From Least Privilege to Intelligent Approvals: Deep Dive into EPM, MAA and Admin Tasks

Per Larsen

Lavanya Lakshman

Sponsors

onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

Rimo3

robopack

numecent

Microsoft

Per Larsen
Denmark, Former Microsoft MVP

Role
Senior Product Manager in Intune

Focus
Intune Suite · Security Copilot in Intune – Cloud Native and Windows security

Blog, Hobbies and more
https://Osddeployment.tech
Collecting LEGO – Tech guy
Author of two books on Intune

Lavanya Lakshman

Principal Product Manager

Focus
Intune · AI· Endpoint Management & Security

Blog, Hobbies and more
Pup Training, Half Marathons, Gardening

Agenda

- Multi admin approval
- Admin Task
- EndPoint Privileged Management

Why This Session Matters

- A single compromised admin account can wipe devices, push malicious scripts, or silently alter security policies at scale
- Protecting your environment requires a layered approach: least-privilege access, approval governance, and intelligent elevation controls
- **What you'll take away:**
  - MAA — add approval gates to high-impact changes
  - Admin Tasks — one view for all approvals and requests
  - EPM — remove local admin rights without disrupting users

Multi Admin Approval

Why MAA?

- A single compromised or mistaken admin can push risky policy to every managed endpoint
- Traditional RBAC gates *who* can act, not *whether* an action should happen
- MAA adds a second pair of eyes on the changes that matter most
- Aligns with Zero Trust: "assume breach" applies to admin accounts too

How it works?

- Admin A creates or edits a protected resource → change is held as a **pending request**
- Admin A adds business justification
- Admin B (from the approver group) reviews the diff and justification
- **Approve** → change goes live | **Reject** → change is discarded with reason
- Requests expire after a configurable window to prevent stale approvals

Resource types you can protect

- App deployments and assignments
- Scripts (PowerShell)
- **Endpoint Privilege Management** rules and policies

Configure it in 4 steps

- Intune admin center → **Tenant administration** → **Multi Admin Approval**
- **Create access policy** → pick the resource type
- Assign an **approver Entra ID group** (must differ from requestors)
- Save → protection is active immediately, no tenant restart

MAA Is Critical — But Not the Full Solution

Limitations of MAA

MAA does not replace strong identity controls or reduce excessive permissions, and can be bypassed if multiple identities are compromised.

Integrated Security Strategy

Effective security combines identity protection, least-privilege RBAC, and MAA to create a layered defense against attacks.

Operationalizing MAA Governance

Define approver groups, manage response expectations, and regularly review logs to maintain robust MAA governance.

Securing Microsoft Intune: Beyond the Basics

MODERN ENDPOINT MANAGEMENT SUMMIT 2026

Least-Privilege Administration

Implement Role-Based Access Control (RBAC) to assign only necessary permissions based on real admin job functions.

Phishing-Resistant Authentication

Use phishing-resistant MFA and Conditional Access to protect privileged identities from compromise.

Multi-Admin Approval (MAA)

Require a second admin's approval for sensitive actions to add oversight and reduce risk of disruption.

Admin Task

Admin Tasks at a Glance

- A single, unified view for all admin tasks — including MAA approvals, EPM elevation requests, and Defender security tasks
- Sort and filter to quickly prioritize what needs your attention first
- Review task details and take action directly from the task list
- No more switching between multiple consoles to manage approvals and requests

The problem it solves

- Standard users hit elevation walls dozens of times a week
- Current options are bad: grant full local admin, or flood the helpdesk
- Admin Tasks threads the needle — users get elevation for *specific, known tasks*, nothing more
- Reduces helpdesk tickets, improves user experience, maintains least-privilege posture

