

Welcome!!



SILVER SPONSOR



GOLD SPONSOR



6th-7th september



Florian Salzmann

Senior Workplace Consultant & MVP



@FlorianSLZ

From Detection to Resolution:

Harnessing the Power of (Proactive) Remediations in Intune



MODERN
ENDPOINT
MANAGEMENT

SUMMIT 2023

6th-7th september

Agenda

01

What are Remediations

Overview, Requirements and where to find them

02

Basics

How they work and how to build a simple package

03

Samples & Demo

Some real world samples

04

Troubleshooting & Demo

What if it something goes wrong?



MODERN
ENDPOINT
MANAGEMENT

SUMMIT 2023

Name changes ;)

① Important

Proactive
Remediation
with Remediation
and other



from Devices >
n are replaced
bear in some blogs

What are Remediations?

- Automatic **Detection** and **Remediation** of issues
- Measurement of desired status configurations
- End-user assessment and notification
- Significantly reduce the number of potential helpdesk calls

Prerequisites



- Device is Azure AD joined or hybrid Azure AD joined
 - enrolled in Intune
 - Co-managed
- Windows 10, version 1903+
- Windows Enterprise or Education (or Pro)

Licences

- Windows 10/11 Enterprise E3, E5 included in Microsoft 365 F3, E3, E5
- Windows 10/11 Education A3, A5 included in Microsoft 365 A3, A5
- Windows 10/11 Virtual Desktop Access (VDA) per user

no support for Microsoft 365 Business Premium 😞

Limitations & point to consider

- Max. 200 script packages per tenant
- Updates every 8h (IntuneManagementExtension)
- Output online max 2048 characters
- Default mode is 32bit



You found them here

Reports

Search (Ctrl+/)

Overview

Device management

Device compliance

Group policy analytics (preview)

Windows updates (preview)

Cloud attached devices (preview)

Endpoint security

Microsoft defender antivirus

Firewall

Analytics

Endpoint analytics

Intune data warehouse

Data warehouse

Azure monitor

Diagnostic settings

Log analytics

Workbooks

Endpoint analytics | Proactive remediations

Search (Ctrl+/) Refresh Create script package Columns

Overview Settings

Reports

Proactive remediations

Recommended software

Create and run script packages on devices to proactively find and fix the top support issues in your organization. Use this table to see the status of your deployed script packages and to monitor the detection and remediation results. Results are shown as number of devices affected. [Learn more](#)

Search by script package name

Script package name	Author	Status	Without issues	With issues
Restart stopped Office C2R svc	Microsoft	Not deployed	0	0
Update stale Group Policies	Microsoft	Not deployed	0	0

And now here ...

Home > **Devices**

Devices | Remediations

Search



Refresh



Create script package



Columns

Provisioning

Windows 365

Policy

Compliance policies

Conditional access

Configuration profiles

Scripts









Remediations

Group Policy analytics (preview)

Update rings for Windows 10 and later

Create and run script packages on devices to proactively find and fix the top support issues in your organization. Use this table to see the status of your deployed script packages and to monitor the detection and remediation results. Results are shown as number of devices affected. [Learn more.](#)

Search by script package name

Script package name 	Author	Status	Without issues 	With issues 
Restart stopped Office C2R svc	 Microsoft	 Not deployed	0	0
Update stale Group Policies	 Microsoft	 Not deployed	0	0
WIN-PR-OutlookSignatur	Florian Salzmann	 Active	0	0



... or

Home > **Devices | Windows** > Windows

Windows | Scripts

Search

Windows devices

Windows enrollment

Windows policies

Compliance policies

Configuration profiles

Scripts

Update rings for Windows 10 and later

Feature updates for Windows 10 and later

Quality updates for Windows 10 and later

Driver updates for Windows 10 and later

Remediations Platform scripts

Create and run script packages on devices to proactively find and fix the top support issues in organization. Use this table to see the status of your deployed script packages and to monitor detection and remediation results. Results are shown as number of devices affected. [Learn more](#)

