Decoding ME3 and ME5: Intune Suite Capabilities and Copilot Inclusion Explained

Eugenie Burrage, Director of Product Marketing

Lavanya Lakshman, Principal Product Manager

Sponsors

onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

Rimo3

robopack

numecent

Microsoft

Eugenie Burrage

Director – Product Marketing

Intune Business Group - Product Strategy

Microsoft Intune Blog | Microsoft Community Hub

https://www.linkedin.com/in/eugeniedaoust

Music, mountains and the cabin on the lake

Lavanya Lakshman

Principal Product Manager

Focus
Intune · AI· Endpoint Management & Security

Blog, Hobbies and more
Community outreach, mentoring,
Pup Training, Half Marathons, Gardening

Agenda

- In case you missed it: blog
- What’s changing July 1, 2026
- What’s that mean for your Microsoft subscription
- Advanced solutions L300 details

Microsoft 365

Microsoft 365 adds advanced Intune solutions + Security Copilot

Elevated endpoint management that helps support secure AI transformation

How these additions help support a secure AI transformation

- **Unify control and strengthen security across diverse endpoints;** helping to safeguard AI-driven business growth
- **Accelerate issue resolution remotely and securely;** workforce stays focused on AI-enabled innovation
- **Anticipate risks and maintain a resilient security posture;** AI adoption is grounded in Zero Trust principles
- **Empower IT with AI-guided insights and remediation;** uphold reliable operations as AI scales

	Microsoft 365 E3	Microsoft 365 E5*
Advanced Analytics	☑	☑
Remote Help	☑	☑
Intune Plan 2	☑	☑
Enterprise Application Management		☑
Endpoint Privilege Management		☑
Cloud PKI		☑
Security Copilot		☑

*Microsoft 365 E5 includes all Microsoft 365 E3 features

Incremental Intune value for Microsoft 365 E3

Instant end-user support keeps AI-driven workflows running

Remote Help enables live screen viewing and assistance to resolve issues, even when users are off-site.

Proactive IT and SecOps teams act before issues disrupt AI productivity

Advanced Analytics surfaces risky or non-compliant issues earlier, helping teams prevent interruptions.

Enable safe AI access everywhere work happens, even on diverse devices

Intune Plan 2 extends secure management to contractors, frontline, and BYOD.

Incremental Intune value for Microsoft 365 E5

Includes all Microsoft 365 E3 additions: Remote Help, Advanced Analytics, and Intune Plan 2

Strengthen Zero Trust

- Endpoint Privilege Management **enforces least privilege** and **verify explicitly** through policy approvals, continually monitoring compliance.
- Cloud PKI helps organizations **assume breach** and minimizes blast radius using certificates to prevent phishing and lateral movement.

Safeguard AI productivity

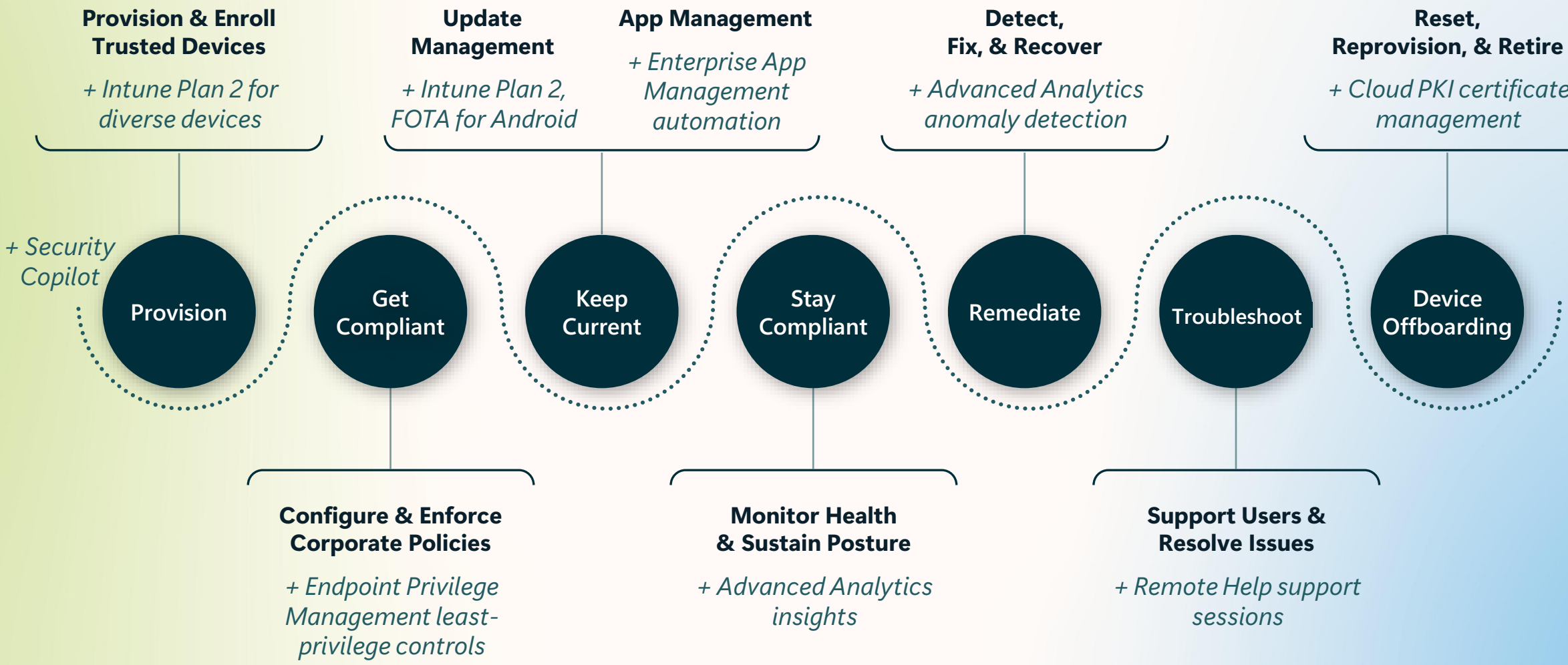
- Intune enables IT to secure employees' AI work by bringing together controls like restricting app elevations to only approved AI apps, enabling app patching and simplifying deployment, and managing device trust through certificates.

Scale operations with AI

- Copilot in Intune **empowers IT teams** to scale operations by provide context-aware troubleshooting.
- Security Copilot agents in Intune **help reduce resolution times** with AI-powered, contextually relevant guidance and analysis.

The foundation AI needs across a device's lifecycle

+ examples where Intune's value lands across the lifecycle



New Intune value in Microsoft 365 E5

Microsoft Intune Remote Help	Secure cloud-based remote support. Helpdesk teams troubleshoot anytime, anywhere.
Microsoft Intune Advanced Analytics	Gain deeper device visibility with endpoint analytics that help you detect and resolve endpoint issues.
Microsoft Tunnel for Mobile Application Management *	Delivers secure per-app VPN connectivity access to company resources without requiring full device enrollment
Specialty device management* Firmware updates*	Provides a range of management, configuration, and protection capabilities for specialized devices, and firmware updates for supported Zebra devices.
Microsoft Intune Endpoint Privilege Management	Help secure privileged access, elevate productivity and drive compliance without granting ongoing admin rights.
Microsoft Intune Enterprise Application Management	Reduce time and effort for IT administrators to package apps and track updates while streamlining fix deployments to keep apps up to date and secure.
Microsoft Cloud PKI	Create multiple certificate authorities and manage certificate lifecycle in the cloud to reduce the cost and complexity tied to on-premise infrastructure.
Security Copilot in Intune	Offer AI and agentic assistance that helps accelerate everyday IT workflows and minimize risk.

*Included in Intune P2

Overview: Microsoft 365 E3 and E5 plan updates with Intune

		FY27 price updates	
	FY26 prices for standalones	Microsoft 365 E3 $39	Microsoft 365 E5 $60
Microsoft 365 E3	EMS E3 $10.64	●	●
	Intune Plan 2 - $4	●	●
	Remote Help - $3.5	●	●
	Advanced Analytics - $5	●	●
Microsoft 365 E5	Enterprise App Mgmt. - $3		●
	Endpoint Privilege Mgmt. - $3		●
	Cloud PKI - $2		●
Security Copilot	Security compute units SCU – consumption	+ SCUs	●

Pricing shown is for illustrative purposes only and subject to change without notice. Taxes and regional variations may apply. Please confirm current pricing with your Microsoft representative.

Inventory of solutions

Copilot in Intune

AI assistance for endpoint management excellence.

Accelerate everyday tasks

Use natural language to bring apps, devices, policies, and user data together in one place, enabling you to act fast on insights, ease troubleshooting and reduce operational disruptions.

Level up and simplify

Empower administrators of all experience levels with assistance and guidance to perform advanced tasks, increasing agility and streamlining workflows.

Minimize risk at scale

Automate discovery and prioritization of vulnerabilities. Autonomous agents assess CVE risks and provide recommended remediation steps.

