nic X edition

May 31 – June 2, Oslo Spektrum

10th anniversary

Deploy and manage **AppLocker** like a pro with Microsoft **Intune** and **Log Analytics**

Sandy Zeng

Senior Cloud Architect

CloudWay

Microsoft MVP | MCT
@sandy_tsang

Maurice Daly

Principal Cloud Architect

CloudWay

Microsoft MVP | MCT
@modaly_it

Introduction

- **What is AppLocker?**
- **Why do we care about AppLocker as a feature**
  - Prevent unapproved apps and scripts from running
- **Managing AppLocker**
  - Group policy-based management
  - Intune CSP based management
  - Auditing vs Enforcement

Introduction Continued

- **Auditing Events Centrally**
- **Reporting on Events**
  - Event Viewer
  - PowerShell
- **Log Analytics Approach**
  - Collection of data from clients
  - Parsing logs to find events
  - Using KQL to generate AppLocker rules
  - Building functional workbooks with drag / drop code

What is AppLocker?

AppLocker is a defense-in-depth security feature and not a security boundary.
Administrators can use it to block or approve applications, installers, DLL’s, modern apps, and scripts.

- **AppLocker Timeline & Features**
  - Originally introduced in Windows 7 and Server 2008 R2
    - Only Enterprise and Ultimate SKU’s allowed enforcement, Pro allowed policy creation ONLY
  - Windows 8 added Packaged App functionality (Store Apps)
  - Windows 8 RT – Not supported
  - Windows Server 2012 R2, 2016 and 2019 support added
  - Windows 10 support added
  - Windows 11 support added

AppLocker & WDAC

Choose when to use WDAC or AppLocker

Generally, it is recommended that customers, who are able to implement application control using WDAC rather than AppLocker, do so. WDAC is undergoing continual improvements, and will be getting added support from Microsoft management platforms. Although AppLocker will continue to receive security fixes, it will not undergo new feature improvements.

However, in some cases, AppLocker may be the more appropriate technology for your organization. AppLocker is best when:

You have a mixed Windows operating system (OS) environment and need to apply the same policy controls to Windows 10 and earlier versions of the OS.

You need to apply different policies for different users or groups on shared computers.

You do not want to enforce application control on application files such as DLLs or drivers.

“AppLocker can also be deployed as a complement to WDAC to add user or group-specific rules for shared device scenarios, where it is important to prevent some users from running specific apps.

As a best practice, you should enforce WDAC at the most restrictive level possible for your organization, and then you can use AppLocker to further fine-tune the restrictions.”

Why Should I Care

Windows 10/11 Enterprise

Both compliance and security features in Windows are similar to a Swiss Army Knife, many features, but seldomly utilized in full..

What do we use?

- BitLocker
- Credential Guard

Sometimes we purchase third party solutions when we don't need to

Why Should I Care?

- No all apps require administrative privileges to execute, therefore, think about security
  - Malware
  - Ransomware
  - Keylogging
  - Malicious Payload
- Does the typical end-user care about which site the application is downloaded from?
- Do users need admin rights for all executable files?
- Does this pose an acceptable threat to your organization?
- Do you want to block outdated applications?
- Do you want to block non-licensed applications?

Implementing AppLocker

AppLocker implementation, typical responses

- I don’t want to deal with the management overhead
- We have far too many applications to think about doing this
- We tried it once and it caused lots of problems

Group Policy Management

- Provides you with the ability to provide access or deny polices based on the following;
  - **Publisher**
    - The most wildly used option as it allows you to trust the digital signer
  - **Path**
    - Common in default configurations for Windows & Program Files, but less wildly used for locations outside of this
  - **File Hash**
    - Used for script and tighter control of the specific files to run

Implementing AppLocker

AppLocker implementation, typical responses

- I don’t want to deal with the management overhead
- We have far too many applications to think about doing this
- We tried it once and it caused lots of problems

Group Policy Management

- Provides you with the ability to provide access or deny polices based on the following;
  - **Publisher**
    - The most wildly used option as it allows you to trust the digital signer
  - **Path**
    - Common in default configurations for Windows & Program Files, but less wildly used for locations outside of this
  - **File Hash**
    - Used for script and tighter control of the specific files to run

Licensing Requirements

NOT ALL LICENSES ARE EQUAL

- AppLocker was originally introduced for Windows 7 Enterprise, i.e. it required an “enterprise” license, therefore, no “enterprise” = no AppLocker?
  - Wrong
- **Windows 10 changed this with the addition of the AppLocker CSP**
  - AppLocker CSP
    - Provides the ability to set policies on ANY edition of Windows 10 supported by MDM
    - Machines managed by Group Policy can only enforce on the Enterprise and Education SKU’s
- In summary. GPO + AppLocker = Enterprise ONLY, MDM + AppLocker = PRO + ENTERPRISE

  Makes sense? Of course not.. But this is a good stick to beat down the path to using MDM!

