



Let's talk Autopilot

Jan Ketil Skanke



ME



Topics

- Some do and don't for Windows Autopilot
- Custom scripts
- Enhancing first user logon experience
- Autopilot device registration

1 Configure company branding in Azure AD

Key elements for Autopilot is

- Square Logo
 - Sign-in page text
 - Azure AD Tenant Name
-
- Required for Hide change account options
 - Enables a nice look and feel during provisioning

1 Configure company branding in Azure AD

Edit default sign-in experience

Basics Layout Header Footer **Sign-in form** Review

Configure other elements such as images, text and hyperlinks inside of the sign-in form.

Banner logo ⓘ

Select file(s)

Browse



Image size: 280x60px
Max file size: 10KB
File Type: Transparent PNG,
JPG, or JPEG

[Remove](#)

Square logo (light theme) ⓘ

Select file(s)

Browse



Image size: 240x240px
(resizable)
Max file size: 50KB
File Type: PNG (preferred),
JPG, or JPEG

[Remove](#)

Square logo (dark theme) ⓘ

Select file(s)

Browse

Microsoft Entra admin center

Home

Favorites

Azure Active Directory

Overview

Users

Groups

Home >

Contoso

+ Add

Manage tenants

What's new

Preview features

Got feedback?

Overview

Monitoring

Properties

Recommendations

Tutorials

Name

ViaMonstra MasterClass

Country or region

United States

1 Configure company branding in Azure AD

Join to Azure AD as ⓘ

Azure AD joined



Microsoft Software License Terms ⓘ

Show

Hide

ⓘ Important information about hiding license terms

Options to change account and start over with a different account appear, respectively, during initial device setup on the company sign-in page, and on the domain error page. To hide these options, you must configure company branding in Azure Active Directory (requires Windows 10, 1809 or later, or Windows 11).

Hide

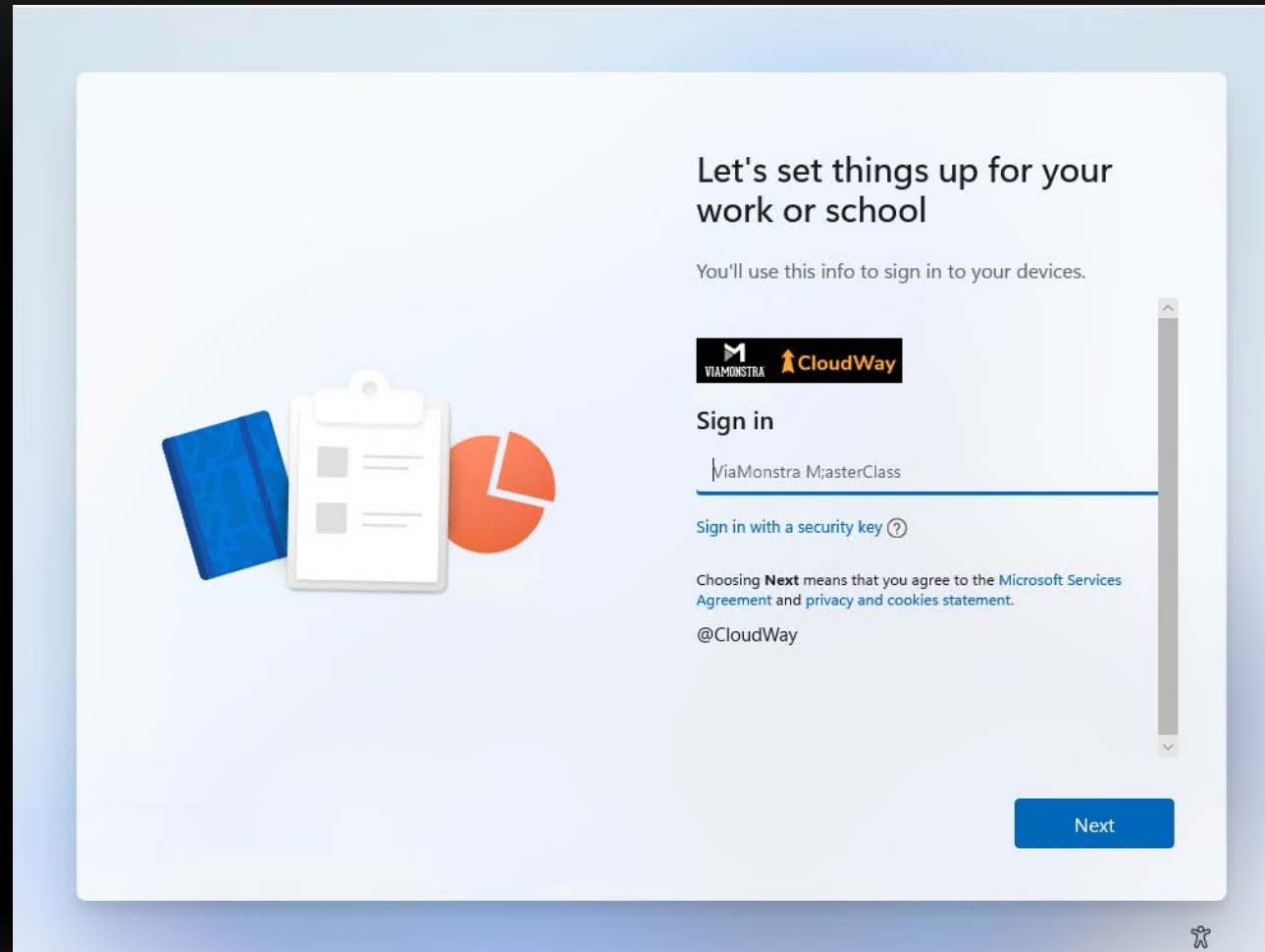
Windows 10, version 1903 and later, or Windows 11.

Hide change account options ⓘ

Show

Hide

1 Configure company branding in Azure AD



2 Create and assign Enrollment Status Page

- ESP Tracks these phases during provisioning
 - Device preparation
 - Device Setup
 - Account Setup

-

Autopilot Provisioning Sequence for AAD Join

Physical Device

Hardware OEM
Existing Devices

Windows OOBE

Pro Edition
Pre-loaded Drivers

Internet

Ethernet
Wifi

Autopilot

User Driven
Self Deployment

Azure AD

AAD Joined
Hybrid -Joined

Intune

Auto-Enrollment
Co-Management

ESP Starts

Config tracking
App tracking

Configuration

Assigned Policies
Certificates, etc

Scripts

IME Installed
PowerShell Scripts run

App Installs

Win32, MSI, Store, M365
Simul. app classes, Apps Seq.