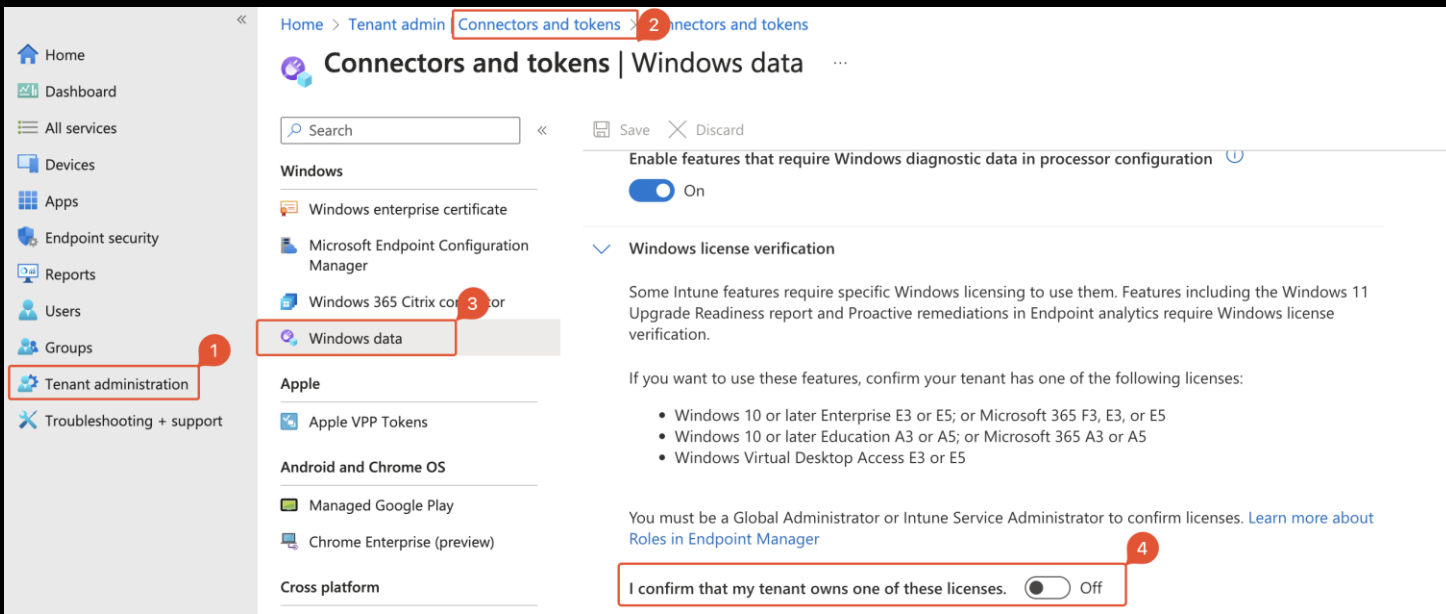
+ Create Refresh Export Columns 4 script packages

Search Add filters

Script package	Author	Status	Without issues	With issues	Issue fixed
PR-WIN-OutlookSignatureSync_OFF	Florian Salzmänn	Active	0	0	0
PR-WIN-q	Florian Salzmänn	Active	0	0	0
Restart	Microsoft	Not	0	0	0

activate Remediations

- Tenant administration >
- Connectors and tokens >
- Windows data >



Home > Tenant admin > Connectors and tokens > 2 Connectors and tokens

Connectors and tokens | Windows data

Search Save Discard

Windows

- Windows enterprise certificate
- Microsoft Endpoint Configuration Manager
- Windows 365 Citrix connector 3
- Windows data

Apple

- Apple VPP Tokens

Android and Chrome OS

- Managed Google Play
- Chrome Enterprise (preview)

Cross platform

Enable features that require Windows diagnostic data in processor configuration ☒ On

Windows license verification

Some Intune features require specific Windows licensing to use them. Features including the Windows 11 Upgrade Readiness report and Proactive remediations in Endpoint analytics require Windows license verification.

If you want to use these features, confirm your tenant has one of the following licenses:

- Windows 10 or later Enterprise E3 or E5; or Microsoft 365 F3, E3, or E5
- Windows 10 or later Education A3 or A5; or Microsoft 365 A3 or A5
- Windows Virtual Desktop Access E3 or E5

You must be a Global Administrator or Intune Service Administrator to confirm licenses. [Learn more about Roles in Endpoint Manager](#)

I confirm that my tenant owns one of these licenses. ☐ Off 4

Basics

Detection

Exit 0 = all good.

Exit 1 = Remediation needed


Remediation

optional

→ After execution, the detection is triggered again

File formatting matters

1_dummy-UTF8BOM.ps1



```
ï»¿# This is a dummy PS1
$website = "scloud.work"
$location = "CH"

try{
    if(Test-Connection $website){
        Write-Output "Website available: $website"
    }
}
```

save

from scripts you've written. By default, scripts will run on assigned devices every day.

