Lessons Learned from the Frontlines of Cloud Native Windows and Zero Trust

Per Larsen

Sponsors

onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

Rimo3

robopack

numecent

Microsoft

Per Larsen
Denmark, Former Microsoft MVP

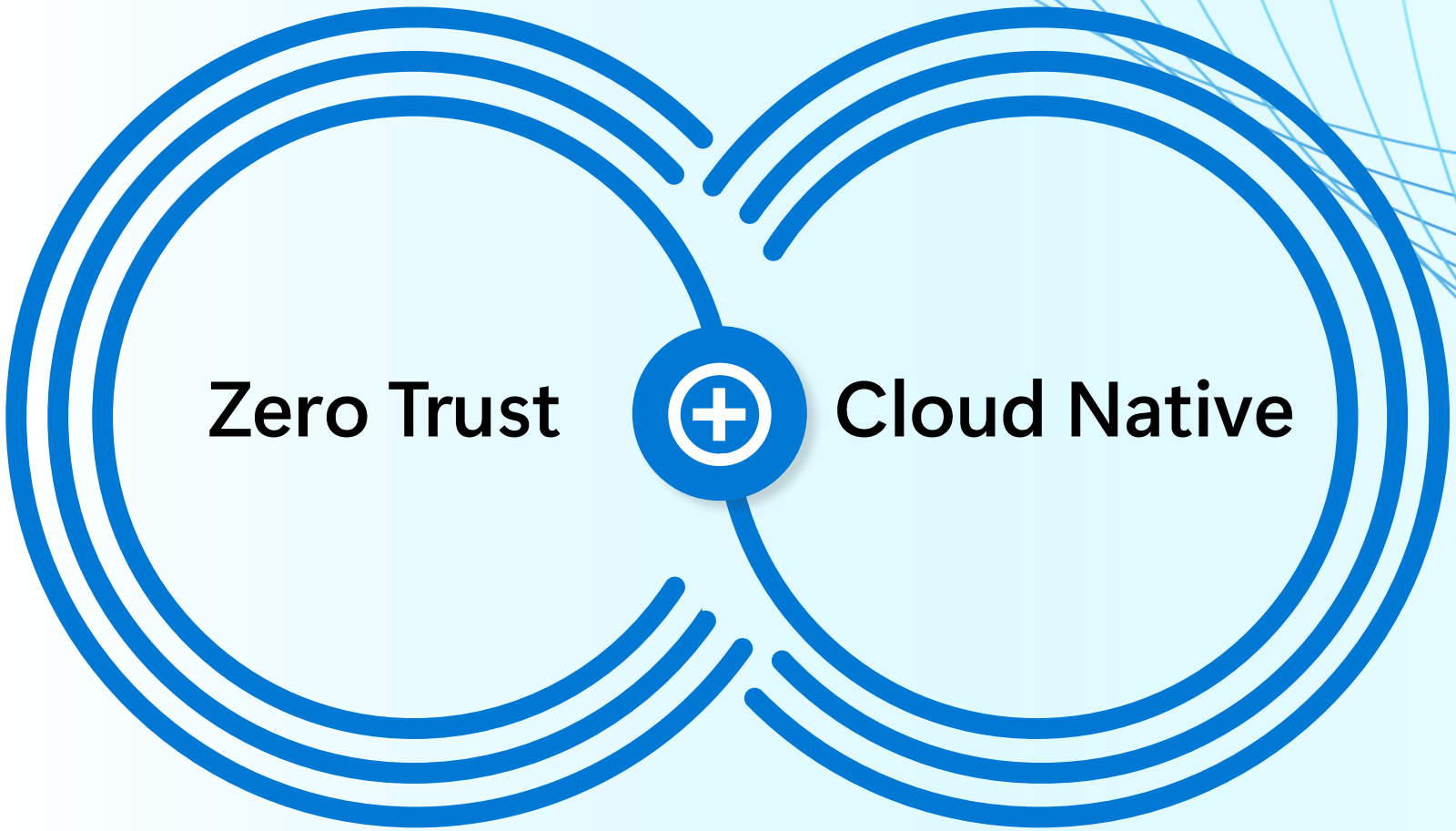
Role
Senior Product Manager in Intune

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

Agenda

- What is Cloud Native
- Windows Autopilot
- Windows Autopilot Device preparation
- Configure Device Compliance and Conditional Access
- Endpoint Privileged Management



Verify explicitly | Least privilege access | Assume breach

Zero Trust: Secure End-to-End by Enforcing, Verifying, and Limiting Access

Assume breach

Act as if already compromised, contain damage swiftly.

- Integrate threat detection and response across identity and security operations.
- Focus on rapid remediation of potential compromises.
- Treat every asset and environment as potentially compromised from the start.

Verify explicitly

Never trust by default; validate identity and context continually.

- Require strong authentication, such as MFA and device registration.
- Continuously assess session risk using user role, location, and device status.
- Apply adaptive policies that respond to changing threat levels in real time.

Use least privilege access

Grant minimal rights needed; review and adjust permissions often.

- Reduce privilege exposure with Just In Time (JIT) access
- Regularly remove unnecessary permissions based on role changes or inactivity.
- Monitor and govern all access throughout the lifecycle, adjusting policies needed.

Zero Trust secures every layer by assuming compromise and allowing only essential access.

Microsoft is actively working with NIST, The Open Group, CISA, and many others across industry to harmonize definitions, model, and architectures for Zero Trust

What is cloud-native endpoint management?