User Session Starts

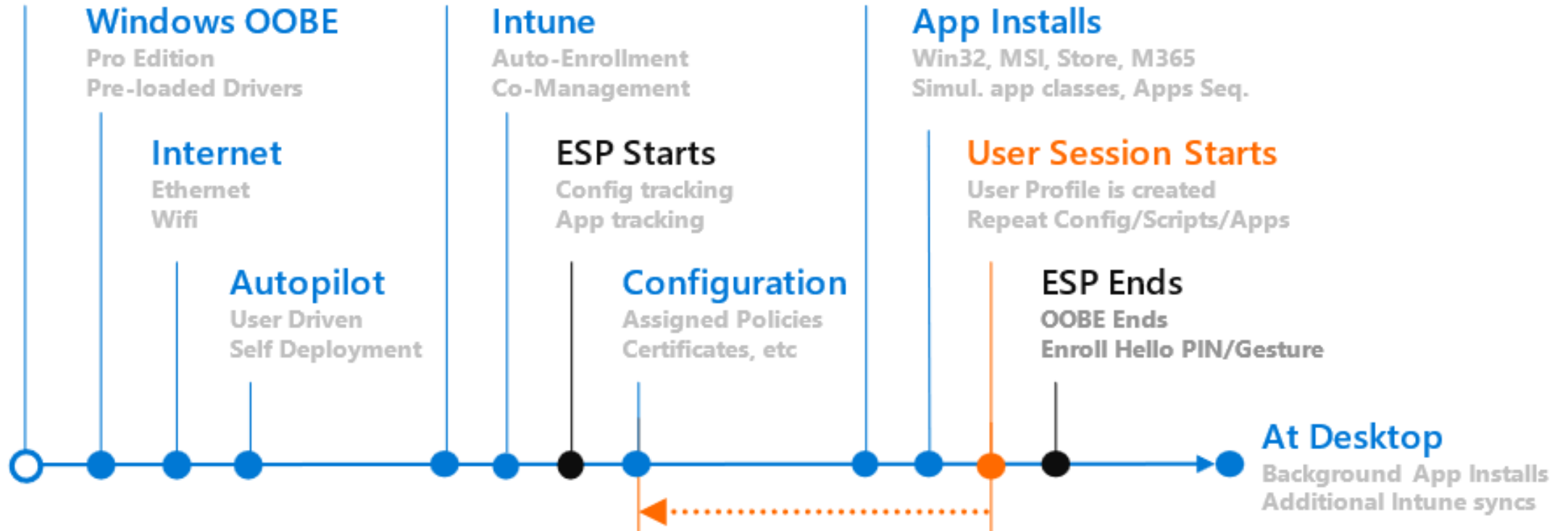
User Profile is created
Repeat Config/Scripts/Apps

ESP Ends

OOBE Ends
Enroll Hello PIN/Gesture

At Desktop

Background App Installs
Additional Intune syncs



2 Create and assign Enrollment Status Page

- Device preparation
 - Securing the hardware
 - Join your organization's network
 - Register your device for mobile management
 - Preparing your device for mobile management
 - Calculate policies and apps required to track in next phase
 - Tracking policy and installation of IME agent



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...



Securing your hardware (Completed)

Joining your organization's network
(Completed)

Registering your device for mobile management
(Completed)

Preparing your device for mobile management
(Working on it...)

Device setup



2 Create and assign Enrollment Status Page

- Device Setup
 - Security policies
 - Certificate profiles
 - Network connection
- Apps
 - Don't mix LOB(MSI) and Win32 apps.
 - Use Win32 and “new” Store apps only
 - Do not use “built-in” Office app install

20

• D



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

✓ Completed

Device setup

Working on it...



Security policies (1 of 1 applied)

Certificates (No setup needed)

Network connections (No setup needed)

Apps (Identifying)

Account setup

Waiting



2 Create and assign Enrollment Status Page

- Account setup
 - Security policies
 - Certificates
 - Network connections
 - Apps

20

• A

•

•

•

•



Setting up for work or school

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

Network connections (No setup needed)

Apps (1 of 1 installed)

Account setup

Working on it...

• •

Joining your organization's network
(Completed)

Security policies (Identifying)

Certificates (Identifying)

Network connections (Identifying)