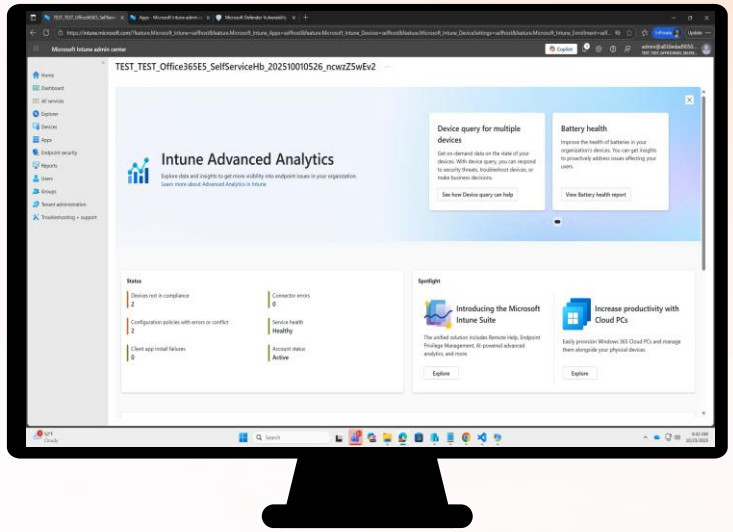
How Admin Tasks Work

- Tasks sync in real time — changes appear within seconds, so you always see the latest status
- Take action on tasks (approve, reject, review) directly from the unified list
- Tasks are assigned to security groups, ensuring only authorized admins see relevant work
- Coming soon: individual task assignment with agent-based routing for faster resolution

Admin Tasks + MAA

- Combine **Admin Tasks** with **Multi Admin Approval** for maximum protection
- Creating or modifying an Admin Task triggers MAA → second admin must approve
- Prevents a compromised admin from quietly adding an elevation rule for a malicious binary
- Closes the loop: least-privilege for users *and* least-privilege for admins

Demo MAA + Admin Tasks



Path to least privilege

Endpoint Privilege Management.

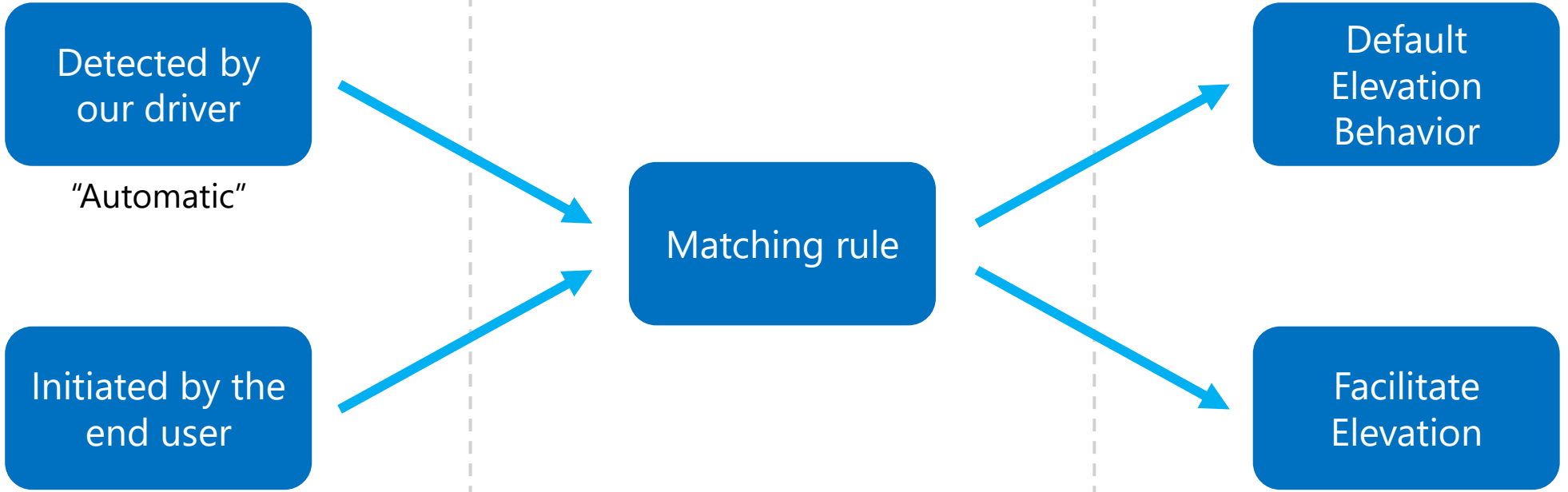
Three main pieces - Policy, Rules, Client-Side Configuration

Available as part of E5, Intune Suite or standalone offering

Seamless elevation management built-in and powered by Intune

Rich set of insights for user experiences requiring elevation

Architecture of an elevation



- Automatic
- User Confirmed
  - ✓ Justification
  - ✓ Authentication
- Support approved
- Elevate as current user
- Deny