Microsoft Entra ID

Microsoft Intune

Cloud-native Windows and Zero Trust:
Complementary and inseparable

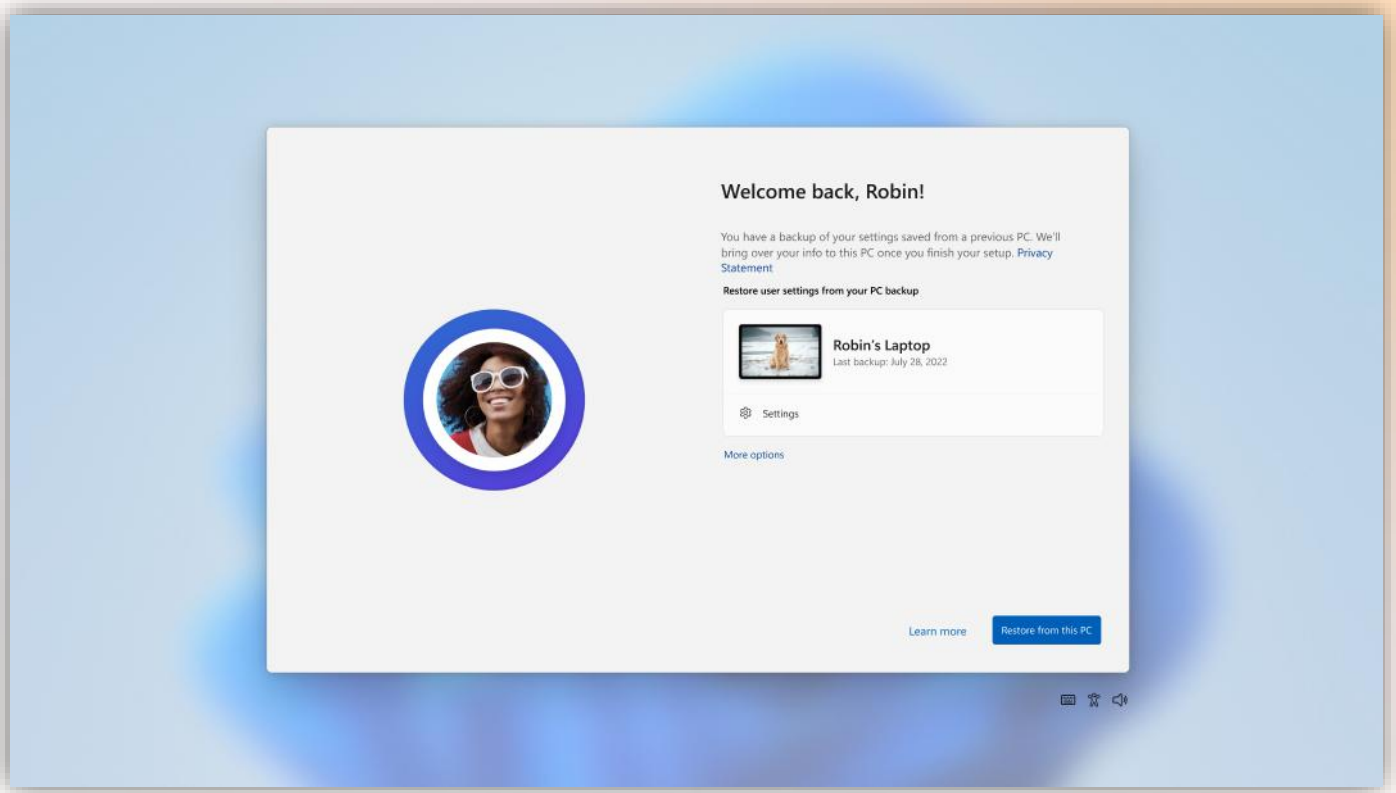
Windows Autopilot

Windows Backup for Organizations

Restores user settings from previous devices

How it works:

1. Configure the **Enable Windows backup** setting in Settings catalog
2. Enable the **Windows Backup and Restore > Show restore page** setting under Enrollment.

