Essential Tips and Tricks for Today's Workplace Admin

Peter Daalmans & Kenneth van Surksum

CONNECT. COLLABORATE. CREATE

MC2MC

—CONNECT—

Peter Daalmans

- Solutions Architect & Modern Workplace Consultant at SecMinds Solutions

Microsoft® MVP Most Valuable Professional

Microsoft CERTIFIED Trainer

@daalmans.com	@EnterpriseMobilityTips
@pdaalmans	pdaalmans
/pdaalmans	secminds.solutions

Kenneth van Surksum

- Modern Workplace Consultant at Secure At Work

MVP Microsoft® Most Valuable Professional

kennethvs.nl

kennethvs

/kennethvansurksum

kennethvs

vansurksum.com

2Pint

PATCH MY PC

robopack

wortell

INGRAM MICRO®

The Collective

bechtle

lebon.IT

ConXioN
The new style of IT

VirtualMetric

veeam

evri

Tip #1
Naming convention?

Naming Conventions

- What the policy does (as granulair as possible)
    - Allows for exclusions
- Version the policy by including a version in its name
- Use descriptions for additional information
- “label” the policy

Example:

W1x – CP – Lock Windows 25H2 – v1.0

CP-Win-Lock Windows 25H2-v1.0-TST

DEMO
Naming convention

CONNECT. COLLABORATE. CREATE

MC2MC

CONNECT

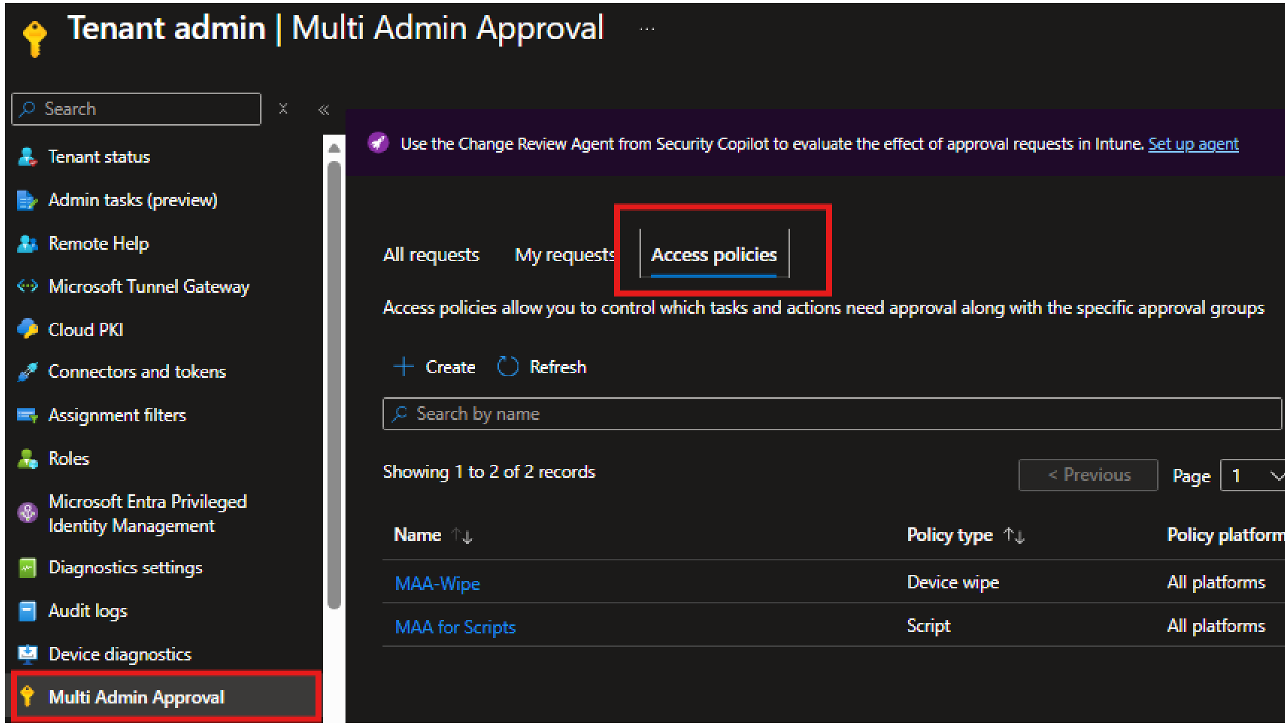
Tip #2 -
Multi Admin Approval

What is Multi Admin Approval ?

