



# Modern Desktop Conversion

Friday, October 13, 2023 9:00 am



**Chris Blackburn**



**Kevan Arden**



**Evan Stueve**

Dive into the different options and considerations for your modern desktop conversion, the risks and requirements, walk through live demos of the process, and walk away with a comparison guide to help in choosing the right journey for your organization.





# Welcome to the MN M365 Fall Workshop Day 2023!

Please help us drive event awareness by tweeting and posting about your  
experience at the Workshop:

@M365MN #M365WorkshopDay

Please join us following the sessions for Happy Hour... Admin Ales, Workshop Wine,  
and more!

Thank you for your participation!

# Thank You To The Sponsors!



Stop by the Booths for “Vendor Bingo” to win prizes!



Microsoft



RBA



SUCCESS  
COMPUTER CONSULTING

MYTECH  
PARTNERS



nowmicro



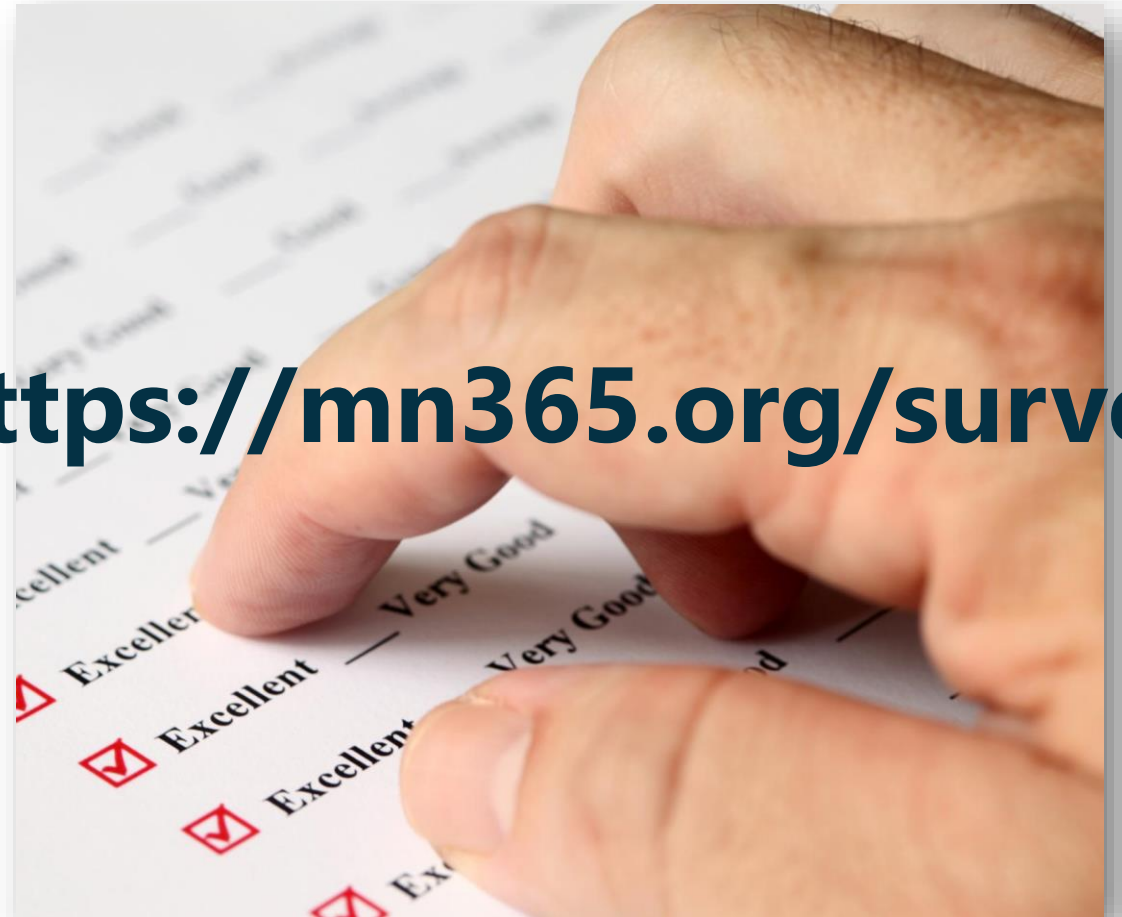


# Workshop Survey

MN365 Fall 2023 Workshop Day



<https://mn365.org/survey>

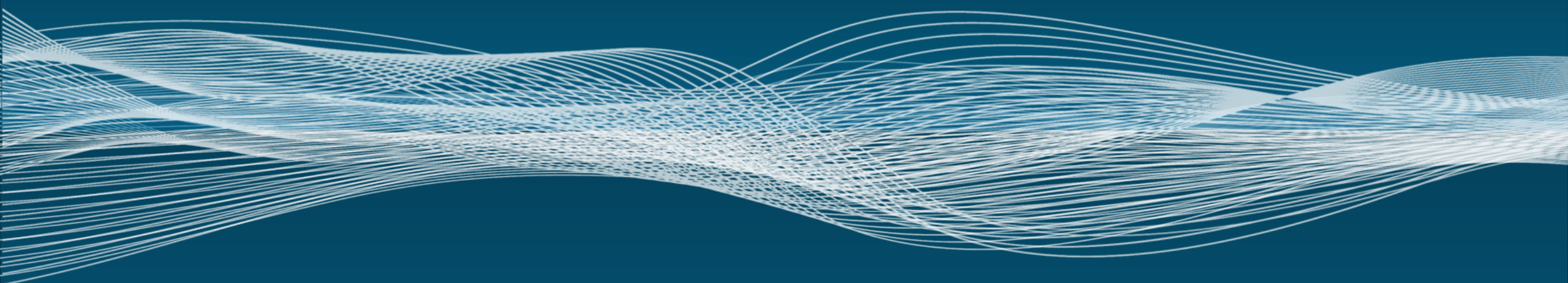


# Agenda

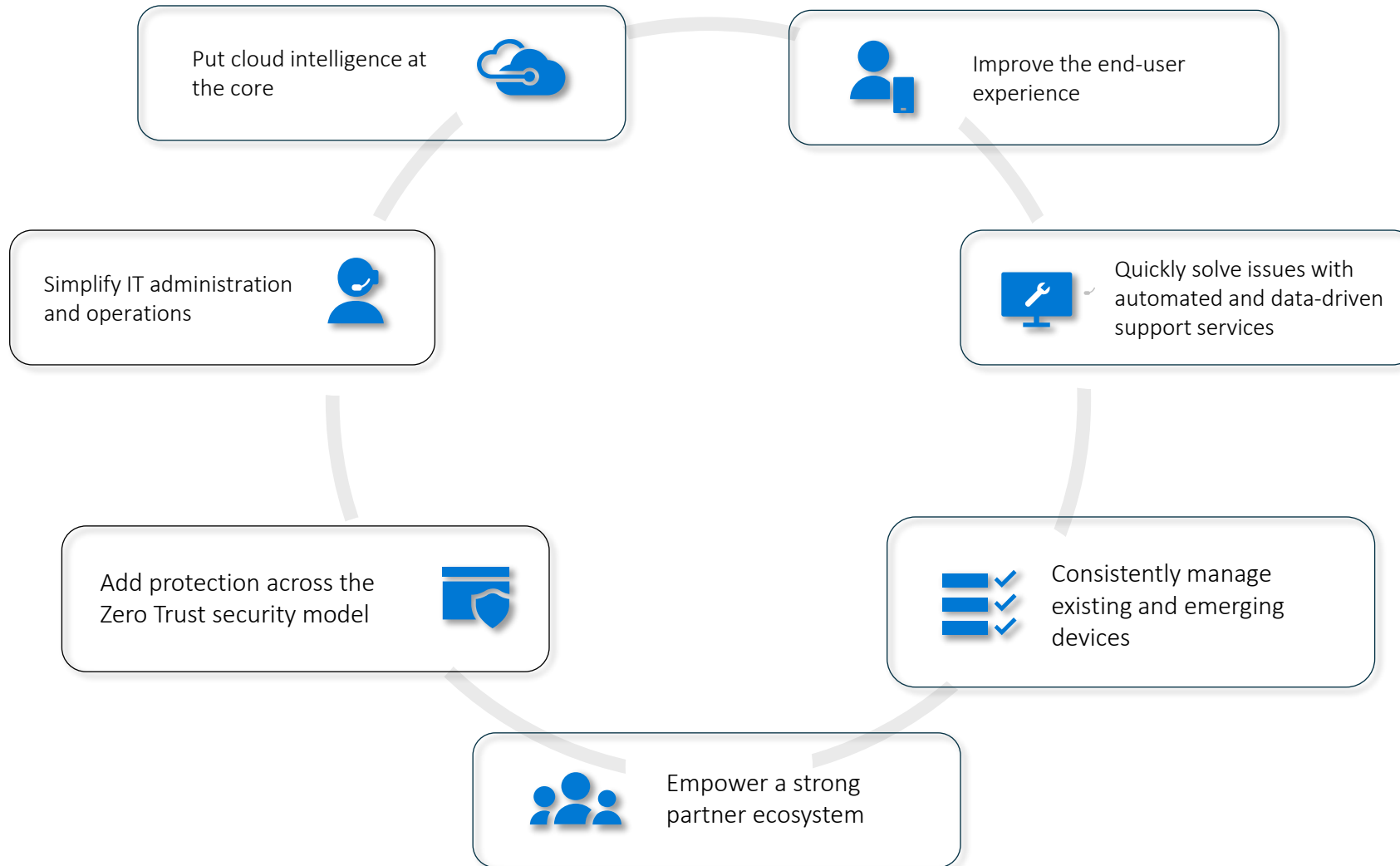
- Why Modern Management
- Requirements, Risks, & Readiness
- Conversion Options + Demos (Break)
- Tooling Comparison
- Q&A



# Why Modern Management?

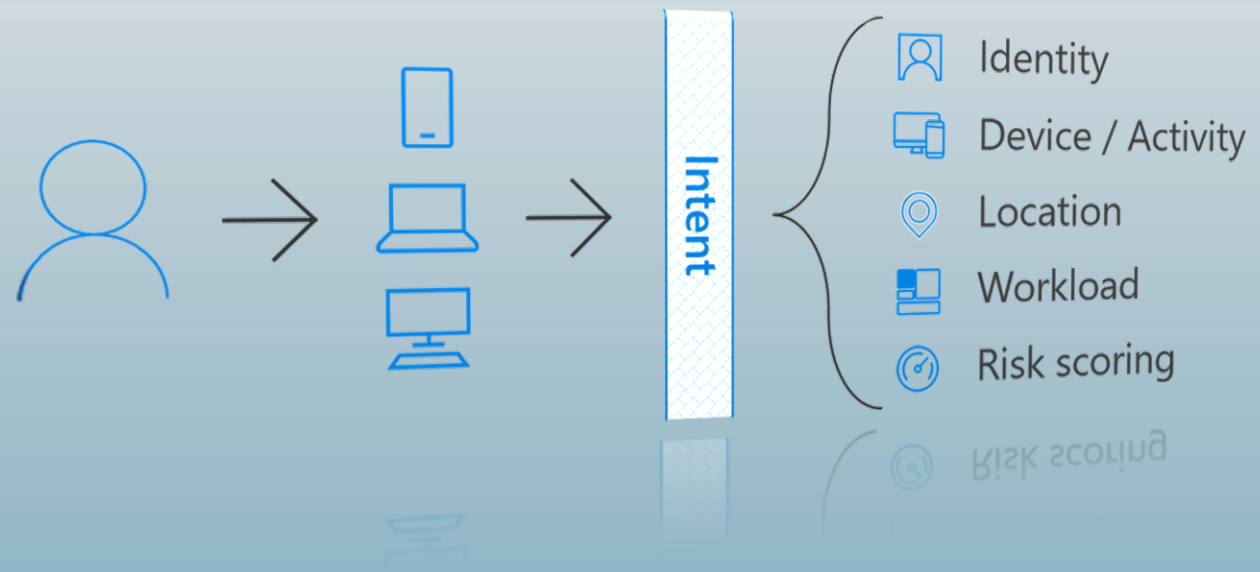


# What is "Modern Management"



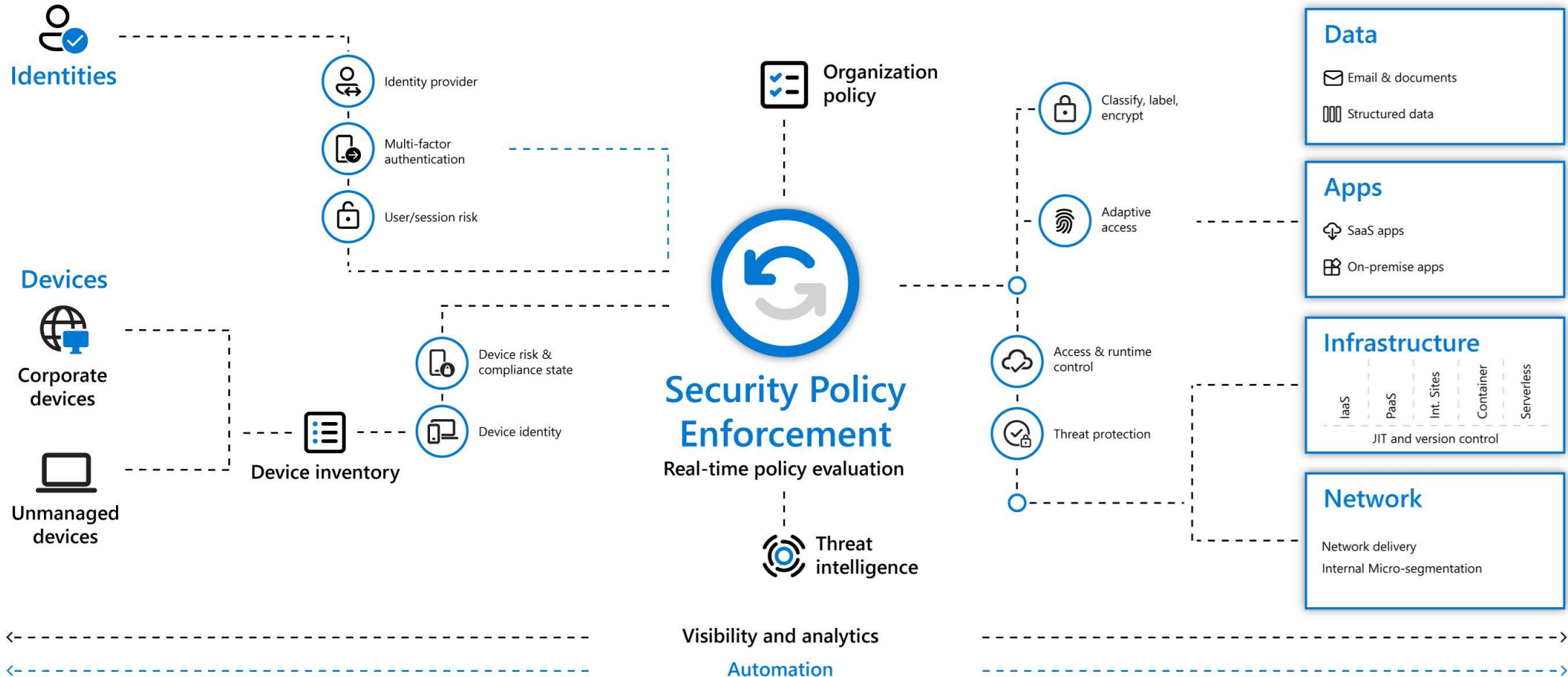
# Why Azure AD Join (AADJ)?

