
# Taming Windows 11

*An Intune Adventure*

# Sponsors


onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

Rimo3

robopack

numecent

Microsoft

**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

# That's me

**Florian Salzmann**
Microsoft MVP · Endpoint & Security

**Role**
Leading Expert at UMB AG, Switzerland

**Focus**
Intune · Windows 365 · Security

**Blog, Hobbies and more**
- All thins Tech
- Travel
- Wine
- scloud.work / msnugget.com


# Time Zone & Regional Settings

# Harder Than You Think


- Auto time zone detection depends on the Windows Location Service
  - Location Service is often disabled by policy, blocked by firewall
- Wrong time zone = confused users = Tickets

# Your Options


- Settings Catalog = Fixed by Policy
- Enable  Privacy Settings, so the User can active the Location service = Bad User Experience
- Enable Location Service by Policy
- Script it :)


# Demo

Time Zone By Script

```
Administrator: C:\Program Files\PowerShell\7\pwsh.exe
PS C:\tmp> .\Set-TimeZoneByIPAddress.ps1
Transcript started, output file is C:\ProgramData\Microsoft\In
t.log
Fetching IANA time zone from ipinfo.io...
Detected IANA Time Zone: Europe/Zurich
Downloading custom XML mapping...
Searching for matching mapping...
Mapped to Windows Time Zone: W. Europe Standard Time
Setting Windows time zone using Set-TimeZone...
Successfully set Windows Time Zone: W. Europe Standard Time
```

File Edit Selection View ··· Search

Set-TimeZoneByIPAddress.ps1

C: > tmp > Set-TimeZoneByIPAddress.ps1 > ...

```powershell
    if (-not $windowsZones) {
        throw "Failed to download or parse the XML mapping file."
    }

    Write-Output "Searching for matching mapping..."
    $mapping = $windowsZones.supplementalData.windowsZones.mapTimezones.mapZone | Where-Object {
        $_.type -split ' ' -contains $ianaTz
    }

    if (-not $mapping) {
        throw "No mapping found for IANA time zone: $ianaTz"
    }

    $windowsTZ = $mapping.other | Select-Object -First 1
    Write-Output "Mapped to Windows Time Zone: $windowsTZ"

    try {
        Write-Output "Setting Windows time zone using Set-TimeZone..."
        Set-TimeZone -Id $windowsTZ
        Write-Output "Successfully set Windows Time Zone: $windowsTZ"
    } catch {
        Write-Error "Set-TimeZone failed. "
    }

} catch {
    Write-Error "Failed to set Windows time zone: $_"
}
```

0 0 Ln 30, Col 46 Spaces: 4 UTF-8 LF { } PowerShell

# Locale, Language, Input

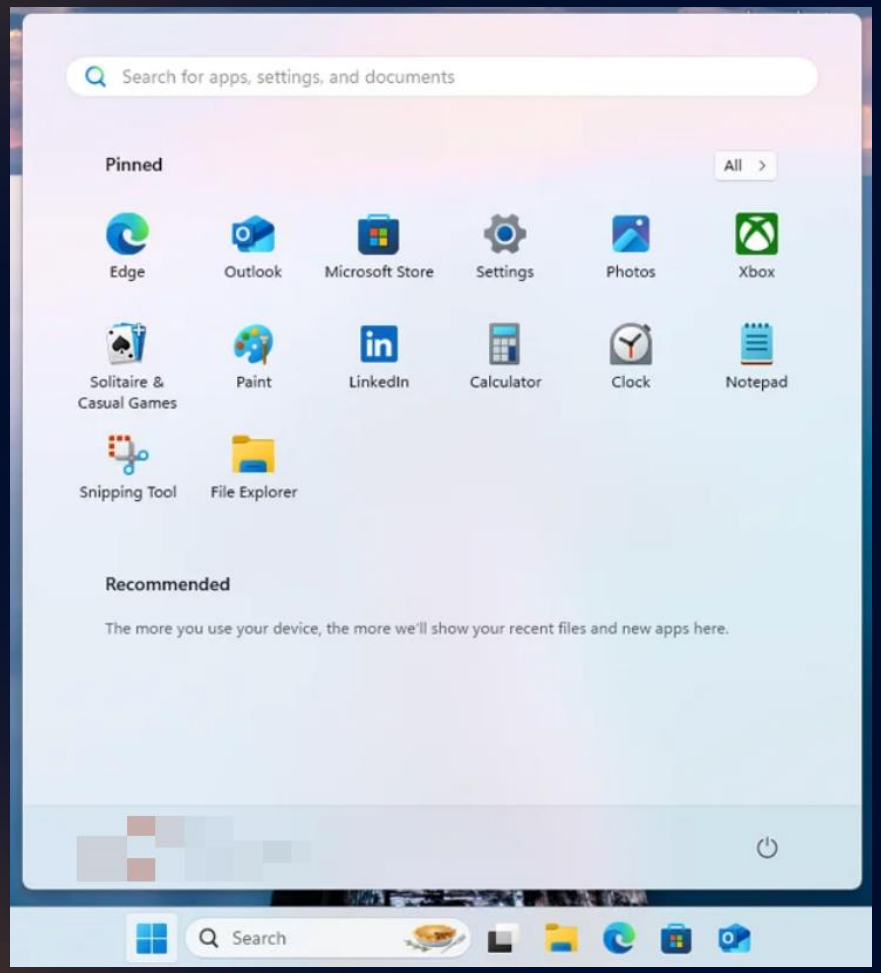

- System locale vs. user locale vs. display language: three different things
- Settings Catalog covers display language and input language
- System locale and regional format (date/currency) often still need PowerShell or provisioning packages

