Jan Ketil Skanke

MVP Enterprise Mobility

Principal Cloud Architect @CloudWay

Twitter: @JankeSkanke
Blog: https://msendpointmgr.com

Let’s dive into Proactive Remediations

Endpoint Analytics in Microsoft Endpoint Manager

Startup Performance

Recommended Software

Proactive Remediations

Proactive Remediations

What is Proactive Remediations?

- Proactive remediations in Endpoint Analytics allows us to
  - Fix common issues
  - Have a desired state config of our clients
  - Notify our users about x , y or z

- Proactive remediations is using script packages that consists of
  - A Detection Script
  - A Remediation Script

Prerequisites

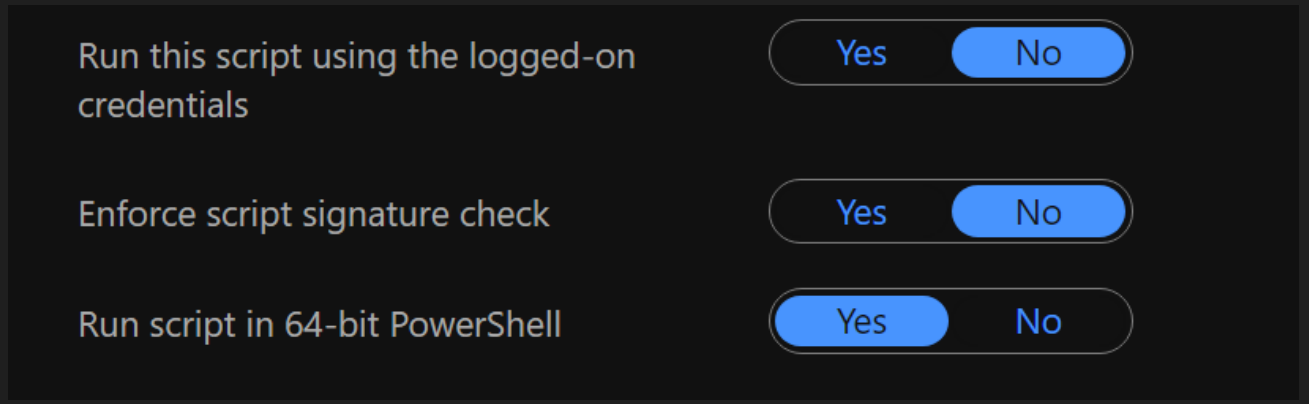
- Devices must be enrolled into Endpoint Analytics

- Devices must be Azure AD joined or hybrid Azure AD joined and meet one of the following conditions:
  - A Windows 10 Enterprise, “Professional”, or Education device that is managed by Intune.
  - A co-managed device running Windows 10, version 1903 or later.

- Licensing: Proactive Remediations:
  - Windows 10 Enterprise E3 or E5
  - Windows 10 Education A3 or A5
  - Windows Virtual Desktop Access E3 or E5

Script Requirements

- PowerShell
- Encode the scripts in UTF-8
  - If you don’t you will get issues.