- Improving security posture (**Always verify in/out of corpnet**)
  - All users/devices need to pass authentication
- Concept of least privilege
  - Users and Admins have the minimum required permissions to do their work
- Network segmentation (Attack surface reduction)
  - Mitigate lateral network movement/access to bolster security
- Robust logging & monitoring





# Why Zero Trust Matters





# Requirements, Risks & Readiness



# We've Observed with Clients

- Functional
  - Remove Dependencies on Active Directory
    - Validate the direction of Azure AD only (zero-trust) or Hybrid Joined (Modern Work)
  - Commoditized end user computing based on Azure AD join, Autopilot, and cloud-managed
    - Bring Your Own Device
  - Tooling must transition on-premises, hybrid AD endpoints to Azure Active Directory
    - Must have minimal user impact
  - Establish a point in time where traditional deployment methods are sunset
    - Avoid licensing and having to convert newly onboarded users and devices
  - User ability to initiate the process when possible
    - Minimal interaction from IT where possible
- Technical
  - Devices must be added en-mass
    - Bulk enrollment token is needed, which some IT orgs will see as a security risk
  - User OneDrive state must be healthy
    - Known Folder Redirection and backup validation before the migration is **important**
  - Device Management and Identity States must be healthy
    - Only one device is showing in Azure AD and the device is showing in Intune

# Transitional Risks

- Device Lifecycle Management
- OneDrive Health + Known Folder Redirection
- Systems Management & Enrollment Methods
- Necessity of Remote Connectivity
- Access to Printing
- Access to File Shares
- Remote Assistance
- App Authentication
- App Deployments

# Device Lifecycle Management

- When is a device "too old" to upgrade or migrate?
- How often does your organization cycle out user devices?



# OneDrive Health

## Keep your users data protected!

- Use the Microsoft 365 Apps Admin Center to monitor health <https://config.office.com>
- Under Setup Grab your tenant key
- Setup a OneDrive ODFB "Device configuration" policy for redirection, SSO & key

Home > Devices | Configuration profiles > WIN10-ODfB Setup >

### Edit profile - WIN10-ODfB Setup

Settings catalog

- Enable sync health reporting for OneDrive  Enabled
- Hide the "Deleted files are removed everywhere" reminder  Enabled
- Prevent users from syncing personal OneDrive accounts (User)  Enabled
- Silently move Windows known folders to OneDrive  Enabled
- Show notification to users after folders have been redirected: (Device) \*
- Tenant ID: (Device)
- Silently sign in users to the OneDrive sync app with their Windows credentials  Enabled
- Sync Admin Reports  Enabled
- Tenant Association Key: (Device)
- Use OneDrive Files On-Demand  Enabled

## OneDrive Sync app health

Overview Devices Issues

Find detailed information about users and devices, including sync errors, operating system, folder backup username, email, or device name.

2 items Filter Search

| User ↑      | User email         | Device name     | Errors    | Known folders | App version      | Operating system |
|-------------|--------------------|-----------------|-----------|---------------|------------------|------------------|
| Alex Wilber | AlexW@corp.conn... | AP-465698321468 | ✔ Healthy | All           | 23.194.0917.0001 | Windows 10       |
| Lee Gu      | LeeG@corp.conne... | CORP-2577815546 | ✔ Healthy | All           | 23.194.0917.0001 | Windows 10       |

- Health
- Apps Health
- Security Update Status
- OneDrive Sync**
- Service Health

Home / Setup

## Setup

### Tenant Association Key

If you need a new key, please click on the button below to generate a new one. You will lose access to actions and inventory of existing devices until the new key has been associated with those devices.

[Generate new key](#)

# Automatic Device Enrollment

Automatic enrollment can be used in the following device management and provisioning scenarios:

- Bring-your-own-device (BYOD), personal devices
- **Bulk enrollment**
- Group Policy
- **Windows Autopilot (user driven and self-deploying)**

Intune allows for mobile device and mobile application management, but Entra AD (formerly Azure Active Directory) manages the identity of the computer object – this must exist **before you can leverage Intune**.

For the methods in this presentation we need a **bulk enrollment** token

- (Not needed for Autopilot reset)
- 90 day token, can be extended to 180 days

For more details: <https://learn.microsoft.com/en-us/mem/intune/enrollment/windows-bulk-enroll>

Home > Devices | Windows > Windows | Windows enrollment >

## Configure

Microsoft Intune

Save Discard Delete

MDM user scope  None  Some  All

MDM terms of use URL  ✓

MDM discovery URL  ✓

MDM compliance URL  ✓

[Restore default MDM URLs](#)

MAM user scope  None  Some  All

MAM terms of use URL  ✓

MAM discovery URL  ✓

MAM compliance URL  ✓

[Restore default MAM URLs](#)

# Configure A Provisioning Package

1. Open Windows Configuration Designer and select "Provision Desktop Devices"
2. Name your migration project and move through the configuration steps, providing details where needed.

- **Set Up Device**

- Determine if the endpoints are going to be renamed, and the standardized naming convention to use.
  - If you want to retain the current PC name enter placeholder in the field. (this is cover these steps in the Advanced Provisioning slide)
- Configure machines for shared use (optional)
- Remove pre-installed software (optional)

- **Set up Network**

- Specify the network SSID to be used for endpoints utilizing a Wi-Fi connection.
- **IMPORTANT:** A network connection is required for the provisioning package to successfully join the endpoint to Azure. *Failure to establish an internet connection will prevent a new Azure profile from being created on the machine and prevent logging in unless a local administrator account is available.*
- Deselect if using wired connection (recommended)

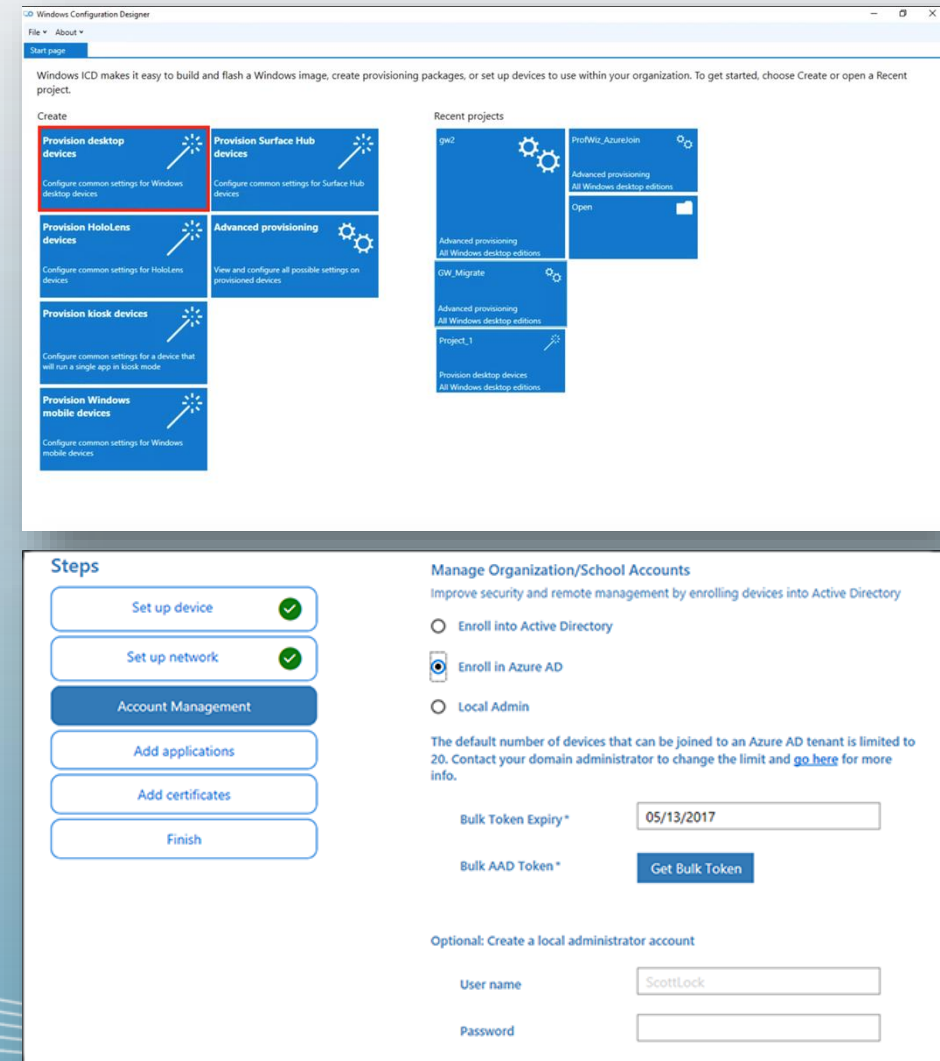
- **Account Management**

- Select "Enroll in Azure AD" and create the bulk AAD token
- **IMPORTANT:** An AAD account with **Application Administrator or Global Admin** privileges will be required to create the bulk AAD token
- Create a local administrator account if desired.

- **Add Applications / Certs**

- These optional components can be deployed with the provisioning package

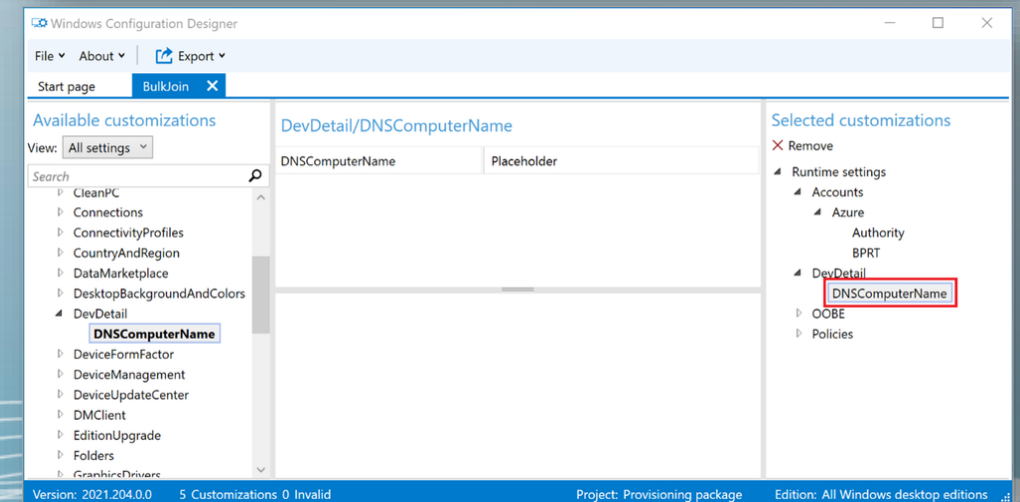
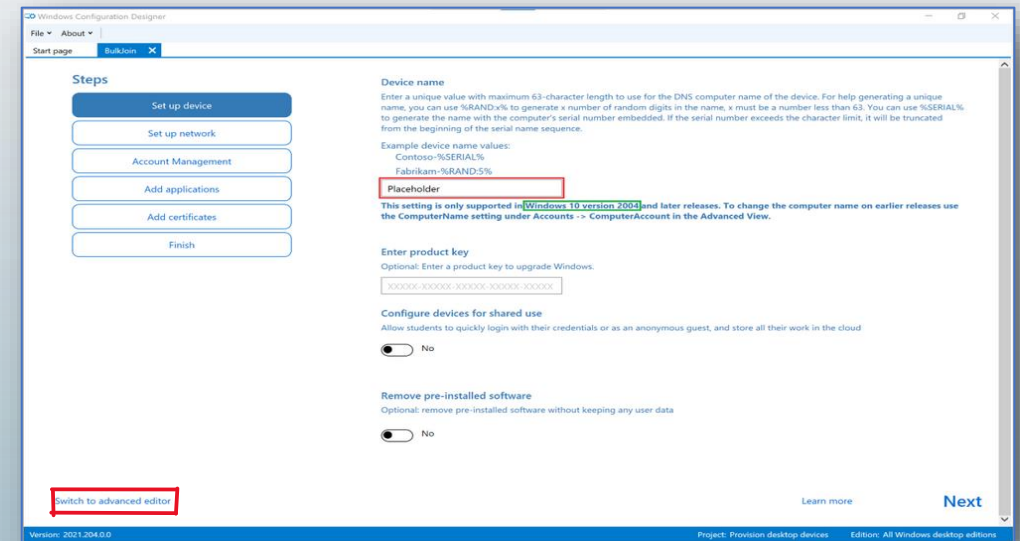
3. Create the provisioning package.