- Intune access policies to require that a second administrative account is used to approve a change before the change is effectively applied
- Helps to protect against compromised admin accounts
- Only for select object types

Prerequisites & support

- At least 2 administrator accounts
- Intune Administrator or Azure Global Administrator role
- Supports changes to:
  - App & Script (deployments)
  - Tenant Configuration
  - Remote actions (Delete, retire, wipe devices)
  - Role
  - Non-Windows versus Windows Only



Tenant admin | Multi Admin Approval

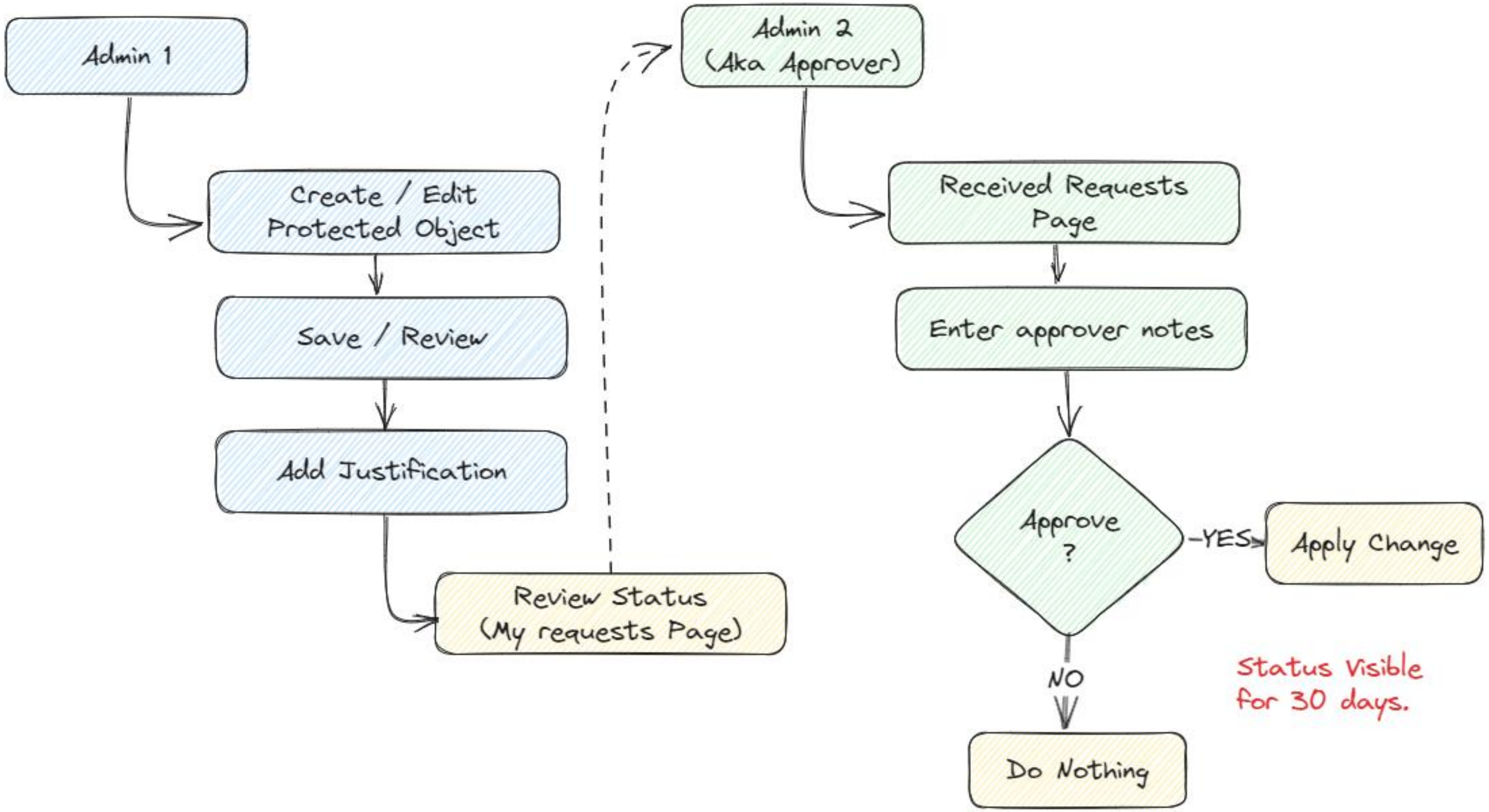
Use the Change Review Agent from Security Copilot to evaluate the effect of approval requests in Intune. Set up agent

Access policies allow you to control which tasks and actions need approval along with the specific approval groups

Showing 1 to 2 of 2 records

Name	Policy type	Policy platform
MAA-Wipe	Device wipe	All platforms
MAA for Scripts	Script	All platforms

Flow



Admin 1
Create / Edit Protected Object
Save / Review
Add Justification
Review Status (My requests Page)
Admin 2 (Aka Approver)
Received Requests Page
Enter approver notes
Approve ?
-YES-
Apply Change
NO
Do Nothing
Status Visible for 30 days.