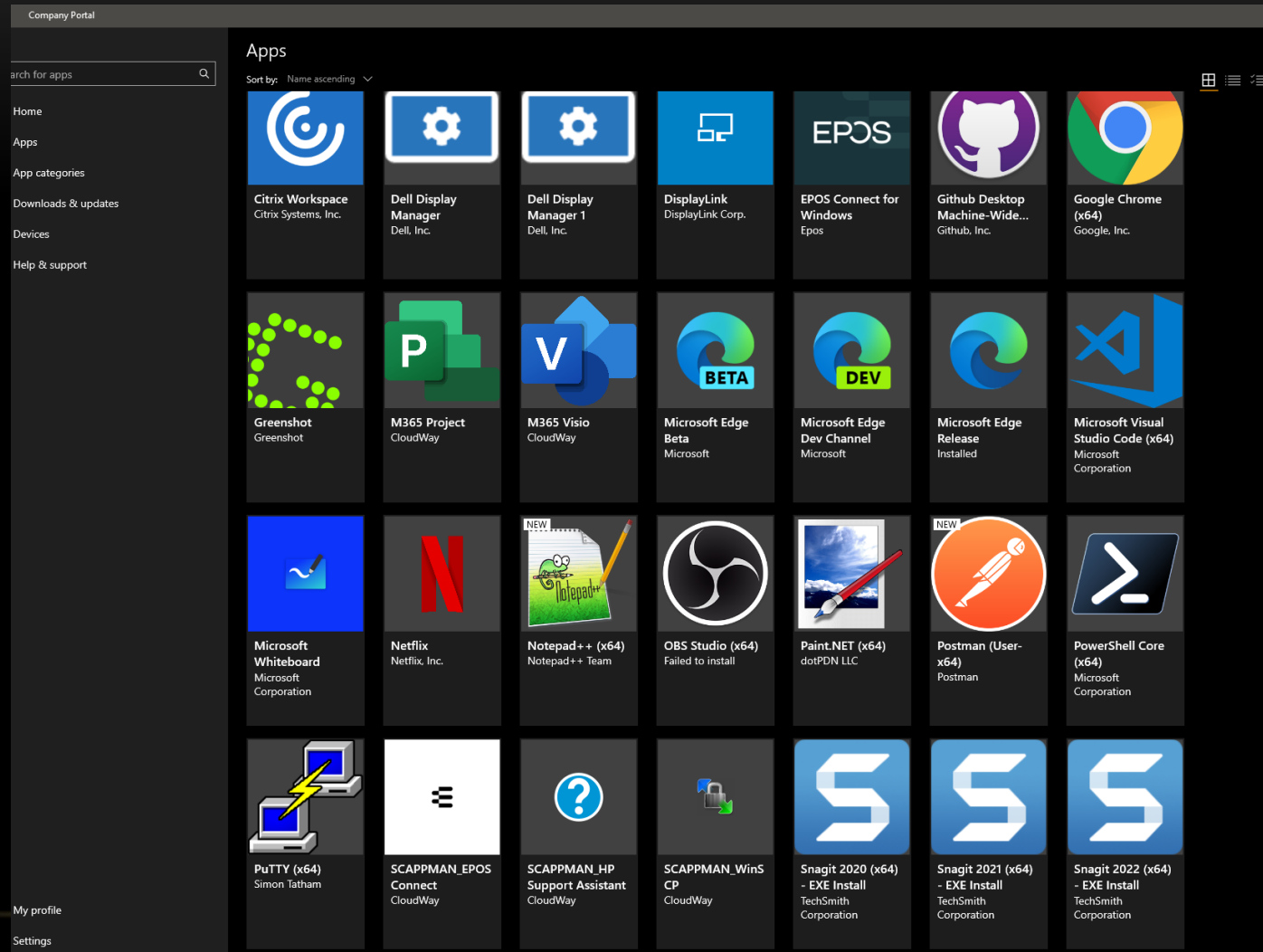
Apps (Identifying)



3 Thinking around required Apps

- Limit the number of required apps.
 - Especially what apps to track during ESP
 - Give the end users the option to self-serve
 - Company portal is there for a reason!
 - How many apps is OK?
-

3 Thinking around required Apps



4.1 - Enhance the first logon experience

- Installation of M365 Apps
 - Use scripted Win32App
 - CSP Office install is not a “real app”
 - Faster and more reliable than Intune built-in option
 - Allows for OEM Cleanup (upcoming version)
 - <https://github.com/MSEndpointMgr/M365Apps>

4.2 - Enhance the first logon experience

- Make sure OneDrive is up to date
- When time passes – the OneDrive version on the box might be out of date
- OneDrive should be 64 bit and run in Machine context
- Make sure OneDrive logs on quicker as it does not have to update in user context

4.3 - Enhance the first logon experience

- Outlook first experience
 - Set the correct policies so that user is automatically logged on
- Edge first experience
 - Set the correct policies so that user automatically is set up with
 - Profile
 - Sync
 - No Welcome messages
 - All required “extensions” comes in

4.4 - Enhance the first logon experience

- Built-in Apps removal
 - Scripted with external control file
- Fix time zone and automatic time/timezone update
 - Scripting is required
 - Standard users not able to turn on or off.
 - Requires location services too

5 - Always be testing

What?

- Make sure it works before you add it to Autopilot/ESP
- Code Signed scripts, make sure certificates are assigned
- Make sure PowerShell script doesn't hang, cause timeout

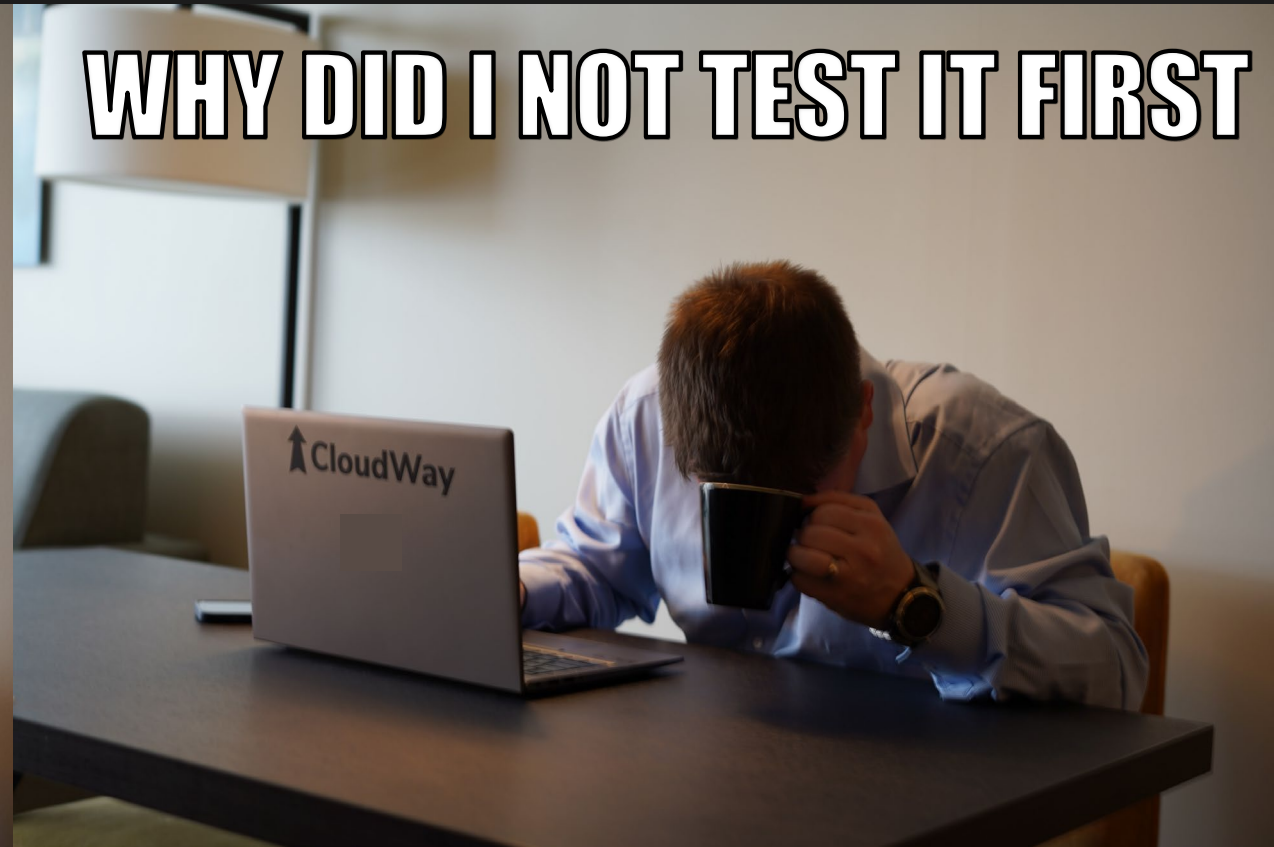
Why?