# Advanced Provisioning (Retain PC name)

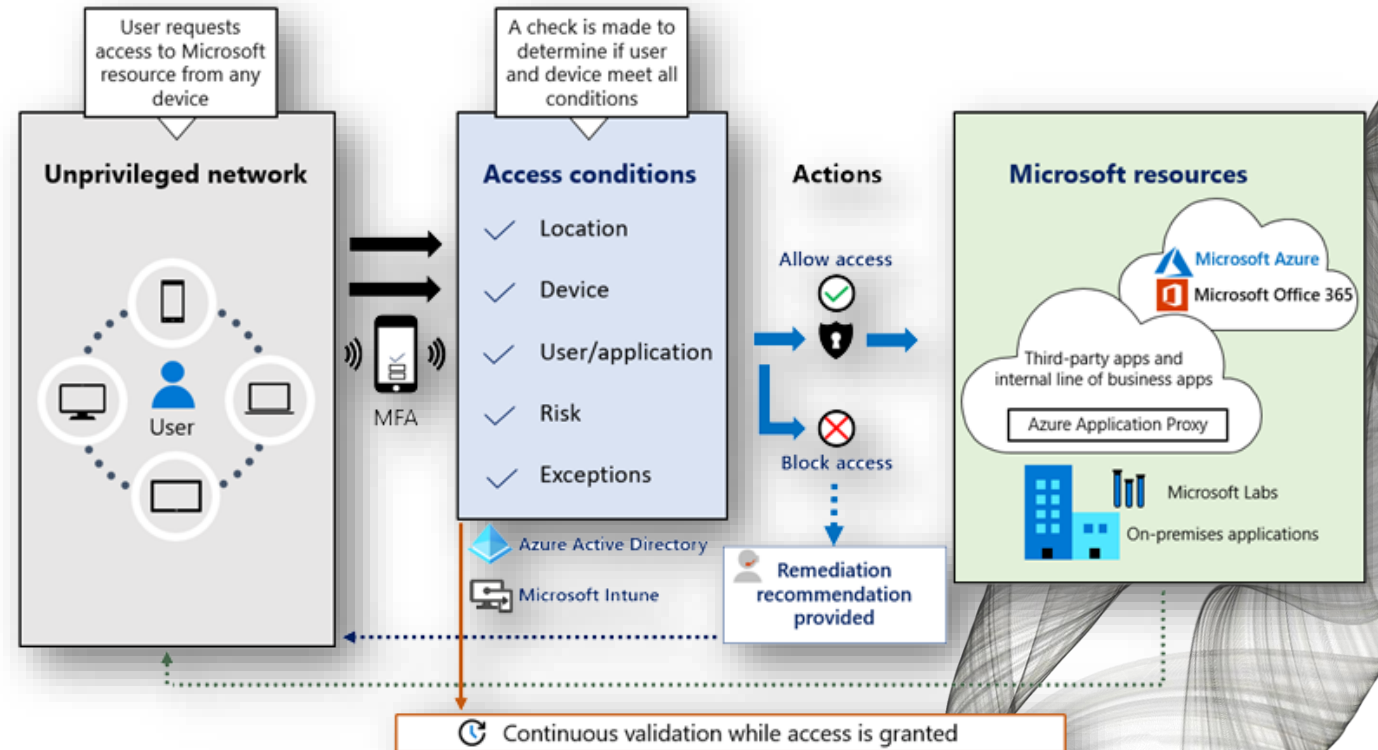
1. Open your existing project and select "Switch to Advanced Editor" in the bottom left of the window (Figure 1)
2. Expand "Runtime Settings" under Available Customizations, in the left pane, select the dropdown for "DevDetail" to reveal the **DNSComputerName** option
3. Locate the DNSComputerName on the right-hand side of the screen. "Remove" to take out the DNSComputerName altogether (Figure 2)
  - Clearing out the field "Placeholder" in the middle pane of the editor will not work, you will have to go to the right pane and select it
4. We are now ready to select "Export" from the menu bar up top, then select Export Provisioning package.
5. At the Describe the provisioning package. Feel free to accept the defaults and click "Next" or provide additional data
  - You might have several provisioning packages for different device types and if so, giving them descriptive names is a very good idea.
6. Up next is the Encrypt & Sign details which we will skip right past for the purpose of this scenario.
  - Selecting to encrypt the package will provide you with a password and the signing process should be straight forward if you are used to signing scripts and have a code signing certificate already available on your device. Click "Next".
7. Select a good place to store the finished provisioning package, then click "Next".
8. On Summary, click "Build".



# Remote Connectivity

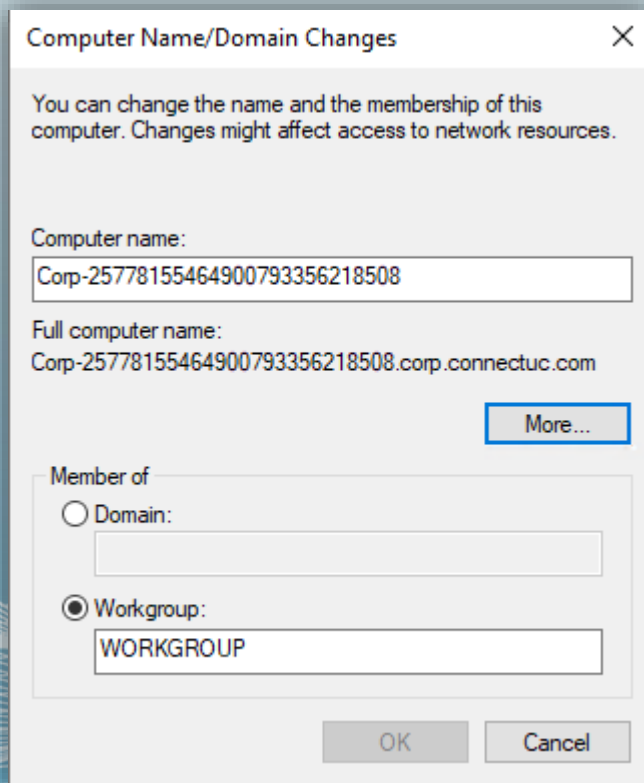
## Reasons on why to Reduce / Eliminate Network Reliance

- **Bandwidth:** Bandwidth utilization will increase with each additional client and residential internet speeds are constantly increasing. It may be difficult to guarantee that your VPN solution will accommodate everyone's traffic.
- **Licensing:** With employees potentially having multiple devices, the price per user may increase
- **Directory Services:** Traditional Active Directory means occasional connectivity, or your device ends up being tombstone (typically 180 days)
- **Files / Apps:** On-premises infrastructure to host data and business applications mean costs for servers, datacenter, bandwidth, etc
- **Security:** Securing the traffic to and from your corporate network may introduce additional costs and configurations such as encryption and multi factor authentication to prevent unauthorized connections

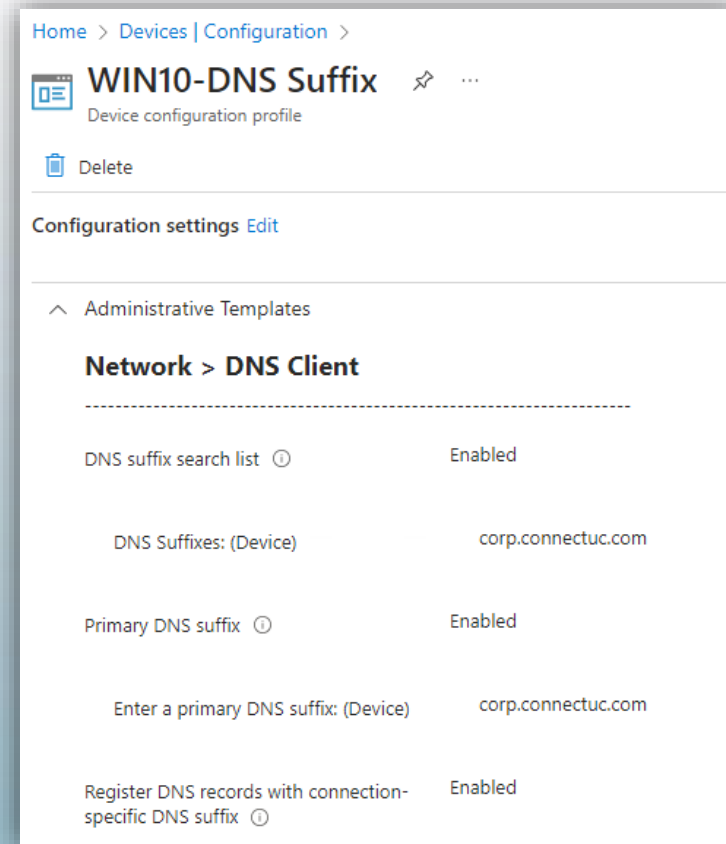
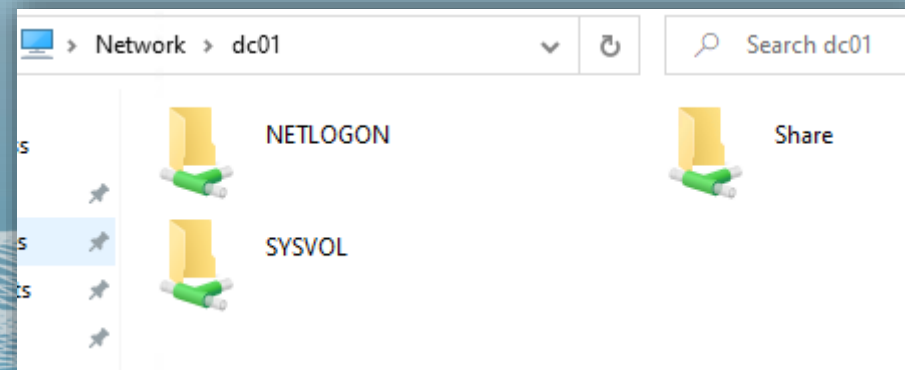


# Name Resolution / DNS

- When connectivity is needed, Netbios access to file shares and servers is possible
- Leverage an Intune device configuration policy to set the FQDN on the machine and register with DNS



With AzureAD join, the device is still a workgroup joined, however with the suffix registered we can access network resources easily



**NOTE:** This “technically” violates one of the core tenants of Zero Trust by allowing lateral movement from PC to server for file access, but the management plane is changes from on-prem to cloud

# Printing

## Universal Print: print from anywhere, anytime without VPN!

- Included in E3, E5
- Each license adds to a "pool" of print jobs
  - 15 copies of a 10-page document sent to the printer is counts as a single print job
  - A tenant with 100 E3 licenses will have 10,000 jobs per month available across the organization
- Install the connector on a server with your printers, and register the devices in the Universal Print admin through Azure
  - There are printers that are compatible to directly connect to the UP service and don't require an agent/Print server.

## Printers & scanners

### Add printers & scanners



Refresh

Work or school printer & scanner

Search location: [Please select a search location](#)

Keywords

Searching for printers and scanners

NPI804E29 (HP LaserJet CM1415fnw)  
Cloud printer

## List of subscriptions that include Universal Print

Organizations that have one of the following subscriptions have licenses for Universal Print.

| Subscription                                |
|---|
| Microsoft 365 Enterprise F3, E3, E5, A3, A5 |
| Windows 10 Enterprise E3, E5, A3, A5        |
| Microsoft 365 Business Premium              |
| Universal Print (standalone)                |

All Universal Print licences grant access to the full suite of features & capabilities offered by the service.

Additionally, each license adds to a pool of print jobs that are available to all users who have a license. The number of jobs that each license contributes to the pool depends on the license type, and unused jobs expire at the end of each month:

| License                                    | Jobs Per Month |
|--|----------------|
| Microsoft 365 E3, E5                       | 100            |
| Microsoft 365 A3, A5, F3, Business Premium | 5              |
| Windows 10 Enterprise E3, E5, A3, A5       | 5              |
| Universal Print (standalone)               | 5              |

Universal Print connector (1.91.8599.40935)

Manage registered printer settings: [Universal Print portal](#)

[Privacy and Cookies](#)

### Universal Print connector configuration

Local service name: Print Connector service  
Local service status: Running  
Connector name: WHISKEY.HOME.LOCAL

### Registered printers:

| <input type="checkbox"/> | Printer name                      |
|--------------------------|-----------------------------------|
| <input type="checkbox"/> | NPI804E29 (HP LaserJet CM1415fnw) |

[Collect printer diagnostics](#) [Collect connector diagnostics](#)

### Billing Summary

Usage this month and information about your purchased print volume

Billed Print Jobs: 0

Remaining Print Jobs: 125

Total Print Capacity: 125

### Totals

Current resource counts

Printers: 1

Shares: 1

Connectors: 1

Home > Universal Print

## Universal Print | Printers

Search

Share Unregister Refresh Edit columns Give Feedback

Add filter

Search by printer name, manufacturer, or model

| <input type="checkbox"/> | Name                              | Printer stat... | Share Status | Share Name        | Last Seen  |
|--------------------------|-----------------------------------|-----------------|--------------|-------------------|------------|
| <input type="checkbox"/> | NPI804E29 (HP LaserJet CM1415fnw) | Ready           | Shared       | NPI804E29 (HP ... | 18 minutes |

# Remote Help

## Support Users :

- Requires Intune subscription AND Remote Help license (add-on or via Intune Suite)
- Supported on Windows 10/11, Windows 10/11 on ARM64, Windows 365, Android Enterprise, macOS 11/12/13
- Requires tenant configuration
- Intune > Tenant administration > Remote help > Settings (tab) > Enable Remote help
  - Configure permissions (Intune RBAC)
    - Elevation: Yes/No
    - View screen: Yes/No
    - Take full control: Yes/No
    - Unattended control: Yes/No
    - *The "Help Desk Operator" Intune role sets these all to "Yes" by default*
- Monitor remote help sessions in Tenant admin > Remote Help

| Average session time | Total sessions |
|----------------------|----------------|
| 100                  | 100            |
| 80                   | 80             |
| 60                   | 60             |
| 40                   | 40             |

\*Session ran longer than 4 hours and/or had an unexpected error.

Showing 0 to 0 of 0 records

| Provider ID ↑↓     | Recipient ID ↑↓ | Recipient name ↑↓ | Device name ↑↓ |
|--------------------|-----------------|-------------------|----------------|
| No sessions found. |                 |                   |                |

Home > Tenant admin

### Tenant admin | Remote Help

Search

- Tenant status
- Remote Help**
- Microsoft Tunnel Gateway
- Connectors and tokens
- Filters
- Roles
- Azure AD Privileged Identity Management
- Diagnostics settings

Monitor **Settings** Remote Help sessions

Refresh Configure

Remote Help: Enabled

Remote Help to unenrolled devices: Allowed

**Remote Help requirements**

Remote Help supports Windows, Android, and macOS at this time. Both the Helpdesk admin who's providing help and the user receiving help must be enrolled in Intune.

[Learn more about Remote Help](#)

- 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)

# Communicating To Your Users

## Does your user base always see important org emails? 😊

- *Intune > Tenant Admin > Organizational Messages*
  - *W11 only*
- *Intune > Tenant Admin > Custom Notifications*
  - *Mobile devices only (Android / iOS)*
  - *Leverages mobile Company Portal app*

**What are Organizational messages?**

You can send messages with your organization's logo directly to your users through their Windows 11 devices. Select from a variety of common messages for display just above their taskbar, in their Notifications, or when they run the Get Started app. [Learn more about organizational messages](#)

ⓘ Assignments support Azure Active Directory user groups only. Device groups aren't supported and mixed groups will deliver messages only to users.

|  |   |   |
|--|---|---|
| <b>Taskbar messages</b><br>Choose this message type to display a message on users' desktops, just above their taskbar.<br><a href="#">View</a> | <b>Notifications area messages</b><br>Select this message type to display a message in your users' Notifications.<br><a href="#">View</a> | <b>Get Started app messages</b><br>These messages appear just once, the first time the Get Started app runs after a device is enrolled in Intune.<br><a href="#">View</a> |
|--|---|---|


### Taskbar messages

**What is a Taskbar message?**

These messages appear attached to the user's taskbar, on top of everything else on the desktop.

**What you'll need**

- Use your MDM tool to enable the AllowWindowsSpotlight, AllowWindowsTips, and EnableOrganizationalMessages policies.
- Prepare a 64 x 64 pixel logo for your organization in PNG format with a transparent background.
- Select a URL for one of your websites that you want your users to visit by following the link in the message.



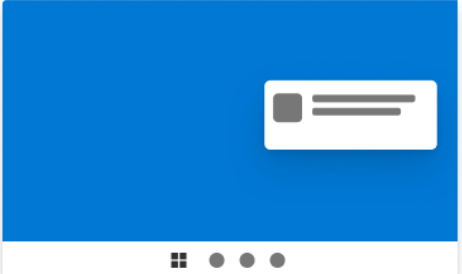
### Notifications area messages

**What is a Notifications area message?**

This message will appear in the Notifications area of your users' devices.

**What you'll need**

- Use your MDM tool to enable the AllowWindowsSpotlight, AllowWindowsSpotlightOnActionCenter, and EnableOrganizationalMessages policies.
- Prepare a version of your organization's logo that's 48 x 48 pixels, in PNG format with a transparent background.
- Select a URL for one of your websites that you want your users to visit by following the link in the message.




