

May 2023

Getting Started with Intune EPM



MEMUG

Nick Moseley

Special Thanks To Our Sponsors!

Let us handle the tedious work of packaging, testing, deploying, and troubleshooting application updates in your ConfigMgr or Intune environment. Easily extend Microsoft Endpoint Manager to deploy and update over third-party applications within your enterprise.

Save time, money, and stay secure by automating the publishing of third-party updates to your environment. Setup only takes minutes. All subscriptions include free in-house support and setup calls!



Recast Software creates tools used by hundreds of thousands of enterprise organizations worldwide, impacting millions of devices and (more importantly) the people who use them. Our mission is to be an integral part of how IT teams create highly secure and compliant environments, capable of handling technological change. We do this by integrating with existing IT infrastructure to provide deeper, more actionable insights, improved productivity, and powerful, scalable automation.



ScriptRunner is the #1 platform for IT infrastructure management with PowerShell. Centralizing, standardizing, automating, delegating, monitoring and controlling routine tasks frees up resources in IT operations. Administrators and DevOps teams can use and customize included script libraries or develop their own scripts.

ScriptRunner allows you to securely delegate administrative tasks to users without PowerShell knowledge or appropriate rights. ScriptRunner is used worldwide by IT teams of all sizes and industries.



Agenda

Getting Started with Intune EPM

Nick Moseley



Announcements

Getting Started with Intune EPM

1. What is Intune EPM?
2. Trial registration and prerequisites.
3. Enrolling users/devices.
4. Basics of EPM rules.



P'za & Beverage Break



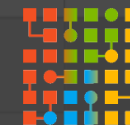
5. Real-world, no cost, no fuss examples.
6. Troubleshooting tips.

Raffle!!



Upcoming Sponsored Event!!

- Sponsored by ScriptRunner
- Friday July 28th – 9 AM (confirmed) to 2 PM (subject to change)
- Multiple sessions for this extended event focused on AI:
 - **Demystifying AI**
Featuring Jennifer Martinez, Strategic Technology Strategist at Microsoft
 - **Enhancing Cybersecurity Using AI to Collect, Collate and Curate**
Featuring Rod Trent, Senior Cloud Advocate at Microsoft. and all-around community leader
 - **Microsoft 365 Copilot**
Featuring Nick Aquino, Senior Technical Specialist at Microsoft
 - Others...?





What is Intune EPM?

Endpoint security is like onions, it has rings.



MEMUG

EPM is part of the Intune Suite



Remote Help



Tunnel for Mobile Application Management



Endpoint Privilege Management



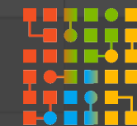
Advanced Endpoint Analytics



Advanced application management (roadmap)