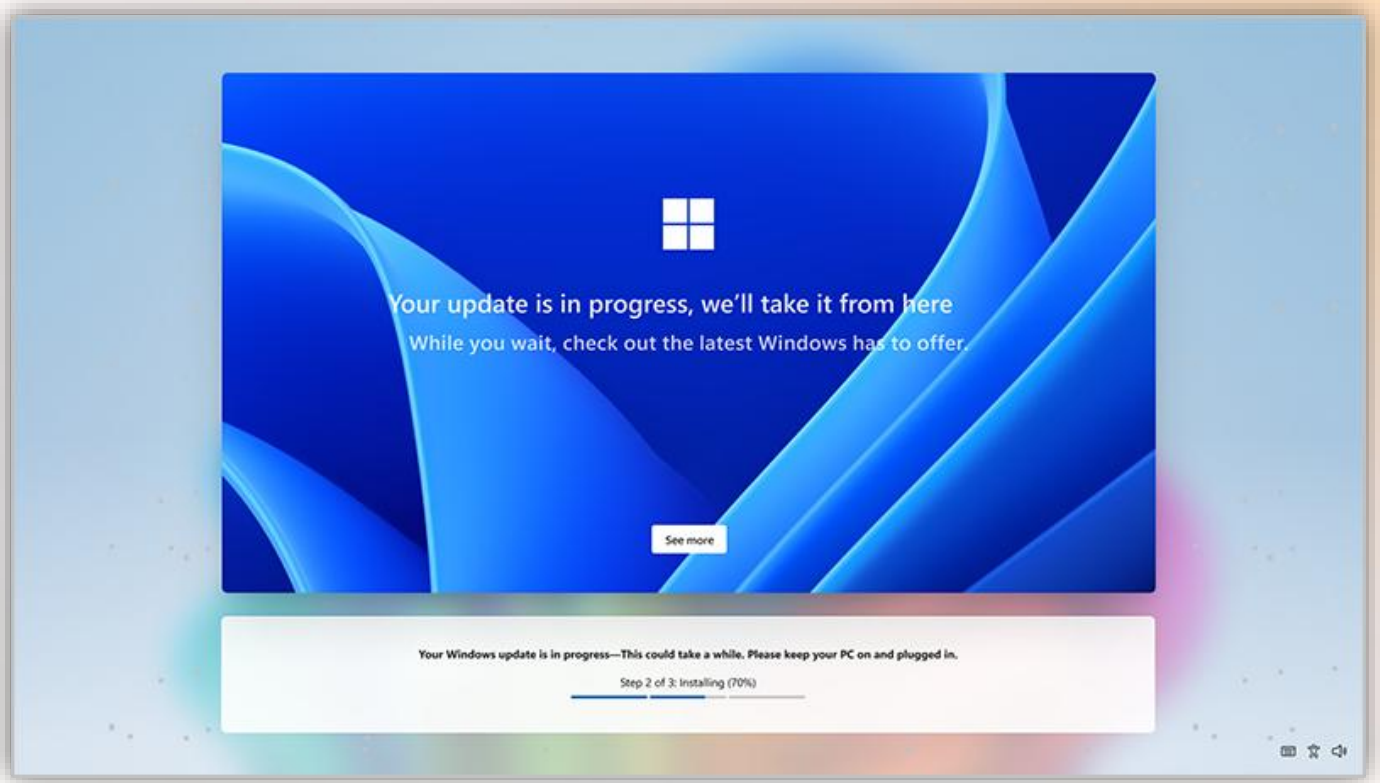


Windows quality updates during OOBE

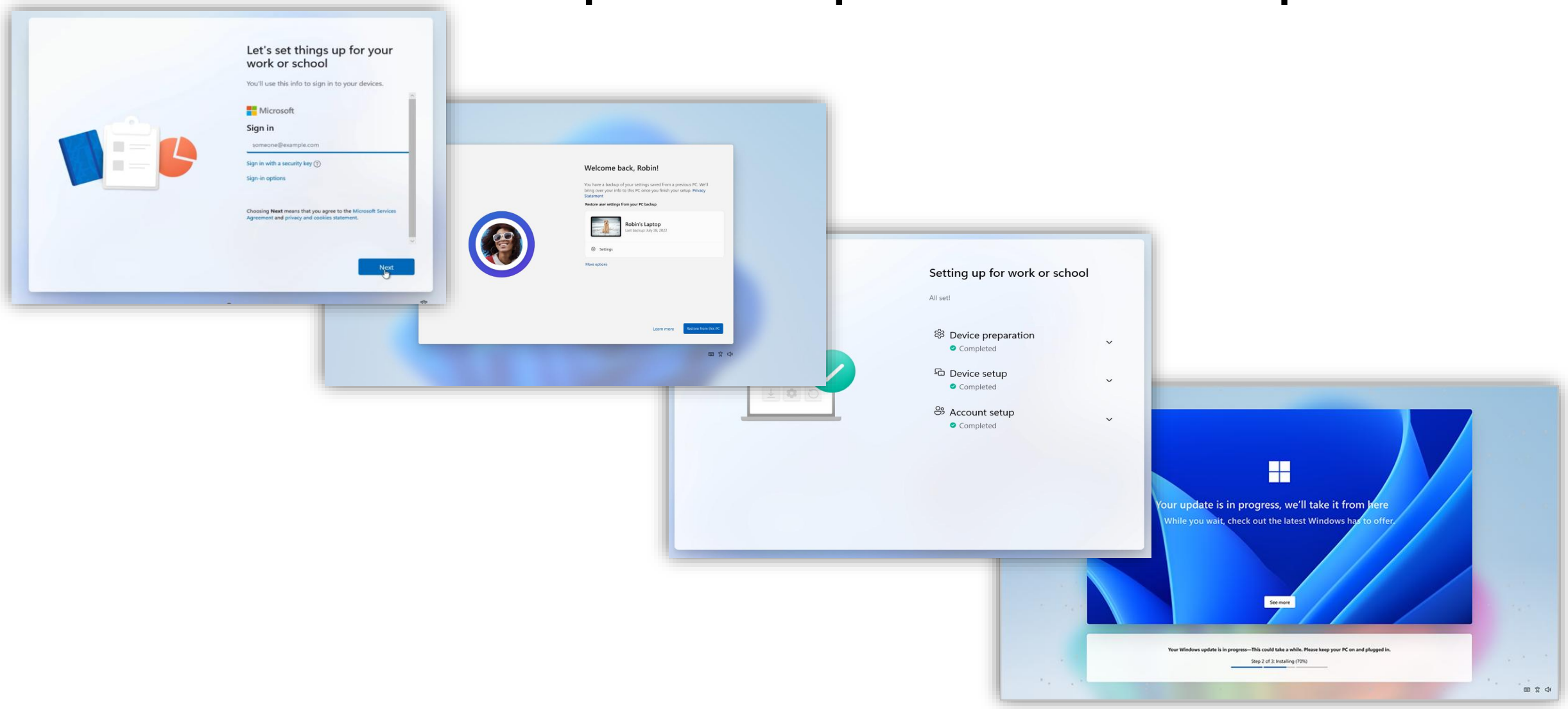
Keep devices secure with latest quality updates during OOBE

How it works:

1. Can be enabled via ESP setting
   - Choose whether to deliver updates in OOBE
   - WUfB/Update ring policies are honored



Windows Backup + Autopilot + OOBE updates



Windows Autopilot device preparation

Windows Autopilot device preparation – what's new?

Simple, Fast, Observable, Reliable.

Enrollment time grouping

Device is added to a security group at enrollment time and configuration is delivered immediately.

Faster and more reliable setup

Granular reporting

Near real-time status of your deployments, including app and scripts details and deployment time.

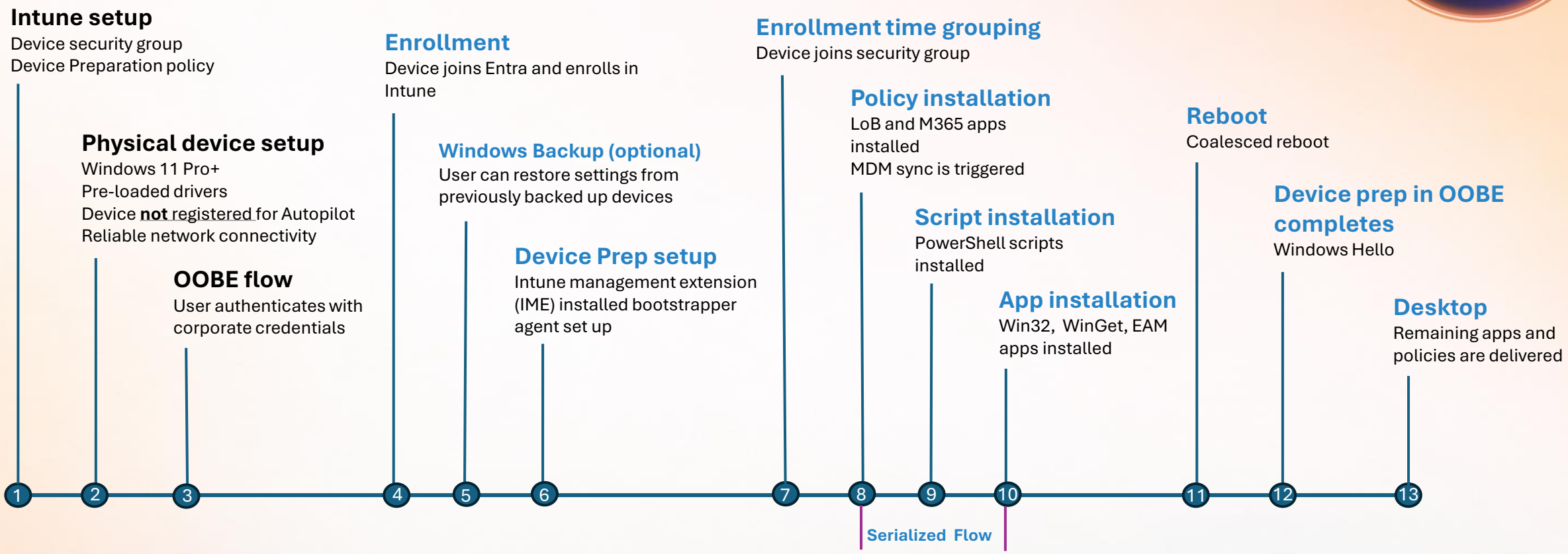
Improved troubleshooting

Better workload coordination

Deliver different types of configuration in specific order to ensure fewer conflicts and consistent experience.