### Get Started app messages

**What is a Get Started app message?**

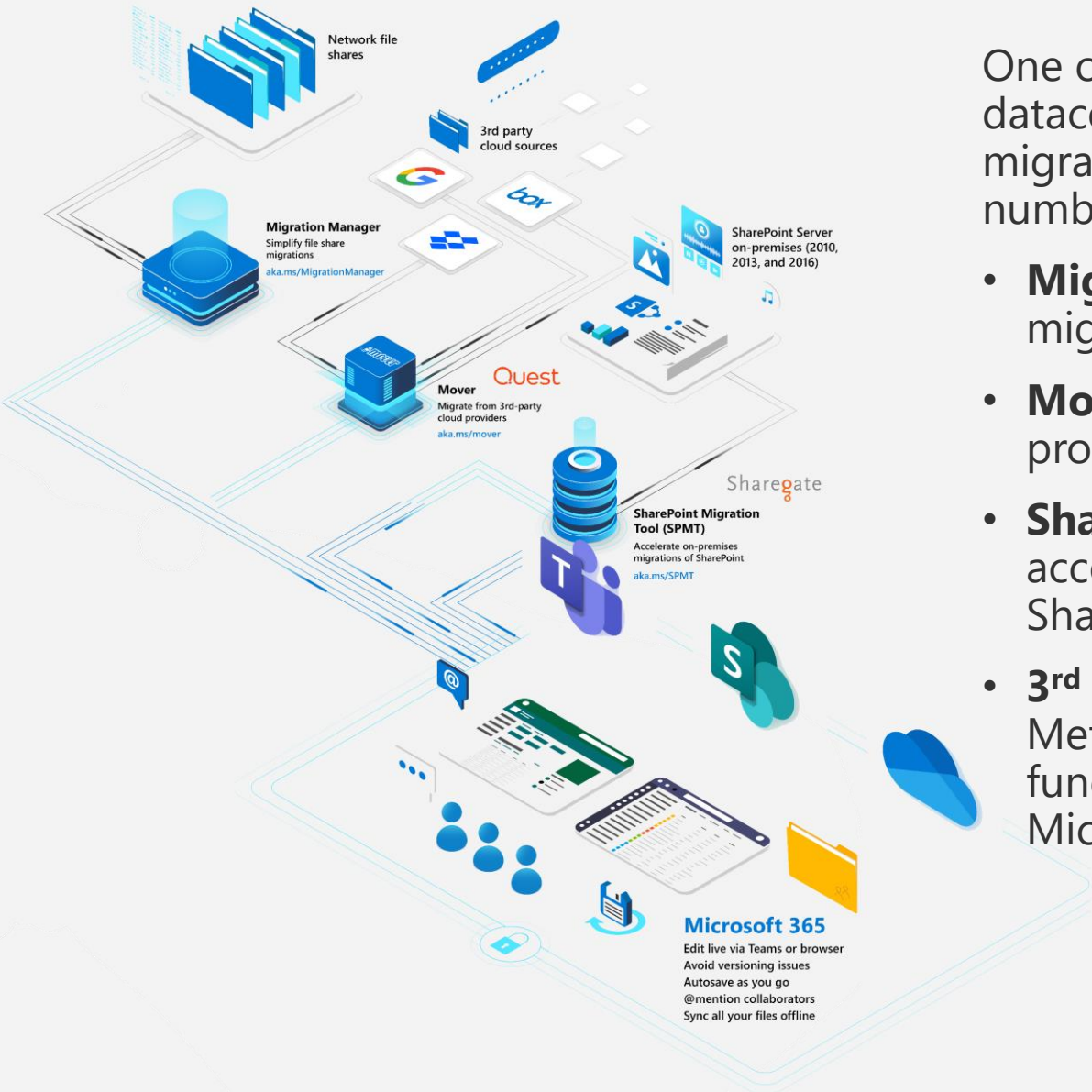
These messages appear in the Get Started app the first time the user runs it after their device is enrolled in Intune. They're great for welcoming new users to your organization, since you can direct them to info about org benefits and structure, device tips, training, org policies, and how to get tech support. There are also links to info about personalizing their device and setting up their PC profile.

**What you'll need**

- Use your MDM tool to enable the AllowWindowsSpotlight and EnableOrganizationalMessages policies and turn off the DisableCloudOptimizedContent policy.
- Prepare a version of your org's logo that's 50 to 100 pixels wide by 50 pixels high in PNG format with a transparent background.
- Select URLs for up to two of your websites that you want users to visit in order to get started.



# Moving Files to the Cloud



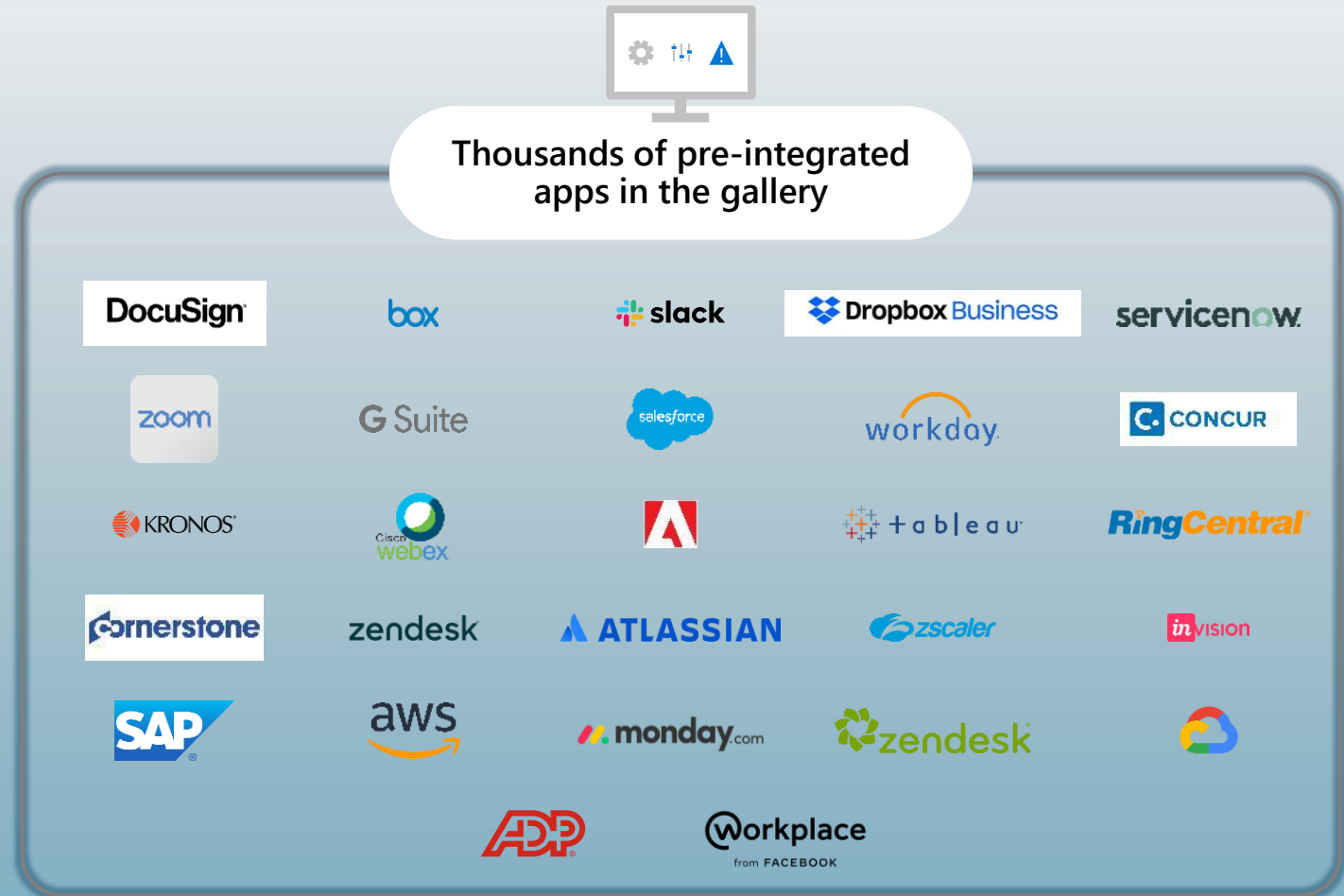
One of the biggest ways to shrink your datacenter footprint is through content / file migration into Microsoft 365, and there are a number of ways to move your data:

- **Migration Manager** – simplify file share migrations
- **Mover** – migrate from 3rd-party cloud providers
- **SharePoint Migration Tool (SPMT)** – accelerate on-premises migrations of SharePoint
- **3<sup>rd</sup> party tools** – using tools like Quest Metalogix or Sharegate provide additional functionality where gaps may exist in Microsoft toolsets

# Moving to Cloud-based Applications

» The Azure AD app gallery has thousands of applications that are pre-integrated for single sign-on

» For applications not available in the Azure AD app gallery, create your own application and connect them directly with custom templates



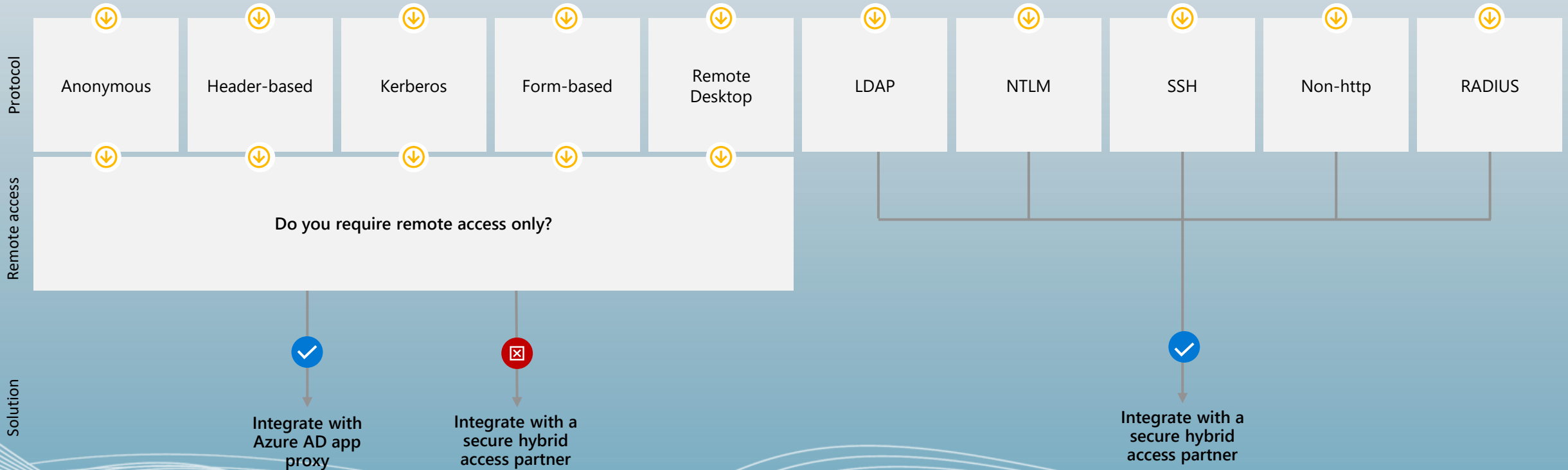


# Transitioning Applications to the Cloud

*For apps that won't be modernized and using legacy authentication protocols*



What legacy authentication protocol is the app using?





# Conversion Options

*One Size Does Not Fit All!*



# Toolsets For the Job



Windows Autopilot

**Quest**<sup>®</sup>  
On Demand Migration



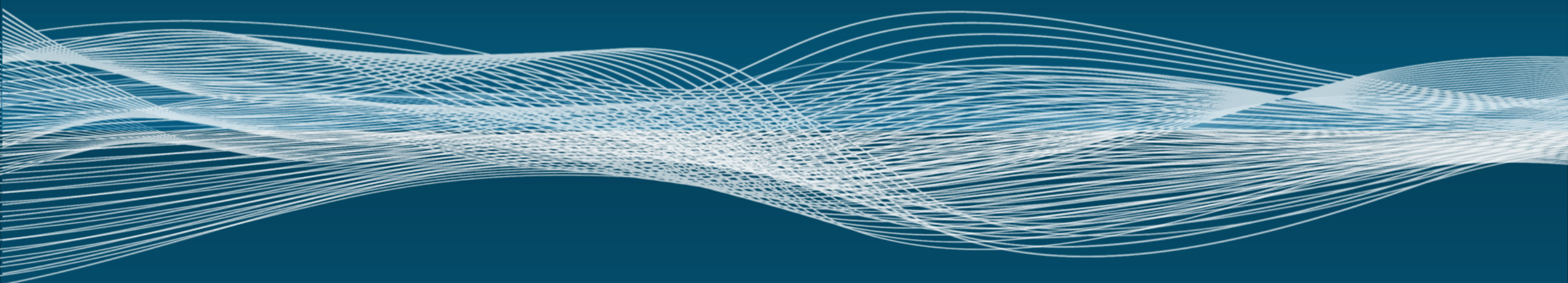
**FORENSIT**

FORENSIT USER PROFILE WIZARD  
CORPORATE EDITION  
DOMAIN TO DOMAIN MIGRATION





# Windows Autopilot



# Windows Autopilot (with reset)

Leveraging an Autopilot config file (JSON) that points the endpoint to an Autopilot deployment profile that pre-exists in the target tenant during OOBE.