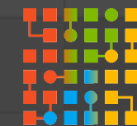
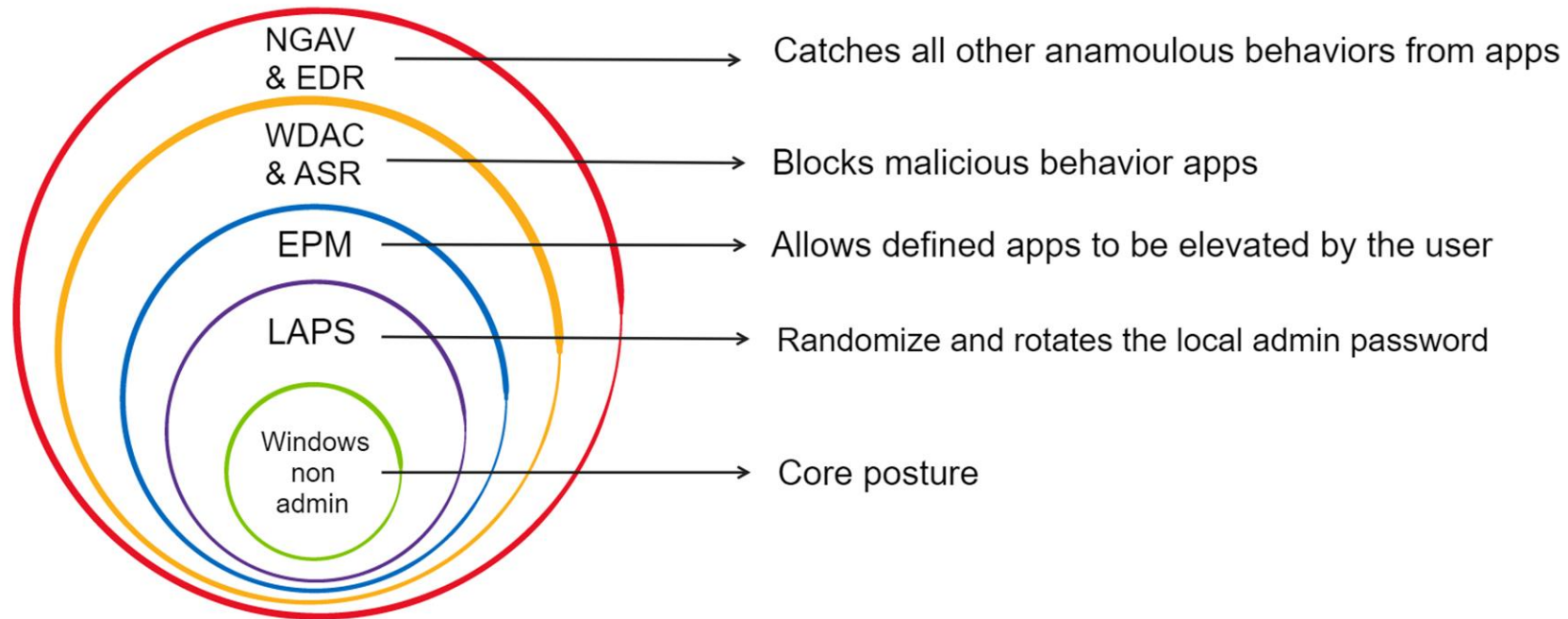


Cloud-based certificate management (roadmap)



MEMUG

Protecting Endpoints from Malware





Environment Readiness

Oh yeah...there's also this thing about Intune configurations or something

Summary of EPM Readiness

Activate EPM trial licenses

- EPM standalone trial or Intune Plan 2
- From the Intune portal or the M365 Admin portal
- Requires Global Admin or Billing Admin

Intune tenant configuration

- [Enable use of Windows diagnostic data by Intune](#)
- [Create a Windows Health Monitoring profile in Intune](#)

Win10 20H2+ or Win11 21H2+

- Managed by Intune
- April 2023 cumulative update installed
- Azure AD joined or hybrid
- Professional or Enterprise



Demo

Environment
Readiness for EPM

Activate EPM trial licenses

Intune tenant configuration

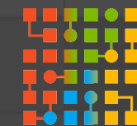
- Diagnostic Data for Windows
- Windows Health Monitoring

Windows 10/11 (using Client Hyper-V)