IMPLEMENTING THROUGH GPO’S

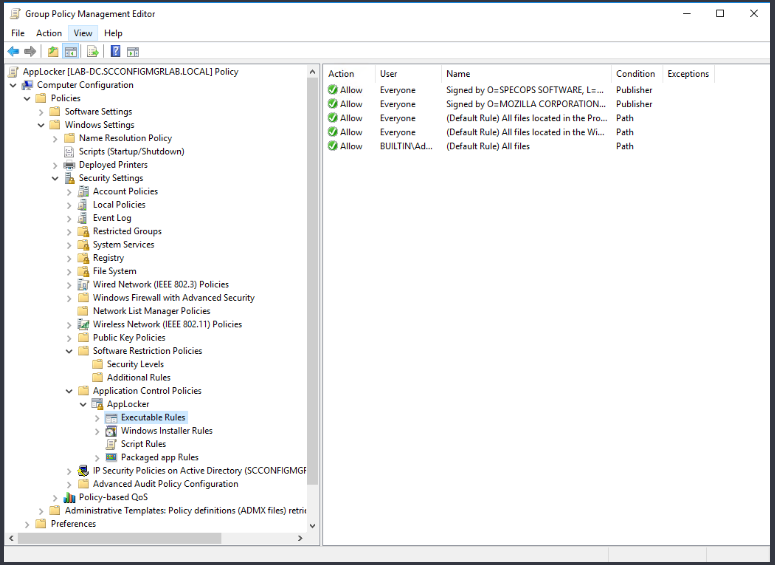
Implementing group policies, the old school way..

Implementing AppLocker – Group Policy

Group Policy Management

- Policy deployed in Computer Configuration \ Policies \ Application Control Policies \ AppLocker
- Rules need to be defined to allow or deny based on the detection method specified
  - Executable Files
  - Windows Installer Files
  - Script Files
  - Packaged App Files
- Application Identity service must be running (set to Automatic)

sc.exe config appidsvc start= auto

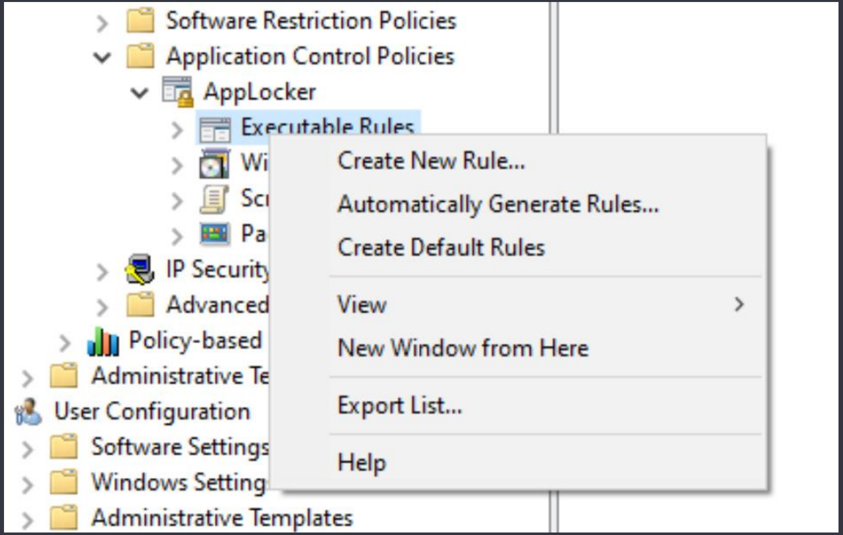

Group Policy Management Editor
File
Action
View
Help
AppLocker [LAB-DC.SCCONFIGMGRLAB.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Security Levels
Additional Rules
Application Control Policies
AppLocker
Executable Rules
Windows Installer Rules
Script Rules
Packaged app Rules
IP Security Policies on Active Directory (SCCONFIGMGF
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX files) retrie
Preferences

Action	User	Name	Condition	Exceptions
✓ Allow	Everyone	Signed by O=SPECOPS SOFTWARE, L=...	Publisher	
✓ Allow	Everyone	Signed by O=MOZILLA CORPORATION...	Publisher	
✓ Allow	Everyone	(Default Rule) All files located in the Pro...	Path	
✓ Allow	Everyone	(Default Rule) All files located in the Wi...	Path	
✓ Allow	BUILTIN\Ad...	(Default Rule) All files	Path	