Select a file

```
ï»¿# This is a dummy PS1
$website = "scloud.work"
$location = "CH"

try{
    if(Test-Connection $website){
        Write-Output "Website available: $website"
    }
}
```

Detection script

Outputs / Verbose

Can be used for reporting

- Don't use Write-Verbose or multiple Outputs
- Use only **one** Output Variable (last one will be used)
- Remember the Output Limit: 2048

```
Windows PowerShell
on." This event was no ordinary lawn mowing contest; it was Chuckleberry's way of celebrating the absurd and showcasing the town's unique sense of humor.

Wally rolled out of bed, put on his mismatched socks (one had polka dots, and the other had stripes), and donned his neon-green jumpsuit, covered in patches that read, "I Brake for Banana Peels" and "Caution: Prone to Puns." Armed with a lawnmower decked out in rainbow streamers, a rubber chicken hat, and a kazoo, he was ready to take on the competition.

As Wally arrived at the Chuckleberry Commons, the crowd erupted into laughter. They had come to expect the unexpected from Wally, and he never disappointed. The judges, a panel of clowns and comedians, raised their oversized scorecards, ready to rate each contestant on their mowing skills, creativity, and, of course, humor.

Wally's strategy was simple but effective. He started his mower, and instead of making a beeline for the grass, he zigzagged across the field while playing his kazoo at a pitch that only dogs could appreciate. Every few feet, he'd stop and tell a quick joke to the audience, like, "Why did the scarecrow win an award? Because he was outstanding in his field!"

The crowd roared with laughter, and even the stoic judges cracked smiles. As Wally continued his mowing routine, he unveiled a stream of puns and visual gags that left everyone in stitches. He juggled rubber chickens, did cartwheels while pushing the mower, and even attempted a lawnmower limbo.

But it was Wally's pièce de résistance that truly stole the show. With a dramatic flourish, he unveiled a remote-control led, dancing lawnmower decked out in a tutu. As the miniature mower twirled and sashayed across the grass to the tune of "The Can-Can," the audience erupted into applause. When it came time for the judges to announce the winner, there was no doubt in anyone's mind. Wally Whimsy had taken the crown once again. His performance had not only mowed the lawn, but had mowed down the competition with hilarity. As Wally accepted his trophy, a giant rubber chicken dressed as a butler handed him a bouquet of rubber daisies. He took a bow and said, "I'd like to dedicate this victory to my lawn, who's always been there for me, putting up with my antics. And to the people of Chuckleberry, who prove that laughter truly is the best fertilizer!" The entire town erupted into applause and laughter, celebrating another year of whimsy and wackiness. And as Wally rode off into the Chuckleberry sunset on his lawnmower, everyone knew that no matter what challenges lay ahead, as long as they had Wally Whimsy, they'd always find a reason to smile.
PS C:\Users\florian.salzmann>
```

