

# PREVIEW.



*By Nicklas Ahlberg and Mattias Melkersen*

# Sponsors



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\MattiasMelkersen> whoami
azuread\mattiasmelkersen
PS C:\Users\MattiasMelkersen>
```



## Mattias Melkersen

Microsoft MVP · Endpoint & Security, Windows

### Role

Modern Workplace Architect

### Focus

Intune · Windows · Security · PowerShell · Architecture

### Blog, Hobbies and more

IT, AI, Building solutions, soccer training





## Nicklas Ahlberg

Microsoft MVP · Windows & Security (Intune)

### Role

Endpoint Consultant

### Focus

Intune · Windows 11 · Endpoint Security

### Blog, Hobbies and more

BBQ and Beer



RockEnroll.tech



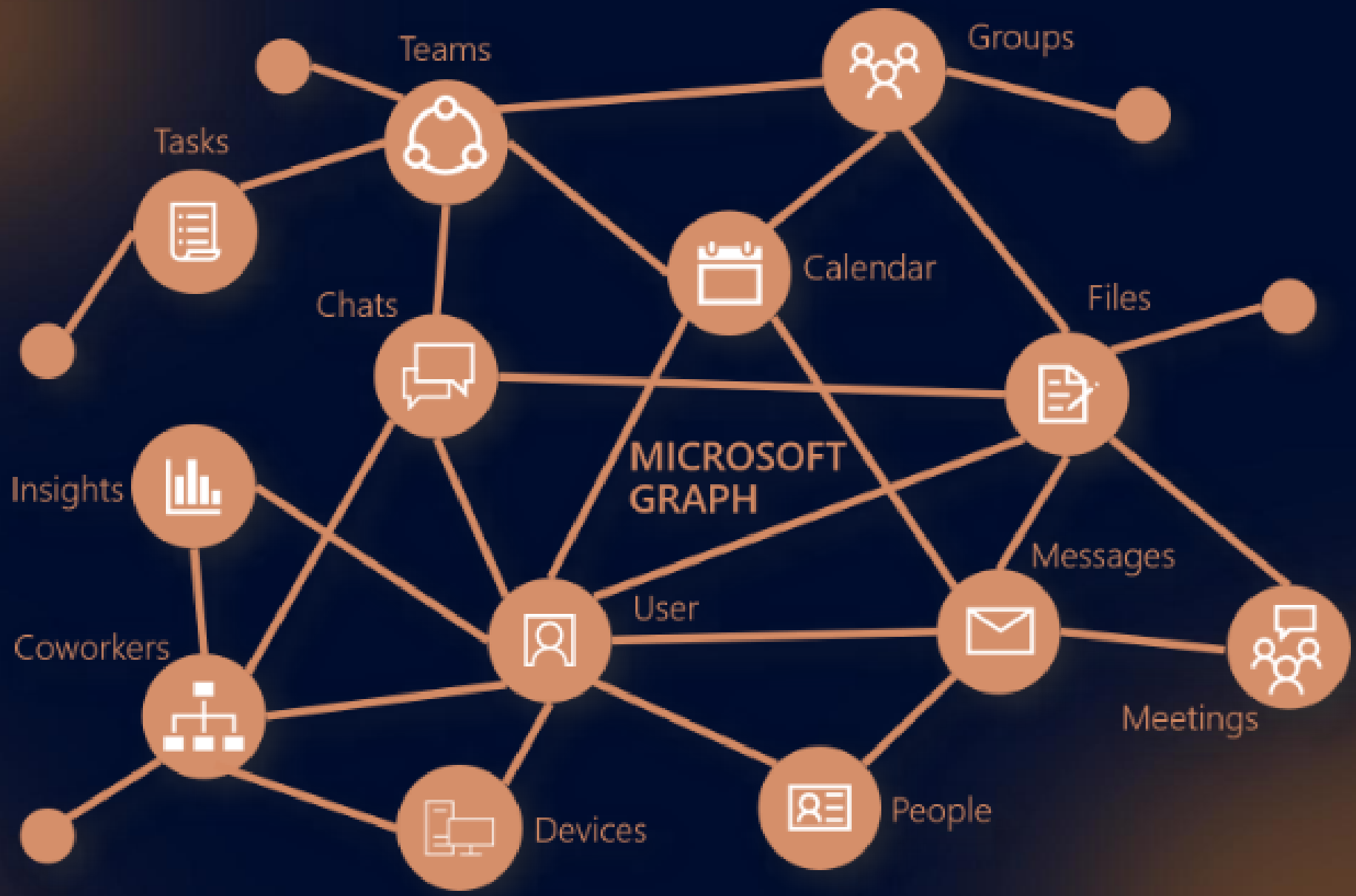
# Microsoft Intune



