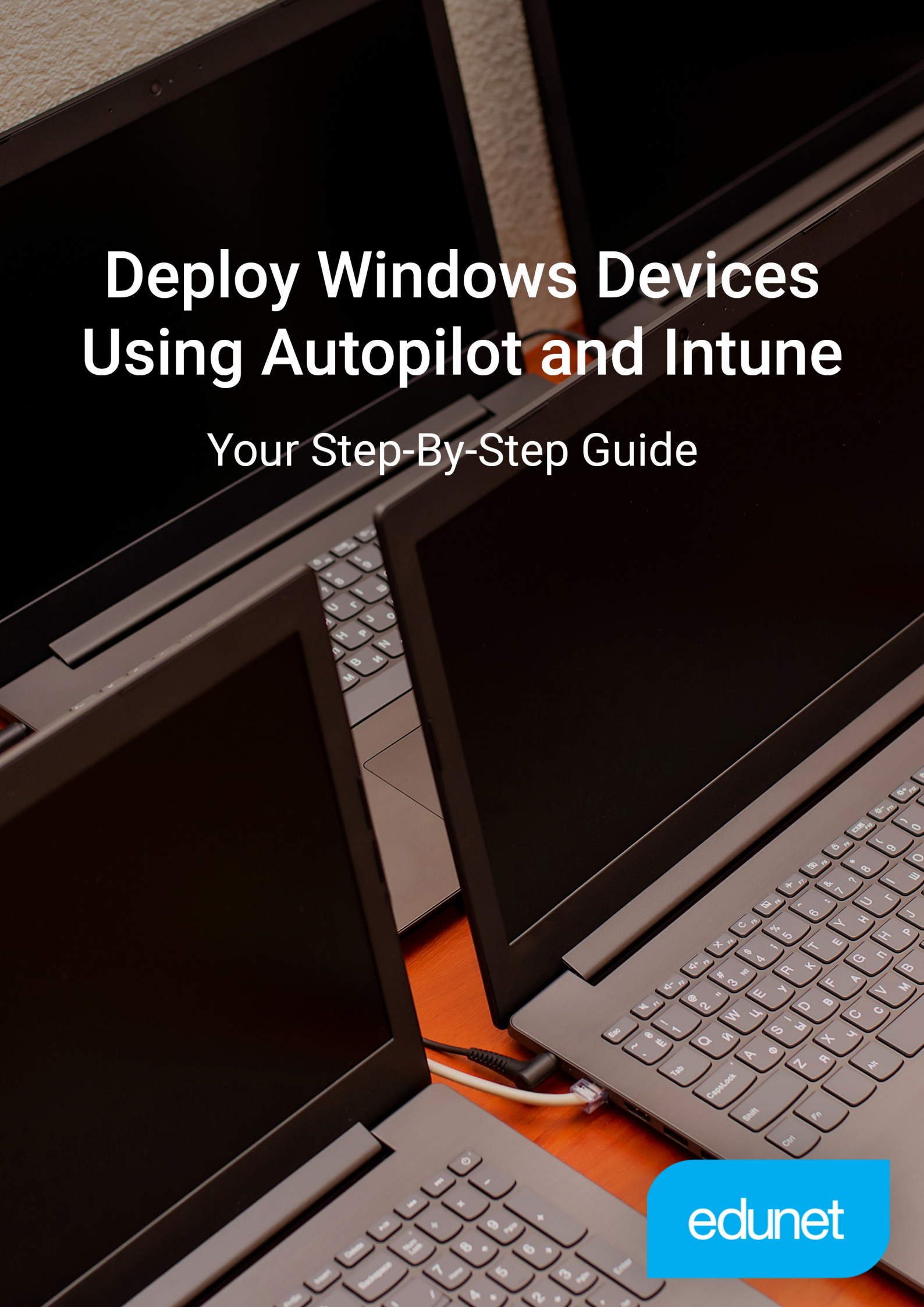
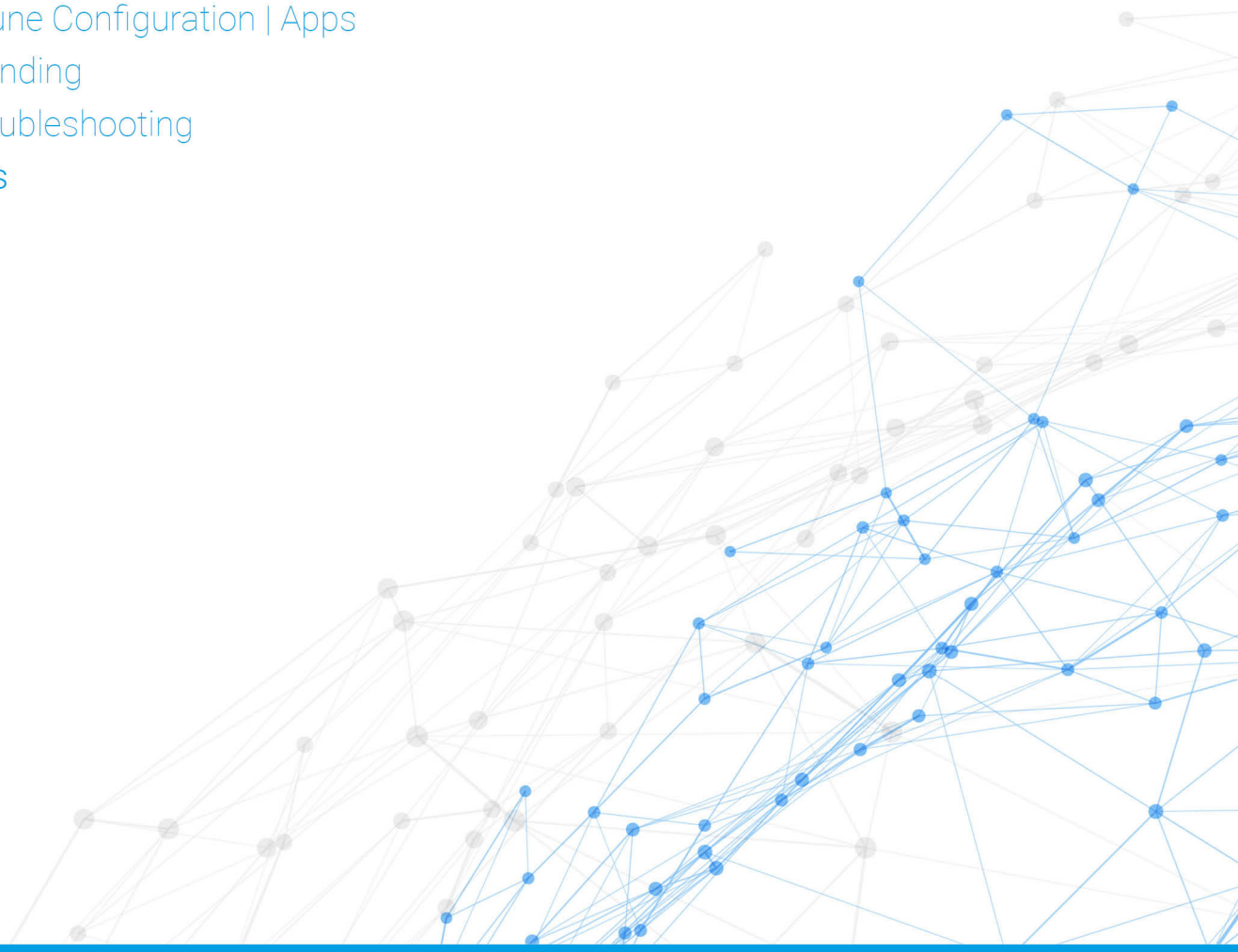