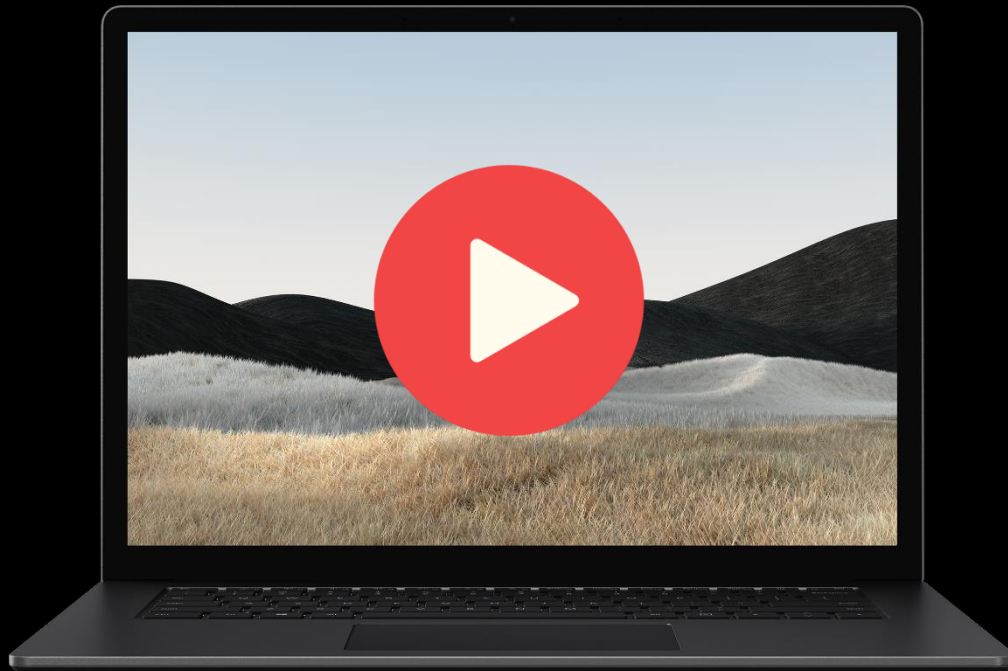


Pre-remediation detection output

LongOutput

But it was Wally's pièce de résistance that truly stole the show. With a dramatic flourish, he unveiled a remote-controlled, dancing lawnmower decked out in a tutu. As the miniature mower twirled and sashayed across the grass to the tune of "The Can-Can," the audience erupted into applause. When it came time for the judges to announce the winner, there was no doubt in anyone's mind. Wally Whimsy had taken the crown once again. His performance had not only mowed the lawn, but had mowed down the competition with hilarity. As Wally accepted his trophy, a giant rubber chicken dressed as a butler handed him a bouquet of rubber daisies. He took a bow and said, "I'd like to dedicate this victory to my lawn, who's always been there for me, putting up with my antics. And to the people of Chuckleberry, who prove that laughter truly is the best fertilizer!" The entire town erupted into applause and laughter, celebrating another year of whimsy and wackiness. And as Wally rode off into the Chuckleberry sunset on his lawnmower, everyone knew that no matter what challenges lay ahead, as long as they had Wally Whimsy, they'd always find a reason to smile.

Basis – Detection & Remediation



Samples and Template

Community Repository

[Endpoint Analysis Proactive Remediation Community Repo](#)

Some ideas

- Registry Keys
- Notifications
- Driver Updates
- Computer Uptime
- Emergency Updates
- Datacollection / Inventory
- Handling local Admins
- Bitlocker Key



Information

Your Download folder has more than 10 GB of data

Download folder size: 12.20 GB

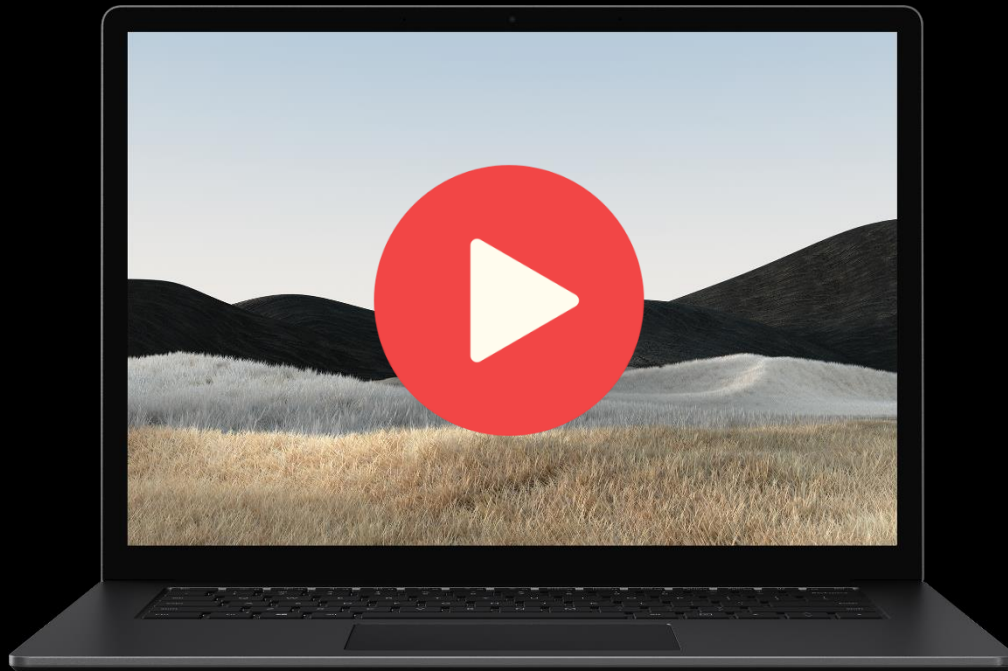
Please consider cleaning it up or moving the data to your Documents. The data in this folder is not protected or backed up.

Open

Delete all

Ignore

Sample – RegKey



Monitoring



Use just a detection to monitor states

Example: BitLocker Key

Why?

Scope Tags do not apply to BitLocker (Entra ID)

Troubleshooting

Health scripts local:

- C:\Windows\IMECache\HealthScripts
- **Cleartext...** so please, no secrets or sensitive data!

Logs:

- C:\ProgramData\Microsoft\IntuneManagementExtension\Logs \ Intunema...

