February 6th-7th

NIC

20/20 VISION

Oslo Spektrum

Moving from reactive to proactive security in Azure

@samilaiho

Sami Laiho

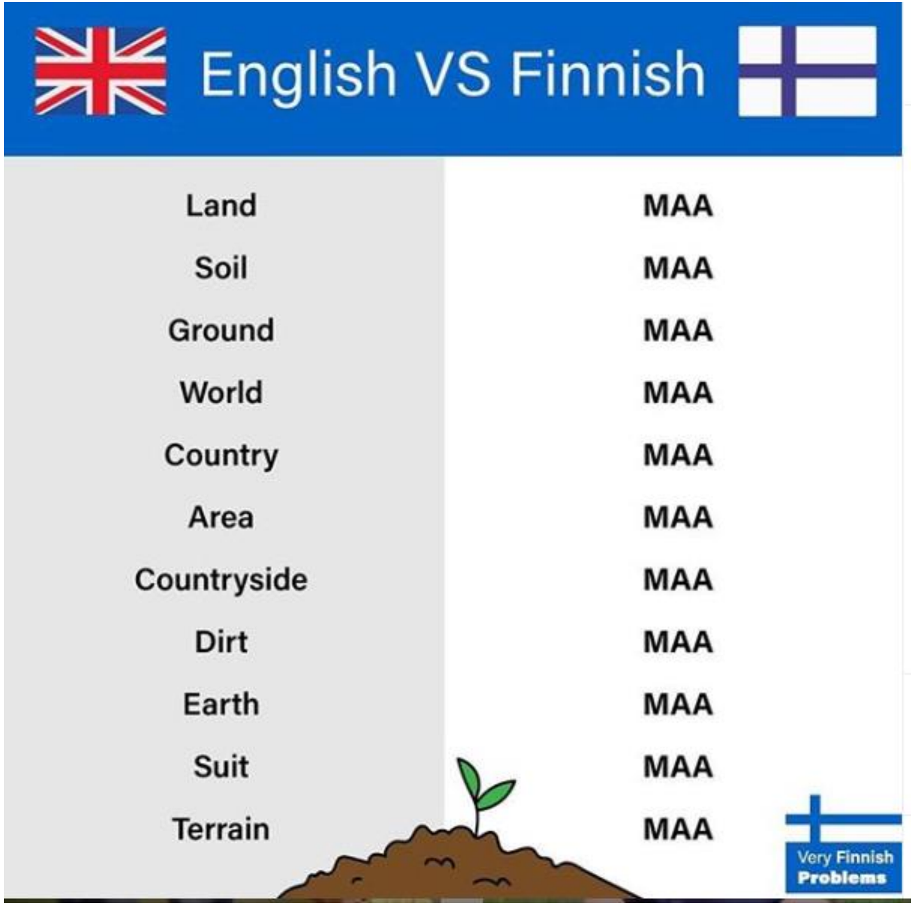
Senior Technical Fellow
adminize.com / Sulava

- IT Admin since 1996, MCT since 2001
- MVP in Windows OS since 2011
- **”100 Most Influencal people in IT in Finland” – TiVi’2019**
- Specializes in and trains:
  - Troubleshooting
  - Windows Internals
  - Security, Social Engineering, Auditing
- Trophies:
  - **Ignite 2018 – Session #1 and #2 (out of 1708) !**
  - Best Speaker at NIC, Oslo 2016, 2017 and 2019
  - Best External Speaker at Ignite 2017
  - TechDays Sweden 2016, 2018 – Best Speaker

Slides and demos from the conference will be available at

https://github.com/nordicinfrastructureconference/2020

My other stuff: https://win-fu.com/share/



English VS Finnish

Land	MAA
Soil	MAA
Ground	MAA
World	MAA
Country	MAA
Area	MAA
Countryside	MAA
Dirt	MAA
Earth	MAA
Suit	MAA
Terrain	MAA

Very Finnish Problems

Finnish facial expressions

EXPLAINED

Happy
Sad
Excited
Irritated
Delighted
In love
Shocked
Depressed
Sorrowful
Romantic
Motivated
Perkele

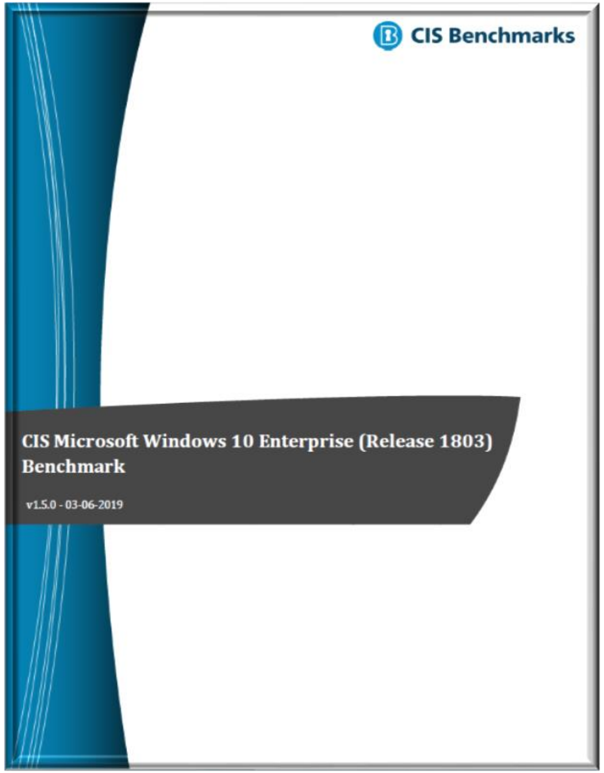
“Make your security better than your neighbours”
- Mikko Hyppönen, F-Secure

Insider threats have increased 47%
https://www.pandasecurity.com/mediacenter/security/cost-insider-threat-report/
Last year, a Canadian bank suffered a data breach that affected some 2.7 million people and around 173,000 companies. The stolen information included names, addresses, dates of birth, social insurance numbers, email addresses and information on customers transaction habits. The culprit of this breach? A malicious insider.

What does the Cloud change?

Implementing baselines

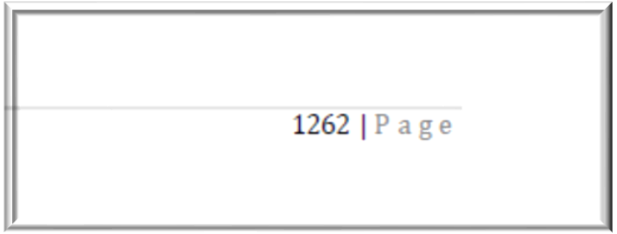
CIS?



CIS Benchmarks

CIS Microsoft Windows 10 Enterprise (Release 1803) Benchmark

v1.5.0 - 03-06-2019

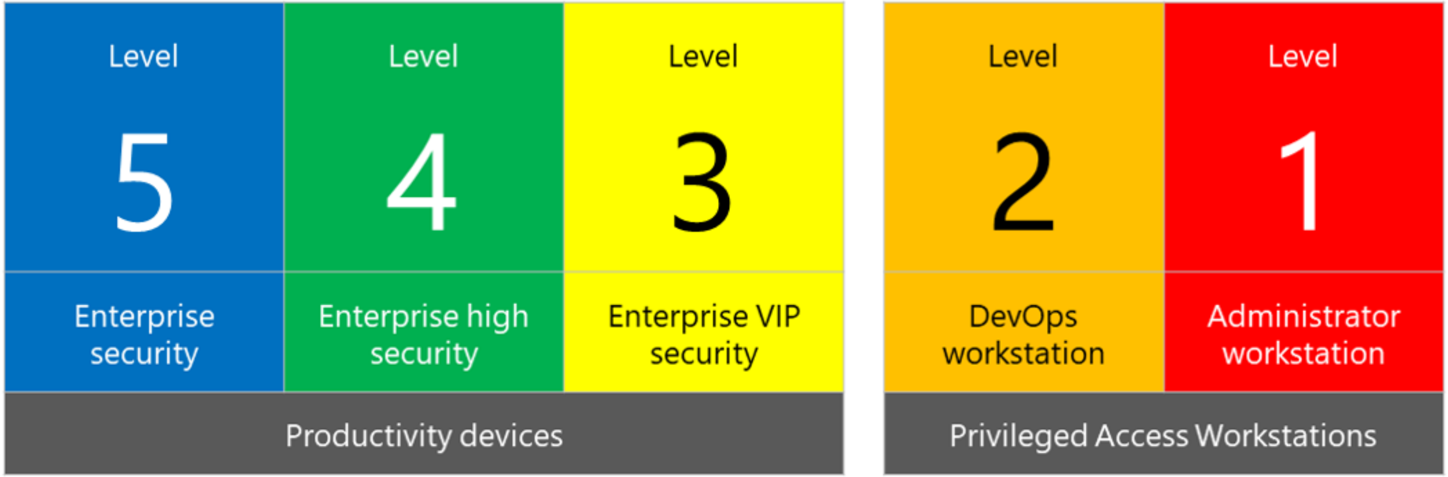


1262 | Page

Getting the baselines for 1809 and 2019

- More traditional way: https://blogs.technet.microsoft.com/secguide/2018/11/20/security-baseline-final-for-windows-10-v1809-and-windows-server-2019/
- For Intune: https://docs.microsoft.com/en-us/intune/security-baselines

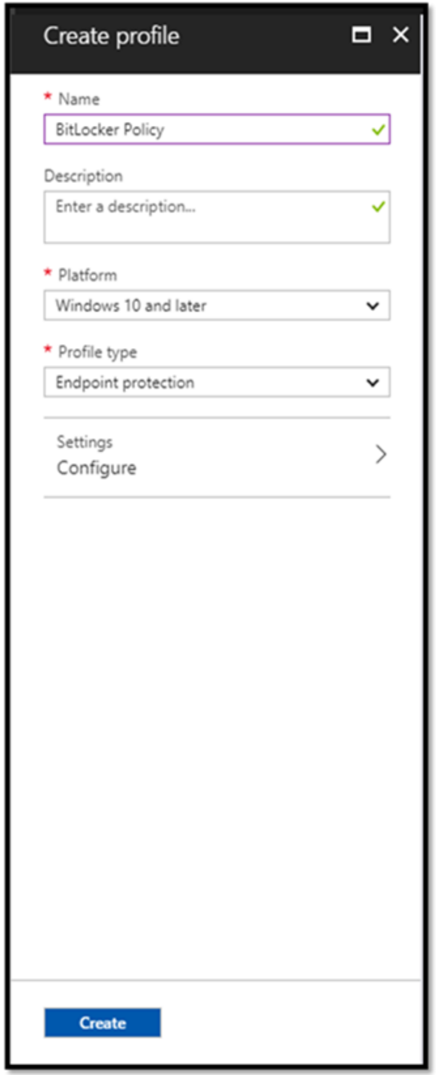
2019→



Level 5	Level 4	Level 3	Level 2	Level 1
Enterprise security	Enterprise high security	Enterprise VIP security	DevOps workstation	Administrator workstation
Productivity devices			Privileged Access Workstations	