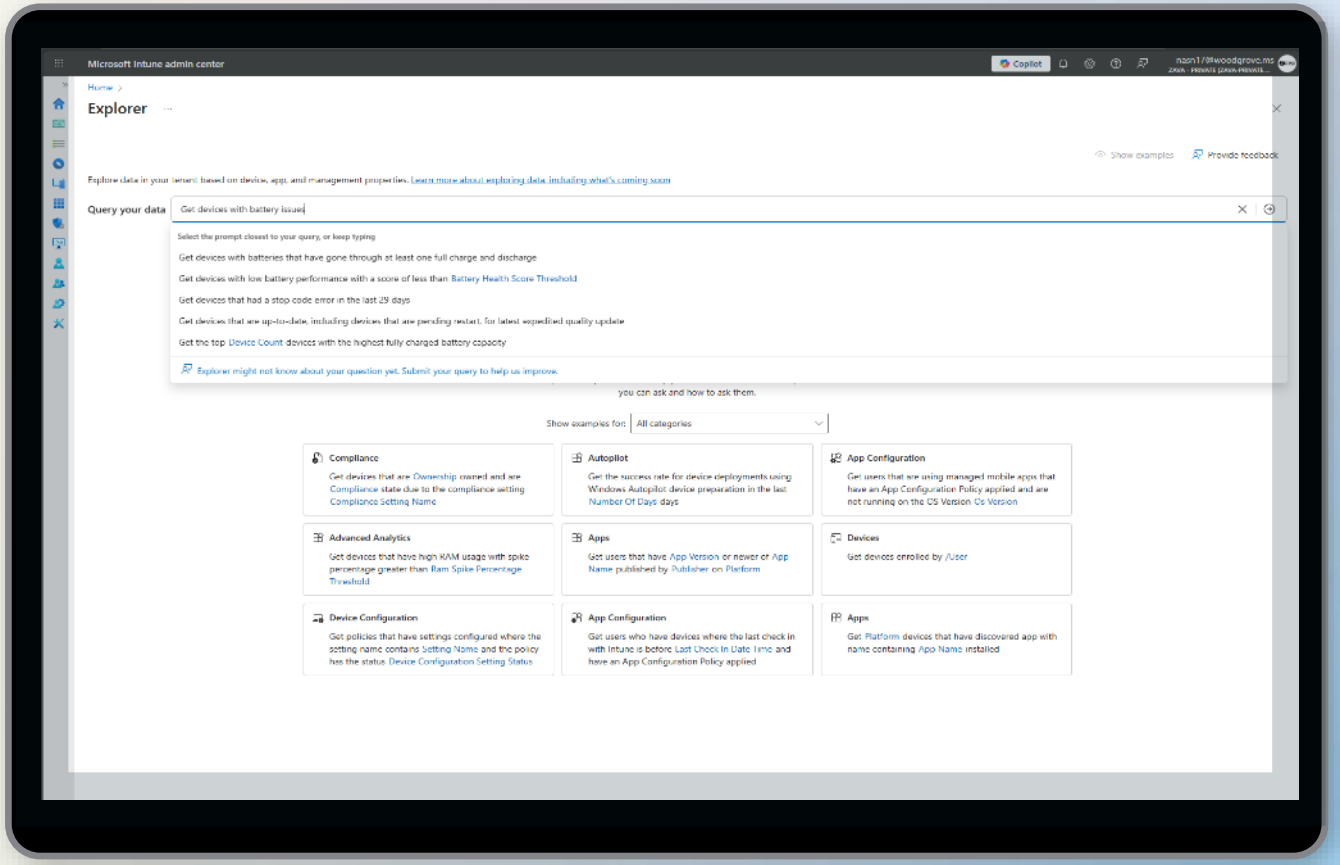
Explore Intune data with Copilot

One central place for assistive AI assistance for investigation, analysis, and getting endpoint management jobs done

Ask Copilot using natural language to find and refine data across platforms and workloads.

Analyze data across devices, apps, users, policies and compliance for physical and virtual devices in one place.

Act on the results to complete management tasks in Intune.



Contextual | Ambient | Always learning

Supports: Windows | iOS | Android | macOS

Intune Advanced Analytics

Empower IT admins with granular insights to discover unreported issues and proactively improve device performance while enhancing the end-user experience.

How it works

Query the state of a device in near real time to gain critical information

Gain awareness of irregularities in apps and devices

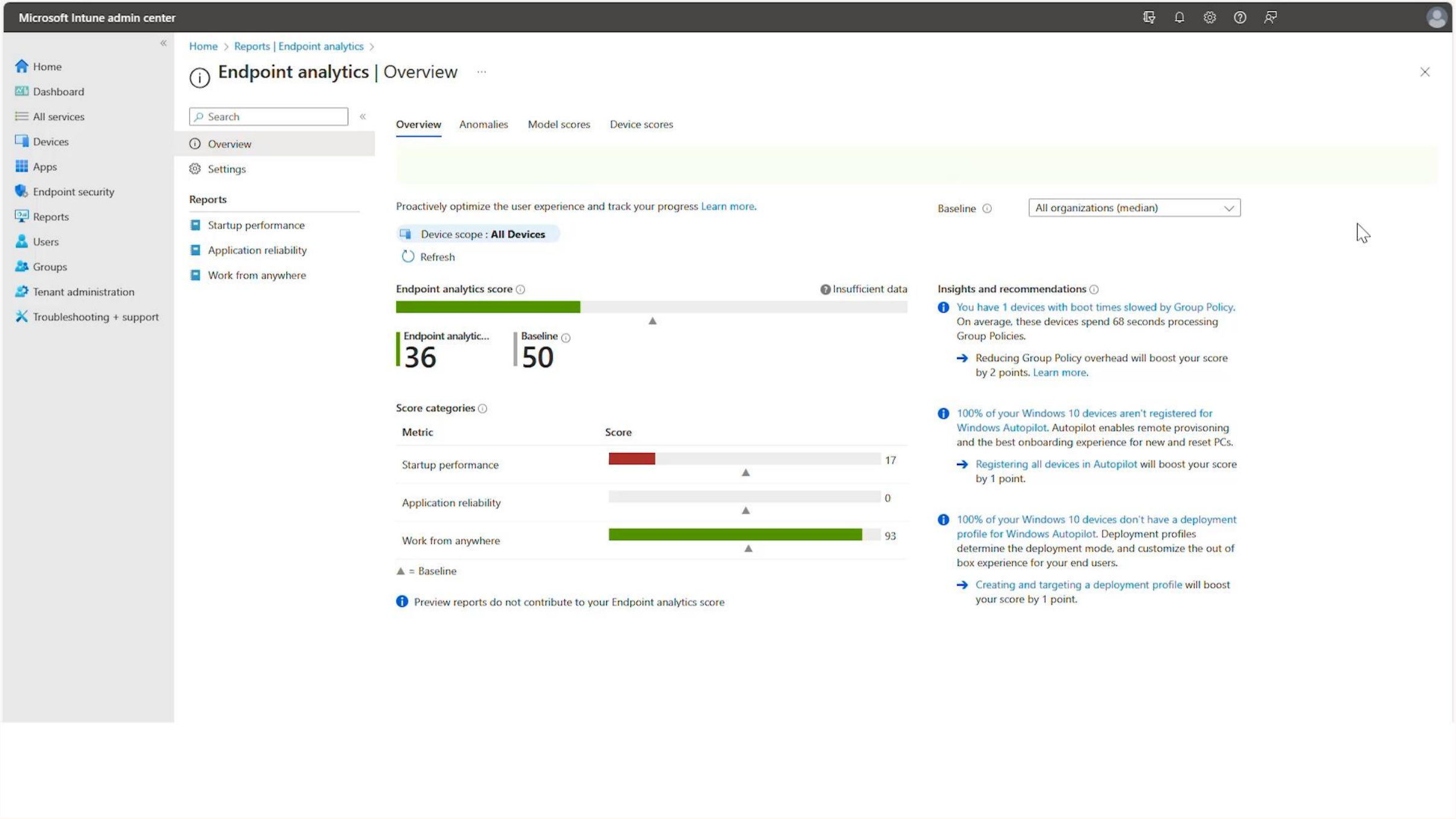
Get insight into device battery health, usage trends, and emerging issues