- Easier troubleshooting
 - Avoid breaking a working deployment!
-

Adding an app to ESP



WHY DID I NOT TEST IT FIRST



6 - What about pre-provisioning

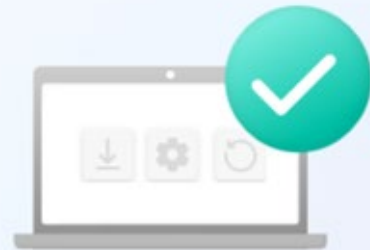
To be used when:

- You have many apps required to be there on first logon
- Poor bandwidth at sites
- Mass distribution of new hardware

Be aware of:

- HW on Shelf will be “outdated” (Compliance)
 - Requires a physical TPM 2.0 (no virtual)
-

What would you like to do?



Install provisioning package

Install a provisioning package for work or school



Pre-provision with Windows Autopilot

Pre-provision this device with settings and apps



Reset device

Reset the device but keep any user accounts

Exit

Next

Pre-provision with Windows Autopilot

Select **Next** to get started with pre-provisioning.

Organization: skanke.net

Deployment profile: TEST 2022

Assigned user: Not assigned



To review or change pre-provisioning configurations:

1. Scan the QR code with the companion app on your phone.
2. Make any needed changes.
3. Select [Refresh](#).



[Cancel](#)

[Next](#)

Your device setup is complete

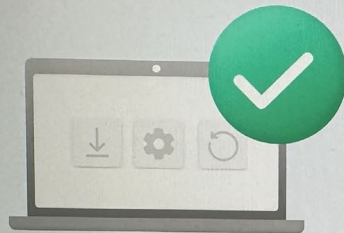
Organization: [REDACTED]

Deployment profile: [REDACTED]

Assigned user: Not assigned

Elapsed time: 0 h 15 min

Print a welcome letter and shipping label, then select **Reseal** to reseal the device.



Reseal

Disabling Microsoft Account Sign-in Assistant will break Autopilot Pre-Provisioning.

ⓘ Note

If the Microsoft Account Sign-In Assistant (wlidsvc) is disabled during the Technician Flow, the Azure AD sign in option may not show. Instead, users are asked to accept the EULA, and create a local account, which may not be what you want.

7 - Device Registration for Autopilot

- Best Option – OEM / Vendor registration
- Second best option – Get help from a MS Partner
- Self registration
 - Script
 - CSV

<https://learn.microsoft.com/en-us/mem/autopilot/registration-overview>

7- OEM / Vendor registration

- No need to collect any data, this is handled by OEM
 - OEM Preinstall Windows
 - Sending “Computer build report to Microsoft”
 - The “Computer Build Report” contains the “hardware hash”
- The OEM associates the device to your tenant

[OEM Activation 3.0 system | Microsoft Learn](#)

7- Reseller, distributor, or partner registration

- Does this mean the OEM has access to my tenant?
 - Windows Autopilot is managed and maintained by Microsoft
 - Backend database associates “hashes” with customer tenants
 - OEM is writing to this database and not customer tenant
 - No permissions are granted or required for OEMS to do this
 - Customer still need grant the OEM Permissions
 - (MS can add devices through supportcase)

7- Reseller, distributor, or partner registration

- Must be part of Microsoft Cloud Solution Partner program
- The CSP partner requests a relationship with the organization. That organization's global administrator approves the request.
- Partner can now register devices on customer behalf with only Make,Model, SerialNumber or SerialNumber + Product Key ID
- Does not required Delegated Admin Privilege

7- Reseller, distributor, or partner registration

- Must be part of Microsoft Cloud Solution Partner program
 - The CSP partner requests a relationship with the organization. That organization's global administrator approves the request.
 - Partner can now register devices on customer behalf with only Make,Model, SerialNumber or SerialNumber + Product Key ID
 - Does not required Delegated Admin Privilege
-

7- Self registration

- Collect Hardware hash and upload via CSV
 - get-windowsautopilotinfo
- Run script manually on a client with –Online to register directly
- Register existing devices from Intune Automatically

<https://learn.microsoft.com/en-us/mem/autopilot/registration-overview>

8- Avoid ESP unexpected reboots

- Reboots are supported during the device setup phase, but not supported during the account setup phase.
- Reboots are only supported if triggered by Intune.
- Device setup phase
 - Security policies
 - Certificates
 - Network connections
 - Apps (If an application needs reboot, don't force it, should specify the return codes to perform a reboot by Intune)
- Account setup phase
 - Joining your organization's network
 - Security policies
 - Certificates
 - Network connections
 - Apps

Reboot required URIs

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Provisioning\SyncML\RebootRequiredURIs