## Strengths

- Flexible deployment
  - Allows user or Admin to initiate process (depending on user permissions)
  - Can customize to include more automation
- Leverages existing environment for prep
  - Pushing JSON file via MDM
- Allows migration directly to Azure AD join or Hybrid (if in network)
- **Microsoft recommended** path from traditional AD Join to Azure AD Join
- Does not require bulk enrollment token

## Challenges

- **Requires device reset**
- **Requires time after reset** for application reinstallation and reconfiguration (up to several hours)
- Data must be restored from OneDrive or other backup post migration.
- Requires preparation of configuration package (Win32 app)
- Requires network connectivity & user interaction (OOBE)

## Other

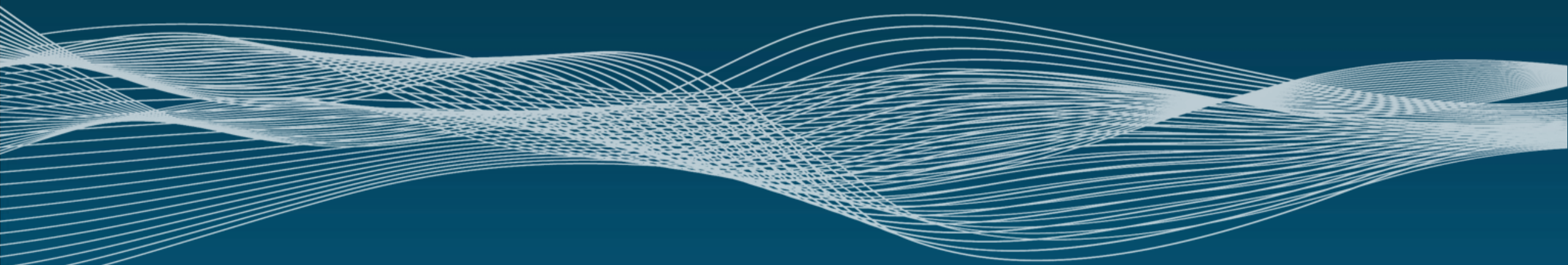
- No additional licensing required, compared to other tools
- Prep Effort: Low
- User Impact: High

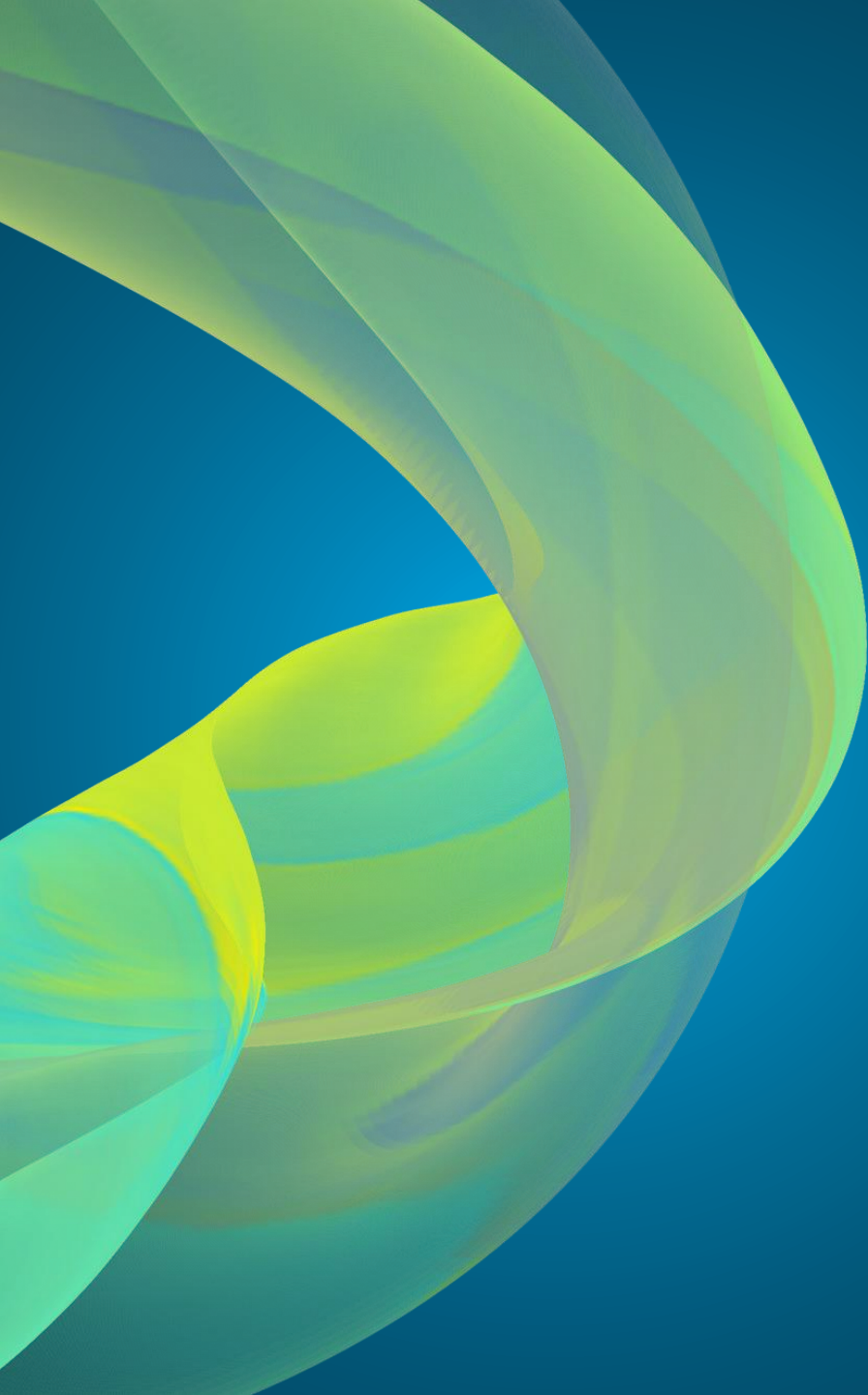
Summary: While this is the Microsoft recommend path for migration, the requirement around device wipe and time needed after reset may not make this the ideal path for migration.



# Demo – AutoPilot Reset

Evan





*Concurrency*

Break

# AutoPilot Reset Overview

## Endpoint Readiness

- Existing MDM authority will determine method for deploying JSON file
- Prepping user data
  - Validating OneDrive health; Healthy sync status, KFM enabled (Desktop, Documents, Pictures)

## Creating JSON file

- Determine Autopilot Deployment Profile/Tenant
- Leverage PowerShell and Graph API to create/extract JSON
- Push JSON file to endpoints (Win32 app)

## Device Wipe

- Admin initiated Intune "wipe" command
- User initiated wipe via Windows settings
- Options to customize
  - i.e. Further automation; simplifying the process further for the users
- Validating success





# Preparing Endpoints - Autopilot Reset

- Determine endpoint management status for method of pushing Autopilot JSON config file.
  - MDM authority in the cloud (i.e. Intune, KACE, Mobile Iron, etc)
  - MDM authority on local domain (i.e. GPO/SCCM)
  - You can also use "dsregcmd /status" in command prompt for a more detailed reporting

- Verify endpoint is ready for migration
  - Review OneDrive health and sync [enable via MDM config policy]
    - Config.office.com > Health > OneDrive sync
    - Confirm PC is listed + backing up (healthy), Known folders: ALL (can use MDM to further configure)
    - MDM policy can enable KFM, health reporting, SSO

```
C:\Users\estueve>dsregcmd /status
```

```
-----+-----+
| Device State |
+-----+-----+

AzureAdJoined : YES
EnterpriseJoined : NO
DomainJoined : NO
Device Name : EV-WORK4

-----+-----+
| Device Details |
+-----+-----+

DeviceId
Thumbprint
DeviceCertificateValidity
KeyContainerId
KeyProvider
TpmProtected
DeviceAuthStatus

-----+-----+
| Tenant Details |
+-----+-----+

TenantName
TenantId
```

### Device state

This section lists the device join state parameters. The criteria that are required for the device to be in various join states are listed in the following table:

| AzureAdJoined | EnterpriseJoined | DomainJoined | Device state                  |
|---------------|------------------|--------------|-------------------------------|
| YES           | NO               | NO           | Microsoft Entra joined        |
| NO            | NO               | YES          | Domain Joined                 |
| YES           | NO               | YES          | Microsoft Entra hybrid joined |
| NO            | YES              | YES          | On-premises DRS Joined        |

**Note**  
The Workplace Joined (Microsoft Entra registered) state is displayed in the "User state" section.

- **AzureAdJoined:** Set the state to YES if the device is joined to Microsoft Entra ID. Otherwise, set the state to NO.
- **EnterpriseJoined:** Set the state to YES if the device is joined to an on-premises data

### OneDrive Sync app health

Overview Devices Issues

Find detailed information about users and devices, including sync errors, operating system, folder ba

| User ↑ | User email         | Device name     | Errors  | Known folders | App version      | Operating system | Last synced | Last st |
|--------|--------------------|-----------------|---------|---------------|------------------|------------------|-------------|---------|
| Lee Gu | LeeG@corp.conne... | CORP-2577815546 | Healthy | All           | 23.189.0910.0001 | Windows 10       | Unknown     | 10/5/2  |

Home > Devices | Configuration profiles > WIN10-ODfB Setup > Edit profile - WIN10-ODfB Setup

Settings catalog

- Enable sync health reporting for OneDrive: Enabled
- Hide the "Deleted files are removed everywhere" reminder: Enabled
- Prevent users from syncing personal OneDrive accounts (User): Enabled
- Silently move Windows known folders to OneDrive: Enabled
- Show notification to users after folders have been redirected: (Device) \* No
- Tenant ID: (Device) 0cf1000a-f2b2-4206-b5de-109ea0169973
- Silently sign in users to the OneDrive sync app with their Windows credentials: Enabled
- Sync Admin Reports: Enabled
- Tenant Association Key: (Device) eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJodHRwOi8vc2NoZW1hcy50...
- Use OneDrive Files On-Demand: Enabled

# Creating JSON config file - Autopilot Reset

- Create an Autopilot Deployment profile in target tenant (or using existing)
  - Autopilot Deployment profile in target is required to extract JSON config file, as it will be the profile the device uses to join AutoPilot after a wipe.
- Creating the JSON config file
  - Determine Autopilot profile to use
  - Use Powershell to create JSON
    - Connect to MgGraph with an account that has the required permissions.
    - Once you are authenticated to your tenant, run the PS command to convert AP profiles to JSON files.

Home > Devices | Windows > Windows | Windows enrollment > Windows Autopilot deployment profiles >

## Create profile

Windows PC

Basics 2 Out-of-box experience (OOBE) 3 Assignments 4

Configure the out-of-box experience for your Autopilot devices

Deployment mode \*

Join to Azure AD as \*

Microsoft Software License Terms

Privacy settings

Hide change account options

**Basics Edit**

Name: Autopilot Azure

Description: \*\*

Convert all targeted devices to Autopilot Yes

Device type: Windows PC

This PC > Windows (C:) > Autopilot >

Name

- Autopilot Profile
- Autopilot Profile 2

AutopilotConfigurationFile.json - Notepad

```
File Edit Format View Help
{"CloudAssignedDomainJoinMethod": 0,
"CloudAssignedDeviceName": "AP-%SERIAL%",
"CloudAssignedAutopilotUpdateTimeout": 1800000,
"CloudAssignedForcedEnrollment": 1,
"Version": 2049,
"CloudAssignedTenantId": "0cf1000a-f2b2-4206-b5de-109",
"CloudAssignedAutopilotUpdateDisabled": 1,
"ZtdCorrelationId": "bcbe44e4-30a0-49b7-97e4-ae6c2dd7",
"Comment_File": "Profile Autopilot Profile 2",
"CloudAssignedAadServerData": "{ \"ZeroTouchConfig\": {",
"CloudAssignedOobeConfig": 1308,
"CloudAssignedTenantDomain": "corp.connectuc.com",
"CloudAssignedLanguage": "os-default"
}
```

```
PS C:\WINDOWS\system32> Connect-MgGraph -tenantID $tenantID -Scopes "Device.ReadWrite"
Welcome to Microsoft Graph!
Connected via delegated access using 14d82eec-204b-4c2f-b7e8-296a70dab67e
Readme: https://aka.ms/graph/sdk/powershell
SDK Docs: https://aka.ms/graph/sdk/powershell/docs
API Docs: https://aka.ms/graph/docs
NOTE: You can use the -NoWelcome parameter to suppress this message.
PS C:\WINDOWS\system32>
```

Microsoft

backupadmin@corp.connectuc.com

### Permissions requested

Microsoft Graph Command Line Tools  
unverified

This app would like to:

- Read and write all device properties
- Read and write Microsoft Intune devices
- Read and write Microsoft Intune configuration
- Read and write domains
- Read and write all groups
- Read and write group memberships
- Sign in and read user profile
- Maintain access to data you have given it access to

Consent on behalf of your organization

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their [terms of service](#) and [privacy statement](#). You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

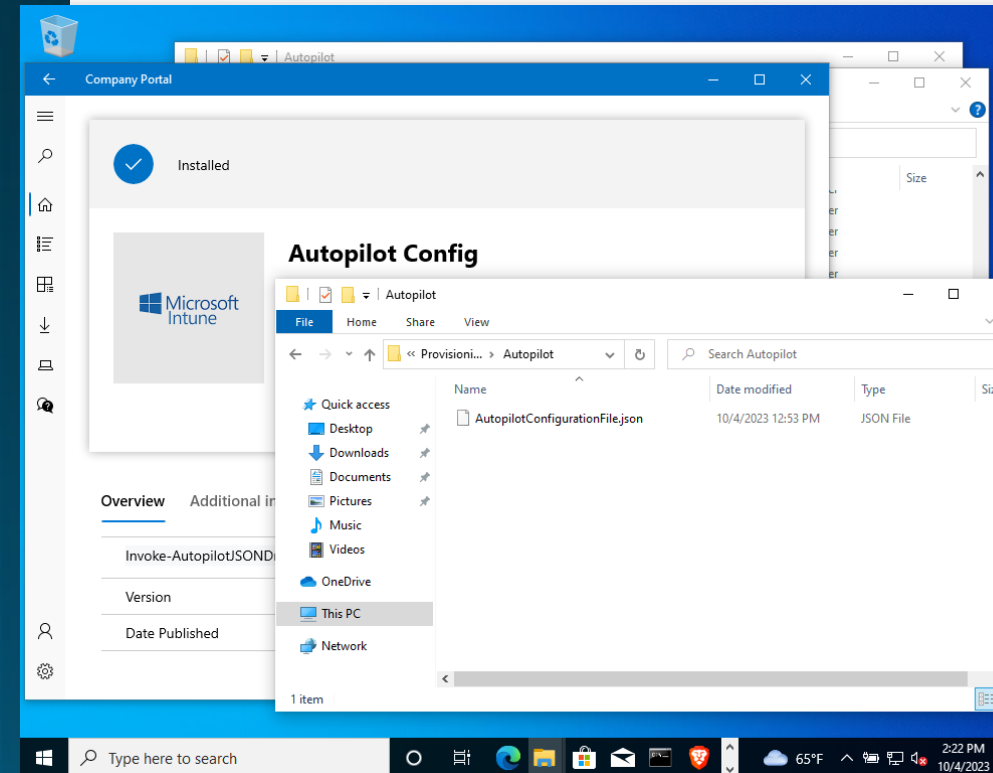
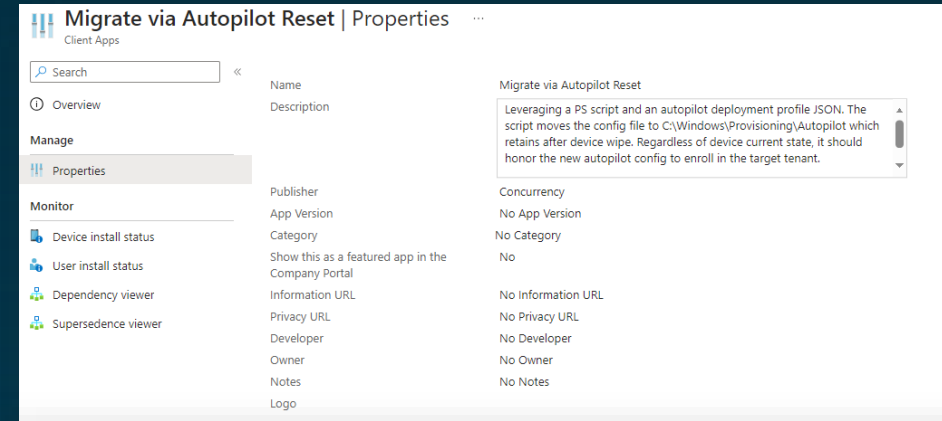
Does this app look suspicious? [Report it here](#)