Important

- Intune does not send notifications
- Process required for monitoring the approval node
- No new requests are possible for an object while an approval is pending

- Intune Audit logs – for request and approvals

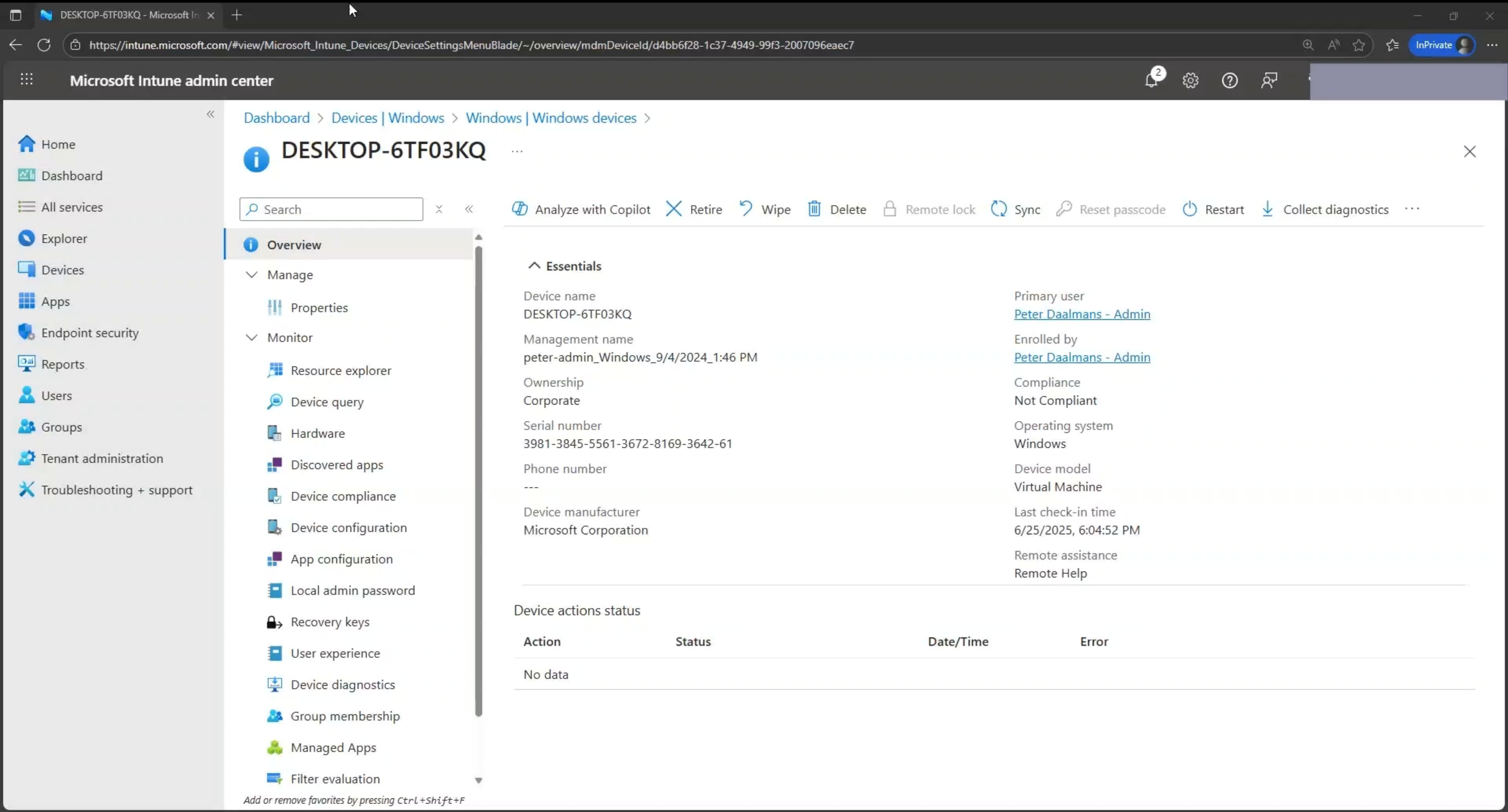
- Status conditions for a request:
  - Needs approval – Request is pending action by an approver
  - Approved – Request is being processed by Intune
  - Completed – Request has been successfully applied
  - Rejected – Request was rejected by an approver
  - Canceled – Request was canceled by the admin who submitted it