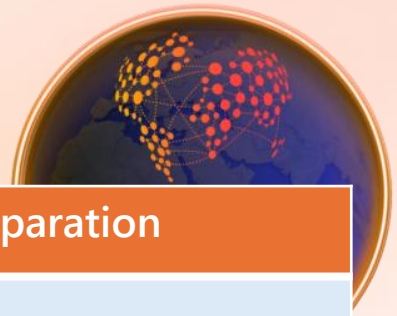
Improved reliability and consistency

OVERVIEW OF DEVICE PREPARATION FLOW



Autopilot device preparation deep dive blog: aka.ms/autopilotdeepdive

Autopilot vs Autopilot device prep



	Windows Autopilot	Windows Autopilot device preparation
What do I get?	• Support for multiple device types • Many options for customization of the provisioning experience	• Available for sovereign clouds • Easier to set up • More consistent provisioning experience • Accurate, detailed, near real-time troubleshooting info
Supported modes	Windows Autopilot scenarios and capabilities | Microsoft Learn	User-driven, Automatic (new!)
Join type	Entra joined or Hybrid Entra joined	Entra joined
Registration required?	Yes	No
What do admins need to configure?	• Autopilot deployment profile • Enrollment status page • (optional) Dynamic Entra ID groups	• Autopilot device preparation policies • Create device security group and add Intune Provisioning Client as owner
Reporting & troubleshooting	Autopilot deployment report: • AP registered devices only • Not real-time	Autopilot device preparation deployment report: • All Autopilot device prep deployments • More data available • More accurate • Near real-time

Which option to choose

- If using **Hybrid Entra join, move to Entra join** for new OOBE deployments: use Autopilot with Entra joined devices.

- If using user-driven Entra joined flows, start deploying **Autopilot device preparation** today

- If using **pre-provisioning**, or **self-deploying modes, remain on Windows Autopilot** at this time

Windows Autopilot device preparation

Device preparation policy

Device association
(coming soon)

Partner and OEM integrations

What will device association enable?

- Associating devices securely with your tenant to ensure only trusted devices are allowed to enroll
- Device targeting for the device prep policy for users with multiple devices
- Streamlined OOBE flow to hide OOBE pages
- Rename device before enrollment
- Block bypassing Autopilot

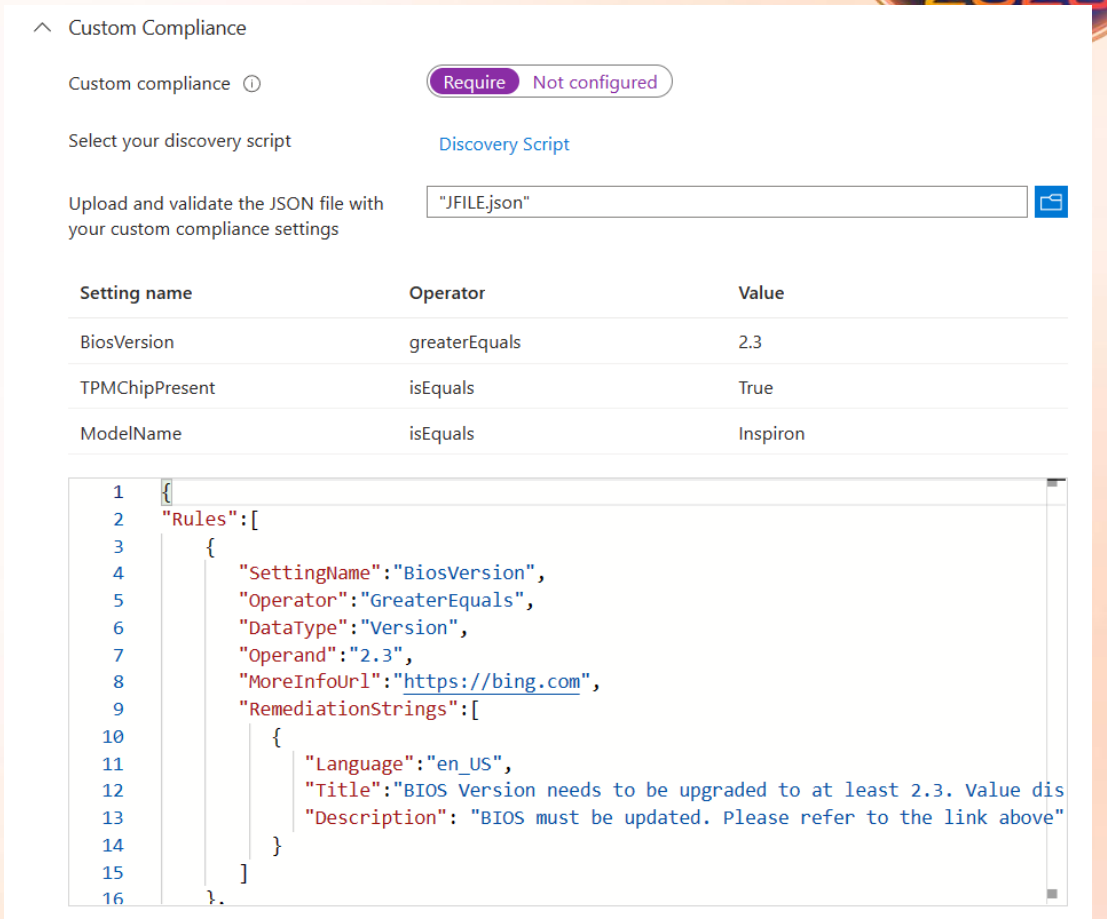
Demo

Configure Device Compliance and Conditional Access

Compliance and Conditional access

Custom Compliance

- With custom compliance settings you can expand on Intune's built-in device compliance options. Custom settings provide flexibility to base compliance on the settings that are available on a device without having to wait for Intune to add those settings.



Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
Learn more

Name *
Windows - CA for M365 Apps

Assignments

Users
Specific users included

Target resources
1 resource included

Network NEW
Not configured

Conditions
2 conditions selected

Access controls

Grant
0 controls selected

Session
0 controls selected

Enable policy
Report-only On Off

Create

Grant

Control access enforcement to block or grant access. Learn more

- Block access
- Grant access

- [ ] Require multifactor authentication
- [ ] Require authentication strength
- [x] Require device to be marked as compliant

Don't lock yourself out! Make sure that your device is compliant. Learn more

- [ ] Require Microsoft Entra hybrid joined device
- [ ] Require approved client app
  See list of approved client apps
- [ ] Require app protection policy
  See list of policy protected client apps
- [ ] Require password change

For multiple controls

- Require all the selected controls
- Require one of the selected controls

Select

Demo

EPM Basics

Path to least privilege and most secure

Local Administrator

- Has persistent full admin rights on Device
- Does not protect from malware or user mistakes
- Admin token unprotected
- No constraint on user action

Local admin with Administrator Protection

- Users can elevate by themself with just in time, non-persistent admin rights
- Uses profile separation to protect the admin user token
- Integration with Windows Hello for secure & convenient elevation
- Protects from malware but does not protect from user mistakes

Standard User with EPM

- Users do not have admin rights
- Can elevate with EPM within the set of rules or request additional rights as needed
- Protects from malware & user mistakes
- Admin protection hooks are leveraged to overcome user dead ends and admin settings (future)

Least privilege with productivity

Elevation 'Actions'

Automatic

User confirmed

Support approved

Deny

Feature Spotlights

Support approval, rule creation, argument controls

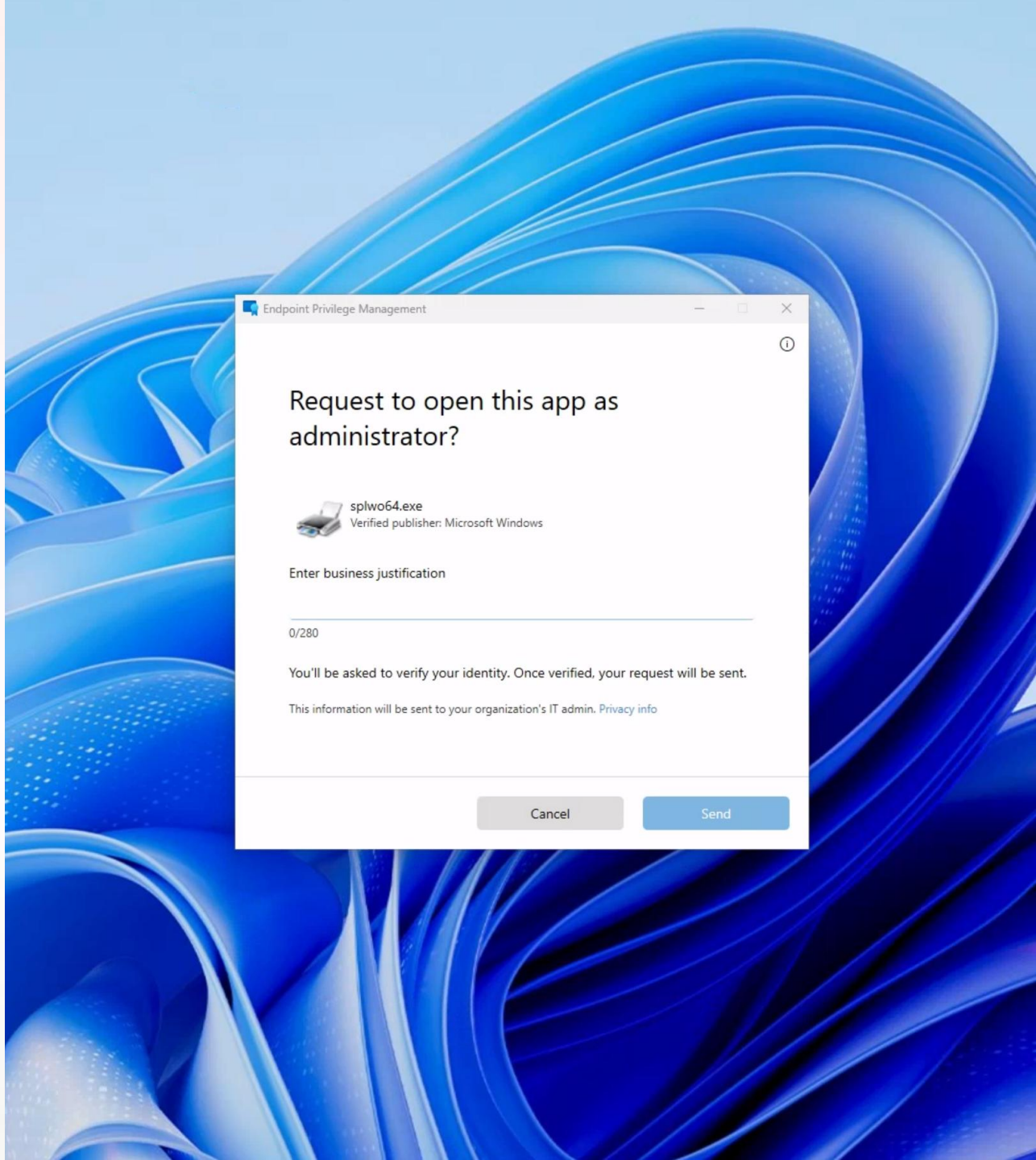
Support approval for elevations

Support approval

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 the **default client behavior**.

