MS Intune

# Overview:

Microsoft Intune is a cloud-based endpoint management solution that helps organizations securely manage devices (Windows, macOS, iOS, Android) and applications. It is part of Microsoft Endpoint Manager and enables IT admins to enforce security policies, control access to corporate resources, and ensure compliance across user devices.

Link : [Microsoft Intune Admin Centre](https://intune.microsoft.com/#home)

# Objectives:

### 1️. Device Management (MDM - Mobile Device Management)

✔️ Enforce security policies on corporate and BYOD (Bring Your Own Device) devices.  
✔️ Control access to corporate resources like emails, apps, and files.  
✔️ Manages Windows, macOS, iOS, and Android devices remotely.

### 2. Application Management (MAM - Mobile Application Management)

✔️ Secure corporate data within approved apps (without managing the entire device).  
✔️ Restrict copy-paste, screenshots, and file sharing in corporate apps.  
✔️ Deploy, update, and remove applications remotely.

### 3. Security & Compliance

✔️ Ensure all devices meet security policies before accessing company resources.  
✔️ Block unapproved apps, enforce encryption, and require strong authentication.  
✔️ Integrate with Microsoft Defender to detect and respond to threats.

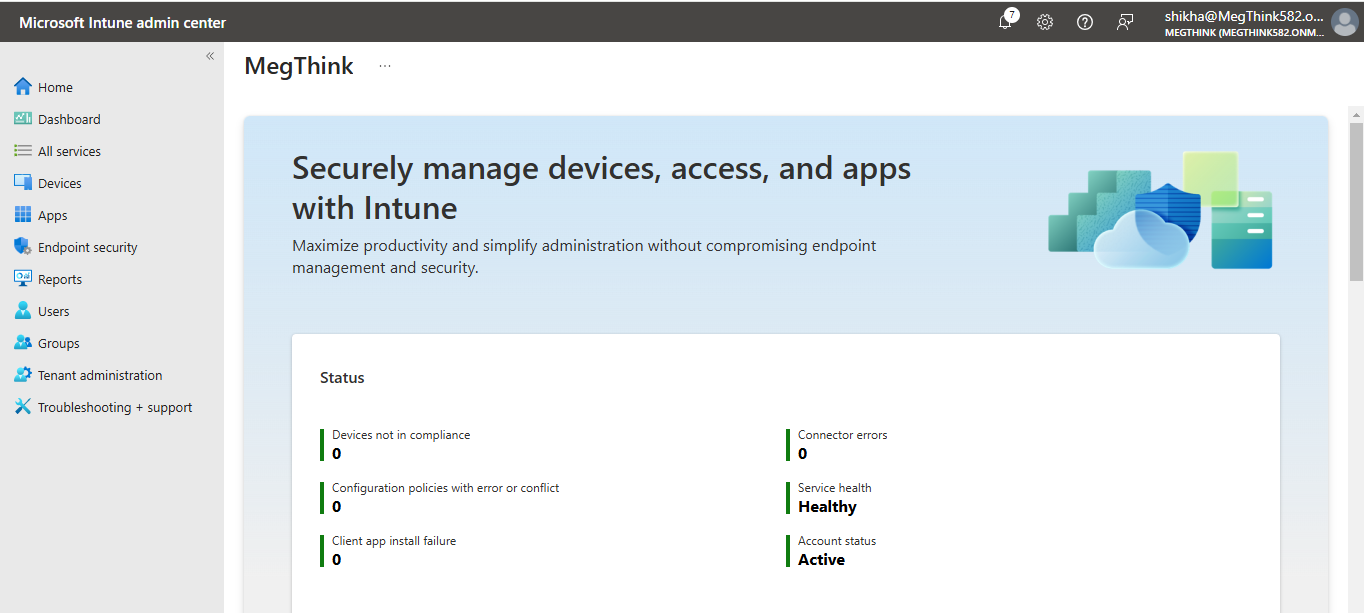
### 4. Conditional Access & Identity Protection

✔️ Enforce multi-factor authentication (MFA) and risk-based access policies.  
✔️ Allow or block access based on device health, location, and compliance status.  
✔️ Seamless integration with Microsoft Entra ID for identity-based security.

### 5. Remote Monitoring & Zero-Touch Deployment

✔️ Windows Autopilot for pre-configured, zero-touch device setup.  
✔️ Monitor device health, compliance status, and user activity.  
✔️ Remotely wipe data from lost or stolen devices (Selective or Full Wipe).

# Core Component of MS Intune



### The three main components of Intune are:

* Devices (Device Management - MDM)
* Apps (Application Management - MAM)
* Endpoint Security

## 1. Devices (MDM - Mobile Device Management)

Intune allows IT admins to manage and enforce security policies on Windows, macOS, iOS, and Android devices.

### Key Features:

✔ Device Enrollment – Onboard devices into Intune (corporate-owned & BYOD).  
✔ Compliance Policies – Ensure devices meet security requirements before accessing company resources.  
✔ Configuration Profiles – Enforce security settings (e.g., block USB, require encryption).  
✔ Remote Actions – Wipe, lock, reset passcode, or retire lost/stolen devices.  
✔ Windows Autopilot – Zero-touch deployment for new Windows devices.  
✔ Conditional Access – Restrict access to corporate apps based on device compliance.

### Enrollment Methods:

* Android Enterprise – Work Profile, Fully Managed, Corporate-Owned Work Profile
* iOS/iPadOS – Apple User Enrollment, Supervised Mode
* Windows – Autopilot, Hybrid AD Join, Azure AD Join
* macOS – Apple Business Manager, User Enrollment

## 2. Apps (MAM - Mobile Application Management)

Intune allows organizations to manage applications on both corporate and personal devices without fully controlling the device.