Adopting EPM: Working towards standard user

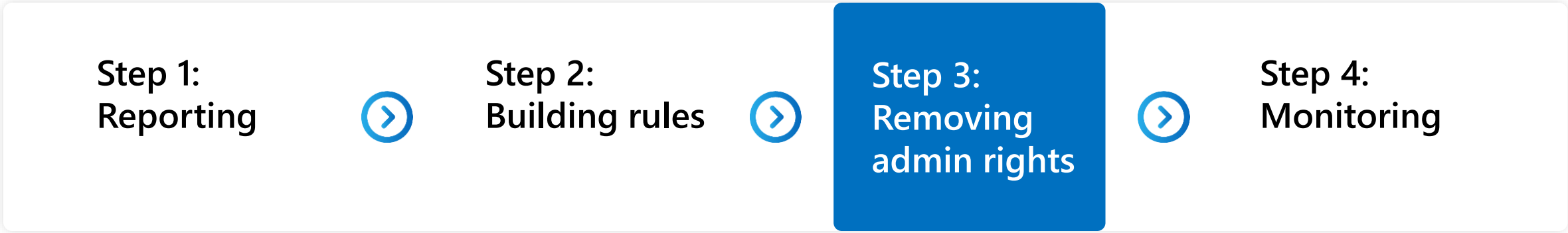
Step 1: Reporting → **Step 2: Building rules** → **Step 3: Removing admin rights** → **Step 4: Monitoring**

- Enable EPM
- No impact to end users
- Elevations detected for admins (including 3rd party software)
- Leverage reporting to start understanding elevation needs

Adopting EPM: Working towards standard user

- Start building EPM rules
- No impact to admin user elevation flow
- Move elevations from unmanaged to managed
- Consider Install vs runtime elevations

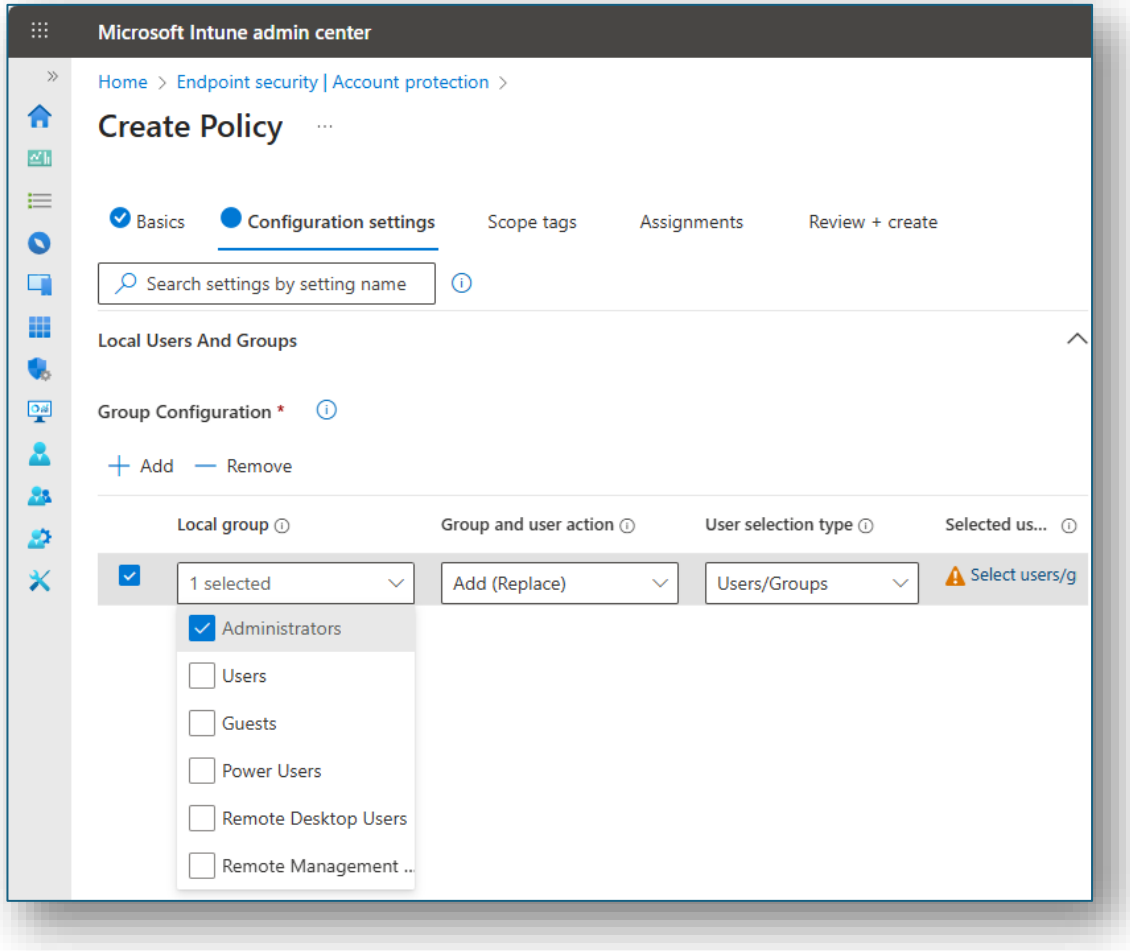
Adopting EPM: Working towards standard user