Registry Editor

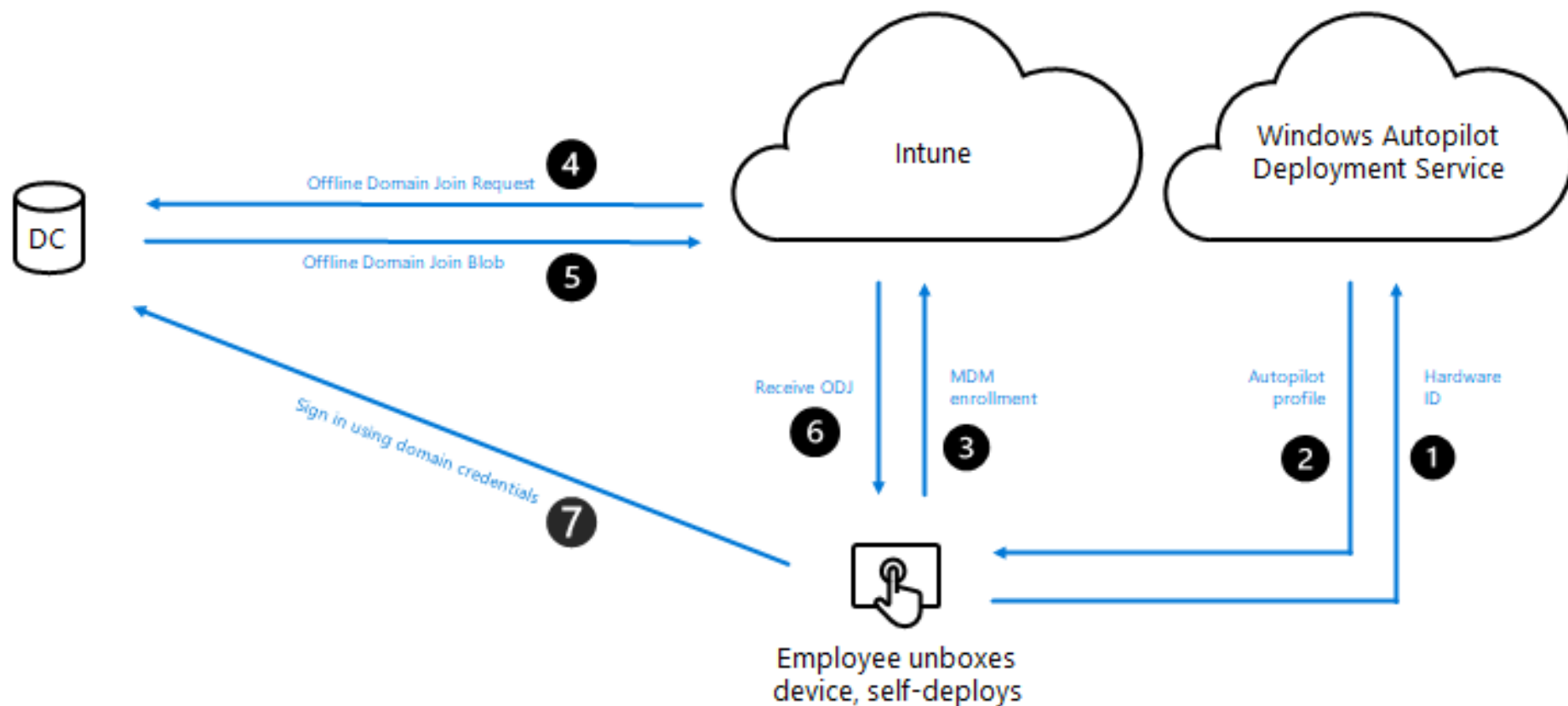
File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Provisioning\SyncML\RebootRequiredURIs

Name	Type	Data
(Default)	REG_SZ	(v
.Device/Vendor/MSFT/Accounts/Domain/ComputerName	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/Connectivity/AllowUSBConnection	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/DeviceGuard/ConfigureSystemGuardLaunch	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/DeviceGuard/EnableVirtualizationBasedSecurity	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/DeviceGuard/LsaCfgFlags	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/DeviceGuard/RequirePlatformSecurityFeatures	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/DmaGuard/DeviceEnumerationPolicy	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/ExploitGuard/ExploitProtectionSettings	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/MixedReality/HeadTrackingMode	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/Notifications/DisallowCloudNotification	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/Notifications/DisallowTileNotification	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/Notifications/WnsEndpoint	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/ServiceControlManager/SvchostProcessMitigation	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/Start/HideChangeAccountSettings	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/Start/HideHibernate	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/Start/HideLock	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/Start/HidePowerButton	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/Start/HideRestart	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/Start/HideShutDown	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/Start/HideSignOut	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/Start/HideSleep	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/Start/HideSwitchAccount	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/Start/HideUserTile	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/Start/ImportEdgeAssets	REG_SZ	
.Device/Vendor/MSFT/Policy/Config/Update/ManagePreviewBuilds	REG_SZ	
.Device/Vendor/MSFT/Uefi/Identity/Apply	REG_SZ	
.Device/Vendor/MSFT/Uefi/Identity2/Apply	REG_SZ	
.Device/Vendor/MSFT/Uefi/Permissions/Apply	REG_SZ	
.Device/Vendor/MSFT/Uefi/Permissions2/Apply	REG_SZ	
.Device/Vendor/MSFT/Uefi/Settings/Apply	REG_SZ	
.Device/Vendor/MSFT/Uefi/Settings2/Apply	REG_SZ	
.Device/Vendor/MSFT/WindowsDefenderApplicationGuard/InstallWindowsDefenderApplicationGuard	REG_SZ	