### Key Features:

✔ App Deployment – Install, update, or remove apps remotely.  
✔ App Protection Policies – Protect corporate data inside apps (e.g., block copy-paste).  
✔ Managed Google Play & Apple VPP – Distribute public and private apps.  
✔ Blocking Unauthorized Apps – Prevent usage of non-compliant apps.  
✔ Conditional Access for Apps – Allow access only from approved apps.

### Types of App Management:

* Managed Apps (MAM-WE) – Protect corporate data inside Office 365 apps (Outlook, Teams).
* LOB (Line-of-Business) Apps – Deploy internal apps securely.
* App Configuration Policies – Pre-configure app settings (e.g., email setup).

## 3. Endpoint Security

Intune integrates with Microsoft Defender for Endpoint to protect devices from threats and enforce security baselines.

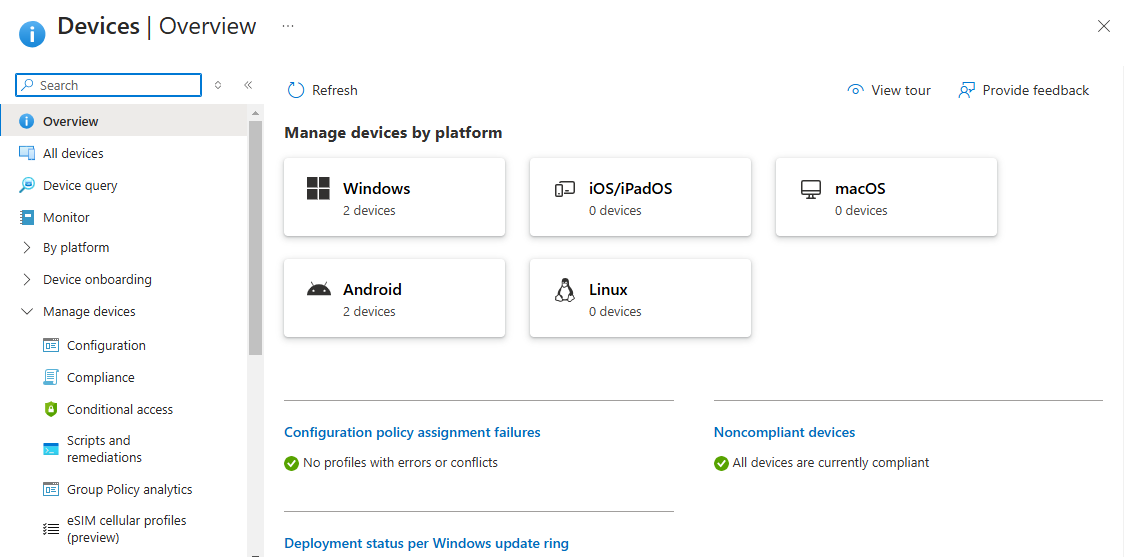
### Key Features:

✔ Security Baselines – Apply industry-recommended security settings.  
✔ Device Compliance & Risk-Based Access – Ensure only secure devices access company data.  
✔ Defender for Endpoint Integration – Detects and responds to malware threats.  
✔ Attack Surface Reduction – Block unauthorized scripts, macros, and USB access.  
✔ BitLocker & FileVault Encryption – Protect data at rest.  
✔ Firewall & Antivirus Policies – Configure network and endpoint protection.

### Security Policies in Intune:

* Antivirus & Ransomware Protection – Configure Defender AV settings.
* Disk Encryption – Enforce BitLocker (Windows) and FileVault (macOS).
* Firewall & Network Protections – Prevent unauthorized access.
* Attack Surface Reduction Rules – Control script execution, block untrusted apps.