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-configuration-framework

Implementing Bitlocker



Create profile

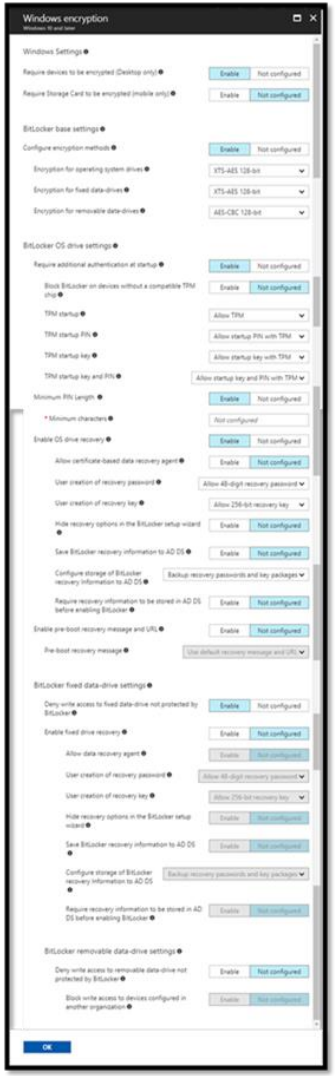
* Name
BitLocker Policy

Description
Enter a description...

* Platform
Windows 10 and later

* Profile type
Endpoint protection

Settings
Configure



Windows encryption

Windows 10 and later

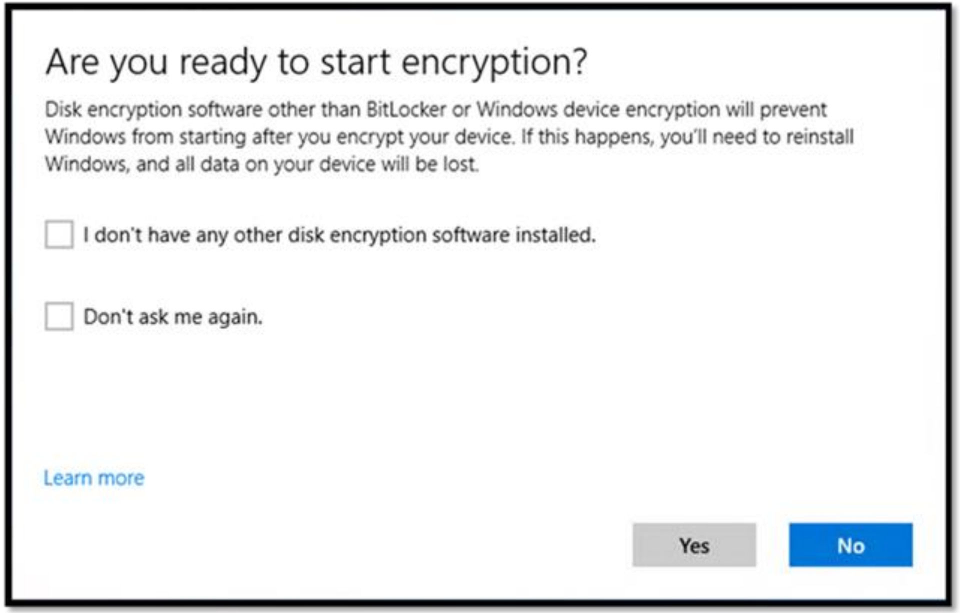
Windows Settings
- Require devices to be encrypted (Desktop only): [✓ Enable] Not configured
- Require Storage Card to be encrypted (mobile only): Enable [✓ Not configured]

BitLocker base settings
- Configure encryption methods: [✓ Enable] Not configured
  - Encryption for operating system drives: XTS-AES 128-bit
  - Encryption for fixed data-drives: XTS-AES 128-bit
  - Encryption for removable data-drives: AES-CBC 128-bit

BitLocker OS drive settings
- Require additional authentication at startup: [✓ Enable] Not configured
  - Block BitLocker on devices without a compatible TPM chip: Enable [✓ Not configured]
  - TPM startup: Allow TPM
  - TPM startup PIN: Allow startup PIN with TPM
  - TPM startup key: Allow startup key with TPM
  - TPM startup key and PIN: Allow startup key and PIN with TPM
- Minimum PIN Length: [✓ Enable] Not configured
  - * Minimum characters: Not configured
- Enable OS drive recovery: [✓ Enable] Not configured
  - Allow certificate-based data recovery agent: Enable [✓ Not configured]
  - User creation of recovery password: Allow 48-digit recovery password
  - User creation of recovery key: Allow 256-bit recovery key
  - Hide recovery options in the BitLocker setup wizard: Enable [✓ Not configured]
  - Save BitLocker recovery information to AD DS: Enable [✓ Not configured]
  - Configure storage of BitLocker recovery information to AD DS: Backup recovery passwords and key packages
  - Require recovery information to be stored in AD DS before enabling BitLocker: Enable [✓ Not configured]
- Enable pre-boot recovery message and URL: Enable [✓ Not configured]
  - Pre-boot recovery message: Use default recovery message and URL

BitLocker fixed data-drive settings
- Deny write access to fixed data-drive not protected by BitLocker: [✓ Enable] Not configured
- Enable fixed drive recovery: Enable [✓ Not configured]
  - Allow data recovery agent: Enable [✓ Not configured]
  - User creation of recovery password: Allow 48-digit recovery password
  - User creation of recovery key: Allow 256-bit recovery key
  - Hide recovery options in the BitLocker setup wizard: Enable [✓ Not configured]
  - Save BitLocker recovery information to AD DS: Enable [✓ Not configured]
  - Configure storage of BitLocker recovery information to AD DS: Backup recovery passwords and key packages
  - Require recovery information to be stored in AD DS before enabling BitLocker: Enable [✓ Not configured]

BitLocker removable data-drive settings
- Deny write access to removable data-drive not protected by BitLocker: Enable [✓ Not configured]
  - Block write access to devices configured in another organization: Enable [✓ Not configured]



Are you ready to start encryption?

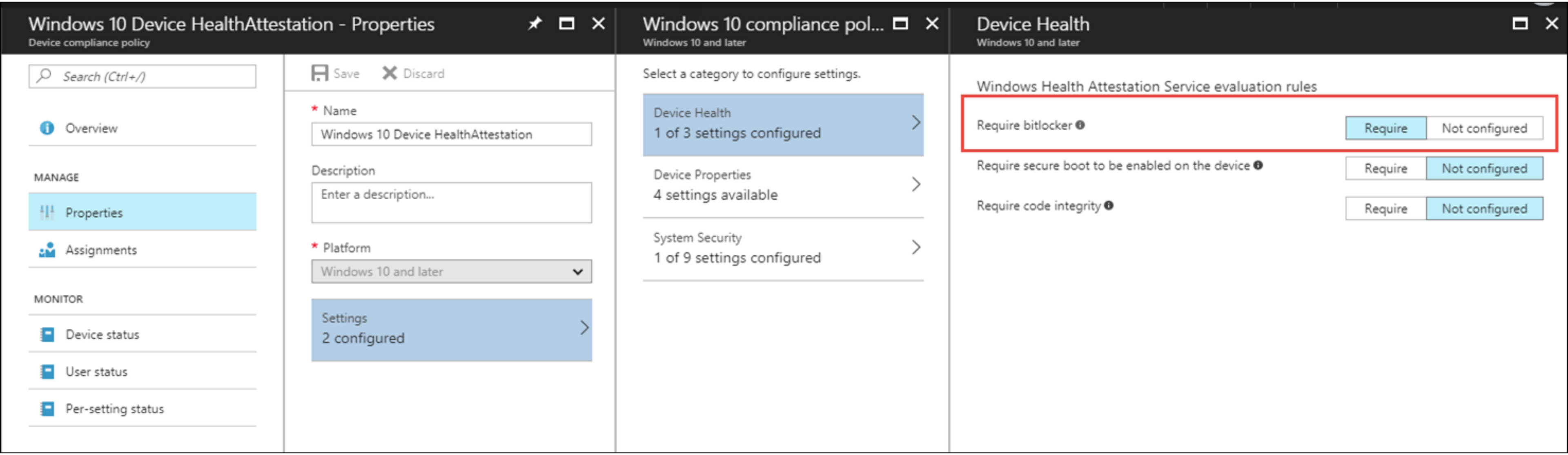
Disk encryption software other than BitLocker or Windows device encryption will prevent Windows from starting after you encrypt your device. If this happens, you'll need to reinstall Windows, and all data on your device will be lost.

☐ I don't have any other disk encryption software installed.

☐ Don't ask me again.

Learn more

nic



Windows 10 Device HealthAttestation - Properties

Device compliance policy

Search (Ctrl+/)

Overview

MANAGE

Properties

Assignments

MONITOR

Device status

User status

Per-setting status

Save ✕ Discard

* Name

Windows 10 Device HealthAttestation

Description

Enter a description...

* Platform

Windows 10 and later

Settings
2 configured

Windows 10 compliance pol...

Windows 10 and later

Select a category to configure settings.