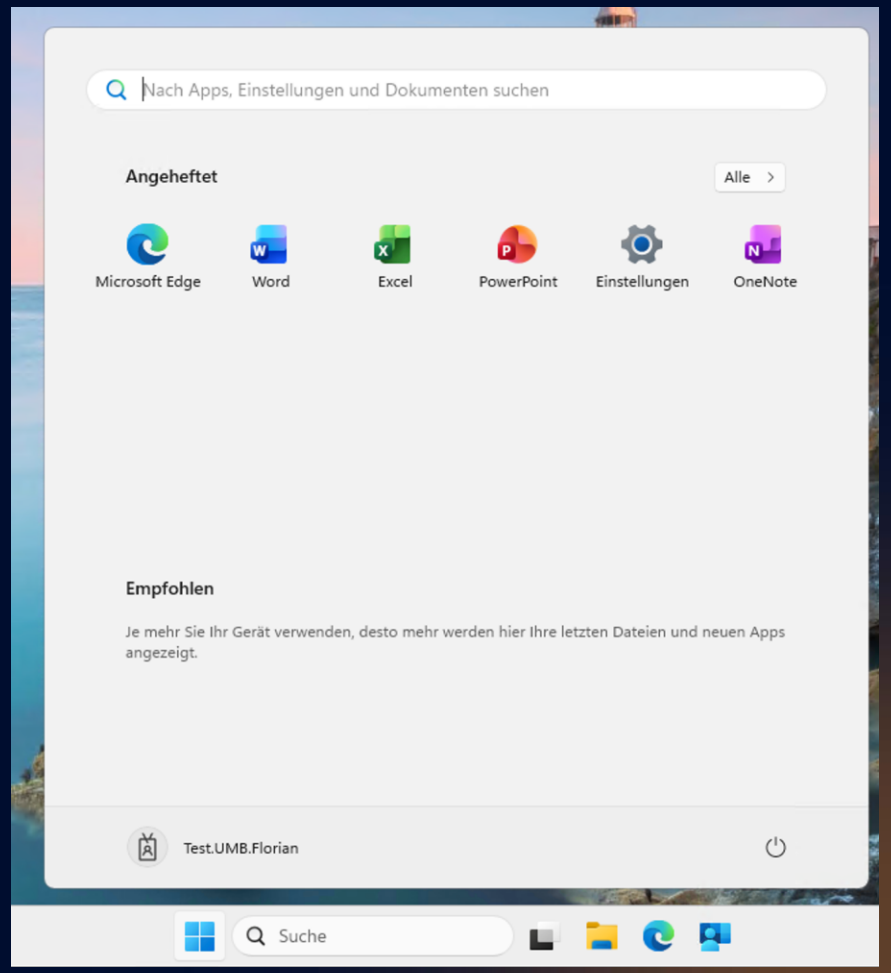
# Common Pitfalls


- For multi-language orgs: deploy language packs alongside regional config
- Watch out: some LOB apps read system locale, others read user locale
  - !! Test both


# Windows Start Menu

# The Goal


Search for apps, settings, and documents
Pinned
All
Edge
Outlook
Microsoft Store
Settings
Photos
Xbox
Solitaire & Casual Games
Paint
LinkedIn
Calculator
Clock
Notepad
Snipping Tool
File Explorer
Recommended
The more you use your device, the more we'll show your recent files and new apps here.
Search

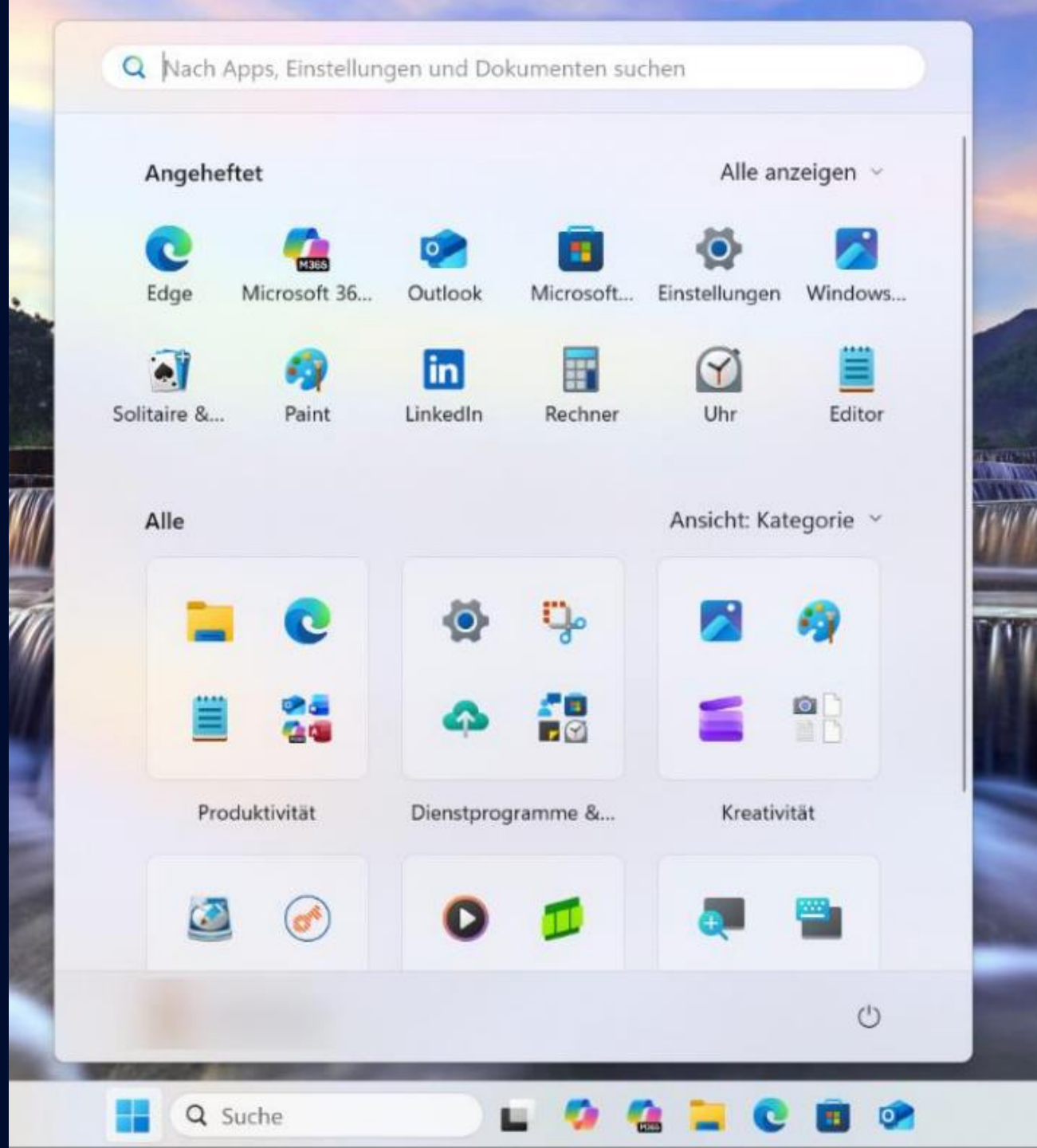

Nach Apps, Einstellungen und Dokumenten suchen
Angeheftet
Alle
Microsoft Edge
Word
Excel
PowerPoint
Einstellungen
OneNote
Empfohlen
Je mehr Sie Ihr Gerät verwenden, desto mehr werden hier Ihre letzten Dateien und neuen Apps angezeigt.
Test.UMB.Florian
Suche

# What's New?


- Windows 10 used XML-based LayoutModification.xml — deprecated in Windows 11
- Windows 11 introduced JSON-based layout configuration
- New "Recommended" section, new pinning behaviour, new headaches
- Admins need a fresh approach for managed desktops

# Heads Up

- New Options Design is coming in Q2
- You can control it
  *--> "HideCategoryView"*