```
PowerShell
Command Prompt: Prompt: Powershell
PS C:\> "Hello from PowerShell"'
```

```
PowerShell
[Detailed PowerShell script content]
```

```
PowerShell
[Detailed PowerShell script content]
```



# Where do I start?





- Export platform scripts from Intune
- Save time on creating and uploading Win32 apps
- Upgrade Windows 11 to current and stay in control
- Unused groups or policies



# F12 Developer Tools

- Use the Intune portal to identify the API calls
  - Graph X-Ray is great 🙌 Merrill Fernando

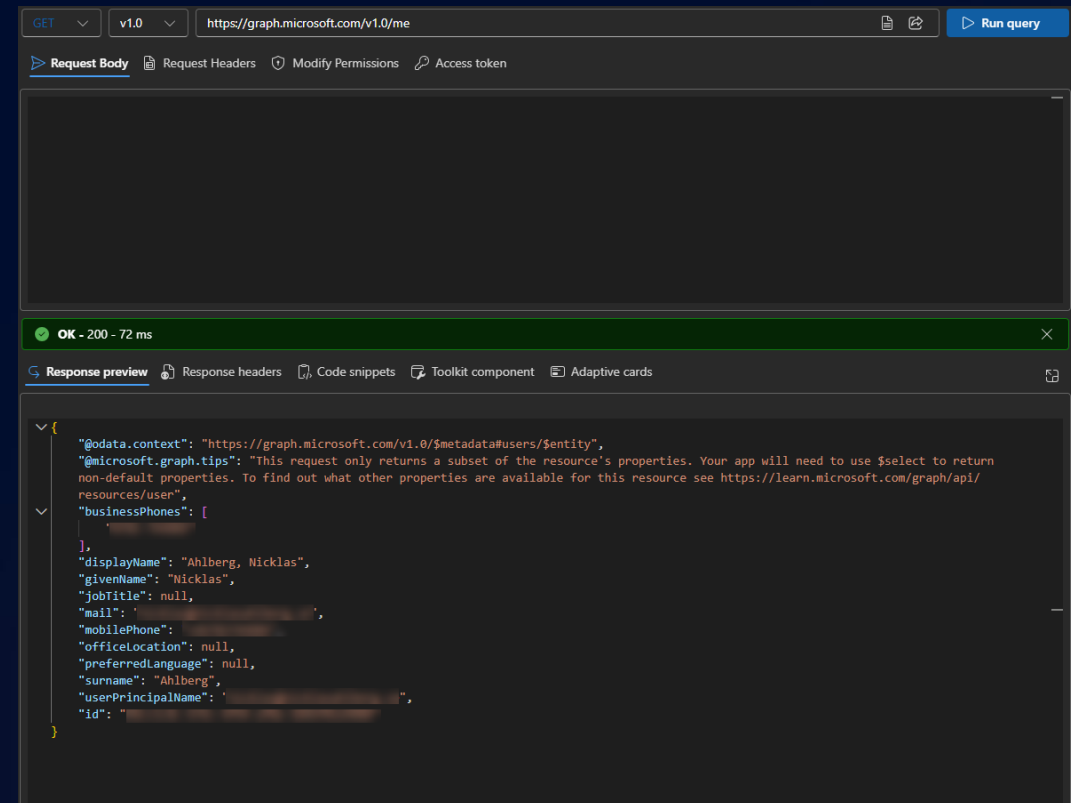


# Graph Explorer



- Identify the API call and use Graph Explorer for initial tests
  - Works perfectly for small quick/tasks
- ... and for testing

 aka.ms/GE



The screenshot shows the Microsoft Graph Explorer interface. At the top, the method is set to GET, the version to v1.0, and the URL to https://graph.microsoft.com/v1.0/me. A "Run query" button is visible. Below the URL bar, there are tabs for "Request Body", "Request Headers", "Modify Permissions", and "Access token". The main area shows a green status bar indicating a successful response: "OK - 200 - 72 ms". Below this, the "Response preview" tab is active, displaying the JSON response. The response includes metadata, a tip, and user profile information for Nicklas Ahlberg.