Device Health
1 of 3 settings configured

Device Properties
4 settings available

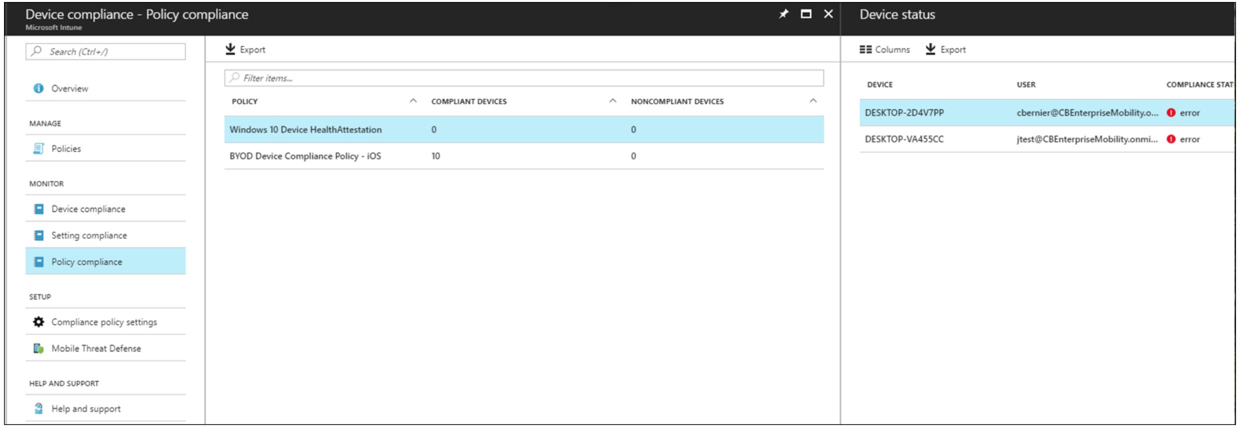
System Security
1 of 9 settings configured

Device Health

Windows 10 and later

Windows Health Attestation Service evaluation rules

Require bitlocker	[✓ Require] Not configured
Require secure boot to be enabled on the device	Require [✓ Not configured]
Require code integrity	Require [✓ Not configured]



Device compliance - Policy compliance

Microsoft Intune

Search (Ctrl+/)

Overview

MANAGE

Policies

MONITOR

Device compliance

Setting compliance

Policy compliance

SETUP

Compliance policy settings

Mobile Threat Defense

HELP AND SUPPORT

Help and support

Export

Filter items...

POLICY	COMPLIANT DEVICES	NONCOMPLIANT DEVICES
Windows 10 Device HealthAttestation	0	0
BYOD Device Compliance Policy - iOS	10	0

Device status

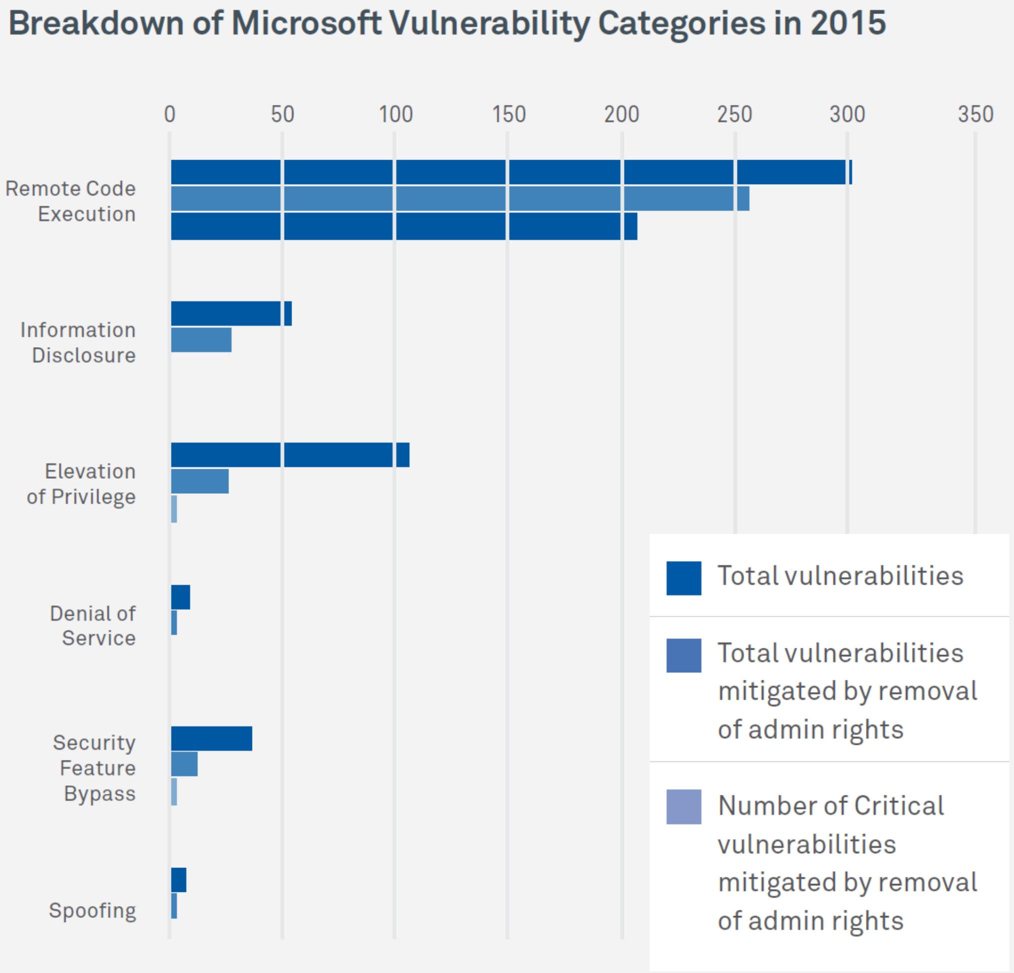
Columns Export

DEVICE	USER	COMPLIANCE STAT
DESKTOP-2D4V7PP	cbernier@CBEnterpriseMobility.o...	error
DESKTOP-VA455CC	jtest@CBEnterpriseMobility.onmi...	error

Implementing least privilege

2015

- Analysis of Microsoft "Patch Tuesday" Security Bulletins from 2015
  - 85% of Critical Microsoft vulnerabilities would be mitigated by removing admin rights
- Windows Server vulnerabilities
  - 85% were found to be mitigated by the removal of admin rights



2016 Microsoft Vulnerabilities Study

Key findings

- Of the 189 vulnerabilities in 2016 with a Critical rating, 94% were concluded to be mitigated by removing administrator rights
- 66% of all Microsoft vulnerabilities reported in 2016 could be mitigated by removing admin rights
- 100% of vulnerabilities impacting Microsoft's latest browser Edge could be mitigated
- 100% of vulnerabilities in Internet Explorer and Chrome could be mitigated by removing admin rights
- 99% of vulnerabilities affecting Microsoft Office could be mitigated by removing admin rights
- 93% Critical vulnerabilities affecting Windows 10 could be mitigated by removing admin rights

Microsoft Vulnerabilities Report 2017

The 2017 report highlights the following key findings:

- Removing admin rights would mitigate 80% of all Critical Microsoft vulnerabilities in 2017.
- 95% of Critical vulnerabilities in Microsoft browsers can be mitigated by removing administrator rights.
- Almost two thirds of all Critical vulnerabilities in Microsoft Office products are mitigated by removing admin rights.
- **88% of all Critical vulnerabilities reported by Microsoft over the last five years would have been mitigated by removing admin rights.**

S*it ‘o’ meter

- DEMO

“75% reduction in tickets after implementing Least Privilege”

