

**Suitable for:** Everyone.



# Mitigating Execution and Persistence Techniques

## Allow execution of only signed PowerShell scripts

Restricting the execution of PowerShell scripts to signed only will prevent malware from using PowerShell. Disabling the execution of PowerShell scripts entirely is not recommended, as it will break many applications.

**MITRE ATT&CK Technique ID:** T1059.001.

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\Windows PowerShell.*

**Policy name:** *Turn on script execution.*

**Recommended settings:** *Enabled.*

*Execution policy: Allow only signed scripts.*

**Effect on security:** Only signed PowerShell scripts will be allowed to run.

**Effects on usability:** Since only signed PowerShell will be allowed to run, capabilities to remotely manage and control the system will be reduced.

**Suitable for:** Office workers.

## Block executable files downloaded via JavaScript or VBScript

Scripts often download payload from the Internet. This policy will block launching of executable files downloaded via JavaScript or VBScript

**MITRE ATT&CK Technique ID:** A subset of T1059.

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction.*

**Policy name:** *Configure Attack Surface Reduction rules.*

**Recommended settings:** *Enabled.*

Show...: Add the following rule ID and its value;

ID	Value
D3E037E1-3EB8-44C8-A917-57927947596D	1

**Effect on security:** Executable files downloaded from JavaScript or VBScript files will not launch.

**Effects on usability:** Some enterprise installers rely on this technique.

**Suitable for:** Everyone.

# Mitigating Execution and Persistence Techniques

## Block executable files originating from mail clients or webmail

Malware is often distributed via emails. While most email services block sending and receiving of executable files via e-mail, it is still a good idea to enforce blocking of such files.

**MITRE ATT&CK Technique ID:** T1566.001

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction.*

**Policy name:** *Configure Attack Surface Reduction rules.*

**Recommended settings:** *Enabled.*

Show...: Add the following rule ID and its value;

ID	Value
BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550	1

**Effect on security:** Executable files distributed via e-mail will not launch.

**Effects on usability:** Legitimate software is almost never distributed via e-mail, so usability impact should be very low.

**Suitable for:** Everyone.

# Encryption & Physical Attacks

## Hardening BitLocker against DMA attacks

Interfaces with DMA (direct memory access) allow for an extraction of encryption keys from memory. Windows features an effective mitigation named Kernel DMA Protection. However, the feature requires hardware and firmware support.

Devices supporting Kernel DMA Protection, with Kernel DMA Protection enabled in the system's EFI, require no further actions, and are protected against DMA attacks by default.

The list of business-class devices with Kernel DMA Protection include:

- HP EliteBook series from 2019 or newer
- HP Elite series from 2019 or newer
- HP ZBook series from 2019 or newer
- Lenovo ThinkPad T series from 2019 or newer
- Lenovo ThinkPad X1 series from 2019 or newer
- Dell Latitude series from 2019 or newer
- ...

The status of Kernel DMA Protection can be verified using **System Information** tool (msinfo32.exe), **Category**: System Summary, **Item**: Kernel DMA Protection.

Locale	United States
Hardware Abstraction Layer	Version = "10.0.18362.752"
User Name	Not Available
Time Zone	Pacific Daylight Time
Installed Physical Memory (RAM)	4.83 GB
Total Physical Memory	4.83 GB
Available Physical Memory	1.71 GB
Total Virtual Memory	6.27 GB
Available Virtual Memory	2.34 GB
Page File Space	1.44 GB
Page File	C:\pagefile.sys
Kernel DMA Protection	Off
Virtualization-based security	Running
Virtualization-based security Re...	Base Virtualization Support, Secure Boot, DMA Protection

*Screenshot 18. Kernel DMA Protection status using msinfo32.exe.*

For legacy devices without the support for Kernel DMA Protection, Windows supports a non-hardware-based solution:

**MITRE ATT&CK Technique ID:** A subset of T1200.

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption.*

**Policy name:** *Disable new DMA devices when this computer is locked.*

**Recommended setting:** *Enabled.*

# Encryption & Physical Attacks

**Effect on security:** Prevents adding new DMA devices on lock screen, thus partly preventing DMA side-channel attacks on in-memory encryption keys.