```
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users/$entity",
  "@microsoft.graph.tips": "This request only returns a subset of the resource's properties. Your app will need to use $select to return non-default properties. To find out what other properties are available for this resource see https://learn.microsoft.com/graph/api/resources/user",
  "businessPhones": [
  ],
  "displayName": "Ahlberg, Nicklas",
  "givenName": "Nicklas",
  "jobTitle": null,
  "mail": " ",
  "mobilePhone": " ",
  "officeLocation": null,
  "preferredLanguage": null,
  "surname": "Ahlberg",
  "userPrincipalName": " ",
  "id": " "
}
```



# Microsoft Graph **v1.0**

- All API sets are in general availability status
- Upcoming API updates are announced beforehand

# Microsoft Graph **BETA**

- This endpoint generates waaaay richer results
- Upcoming updates could break your current scripts



# PowerShell: why?

- Combine data from different sources
- Create reports
- Decode BASE64 payloads

## Example:

Identify stale objects and corresponding BitLocker and WLAPS password before deletion...

Or create a good-looking report with exactly the data and format you need.

# DEMO

- Windows LAPS
  - F12 dev tools
  - Graph Explorer
- v1 vs BETA





# PowerShell: The True Hero





THE NAME'S POWERSHELL.

THE LEGENDS ARE TRUE\*! THE POWERFUL SHELL THAT WILL ENSURE SAFE PASSAGE TO THE CLOUD!

BUT HOW?

THAT'S A HECK OF AN INTRO! PUTS MINE TO SHAME, EHP?

I'VE LONG BATTLED *SHADOW I.T.*, AND HAVE BEEN MONITORING YOUR SITUATION FROM MY *COMMAND CENTER*. YOU NEED MY HELP.

OUR BITEY LITTLE FRIENDS COULD LEARN TO MIND THEIR MANNERS! BUT OTHER THAN THAT...



HOW DO WE STOP THAT THING?

I'VE LEARNED THE WISDOM OF THOSE BEFORE US—AND UNLOCKED THE TOOLS THAT CAN DEFEAT *SHADOW I.T.*

# PowerShell: how?



- Use PowerShell to execute the API calls
  - Great for more advanced scenarios such as creating reports
  - BASE64 decoding
- 💡 PowerShell modules are great but not always required

# DEMO

- Dad jokes!
- JWT



# Some of our **greatest** PS tips:



- Less is more
- Hash tables
  - PSCustomObject
  - Modules: Only when necessary
  - NextLink
  - Throttling



# Windows LAPS history



- The portal will only show the current password
- There are scenarios where we need old passwords

# Intune Win32 Apps



- Use PowerShell to wrap and upload Win32 apps. Supports icon ★
- Huge time saver!!

*Author: Nickolaj Andersen*

# TPM / Hardware info



- Use Graph to identify TPM manufacturer.
- Known issue with RSA 3072bit
- Nuvoton and ST Micro

## **TPM attestation isn't working for TPMs which use high-range RSA 3072EK**

Date added: *April 4, 2025*

Platforms with TPMs which use high-range RSA 3072EK might fail TPM attestation. This failure impacts Windows Autopilot pre-provisioning and Windows Autopilot self-deploying flows. The issue is being investigated.

# Custom Compliance Script and JSON payload



- Custom compliance requires an inventory script and JSON for validation
- Standard compliance policies doesn't measure the running value 🙄

```
$devGuard = Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard

# Firewall
$domainFW = Get-NetFirewallProfile | Where-Object { $_.Name -eq 'Domain' }
$publicFW = Get-NetFirewallProfile | Where-Object { $_.Name -eq 'Public' }
$privateFW = Get-NetFirewallProfile | Where-Object { $_.Name -eq 'Private' }

# Run checks and store results in hashtable
$hashTable = @{
    "CredentialGuardRunning" = ($devGuard.SecurityServicesRunning -contains 1)
    "MemoryIntegrityRunning" = ($devGuard.SecurityServicesRunning -contains 2)
    "VBSRunning" = ($devGuard.VirtualizationBasedSecurityStatus -contains 2)
    "DomainFirewallEnabled" = ($domainFW.Enabled -eq 'True')
    "PublicFirewallEnabled" = ($publicFW.Enabled -eq 'True')
    "PrivateFirewallEnabled" = ($privateFW.Enabled -eq 'True')
    "SecureBootEnabled" = (Confirm-SecureBootUEFI)
}

Return $hashTable | ConvertTo-Json -Compress
```

# Device mapping, based upon primary user

## Yes, please!



- Dividing devices into groups could be hard while not using a device name prefix
- If we know where the user belongs, we could use that to tag devices with extensionAttributes