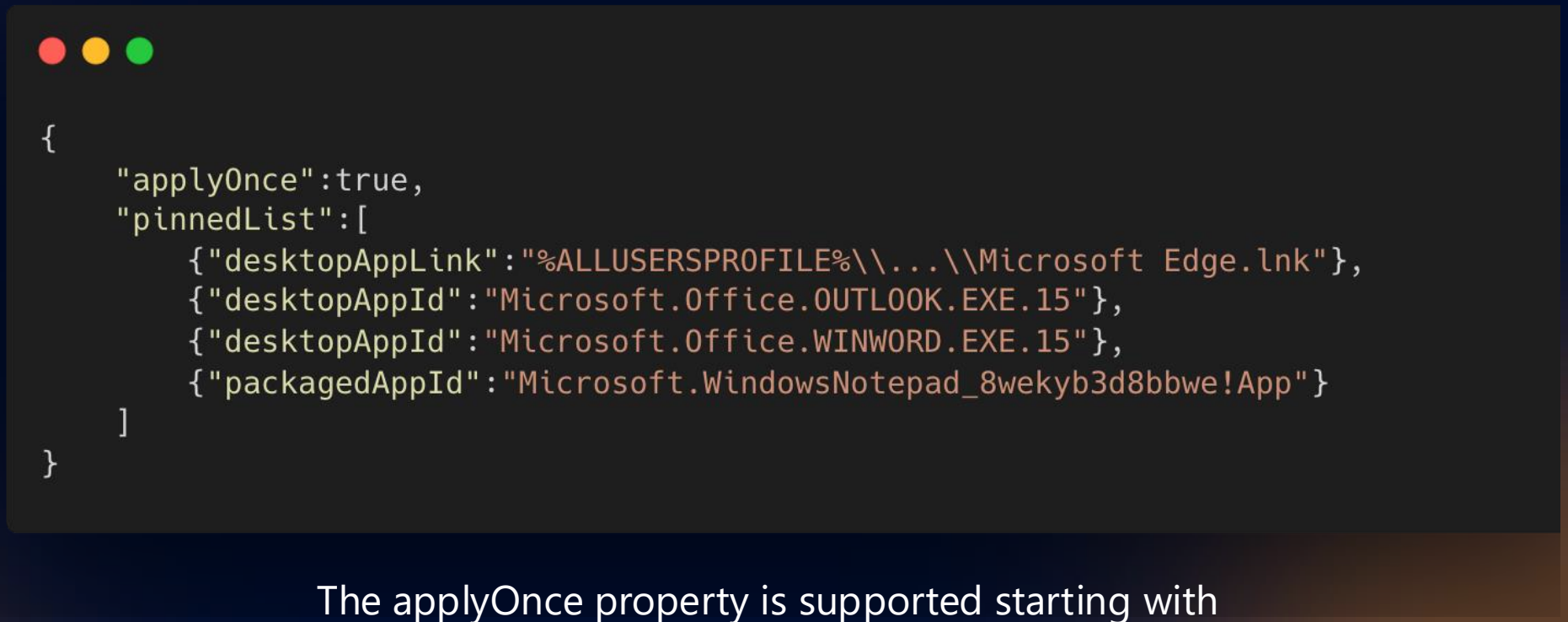
# How Can We Manage This via Intune?


- Settings Catalog: ConfigureTaskbarPins (JSON-based)
- Settings Catalog: Start Menu layout (pinned apps, folder groups)

- Full lockdown vs. partial layout (forced vs. user-customisable)
- Key decision: do you want total control or a sensible default users can tweak?

# JSON Setting

**Export-StartLayout** -Path "C:\YourStartMenuLayout.json"



```
{
    "applyOnce":true,
    "pinnedList":[
        {"desktopAppLink":"%ALLUSERSPROFILE%\\...\\Microsoft Edge.lnk"},
        {"desktopAppId":"Microsoft.Office.OUTLOOK.EXE.15"},
        {"desktopAppId":"Microsoft.Office.WINWORD.EXE.15"},
        {"packagedAppId":"Microsoft.WindowsNotepad_8wekyb3d8bbwe!App"}
    ]
}
```

The applyOnce property is supported starting with Windows 11, version 24H2 with KB5062660, and it's ignored on earlier versions of Windows 11.

# Start Menu "Set Once" Option


- PowerShell to the rescue :)
- Set the Default User Start Menu

# Set Menu once with PowerShell


```
Copy-Item "Start2.bin"
-Destination
"C:\Users\Default\AppData\Local\Packages\Microsoft.Windows.StartMenuExperienceHos
t_cw5n1h2txyewy\LocalSta
te\Start2.bin"
```

**Why?**

Changes on this file will only affect new users

# Taskbar Pinning


- JSON defines which apps appear pinned on the Taskbar
- Apps must be installed on the device, otherwise the pin silently fails

- Blue = Windows Default
- Red = User choice
- Green = Policy

# Who wants Taskbar Pins backed up in Windows Backup for Orgs?


# Windows Backup for Organizations

# Restore my stuff during OOBE.. YES please!


- Tenant-wide
- Supports CloudPCs (at first sign in after device enrollment)
- Windows Backup app is installed with the backup policy
- Combine with MS Edge Enterprise sync?

# How it works


## Backup

1. We must enable and configure a backup policy
2. A scheduled task will initiate the backup of a Windows device
   Every 8 days
3. Optional: Use the Windows Backup app to manually initiate a backup

## Restore

1. We must enable and configure a restore policy
2. User signs in during OOBE
3. Restore page is shown

RE-APv1-02 on RE-CNRMTQ3 - Virtual Machine Connection

File Action Media Clipboard View Help

# Let's set things up for your work or school

You'll use this info to sign in to your devices.

RockEnroll.tech

nicklas@nicklasahlberg.se

## Enter password

••••••••••

Forgot my password

Sign in another way

Sign in

Status: Running

MODERN ENDPOINT MANAGEMENT SUMMIT 2026

RE-APv1-02 on RE-CNRMTQ3 - Virtual Machine Connection

File Action Media Clipboard View Help

## Welcome back, Nicklas!

There's a backup of your previous PC which may have settings and Microsoft Store apps saved. We can bring over your info to this PC once you finish your setup. Privacy Statement

Restore from your PC backup

CPC-MALMO-WKK64
Last backup: January 19, 2026

More options

Learn more

Continue

Status: Running

RE-APv1-02 on RE-CNRMTQ3 - Virtual Machine Connection

File Action Media Clipboard View Help

## Setting up for work or school

This will take a few minutes. Your device might need to restart as we complete the setup.