Enrolling Devices

Remember that users need to get on board with this whole thing too

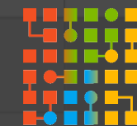
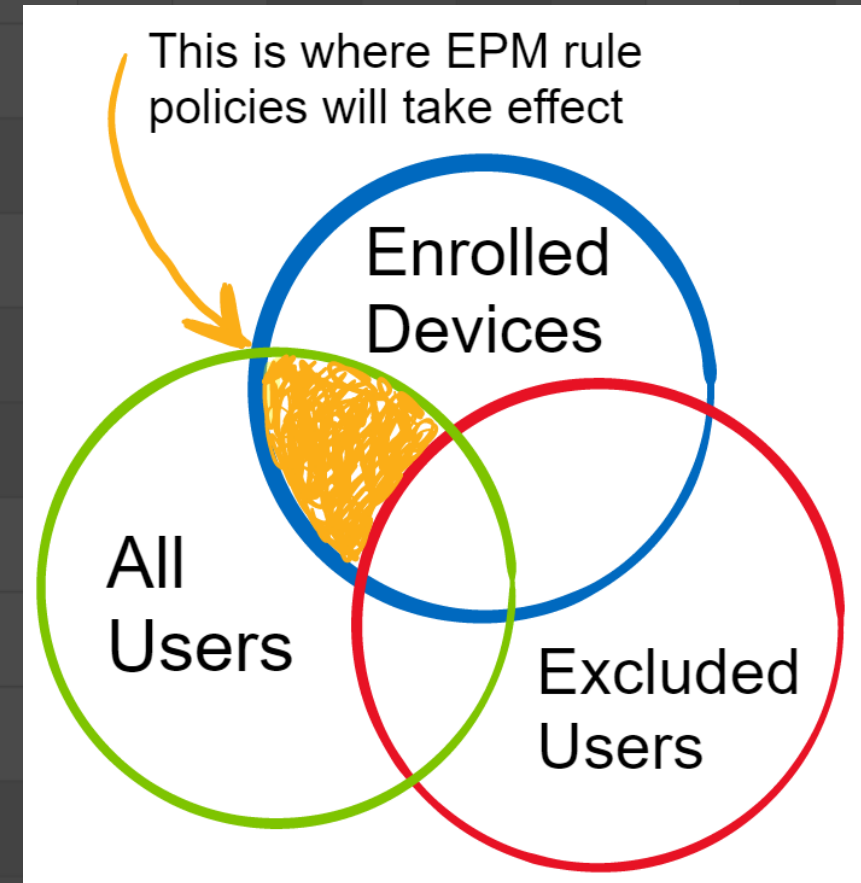


MEMUG

Enroll Devices...or Enroll Users?

Answer: it depends

- Flexibility to target users, devices, or mix of both.
- Approach for a POC is to:
 - Enroll specific devices
 - Target all users with the elevation rule policies
 - Exclude any undesired users, like desktop admins



Demo

Creating EPM client
settings policies

Create profile ...

Elevation settings policy

1 Basics 2 Configuration settings 3 Scope tags 4 Assignments 5 Review + create

Privilege Management Elevation Client Settings

Elevation settings establish the default behaviors for the endpoint elevation client.

Endpoint Privilege Management Enabled

Send elevation data for reporting * Yes

Reporting scope * Diagnostic data and all endpoint elevations

Default elevation response

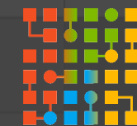
- Not configured
- Deny all requests
- Require user confirmation
- Not configured

Most Restrictive
Most Flexibility



Basics of EPM Elevation Rules

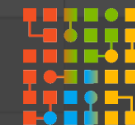
It's simple, really simple... seriously, I'm not lying



MEMUG

Application Identification Methods

Trust Level	Elevation Rule Type
No bueno	File properties such as name, path, version, etc.
Good	Certificate
Better	Hash
Best	Hash + certificate
Best of the best	Hash + certificate + file properties



Collecting Hashes – pretty easy to do

```
Administrator: C:\Windows\system32\cmd.exe - powershell
PS C:\temp> Get-FileHash .\procmon64.exe
```

Algorithm	Hash	Path
SHA256	CBE952CBCF66A0DE40D4E494C970A310257712D44363DDB157F469A351D57ACB	C:\temp\procmon64.exe

Collecting Certificates – more involved

Step 1 – Import the Certificate into a cert store

The image shows a sequence of four Windows dialog boxes illustrating the process of importing a certificate:

- MicrosoftEdgeSetupDev.exe Properties**: The **Digital Signatures** tab is selected. A table lists the signature details:

Name of signer:	Digest algorithm	Timestamp
Microsoft Corporation	sha256	Tuesday, March 28
C2RService	sha256	Not available