Implementing AppLocker – Group Policy

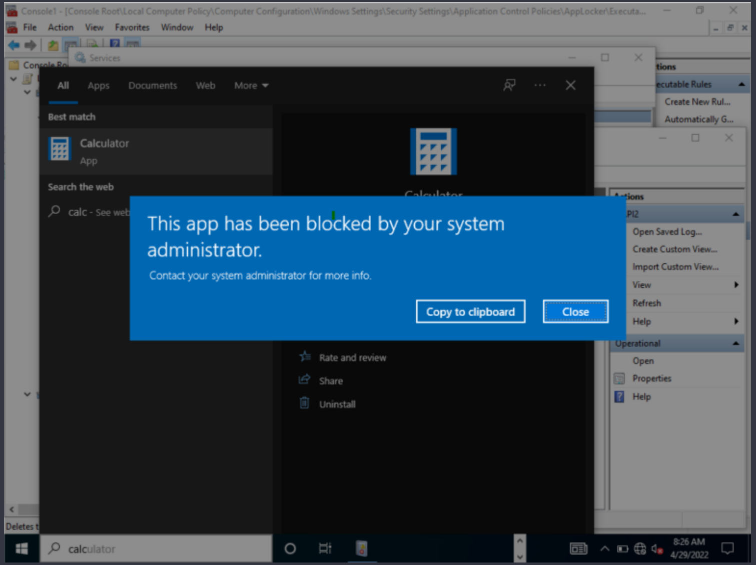
Group Policy Management

- Create Default Rules
  - This effectively whitelists the following;
    - C:\Windows
    - C:\Program Files
    - Any EXE for local admins
  - Potential risk of items running inside the Windows and Program Files directory
- Automatically Generate Rules
  - Gather application information on a source device
  - More policy rich, but source needs to be a refection on your production machines



AppLocker End User Experience

- **End User Experience**
  - Applications not included as allowed, or applications explicitly set to denied are blocked
- **Auditing**
  - It is vital that you run AppLocker in audit mode to gather information BEFORE pressing the big red button and pushing the policy as “enforced”
- **BE CAREFUL**
  - If you create a policy and accidentally remove all rules, with the policy in effect, it will prevent something like the entire OS from working.. …kind of bad



This app has been blocked by your system administrator.

Contact your system administrator for more info.

GPO Based Management

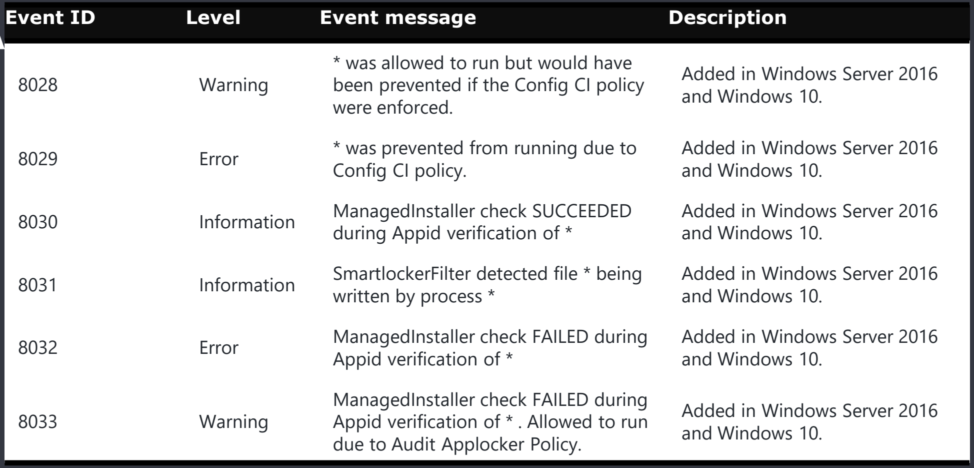
AppLocker – Event Logs

- Events are written into the registry in the following locations;
  - Microsoft-Windows-AppLocker/EXE and DLL
  - Microsoft-Windows-AppLocker/MSI and Script
  - Microsoft-Windows-AppLocker/Packaged app-Deployment
  - Microsoft-Windows-AppLocker/Packaged app-Execution
- PowerShell can be used to harvest events using
  - *Get-AppLockerFileInformation*
    - Provides details on executables and their audit / blocked states
  - *Get-WinEvent -LogName "Microsoft-Windows-Applocker/EXE and DLL“*
    - Same as above but direct from the event log

AppLocker – Missing Event Logs..

But wait.. Isn’t there Windows 10, 11 and Server 2016, 2019?