9- Do not do Autopilot Hybrid Join

Windows Autopilot // User-Driven deployment with Hybrid Azure AD



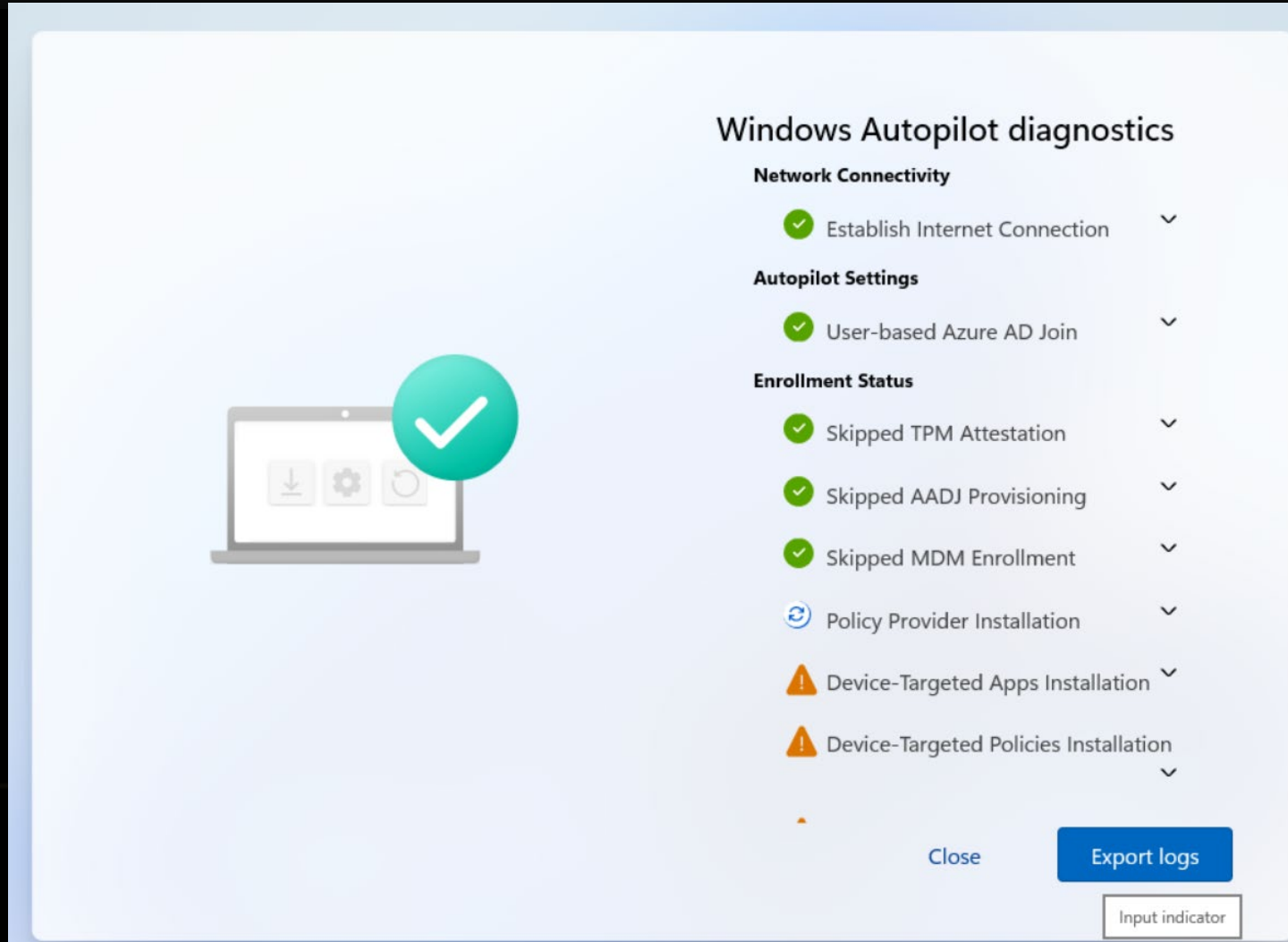
9- Do not do Autopilot Hybrid Join

Windows Autopilot // User-Driven Deployment with Hybrid Azure AD



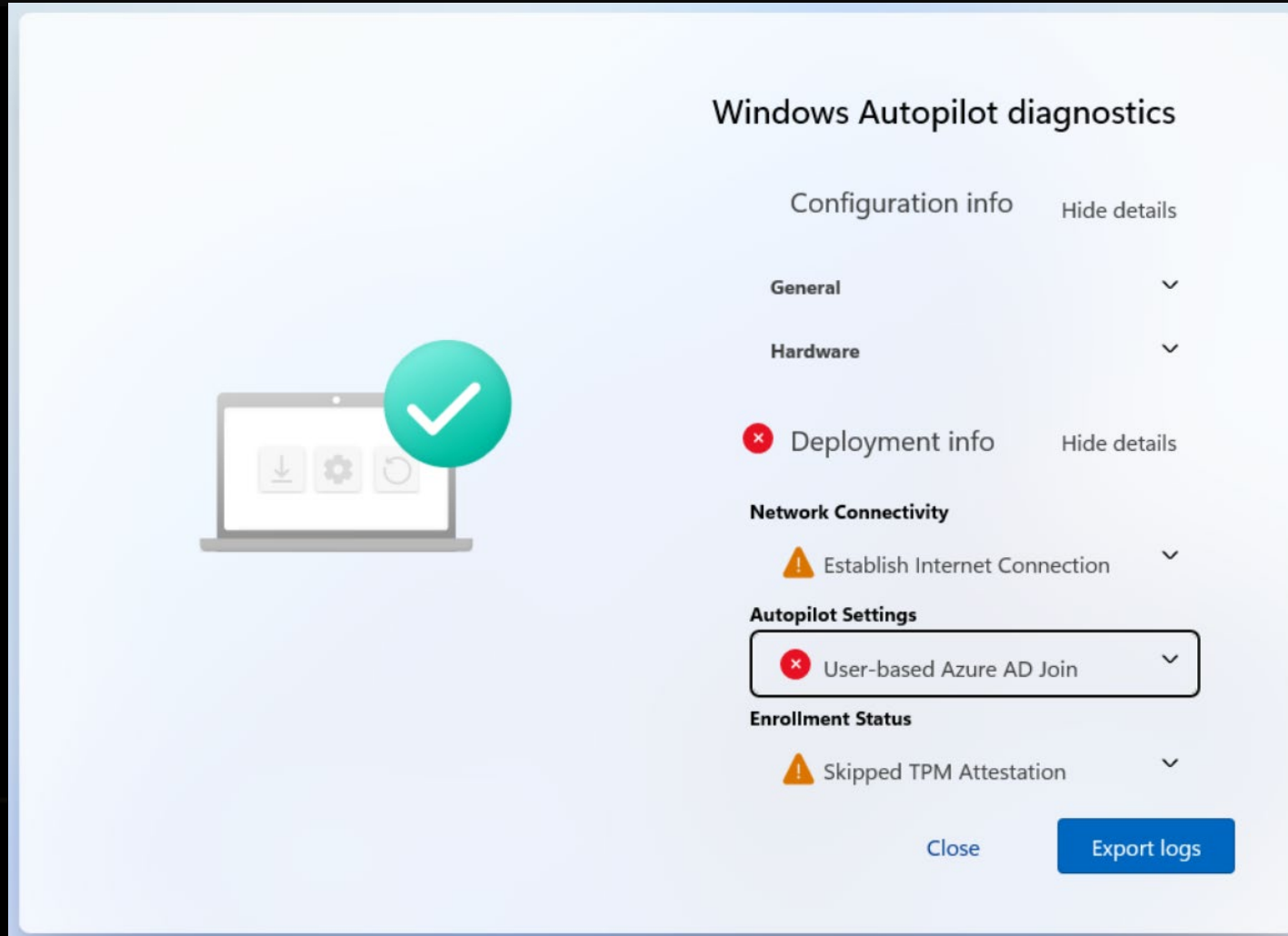
10 – Troubleshooting

- Autopilot Diagnostics Page (Ctrl-shift-D)



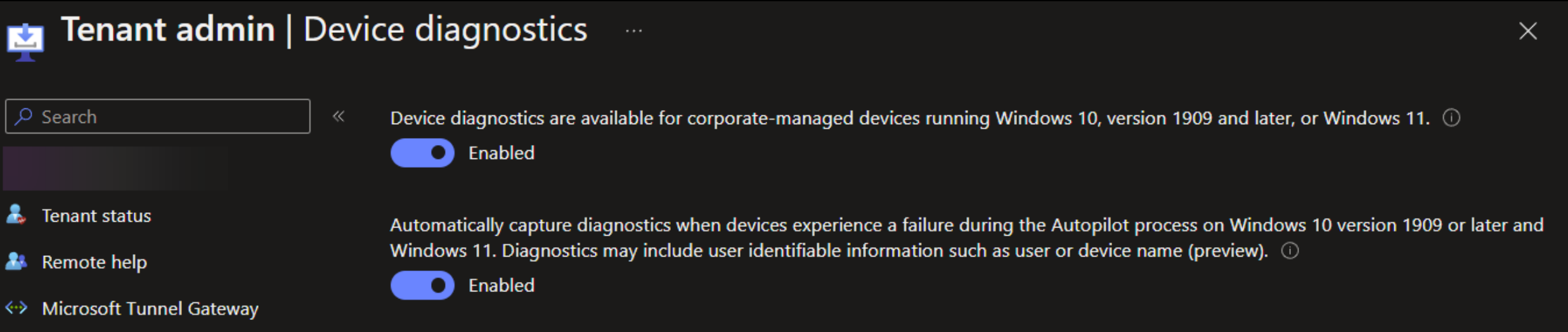
10 – Troubleshooting

- Autopilot Diagnostics Page (Ctrl-shift-D)



10 – Troubleshooting

- Autopilot Diagnostics Page (Ctrl-shift-D)
- Turn on Automatic Log Collection on failure
 - Or collect locally with MdmDiagnosticsTool.exe -area Autopilot -cab C:\LOGS.zip



The screenshot shows the 'Tenant admin | Device diagnostics' page. On the left is a sidebar with a search bar and navigation links: 'Tenant status', 'Remote help', and 'Microsoft Tunnel Gateway'. The main content area has a title bar with a close button. Below the title bar, there is a section for 'Device diagnostics' with a toggle switch set to 'Enabled'. A descriptive text explains that diagnostics are available for corporate-managed devices on Windows 10 (version 1909 and later) or Windows 11. Below this, another section titled 'Automatically capture diagnostics when devices experience a failure during the Autopilot process on Windows 10 version 1909 or later and Windows 11' also has a toggle switch set to 'Enabled'. A note specifies that diagnostics may include user identifiable information like user or device name (preview).

Tenant admin | Device diagnostics

Search

Device diagnostics are available for corporate-managed devices running Windows 10, version 1909 and later, or Windows 11.

Enabled

Automatically capture diagnostics when devices experience a failure during the Autopilot process on Windows 10 version 1909 or later and Windows 11. Diagnostics may include user identifiable information such as user or device name (preview).

