HOW TO MANAGE DEVICES

#htmdcommunity

@htmdcommunity

HTMD Community Conference - 2024

Microsoft

PATCH MY PC

ZERO TOUCH

nerdio

Thank You Sponsors!

Microsoft

PATCH MY PC

ZERO TOUCH

nerdio

Speaker

Vaishnav K

11+ years of experience in SCCM, Device Management, and Automation Solutions. I writes and imparts my knowledge about Microsoft Intune, Azure, PowerShell scripting and automation via HTMD Community

https://www.linkedin.com/in/vaishnav-k-957b0589/

https://x.com/vaishnavk93

Endpoint Privilege Management Policies & Concepts in Microsoft Intune

Agenda

- What is Endpoint Privilege Management (EPM)
- Prerequisites and Requirements for Endpoint Privilege Management
- Elevation Settings Policy & Elevation Rule Policies
- What is Support Approved Elevation Policy
- Create, Deploy & Monitor Support Approved Elevation
- End User Experience – Support Approved Elevation
- Q & A

What is Endpoint Privilege Management (EPM)

- With Microsoft Intune **Endpoint Privilege Management (EPM)** your organization's users can run as a standard user (without administrator rights) and complete tasks that require elevated privileges. Tasks that commonly require administrative privileges are application installs (like Microsoft 365 Applications), updating device drivers, and running certain Windows diagnostics.

- Endpoint Privilege Management supports your **Zero Trust** journey by helping your organization achieve a broad user base running with least privilege, while allowing users to still run tasks allowed by your organization to remain productive.

- The following slides discuss requirements to use EPM, provide a functional overview of how this capability works, and introduce important concepts for EPM.

- Applies to:
- **Windows 10**
- **Windows 11**

Prerequisites and Requirements for Endpoint Privilege Management

- Endpoint Privilege Management requires an additional license beyond the Microsoft Intune Plan 1 license. You can choose between a stand-alone license that adds only **EPM**, or license EPM as part of the **Microsoft Intune Suite**

- Microsoft **Entra joined** or Microsoft **Entra hybrid joined**
- **Microsoft Intune** Enrolled or **Microsoft Configuration Manager** co-managed devices (no workload requirements)
- Clear line of sight (without SSL-Inspection) to the required endpoints

Supported Operating Systems
Windows 11, version 24H2
Windows 11, version 23H2 (22631.2506 or later) with KB5031455
Windows 11, version 22H2 (22621.2215 or later) with KB5029351
Windows 11, version 21H2 (22000.2713 or later) with KB5034121
Windows 10, version 22H2 (19045.3393 or later) with KB5030211
Windows 10, version 21H2 (19044.3393 or later) with KB5030211

Points to Note

- Elevation settings policy will show as not applicable for devices that don't run a supported operating system version.

- **Windows 365 (CloudPC)** is supported using a supported operating system version

- **Workplace-join devices** are not supported by Endpoint Privilege Management

- **Azure Virtual Desktop** is not supported by Endpoint Privilege Management

- Government cloud support

a) U.S. Government Community Cloud (GCC) High

b) U.S. Department of Defense (DoD)

- RBAC Roles Supported :
- **Endpoint Privilege Manager, Endpoint Privilege Reader, Endpoint Security Manager, Read Only Operator**

Elevation Settings Policy & Elevation Rule Policies

Before you can use Endpoint Privilege Management policies, you must license EPM in your tenant as an **Intune add-on**

Elevation Settings Policy

An elevation settings policy activates **EPM on the client device**. This policy also allows you to configure settings that are specific to the client but aren't necessarily related to the elevation of individual applications or tasks.

Elevation Rule Policies

An elevation rule policy links an application or task to an elevation action. Use this policy to configure the elevation behavior for applications your organization allows when the applications run on the device.

What is Support Approved Elevations

- Support approved elevations allow you to require approval before an elevation being allowed. You can use the support approved functionality as part of an **elevation rule, or as default client behavior**. Requests that are submitted require Intune administrators to approve the request on a case-by-case basis.

- When a user tries to run a file in an elevated context, and that file is managed by the support approved file elevation type, Intune shows a prompt to the user to submit an elevation request. The elevation request is then sent to Intune for review by an **Intune admin**. When an admin approves the elevation request, the user on the device is notified, and the file can then be run in the elevated context. To approve requests, the Intune admin's account must have extra permissions that are specific to the review and approval task.

Elevation Request Details

- **General details**:

a) File - The name of the file that was requested for elevation.

b) Publisher - The name of the publisher that signed the file that was requested for elevation. The name of the publisher is a link that retrieves the certificate chain for the file for download

c) Device - The device where the elevation was requested from. The device name is a link that opens the device object in the admin center.

d) Intune compliant - The Intune compliance state of the device

- **Request details:**

a) Status - Status of the request. Requests start as *Pending* and can be either *approved* or *denied* by an administrator.

b) By - The account of the administrator who *approved* or *denied* the request.

c) Last modified - The last time the request entry was modified.

d) User's justification - The justification provided by the user for the elevation request.

e) Approval expiration - The time that the approval expires. Until this expiry time is reached, elevation of the approved file is allowed.

f) Admin's reason - Justification provided by the admin when an *approval* or *denial* is completed

- **File information -** Specifics of the metadata for the file that was requested for approval.