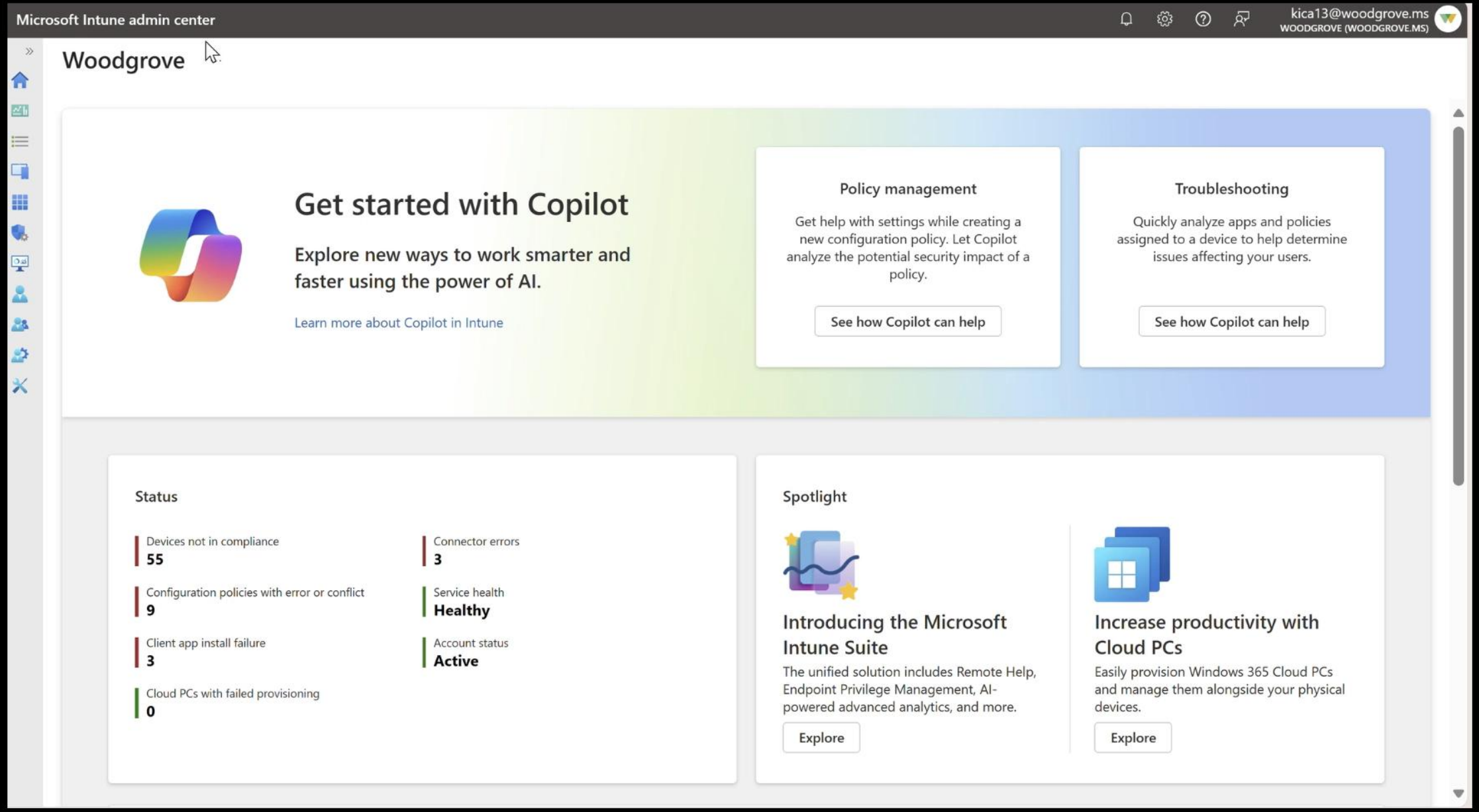
Outcomes

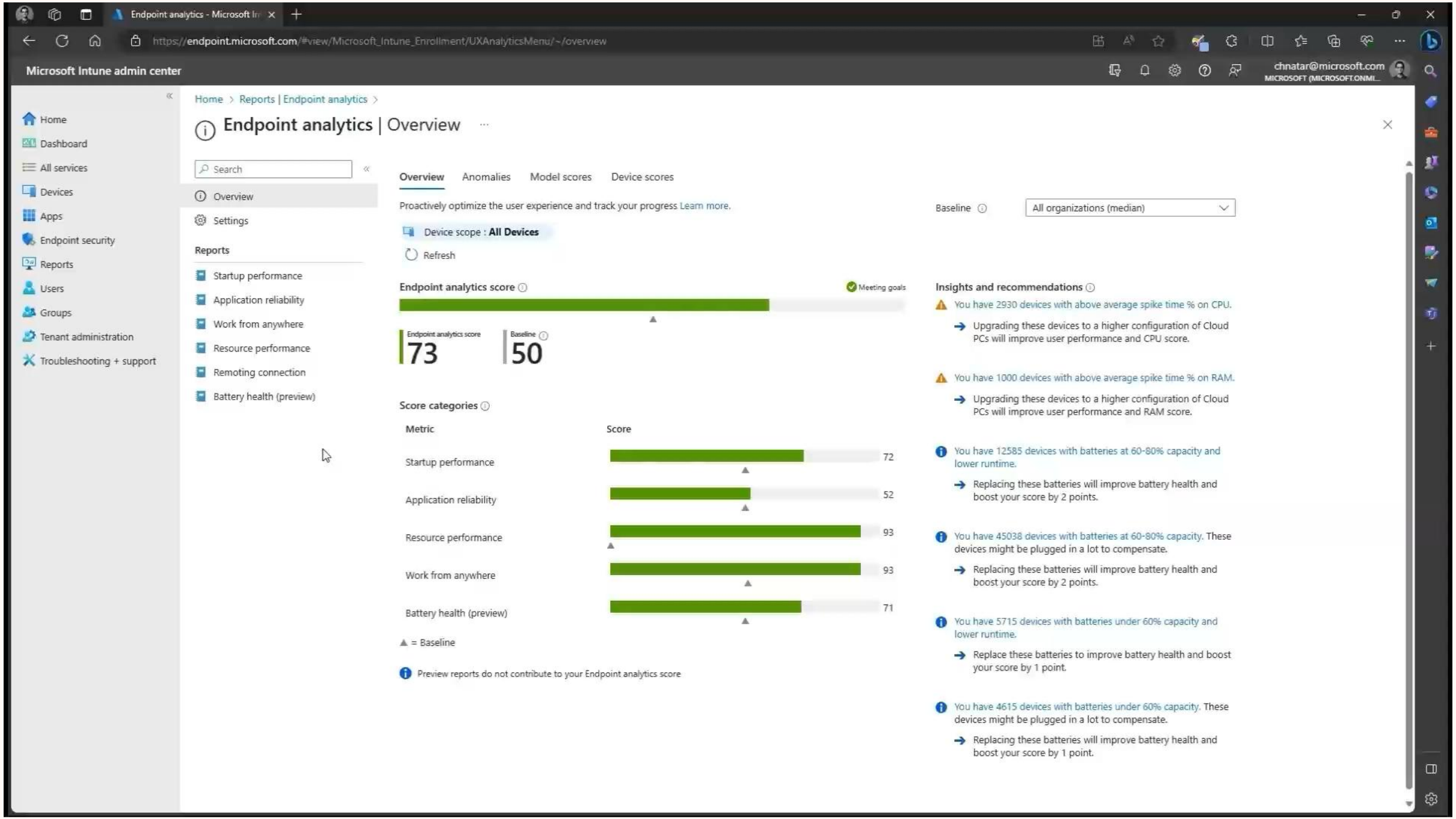
- ✓ **Get fuller visibility** into device state and configuration to enable simple and secure endpoint management
- ✓ Identify and **discover meaningful patterns** and trends using analytics, and machine learning
- ✓ Resolve issues quickly and **reduce downtime** by assessing the state of devices and configurations

Intune Advanced Analytics

Visibility into device health and performance across tenant	**Battery Health** Gain insight into battery health and performance for endpoints across the tenant	**Anomaly Detection** Identify app regression and BSOD related anomalies	**Resource Performance** Get visibility into the performance of processors and RAM in cloud-managed Windows devices
Quickly troubleshoot a single device	**Enhanced Device Timeline** Troubleshoot problematic devices using device historic data	**Device Query – Single device** Gain real time visibility into device data	**Device Action** Remediate and fix device issues by taking immediate action
Assess the scope of issues across multiple endpoints	**Device query – Multiple devices (Windows)** Gain insights into device health and configuration across Windows fleet	**Device query – Multiple devices (Cross Plat)** Identify trends and assess issues across different platforms in one view	


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Reports | Endpoint analytics >
Endpoint analytics | Overview
Search
Overview
Settings
Reports
Startup performance
Application reliability
Work from anywhere
Overview
Anomalies
Model scores
Device scores
Proactively optimize the user experience and track your progress Learn more.
Device scope : All Devices
Refresh
Baseline
All organizations (median)
Endpoint analytics score
Insufficient data
Endpoint analytic...
36
Baseline
50
Score categories
Metric
Score
Startup performance
17
Application reliability
0
Work from anywhere
93
▲ = Baseline
Preview reports do not contribute to your Endpoint analytics score
Insights and recommendations
You have 1 devices with boot times slowed by Group Policy. On average, these devices spend 68 seconds processing Group Policies.
Reducing Group Policy overhead will boost your score by 2 points. Learn more.
100% of your Windows 10 devices aren't registered for Windows Autopilot. Autopilot enables remote provisoning and the best onboarding experience for new and reset PCs.
Registering all devices in Autopilot will boost your score by 1 point.
100% of your Windows 10 devices don't have a deployment profile for Windows Autopilot. Deployment profiles determine the deployment mode, and customize the out of box experience for your end users.
Creating and targeting a deployment profile will boost your score by 1 point.


Microsoft Intune admin center
kica13@woodgrove.ms
WOODGROVE (WOODGROVE.MS)
Woodgrove
Get started with Copilot
Explore new ways to work smarter and faster using the power of AI.
Learn more about Copilot in Intune
Policy management
Get help with settings while creating a new configuration policy. Let Copilot analyze the potential security impact of a policy.
See how Copilot can help
Troubleshooting
Quickly analyze apps and policies assigned to a device to help determine issues affecting your users.
See how Copilot can help
Status
Devices not in compliance
55
Configuration policies with error or conflict
9
Client app install failure
3
Cloud PCs with failed provisioning
0
Connector errors
3
Service health
Healthy
Account status
Active
Spotlight
Introducing the Microsoft Intune Suite
The unified solution includes Remote Help, Endpoint Privilege Management, AI-powered advanced analytics, and more.
Explore
Increase productivity with Cloud PCs
Easily provision Windows 365 Cloud PCs and manage them alongside your physical devices.
Explore


Endpoint analytics - Microsoft Intune
https://endpoint.microsoft.com/#view/Microsoft_Intune_Enrollment/UXAnalyticsMenu/~/overview
Microsoft Intune admin center
chnatar@microsoft.com
MICROSOFT (MICROSOFT.ONMI...
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Reports | Endpoint analytics >
Endpoint analytics | Overview
Search
Overview
Settings
Reports
Startup performance
Application reliability
Work from anywhere
Resource performance
Remoting connection
Battery health (preview)
Overview
Anomalies
Model scores
Device scores
Proactively optimize the user experience and track your progress Learn more.
Baseline
All organizations (median)
Device scope : All Devices
Refresh
Endpoint analytics score
Meeting goals
Endpoint analytics score
73
Baseline
50
Score categories
Metric
Score
Startup performance
72
Application reliability
52
Resource performance
93
Work from anywhere
93
Battery health (preview)
71
▲ = Baseline
Preview reports do not contribute to your Endpoint analytics score
Insights and recommendations
You have 2930 devices with above average spike time % on CPU.
Upgrading these devices to a higher configuration of Cloud PCs will improve user performance and CPU score.
You have 1000 devices with above average spike time % on RAM.
Upgrading these devices to a higher configuration of Cloud PCs will improve user performance and RAM score.
You have 12585 devices with batteries at 60-80% capacity and lower runtime.
Replacing these batteries will improve battery health and boost your score by 2 points.
You have 45038 devices with batteries at 60-80% capacity. These devices might be plugged in a lot to compensate.
Replacing these batteries will improve battery health and boost your score by 2 points.
You have 5715 devices with batteries under 60% capacity and lower runtime.
Replace these batteries to improve battery health and boost your score by 1 point.
You have 4615 devices with batteries under 60% capacity. These devices might be plugged in a lot to compensate.
Replacing these batteries will improve battery health and boost your score by 1 point.

Supports: Windows | Android | macOS

Intune Remote Help

Secure cloud-based remote support. Helpdesk teams troubleshoot anytime, anywhere.

How it works

Protect every helpdesk connection with an easy-to-use app, conditional access policies, and multifactor authentication

Identify devices that are out of compliance before a connection begins and proactively remediate vulnerabilities

Provide a trusted connection with verified company profile information

Outcomes

- ✓ **Improve IT to end user helpdesk efficiency**
- ✓ **Mitigate security risks** to help support Zero Trust, MFA, and compliance
- ✓ **Empower remote workers** anywhere, on any device

Remote Help

Pain points

- Limited IT support for remote workers
- Security concerns with traditional remote access tools
- Lack of visibility and control for IT admins
- Inconsistent support experience across platforms

- Support for view only and full control modes
- Intune audit logs show who helped whom, can be exported
- Full threaded chat experience
- Integration with Conditional access
- Show reasons for non-compliance prior to accessing device

Remote Help Enablement

Licensing Requirements

Remote Help is available as part of Microsoft 365 E3 and E5 effective July 1, 2026, , via the Intune Suite or as a standalone add-on.

Both helpers and sharers must be licensed.

Tenant Configuration

Enable Remote Help in Intune Tenant Admin.

Assign RBAC roles with Remote Help permissions.

Configure Conditional Access policies (e.g., MFA, compliant device requirement).