Deploy Windows Devices Using Autopilot and Intune

Your Step-By-Step Guide

edunet

Table of Contents



Introduction

Welcome to your guide for how to set up a new Microsoft Intune and Windows Autopilot service!

You will learn what prerequisites are needed before you can enrol your devices, how to connect to your on-site AD with Azure, and different Intune setups.

You'll also learn how to enrol devices from new providers and existing devices, as well as receive an overview of what the end users will see.

Overview

Windows Autopilot enables your I.T administrators to:

- Automatically join devices to Azure Active Directory (Azure AD) or Active Directory (via Hybrid Azure AD Join).
- Auto-enrol devices into MDM services, such as Microsoft Intune (Requires an Azure AD Premium subscription for configuration).
- Restrict the administrator account creation.
- Create and auto-assign devices to configuration groups based on a device's profile.
- Customize the out-of-box content specific to your organization.

As well as working with Microsoft Intune:

- See the devices enrolled and get an inventory of devices accessing organization resources.
- Configure devices so they meet your security and health standards.
- Push certificates to devices so users can easily access your Wi-Fi network, or use a VPN to connect to your network.
- See reports on users and devices that are compliant and not compliant.
- Remove organization data if a device is lost, stolen, or not used anymore.
- Add and assign apps to user groups and devices, including users in specific groups as well as devices in specific groups.
- Configure apps to start or run with specific settings enabled and update existing apps already on the device.
- See reports on which apps are used and track their usage.
- Do a selective wipe by removing only organization data from apps.

By the end of this guide you will have a working system for deploying machines without the need to touch the device!