**Effects on usability:** Peripheral devices using Thunderbolt will not work when connected to a locked computer.

**Suitable for:** Everyone.

## Use of 256-bit AES for operating system drives and fixed data drives

BitLocker uses 128-bit AES in XTS block cipher mode by default. Enforcing 256-bit AES-XTS is possible with little-to-no performance impact.

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption.*

**Policy name:** *Choose drive encryption method and cipher strength (Windows 10 [Version 1511] and later).*

**Recommended settings:** *Enabled.*

*Select the encryption method for operating system drives: XTS-AES 256-bit.*

*Select the encryption method for fixed data drives: XTS-AES 256-bit.*

**Effect on security:** Stronger encryption with 256-bit keys.

**Effects on usability:** Little-to-no performance impact.

**Suitable for:** Everyone.

## Use of 256-bit AES in XTS mode for removable data drives

BitLocker uses 128-bit AES in CBC block cipher mode for removable drives by default. Enforcing 256-bit AES-XTS is possible with little-to-no performance impact, however, it will result in compatibility issues with older versions of Windows.

BitLocker in AES-CBC mode has well-known weakness, resulting in some ability to modify plaintext without an encryption key. This can be used to execute code and therefore, bypass encryption.

BitLocker in XTS mode was introduced with Windows 10 version 1511, with the goals of improving security without the negative performance effects of the previous solution, the Elephant Diffuser. Older versions of Windows will not unlock removable drives encrypted with BitLocker in AES-XTS mode.

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption.*

# Encryption & Physical Attacks

**Policy name:** *Choose drive encryption method and cipher strength (Windows 10 [Version 1511] and later).*

**Recommended settings:** *Enabled.*

*Select the encryption method for removable data drives: XTS-AES 256-bit.*

**Effect on security:** Stronger encryption with 256-bit keys & protection against ciphertext modification.

**Effects on usability:** Little-to-no performance impact. Compatibility issues with version of Windows older than 1511.

**Suitable for:** Everyone.

## Enforcing Full encryption type

BitLocker supports two encryption types: Full encryption and Used Space Only encryption. In default configuration, the selection is left to the user. Used Space Only encryption, like the name suggest, is encrypting only used space of a drive. When used on a drive that was previously in-use, it is preferable to overwrite the entire drive when encryption. Otherwise, previously written data might be extracted during forensic analysis.

To prevent user error, it is recommended to enforce Full encryption.

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives.*

**Policy name:** *Enforce drive encryption type on operating system drives.*

**Recommended settings:** *Enabled.*

*Select the encryption type: Full encryption.*

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives.*

**Policy name:** *Enforce drive encryption type on fixed data drives.*

**Recommended settings:** *Enabled.*

*Select the encryption type: Full encryption.*

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives.*

**Policy name:** *Enforce drive encryption type on removable data drives.*

**Recommended settings:** *Enabled.*

*Select the encryption type: Full encryption.*

# Encryption & Physical Attacks

**Effect on security:** Entire drive is overwritten when encrypting to prevent extraction of previously deleted data in plain text.

**Effects on usability:** Longer initial encryption time.

**Suitable for:** Everyone.

## Enable stronger authentication for BitLocker

In its default setting, BitLocker uses only Trusted Platform Module (TPM) for authentication. While it provides reasonable levels of security and requires no user interaction at startup, it is not recommended for high-value computers. Vulnerabilities in TPM or Intel Platform Trust Technology (PTT) might allow for extraction of secrets and subsequent decryption of the entire drive.

It is recommended to enable additional authentication via startup PIN.