File path, Hash Value , File Version, File Description, Product name, Internal name

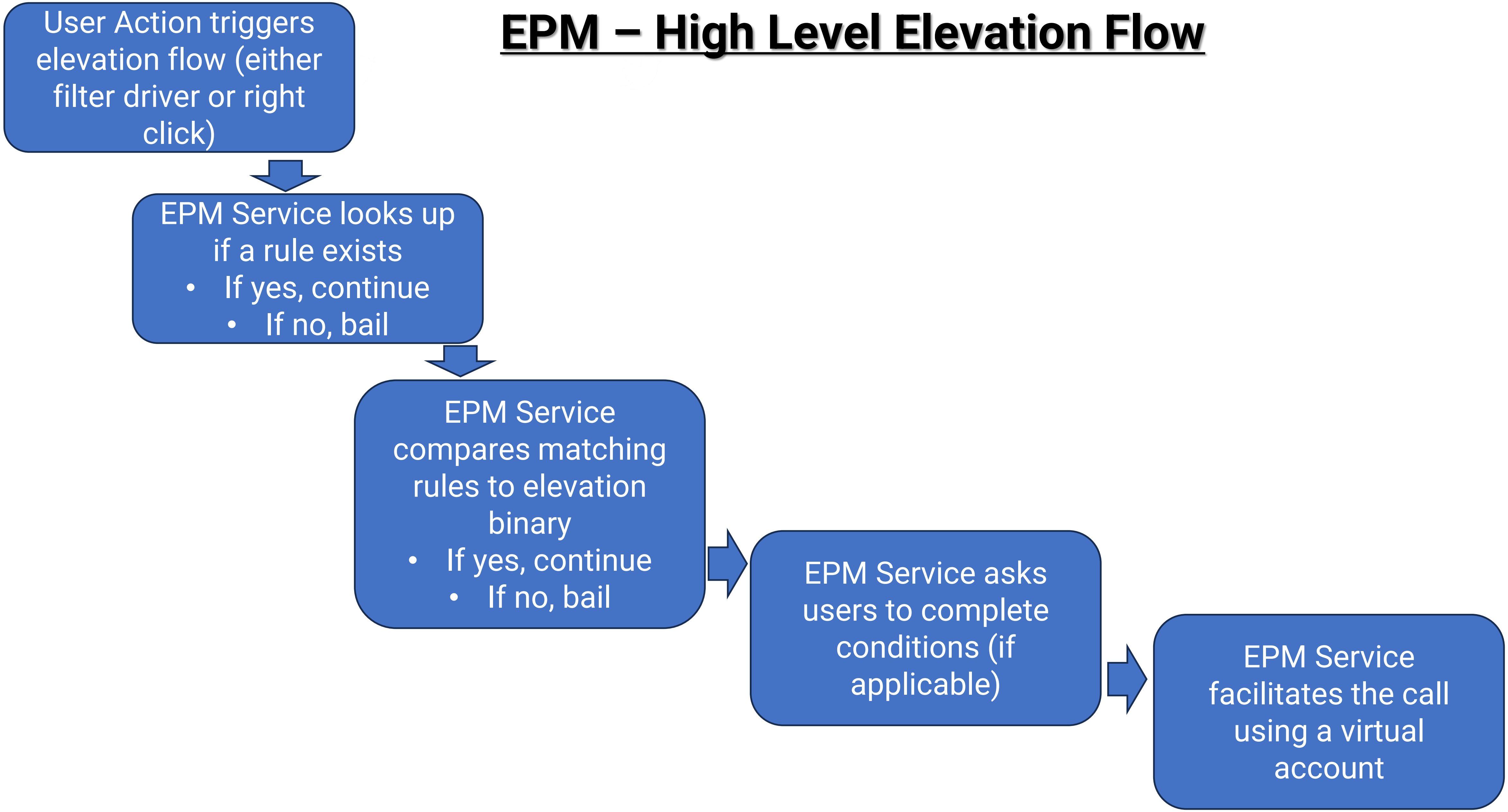
Here are some other Default Elevation Response Options

- **Deny all requests**: EPM will block the elevation of files and show a pop-up window to the user.
- **Require support approval**: EPM will prompt the user to submit a support approved request.
- **Require user confirmation**: EPM will prompt the user to confirm their intent to run the file.

a) ***Business justification***: EPM will require the user to enter a justification for running the file.

b) ***Windows authentication***: EPM will require the user to authenticate using their organization credentials

EPM – High Level Elevation Flow



User Action triggers elevation flow (either filter driver or right click)

EPM Service looks up if a rule exists
- If yes, continue
- If no, bail

EPM Service compares matching rules to elevation binary
- If yes, continue
- If no, bail

EPM Service asks users to complete conditions (if applicable)

EPM Service facilitates the call using a virtual account

DEMO TIME

Thank You! ☺