Local history and status:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\IntuneManagementExtension\SideCarPolicies\Scripts

Troubleshooting – locally

Script output in registry:

HKLM:\SOFTWARE\Microsoft\IntuneManagementExtension\SideCarPolicies\Scripts\Reports\<USER_GUID>\<SCRIPT_ID>



File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\IntuneManagementExtension\SideCarPolicies\Scripts\Reports

- IntuneManagementExtension
 - Content
 - DownloadJobs
 - EspTrackingWin32Apps

Name	Type
ab (Default)	REG_SZ

Troubleshooting – locally

- Proxies
- RebootSettings
- sensor
- Settings
- SideCarPolicies
 - Scripts
 - Execution
 - Reports
 - 00000000-0000-0000-0000-000000000000
 - 6a39b22b-2eb3-4b9e-9ddb-1480b963ed2c_1
 - Result
 - 154ace5f-cf3f-4c08-a0eb-8a84d7081031
 - 639ee0ca-911f-48b2-a06f-25f1e86df4f7_1
 - 6a39b22b-2eb3-4b9e-9ddb-1480b963ed2c_5
 - Result

Device Scope

Script ID (Azure)

User Scope

Troubleshooting – locally



MODERN
ENDPOINT
MANAGEMENT

SUMMIT 2023

endpoint.microsoft.com/#view/Microsoft_Intune_Enrollment/UXAnalyticsScriptMenu/~./overview/id/639ee0ca-911f-48b2-a06f-25f1e86df4f7/scriptName/PR-WIN...

M365

Microsoft Intune admin center

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant admin

Troubleshooting

Home > Devices | Overview > Windows | Scripts >

PR-WIN-OutlookSignatureSync_OFF | Overview

Proactive remediations

Search

Delete

Overview

Manage

Properties

Monitor

This gives information about how your script package is performing and the health of your devices. The scripts run according to your defined scheduling preferences. The detection bar chart reflects the returned value from the detection script while the remediation bar chart describes the remediation script output. [Learn more.](#)

Detection status

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\IntuneManagementExtension\SideCarPolicies\Scripts\Reports\154ace5f-cf3f-4c08-a0eb-8a84d7081031\6a39b22b-2eb3-4b9e-9ddb-1480b963ed2c_5\Result

Scripts
Execution
Reports
00000000-0000-0000-0000-000000000000
6a39b22b-2eb3-4b9e-9ddb-1480b963ed2c_1
Result
154ace5f-cf3f-4c08-a0eb-8a84d7081031
639ee0ca-911f-48b2-a06f-25f1e86df4f7_1
6a39b22b-2eb3-4b9e-9ddb-1480b963ed2c_5
Result

Name	Type	Data
(Default)	REG_SZ	(value not set)
Result	REG_SZ	["PolicyId": "6a39b22b-2eb3-4b9e-9ddb-1480b963ed2c", "UserId": "154ace5f-cf3f-4c08-a0eb-8a84d7081031", "PolicyHash": null, "Result": 3, "ResultDetails": ...]

Troubleshooting – The PowerShell way



```
$User_id = "00000000-0000-0000-0000-000000000000"  
$Script_id = "xxx"  
$RegPath = "HKLM:\SOFTWARE\Microsoft\IntuneManagementExtension\SideCarPolicies\Scripts\Reports\$User_id\$Script_id\Result"  
  
Get-ItemProperty -Path $RegPath | Select-Object -ExpandProperty Result | ConvertFrom-Json | fl *Output*
```

To get all Scripts from all users:

[scloud/Proactive Remediation/localTroubleshooting_Remediations.ps1](#)

[FlorianSLZ/scloud \(github.com\)](#)