# Deploying JSON file – Autopilot Reset

## Creating an Intune Win32 app with PowerShell to push the JSON config file and put it in the correct directory

- Download the Win32 Content Prep Tool from GitHub
- Generate JSON file for your target Autopilot deployment profile using "Invoke-AutopilotJSONDrop.ps1".
- Upload packaged app to Intune
- Determine how app will be deployed:
  - Group assignment: Set to required – force installs automatically
  - Group assignment: Set to available – user or admin can manually install on demand via Company Portal

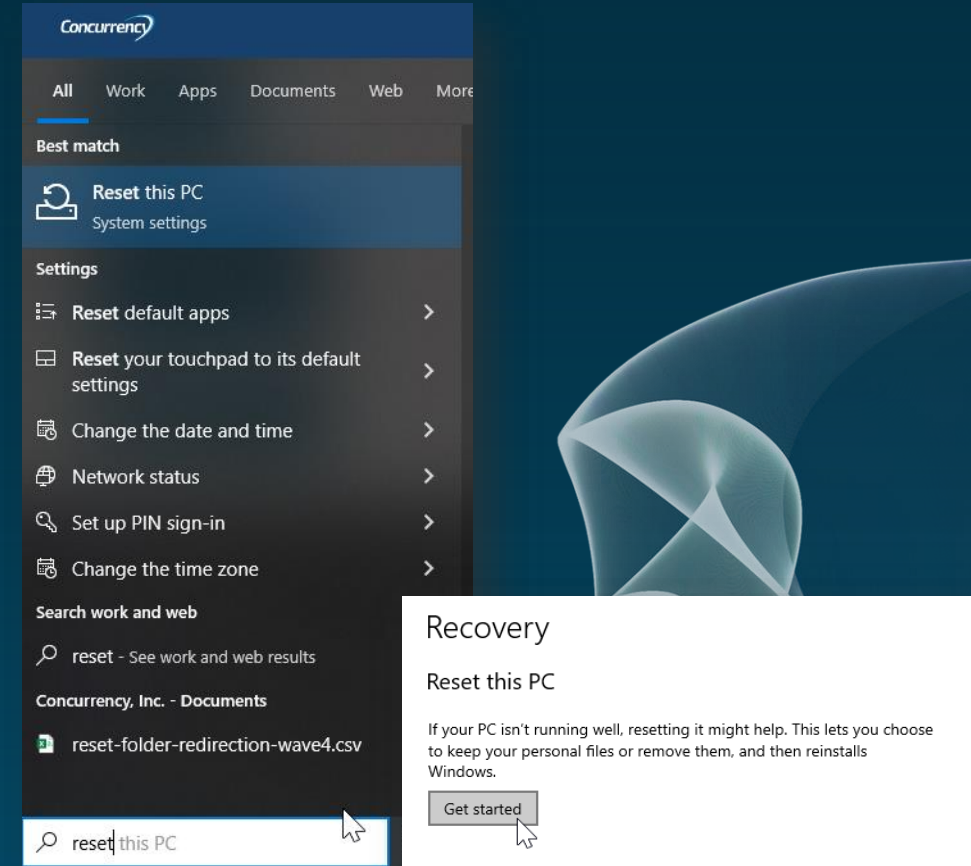
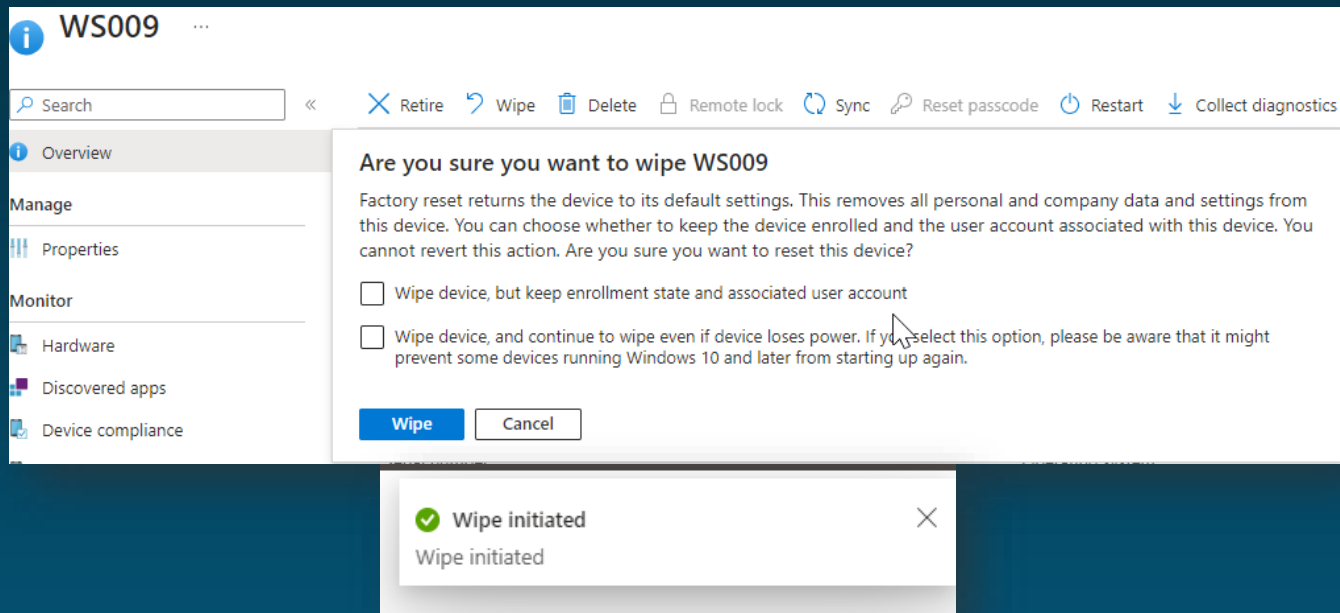
This is a **supported process** by Microsoft; more details @ <https://learn.microsoft.com/en-us/autopilot/tutorial/existing-devices/create-json-file>



# Device Wipe – Autopilot Reset

## Reset Device

1. Administrator reset – Intune "Wipe" command on Device page
2. Manual/user-initiated reset -- "Reset this PC" (must have local administrator rights)
3. Scripted interactive process



# Validating Success – Autopilot Reset

- "Welcome to [Company]!" screen during OOB (user experience)
- Device name is updated based on the Deployment profile for Autopilot i.e. AP-%SERIAL%
- IF you have a Windows Hello policy, you'll have to setup enrollment again
- Once the user is in Windows, it may take several hours to deploy configuration profiles and applications

Windows | Windows devices

Apply device name template Yes  
Enter a name AP-%SERIAL%

Search Refresh Export Columns Bulk device actions

Windows devices  
Windows enrollment

OS: Windows, Windows Mobile, Windows Holographic

| Device name     | Managed by | Ownership | Compliance |
|-----------------|------------|-----------|------------|
| AP-465698321468 | Intune     | Corporate | Compliant  |

Account

Welcome to Contoso!  
Enter your Contoso email.

alexw@corp.connectuc.com

Sign in with a security key

Need help?  
Contoso

Privacy & cookies Terms of use Next

Home > Devices | Overview > Windows | Windows devices > AP-797011211784

AP-797011211784 | Device configuration

Search Export

Overview

Manage

Properties

Monitor

Hardware

Discovered apps

Device compliance

| Policy                          | Logged in user           |
|---------------------------------|--------------------------|
| WIN10-DNS Suffix                | AlexW@corp.connectuc.com |
| WIN10-ODfB Setup                | System account           |
| WIN10-ODfB Setup                | AlexW@corp.connectuc.com |
| Win10-DeviceConfig-Restrictions | System account           |
| Win10-DeviceConfig-Restrictions | AlexW@corp.connectuc.com |

Home > Devices | Overview > Windows | Windows devices > AP-797011211784

AP-797011211784 | Managed Apps

Search Refresh

Overview

Manage

Properties

Monitor

Hardware

Discovered apps

Device compliance

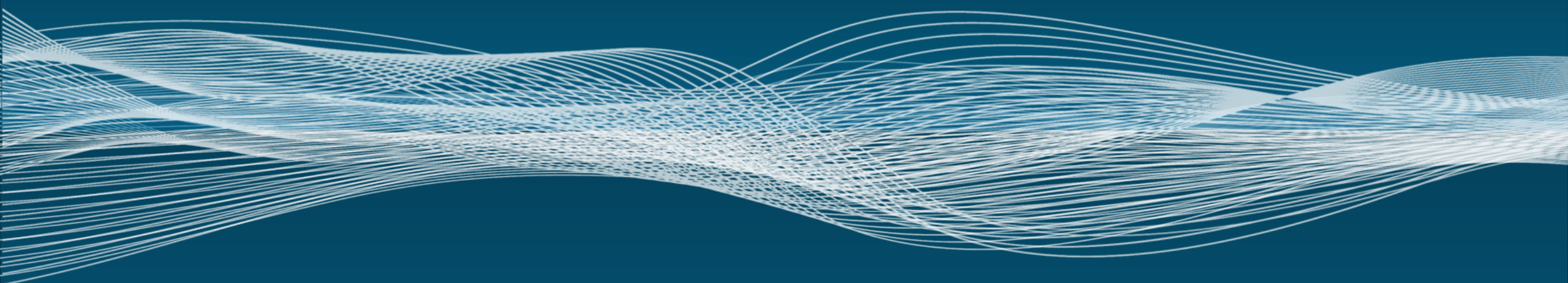
Device configuration

App configuration

| Application                            | Version       | Resolved intent  | Installation status     |
|--|---------------|------------------|-------------------------|
| Microsoft 365 Apps for Windows 10 ...  |               | Required install | Waiting for install ... |
| Microsoft Edge for Windows 10 and I... | 117.0.2045.60 | Required install | Installed               |
| Remote Help Installer                  |               | Required install | Installed               |
| Company Portal                         | 11.2.179.0    | Required install | Installed               |
| ForensIT User Profile Wizard           | 1.3           | Available        | Available for install   |
| Migrate via Autopilot Reset            |               | Available        | Available for install   |



# ForensIT User Profile Wizard (ProfWiz)



# User Profile Wizard (ProfWiz)

## Strengths

- Migrates all user profile data and settings on Windows 10 and Windows 11
- Automatically joins a machine to a new domain
- Includes Enterprise strength scripting support
- Supports push migrations of remote machines over a VPN
- Does not move, copy or delete any data. Instead, it configures the profile "in place"
- Migrates user profile and device quickly compared to other migration options
- **Agentless deployment**

## Challenges

- Not an officially recommended Microsoft path to Azure AD Join
- May require extra orchestration / change management to communicate to users
- Live monitoring capability is limited to Azure/Intune; no direct interface
- Customizable, but options can be limited

## Other

- ProfWiz Enterprise Licensing per endpoint (**\$2.95 per device, minimum 50**)
- Prep Effort: Medium
- User Impact: Low

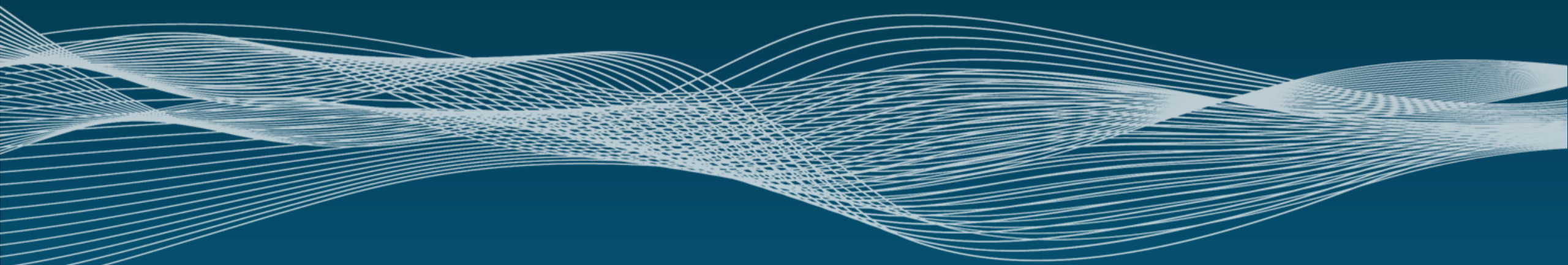
Summary: Recommended option as it meets the most requirements. Requires additional licensing.