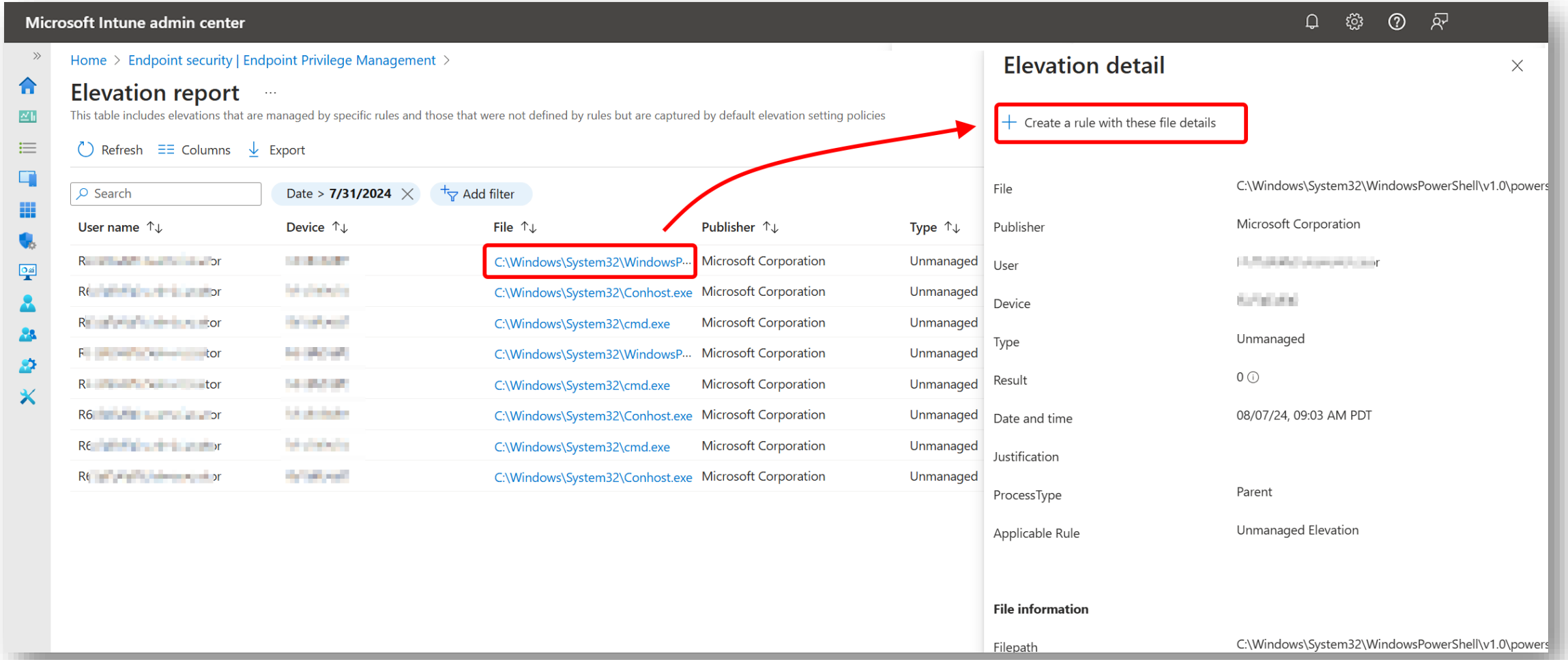
Requests that are submitted require Intune administrators to approve the request on a case-by-case basis.



Create a rule from a report

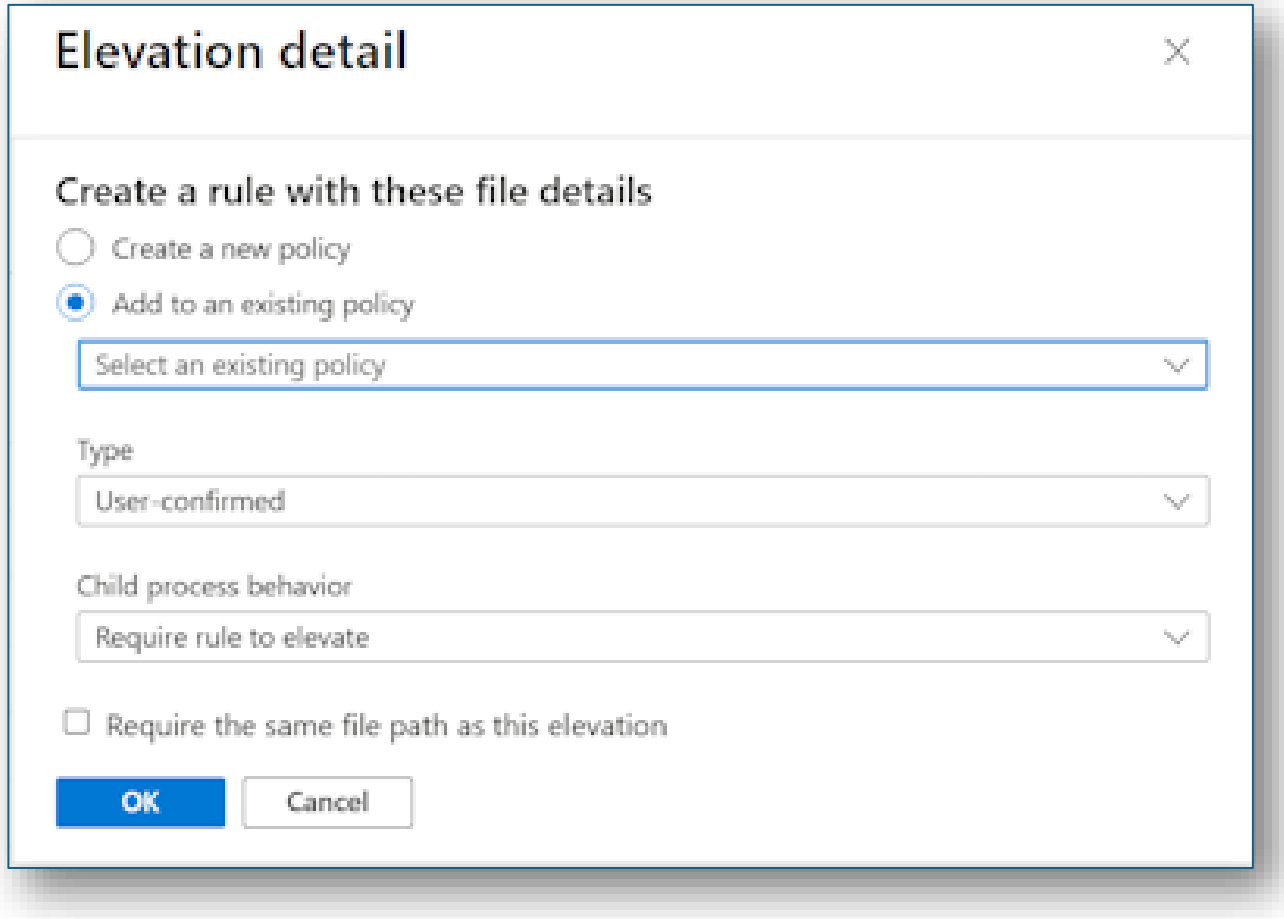
Solution

Instead of just viewing the report details or approving or denying the elevation request, you can now select the option to add this instance to a rule or create a new rule.