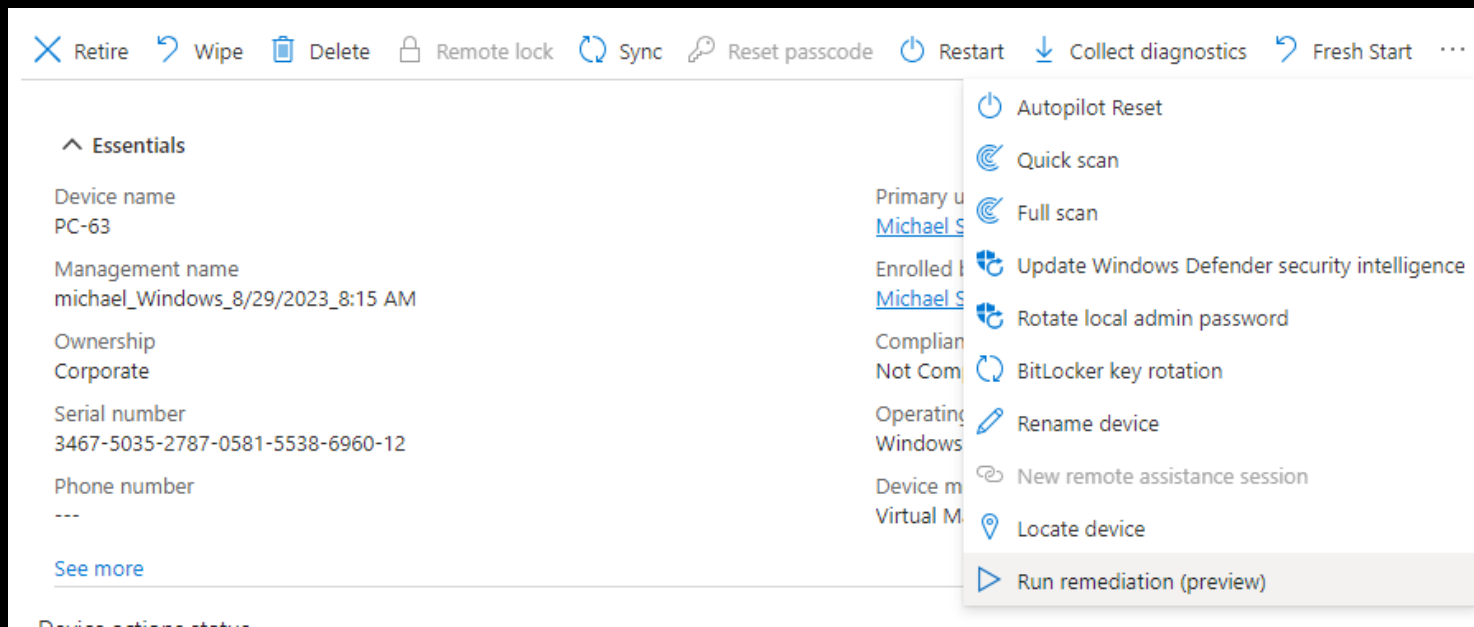
Troubleshooting – Force re-run

1. HKLM\SOFTWARE\Microsoft\IntuneManagementExtension\SideCarPolicies\Scripts

- **Execution\<USER_GUID>\<SCRIPT_ID>**
- **Reports\<USER_GUID>\<SCRIPT_ID>**

2. Restart IME

→ Or...
run them manually



Retire Wipe Delete Remote lock Sync Reset passcode Restart Collect diagnostics Fresh Start ...