# Devices

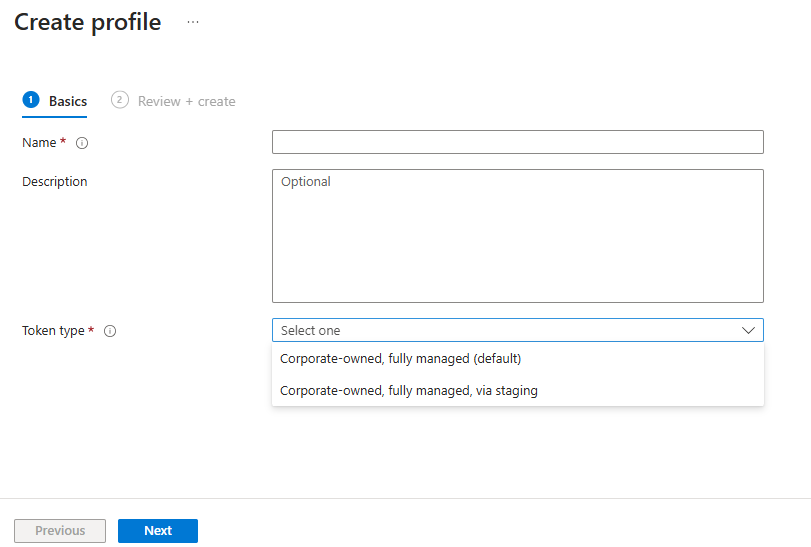


## Steps to Enroll BYOD (Bring Your Own Device) - Android in Microsoft Intune

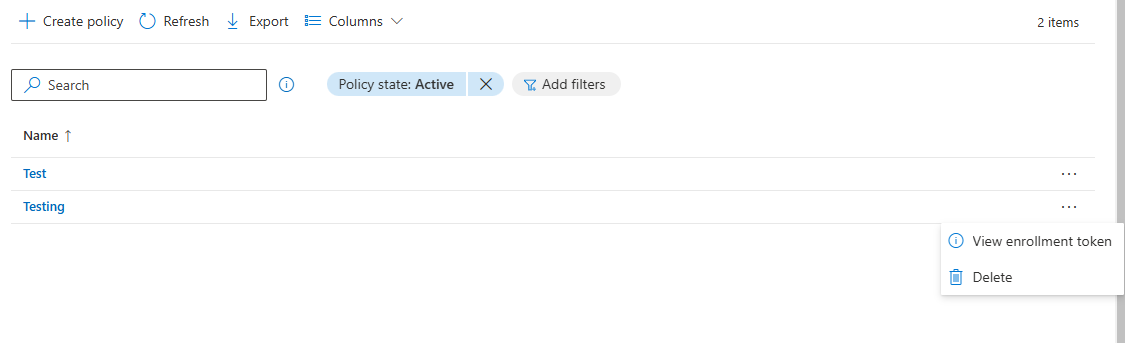
1. Download **Intune Company Portal**.
2. Open the App & Sign In with your work account.
3. Follow the on-screen steps and create a work profile.
4. In company portal, go to **settings →sync**

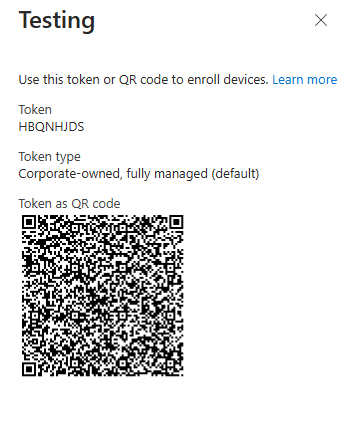
## Steps to Enroll Corporate-Owned Fully Managed - Android in Microsoft Intune

1. Navigate to **Devices → Android → Enrollment**.
2. Select **Corporate-Owned Fully Managed Devices**.
3. Click on **Create Policy**.



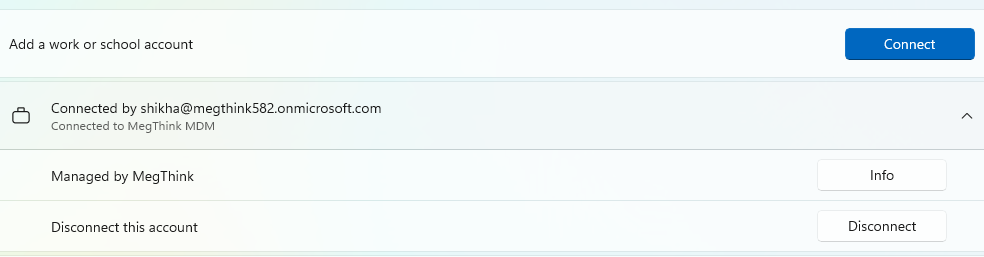
1. Give some **Name** and **Description**.
2. In **Token type**, Select **Corporate-owned, fully managed(default)** option and click on Next.
3. Then review and create.
4. Click on 3 dots → **view enrollment token**.



1. The following screen will appear to scan the QR-code**.**  
   
2. Turn on the Android device and perform a **Factory Reset** (if not already done).
3. At the Welcome Screen, tap **6 times** anywhere to open the **QR code scanner**.
4. Scan the QR Code generated in Intune.
5. The device will download and install the **Microsoft Intune Company Portal app** automatically.
6. Sign in using the work account.
7. Follow the on-screen instructions.
8. Once enrollment is complete, the device is fully managed by Intune.

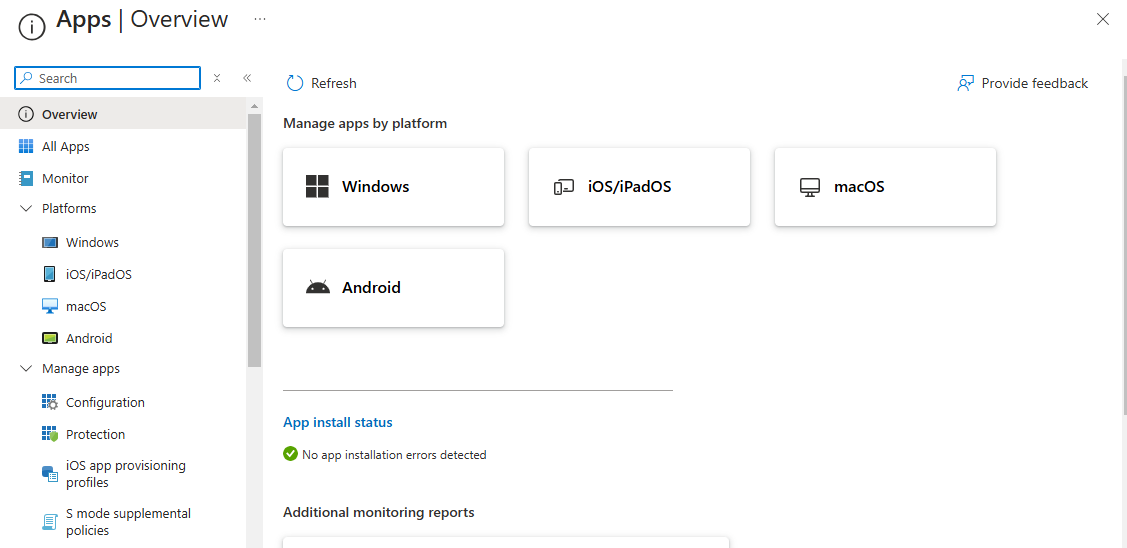
## Steps to Enroll Windows device in Microsoft Intune

1. Go to **Settings → Accounts → Access work or school**.
2. Click on **Add a work or school account**.
3. Follow the on-screen instructions and set-up your work profile.
4. Click on **Info → Sync**.