A



Event ID	Level	Event message	Description
8028	Warning	* was allowed to run but would have been prevented if the Config CI policy were enforced.	Added in Windows Server 2016 and Windows 10.
8029	Error	* was prevented from running due to Config CI policy.	Added in Windows Server 2016 and Windows 10.
8030	Information	ManagedInstaller check SUCCEEDED during Appid verification of *	Added in Windows Server 2016 and Windows 10.
8031	Information	SmartlockerFilter detected file * being written by process *	Added in Windows Server 2016 and Windows 10.
8032	Error	ManagedInstaller check FAILED during Appid verification of *	Added in Windows Server 2016 and Windows 10.
8033	Warning	ManagedInstaller check FAILED during Appid verification of * . Allowed to run due to Audit Applocker Policy.	Added in Windows Server 2016 and Windows 10.

Good news – Docs are updated - https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/using-event-viewer-with-applocker

Event ID’s 8028 – 8040 added.. YOU ARE WELCOME

Windows Client Demo

IT HELPDESK ENGINEERS BE LIKE..

LOOK AT THE NUMBER OF HELPDESK ISSUES..
I GUESS YOU WON THE BET ON HOW QUICKLY
APPLOCKER WOULD BE ROLLED BACK

AppLocker Auditing

- AppLocker policy rollout needs to be audited first, **NEVER** go straight to production
- Centralized reporting can be carried out through PowerShell
  - Script included here. You're welcome.
  - Make use of the Get-AppLockerFileInformation cmdlet
  - Go further by reading the Event Log
    Get-EventLog
    Get-WinEvent
  - Run the PowerShell audit script as a PR or Scheduled Task depending on your license
  - Azure Monitor agent on Windows client devices (Preview)
    https://docs.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-windows-client

- **Audit for at least 30 days prior to enforcement**

Implementing AppLocker - MDM

- AppLocker configuration within Intune is handled through the AppLocker CSP
  - https://docs.microsoft.com/en-us/windows/client-management/mdm/applocker-csp
- Policy implemented through OMA-URI based policy (Custom)
  - Policy **CAN NOT** be imported through Group Policy Analytics
  - Unfriendly method, but the rules are just XML
    - Using String (XML File) provides a better formatting experience, but policies can’t be edited in place

  - Example:

Implementing AppLocker - MDM

EXE File

./Vendor/MSFT/AppLocker/ApplicationLaunchRestrictions/AllowedApps01/EXE/Policy

Store Apps

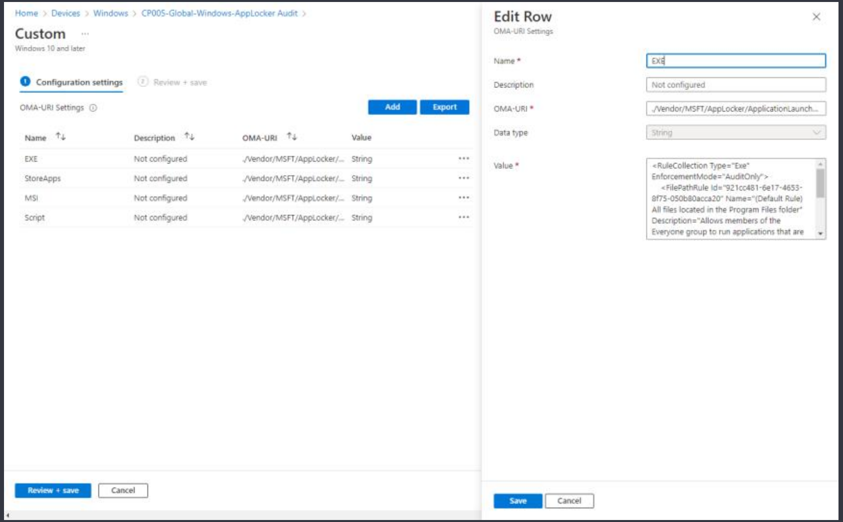
./Vendor/MSFT/AppLocker/ApplicationLaunchRestrictions/AllowedApps01/StoreApps/Policy

MSI File

./Vendor/MSFT/AppLocker/ApplicationLaunchRestrictions/AllowedApps01/MSI/Policy

Script File

/Vendor/MSFT/AppLocker/ApplicationLaunchRestrictions/AllowedApps01/Script/Policy



Name	Description	OMA-URI	Value
EXE	Not configured	./Vendor/MSFT/AppLocker/...	String
StoreApps	Not configured	./Vendor/MSFT/AppLocker/...	String
MSI	Not configured	./Vendor/MSFT/AppLocker/...	String
Script	Not configured	./Vendor/MSFT/AppLocker/...	String

Name *: EXE

Description: Not configured

OMA-URI *: ./Vendor/MSFT/AppLocker/ApplicationLaunch...