Essentials

Device name
PC-63

Management name
michael_Windows_8/29/2023_8:15 AM

Ownership
Corporate

Serial number
3467-5035-2787-0581-5538-6960-12

Phone number

See more

Primary user
Michael S

Enrolled by
Michael S

Compliance
Not Compliant

Operating system
Windows 10

Device model
Virtual Machine

Autopilot Reset

Quick scan

Full scan

Update Windows Defender security intelligence

Rotate local admin password

BitLocker key rotation

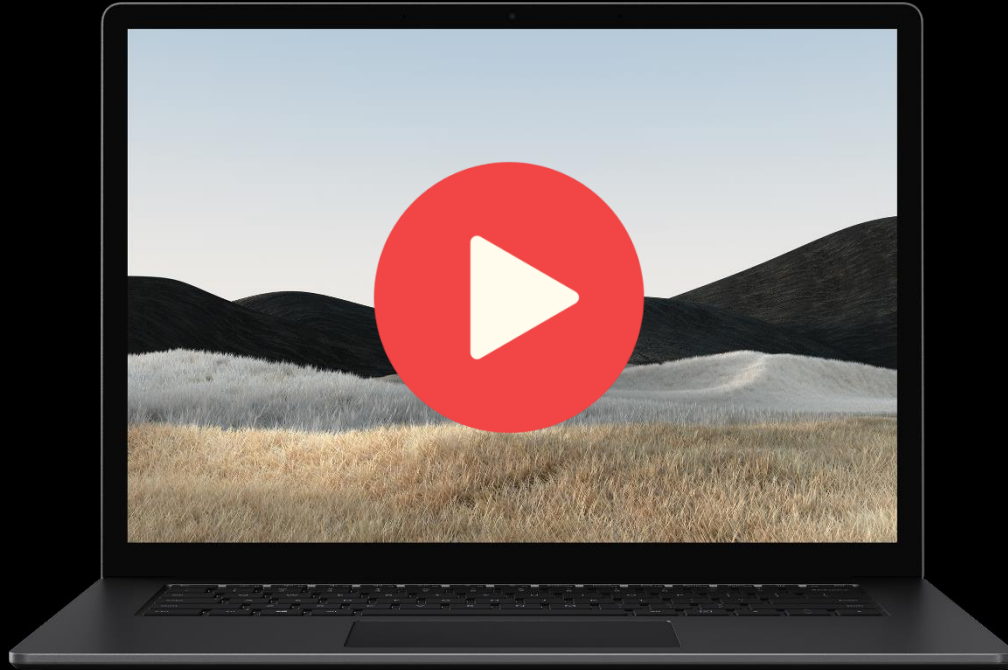
Rename device

New remote assistance session

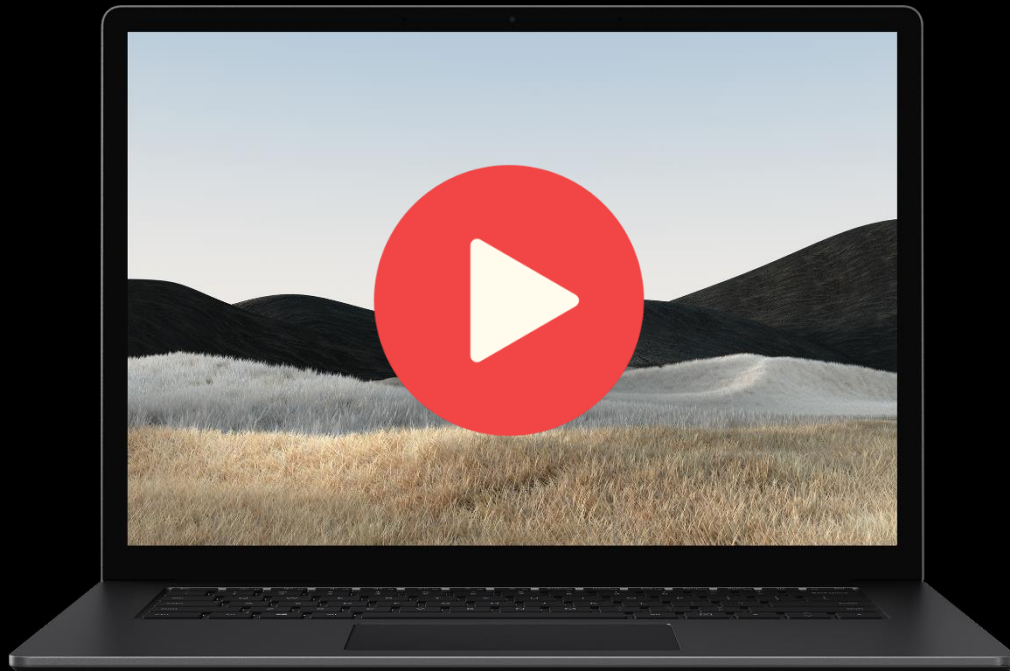
Locate device

Run remediation (preview)