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives.*

**Policy name:** *Require additional authentication at startup.*

**Recommended settings:** *Enabled.*

Uncheck: *Allow BitLocker without a compatible TPM.*

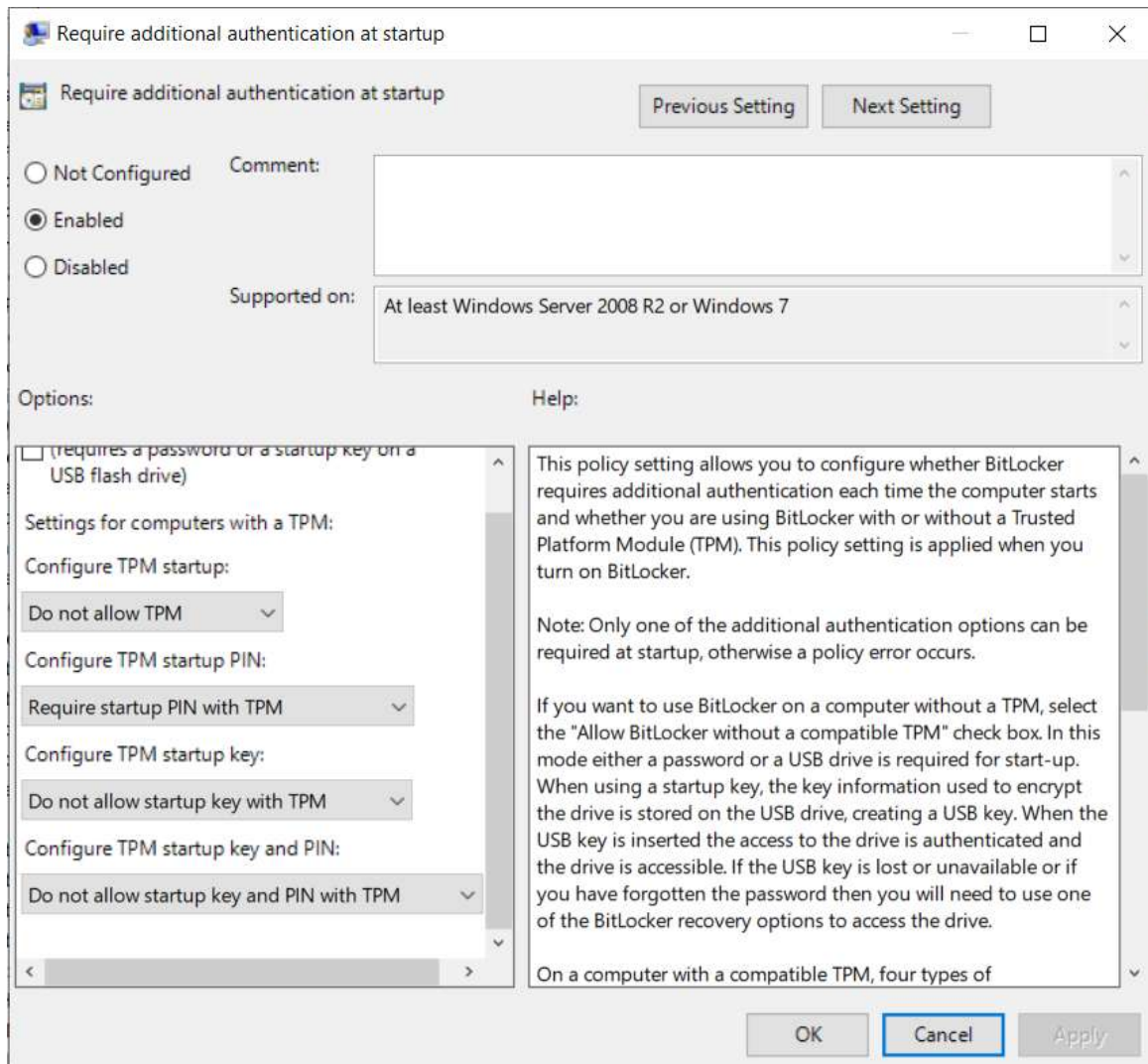
Configure TPM startup PIN: *Require Startup PIN with TPM.*

Configure TPM startup key: *Do not allow startup key with TPM.*

Configure TPM startup key and PIN: *Do not allow startup key and PIN and TPM.*



# Encryption & Physical Attacks



*Screenshot 19. Additional authentication configuration.*

**Effect on security:** Extra protection against vulnerabilities in lock screen, TPM modules or firmware implementations of TPM (Intel PTT or AMD PSP).

**Effects on usability:** Additional password required at boot.

**Suitable for:** Everyone.

# Encryption & Physical Attacks

## Protection against BadUSB attacks

BadUSBs are devices, usually modified flash drives, which are acting as keyboards or network adapters to perform a malicious activity once connected to a computer.

While BadUSB are generally very hard to protect against, as we cannot distinguish a „legitimate“ keyboard from a „bad“ keyboard. However, we can prevent adding new devices once the computer is fully set up.