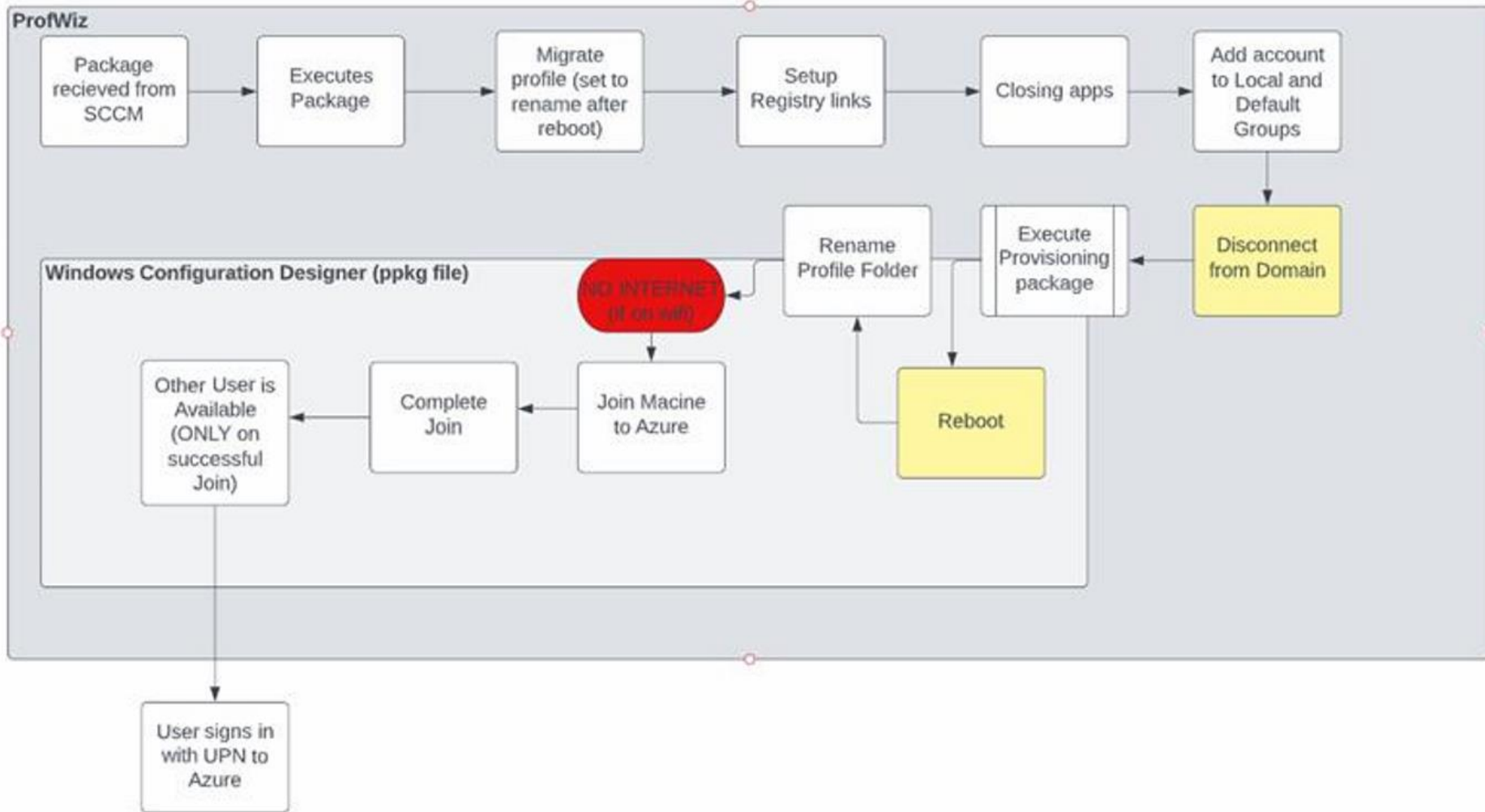
# Demo – ProfWiz

Kevan



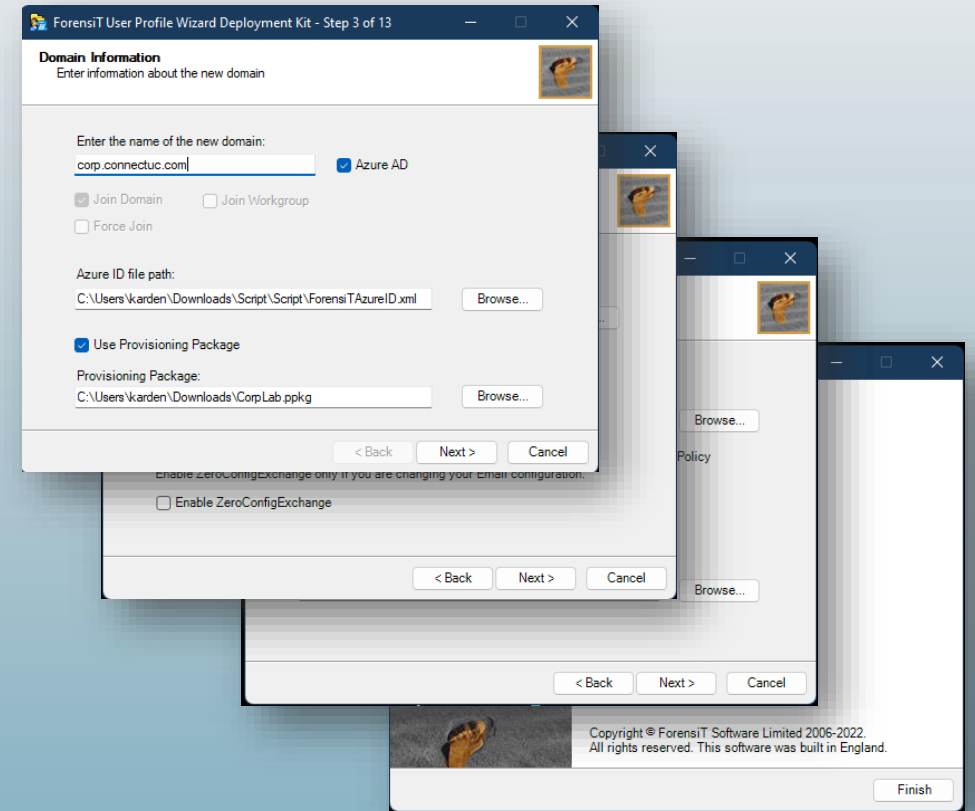


# ProfWiz Visual Workflow



# Create ProfWiz Config File

- Add license
- Create the XML configuration file needed for ProfWiz to automate a migration on a large scale.
- Create the User Lookup File .CSV
- Open the **User Profile Wizard Deployment Kit** and, create your migration project, and generate your Deployment file.



# Profwiz Migration Process

- We can monitor the [successful] migration process thru the Audit log in Azure AD, or on the workstation
- Detection method in Intune app will rely on the ForensITMigrated file to report a successful install

```

Migrate - Notepad
File Edit Format View Help
ForensIT User Profile Wizard 24.4.1289
Licensed to [REDACTED] (1000000 Seats) License No. [REDACTED]
Copyright (c) 2002-2022 ForensIT Software Ltd
www.ForensIT.com

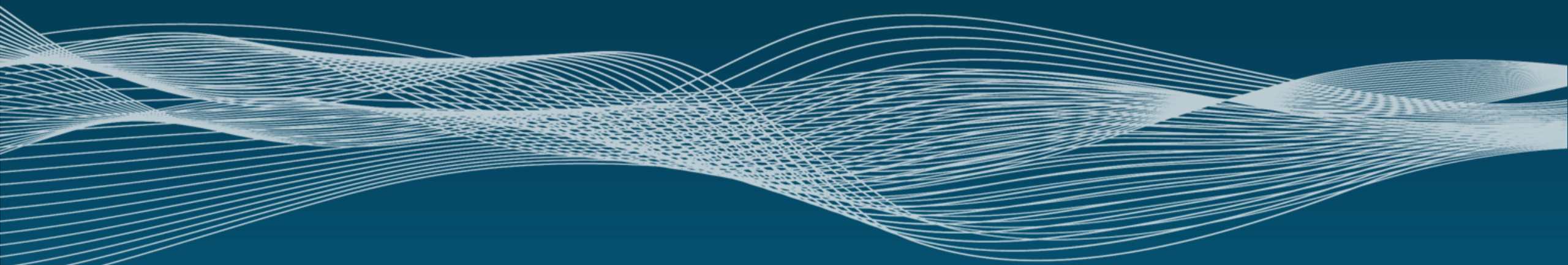
27/09/2023 15:26:38.230 Creating migration service... Done.
27/09/2023 15:26:38.386 Starting migration service... Done.
27/09/2023 15:26:39.585 Target device: WS008
27/09/2023 15:26:39.658 OS build 10.0.19045.3448. Version 22H2.
27/09/2023 15:26:39.687 Domain: CORP
27/09/2023 15:26:39.751 Migrating user account "LeeG"
27/09/2023 15:26:39.903 Processing UWP Apps... Done.
27/09/2023 15:26:41.154 Setting Registry ACLs... Done.
27/09/2023 15:26:43.935 Set Registry ACLs in 2.727 seconds.
27/09/2023 15:26:43.947 Closing Apps... Done.
27/09/2023 15:26:44.319 Setting Profile ACL... Done.
27/09/2023 15:26:53.229 Set Profile ACL in 8.889 seconds.
27/09/2023 15:26:53.243 Creating Profile registry keys... Done.
27/09/2023 15:26:53.271 Renaming Profile Folder... Done.
27/09/2023 15:26:55.287 Rename on reboot.
27/09/2023 15:26:55.531 Adding new account to local groups... Done.
27/09/2023 15:26:55.822 Setting LeeGu as default logon... Done.
27/09/2023 15:26:56.037 Excluding user account "Administrator"
27/09/2023 15:27:26.225 Calling Provisioning Package... Done.
27/09/2023 15:27:43.549 Migration Complete!
  
```

|                        |                              |        |                                    |         |                           |                              |
|------------------------|------------------------------|--------|------------------------------------|---------|---------------------------|------------------------------|
| 9/27/2023, 10:08:27 PM | Core Directory               | Device | Update device                      | Success | WS008                     | Device Registration Servi... |
| 9/27/2023, 3:56:04 PM  | Core Directory               | Device | Add device                         | Success | WS008                     | Sync_DC01_8b4cd0d9a2...      |
| 9/27/2023, 3:48:38 PM  | Core Directory               | Device | Add registered users to device     | Success | LeeG@corp.connectuc.c...  | Microsoft Intune             |
| 9/27/2023, 3:48:38 PM  | Core Directory               | Device | Update device                      | Success | Corp-257781554649007...   | Microsoft Intune             |
| 9/27/2023, 3:48:37 PM  | Core Directory               | Device | Add registered owner to device     | Success | LeeG@corp.connectuc.c...  | Microsoft Intune             |
| 9/27/2023, 3:48:37 PM  | Core Directory               | Device | Update device                      | Success | Corp-257781554649007...   | Microsoft Intune             |
| 9/27/2023, 3:48:37 PM  | Core Directory               | Device | Remove registered users from de... | Success | package_0f4aa142-ea2c-... | Microsoft Intune             |
| 9/27/2023, 3:48:37 PM  | Core Directory               | Device | Update device                      | Success | Corp-257781554649007...   | Microsoft Intune             |
| 9/27/2023, 3:48:37 PM  | Core Directory               | Device | Remove registered owner from d...  | Success | package_0f4aa142-ea2c-... | Microsoft Intune             |
| 9/27/2023, 3:48:37 PM  | Core Directory               | Device | Update device                      | Success | Corp-257781554649007...   | Microsoft Intune             |
| 9/27/2023, 3:37:39 PM  | Core Directory               | Device | Update device                      | Success | Corp-257781554649007...   | Microsoft Intune             |
| 9/27/2023, 3:37:34 PM  | Core Directory               | Device | Update device                      | Success | Corp-257781554649007...   | Microsoft Intune             |
| 9/27/2023, 3:36:30 PM  | Core Directory               | Device | Update device                      | Success | CORP-2577815546           | Microsoft Intune             |
| 9/27/2023, 3:36:29 PM  | Core Directory               | Device | Update device                      | Success | CORP-2577815546           | Microsoft Intune             |
| 9/27/2023, 3:34:51 PM  | Device Registration Servi... | Device | Register device                    | Success |                           | package_0f4aa142-ea2c-...    |
| 9/27/2023, 3:34:51 PM  | Core Directory               | Device | Add registered users to device     | Success | package_0f4aa142-ea2c-... | Device Registration Servi... |
| 9/27/2023, 3:34:51 PM  | Core Directory               | Device | Add registered owner to device     | Success | package_0f4aa142-ea2c-... | Device Registration Servi... |
| 9/27/2023, 3:34:51 PM  | Core Directory               | Device | Add device                         | Success | Corp-257781554649007...   | Device Registration Servi... |
| 9/27/2023, 3:34:01 PM  | Device Registration Servi... | Device | Unregister device                  | Success |                           | 9df1be97-920a-490f-bd...     |
| 9/27/2023, 3:34:01 PM  | Core Directory               | Device | Delete device                      | Success | Corp-257781554649007...   | Device Registration Servi... |
| 9/27/2023, 3:33:55 PM  | Device Registration Servi... | Device | Register device                    | Success |                           | package_0f4aa142-ea2c-...    |
| 9/27/2023, 3:33:55 PM  | Core Directory               | Device | Add registered users to device     | Success | package_0f4aa142-ea2c-... | Device Registration Servi... |
| 9/27/2023, 3:33:55 PM  | Core Directory               | Device | Add registered owner to device     | Success | package_0f4aa142-ea2c-... | Device Registration Servi... |
| 9/27/2023, 3:33:55 PM  | Core Directory               | Device | Add device                         | Success | Corp-257781554649007...   | Device Registration Servi... |
| 9/27/2023, 3:29:43 PM  | Device Registration Servi... | Device | Unregister device                  | Success |                           | 4c3f7b39-65eb-4017-8f...     |
| 9/27/2023, 3:29:43 PM  | Core Directory               | Device | Delete device                      | Success | WS008                     | Device Registration Servi... |



# Demo – ProfWiz

Kevan



# Considerations

## Environment

---

- Does not migrate encrypted data (ODBC connections / Saved Passwords)
- Does not migrate Edge Favorites or Chrome Bookmarks (will need to be signed in or exported)
- AV software can potentially block required processes; whitelisting required
- If wireless is managed by a 3rd party software (Cisco NAM) auto-reconnect option is needed for AADJ process to complete
- Cisco ISE can be a problem depending on how users authenticate on your corporate wireless network
- Conditional Access policies for MFA prompt need exclusions for off trusted network migrations or AADJ will fail
- There may be other environment caused issues not listed; pilot testing is very important

## Tool

---

- Requires WCD (Windows Configuration Designer) and Bulk Tokens
- Admin creating ppkg via WCD needs Administrator access to Azure AD, the Cloud Application Administrator role and Administrator rights to your SCCM environment (if using for deployment).
- Customizable using PS1 scripts wrapped into deployment package and/or via WCD Advanced options
- In a hybrid setup, a script to remove existing enrollments from the registry may be required to avoid a failure to AADJ
- Uses a user lookup file that will need updated regularly unless you implement a new on-boarding process prior to migration kick-off to allow net new users/devices to be deployed in the future state. This saves money on licensing since one is not consumed unnecessarily.

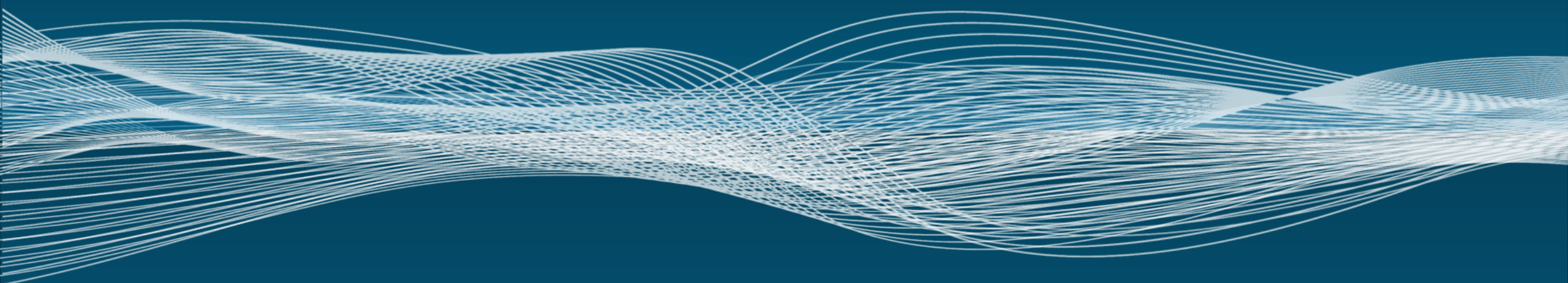
## OCM

---

- Pending updates should be completed prior to migration
- Quickly migrates user data and performs AADJ (20 minutes on avg.)
- OneDrive may need set back up as old path is based on SAM account name (When moving from On-prem to AAD)
- Drive mappings are retained (on-prem drives will require network access ie: directly on network or VPN connection)
- Unintended/premature user interaction can cause failures (user reboots during AADJ process due to impatience) Pilot testing is very important.
- End user comms need to be clear that user is to sign in with UPN account. Previous SAM account will show after completed migration and signing into this account creates temp accounts



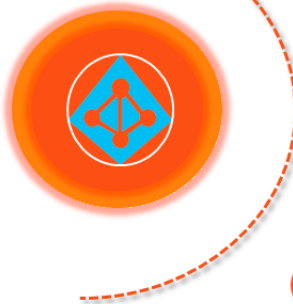
# Quest On-Demand Migration



# ODM AD(SaaS)

## Supported Migration Path

On Demand Migration Active Directory support many migration path scenarios to and from Microsoft Azure AD



Hybrid Azure AD → Hybrid Azure AD

On-Prem AD → Hybrid Azure AD

Hybrid Azure AD → Azure AD

On-Prem AD → Azure AD

From Azure AD (in a future release)

Quest

quest.com | confidential

Where Next

The screenshot shows a migration tool interface with a table of devices and an open 'AzureAD Cutover' dialog box. The dialog box has the following fields and options:

- AzureAD Cutover** (Title)
- AZUREAD PROFILE** (Section Header)
- Demo1-AZjoin** (Dropdown menu)
- IGNORE REACL STATUS**
- DO NOT START BEFORE** (08/31/2022 04:09 PM)
- APPLY** (Button)
- CANCEL** (Button)

The background interface shows a table with columns for 'Wave', 'sAMAccount Name', and 'Registered'. A row is selected with 'LAB1-W10AZs' and 'true'. The table has a search bar and a '1 of 1 selected' indicator.