```
[2026-04-20 12:50:15] [INFO] =====  
[2026-04-20 12:50:15] [INFO] SUMMARY REPORT  
[2026-04-20 12:50:15] [INFO] -----  
[2026-04-20 12:50:15] [INFO] Runtime : 1755s  
[2026-04-20 12:50:15] [INFO] Site groups discovered : 201  
[2026-04-20 12:50:15] [INFO] Sites processed : 128  
[2026-04-20 12:50:15] [INFO] Sites skipped : 73 (no devices found or token refresh failed)  
[2026-04-20 12:50:15] [INFO] -----  
[2026-04-20 12:50:15] [INFO] Group members found : 12239  
[2026-04-20 12:50:15] [INFO] Windows devices found : 8936  
[2026-04-20 12:50:16] [INFO] Attributes already correct : 10  
[2026-04-20 12:50:16] [INFO] Attributes updated : 8918  
[2026-04-20 12:50:16] [INFO] No Entra object found : 8  
[2026-04-20 12:50:16] [INFO] Device processing errors : 0  
[2026-04-20 12:50:16] [INFO] -----  
[2026-04-20 12:50:16] [INFO] MDE tagging : DISABLED  
[2026-04-20 12:50:16] [INFO] -----  
[2026-04-20 12:50:16] [INFO] Dynamic device groups : DISABLED  
[2026-04-20 12:50:16] [INFO] =====  
[2026-04-20 12:50:17] [INFO] === Script finished ===
```



# Configuration as code

- Less clicks, more testing... let's focus on the correct stuff
- Check in policies, create backups and just enjoy your day to day

```
[17/18] Settings Catalog/Level 2/CIS (L2) Section 12 - 98 - Windows 11 Intune 4.0.0.json
      CIS (L2) Section 12 - 98 - Windows 11 Intune 4.0.0
[16:42:53] Exists in tenant (id: 995d15d2-7218-4599-8d11-f4849423410d)
[16:42:53] - No changes detected - policy is up to date

[18/18] Settings Catalog/Bitlocker/CIS (BL) BitLocker - Windows 11 Intune 4.0.0.json
      CIS (BL) BitLocker - Windows 11 Intune 4.0.0
[16:42:53] Exists in tenant (id: d29ca6b2-54a2-4ce0-a8cd-aa34d36660c9)
[16:42:53] - No changes detected - policy is up to date
Run Summary
```

---