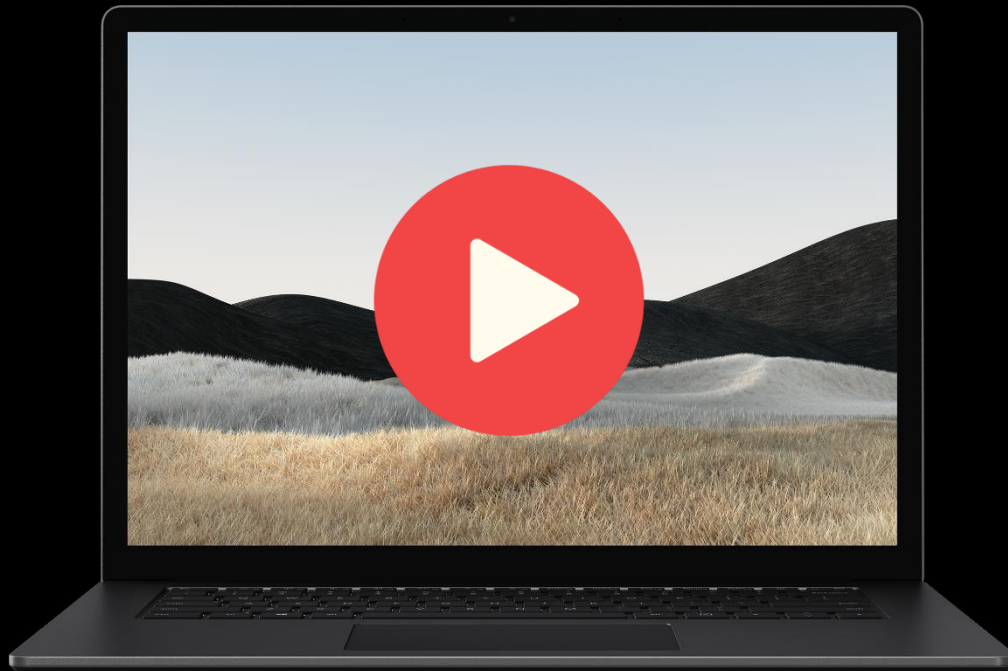
Sample – User notification



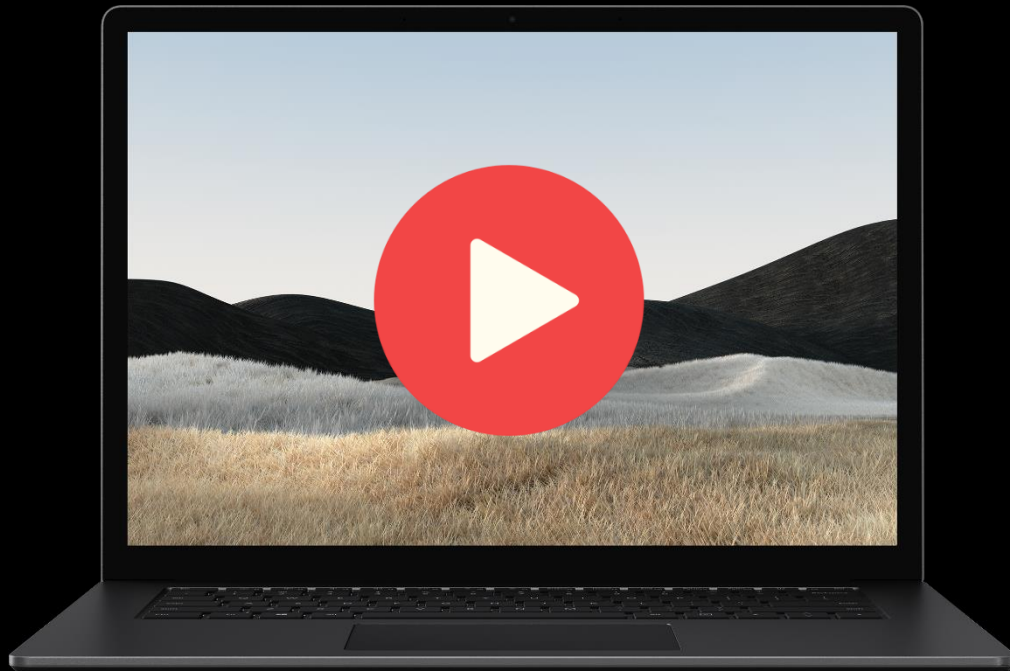
Sample – Admin for LAPS



Sample – Office Updates

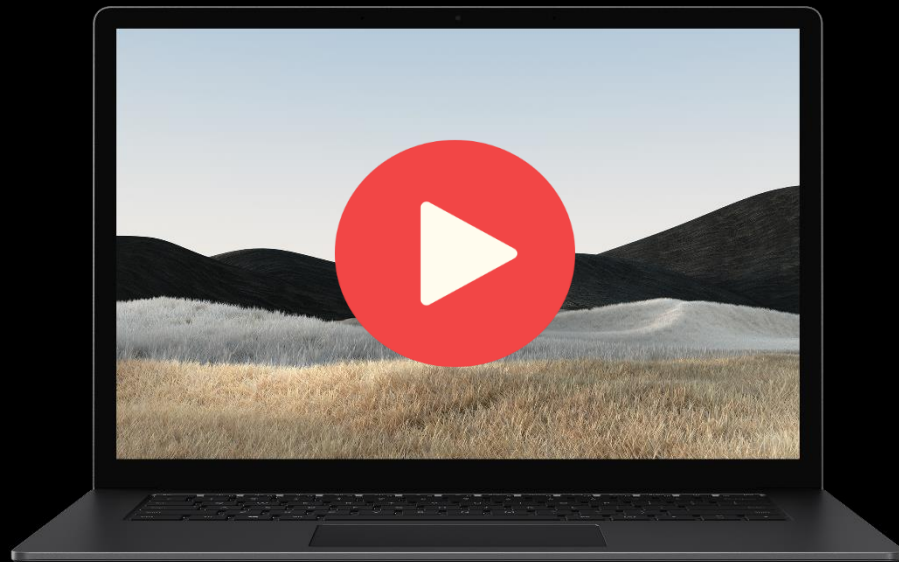


Sample – Winget updates



Bonus: Proactive Remediations for Business

["Proactive Remediation for Business" | scloud](#)





Presentation
and Scripts

That's it, thanks for sticking around 🖐️

Thank you!!



SILVER SPONSOR



GOLD SPONSOR



6th-7th september