**Device preparation**
Working on it...

**Device setup**
Waiting

**Account setup**
Waiting

Status: Running

MODERN ENDPOINT MANAGEMENT SUMMIT 2026

# Enterprise State Roaming (ESR)


- Moving to Backup for organizations
- We have until June 2026 to move the policies

💡 If you take no action, Windows will honor both ESR and GPO/MDM roaming controls for one year (prioritizing GPO/MDM); after that, ESR will no longer work, and roaming must be managed through Windows Backup for Organizations policies.


# Windows First Sign-in Restore

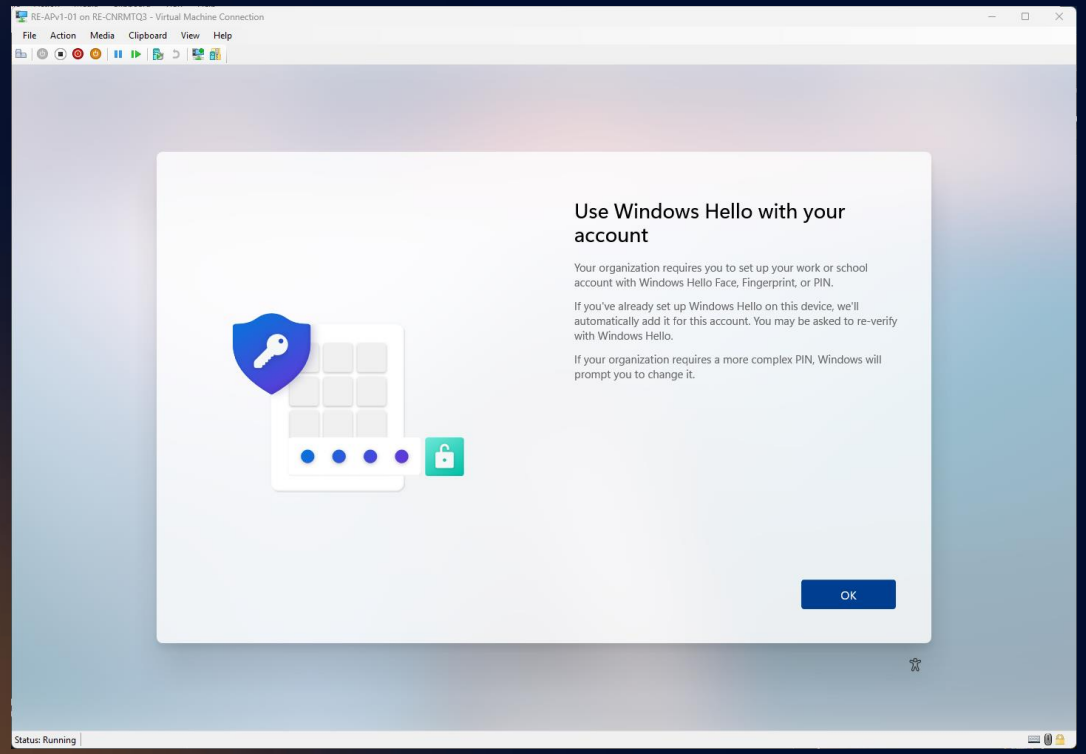
# At first sign in instead of during OOBE

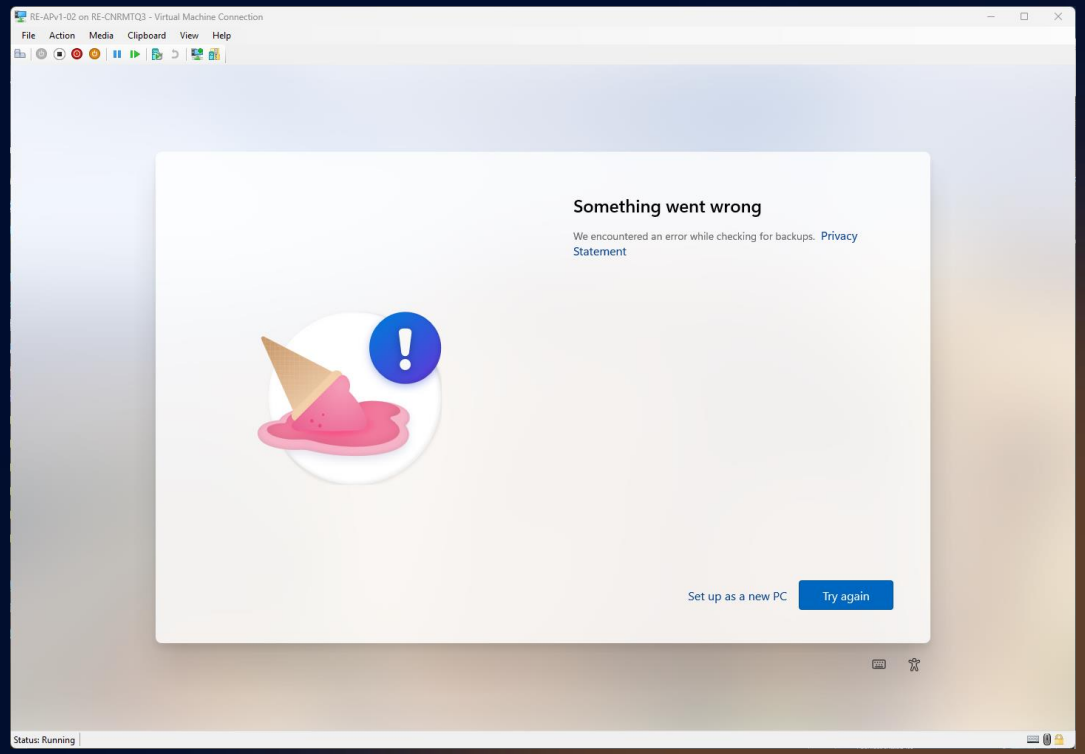

- Restore your stuff at first sign-in instead of during OOBE
- If a user decides not to restore during OOBE, this is honored
- during first sign-in as well
- Enabled per group instead of tenant-wide
- Requires Windows 11 24H2/25H2 and **2026-03** CU

💡 Make sure backups have been taken.. no backup = nothing to restore

# Good to know

- Phishing resistant MFA is supported. Remember to exclude d32c68ad-72d2-4acb-a0c7-46bb2cf93873 from CA



RE-APv1-02 on RE-CNRMTQ3 - Virtual Machine Connection

File Action Media Clipboard View Help

## Something went wrong

We encountered an error while checking for backups. Privacy Statement

Set up as a new PC | Try again

Status: Running

MODERN ENDPOINT MANAGEMENT SUMMIT 2026

**Assignments**

**User**
Weak Weaksson — Matched

**Resource**
Microsoft Activity Feed Service — Matched

All resources included

| Audience | Application Id |
|---|---|
| Microsoft Activity Feed Service | d32c68ad-72d2-4acb-a0c7-46bb2cf93873 |