1. Go to the **Microsoft store** and download the **Company Portal app.**
2. Set-up your work profile on company portal
3. Click on **Setting –> Sync**.

# Apps



## Steps to Add and Deploy Apps in Intune:

1. Navigate to **Apps** → **All Apps**.
2. Click **Create** to start adding an app.
3. Select **App Type** (Windows & Android).

## For Android:

1. Select **App Type** as **Managed Google Play Store App**.
2. Click **Select** to open Google Play Store within Intune.
3. Search for the app (e.g., Microsoft Teams).
4. Click on **Select**.
5. Click **Sync** to update Intune with the app.
6. Assign the App to Users or Devices
7. Go to **Apps → All Apps → Select the app**.
8. Click **Properties → Assignments → Edit**.
9. Choose an assignment type:

* **Required** → Forces app installation on devices.
* **Available** → Users can install from Company Portal.
* **Uninstall** → Removes the app from devices.

1. Select **User groups or Device groups**.
2. Click **Review + Save**.

## For Windows

1. Select **App Type** as **Microsoft Store App**.
2. Enter the **App Name** (e.g., Microsoft Edge, Teams, or OneDrive).
3. Select the app and click **Next**.
4. Enter **App Information** (name, description, category).
5. In the **Assignments** section, choose how to deploy:

* **Required** → Auto-install on devices.
* **Available** → Users can install via Company Portal.
* **Uninstall** → Remove from devices.

1. Select **User or Device Groups** for deployment.
2. Click **Next → Create.**

# Compliance and Configuration

## 1. Compliance Policies

* **Purpose:** Ensure that devices meet security and organizational standards before granting access to resources.
* **Functionality:**
  + Define minimum security requirements (e.g., OS version, encryption, password complexity).
  + Devices that fail compliance policies can be flagged as non-compliant and can be restricted from accessing company resources via Conditional Access.
  + Helps enforce Zero Trust security principles.
* **Example Policies:**
  + Require devices to have BitLocker enabled.
  + Ensure OS version is up to date.
  + Enforce password complexity.

### Steps to create a compliance policy:

1. Navigate to **Devices → Compliance**.
2. Click **+ Create Policy**.
3. Select the **Platform** (e.g., Windows 10/11, macOS, iOS/iPadOS, Android).
4. Click **Create**.
5. Under **Compliance settings**, configure security rules.
6. Go to **Actions for noncompliance**.
7. Set up actions such as:

* **Mark as non-compliant** immediately or after a grace period.
* **Send email notifications** to the user/admin.
* **Retire or wipe the device** after repeated non-compliance.

1. Click **Next** to reach **Assignments**.
2. Then click on **Review + Create**.

Without Conditional Access, non-compliant or unmanaged devices might still access corporate data, increasing security risks. Configuring Conditional Access ensures that only secure and managed devices are allowed in your organization’s environment.

To improve security, set up a **compliance-based Conditional Access policy** in Microsoft Entra ID by:

1. **Go to Entra ID → Conditional Access** in the **Microsoft Entra admin center**.
2. **Create a new policy** with conditions such as:

* Assign to **specific users or groups**.
* Select **"Require device to be marked as compliant"** as a condition.
* Apply it to apps like **Microsoft 365, Exchange, etc.**.

1. **Enable the policy** to enforce security.

## 2. Configuration Profiles

* **Purpose:** Deploy settings, policies, and applications to configure devices as per organizational needs.
* **Functionality:**
  + Configure Wi-Fi, VPN, email settings, security settings, and more.
  + Can enforce restrictions (e.g., disable USB access, prevent installing untrusted apps).
  + Used to pre-configure devices before users start using them.
* **Example Configurations:**
  + Set up Wi-Fi profiles for automatic connection.
  + Deploy corporate email settings to devices.
  + Restrict access to certain apps or features.

### Steps to create a Configuration Profile:

1. Navigate to **Devices → Configuration**.
2. Click **on Create → New Policy** .
3. **Select a platform** (Windows, macOS, iOS/iPadOS, Android).
4. **Choose a Profile Type**, such as:
   1. **Settings catalog** (Recommended) – Provides a comprehensive list of settings.
   2. **Templates** – Predefined settings (e.g., Wi-Fi, VPN, Email, Device restrictions).

## Configure **Profile Settings**.

1. Click **Next** to reach the **Assignments** page.
2. Assign the profile to:
   1. All Users or All Devices.
   2. Specific groups (e.g., security groups in Entra ID).
3. Click **Next** to proceed.
4. Then **Review + Create**.

# 

# How Compliance Policy works with Conditional Access Policy:

### Step 1: Create a Compliance Policy in Intune

1. Navigate to **Devices > Compliance policies > Policies > Create policy**.
2. Select the **Platform** (Windows, iOS, Android, etc.).
3. Configure Compliance settings (e.g., OS version, BitLocker encryption, Antivirus enabled, etc.).
4. Define Actions for noncompliance (e.g., send notifications or mark the device as noncompliant).
5. Assign the policy to users/groups.