Data type: String

Value *:

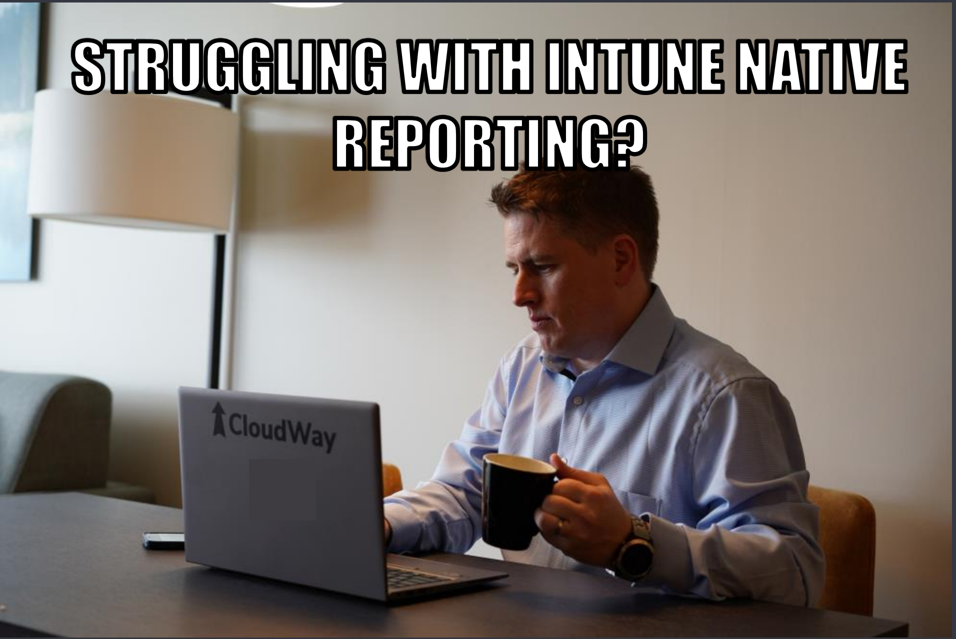
```
<RuleCollection Type="Exe"
EnforcementMode="AuditOnly">
   <FilePathRule Id="921cc481-6e17-4653-
8f75-050b80acca20" Name="(Default Rule)
All files located in the Program Files folder"
Description="Allows members of the
Everyone group to run applications that are
```

Intune Policy Deployment

Intune AppLocker Reporting

SPOILER ALERT: THERE ISN'T ANY

“Product Limitations”.. No worries



Intune AppLocker Reporting - KQL

Log Analytics / KQL to the rescue!!!

- Reading in the AppLocker events from the event logs, we have the following;
  - Application Name
  - Application Path
  - Publisher Name
  - Version
  - File Hash

How do I get this information from the clients?

- Proactive Remediations

Deploying AppLocker Like A Pro

- Leverage AppLocker event logs and log analytics, together in the form of a workbook
- Benefits?
  - Reports that you can share with management showing your AppLocker rollout success and what is being blocked inside your organization
  - Create drag and drop rules in the workbook!
    - **No more GPO AppLocker policy creation with XML export required**
  - Other possibilities - Create alerts on new blocked applications for the helpdesk to examine

Modern Reporting

Where Can I Get This Workbook?

- At present a community version is available on the MSEndpointMgr blog which detects and reports based on EXE’s only
- But good news!
    - The version demonstrated today will be made available soon on the MSEndpointMgr.com blog
        - Consists of;
          Proactive Remediation Script (PowerShell PS1)
          Workbook (JSON)

Troubleshooting

- **Making changes, but no change locally on the client?**
  - Stop the Application Identity Service
  - Delete the local cached AppLocker rules from C:\Windows\System32\AppLocker
  - Start the Application Identity Service
  - Test again..

- ~~**Current Situation – MDM Reporting Bug**~~
  - ~~At present if you deploy an AppLocker policy in either enforcement state, the results of the application of the policy show as.. 0..~~

Conclusion

- Defender Application Control uses the same type of mechanisms to block applications, but this is based on reputational values of the applications
- **AppLocker provides granular security**
  - WDAC provides reputational, but AppLocker can supplement
- Reporting can be made easy
- Rules can be made easy
- Implement AppLocker as part of your overall security model

CONGRATULATIONS
YOU NOW KNOW ABOUT APPLOCKER MANAGENENT

Slides and demos from the conference will be available at

https://github.com/nordicinfrastructureconference/2022

nic X edition