DEMO
Multi Admin Approval

CONNECT. COLLABORATE. CREATE

MC2MC

CONNECT



DESKTOP-6TF03KQ

Essentials

Device name
DESKTOP-6TF03KQ

Management name
peter-admin_Windows_9/4/2024_1:46 PM

Ownership
Corporate

Serial number
3981-3845-5561-3672-8169-3642-61

Phone number

Device manufacturer
Microsoft Corporation

Primary user
Peter Daalmans - Admin

Enrolled by
Peter Daalmans - Admin

Compliance
Not Compliant

Operating system
Windows

Device model
Virtual Machine

Last check-in time
6/25/2025, 6:04:52 PM

Remote assistance
Remote Help

Device actions status

Action	Status	Date/Time	Error
No data			

Tip #3 - Compliance Policies

Compliance Policies – One versus Many

- One versus Many
- Built your Compliance Policies based on your grace period timeout requirements
- Did you know that you can also use 0.5 days as a way to say that the grace period is ½ day

- Create different compliance policy for:
  - Things you want to be non-compliant immediately
  - Things you want to be non-compliant only for a short time (Bitlocker as part of device health)
  - Things which you want to give some time, like f.e. OS version or OS quality update

DEMO
Granular Compliance Policies

CONNECT. COLLABORATE. CREATE

MC2MC

CONNECT

Tip #4 - Admin Tasks

Admin Tasks

One centralized view for all admin tasks

Role-based and scoped visibility.

Faster triage and consistent workflows

DEMO
Admin Tasks

CONNECT. COLLABORATE. CREATE

MC2MC

CONNECT

Tip #5 - Dynamic Groups v.s. Filters

CONNECT. COLLABORATE. CREATE

MC2MC

CONNECT

Dynamic Groups v.s. Filters

- Dynamic Groups can be useful
  - No guarantee **when** they calculate
- Filters
  - Calculate on the device itself
  - When used with All Users/All Devices you are limited to other assignments
- Be careful with filters though, you cannot query on properties you don’t receive. So always check

Example:

(device.enrollmentProfileName -startsWith "AE - Corporate-owned, fully managed device profile - v")

versus

(device.enrollmentProfileName -startsWith "AE - Corporate-owned, fully managed device profile - v") and (device.enrollmentProfileName -ne $null)

Tip #6 -
Endpoint Analytics

Why do you want to look at Endpoint Analytics?

Because you want …

…. to be proactive

…. to have insights about

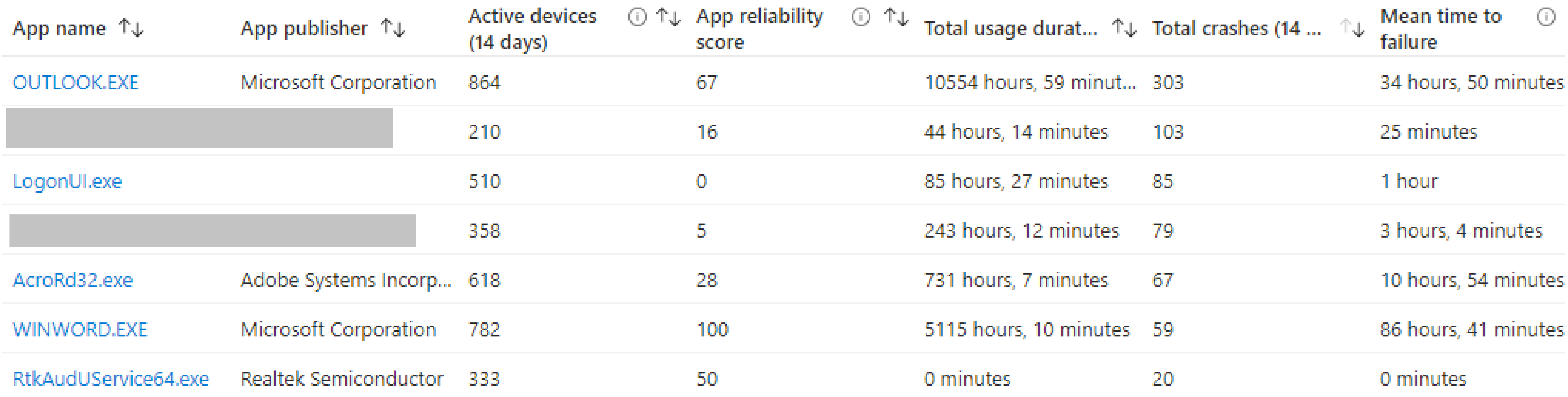
It’s not only Intune Suite, but a lot is also already there