App Deployment

Deploy Remote Help app to Windows/macOS/Android via Intune.

RBAC in Remote Help

How the features help solve it

Custom Role definitions

Remote Help uses Intune's RBAC to define granular helper roles. You can create custom roles or use built-in ones like "Helpdesk Operator" with scoped permissions for Remote Help.

Support roles can be scoped to

Roles can be scoped to specific Entra groups, device groups, or user groups.

Session types: RBAC allows differentiation between view-only, full control, unattended, and admin elevation capabilities.

RBAC ensures

Least privilege access for helpers

Audit Trail: All RBAC-enforced actions are logged in Intune Audit Logs

Session Records & Monitoring

Session Metadata Logging

Helper and sharer identities

Device name and ID

Session start/end timestamps

Session type (view-only or full control)

Attended/Unartended

Audit Logs

Separate from session logs

Administrative actions (e.g., enabling Remote Help, role assignments)

Session creation and termination events

RBAC and Conditional Access enforcement

Retention Policy

Logs are stored for 30 days in Microsoft's cloud, aligned with data residency policies.

Microsoft does not store screen content, chat transcripts, keystrokes, or audio. Only metadata is retained

Logs can be exported

Remote Help on Windows

How the features help solve it

Interactive Support Sessions

Helpers can view and control the end user's screen, interact with applications, and guide troubleshooting—all within a compliant and auditable framework.

Support for enrolled & unenrolled devices.

Admin Elevation Support

Helpers can assist users through UAC prompts and elevated workflows when permitted. This is critical for resolving issues that require administrative privileges without compromising security.

Secure Session

Before a session begins, both helper and sharer must authenticate using Entra credentials.

For unenrolled devices, the sharer receives a unique session code to enter session.

Remote Help on Android

Attended and Unattended Support

Attended sessions: Helper and sharer are both present; session initiated via Intune

Unattended sessions: Helper initiates session without sharer present

Support for enrolled devices only

Full Control & Screen Sharing

View the screen in real time

Navigate apps and settings

Perform troubleshooting and configuration tasks

This is especially valuable for kiosk-style deployments and frontline scenarios.

Enrollment/OEM-Specific Support

Enrolled Samsung and Zebra devices via Android Enterprise Dedicated (COSU)

Remote Help on macOS

Support via Web App or Native Client

A native macOS app with full control and view-only capabilities

A web-based experience that allows helpers to view the sharer's screen without requiring app installation

Support for enrolled & unenrolled devices

Key Capabilities

Includes **chat** thread that supports special characters and multiple languages

Compliance Warning, before connecting, if the sharer's device is non-compliant.

Supports **Conditional Access**

OS Requirements

Native App: macOS versions 13, 14, 15

Web App:

Safari (version 16.4.1+)

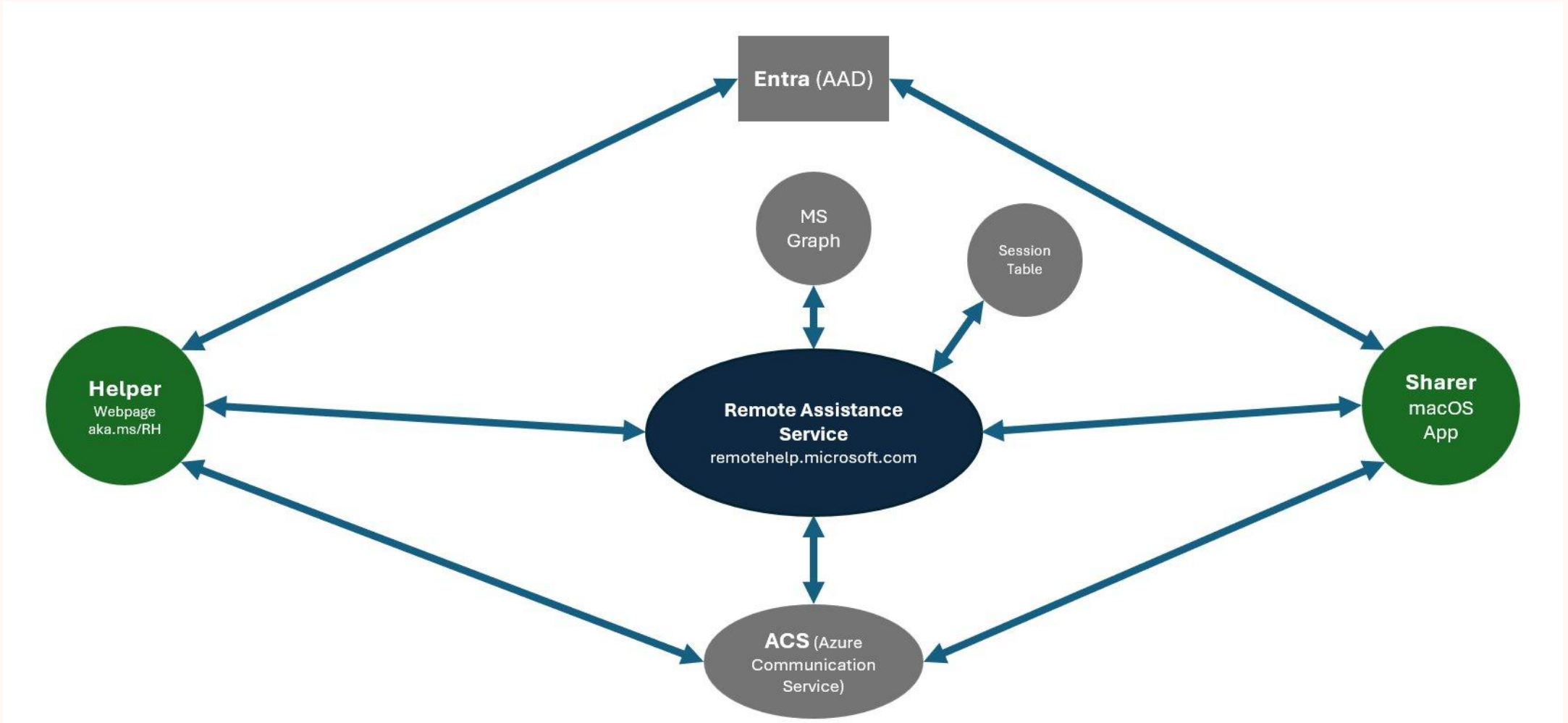
Chrome (version 109+)

Edge (version 109+)

Firefox (version 122+)

Architecture

Remote Help for macOS



Supports: Windows

Intune Endpoint Privilege Management

Secure privileged access, elevate productivity and drive compliance without granting ongoing admin rights.

How it works

Standard users run trusted applications/tasks with admin permissions only when authorized

Admins set granular rules for elevation, leveraging criteria like publisher, file hash, or argument support

All elevation activity is logged and reported for compliance, insight, and suspicious activity monitoring

Outcomes

- ✓ **Enforce least privilege** across Windows endpoints, reducing attack surface and insider risk
- ✓ **Drive user productivity** by empowering safe, temporary elevation for necessary tasks
- ✓ **Gain actionable insights** with full audit logs and reporting

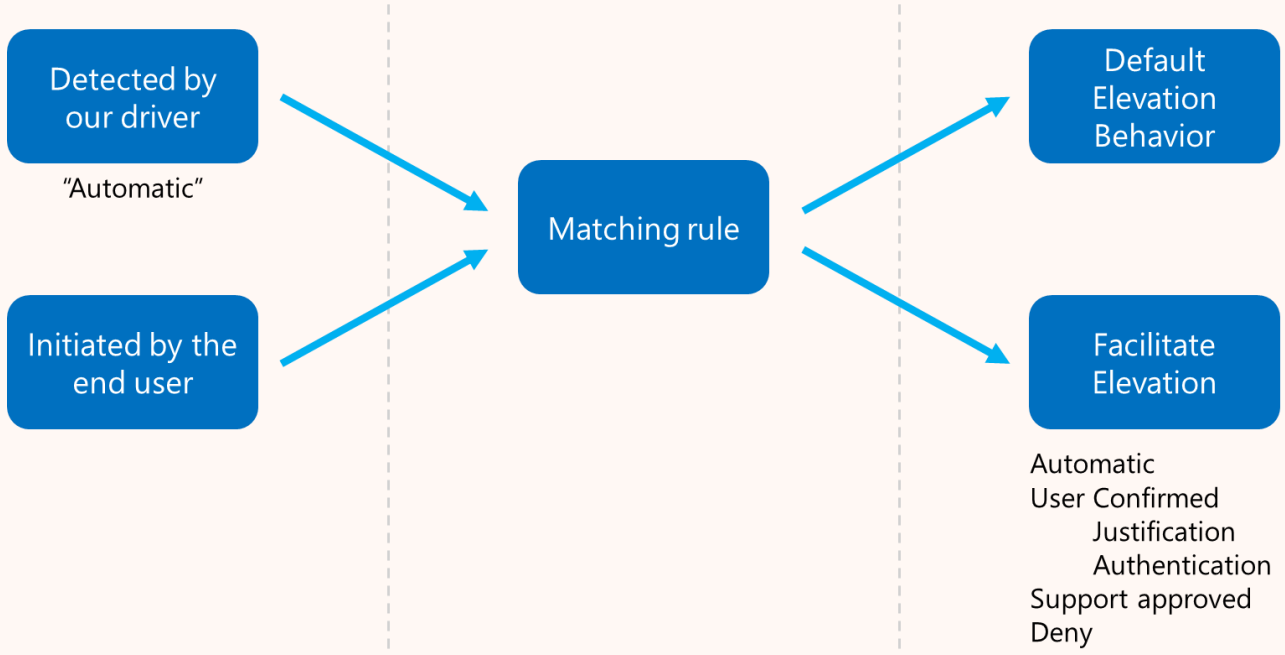
Endpoint Privilege Management

Pain point	EPM capability that solves it
Overprivileged users pose security risks	Removes standing admin rights, provides just-in-time elevation
Excessive help desk tickets for admin tasks	Allows self-service elevation for approved apps
Multiple agents introduces Complex policy enforcement across distributed endpoints	Centralized, policy-driven management via Intune
Lack of auditing on privilege usage	Detailed logs and audit trails integrated with Microsoft security
Balancing security & productivity for hybrid work	Secure elevation across all managed Windows endpoints