- Digital Signature Details**: Shows the **Digital Signature Information** for the Microsoft Corporation signature. The **View Certificate** button is highlighted.
- Certificate**: Shows the **Certificate Information** for the selected certificate. The **Install Certificate...** button is highlighted.
- Certificate Import Wizard**: Shows the **Completing the Certificate Import Wizard** screen. The settings for the certificate store are highlighted:

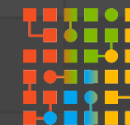
Setting	Value
Certificate Store Selected by User	Personal
Content	Certificate

Collecting Certificates – more involved

Step 2 – Export the certificate file Base64 encoded

The screenshot shows the Windows Certificate Manager (certmgr) interface. The main window displays a list of certificates under 'Certificates - Current User > Personal > Certificates'. A context menu is open over the selected certificate, with the 'Export...' option highlighted. The 'Certificate Export Wizard' dialog box is open, showing the 'Export File Format' section. The 'Base-64 encoded X.509 (.CER)' option is selected and circled in red. Other options include 'DER encoded binary X.509 (.CER)', 'Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)', 'Personal Information Exchange - PKCS #12 (.PFX)', and 'Microsoft Serialized Certificate Store (.SST)'. The 'Next' and 'Cancel' buttons are visible at the bottom of the wizard.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
Microsoft Corporation	Microsoft Code Signing PCA 2011	1/31/2024	Windows RT Verific...	<None>		
Nick Moseley	WIN - MSIT1	7/20/2023	Smart Card Logon, ...	<None>		1.3.6.1.4.1.311....



Collecting Certificates – more involved

Step 3 – Upload into EPM as a reusable setting

Home > Endpoint security

Endpoint security | Endpoint Privilege Management

Search

Overview

- Overview
- All devices
- Security baselines
- Security tasks

Reports Policies **Reusable settings**

+ Add Refresh

Search by setting name

Setting group name

Configure reusable settings (preview)

Windows 10 and later

Basics **2 Configuration settings** Review + Save

Upload a certificate from your organization.

Privilege Management

Certificate file

Base 64 value

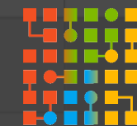
```
-----BEGIN CERTIFICATE-----  
MIIF9DCCA9ygAwIBAgITMwAAAz5jOoa/QXPX4AAAAADPjANBgkqhki  
G9w0BAQsF  
ADB+MQswCQYDVQQGEwJVUzETMBEGA1UECBMKV2FzaGluZ3RvbjEQ  
MA4GA1UEBxMH  
UmVkbW9uZDEeMBwGA1UEChMVTWljcm9zb2Z0IENvcnBvcnF0aW9u  
MSgwJgYDVQQD
```



**What I need now is
lots and lots of coffee.**

Example Elevation Rules

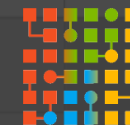
Like a cup of coffee in the morning, these example will get you going



MEMUG

Example Applications

Application	Version	Elevation Behavior	POC Purpose
NotMyFault	4.21	Always	Will not be allowed to run. <i>(As defined by the client default configuration to Deny All)</i>
Process Monitor	3.93	Always	Will be automatically elevated without any user interaction necessary.
VMMap	3.32	Partial	Can partially run under user's non-admin rights, but then can be elevated to provide the full application experience with Windows authentication.
Edge Insider	N/A	Partial	Uses the signing certificate to allow <i>any version of the application</i> to be elevated. In this case, it represents a vendor's application to be installed by the user.
CMD Shell	Per OS	Partial	Will require business justification and Windows authentication together in order to elevate. Also uses one hash per OS.



Demo

Creating these real-world examples in real-time!

User experience(s) with the application

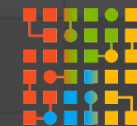
Let's hope this works seamlessly!