- Already in Intune
- Startup performance
  - Model performance
  - Device performance (incl BSOD)
  - Startup process info
  - Restart info
- Application reliability
  - App Crashes
  - App Performance
  - Model performance
- Model/device score

- Added by Intune Suite
  - Battery health
  - Resource performance
  - Device timeline
  - Device query

SOON PART OF Microsoft 365 E3 and EMS E3

Application reliability



App name	App publisher	Active devices (14 days)	App reliability score	Total usage durat...	Total crashes (14 ...	Mean time to failure
OUTLOOK.EXE	Microsoft Corporation	864	67	10554 hours, 59 minut...	303	34 hours, 50 minutes
[redacted]	[redacted]	210	16	44 hours, 14 minutes	103	25 minutes
LogonUI.exe		510	0	85 hours, 27 minutes	85	1 hour
[redacted]	[redacted]	358	5	243 hours, 12 minutes	79	3 hours, 4 minutes
AcroRd32.exe	Adobe Systems Incorp...	618	28	731 hours, 7 minutes	67	10 hours, 54 minutes
WINWORD.EXE	Microsoft Corporation	782	100	5115 hours, 10 minutes	59	86 hours, 41 minutes
RtkAudUService64.exe	Realtek Semiconductor	333	50	0 minutes	20	0 minutes