# ODM AD (SaaS)

## Strengths

- Allows migration directly to Hybrid or AADJ with no on-premise requirement
- Does not require device reset
- Does not require time after reset for application reinstallation and reconfiguration
- Allows high customization and orchestration for change of apps and settings
- Better management pane of glass over other methods

## Challenges

- Moderate up front Administrator configuration needed to implement
- User cannot initiate migration, must be pushed from portal (future release)

## Other

- **Quest On Demand for Active Directory license (\$5 per device/ \$5 per named user for synchronization)**
- Prep Effort: High
- User Impact: Low

Summary: Recommended option if administrative migration only is acceptable. Limitation of no self-service migration and has a per device licensing cost.

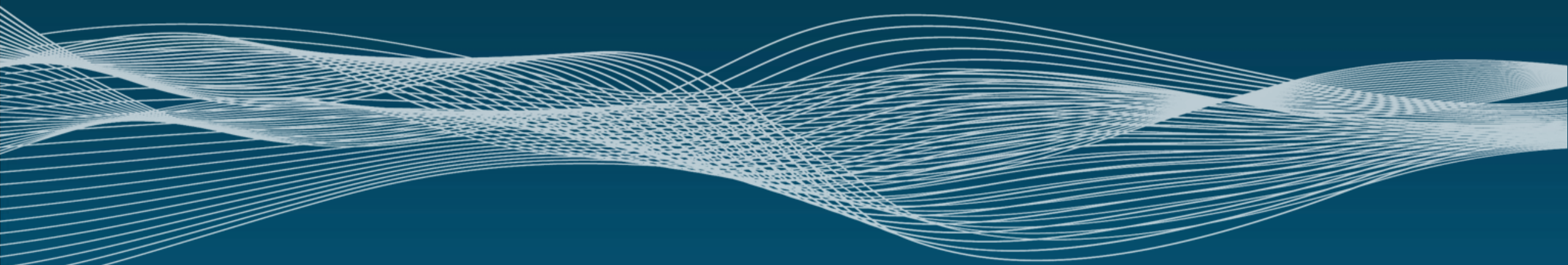




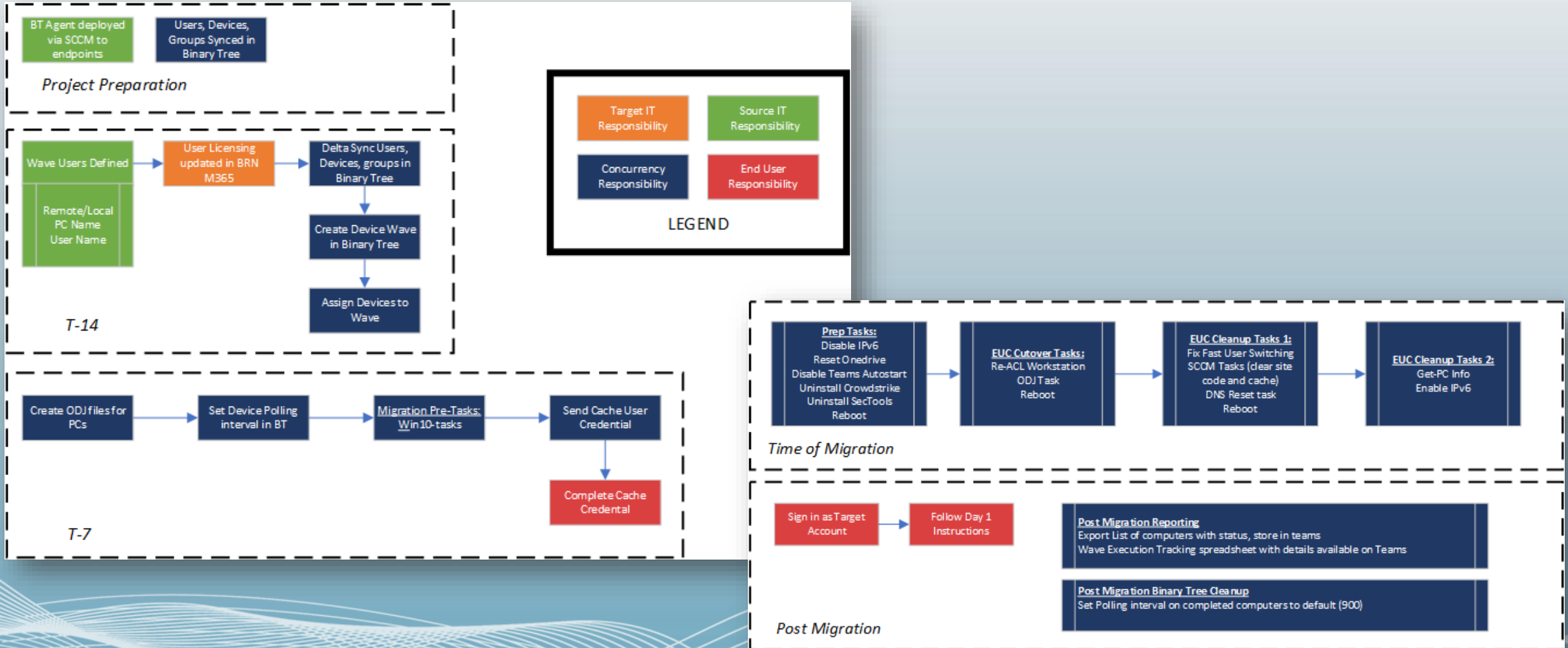


# Demo – ODM AD

Chris



# Sample Migration Workflow



# Considerations

## Environment

- Does not migrate encrypted data (ODBC connections / Saved Passwords)
- Does not migrate Edge Favorites or Chrome Bookmarks (will need to be signed in or exported)
- AV software can potentially block required processes; whitelisting required
- If wireless is managed by a 3rd party software (Cisco NAM) auto-reconnect option is needed for AADJ process to complete
- Cisco ISE can be a problem depending on how users authenticate on your corporate wireless network
- Conditional Access policies for MFA prompt need exclusions for off trusted network migrations or AADJ will fail
- There may be other environment caused issues not listed; pilot testing is very important

## Tool

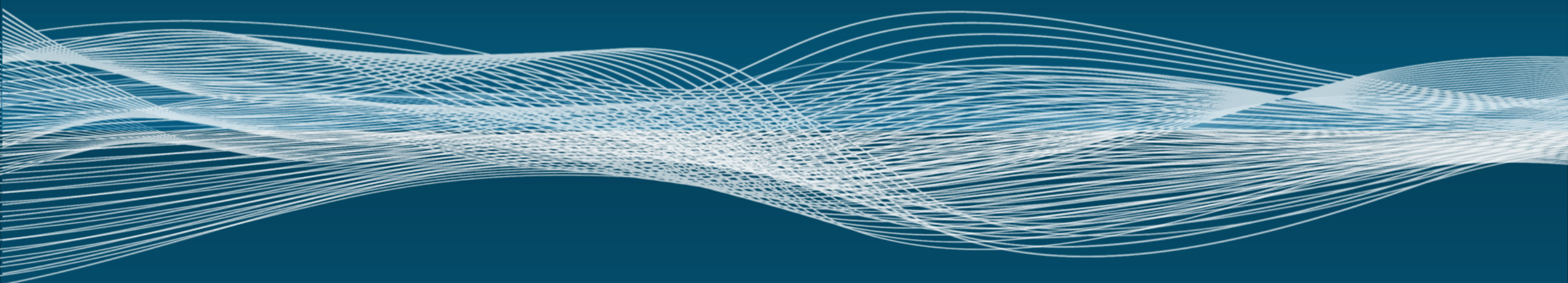
- Requires WCD (Windows Configuration Designer) and Bulk Tokens
- Admin creating ppkg via WCD needs Administrator access to Azure AD to be added to Quest On-Demand
- A server is needed to install the agent to sync directory objects for migration

## OCM

- Pending updates should be completed prior to migration
- Quickly migrates user data and performs AADJ (30 minutes on avg.)
- OneDrive will need to be logged back (When moving from On-prem to AAD)
- Drive mappings are retained (on-prem drives will require network access ie: directly on network or VPN connection)
- Unintended/premature user interaction can cause failures (user reboots during AADJ process due to impatience) Pilot testing is very important.
- End user comms need to be clear that user is to sign in with UPN account. Previous SAM account will show after completed migration and signing into this account creates temp accounts



# Custom Migration



# Custom Migration

## Strengths

- Allows user to initiate process or administrative initiation
- Does not require device reset
- Does not require time after reset for application reinstallation and reconfiguration
- Allows customization and orchestration for change of apps and settings

## Challenges

- Requires thorough development and testing of custom process that has not been previously executed.
- No true supportability (community project)

## Other

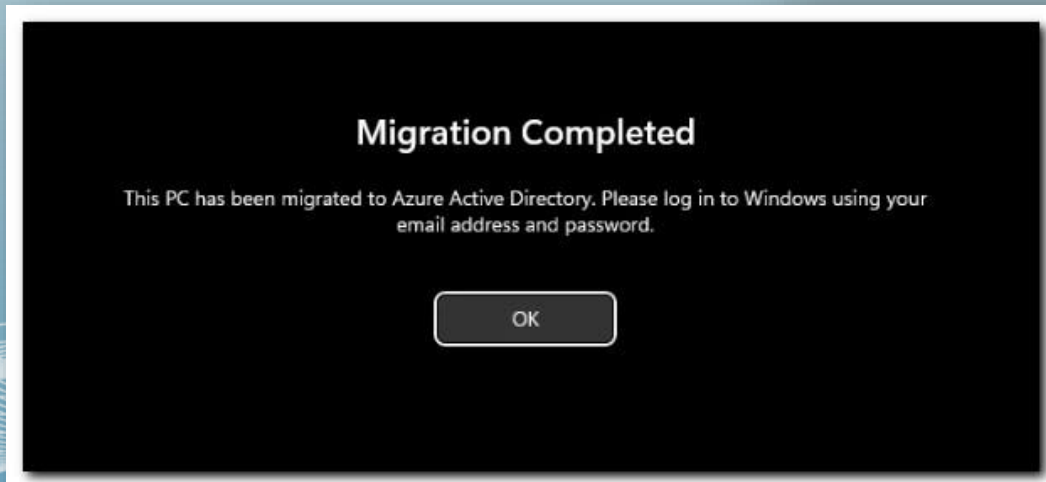
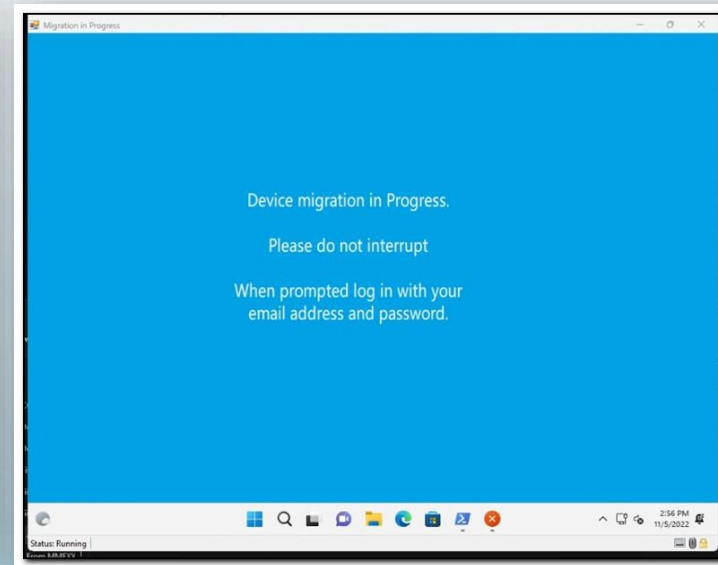
- **No Cost**
- Prep Effort: High
- User Impact: Low

Summary: Viable option as it allows meets the most requirements, however no support options if there are issues



# Custom Migration User Visuals

[Domain Join to Cloud Only \(AADJ\) Migration without Wipe and Load!!](#)



<https://www.modernendpoint.com/managed/Migrating-AD-Domain-Joined-Computer-to-Azure-AD-Cloud-only-join/#determine-your-delivery-method-and-update-prepare-devicemigrationps>



# Tooling Comparison



# Tooling Comparison

| Product               | AutoPilot  | ODM AD   | ProfWiz  | Custom Script   |
|-----------------------|--|--|--|---|
| License Cost          | Included with Intune license, or E3 / E5   | 5.00 per year / per device + 5.00 per year / per user (directory sync)<br>Must acquire thru reseller | 2.95 per year/per device (50 license minimum)<br>Can Acquire thru website for Enterprise license | No licensing cost   |
| Supportability        | Microsoft support ticket   | Quest  | ForensIT Support (with Corporate Edition license)  | Community driven – no supportability outside peers                      |
| IT Time               | If existing AutoPilot process exists, there is little time outside of validating environment / risks | Requires setup of Quest On Demand toolset (profiles, deployment of agent)                            | Variable (depends on environment, delivery method)   | Significant time for configuration and deployment as well as validation |
| Bulk Enrollment Token | N/A  | Required for AADJ  | Required for AADJ  | Required for AADJ   |
| Delivery Method       | SCCM, GPO, Intune  | Quest On-Demand Agent (must be deployed before migration)  | SCCM, GPO, Intune, Manual (SharePoint, Tech USB)   | SCCM, GPO, Intune   |
| End User Impact       | High (device wipe)   | Low (migrates profile as-is but requires OCM)  | Low (migrates profile as-is but requires OCM)  | Low to Medium (addition)  |
| End User Time         | Medium to High (waiting for autopilot process & apps)  | ~30min once migration starts   | ~30min once migration starts   | ~30min once migration starts  |





*Concurrency*

Q&A

# Workshop Survey

MN365 Fall 2023 Workshop Day

A close-up photograph of a hand pointing to a survey form. The form has several rows of text, each followed by a red checkmark in a square box. The visible text includes 'Excellent' and 'Very Good'.

<https://mn365.org/survey>



# Thank You