- Remove admin rights
- Minimize user impact
- Leverage ‘support approved’ as the backup plan
- Consider impact of local users and groups

Removing Admin Rights using Local Users and Groups

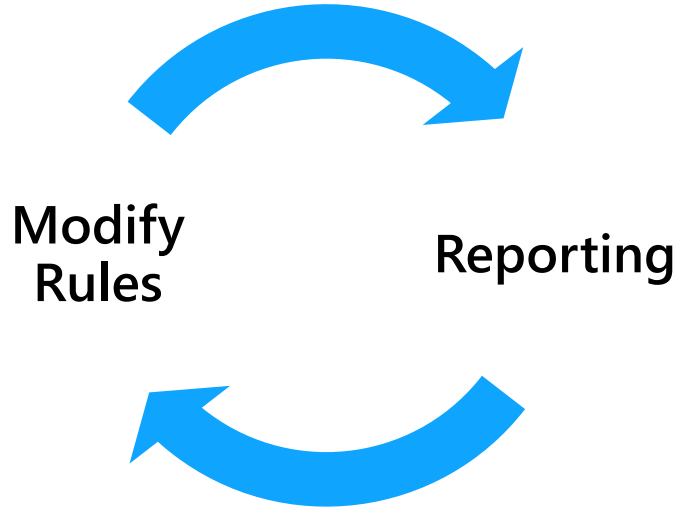
If you want to change the local administrators on a device, you can use the **Local Users and Groups** policy under **Endpoint Security** > **Account Protection** to update or replace the membership.



Adopting EPM: Working towards standard user

Step 1: Reporting → Step 2: Building rules → Step 3: Removing admin rights → **Step 4: Monitoring**

- Iterate and refine
- Monitor rule usage
- Updating certificates
- Identify complex usage scenarios
- Understand ROI



Features released in 2024

Feature	Date	Summary
Assignment filter support	February 2024	EPM rules and elevation policy can be assigned using filters.
Require support approval for elevations	March 2024	An IT Admin can specify that end user can request elevation for binaries and have the request approved by the help desk.
File Hander Support (MSI's and handled file types)	June 2024	EPM can handle elevations for .EXE, .PS1, and .MSI
Intune EPM Support for US Gov Cloud (GCC-H Support)	August 2024	EPM is available in the US Government cloud
Create a rule or reusable setting from an elevation	September 2024	An IT admin can create a new rule based on an elevation request or reporting data. They can also add the rule to an existing policy.

Features released in 2025

Feature	Date	Summary
EPM with Copilot for Security	Feb 2025	Copilot will check the file hash of an elevation against Microsoft Defender Threat Intelligence and provide any indicators of potential compromise.
Arm64 support	March 2025	EPM will support running on Windows devices with Arm64 processors.
Argument Support	April 2025	An IT admin can granularly set the allowed arguments or parameters for elevation.
Deny rules	May 2025	Create rules to deny elevations for actions that match the rule.
Wildcards in rules	July 2025	Instead of creating separate rules for every versioned executable, administrators can use wildcards to match dynamic file names or version patterns.
Operational dashboard	Dec 2025	This is a dashboard to provide insights on the EPM rollout and operations for the IT admin. It is focused on standard user readiness based on managed vs unmanaged elevations as well as support approval stats.

Features released in 2026

Feature	Date	Summary
Support for Single session AVD	Feb 2026	Allow MMP-C onboarding for Single session non-persistent AVD – also brought hardware inventory and MDQ
Support approved notification	Feb 2026	Windows fixed Support approve delays for WNS
Support for scope TAG in EPM reporting	April 2026	An IT admin can granularly see elevation data in reports.
Support approve for non-primary user	April 2026	Allows Support approved request for all Entra users on a device.
Network settings – Private preview	April 2026	Allow creating rules for Network settings an integration it with >Company Portal

Demo EPM

Try This When You Get Back

Three quick wins you can start this week

Audit RBAC Roles

Replace broad admin roles with scoped, built-in Intune roles

Enable MAA

Require approval for device wipe, script deployment, and other high-impact actions

Turn On EPM Reporting

See which apps need elevation before removing local admin rights

Please rate this session on Sched.com

We would love to hear what you liked and how we could improve!

Thanks!


MODERN
ENDPOINT
MANAGEMENT
SUMMIT
2026