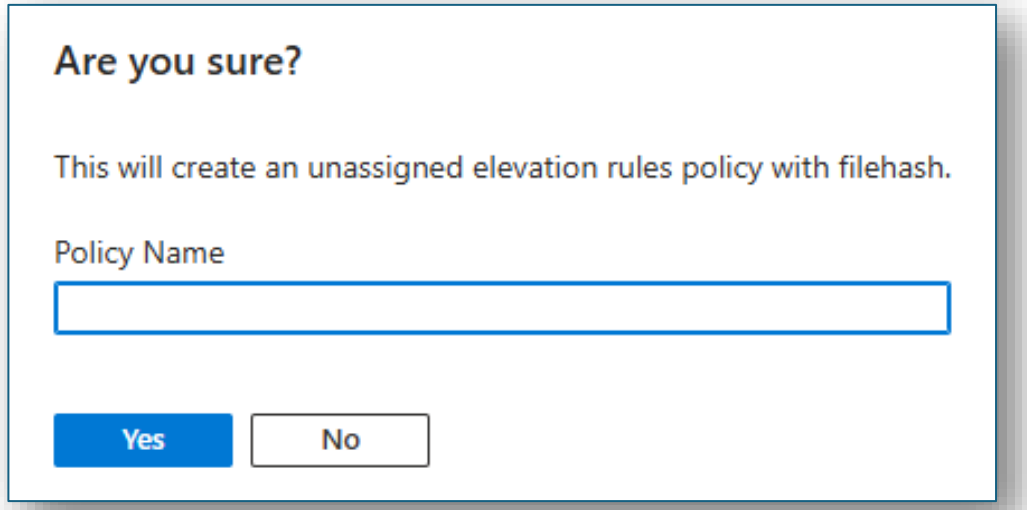
Solution

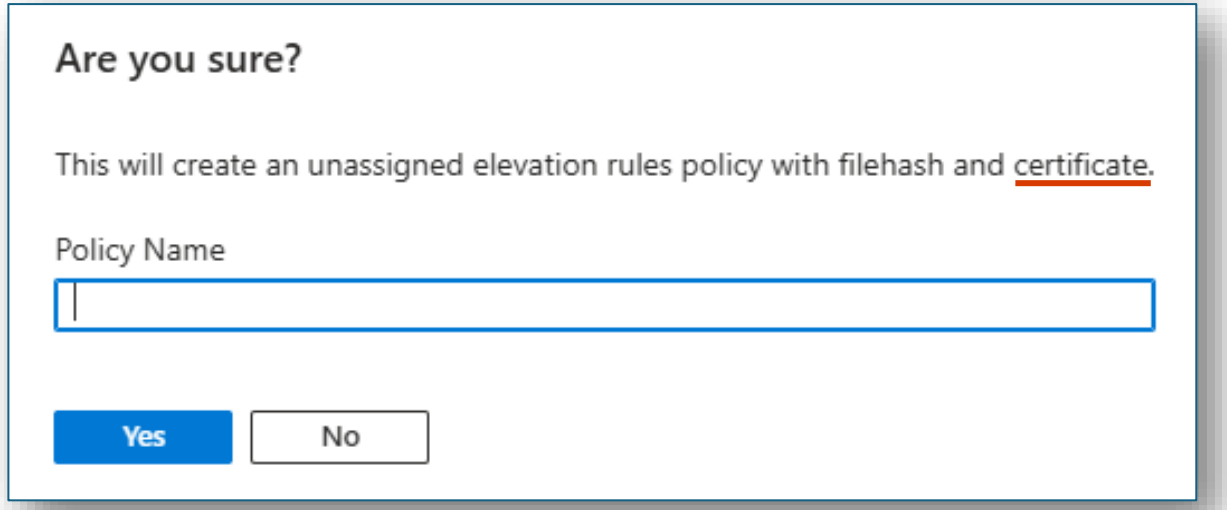
- You can now select the option to add this elevation information to a rule or create a new rule.
- This saves precious time previously spent gathering information from the report and manually entering it into a new rule.
- At creation, you can specify elevation type, required validation, and child process behavior.



Solution

- The new rule will contain all data available from the elevation.
- This includes the file hash and the certificate, if available
- Alternatively, you can add the certificate to a reusable object to be referenced by other rules.





New or existing rule

Existing Rule

- If the you opt to add this metadata to an existing rule, you are asked to select a policy from the dropdown of existing policies
- This policy **will** have assignment data associated with it
- The rule will deploy to machines immediately

New Rule

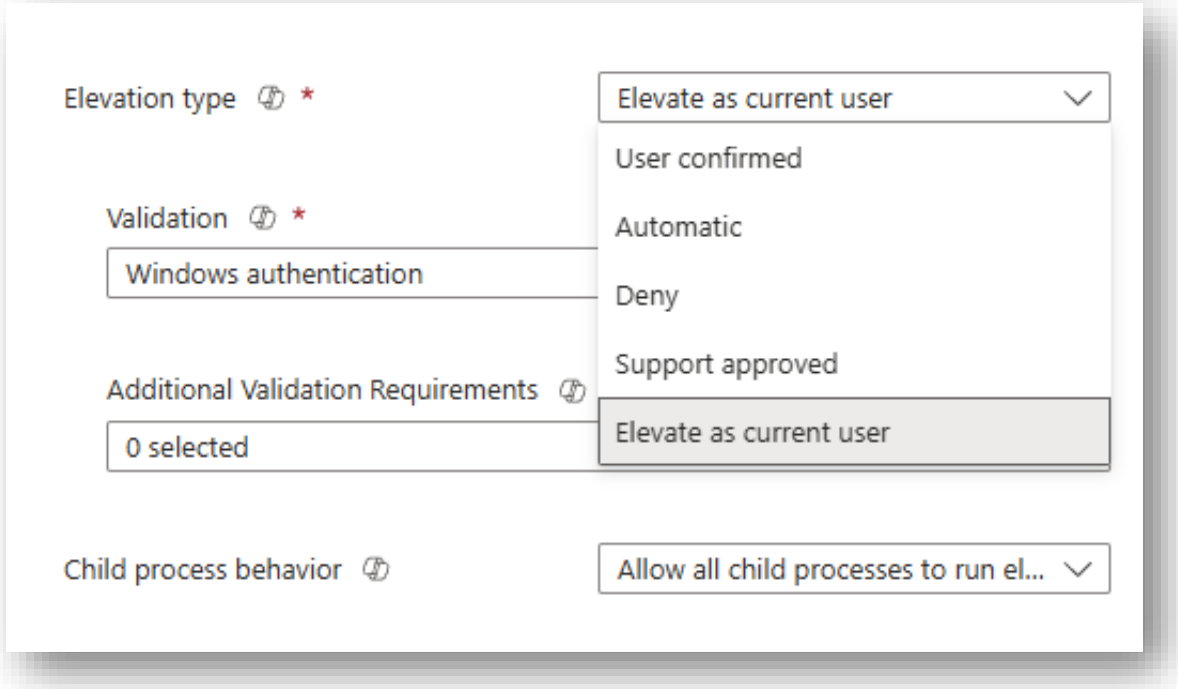
- If you opt to add this metadata to a new rule you are prompted to name the new rule
- This new policy will have no assignment data associated with it
- The policy will not deploy until it is assigned