Interfaces

The Azure portal will contain all links to the needed areas to configure both Intune, Azure and Autopilot.

It can be found at: https://www.portal.azure.com/.

Some options can be configured from other locations such as the Microsoft Store for Business and Microsoft Endpoint Manager. In this case, only the Azure AD and Intune from the above portal will help with the work flow of the setup.

Prerequisites

- A working on-site Active Directory and DNS server.
- An Azure Active Directory Premium subscription.
- An Intune License per user or device.

Note that when trying to enrol imaged machines, the device must be running Windows 10 Professional or Education versions, 2004+.

Licences

It is recommended that you activate all your licences to the administrator account before attempting to follow the guide as some of the licences may require up to 24 hours to take effect.

You will need at least one Azure Active Directory Premium subscription assigned to the administrator account and for each device or user you wish to enrol an Intune licence.

Azure AD Setup

Firstly, you should sign into the Azure portal and check if the licences are active. If not, activate them either though the Azure portal > Licenses > All Products or by the Office 365 Admin Portal.

Once all the licenses are active and synced we can make a tenant. On the first page select Azure Active Directory before clicking next, then on the "Configuration" page you can add your organization's name and domain name, as well as your county and region.

As an example, we would input the following:

Organization Name: Edunet College
Initial Domain Name: EdunetCollege

County/Region: Australia

Once filled in, proceed by clicking next and review and finish on the next page.

Linking Azure with AD Connect

Once we have a tenant setup, we need to bridge the connection between the on-site active directory and the Azure cloud. We do this with a program called AD Connect that can be downloaded for free from Microsoft's website: https://www.microsoft.com/en-us/download/details.aspx?id=47594.

While setting this up we will have to chose what type of syncing we want to use. There are three options:

1. A federated server.
2. Pass-through authentication.
3. Password hash synchronization.

Password hash synchronization is the simplest way to enable authentication for on-premises active directory objects to the Azure AD. Users can use the same username and password that they use on-premises without having to deploy any additional infrastructure.

Some premium features of Azure AD (like Identity Protection and Azure AD Domain Services) require password hash synchronization, no matter which authentication method you choose.

Pass-through authentication provides a simple password validation for Azure to authenticate by using a software agent that runs on the on-premises server. The servers validate the users directly with your on-premises Active Directory, which ensures that the password validation doesn't happen in the cloud.

Federated authentication is the more advanced approach and requires a SSL certificate to work and when you choose this authentication method, Azure hands off the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS), to validate the user's password.

Installs of each of these are quite similar and by following the setup wizard you will end up with a working AD connection.

You can check this by looking under the Azure Overview dashboard where it will show the current status and when the last sync took place. If the on-site Active Directory is large it may take a while to complete the first sync.

1. On the Domain controller, download and install the program called "AD Connect" found on Microsoft's website.
2. During the setup it will ask which type of password synchronisation you would like:
    a. Federation Server (AD FS). Please remember this option will require an SSL Certificate.

b. Pass Thought (PTA).

c. Password Hash Sync.

3. Continue though the setup, it will ask for accounts and other basic settings based on what has been picked.

Azure Configuration

Azure itself does not require a huge amount of changes from the default for Autopilot to work, although it will be used to manage devices and users after they have been enrolled. For now, we need to configure who has access to enrol devices:

1. In the Azure portal go Azure Active Directory > Mobility (MDM and MAM) > Microsoft Intune.

2. Under MDM User Scope select:

   a. "Some" to define who can enrol devices by allowing designated groups to enrol devices.

   i. "All" if you want all users to be able to enrol. Note that the devices are still set by the admin, meaning even if you set all users, they can only enrol devices that you specify.

Intune Configuration

To configure Intune to join an enrolled device into Azure, a deployment profile needs to be made with a few settings as well as others to fit your needs. The following is a basic profile that works:

1. In the Azure portal go Intune > Device Enrolment > Windows Enrolment > Deployment Profiles.

2. Under the banner you can find the create button, under which you create the profile that is responsible for connecting the new device to the domain.

3. Under "1 Basics" name and create a description to the profile. Leave "Convert all targeted to autopilot" as "NO".

Example:

Name: AAD Domain Join
Description: This is the profile used to join the devices to the domain
Convert all targeted devices to Autopilot: NO

4. On the next page you can edit the options to your own liking, only requiring the ones following to be set or unchanged:

i. **Deployment mode:** User-Driven
ii. **Join to Azure AD as:** Azure AD joined
iii. **Allow White Glove OOBE:** YES

5. Hit next. You will find Assignments, where you can choose to assign the profile to a group of devices or to all devices within Intune.