Application	Rule Type	Outcome
NotMyFault	No rule defined	Will be blocked by both standard user and default EPM settings
CMD Shell	Hash / Windows auth and biz justification	Can run elevated – don't do this in production ;-)
Process Monitor	Hash / Auto-elevate	No explicit user action
VMMMap	Hash / Windows auth	Two user experiences
Edge Insider	Cert / Biz Justification	Allowed to install



Troubleshooting EPM

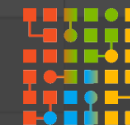
When your stuck, these tips will help you navigate the darkness



MEMUG

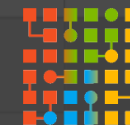
The Things to Use for Troubleshooting

What	Where	How to Use What
Environment Prereqs	Learn about using EPM with Intune Prereqs	Do you have the right OS version?
Reporting	Intune portal EPM	Per-policy reports with info per device.
Client-side log files	C:\Program Files\Microsoft EPM Agent\Logs\	<ul style="list-style-type: none">• EPM.Log - Rule Management Library, Extensibility Adapter, Interop Functions, Client Stub• EPMConsentUI.log - UX for EPM• EPMService.log - EPM Service operations• EPMServiceStub.log - Post validation file launch
Registry keys	HKLM:\SOFTWARE\Microsoft\PolicyManager\current\device\ DeviceHealthMonitoring	“PrivilegeManagement” is set for value DHMScopeValue & ConfigDeviceHealthMonitoringScope
Windows services	<ul style="list-style-type: none">• Microsoft EPM Agent Service• Microsoft Intune Management Extension	Ensure they are running and not disabled.



The Things to Use for Troubleshooting

What	Where	How to Use What
Windows events	Application and Service Logs > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider	Admin > event 4023 (enrollment)
Task Scheduler	Microsoft > Windows > EnterpriseMgmt	Two entries with GUIDs
PowerShell module	C:\Program Files\Microsoft EPM Agent\EpmTools	Import-Module .\EpmCmdlets.dll <ul style="list-style-type: none">• Get-Policies• Get-DeclaredConfiguration• Get-DeclaredConfigurationAnalysis• Get-ElevationRules• Get-ClientSettings



Demo

Troubleshooting
EPM

- Intune portal – EPM reporting
- Client-side log files
- PowerShell Module

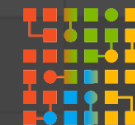


Other Training

Today's session is not intended as the "be all, end all" of learning

More Resources on the Intune Suite

- [Intune EPM « t3chn1ck \(wordpress.com\)](#)
- [Microsoft Intune Blog - Microsoft Community Hub](#)
- [Tech Accelerator: Microsoft Intune Suite | Digital event, April 2023](#)
- [New Microsoft Intune Suite with Privilege Management, Advanced Analytics, Remote Help & App VPN](#)
- [The Projected Total Economic Impact™ Of The Microsoft Intune Suite](#)
- Roadmap: <https://aka.ms/M365roadmap>
- [Unpacking Endpoint Management - YouTube](#)



Special Thanks To Our Sponsors!

Let us handle the tedious work of packaging, testing, deploying, and troubleshooting application updates in your ConfigMgr or Intune environment. Easily extend Microsoft Endpoint Manager to deploy and update over third-party applications within your enterprise.

Save time, money, and stay secure by automating the publishing of third-party updates to your environment. Setup only takes minutes. All subscriptions include free in-house support and setup calls!



Recast Software creates tools used by hundreds of thousands of enterprise organizations worldwide, impacting millions of devices and (more importantly) the people who use them. Our mission is to be an integral part of how IT teams create highly secure and compliant environments, capable of handling technological change. We do this by integrating with existing IT infrastructure to provide deeper, more actionable insights, improved productivity, and powerful, scalable automation.



ScriptRunner is the #1 platform for IT infrastructure management with PowerShell. Centralizing, standardizing, automating, delegating, monitoring and controlling routine tasks frees up resources in IT operations. Administrators and DevOps teams can use and customize included script libraries or develop their own scripts.

ScriptRunner allows you to securely delegate administrative tasks to users without PowerShell knowledge or appropriate rights. ScriptRunner is used worldwide by IT teams of all sizes and industries.