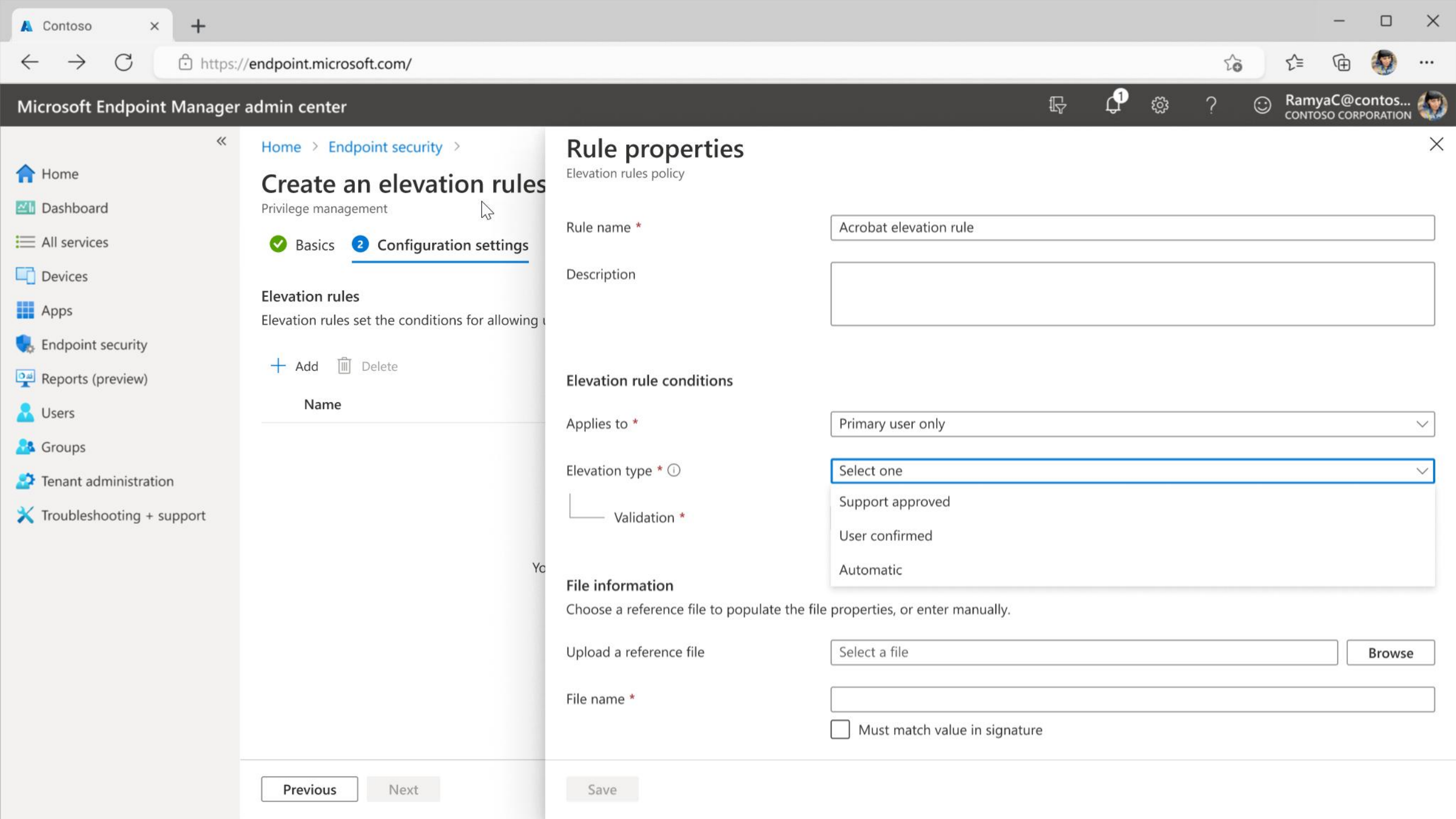
Endpoint Privilege Management

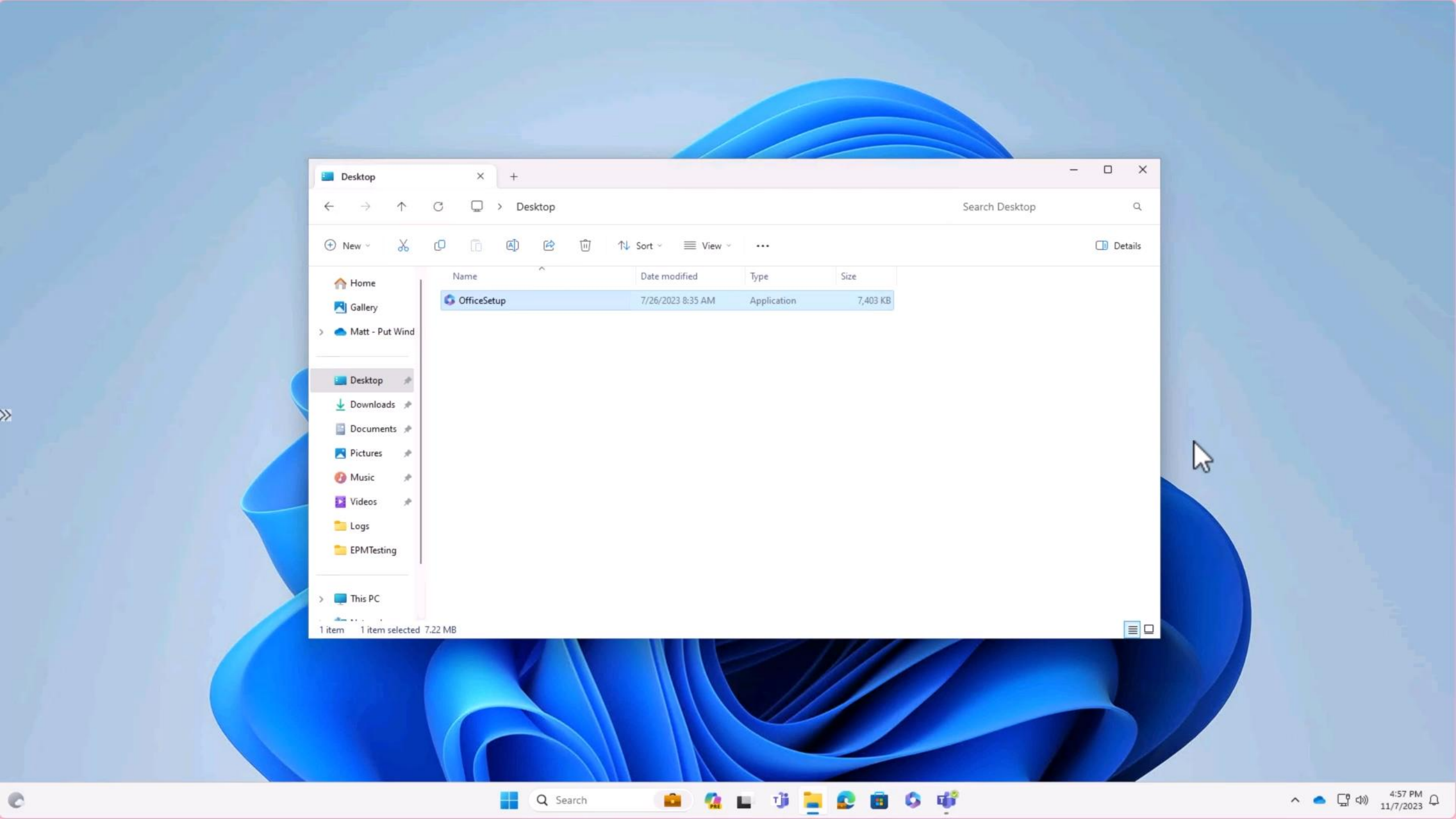
Support Arbitrated Elevations

Architecture of an elevation



- Automatic and user-confirmed elevations
- Insights based on elevation audits
- Rules based on organizational requirements
- Easy addition or removal of rules
- Tenant-level enablement, per device rollout
- Now supports Windows 365


Contoso
https://endpoint.microsoft.com/
Microsoft Endpoint Manager admin center
RamyaC@contos...
CONTOSO CORPORATION
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports (preview)
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security >
Create an elevation rules
Privilege management
Basics
2 Configuration settings
Elevation rules
Elevation rules set the conditions for allowing
Add
Delete
Name
Previous
Next
Rule properties
Elevation rules policy
Rule name *
Acrobat elevation rule
Description
Elevation rule conditions
Applies to *
Primary user only
Elevation type *
Select one
Support approved
User confirmed
Automatic
Validation *
File information
Choose a reference file to populate the file properties, or enter manually.
Upload a reference file
Select a file
Browse
File name *
Must match value in signature
Save

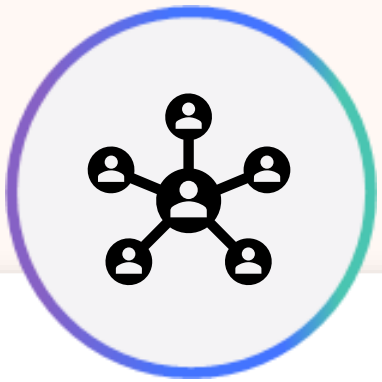

Desktop
Desktop
Search Desktop
New
Sort
View
Details
Home
Gallery
Matt - Put Wind
Desktop
Downloads
Documents
Pictures
Music
Videos
Logs
EPMTesting
This PC
Name
Date modified
Type
Size
OfficeSetup
7/26/2023 8:35 AM
Application
7,403 KB
1 item
1 item selected 7.22 MB
Search
4:57 PM
11/7/2023

What is the virtual account?

A **virtual account** is a separate account are automatically managed by the operating system. These accounts are not listed in users and groups and don't have passwords.

Automatically managed and transparent to the end user.