```
Run Summary
```

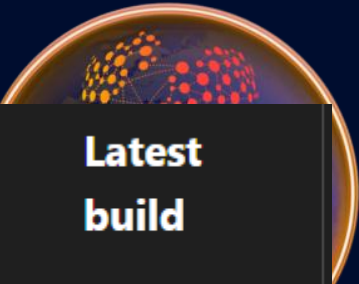
---

Runtime	8s
Files processed	18
Created	0
Updated	0
Skipped	18
Failed	0

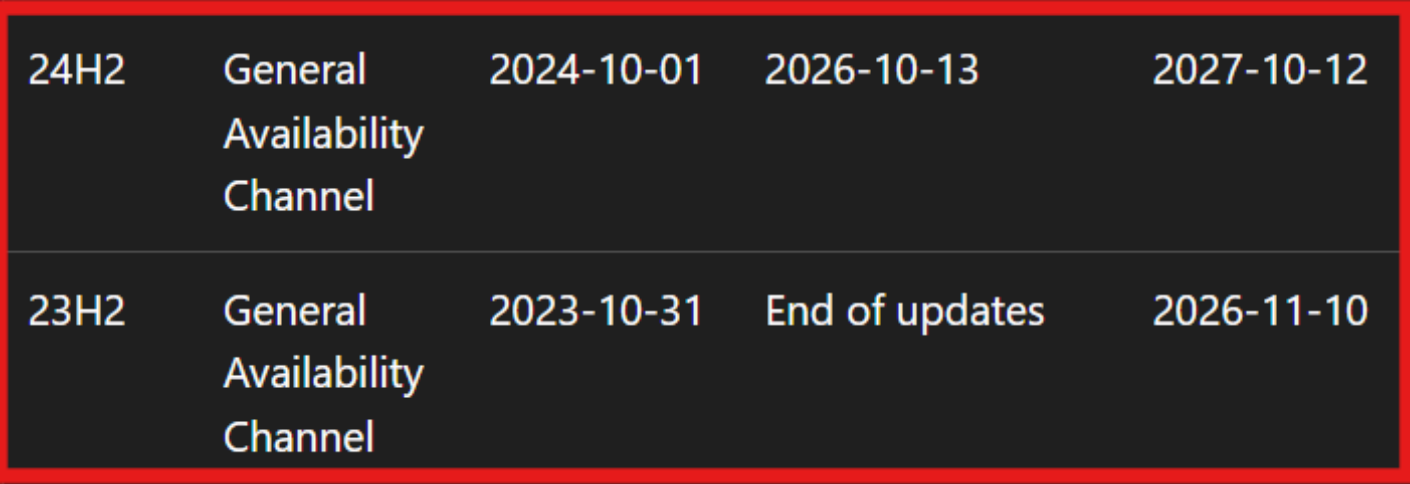
```
[16:42:53] v Deployment complete
```

# Scope tags... Huge manual work!





Version	Servicing option	Availability date	End of updates: Home, Pro, Pro Education, and Pro for Workstations	End of updates: Enterprise, Education, IoT Enterprise, and Enterprise multi-session	Latest update for ESU	Latest revision date	Latest build
25H2	General Availability Channel	2025-09-30	2027-10-12	2028-10-10	<a href="#">2026-01 D</a>	2026-01-29	26200.7705
24H2	General Availability Channel	2024-10-01	2026-10-13	2027-10-12	<a href="#">2026-01 D</a>	2026-01-29	26100.7705
23H2	General Availability Channel	2023-10-31	End of updates	2026-11-10	<a href="#">2026-01 OOB</a>	2026-01-24	22631.6495



# Windows feature updates



- The eco system of Microsoft requires us to stay current to ensure we stay supported.
- The only constant is that we know we have to move.
- For Windows that means new features introduced, old deprecated.
- When new features are introduced, we as admins needs to know about them and take action. The same needs to happen to have a clean environment that keeps being healthy and simpler to manage.
- Where do we start?

# Windows feature updates technology



- To stay current, we have multiple options available.
- Autopatch
- Windows update for business
- WSUS

API management to Windows Update for Business deployment services

# PowerShell is the answer to many things



## Security Features

TPM Present	True
TPM Enabled	True
TPM Version	2.0, 0, 1.38
SecureBoot Enabled	Enabled
Virtualization-Based Security	Enabled
Device Guard Status	Running
Credential Guard Status	Enabled with UEFI lock
HVCI (Memory Integrity)	Disabled

0 Event Log Errors	0 Event Log Warnings	0 Intune Log Errors	0 Intune Log Warnings
266 AppX Packages	22 Enabled Features	111 Disabled Features	233 Installed Programs
185 Intune MDM Policies	340 Windows Services	295 Scheduled Tasks	260 Installed Drivers
SecureBoot Enabled			

# Control your Intune environment



- Do you have full control of your environment?
- Some will say, YES, but our bet is that most have already started to build up technical dept, just as we did with good old GPO's.

FILTER BY POLICY TYPE: All Policy Types

FILTER BY LAST MODIFIED: All Time

Clear All Filters

Unassigned Policies 87

Assigned Policies 108

Deprecated/Test 26

### Assigned Policies (108)

These policies are actively assigned to groups, devices, or users in your organization.

Show 25 policies per page

Filter policies:

POLICY TYPE	POLICY NAME	LAST MODIFIED	ASSIGNMENTS	CHANGE STATUS
GroupPolicyConfigurations	Global-Device-CMW-LenovoPatch-Ring 1	2026-01-21 21:02	Group (Include): 3Ring03-Fast-Users Group (Include): 3Ring02-First-Users Group (Include): 3Ring02-First-Devices	
RemediationScripts	Global-Device-CMW-Script-WufBRemoveKeys v2.5	2026-01-21 20:58	Group (Include): Birkerød Skole	
PowerShellScripts	Global-Device-CMW-Script-DateFormat v1.0	2026-01-21 20:57	All Devices: All Devices	
EnrollmentStatusPage	Windows 10 - Autopilot AAD only	2025-12-12 08:17	Group (Include): MEM-AutopilotAADOnly	
ConfigurationPolicies	Sharepoint Homepage	2025-11-24 12:45	Group (Include): Intune-Edge-HomePage-Devices	
MobileApps	Custom PSADT Banner	2025-10-27 14:00	All Devices: All Devices All Users: All Users	

# DEMO

- Windows 11 23H2 -> 25H2
- Intune TOTAL control.



Please rate this session on  
Sched.com



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

# Thanks!