**Conditions**

**Sign-in risk**
None — Not configured

**Device platform**
Windows10 — Not configured

**Network (formerly location)** — Not configured

**Client app**
Browser — Not configured

**Device** — Not configured

**User risk** — Not configured

**Insider risk** — Not configured

**Authentication flows** — Not configured

**Access controls**

**Grant Controls** — Not satisfied

Require Authentication strength - Phishing-resistant MFA: The user could satisfy this authentication strength by registering for one or more MFA methods.
Require compliant device

**Session Controls** — Not configured

Name *
CA004 - UAT - Enforce WHfB

Assignments

Users or agents (Preview)
Specific users included and specific users excluded

Target resources
All resources (formerly 'All cloud apps') included and 2 resources excluded

Network NEW
Not configured

...itions
0 conditions

Access controls

Grant *
2 controls selected

Session *
0 controls selected

Select what this policy applies to
Resources (formerly cloud apps)

Include | Exclude

Select the re... exempt from the policy

- None
- All internet resources with Global Secure Access
- All agent resources (Preview)
- Select resources

Select resources based on attributes
None

Select specific resources
Microsoft App Access Panel and ...

MA Microsoft Activity Feed Service
d32c68ad-72d2-4acb-a0c7-46bb2cf93873

MA Microsoft App Access Panel
0000000c-0000-0000-c000-0000000000...

To create a Conditional Access policy targeting members in your tenant with Global Secure Access (GSA) as a resource, make sure GSA is deployed in your tenant. Learn more

RE-APv1-02 on RE-CNRMTQ3 - Virtual Machine Connection

File Action Media Clipboard View Help

## Welcome back, Weak!

There's a backup of your previous PC which may have settings and Microsoft Store apps saved. We can bring over your info to this PC once you finish your setup. Privacy Statement

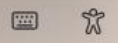
Restore from your PC backup

RE-292857755588
Last backup: April 18, 2026

More options

Learn more

Continue




Status: Running


# Remove Built in Apps

*The modern way....*

# Requirements


- Windows Enterprise and Education, no Pro support
- Windows 25H2 or newer

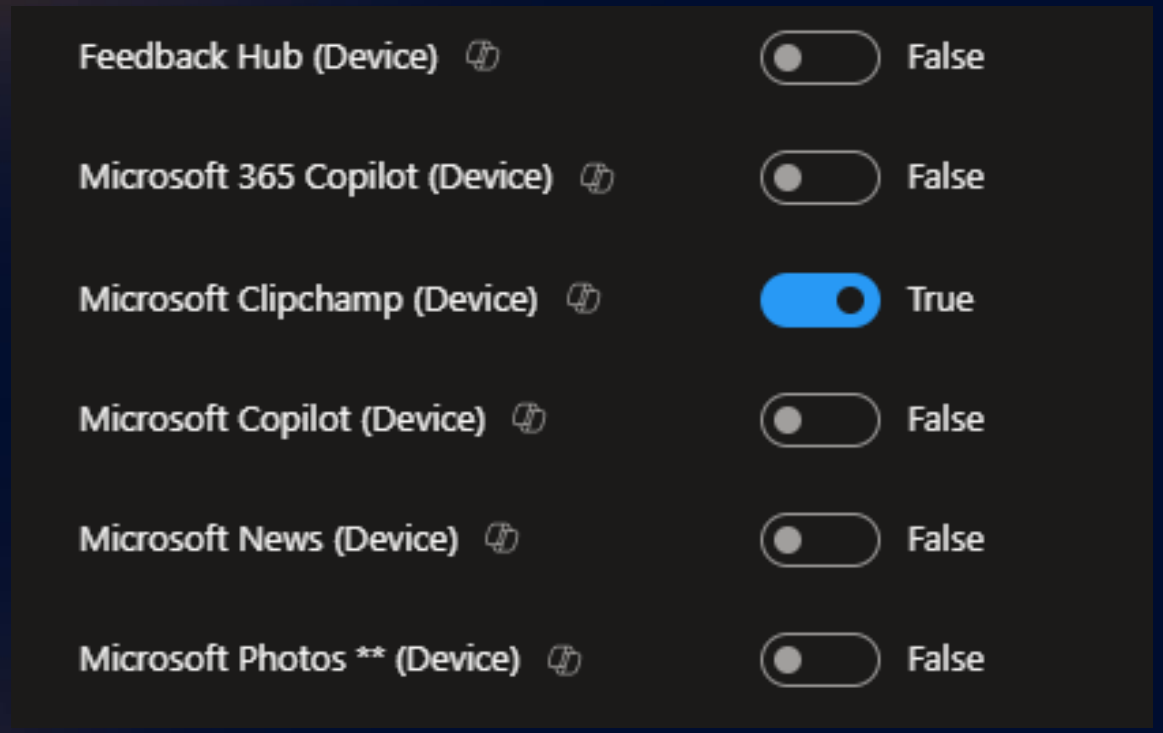
**Applied at**:

- Out-of-box experience (OOBE)
- User sign-in after an OS upgrade
- User sign-in after an update to the policy

💡 The policy-based in-box app removal feature doesn't support multi-session environments.

💡 Policy is removed on device level. All users on same device will lose the app once removed.

Administrative templates -> Windows components -> App package deployment -> **Remove Default Microsoft Store packages from the system**