### Step 2: Configure Conditional Access in Entra ID:

1. Navigate to **Protection > Conditional Access > New policy**.
2. Name the policy (e.g., "Require compliant device for access").
3. Assign users/groups: Under Assignments, select Users or Groups to whom this policy applies.
4. Select **Cloud Apps**: Choose apps to protect (e.g., Microsoft 365, Exchange Online, etc.).
5. Require **Device Compliance**: Under Grant, select Require device to be marked as compliant.
6. Click **Select** and **Enable Policy**.
7. **Save** and **Enable** the Policy.

### How It Works

* When a user tries to access a protected app, Entra ID checks if the device is compliant (as per Intune).
* If **compliant**, access is granted.
* If **noncompliant**, access is denied, or users may be redirected to remediate compliance issues.

# Endpoint Security

Endpoint Security in Microsoft Intune helps IT teams **secure, monitor, and manage** enterprise devices (Windows, macOS, iOS, Android). It prevents cyber threats, enforces security policies, and ensures compliance with security standards.

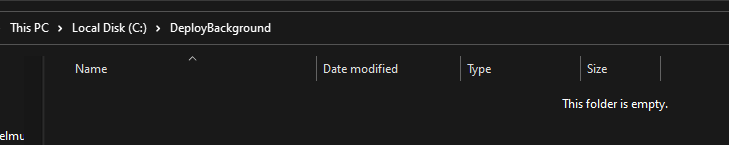
✅ Protects corporate devices from malware, phishing, and unauthorized access.  
✅ Integrates with Microsoft Defender for Endpoint (MDE) for advanced threat detection.  
✅ Provides centralized security management for all devices in an organization.

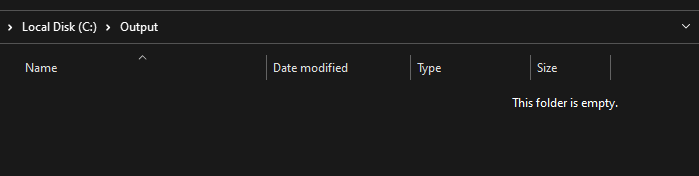
| **Feature** | **Purpose** | **Real-Life Scenario** |
| --- | --- | --- |
| Security Baselines | Apply Microsoft's recommended security settings easily. | A company wants to quickly secure all laptops with best practices without configuring each setting manually. |
| Antivirus (Microsoft Defender) | Protects devices from malware, viruses, ransomware. | An employee accidentally downloads a phishing email attachment, but Defender detects and blocks it. |
| Disk Encryption (BitLocker & FileVault) | Encrypts device storage to prevent data theft | A lost laptop contains confidential client data; thanks to BitLocker encryption, the data remains inaccessible. |
| EDR (Endpoint Detection & Response) | Detects and responds to cyber threats | A hacker tries to exploit unpatched software; EDR detects suspicious activity and alerts the IT team. |
| Firewall | Control network traffic and block unauthorized access. | A user connects to a public Wi-Fi at a café; the firewall blocks unsafe connections, preventing data leaks. |
| Attack Surface Reduction (ASR) | Minimize the attack surface to prevent malware and phishing. | Employees get a malicious Office document via email; ASR blocks macros from running, stopping the attack. |
| Account Protection | Strengthens authentication & prevents unauthorized logins | A company enforces Windows Hello (biometric login), making it impossible for stolen passwords to be misused. |
| Device Control | Restrict USB, Bluetooth, camera, and external devices. | A contractor plugs in an unknown USB drive; Intune blocks it, preventing malware infection. |
| Managed Installer | Restrict app installation to only trusted sources. | Employees try to install unapproved software; Intune blocks unauthorized app installations. |

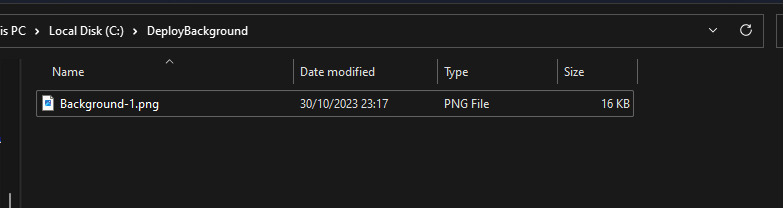
# Deploy Wallpaper with Microsoft Intune :-

We first have to make sure, that our new wallpaper image is packed into an IntuneWin file. So make sure you have your background image ready. Follow this steps.