Intune Enrolment

To enrol a device into Intune you need will need to upload a .CSV into Intune. There are two ways to get your hands on the .CSV. One is from your device's supplier, the other is by running a PowerShell script:

1. In the Azure portal go Intune > Device Enrolment > Windows Enrolment > Devices.

2. Under the banner you can find the import button, under which you can upload a .CSV.

3. You can obtain this .CSV in two ways:

    a. It can be requested to be sent to you when you order new devices though some dealers.

    b. It can be retrieved off individual devices by running, allowing all commands and finding the .CSV under C: drive, then HWID:

        i. md c:\\HWID
        ii. Set-Location c:\\HWID
        iii. Set-ExecutionPolicy -Scope Process -ExecutionPolicy Unrestricted
        iv. Install-Script -Name Get-WindowsAutoPilotInfo
        v. Get-WindowsAutoPilotInfo.ps1 -OutputFile AutoPilotHWID.csv

Please wait about 15 minutes for the devices to sync.

End-User

After completing the previous steps on the device that has been enrolled in the .CSV step, simply boot the device and you will get the normal Windows 10 setup screen.

This is only until it joins the internet during the Wi-Fi step, after which it will display your organisation's sign in screen where users can enter their details (email and password) then AutoPilot will take care of the rest!

Additional Setup

In this area we will review optional and individual setups.

Enrolment Status Page

The enrolment status page, while not necessary, is extremely useful for troubleshooting. It displays as a page shown while the device is being configured, after the user has signed in and the initial handshake has happened between the device and the Azure AD.

This enables the administrators to determine where the enrolment fails and narrow down the search, as well as enables the administrator set conditions for fails including time-outs and messages to users as away to contact the end user.

Azure Portal > Intune > Device Enrolment > Windows Enrolment > Enrolment Status page.

Windows Hello

By default, the Windows Hello for Business is enabled and can be customized to your needs. Its settings for default are found at:

Azure Portal > Intune > Device Enrolment > Windows Enrolment > Windows Hello for Business.

They can ether be turned off or customized by editing the default and saving it. There is also the option for assigning certain groups to different levels for security or to accommodate the needs of the group.

Custom Domain Names

This is for changing the Azure domain from “Organisation.onmicrosoft.com” to your preferred domain name, such as “Organisation.com.au” instead.

This does require some changes with your registrar to verify. What those changes are vary based on how yours is set up.

Intune Configuration | Profiles

One of the limitations of Autopilot is that devices enrolled with it will be unable to use group policy for management. Instead, the devices can be managed by using Intune’s device configuration and profiles, found at:

Azure Portal > Intune > Device Configuration > Profiles.

There are profiles that allow administrators to control a multitude of aspects of a device, including wireless settings, locking a device to kiosk mode, as well as the ability to create custom profiles

using OMA-URI settings.

Intune Configuration | Apps

For the deployment of applications though Intune there are three options. Deployment of apps found in the Windows store, through Microsoft 365, or though the Microsoft Win32 Content Prop tool.

The last option will create an .intunewin file for upload, but with a few restrictions including file size.

Branding

Azure Portal > Azure > Company Branding. Fields of note here are:

“Username hint” is what is shown to the users in the sign-in box on first sign-in.

“Sign-in page text” is what is displayed under the sign-in box.

Troubleshooting

1. If items are appearing greyed-out within Intune, double check you have an Intune licence assigned to your account or that you have an Intune licence included in one of your licensed products. If you are still having issues, please check the next troubleshooting option.

2. If items are still appearing greyed-out within Intune, there can be an issue where Intune has not been set as the default MDM.

   To resolve this issue, create a new account and assign them a licence for Intune as well as rights as an administrator before signing into this account in Intune. Doing this should make a banner appear asking if you want to make Intune the default MDM, click yes and follow the prompts.

   Items that were previously greyed out should now be working. It is mainly Windows Hello for Business and the Enrolment Status page which suffer from being greyed out.

3. Some other common licence errors come from Intune being included in some Microsoft 365 and not Office 365 products, as each user will require a licence to be able to enrol a device. Check that your 365 products have included an Intune licence or have been assigned a standalone one.

Final Notes:

1. If you reimage or otherwise reinstall Windows by an installation, and not by Windows reset, the hardware ID can change. The device will sometimes still be able to be enrolled but it is possible for the device to need to have its ID refreshed in Intune for it to connect again.

2. Unless you have created a local administrator prior to enrolling the device, either though imaging or creating a profile to create one, the default device setup disables the inbuilt administrator account.

   This can cause issues if you need to access a device that is having issues. The device can still be reset if needed by booting into safe mode and selecting “Reset PC” under Troubleshooting.

3. By using Azure AD and Intune the device cannot be managed by a group policy. Intune does offer the ability to manage the device via the use of configuration profiles instead, however.