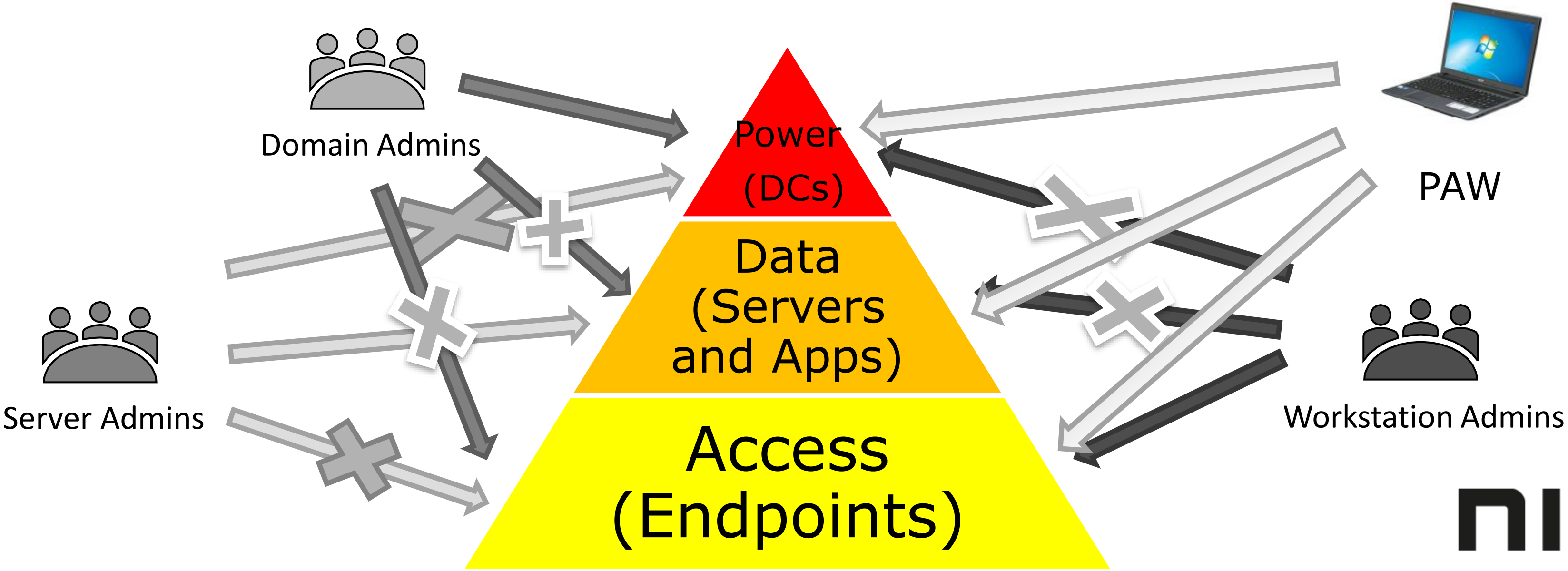
Same as for on-prem

- Centero Carillon
- PolicyPak
- BeyondTrust

Implementing the Tier Model

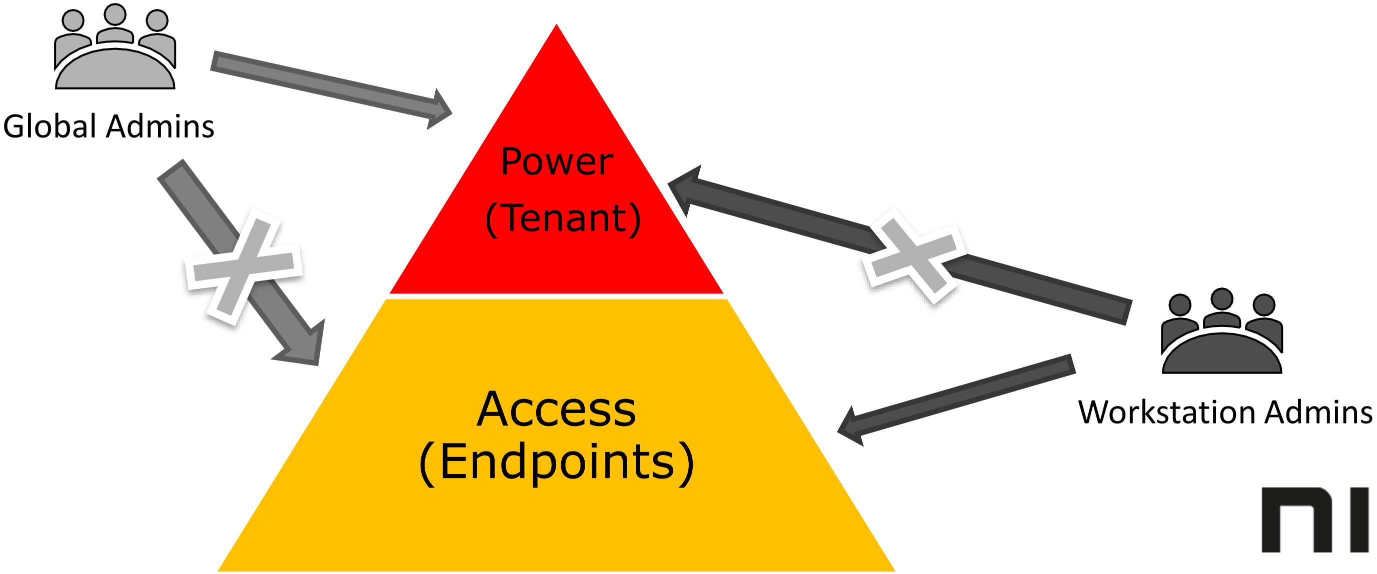
Mitigating PtH (IAAS)

- Split your environment into three layers (Azure minimum 2 layers)
- Never allow higher layer admins to logon to lower layers



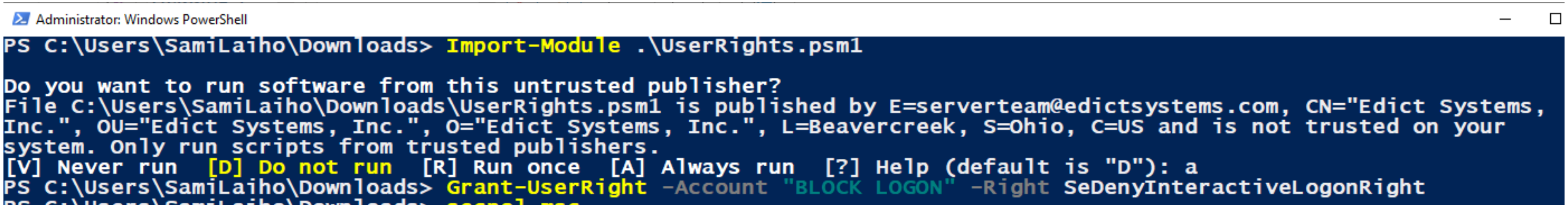
Mitigating PtH (Native Cloud)

- Split your environment into two layers
- Never allow higher layer admins to logon to lower layers



Implementing

- Create a local group
  - New-LocalGroup -Name "BLOCK LOGON“
- Block logon from them

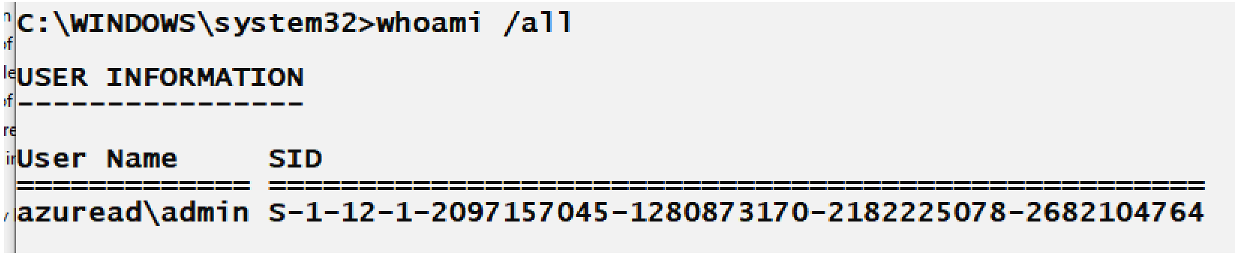


```
PS C:\Users\SamiLaiho\Downloads> Import-Module .\UserRights.psm1

Do you want to run software from this untrusted publisher?
File C:\Users\SamiLaiho\Downloads\UserRights.psm1 is published by E=serverteam@edictsystems.com, CN="Edict Systems,
Inc.", OU="Edict Systems, Inc.", O="Edict Systems, Inc.", L=Beavercreek, S=Ohio, C=US and is not trusted on your
system. Only run scripts from trusted publishers.
[V] Never run  [D] Do not run  [R] Run once  [A] Always run  [?] Help (default is "D"): a
PS C:\Users\SamiLaiho\Downloads> Grant-UserRight -Account "BLOCK LOGON" -Right SeDenyInteractiveLogonRight
PS C:\Users\SamiLaiho\Downloads> secpol.msc
```

- https://gallery.technet.microsoft.com/scriptcenter/Grant-Revoke-Query-user-26e259b0
- Add the Global Admins to this group

Global Admins

- There should only be a very limited amount of them anyway
- Figure out their SIDs from the local machine and add to the group with PowerShell

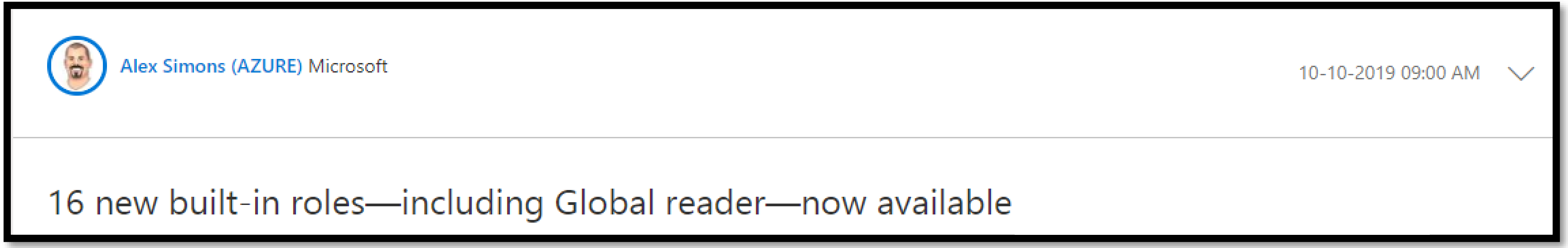


```
C:\WINDOWS\system32>whoami /all

USER INFORMATION
----------------

User Name      SID
============== ==============================================
azuread\admin  S-1-12-1-2097157045-1280873170-2182225078-2682104764
```

- Add-LocalGroupMember -Group "BLOCK LOGON" -Member S-1-12-1-2097157045-1280873170-2182225078-2682104764

Global Reader

- https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/16-new-built-in-roles-including-Global-reader-now-available-in/ba-p/900749



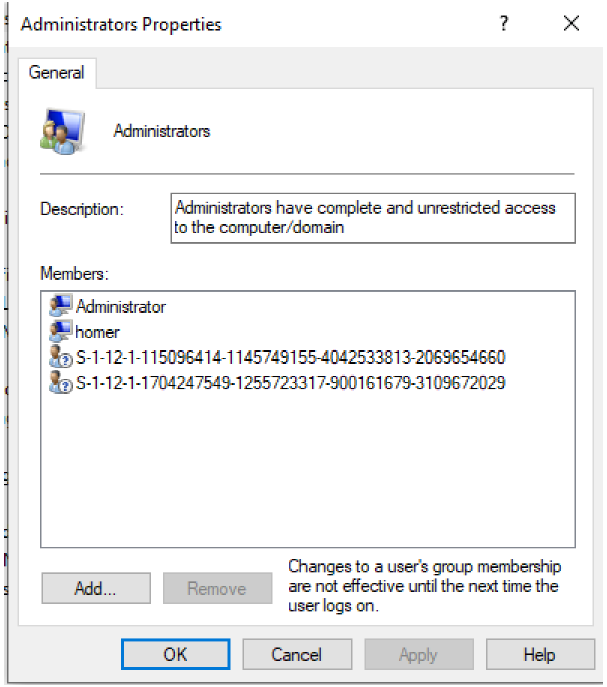
Alex Simons (AZURE) Microsoft

10-10-2019 09:00 AM

16 new built-in roles—including Global reader—now available

Don’t remove these

Applies to all “Azure admins” including “Device Administrators”



Administrators Properties

General

Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

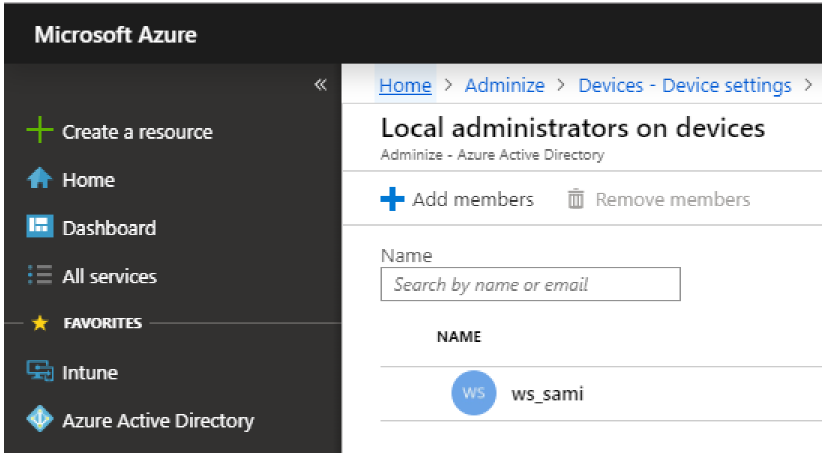
Members:

- Administrator
- homer
- S-1-12-1-115096414-1145749155-4042533813-2069654660
- S-1-12-1-1704247549-1255723317-900161679-3109672029

Changes to a user's group membership are not effective until the next time the user logs on.