**MITRE ATT&CK Technique ID:** A subset of T1200.

**Policy path:** *Computer Configuration\Administrative Templates\System\Device Installation\Device Installation Restrictions.*

**Policy name:** *Prevent installation of devices using drivers that match these device setup classes.*

**Recommended settings:** *Enabled.*

Show...: Add the following GUIDs;

GUID	Description
4d36e96b-E325-11CE-BFC1-08402BE10318	USB Keyboards
4D36E972-E325-11CE-BFC1-08012BE10318	Network interface controllers
e0cbf06c-cd8b-4647-bb8a-263b45f0f974	Bluetooth adapters

**Effect on security:** Prevents adding new keyboards and network adapters, which is a technique used in many types of BadUSB attacks.

**Effects on usability:** No new keyboard or network adapter will work when connected.

**Suitable for:** Office Workers.

## Prevent code execution from removable drives

Executing code from removable drives is a common technique by attackers with physical access to the system. With security policies in Windows 10, code execution (.exe, .dll, ...) of untrusted files from removable drives can be blocked.

Trust is determined by Microsoft Defender, and is calculated by various factors: prevalence, digital signature, cloud analysis..

**MITRE ATT&CK Technique ID:** A subset of T1200.

**Policy path:** *Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction.*

**Policy name:** *Configure Attack Surface Reduction rules.*



# Encryption & Physical Attacks

**Recommended settings:** *Enabled.*

Show...: Add the following rule ID and its value;

ID	Value
b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4	1

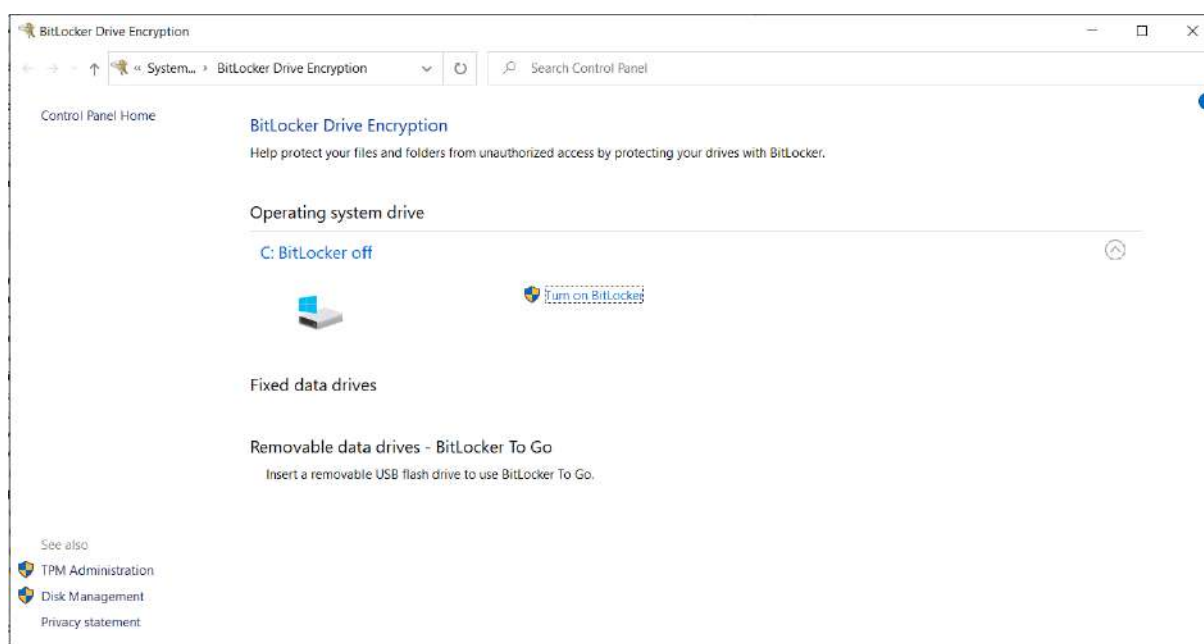
**Effect on security:** Code execution of untrusted files from removable drives will be blocked.

**Effects on usability:** No untrusted programs will launch from removable drives, including some live IR tools.

**Suitable for:** Office Workers.

## Enable BitLocker

After hardening BitLocker, it is ready to be enabled. Make sure that BitLocker is enabled for each drive in the system.



*Screenshot 20. BitLocker menu in the Control Panel.*

# Conclusion

After applying policies and recommendations from this paper, the system will be hardened against most malware and network level attacks. Drives will be encrypted and extensive logging will be configured.