DEMO
Endpoint Analytics

CONNECT. COLLABORATE. CREATE

MC2MC

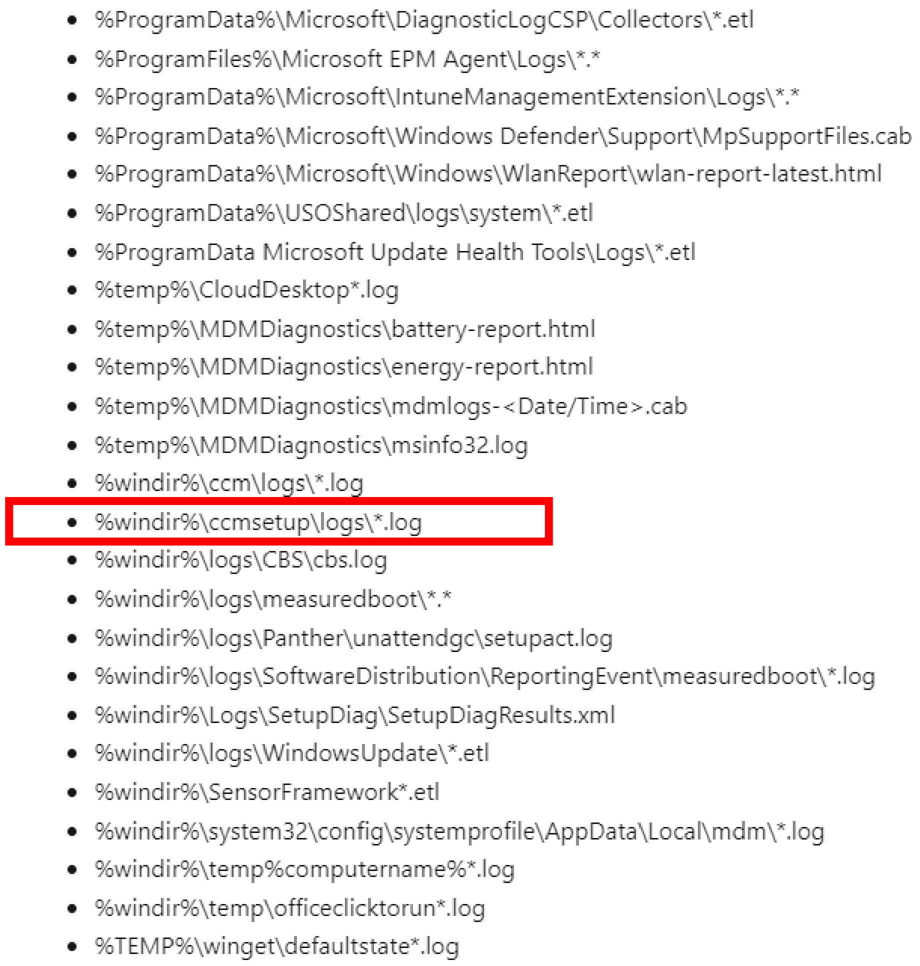
CONNECT

Tip #7 –
Gathering Custom log files

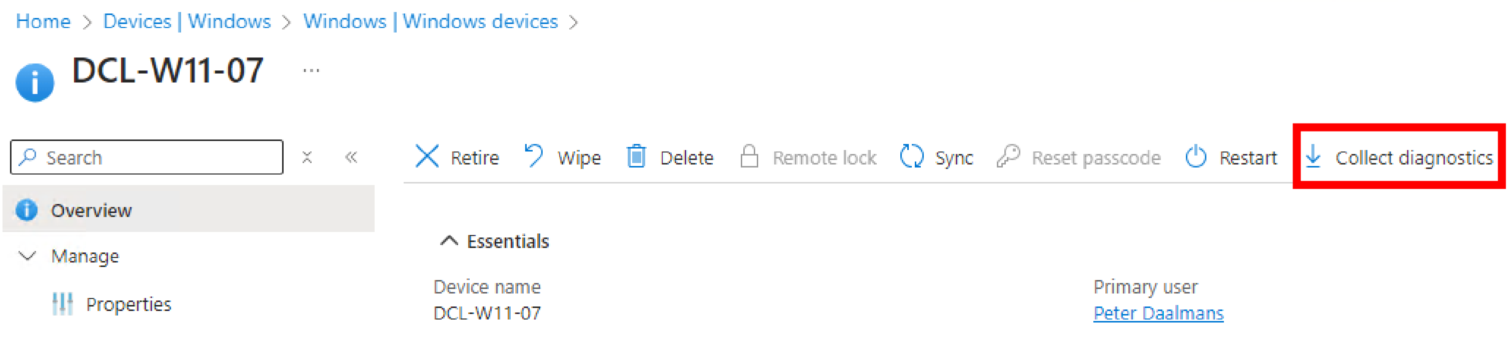
How to retrieve custom logs files file

- Include custom logs in diagnostics zip

```
msiexec /I “filename.msi” /qn /l*v
%windir%\ccm\Logs\logfile-application-version.log
```



- %ProgramData%\Microsoft\DiagnosticLogCSP\Collectors\*.etl
- %ProgramFiles%\Microsoft EPM Agent\Logs\*.*
- %ProgramData%\Microsoft\IntuneManagementExtension\Logs\*.*
- %ProgramData%\Microsoft\Windows Defender\Support\MpSupportFiles.cab
- %ProgramData%\Microsoft\Windows\WlanReport\wlan-report-latest.html
- %ProgramData%\USOShared\logs\system\*.etl
- %ProgramData Microsoft Update Health Tools\Logs\*.etl
- %temp%\CloudDesktop*.log
- %temp%\MDMDiagnostics\battery-report.html
- %temp%\MDMDiagnostics\energy-report.html
- %temp%\MDMDiagnostics\mdmlogs-<Date/Time>.cab
- %temp%\MDMDiagnostics\msinfo32.log
- %windir%\ccm\logs\*.log
- %windir%\ccmsetup\logs\*.log
- %windir%\logs\CBS\cbs.log
- %windir%\logs\measuredboot\*.*
- %windir%\logs\Panther\unattendgc\setupact.log
- %windir%\logs\SoftwareDistribution\ReportingEvent\measuredboot\*.log
- %windir%\Logs\SetupDiag\SetupDiagResults.xml
- %windir%\logs\WindowsUpdate\*.etl
- %windir%\SensorFramework*.etl
- %windir%\system32\config\systemprofile\AppData\Local\mdm\*.log
- %windir%\temp%computername%*.log
- %windir%\temp\officeclicktorun*.log
- %TEMP%\winget\defaultstate*.log