Add Device Admins

- Hopefully soon via a group



Local administrators on devices

Adminize - Azure Active Directory

Name

Search by name or email

ws_sami

Implementing PAWs

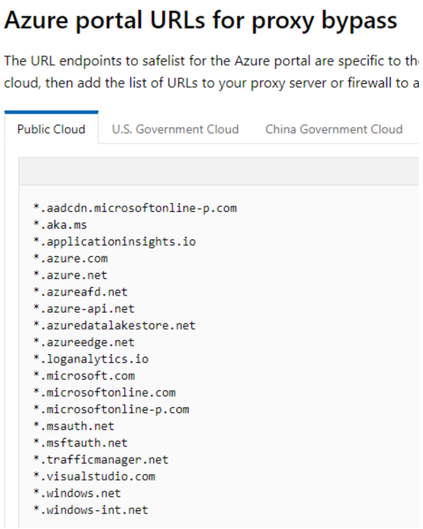
Concept of PAW

- You should do management from a PAW
- You can enforce by Firewall-rules, Proxies etc.

PAW

Safe addresses

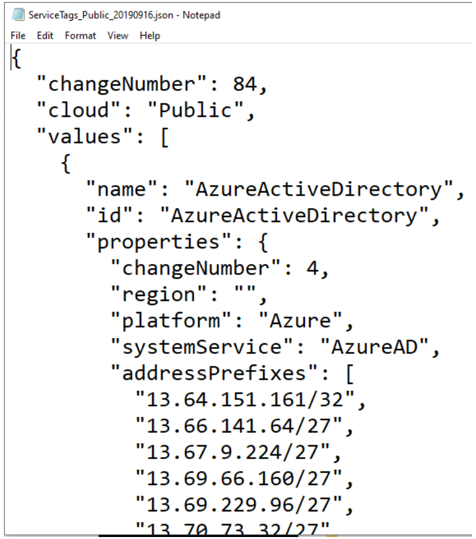
- https://docs.microsoft.com/en-us/azure/azure-portal/azure-portal-safelist-urls?tabs=public-cloud



Azure portal URLs for proxy bypass

The URL endpoints to safelist for the Azure portal are specific to th
cloud, then add the list of URLs to your proxy server or firewall to a

```
*.aadcdn.microsoftonline-p.com
*.aka.ms
*.applicationinsights.io
*.azure.com
*.azure.net
*.azureafd.net
*.azure-api.net
*.azuredatalakestore.net
*.azureedge.net
*.loganalytics.io
*.microsoft.com
*.microsoftonline.com
*.microsoftonline-p.com
*.msauth.net
*.msftauth.net
*.trafficmanager.net
*.visualstudio.com
*.windows.net
*.windows-int.net
```



ServiceTags_Public_20190916.json - Notepad
File Edit Format View Help

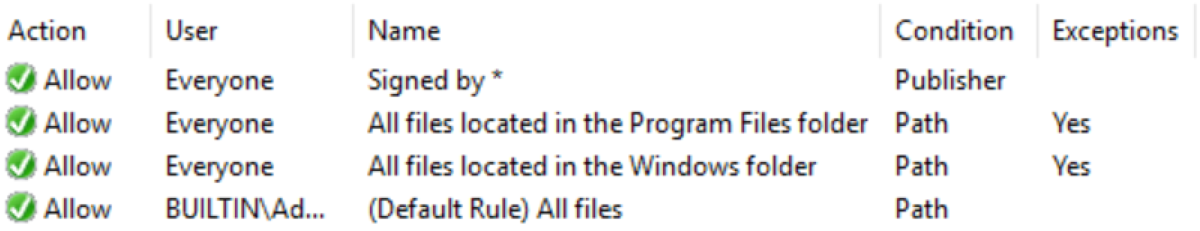
```
{
  "changeNumber": 84,
  "cloud": "Public",
  "values": [
    {
      "name": "AzureActiveDirectory",
      "id": "AzureActiveDirectory",
      "properties": {
        "changeNumber": 4,
        "region": "",
        "platform": "Azure",
        "systemService": "AzureAD",
        "addressPrefixes": [
          "13.64.151.161/32",
          "13.66.141.64/27",
          "13.67.9.224/27",
          "13.69.66.160/27",
          "13.69.229.96/27",
          "13.70.73.32/27"
```

Implementing Whitelisting

AppLocker HOW TO

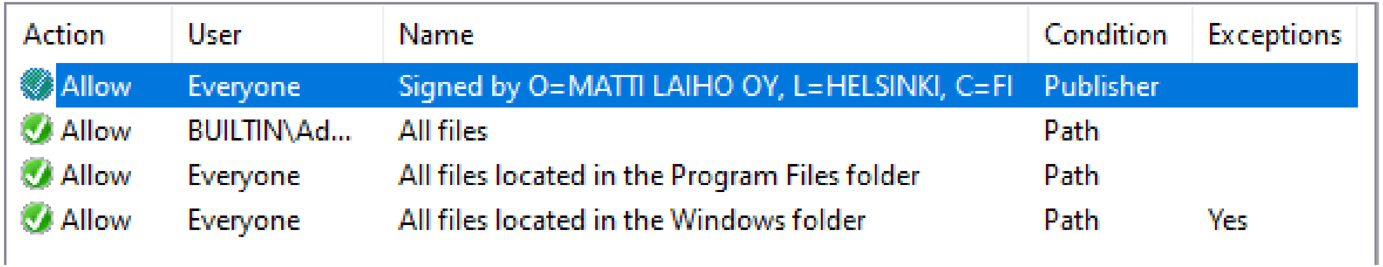
- Keep to containers not items – Folders vs Files, Publishers vs Hashes
- Remember to audit your installation with AccessChk!
- Remember NO ADMIN RIGHTS!!

Simplest AppLocker



Action	User	Name	Condition	Exceptions
✓ Allow	Everyone	Signed by *	Publisher	
✓ Allow	Everyone	All files located in the Program Files folder	Path	Yes
✓ Allow	Everyone	All files located in the Windows folder	Path	Yes
✓ Allow	BUILTIN\Ad...	(Default Rule) All files	Path	

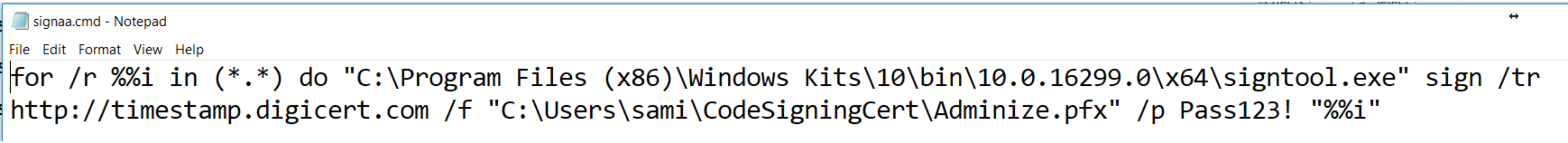
Simplest AppLocker for many



Action	User	Name	Condition	Exceptions
✓ Allow	Everyone	Signed by O=MATTI LAIHO OY, L=HELSINKI, C=FI	Publisher	
✓ Allow	BUILTIN\Ad...	All files	Path	
✓ Allow	Everyone	All files located in the Program Files folder	Path	
✓ Allow	Everyone	All files located in the Windows folder	Path	Yes

Signing

- 95% of Malware is not signed – just something to think about
- You can sign apps yourself
    - Use Timestamp if possible!
- If you have the cert on your computer installed:
    - **Signtool sign /v /s MY /n MyPrivateCert /t** http://timestamp.verisign.com/scripts/timstamp.dll **FileToSign.exe**
- If not:



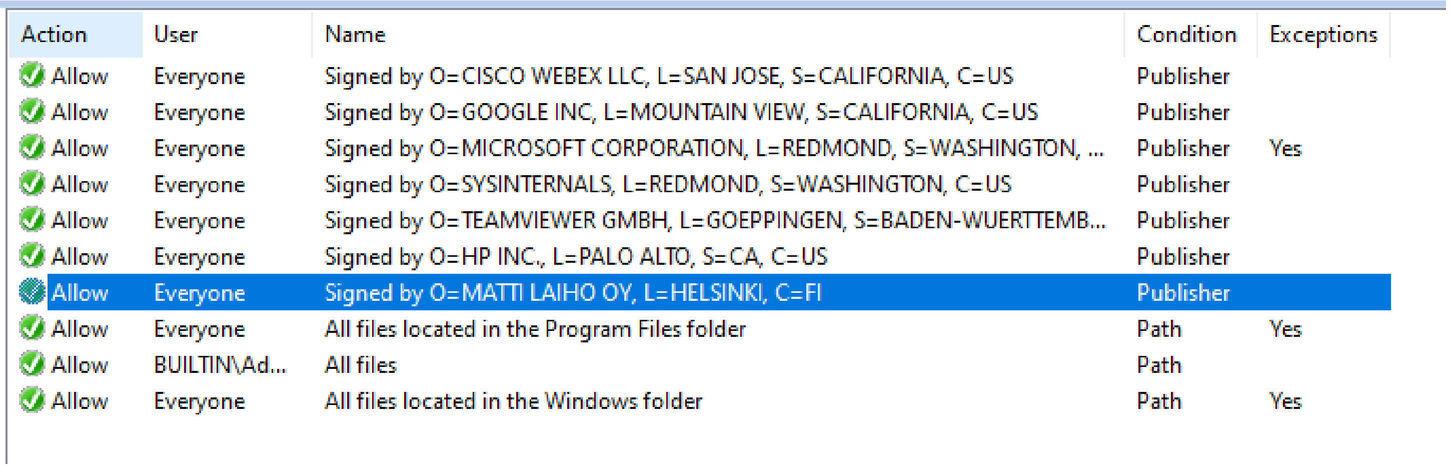
```
for /r %%i in (*.*) do "C:\Program Files (x86)\Windows Kits\10\bin\10.0.16299.0\x64\signtool.exe" sign /tr
http://timestamp.digicert.com /f "C:\Users\sami\CodeSigningCert\Adminize.pfx" /p Pass123! "%%i"
```