True = Remove

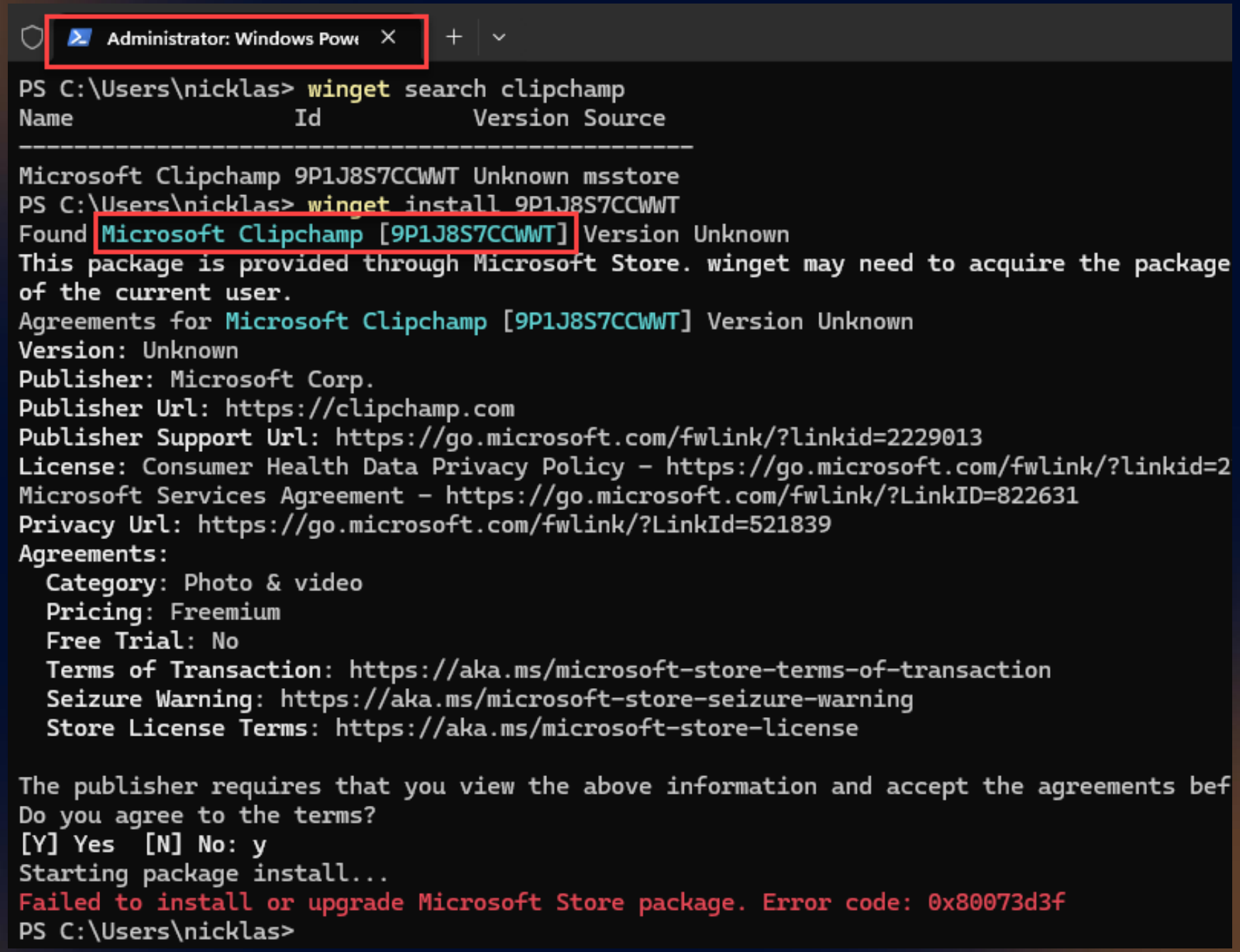
False = Keep

# HKLM:\Software\Policies\Microsoft\Windows\Appx**RemoveDefaultMicrosoftStorePackage**

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Appx\RemoveDefaultMicrosoftStorePackages

- RemoveDefaultMicrosoftStorePackages
  - Clipchamp.Clipchamp_yxz26nhyzhsrt
  - Microsoft.BingNews_8wekyb3d8bbwe
  - Microsoft.BingWeather_8wekyb3d8bbwe
  - Microsoft.Copilot_8wekyb3d8bbwe
  - Microsoft.GamingApp_8wekyb3d8bbwe
  - Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe
  - Microsoft.MicrosoftSolitaireCollection_8wekyb3d8bbwe
  - Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe
  - Microsoft.OutlookForWindows_8wekyb3d8bbwe
  - Microsoft.Paint_8wekyb3d8bbwe
  - Microsoft.ScreenSketch_8wekyb3d8bbwe
  - Microsoft.Todos_8wekyb3d8bbwe
  - Microsoft.Windows.Photos_8wekyb3d8bbwe
  - Microsoft.WindowsCalculator_8wekyb3d8bbwe
  - Microsoft.WindowsCamera_8wekyb3d8bbwe
  - Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe
  - Microsoft.WindowsNotepad_8wekyb3d8bbwe
  - Microsoft.WindowsSoundRecorder_8wekyb3d8bbwe
  - Microsoft.WindowsTerminal_8wekyb3d8bbwe
  - Microsoft.Xbox.TCUI_8wekyb3d8bbwe
  - Microsoft.XboxIdentityProvider_8wekyb3d8bbwe
  - Microsoft.XboxSpeechToTextOverlay_8wekyb3d8bbwe
  - Microsoft.ZuneMusic_8wekyb3d8bbwe
  - MicrosoftCorporationII.QuickAssist_8wekyb3d8bbwe
  - MSTeams_8wekyb3d8bbwe

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| Enabled | REG_DWORD | 0x00000001 (1) |


Administrator: Windows Powe
PS C:\Users\nicklas> winget search clipchamp
Name Id Version Source
Microsoft Clipchamp 9P1J8S7CCWWT Unknown msstore
PS C:\Users\nicklas> winget install 9P1J8S7CCWWT
Found Microsoft Clipchamp [9P1J8S7CCWWT] Version Unknown
This package is provided through Microsoft Store. winget may need to acquire the package
of the current user.
Agreements for Microsoft Clipchamp [9P1J8S7CCWWT] Version Unknown
Version: Unknown
Publisher: Microsoft Corp.
Publisher Url: https://clipchamp.com
Publisher Support Url: https://go.microsoft.com/fwlink/?linkid=2229013
License: Consumer Health Data Privacy Policy - https://go.microsoft.com/fwlink/?linkid=2
Microsoft Services Agreement - https://go.microsoft.com/fwlink/?LinkID=822631
Privacy Url: https://go.microsoft.com/fwlink/?LinkId=521839
Agreements:
Category: Photo & video
Pricing: Freemium
Free Trial: No
Terms of Transaction: https://aka.ms/microsoft-store-terms-of-transaction
Seizure Warning: https://aka.ms/microsoft-store-seizure-warning
Store License Terms: https://aka.ms/microsoft-store-license
The publisher requires that you view the above information and accept the agreements bef
Do you agree to the terms?
[Y] Yes [N] No: y
Starting package install...
Failed to install or upgrade Microsoft Store package. Error code: 0x80073d3f
PS C:\Users\nicklas>


MODERN
ENDPOINT
MANAGEMENT
SUMMIT
2026


🛡️ Protects against credential theft, such as pass-the-hash

- **New installations:** Enabled by default on W11 (without UEFI lock)
- **Existing installations:** No change when updating to W11
- **Controls:** Security baseline, CSP, Settings Catalog, Account protection
- **UEFI lock:** Block remote disablement (Intune/script/GPO)
- **Hardware requirements:** FW, TPM (1.2 & 2.0), VBS, Secure Boot

> **Note**
>
> While Credential Guard is a powerful mitigation, persistent threat attacks will likely shift to new attack techniques, and you should also incorporate other security strategies and architectures.

- We can
- Intune re
configur

redential
e

**Device status**

Can't access company resources

This device does not meet CCMEXEC compliance and security policies. You need to make some changes to this device so that you can access company resources.