Device name
DCL-W11-07

Primary user
Peter Daalmans

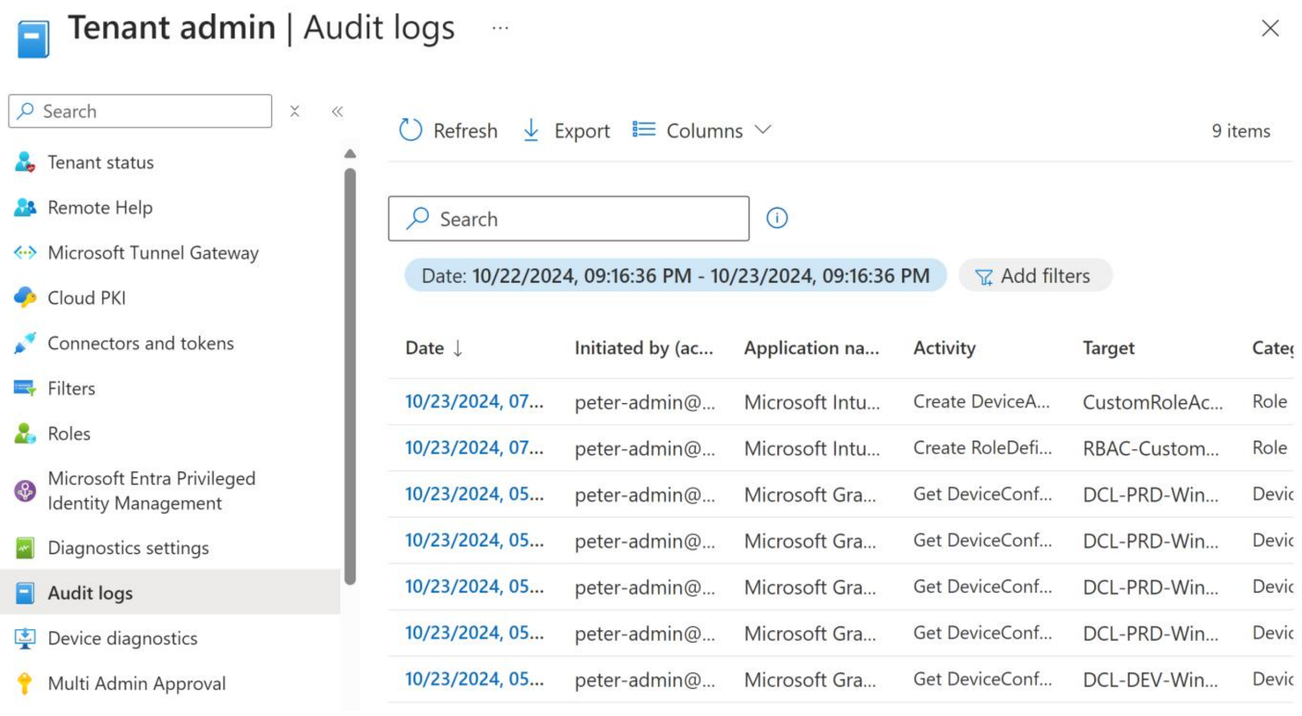
Tip #8 –
When working with colleagues, visibility is key!

CONNECT. COLLABORATE. CREATE

MC2MC
CONNECT

Intune Auditing

- Enabled by default in the Intune tenant
- Built-in audit logs record change activities
  - Create
  - Edit
  - Delete
  - Assign
  - Remote Actions
- Accessible for
  - Global Administrators
  - Intune Service Administrators
  - Intune custom role w Audit data read permissions