- Guide: https://blogs.msdn.microsoft.com/winsdk/2009/11/13/steps-to-sign-a-file-using-signtool-exe/

AppLocker Example Policies

AppLocker example

- My current baseline
  - Replace Matti Laiho with you companies own cert
  - Replace HP with your UEFI provider
  - Add Block-rules for known weaknesses: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules



Action	User	Name	Condition	Exceptions
✓ Allow	Everyone	Signed by O=CISCO WEBEX LLC, L=SAN JOSE, S=CALIFORNIA, C=US	Publisher	
✓ Allow	Everyone	Signed by O=GOOGLE INC, L=MOUNTAIN VIEW, S=CALIFORNIA, C=US	Publisher	
✓ Allow	Everyone	Signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, ...	Publisher	Yes
✓ Allow	Everyone	Signed by O=SYSINTERNALS, L=REDMOND, S=WASHINGTON, C=US	Publisher	
✓ Allow	Everyone	Signed by O=TEAMVIEWER GMBH, L=GOEPPINGEN, S=BADEN-WUERTTEMB...	Publisher	
✓ Allow	Everyone	Signed by O=HP INC., L=PALO ALTO, S=CA, C=US	Publisher	
✓ Allow	Everyone	Signed by O=MATTI LAIHO OY, L=HELSINKI, C=FI	Publisher	
✓ Allow	Everyone	All files located in the Program Files folder	Path	Yes
✓ Allow	BUILTIN\Ad...	All files	Path	
✓ Allow	Everyone	All files located in the Windows folder	Path	Yes

My customer devices

- Basic rules + AccessChk revealed exceptions
- Use certificates if you can (and trust the company)
- **Then add required network locations with**
  - UNC
  - IP
  - FQDN
  - Sometimes also with the drive letter: P:, \\SVR\Share, \\SVR.dom.com\share, and \\192.1.1.2\Share
- Then add local applications outside of the default folders with Certs, Folders (if they can be blocked from writing to by limited users)
- Problematic ones
  - Self-updating, not signed and stored in users profile
  - TIP! File/Folder rules allow * at any point!
    - Use with caution – but usually need some! Try to use HASH rather if possible!

Tip for Companies (why not consumers)

- Block PowerShell from limited users – not a single ransomware would have worked so far ☺

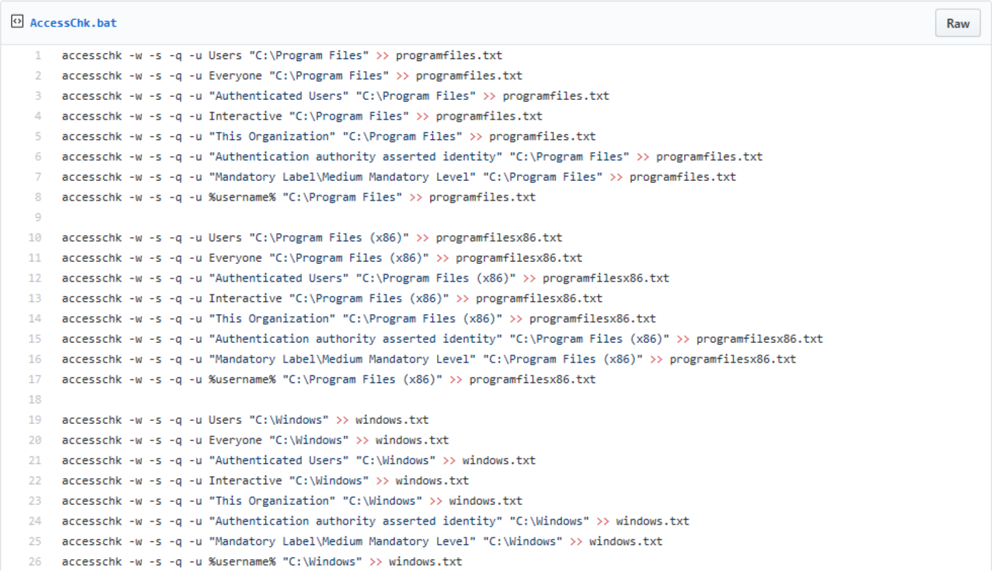
Hardening Applocker

Twitter

- @Oddvarmoe
- @subTee
- @mattifestation
- @enigma0x3
- @aionescu
- @tifkin_
- @bohops
- @PhilipTsukerman
- @samilaiho ;)

Hardening Whitelisting

Make sure your containers don’t leak (this is one batch file) – CHECK THE LATEST FROM GITHUB!

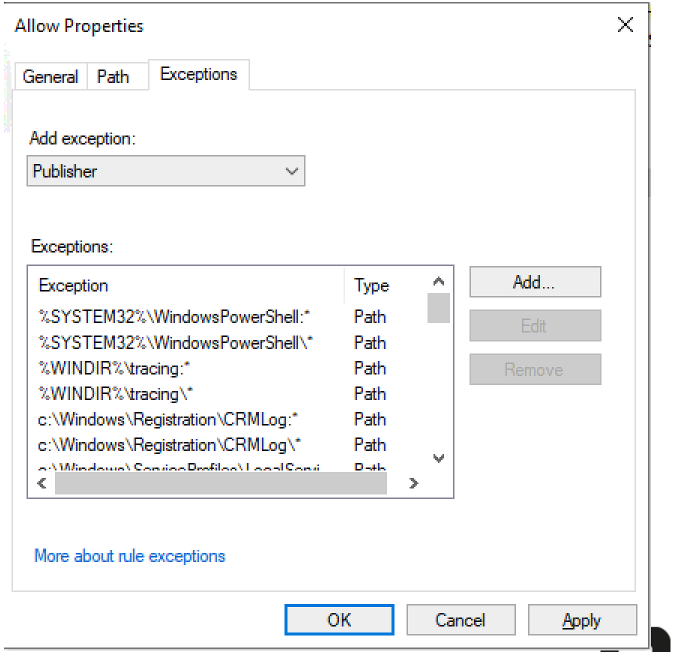


```
accesschk -w -s -q -u Users "C:\Program Files" >> programfiles.txt
accesschk -w -s -q -u Everyone "C:\Program Files" >> programfiles.txt
accesschk -w -s -q -u "Authenticated Users" "C:\Program Files" >> programfiles.txt
accesschk -w -s -q -u Interactive "C:\Program Files" >> programfiles.txt
accesschk -w -s -q -u "This Organization" "C:\Program Files" >> programfiles.txt
accesschk -w -s -q -u "Authentication authority asserted identity" "C:\Program Files" >> programfiles.txt
accesschk -w -s -q -u "Mandatory Label\Medium Mandatory Level" "C:\Program Files" >> programfiles.txt
accesschk -w -s -q -u %username% "C:\Program Files" >> programfiles.txt

accesschk -w -s -q -u Users "C:\Program Files (x86)" >> programfilesx86.txt
accesschk -w -s -q -u Everyone "C:\Program Files (x86)" >> programfilesx86.txt
accesschk -w -s -q -u "Authenticated Users" "C:\Program Files (x86)" >> programfilesx86.txt
accesschk -w -s -q -u Interactive "C:\Program Files (x86)" >> programfilesx86.txt
accesschk -w -s -q -u "This Organization" "C:\Program Files (x86)" >> programfilesx86.txt
accesschk -w -s -q -u "Authentication authority asserted identity" "C:\Program Files (x86)" >> programfilesx86.txt
accesschk -w -s -q -u "Mandatory Label\Medium Mandatory Level" "C:\Program Files (x86)" >> programfilesx86.txt
accesschk -w -s -q -u %username% "C:\Program Files (x86)" >> programfilesx86.txt

accesschk -w -s -q -u Users "C:\Windows" >> windows.txt
accesschk -w -s -q -u Everyone "C:\Windows" >> windows.txt
accesschk -w -s -q -u "Authenticated Users" "C:\Windows" >> windows.txt
accesschk -w -s -q -u Interactive "C:\Windows" >> windows.txt
accesschk -w -s -q -u "This Organization" "C:\Windows" >> windows.txt
accesschk -w -s -q -u "Authentication authority asserted identity" "C:\Windows" >> windows.txt
accesschk -w -s -q -u "Mandatory Label\Medium Mandatory Level" "C:\Windows" >> windows.txt
accesschk -w -s -q -u %username% "C:\Windows" >> windows.txt
```

https://gist.github.com/api0cradle/95cd51fa1aa735d9331186f934df4df9#file-accesschk-bat

Add always the ADS-version of a folder as well

- %WINDIR%\tracing\*
- %WINDIR%\tracing:*



Allow Properties

Add exception:

Publisher

Exceptions:

Exception	Type
%SYSTEM32%\WindowsPowerShell:*	Path
%SYSTEM32%\WindowsPowerShell\*	Path
%WINDIR%\tracing:*	Path
%WINDIR%\tracing\*	Path
c:\Windows\Registration\CRMLog:*	Path
c:\Windows\Registration\CRMLog\*	Path
c:\Windows\ServiceProfiles\LocalServi	Path