Turn on device encryption — More

Credential Guard is not enabled — Less

Please make sure that Credential Guard is enabled on your device. For more information, contact servicedesk

| | |
|---|---|
| Kernel DMA Protection | On |
| Virtualisation-based security | Running |
| Virtualisation-based security required security properties | Base Virtualisation Support, Secure Boot |
| Virtualisation-based security available security properties | Base Virtualisation Support, Secure Boot, DMA Protection, Secure Memory Overwrite, UEFI Code Readonly |
| Virtualisation-based security services configured | Credential Guard, Hypervisor enforced Code Integrity, Secure Launch |
| Virtualisation-based security services running | Hypervisor enforced Code Integrity, Secure Launch |
| Windows Defender Application Control policy | Enforced |

```powershell
# Custom Compliance Check for Credential Guard
1 reference
function Test-CredentialGuardCompliance {···
}

# Run the compliance check
$complianceResult = Test-CredentialGuardCompliance

# Create hash table for Intune reporting
$hash = @{
    CredentialGuardCompliant = $complianceResult.IsCompliant
    ConfigurationStatus = $complianceResult.ConfigurationStatus
    RuntimeStatus = $complianceResult.RuntimeStatus
    Timestamp = $complianceResult.Timestamp
}

# Add error information if present
if ($complianceResult.Error) {
    $hash.Error = $complianceResult.Error
}

# Return JSON for Intune
return $hash | ConvertTo-Json -Compress
```

# JSON


```
{
    "Rules": [
        {
            "SettingName": "CredentialGuardCompliant",
            "Operator": "IsEquals",
            "DataType": "Boolean",
            "Operand": true,
            "MoreInfoUrl": "https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/",
            "RemediationStrings": [
                {
                    "Language": "en_US",
                    "Title": "Credential Guard must be enabled and running. Current status: {ActualValue}.",
                    "Description": "Credential Guard provides enhanced security for domain credentials. Please refer to the link above for configuration steps."
                }
            ]
        }
    ]
}
```


# Windows 365 Data Protection

# Device redirection for cloud PCs

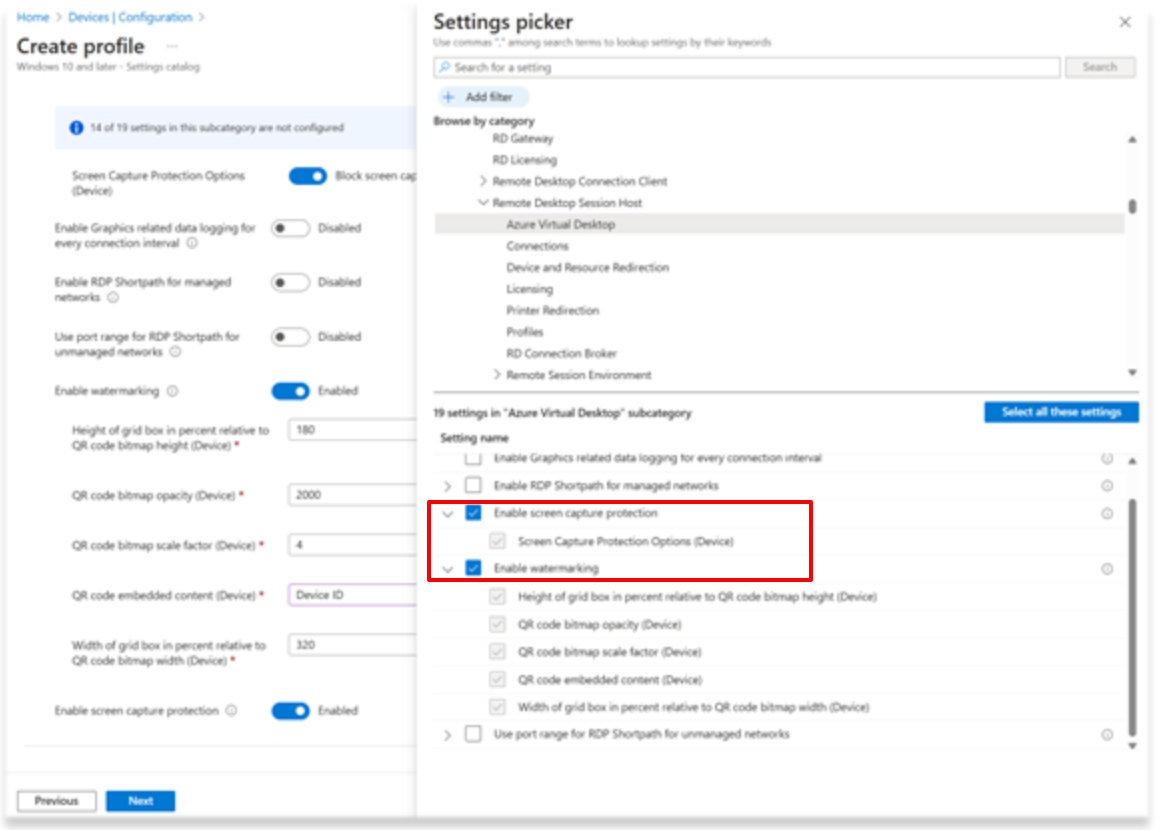

| Redirection | Policy |
|---|---|
| Audio input | Allow audio recording redirection |
| Audio output | Allow audio and video playback redirection |
| Cameras | Do not allow video capture redirection |
| Clipboard | Do not allow Clipboard redirection |
| COM ports | Do not allow COM port redirection |
| Drives | Do not allow drive redirection |
| Location | Do not allow location redirection |
| Printers | Do not allow client printer redirection |
| Smartcards | Do not allow smart card device redirection |
| USB drives | Do not allow supported Plug and Play device redirection |