Specific permissions can be assigned to the virtual account



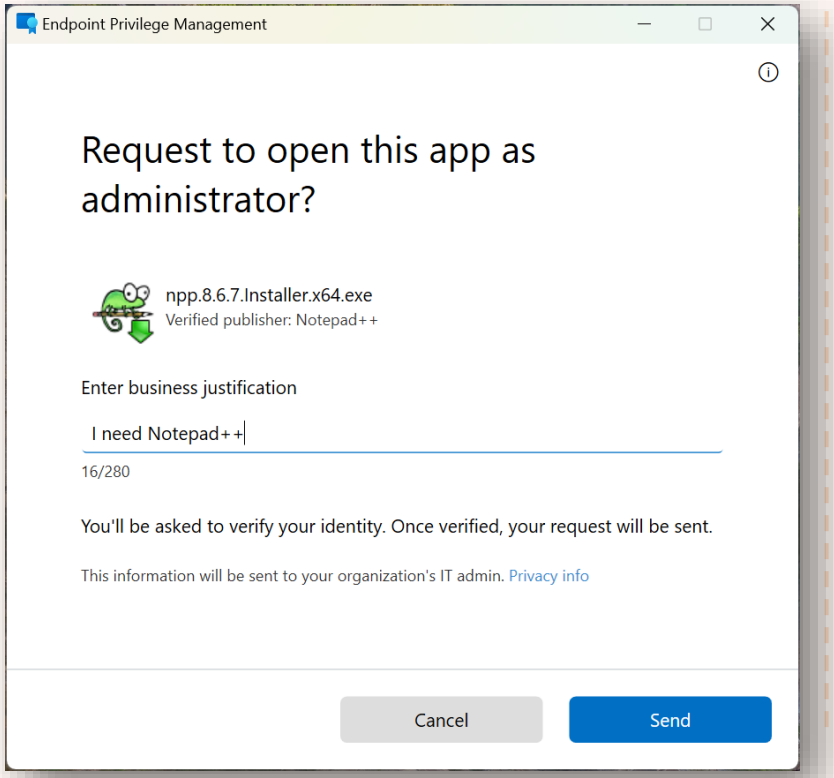
Reduced risk of lateral movement.

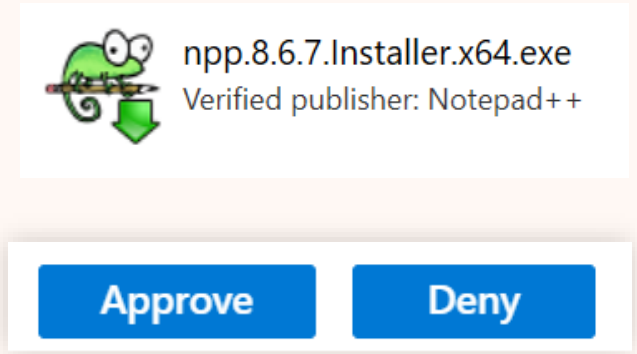
Support approval flow

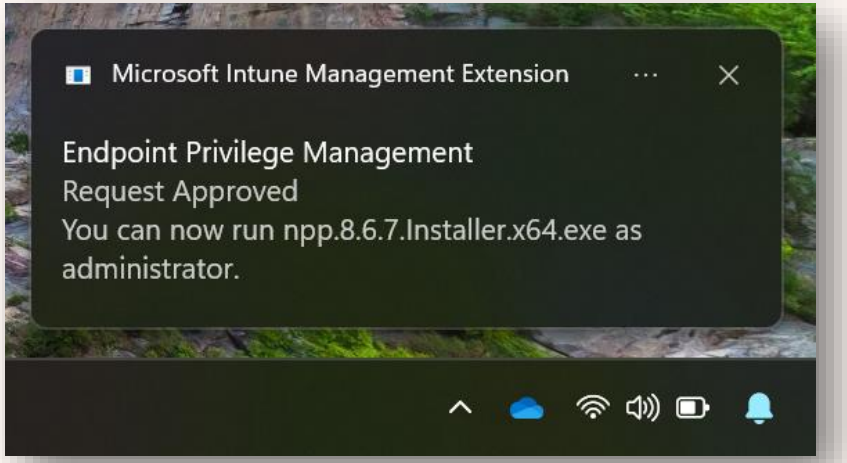
Initiated by the end user

Admin reviews in Intune Admin Center

Client allowed to elevate the app for 24 hours







And it’s all logged…

EPM Logs are in C:\Program Files\Microsoft EPM Agent\Logs

File	Details
EPM.Log	Rule elevation, general EPM operation, good starting place
EPMConsentUI.log	UX for EPM that pops client side and all the interactions with it
EPMService.log	Low level service information
EPMServiceStub.log	Post validation shows information on launching the binary

MDM and MMPC logs are available in the event log.

Event Log	Path
Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider \ Admin	Applications and Service Logs \ Microsoft \ Windows

Logs can be downloaded from a remote device using “Collect Diagnostics” in Intune.

Supports: Windows | Android | macOS | iOS

Microsoft Cloud PKI

Create multiple certificate authorities and manage certificate lifecycle in the cloud to reduce the cost and complexity tied to on-premise infrastructure

How it works

Automate certificate issuance, delivery, and revocation without the need for extensive technical expertise

Manage multiple tiers (root and issuing CAs) in the cloud

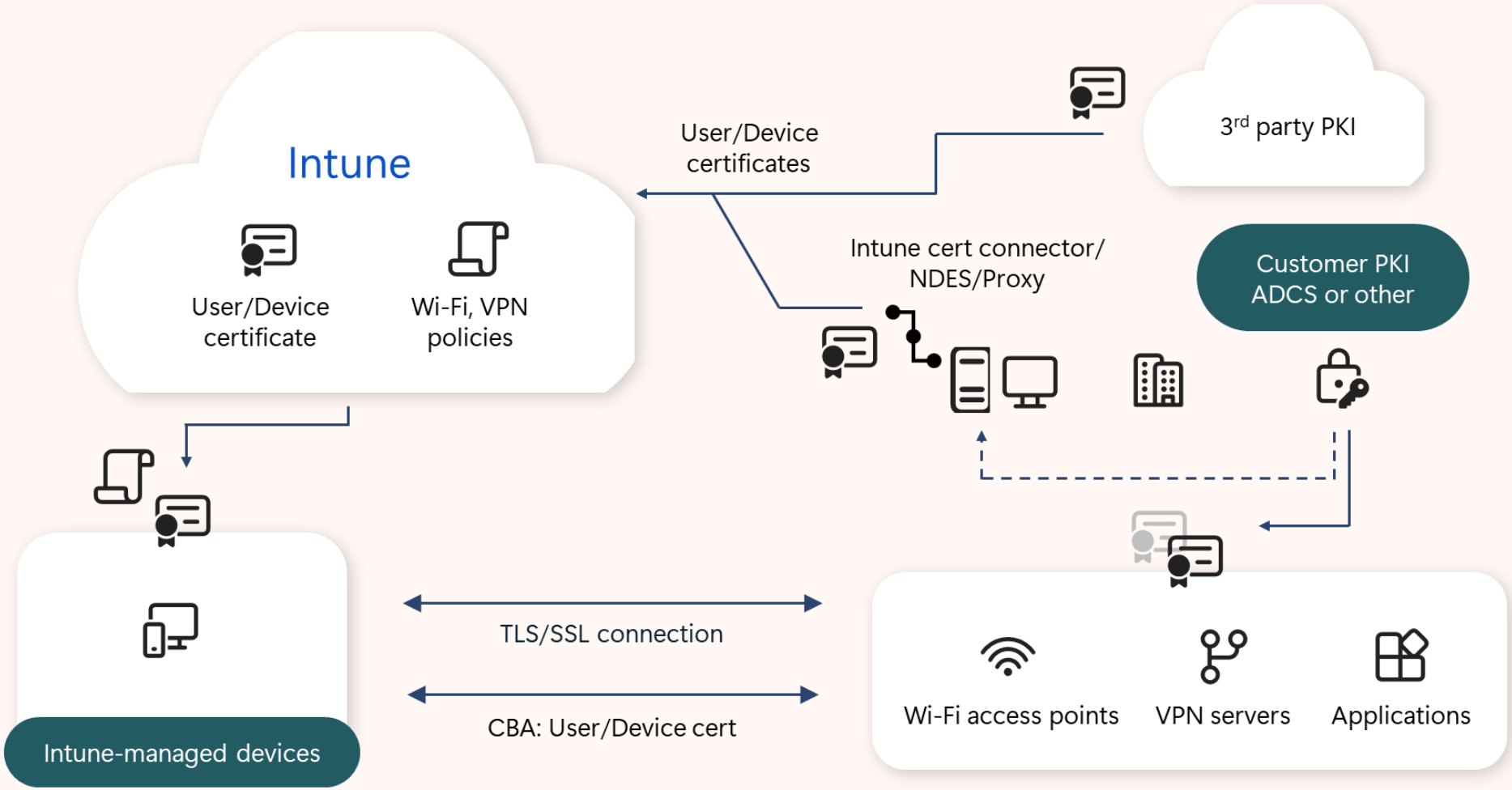
Secure certificate-based authentication, including SCEP for enrolled devices