Elevate as current user

Elevate as current user

When a binary is launched, sometimes the binaries need access to the local user's profile either to run, update files, or authenticate as the current user to active a license or access data.

This is a per rule basis configuration option and not a device wide setting, it will only work together with the Windows authentication option.



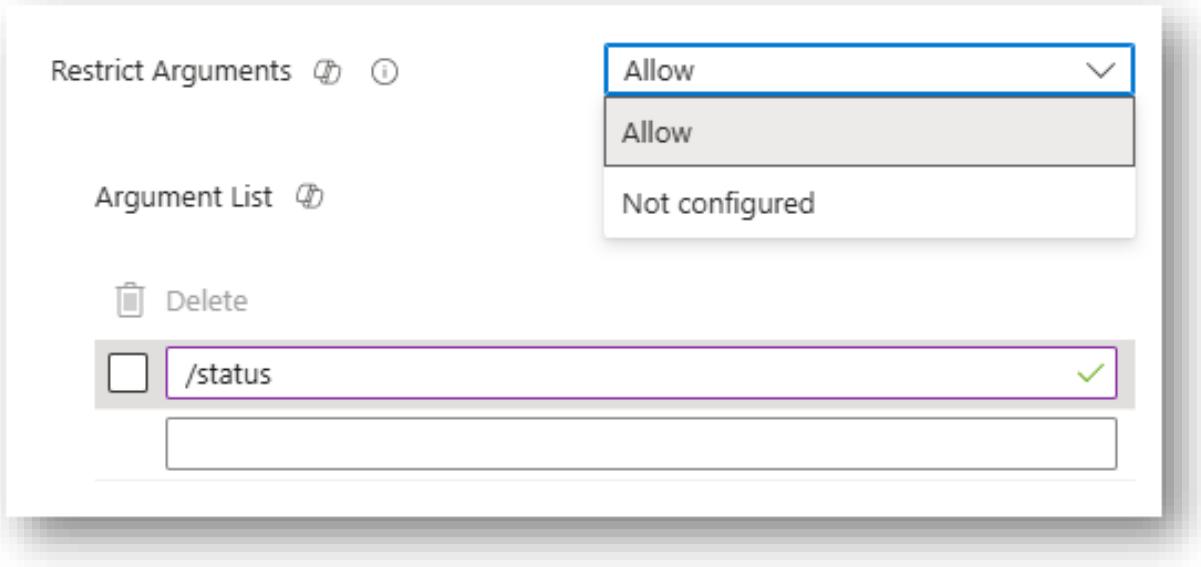
Ideas:

- Allow **devenv.exe** to elevate as current user so the end user are allowed to install and update extensions.
- Validation **Windows authentication** are required.

Argument controls

Argument support

When a binary is launched, EPM can be configured to approve or deny the elevation based on the arguments passed to the binary. This allow administrators to control exactly which arguments are allowed or mandatory.



Ideas:

- Allow **netsh.exe** to elevate only when non-destructive arguments are specified.
- Allow **dsregcmd /status** but not **/leave**

So, what will this feature cover?

- When a binary is launched, EPM approves or denies the elevation based on the arguments passed to the binary
- Allow administrators to control exactly which arguments are allowed to elevate

Ideas:

- Allow **netsh.exe** to elevate only when non-destructive arguments are specified.
- I can allow **dsregcmd /status** but not **/leave**

```
DSREGCMD switches
                    /? : Displays the help message for DSREGCMD
                /status : Displays the device join status
            /status_old : Displays the device join status in old format
                 /join : Schedules and monitors the Autojoin task to Hybrid Join the device
                /leave : Performs Hybrid Unjoin
                /debug : Displays debug messages
            /refreshprt : Refreshes PRT in the CloudAP cache
       /refreshp2pcerts : Refreshes P2P certificates
       /cleanupaccounts : Deletes all WAM accounts
          /listaccounts : Lists all WAM accounts
          /UpdateDevice : Update device attributes to Azure AD
```

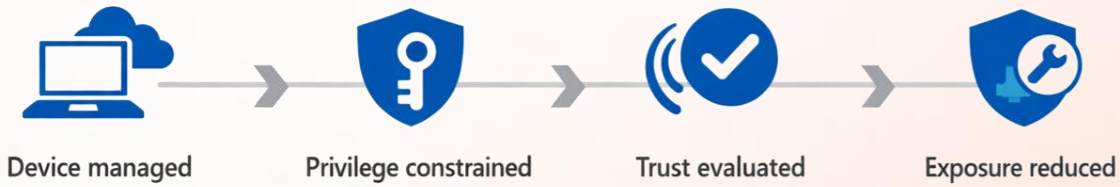
Demo

Putting it all together

Cloud-native Windows + Zero Trust
A system outcome, not a feature choice.

Continuous control with Intune
Devices enrolled, configured, and managed from the cloud.

Security outcomes, not silos
Least privilege enforced, trust verified explicitly, exposure reduced by patch velocity.



Verify explicitly | Least privilege access | Assume breach

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

Sponsors

onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

Rimo3

robopack

numecent

Microsoft

Michael Scott
Microsoft MVP · Endpoint & Security

Role
Manager

Focus
Intune · Windows 365 · Security

Blog, Hobbies and more
Being awesome

Agenda

- My First Point
- My Second Point
- And so on...

Demo

Please rate this session on Sched.com

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

Thanks!