Enabled

Tenant status

Remote help

Microsoft Tunnel Gateway

10 – Troubleshooting

- Autopilot Diagnostics Page (Ctrl-shift-D)
- Turn on Automatic Log Collection on failure
 - Or collect locally with MdmDiagnosticsTool.exe -area Autopilot -cab C:\LOGS.zip
- Get-AutopilotDiagnostics
- <https://learn.microsoft.com/en-us/mem/autopilot/troubleshoot-oobe>

```
PS C:\Windows\system32> Get-AutopilotDiagnostics.ps1
```

AUTOPILOT DIAGNOSTICS

```
OS version:          10.0.22000
Profile:             TEST 2022
TenantDomain:       skanke.net
TenantID:            e87630f5-66df-47f3-8747-84801dbf1be7
ZTDID:              cd2cb78e-085a-4e45-9916-f265f1678091
```

```
EntDMID:
OobeConfig:          286
Skip keyboard:       No      0 - - - - -
Enable patch download: No    - 0 - - - - -
Skip Windows upgrade UX: Yes  - - 1 - - - - -
AAD TPM Required:    No      - - - 0 - - - - -
AAD device auth:     No      - - - - 0 - - - - -
TPM attestation:     No      - - - - - 0 - - - - -
Skip EULA:           Yes     - - - - - 1 - - - - -
Skip OEM registration: Yes    - - - - - 1 - - - - -
Skip express settings: Yes    - - - - - 1 - - - - -
Disallow admin:      Yes     - - - - - 1 - - - - -
```

```
Scenario:            Azure AD Join
```

Delivery Optimization statistics:

```
Total bytes downloaded: 41525881
From peers:              0% (0)
From Connected Cache:    0% (0)
```

```
ESP diagnostics info does not (yet) exist.
```

OBSERVED TIMELINE:

Date	Status	Detail
----	-----	-----
2022-10-03 10:48:29Z	Profile downloaded	Autopilot profile

re

re-area Autopilot -cab

10 – Troubleshooting

- Autopilot Diagnostics Page (Ctrl-shift-D)
- Turn on Automatic Log Collection on failure
 - Or collect locally with MdmDiagnosticsTool.exe -area Autopilot -cab C:\LOGS.zip
- Get-AutopilotDiagnostics
- <https://learn.microsoft.com/en-us/mem/autopilot/troubleshoot-oobe>