Outcomes

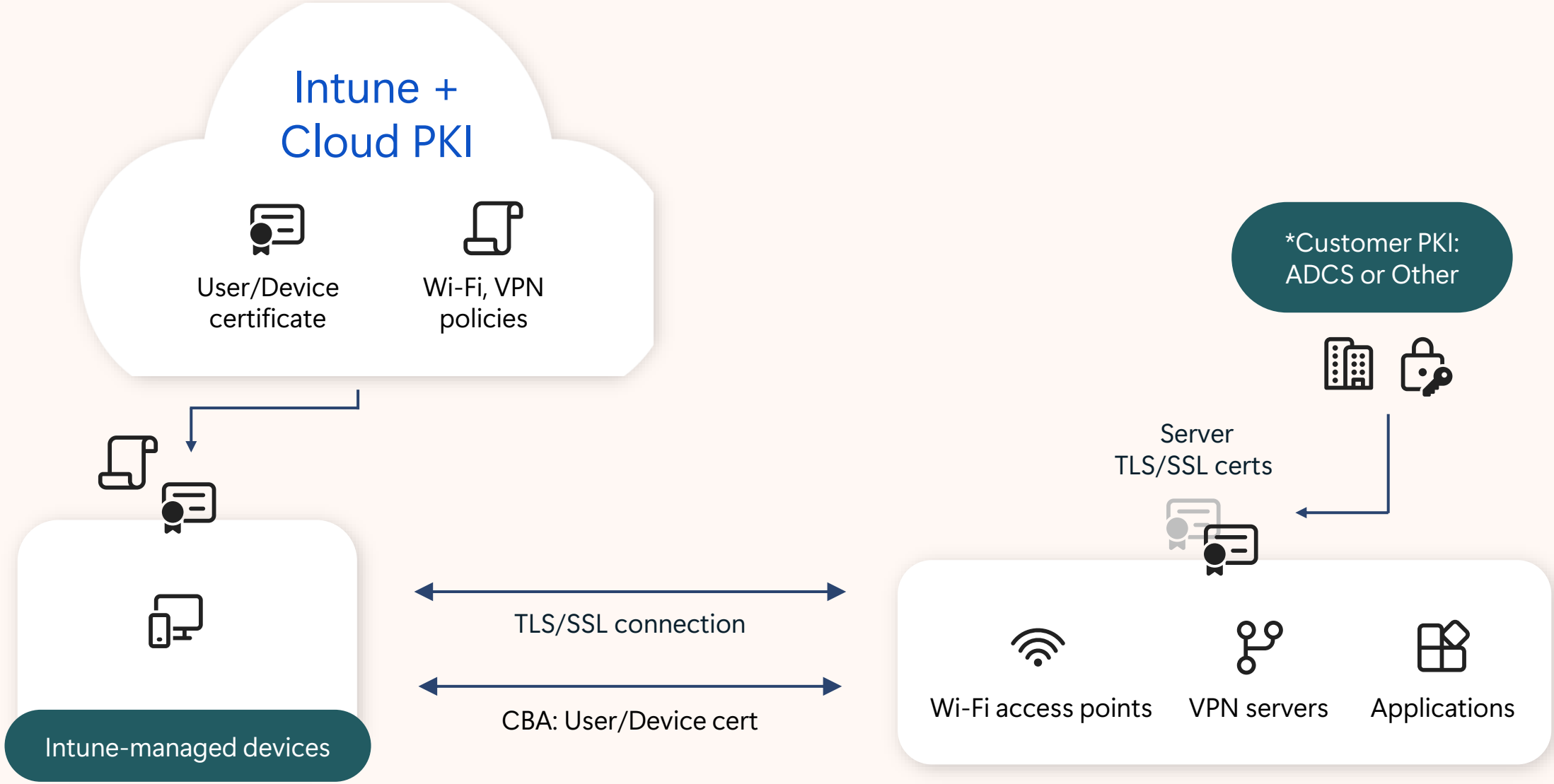
- ✓ **Simplifies PKI deployment** and management
- ✓ **Accelerates cloud transformation** and certificate management efficiency
- ✓ **Eliminates need for on-premises PKI** or connectors

Cert deliver choices before Cloud PKI:
On-premise certificate connector or 3rd-party SCEP API

COMPLEX AND COSTLY



Microsoft Cloud PKI



High level feature summary

Issue certificates for Intune-managed devices

- Platforms: Windows, iOS, macOS, Android
- Provide a certificate registration authority to deploy certificates (SCEP protocol)
- Automatically deploy certificates to Intune-managed devices

Monitor and reporting

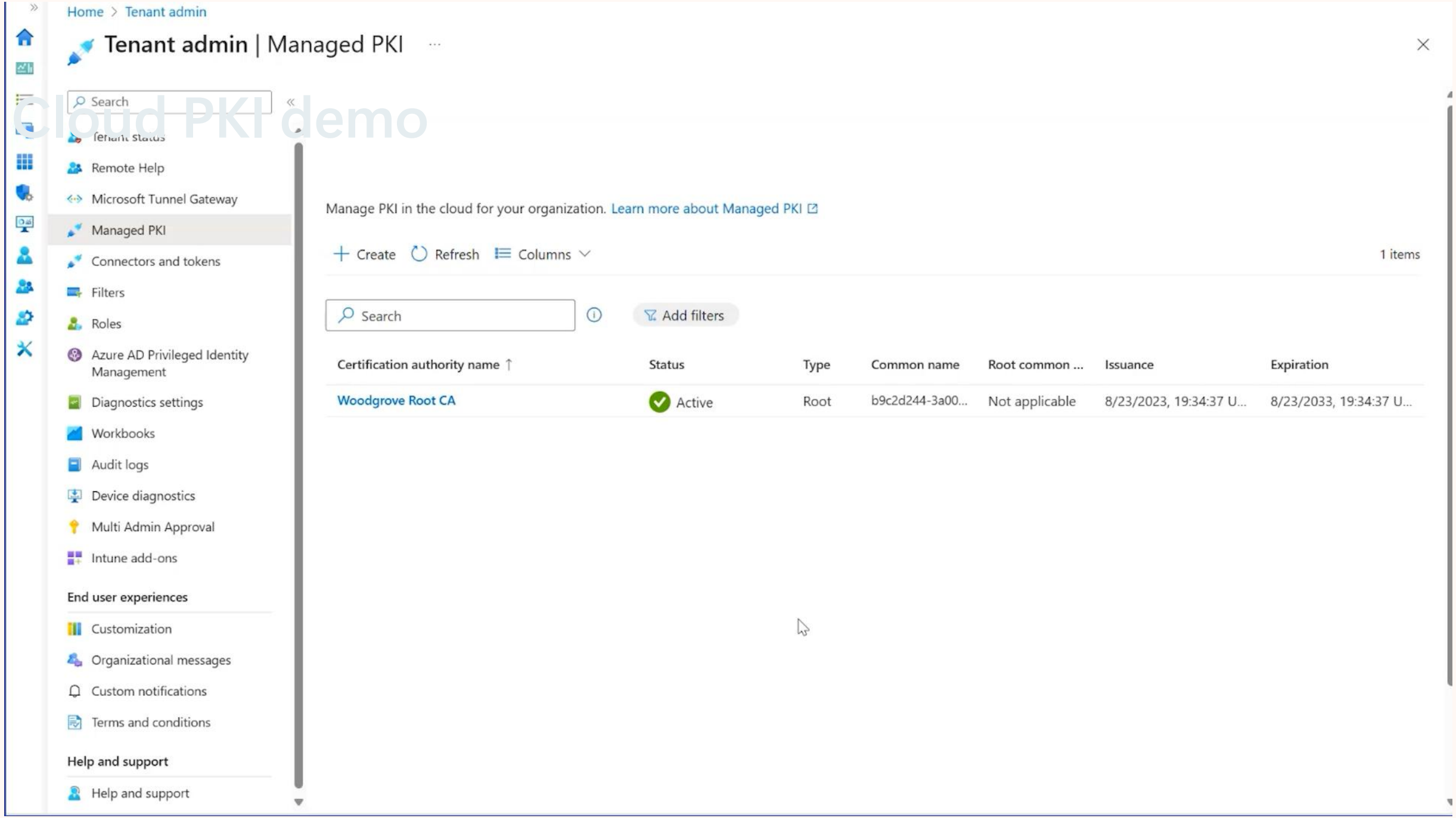
- Dashboard metrics (issued, revoked, expired certificates)
- Detailed reports for issued certificates (users, devices, policy)

Manage issued certificates

- Support automatic and manual certificate revocation
- Remove certificates from devices (triggered by retire, delete, wipe device actions)

Certificate-Based Authentication (CBA)

- Support current scenarios (Wi-Fi, VPN, applications)


Home > Tenant admin
Tenant admin | Managed PKI
Search
Cloud PKI demo
Remote Help
Microsoft Tunnel Gateway
Managed PKI
Connectors and tokens
Filters
Roles
Azure AD Privileged Identity Management
Diagnostics settings
Workbooks
Audit logs
Device diagnostics
Multi Admin Approval
Intune add-ons
End user experiences
Customization
Organizational messages
Custom notifications
Terms and conditions
Help and support
Help and support
Manage PKI in the cloud for your organization. Learn more about Managed PKI
Create
Refresh
Columns
1 items
Search
Add filters
Certification authority name
Status
Type
Common name
Root common ...
Issuance
Expiration
Woodgrove Root CA
Active
Root
b9c2d244-3a00...
Not applicable
8/23/2023, 19:34:37 U...
8/23/2033, 19:34:37 U...

Tenant admin | Managed PKI

Search

Tenant status
Remote Help
Microsoft Tunnel Gateway
Managed PKI
Connectors and tokens
Filters
Roles
Azure AD Privileged Identity Management
Diagnostics settings
Workbooks
Audit logs
Device diagnostics
Multi Admin Approval
Intune add-ons

End user experiences

Customization
Organizational messages
Custom notifications
Terms and conditions

Help and support

Managed PKI is currently offered in preview. When it becomes generally available, your Global or Billing Administrator can add it for an additional cost to the licensing options that include Microsoft Intune.

Manage PKI in the cloud for your organization. Learn more about Managed PKI

Create | Refresh | Columns | 1 items

Search | Add filters

Certification authority name ↑	Status	Type	Common name	Root common ...	Issuance	Expiration
Woodgrove Root CA	Active	Root	b9c2d244-3a00...	Not applicable	8/23/2023, 19:34:37 U...	8/23/2033, 19:34:37 U...

Supports: Windows

Intune Enterprise Application Management

Reduce time and effort for IT administrators to package apps and track updates while streamlining fix deployments to keep apps up to date and secure.

How it works

Automates app packaging and deployment from an enterprise catalog (currently Win32 apps)