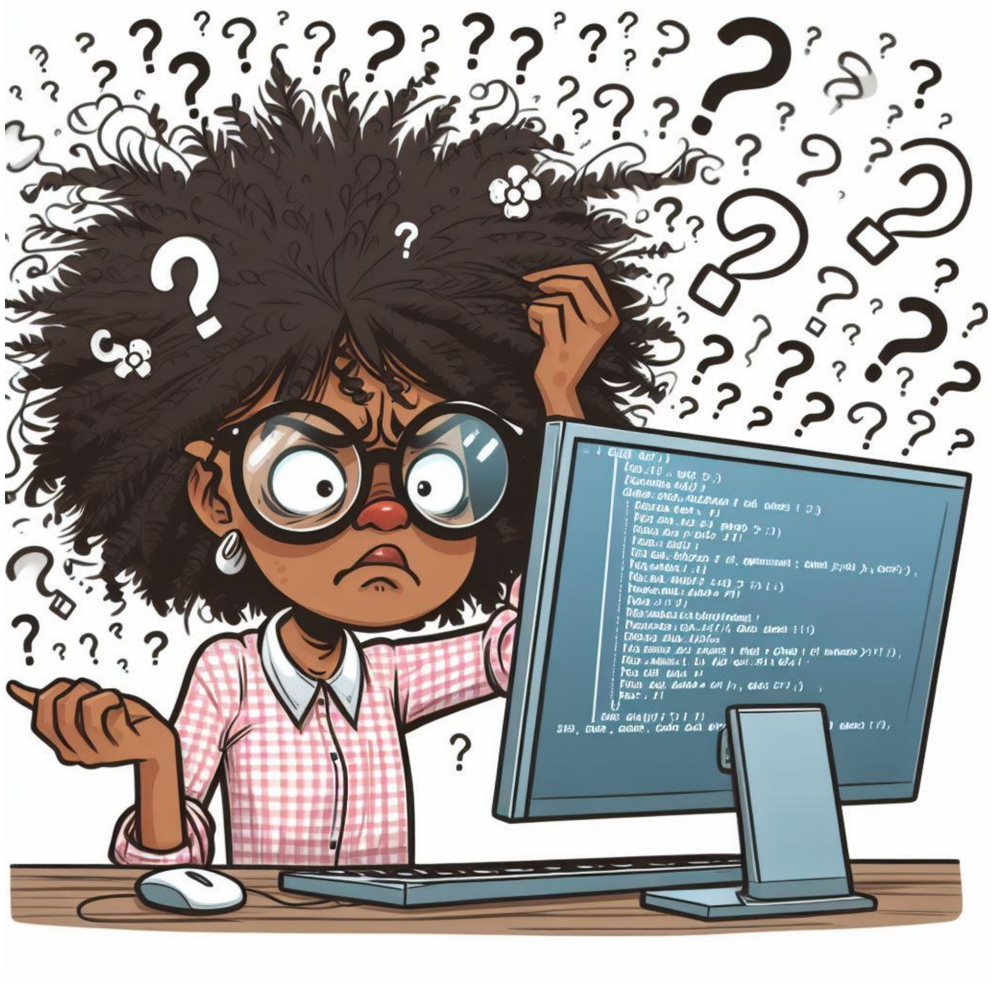
Tenant admin | Audit logs

Date: 10/22/2024, 09:16:36 PM - 10/23/2024, 09:16:36 PM

Date ↓	Initiated by (ac...	Application na...	Activity	Target	Cate
10/23/2024, 07...	peter-admin@...	Microsoft Intu...	Create DeviceA...	CustomRoleAc...	Role
10/23/2024, 07...	peter-admin@...	Microsoft Intu...	Create RoleDefi...	RBAC-Custom...	Role
10/23/2024, 05...	peter-admin@...	Microsoft Gra...	Get DeviceConf...	DCL-PRD-Win...	Devic
10/23/2024, 05...	peter-admin@...	Microsoft Gra...	Get DeviceConf...	DCL-PRD-Win...	Devic
10/23/2024, 05...	peter-admin@...	Microsoft Gra...	Get DeviceConf...	DCL-PRD-Win...	Devic
10/23/2024, 05...	peter-admin@...	Microsoft Gra...	Get DeviceConf...	DCL-PRD-Win...	Devic
10/23/2024, 05...	peter-admin@...	Microsoft Gra...	Get DeviceConf...	DCL-DEV-Win...	Devic

Get in to control via simple life hacks

- Get in control via:
  - Removing permissions ;)
  - Implement RBAC (least privileged)
  - Notification of (production) changes in Microsoft Intune
  - Great examples by Peter Klapwijk; inthecloud247.com



DEMO
PowerApps & Intune

CONNECT. COLLABORATE. CREATE

MC2MC

CONNECT

Tip #9 –
know your community tools!

CONNECT. COLLABORATE. CREATE

MC2MC

CONNECT

Community Tools

- IntuneAssistant – https://intuneassistant.cloud
- IntuneDiff – https://intunediff.com
- IntuneMermaid – https://intunemermaid.com
- Awesome Intune – https://awesomeintune.com
- Modern Endpoint Management Group on LinkedIn - https://www.linkedin.com/groups/8761296/
- Intune Manager - https://github.com/Micke-K/IntuneManagement
- Reddit - https://www.reddit.com/r/Intune/

CONNECT. COLLABORATE. CREATE

MC2MC

CONNECT

Session feedback available in home feed of the app after the session

run
events

CONNECT. COLLABORATE. CREATE

MC2MC

CONNECT