# Data Protection

## Watermarking

Add traceable watermarks

## Screen capture protection

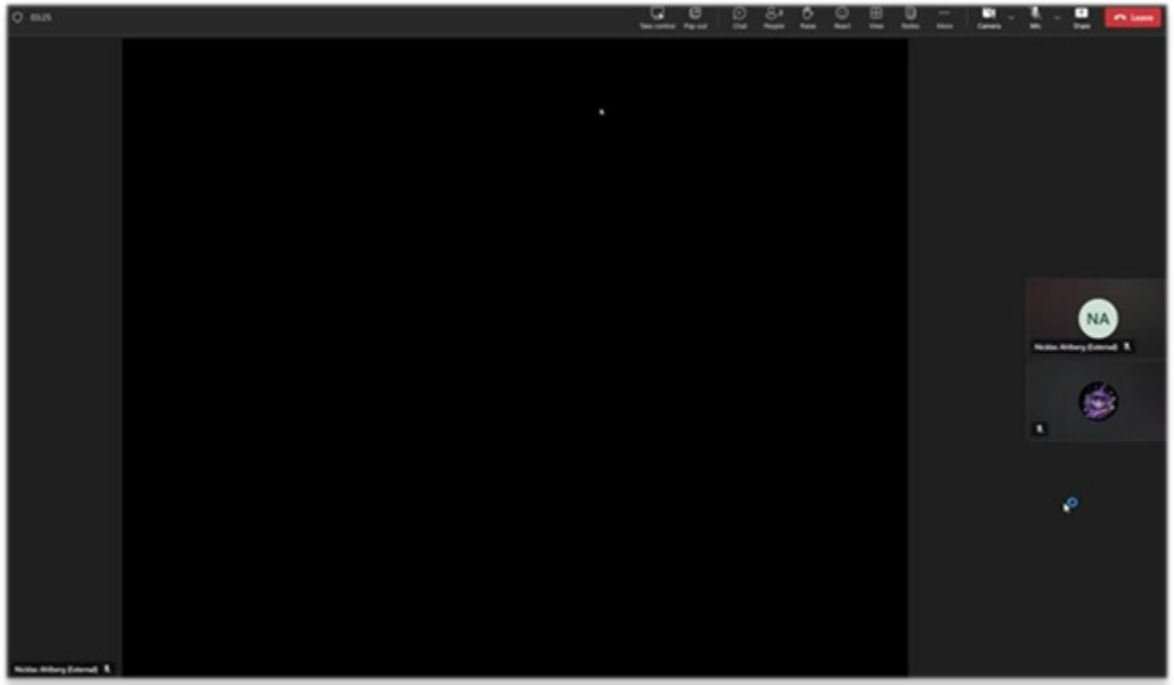



Block/hide remote content in screenshots and screen sharing

## Screen capture protection (try to take a print screen)

Print screen = black screen

## Screen capture protection (try to share in Teams)




Teams sharing = black screen

# Watermarking: Good to know

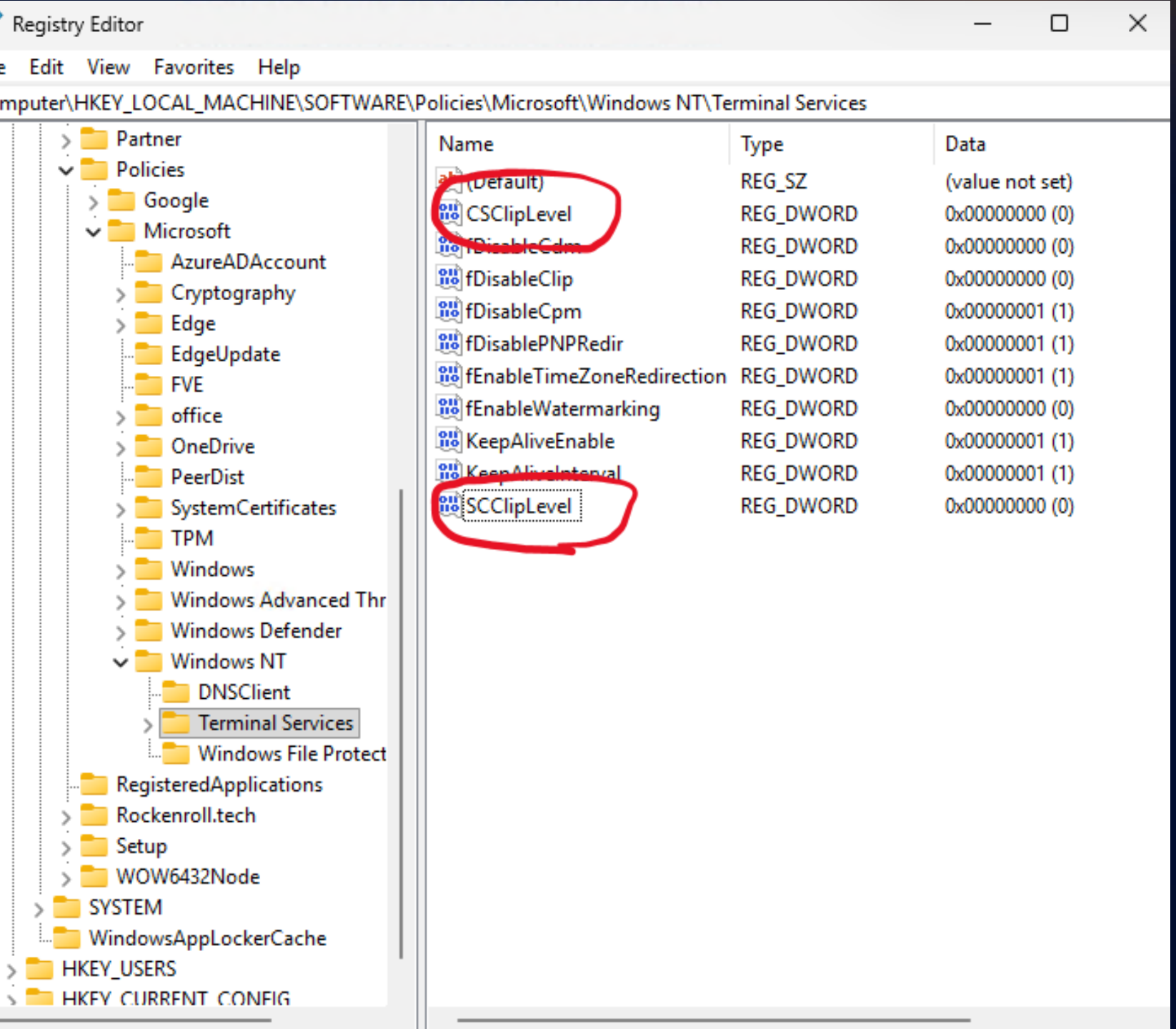

## Watermarking support in Windows 365

Watermarking support is configured on session hosts and enforced by the Remote Desktop client. The settings for Watermarking support can be configured via Group Policy (GPO) or the Intune Settings Catalog. The default for the QR code embedded content setting doesn't allow administrators to look up device information from leaked images for Cloud PCs.

# Device redirection for Cloud PCs


ⓘ Important

- Network drives that are disconnected aren't redirected. Once the network drives are reconnected, they're not automatically redirected during the remote session. You need to disconnect and reconnect to the remote session to redirect the network drives.
- If you disable drive redirection using Intune or Group Policy, it also prevents files being transferred between the local device and remote session using the clipboard. Other content, such as text or images, isn't affected.




MODERN ENDPOINT MANAGEMENT SUMMIT 2026

CS = Client -> Server

SC = Server -> Client


# Windows Hello for Business:
## Multifactor Unlock

# Shoulder surfing is a thing!

- Require another factor to sign in
- Shoulder surfing 👀
- Passwords and security key will not require MFU
- Supports: PIN, Facial, Fingerprint and passive (connected to a specific network or Bluetooth device)


Please rate this session on Sched.com or in the app

# Thanks!