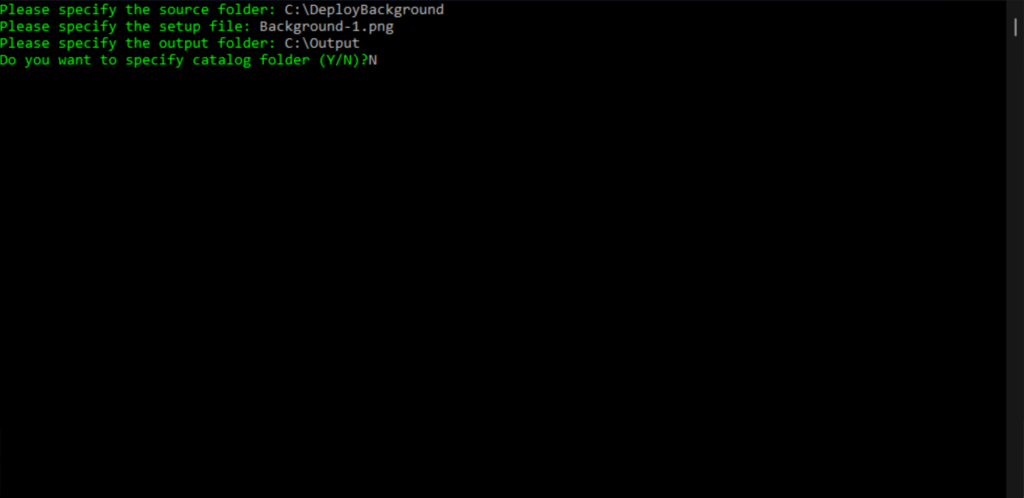
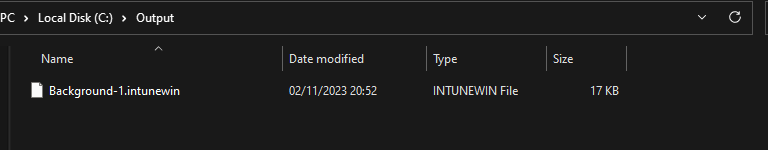
* Create a new folder called **DeployBackground** on **C.**
* Create a new folder called **Output** on **C**.



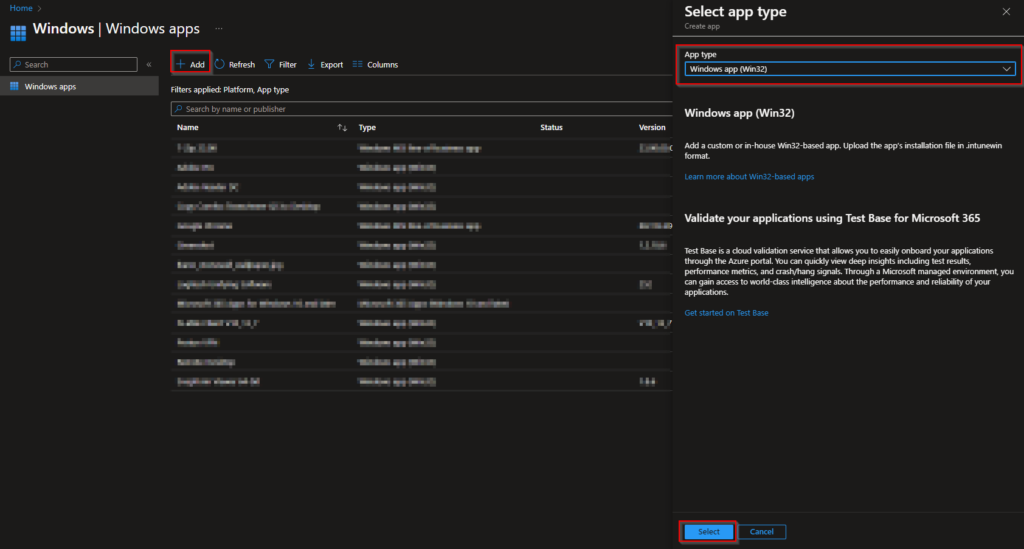


* Copy your new background to the **DeployBackground** folder
* I named my background “**Background-1**”. You can of sure name it different but just keep the name in mind.
* 
* Download the official Microsoft Intune **Win App Tool**
* Download from below link
* <https://github.com/Microsoft/Microsoft-Win32-Content-Prep-Tool/raw/master/IntuneWinAppUtil.exe>

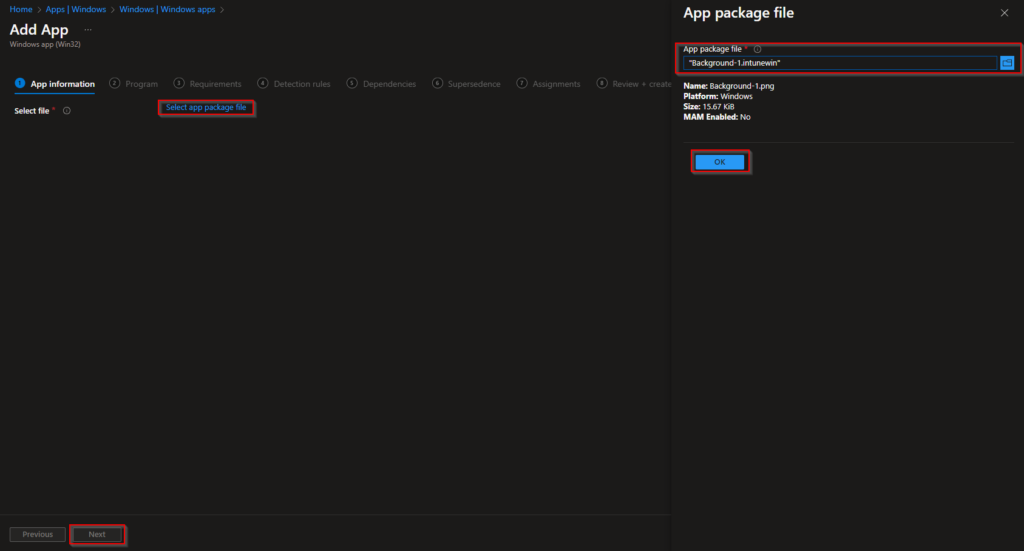
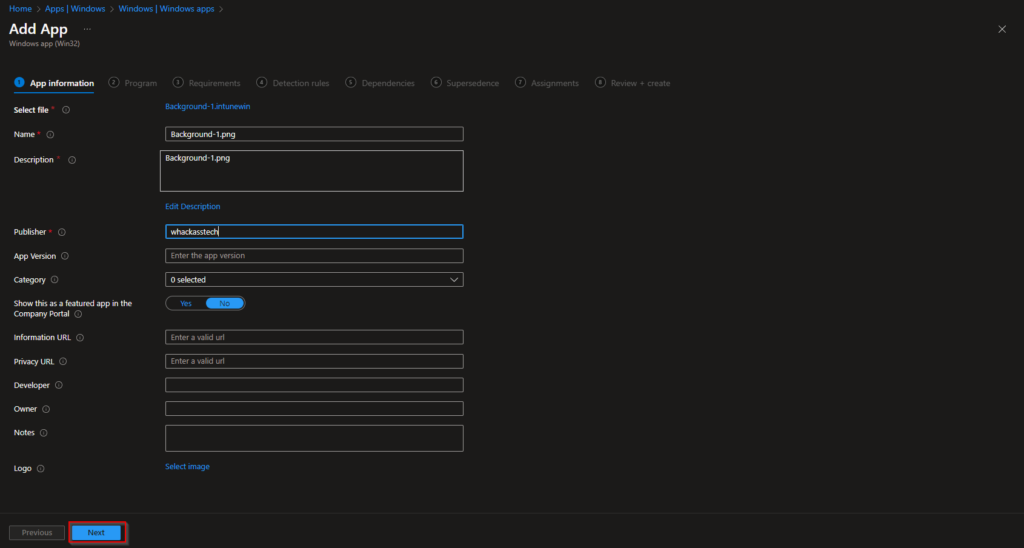
In the Win App Tool application fill out the following.