Hardening Whitelisting

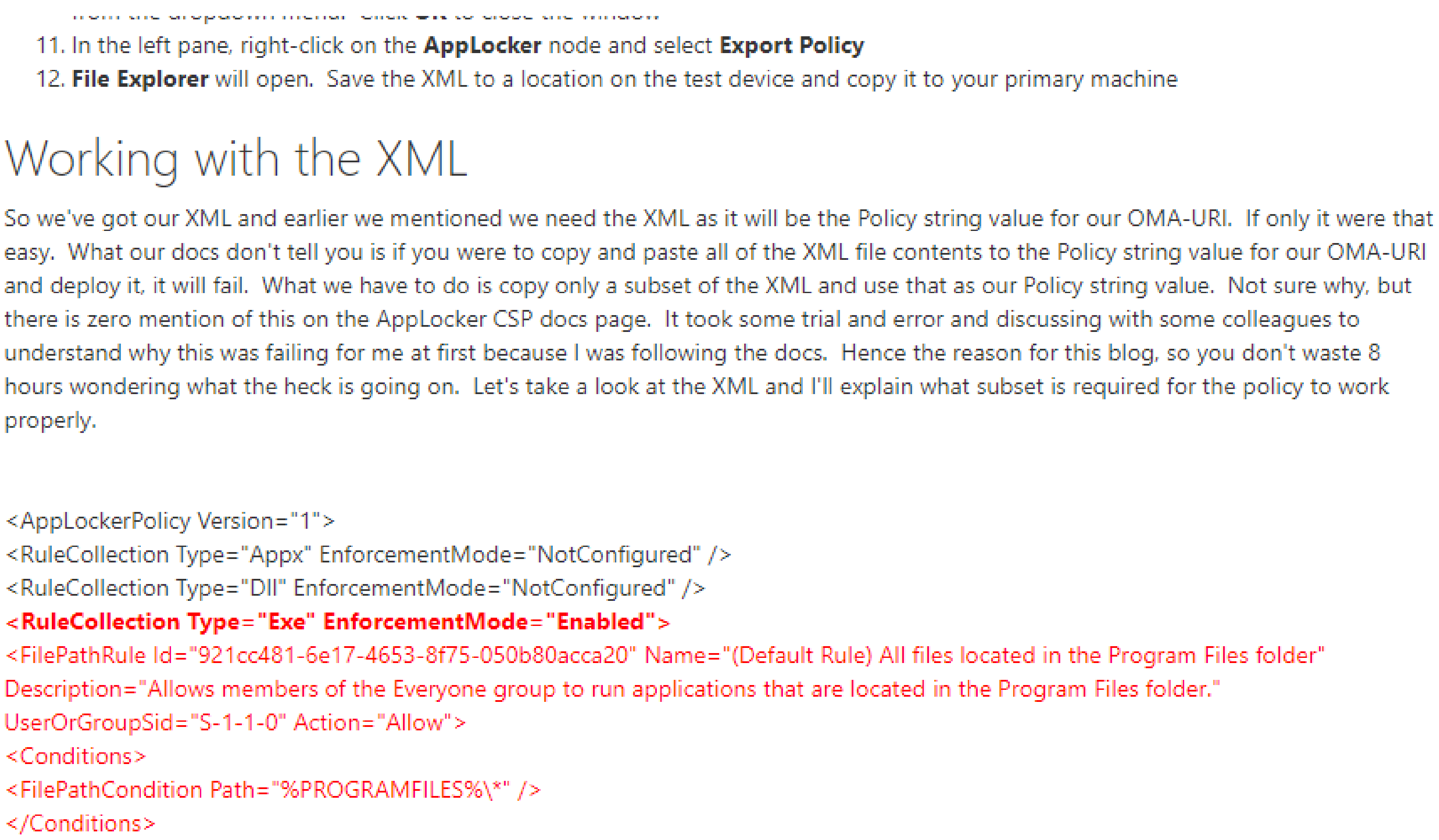
- Remember to repeat the previous for every Folder-Rule you have…

Tools to help

- Oddvar Moe’s
  - **Ultimate AppLocker ByPass List**
    - https://github.com/api0cradle/UltimateAppLockerByPassList
  - PowerAL
    - https://github.com/api0cradle/PowerAL
- AaronLocker
  - https://blogs.msdn.microsoft.com/aaron_margosis/2019/01/28/aaronlocker-moved-to-github/
- Microsoft’s list of what to block: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules

InTune + AppLocker

- https://blogs.technet.microsoft.com/matt_hinsons_manageability_blog/2018/08/21/blocking-apps-with-intune-and-applocker-csp/



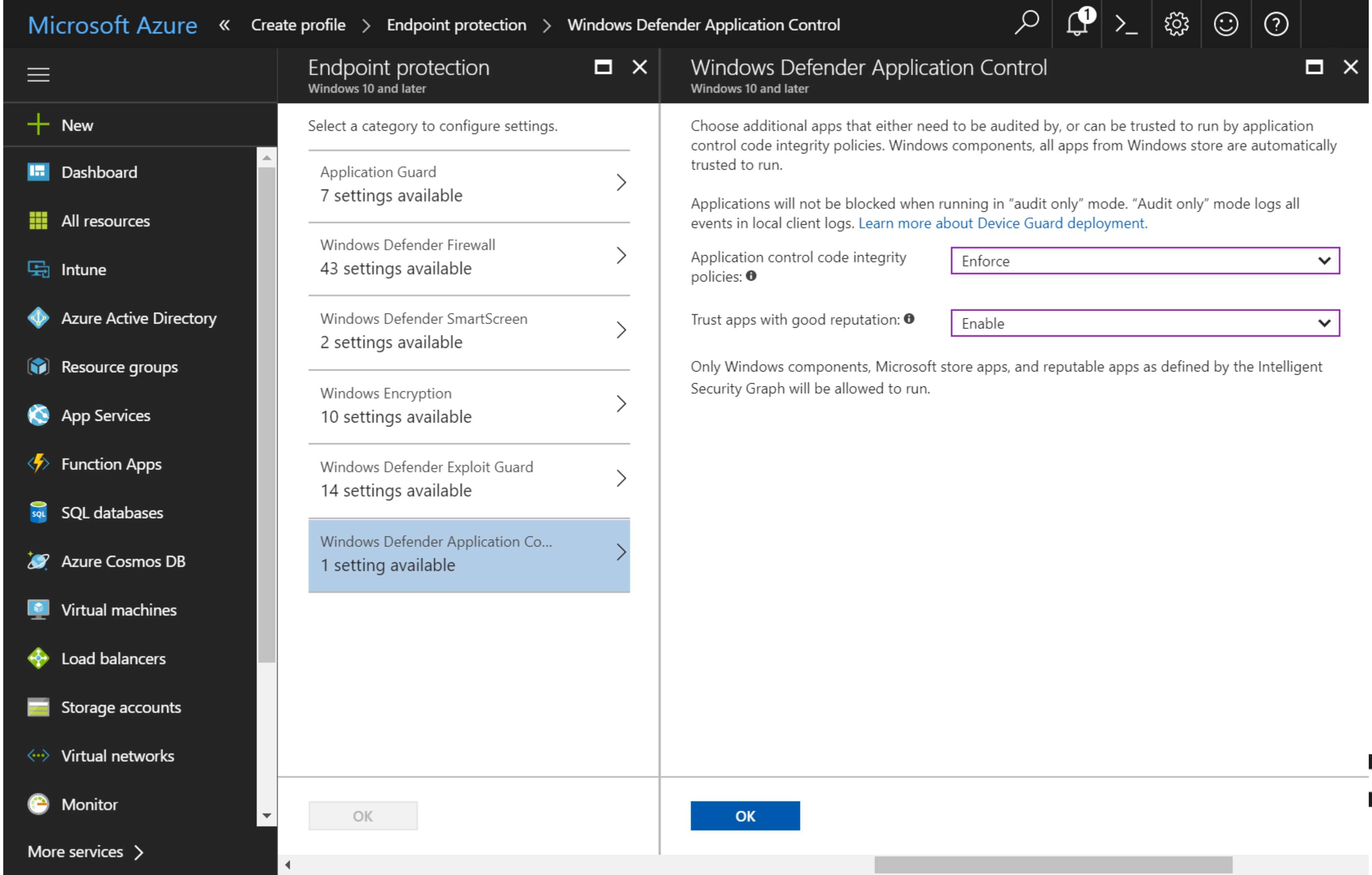
from the dropdown menu. Click **OK** to close the window

11. In the left pane, right-click on the **AppLocker** node and select **Export Policy**
12. **File Explorer** will open. Save the XML to a location on the test device and copy it to your primary machine

Working with the XML

So we've got our XML and earlier we mentioned we need the XML as it will be the Policy string value for our OMA-URI. If only it were that easy. What our docs don't tell you is if you were to copy and paste all of the XML file contents to the Policy string value for our OMA-URI and deploy it, it will fail. What we have to do is copy only a subset of the XML and use that as our Policy string value. Not sure why, but there is zero mention of this on the AppLocker CSP docs page. It took some trial and error and discussing with some colleagues to understand why this was failing for me at first because I was following the docs. Hence the reason for this blog, so you don't waste 8 hours wondering what the heck is going on. Let's take a look at the XML and I'll explain what subset is required for the policy to work properly.

```
<AppLockerPolicy Version="1">
<RuleCollection Type="Appx" EnforcementMode="NotConfigured" />
<RuleCollection Type="Dll" EnforcementMode="NotConfigured" />
<RuleCollection Type="Exe" EnforcementMode="Enabled">
<FilePathRule Id="921cc481-6e17-4653-8f75-050b80acca20" Name="(Default Rule) All files located in the Program Files folder"
Description="Allows members of the Everyone group to run applications that are located in the Program Files folder."
UserOrGroupSid="S-1-1-0" Action="Allow">
<Conditions>
<FilePathCondition Path="%PROGRAMFILES%\*" />
</Conditions>
```



Endpoint protection
Windows 10 and later

Select a category to configure settings.

Application Guard
7 settings available

Windows Defender Firewall
43 settings available

Windows Defender SmartScreen
2 settings available

Windows Encryption
10 settings available

Windows Defender Exploit Guard
14 settings available

Windows Defender Application Co...
1 setting available

Windows Defender Application Control
Windows 10 and later

Choose additional apps that either need to be audited by, or can be trusted to run by application control code integrity policies. Windows components, all apps from Windows store are automatically trusted to run.

Applications will not be blocked when running in "audit only" mode. "Audit only" mode logs all events in local client logs. Learn more about Device Guard deployment.