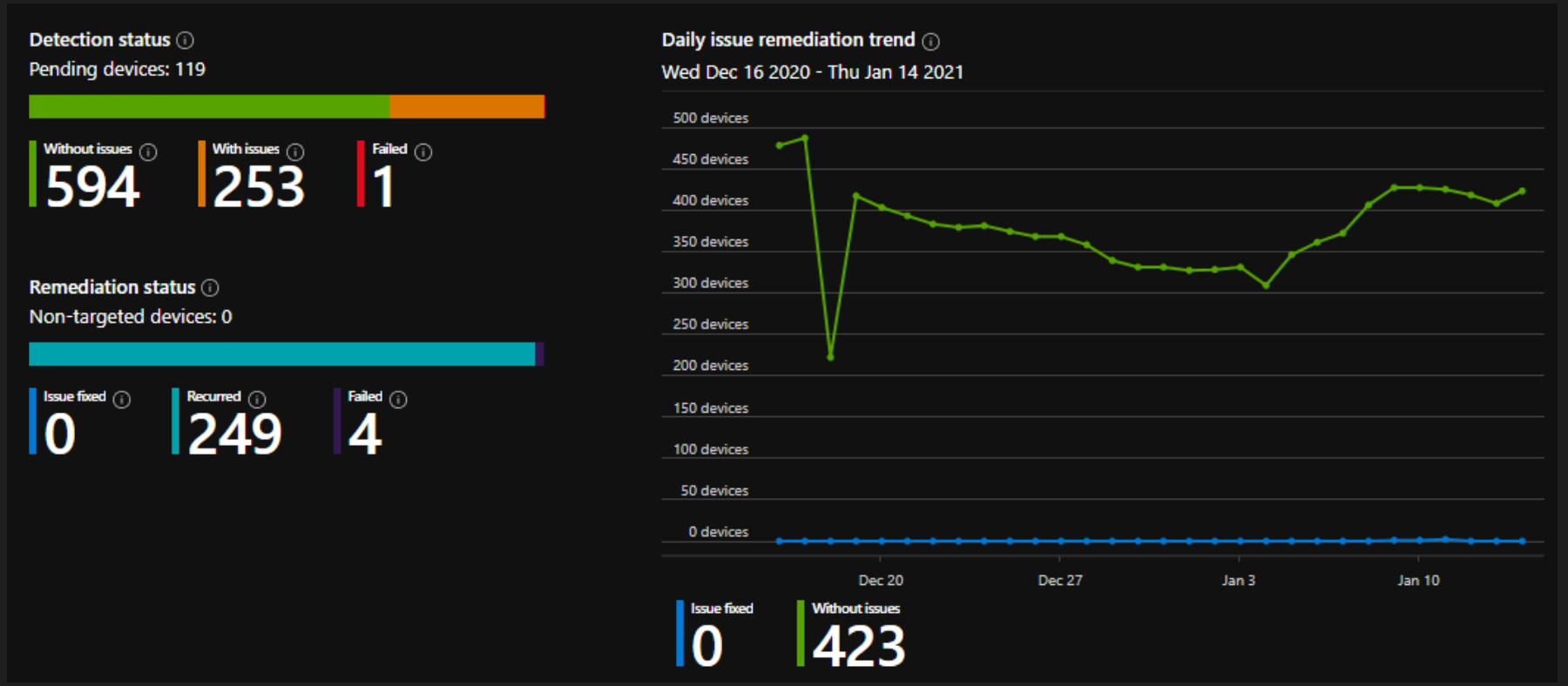


- Maximize output limit from script is 2048 Characters

- Scripts without the Enforce Script Signature check use the Bypass execution policy
  - Scripts with the check will use the execution device’s policy (default restricted)

Benefits

- Script jobs can be scheduled
- Run in user context vs system context
- Run in 64bit PowerShell or not
- Good Reporting



DEMO TIME
THE MAGIC IS IN “EXIT 0 – EXIT 1”

Some use cases

- Battery Health with end user notification
- Disk space with end user notification
- Uptime check (has the computer rebooted the last x days) with notification
- Reporting on Bitlocker status
- Collect Custom Inventory
- Manage local admins

- And much more.. And ideas come to mind?

DEMO TIME
Deploying a Script package

Some use cases

- Battery Health with end user notification
- Disk space with end user notification
- Uptime check (has the computer rebooted the last x days) with notification
- Reporting on Bitlocker status
- Collect Custom Inventory
- Manage local admins

- And much more.. And ideas come to mind?

DEMO TIME

REPORTS AND STATUS OF JOBS

DEMO TIME
DIVING INTO THE DETAILS

Where is the stuff?

- Health scripts is copied down to the local device:
  - C:\Windows\IMECache\HealthScripts
- Local Logs is found here:
  - C:\ProgramData\Microsoft\IntuneManagementExtension\Logs
- Local status information in registry:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\IntuneManagementExtension\SideCarPolicies\Scripts
- List Policy IDs from Graph
  - https://graph.microsoft.com/beta/deviceManagement/deviceHealthScripts?select= id, displayname

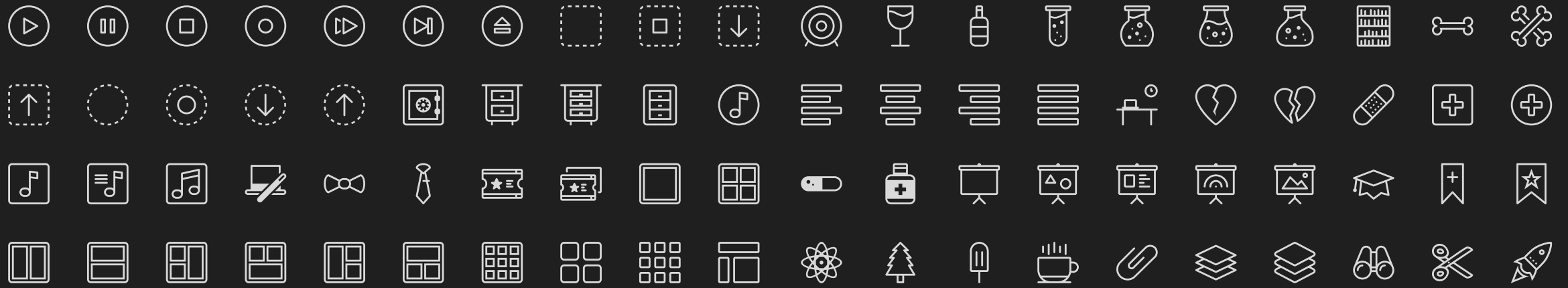
Questions?

Twitter: @JankeSkanke

Thank YOU

Twitter: @JankeSkanke

General

Electronics

Miscellaneous