* Please specify the source folder: **C:\DeployBackground**
* Please specify the setup file: **Background-1.png** [background name]
* Please specify the output folder: **C:\Output**
* Do you want to specify catalog folder: **N**
* 
* In your **C:\Output** folder there should be a new Intune Win file. Save this file we need this in step two.
* 

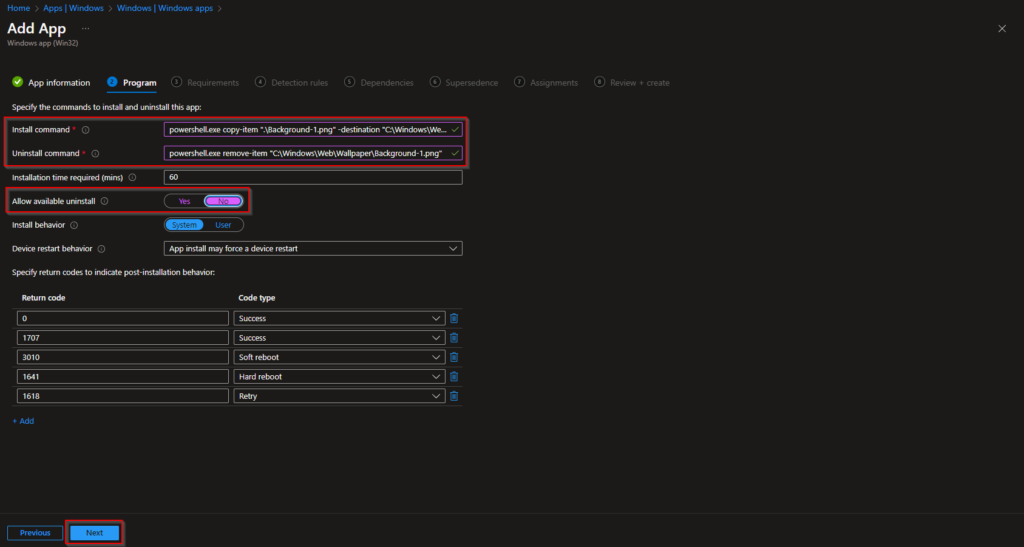
### **Import and deploy with Intune**

* Go to [intune.microsoft.com](https://intune.microsoft.com/)
* Click on Apps
* Click on Windows
* Click on Add
* Chose App type Windows app (win32)
* Click on Select
* 

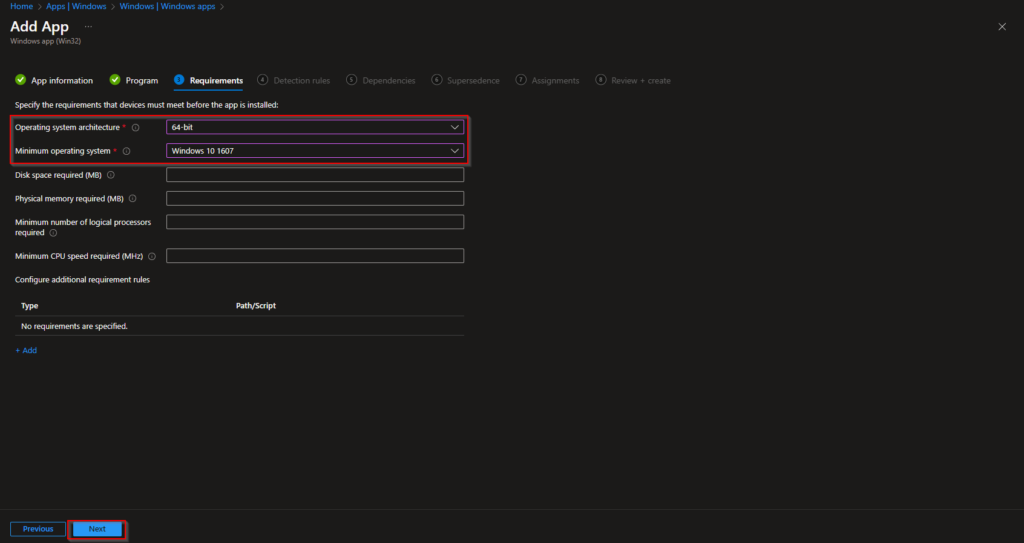
Click on Select app package file

* Upload your IntuneWin file which is located in C:\Output
* Click on
* 
* Here you can change the Settings. I leave it as it is. Dont forget to enter a Publisher
* Click on Next
* 