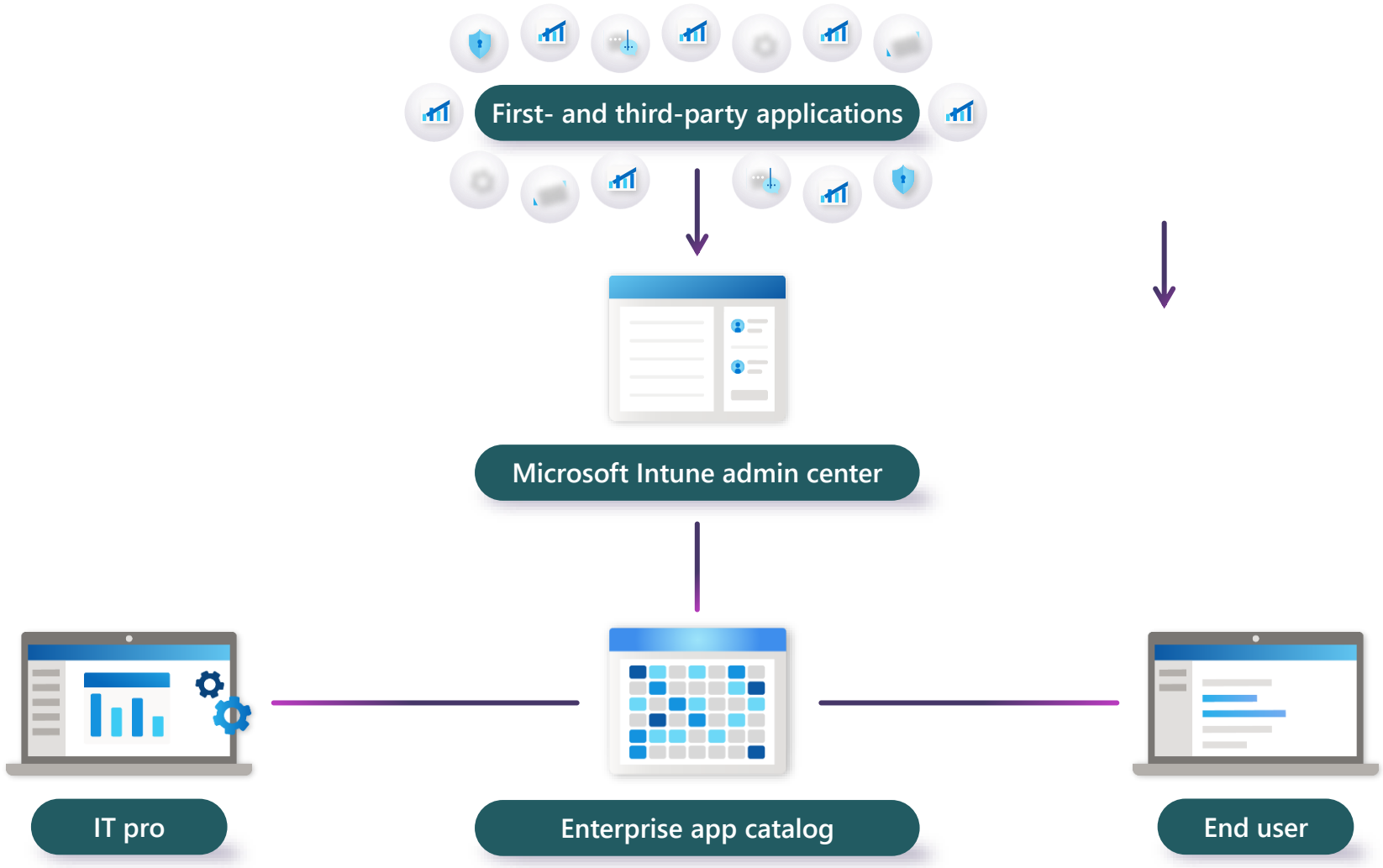
Proactively updates and patches apps for security and compliance

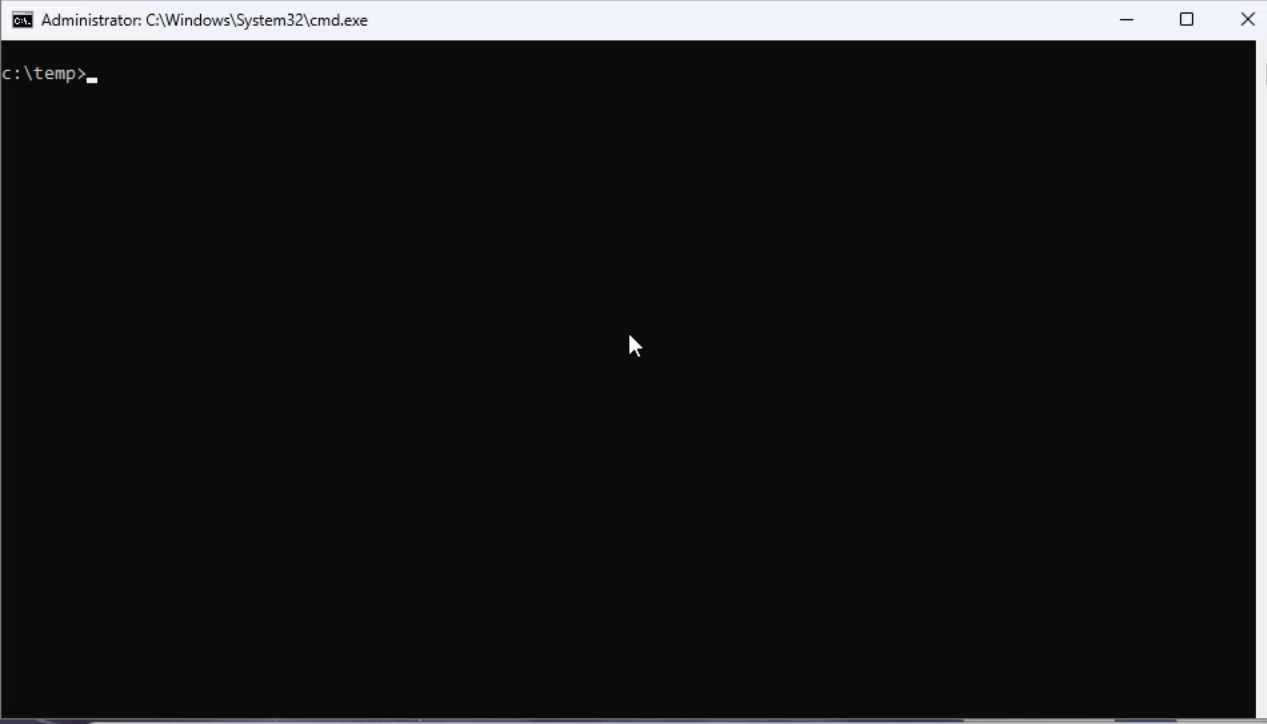
Tracks deployment status and update alerts from a unified dashboard

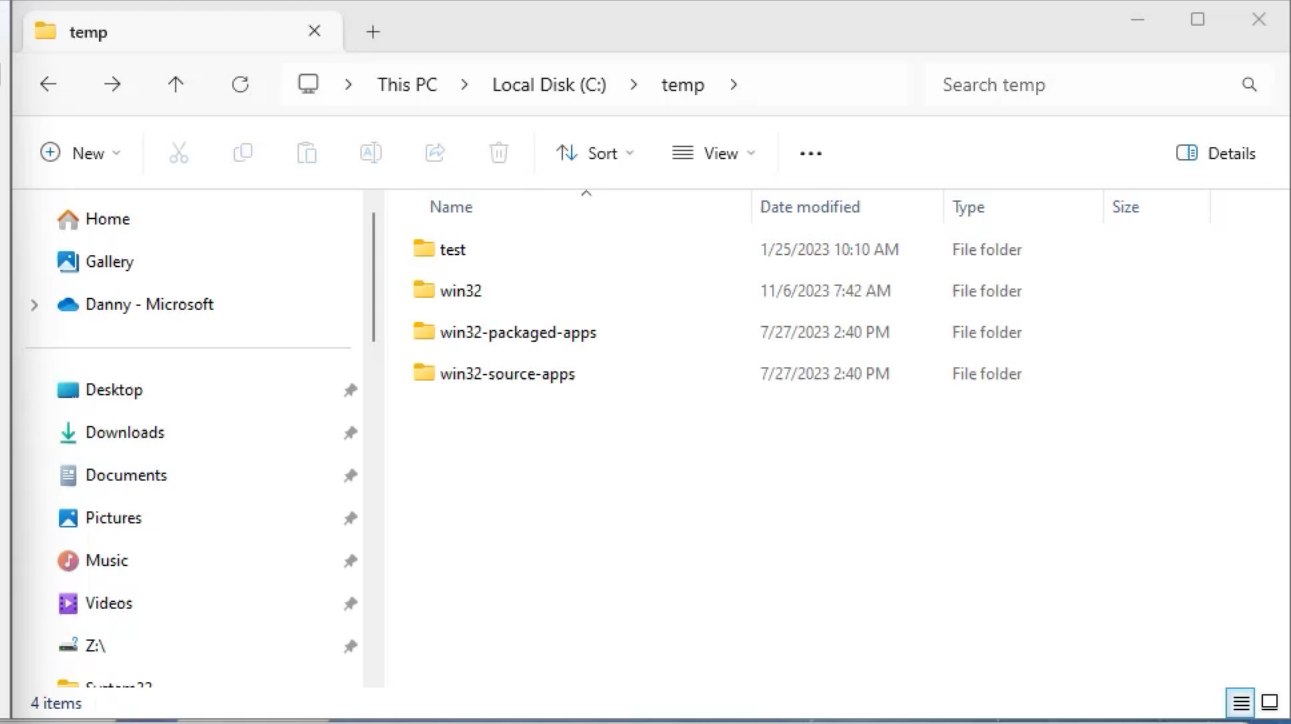
Outcomes

- ✓ **Lowers risk of cyber incidents** by ensuring critical and third-party applications are always current with the latest security patches
- ✓ **Simplifies advanced app and device management** with integrated policies and reporting
- ✓ **Accelerates onboarding and device readiness** for new hires by allowing rapid, automated app provisioning

Enterprise App Management







GitHub - microsoft/Microsoft-Win32-Content-Prep-Tool: A tool to wrap Win32 App and then it can be uploaded to Intune

https://github.com/Microsoft/Microsoft-Win32-Content-Prep-Tool

- For MSI setup file, this tool will retrieve required information for Intune.
  - If -a is specified, all catalog files in that folder will be bundled into the .intunewin file.
  - If -q is specified, it will be in quiet mode. If the output file already exists, it will be overwritten.
  - Also, if the output folder does not exist, it will be created automatically.
- IntuneWinAppUtil
  - If no parameter is specified, this tool will guide you to input the required parameters step by step.

Command-line parameters available

- -h Help
- -v Tool version (Only available starting version 1.8.2).
- -c <setup_folder> Setup folder for all setup files. All files in this folder will be compressed into .intunewin file.
  - Only the setup files for this app should be in this folder.
- -s <setup_file> Setup file (e.g. setup.exe or setup.msi).
- -o <output_file> Output folder for the generated .intunewin file.
- -a <catalog_folder> Catalog folder for all catalog files. All files in this folder will be treated as catalog file for Win10 S mode.

Note: The generated .intunewin file contains all compressed and encrypted source setup files and the encryption

Supports: Android | iOS

Microsoft Tunnel for Mobile Application Management

Create multiple certificate authorities and manage certificate lifecycle in the cloud.

How it works

Enables secure access to on-premises resources on personal (BYOD) devices without device enrollment

Manage multiple tiers (root and issuing CAs) in the cloud

VPN auto-launches when approved apps are launched

Outcomes

- ✓ **Reduces risk** from unmanaged device access to business resources
- ✓ **Empowers secure BYOD** and flexible work while ensuring IT retains control over access to sensitive data
- ✓ **Delivers secure access** with Single Sign-On (SSO), Conditional Access, and automatic VPN for approved applications

Please rate this session on Sched.com

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

Thanks!