10 -

- Autopilot

- Tutorial

-

- Getting

- https

```
PS C:\Windows\system32> Get-AutopilotDiagnostics.ps1

AUTOPILOT DIAGNOSTICS

OS version:                10.0.22000
Profile:                    TEST 2022
TenantDomain:               skanke.net
TenantID:                   e87630f5-66df-47f3-8747-84801dbf1be7
ZTDID:                      cd2cb78e-085a-4e45-9916-f265f1678091
EntDMID:
OobeConfig:                 286
  Skip keyboard:            No      0 - - - - -
  Enable patch download:    No      - 0 - - - - -
  Skip Windows upgrade UX:  Yes     - - 1 - - - - -
  AAD TPM Required:         No      - - - 0 - - - - -
  AAD device auth:          No      - - - - 0 - - - - -
  TPM attestation:          No      - - - - - 0 - - - - -
  Skip EULA:                Yes     - - - - - 1 - - - - -
  Skip OEM registration:    Yes     - - - - - - 1 - - - - -
  Skip express settings:    Yes     - - - - - - - 1 - - - - -
  Disallow admin:           Yes     - - - - - - - - 1 - - - - -
Scenario:                   Azure AD Join
Delivery Optimization statistics:
  Total bytes downloaded:   41525881
  From peers:               0% (0)
  From Connected Cache:    0% (0)
ESP diagnostics info does not (yet) exist.

OBSERVED TIMELINE:

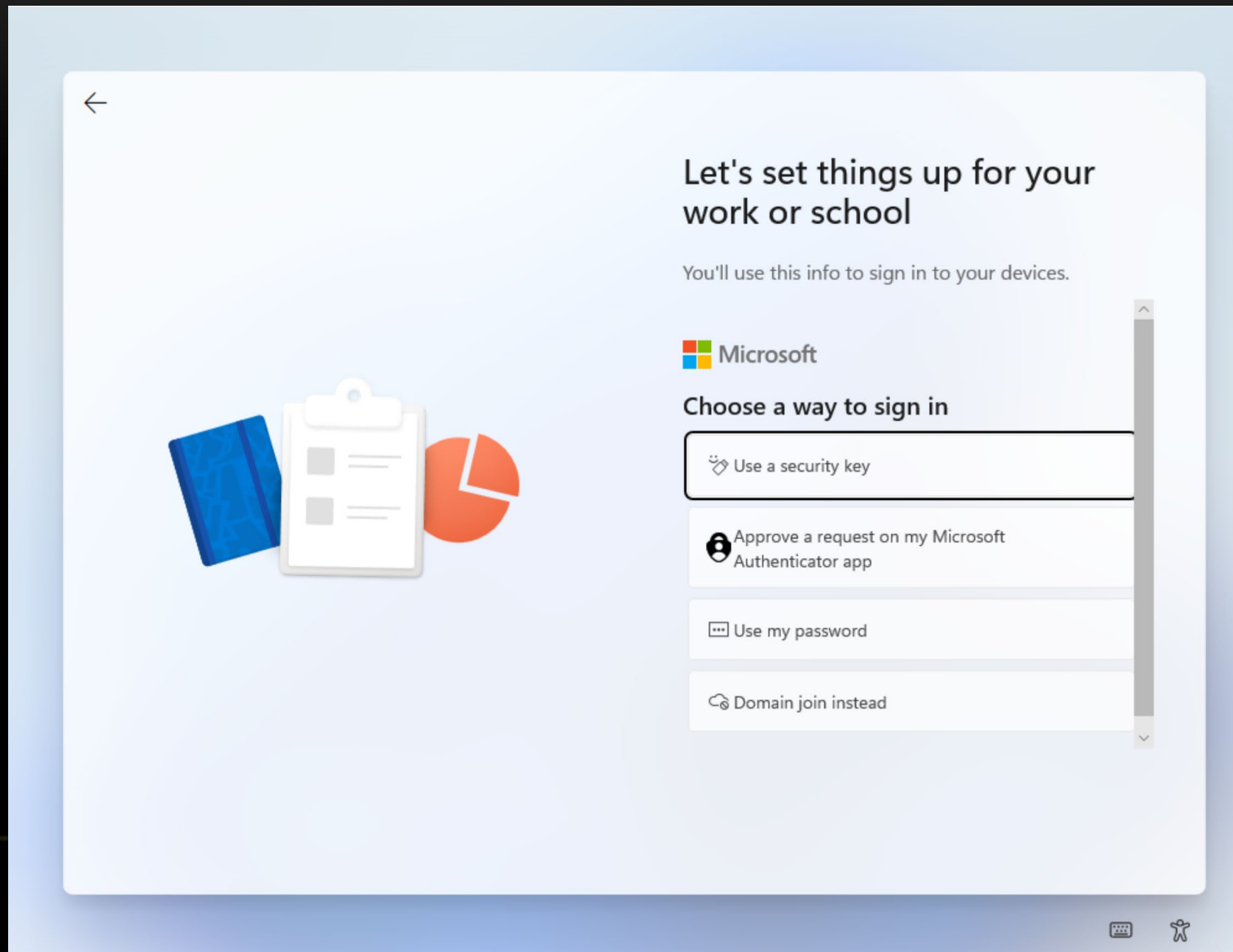
Date                Status                Detail
----                -
2022-10-03 10:48:29Z Profile downloaded Autopilot profile
```

Autopilot -cab

10 – Troubleshooting

- Autopilot Diagnostics Page (Ctrl-shift-D)
- Turn on Automatic Log Collection on failure
 - Or collect locally with MdmDiagnosticsTool.exe -area Autopilot -cab C:\LOGS.zip
- Get-AutopilotDiagnostics
- <https://learn.microsoft.com/en-us/mem/autopilot/troubleshoot-oobe>

One last thing.. Go Passwordless



Resources

- M365 App Install : [MSEndpointMgr/M365Apps: Scripted option to install M365 Apps, Project, Visio and Proofing tools using ODT \(github.com\)](#)