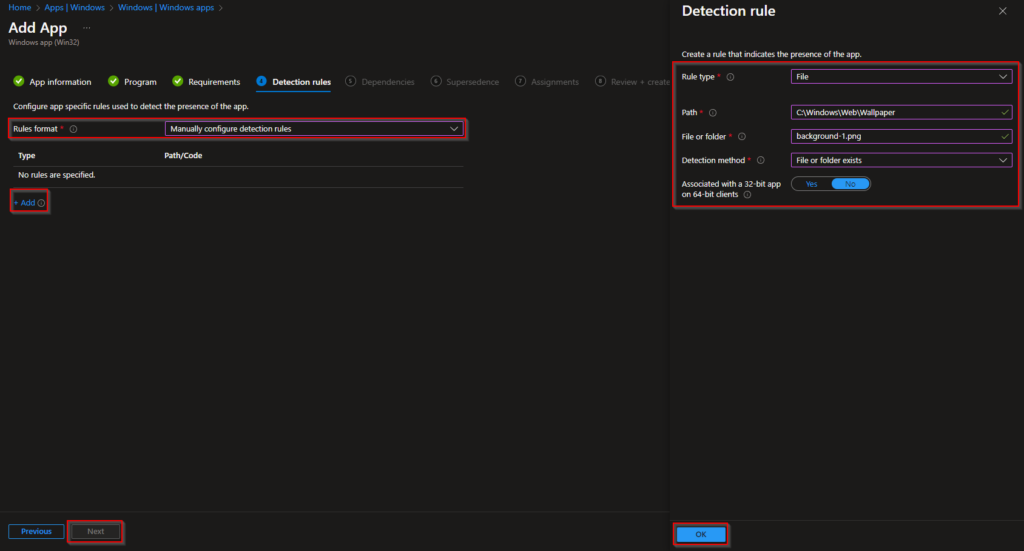
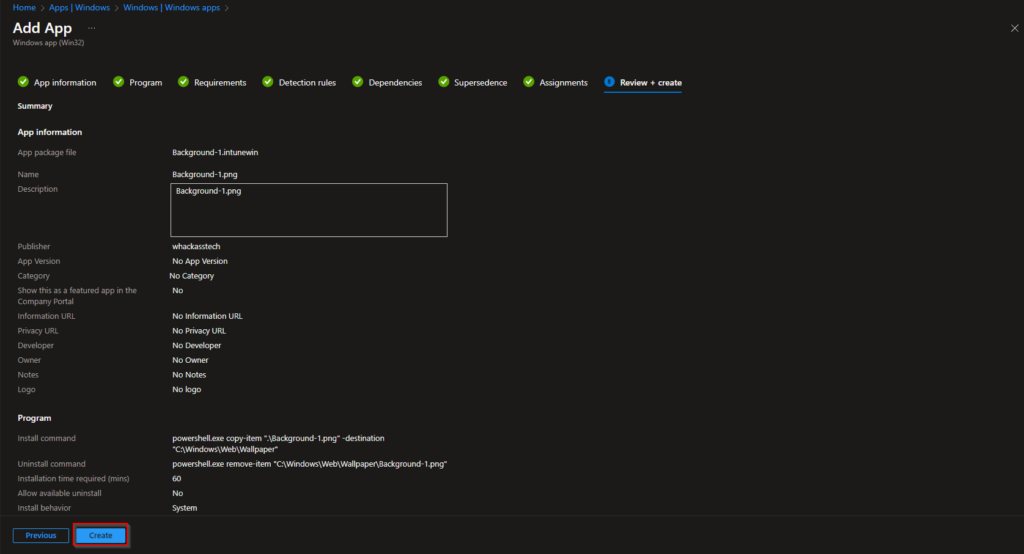
Enter the following Commands:

* Install Command: powershell.exe copy-item “.\Background-1.png” -destination “C:\Windows\Web\Wallpaper”{here if you copy paste it will take unnecessary spaces}
* Uninstall command: powershell.exe remove-item “C:\Windows\Web\Wallpaper\Background-1.png”
* Allow available uninstall: No
* Install behavior: System
* Device restart behavior: no specific Action
* Click on Next
* If your background has a different name note to change this in the Install and Uninstall command.
* 

On the Requirements tab enter:

* Operating system architecture: 64-bit
* Minimum operating system: Windows 10 1607
* Click on Next
* 

On the Detection rules tab:

* Rules format: Manually configure detection rules
* Click on Add
* Rule type: File
* Path: C:\Windows\Web\Wallpaper
* File or Folder: Background-1.png [background name]
* Detection method: File or folder exists
* Associated with a 32-bit app on 64-bit clients: No
* Click on Ok and on Next
* 
* You can skip the Dependencies
* You can skip the Supersedence
* On the Assignments tab assign the Policy to a Group or to All User
* Click on Next
* And Review + Create the Policy
* 
* congratulations! You have successfully deployed the policy. You can now go to Step 3 to create a configuration profile.