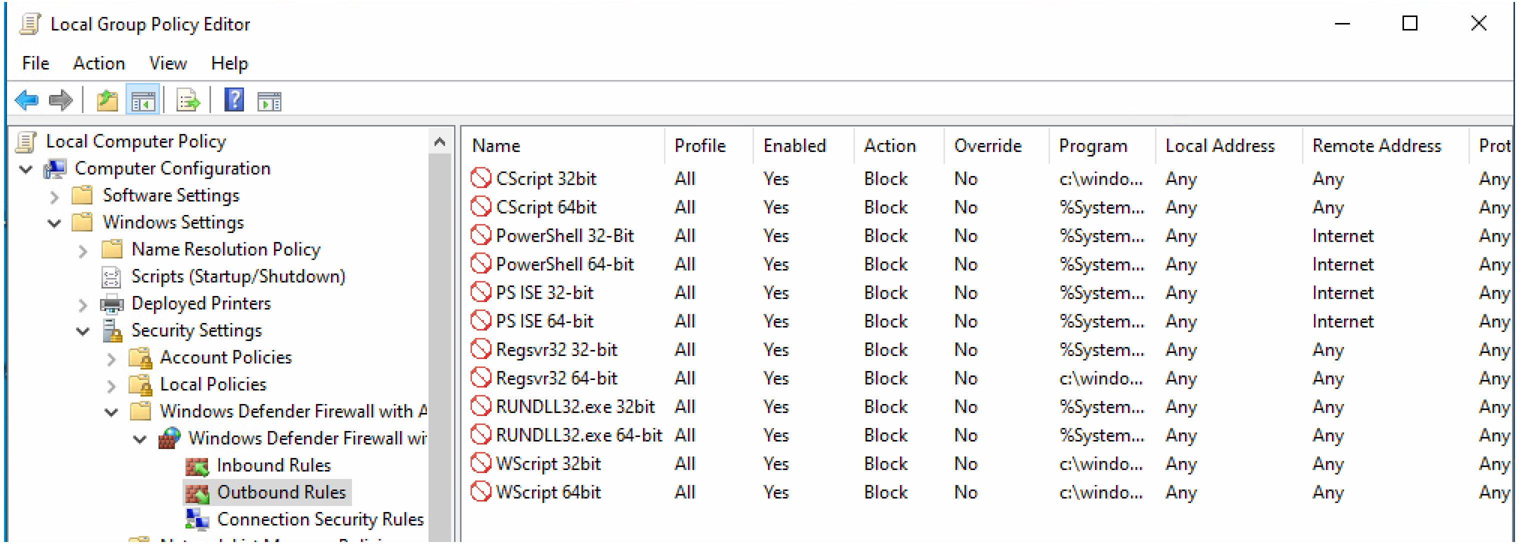
Application control code integrity policies: Enforce

Trust apps with good reputation: Enable

Only Windows components, Microsoft store apps, and reputable apps as defined by the Intelligent Security Graph will be allowed to run.

Implementing Firewall and IPsec

Firewall



Name	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Prot
CScript 32bit	All	Yes	Block	No	c:\windo...	Any	Any	Any
CScript 64bit	All	Yes	Block	No	%System...	Any	Any	Any
PowerShell 32-Bit	All	Yes	Block	No	%System...	Any	Internet	Any
PowerShell 64-bit	All	Yes	Block	No	%System...	Any	Internet	Any
PS ISE 32-bit	All	Yes	Block	No	%System...	Any	Internet	Any
PS ISE 64-bit	All	Yes	Block	No	%System...	Any	Internet	Any
Regsvr32 32-bit	All	Yes	Block	No	%System...	Any	Any	Any
Regsvr32 64-bit	All	Yes	Block	No	c:\windo...	Any	Any	Any
RUNDLL32.exe 32bit	All	Yes	Block	No	%System...	Any	Any	Any
RUNDLL32.exe 64-bit	All	Yes	Block	No	%System...	Any	Any	Any
WScript 32bit	All	Yes	Block	No	c:\windo...	Any	Any	Any
WScript 64bit	All	Yes	Block	No	c:\windo...	Any	Any	Any

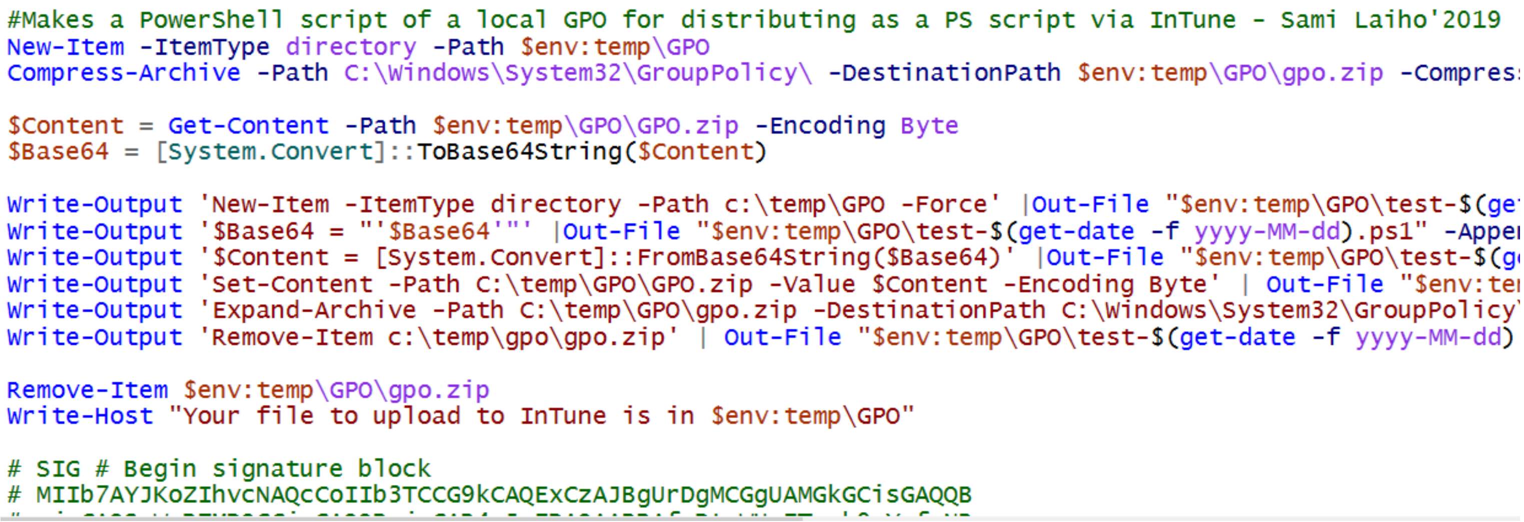
How I use IPsec

- Require Inbound, Request Outbound
- Kerberos for users and computers
- Exclude DC’s and hard cases – You don’t need to get to 100%!
- Buy printers (etc) that can have a certificate if possible

Implementing Group Policy

InTune and AppLocker/Firewall

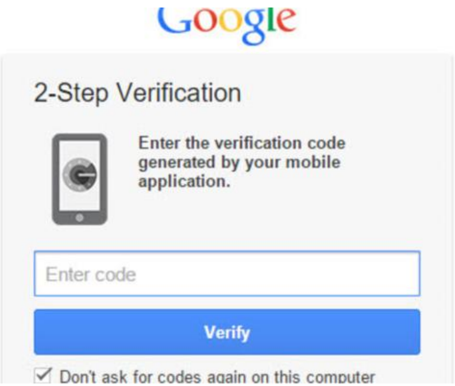
GPO2INTUNE ☺



```
#Makes a PowerShell script of a local GPO for distributing as a PS script via InTune - Sami Laiho'2019
New-Item -ItemType directory -Path $env:temp\GPO
Compress-Archive -Path C:\Windows\System32\GroupPolicy\ -DestinationPath $env:temp\GPO\gpo.zip -Compres

$Content = Get-Content -Path $env:temp\GPO\GPO.zip -Encoding Byte
$Base64 = [System.Convert]::ToBase64String($Content)

Write-Output 'New-Item -ItemType directory -Path c:\temp\GPO -Force' |Out-File "$env:temp\GPO\test-$(ge
Write-Output '$Base64 = "'$Base64'"' |Out-File "$env:temp\GPO\test-$(get-date -f yyyy-MM-dd).ps1" -Appe
Write-Output '$Content = [System.Convert]::FromBase64String($Base64)' |Out-File "$env:temp\GPO\test-$(g
Write-Output 'Set-Content -Path C:\temp\GPO\GPO.zip -Value $Content -Encoding Byte' | Out-File "$env:te
Write-Output 'Expand-Archive -Path C:\temp\GPO\gpo.zip -DestinationPath C:\Windows\System32\GroupPolicy'
Write-Output 'Remove-Item c:\temp\gpo\gpo.zip' | Out-File "$env:temp\GPO\test-$(get-date -f yyyy-MM-dd)

Remove-Item $env:temp\GPO\gpo.zip
Write-Host "Your file to upload to InTune is in $env:temp\GPO"

# SIG # Begin signature block
# MIIb7AYJKoZIhvcNAQcCoIIb3TCCG9kCAQExCzAJBgUrDgMCGgUAMGkGCisGAQQB
```

Setup MFA where ever possible

- Setup Multi-Factor Authentication (MFA) service settings and enable MFA for all possible accounts
  - https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#mfa-service-settings



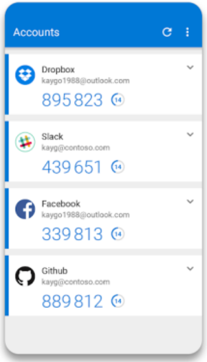
Google

2-Step Verification

Enter the verification code generated by your mobile application.

☑ Don't ask for codes again on this computer

More secure



Accounts

Dropbox
kaygo1988@outlook.com
895823 14

Slack
kayg@contoso.com
439651 14

Facebook
kaygo1988@outlook.com
339813 14

Github
kayg@contoso.com
889812 14

2 Factor Authentication!

Smart Cards are difficult, Virtual Smart Cards will be deprecated… So let me introduce the Future of 2FA……..

Name: Token

Token Type: Live, Hedgehog

Token lifetime: 5-8 years

Tamper Protection: Yes

006

Checklist for Security

- https://www.itpromentor.com/azure-ad-checklist/

Contact

- sami@adminize.com
- Twitter: @samilaiho
- Blog: http://blog.win-fu.com/
  - New on https://4sysops.com/
- Free newsletter: http://eepurl.com/F-GOj
- My trainings:
  - https://win-fu.com/events
  - https://win-fu.com/dojo/
    - Free for one month!! Code:"Trial2018"
  - PluralSight: If you need a code email me!