# SOP: Enrolling and Managing Endpoint Devices with Microsoft Intune

**Date:** 03/21/2025
**Owner:** IT Department
**Version:** 1.0

## Table of Content

## 1. Introduction

Microsoft Intune is a cloud-based endpoint management solution that enables organizations to securely enroll, configure, and monitor devices across various platforms, including Windows, macOS, iOS, and Android. This Standard Operating Procedure (SOP) provides a step-by-step guide for IT administrators and support staff to set up and manage endpoint devices using Microsoft Intune. Designed for beginners, this guide ensures clear and simple instructions for seamless device enrollment, application deployment, and security configuration.

## 2. Prerequisites

Before beginning the device enrollment process, ensure that the following requirements are met:

1. **Microsoft 365 Subscription** – A valid subscription that includes Microsoft Intune, such as Microsoft 365 Business Premium or Enterprise Mobility + Security (EMS).
2. **Admin Access** – You must have administrator privileges in the Microsoft Endpoint Manager Admin Center (Intune Admin or Global Admin role).
3. **Supported Devices** – Ensure that the endpoint devices to be enrolled (Windows, macOS, iOS, or Android) meet the necessary system requirements.
4. **Corporate Credentials** – Users must have an active Azure Active Directory (Azure AD) account for device authentication and enrollment.

## 3. Accessing Microsoft Intune Admin Center

**Step 1: Sign In to Intune**

1. **Open a Web Browser**: Launch a web browser (e.g., Chrome, Edge, Firefox).
2. **Go to the Microsoft Admin Center**: Type in the URL: https://intune.microsoft.com.
3. **Sign in**: Use your **Microsoft 365** admin credentials (e.g., **admin@yourdomain.com**) to sign in.

You should now see the **Intune Admin Console** dashboard. From here, you can manage devices, apps, users, and security policies.

## 4. Enrolling Devices into Microsoft Intune

**Step 1: Device Enrollment**

1. **Automatic Enrollment**: If the automatic enrollment for Windows 10/11 devices has been configured, the device will automatically enroll in **Microsoft Intune** once the company account is added.
2. **Check Enrollment Status**:
   - Go to **Settings** > **Accounts** > **Access work or school**. Your **organization account** should appear.

     Step 1: Go to Settings.

     Step 2: Click on the accounts.

**Step 2: Add Work Account on the Device**

1. **Turn on the Device**: Power up the Windows 10/11 device and wait for the sign-in screen.
2. **Open Settings**: Click on the **Start Menu** > **Settings**.
3. **Go to Accounts**: Select **Accounts** > **Access work or school**.
4. **Add Work Account**: Click **+ Add work or school account**.
5. **Enter Corporate Email**: Type in your corporate **Azure AD email address** (e.g., user@yourcompany.com) and press **Next**.
6. **Sign In**: Enter your **corporate credentials** (password or MFA) to sign in.

**Step 3: The following screen appears. Now, click on the Access Work or School option.**

- The device will be listed as enrolled automatically.

**Step 4: Verify Enrollment in the Admin Center**

1. Go to the **Microsoft Endpoint Manager Admin Center**.
2. Navigate to **Devices** > **Windows** > **All Windows Devices**.
3. Search for the device by its name or user. If it is listed, the enrollment was successful.

# 5. Steps to Install/Remove Applications on Windows Devices Using Intune

## 5.1 Installing the Apps on Endpoint Devices

**Step 1: Log into Microsoft Endpoint Manager (MEM)**

1. Open a web browser and go to https://intune.microsoft.com.
2. Sign in using your **Intune administrator account**.
3. In the left-hand menu, click **Apps**.

**Step 2: Select the Application Type**

1. Click **Apps** > **All Apps**.
2. Click **+ Add** to create a new app deployment.
3. Under **App type**, select the appropriate category:
   - **Windows app (Win32)** → For .exe or .msi files (requires .intunewin conversion).
   - **Microsoft Store app (new)** → For apps available in the Microsoft Store.
   - **Line-of-business app** → For .msi applications without repackaging.
4. Click **Select** to proceed.

**Step 3: Configure App Information**

1. Fill in the required details:
   - **Name** (Example: "Google Chrome")
   - **Publisher** (Example: "Google LLC")
   - **Description** (Short description of the app)
   - **Category** (Optional)
2. Upload the **installation file** (if applicable).
3. Click **Next**.

**Step 4: Configure Installation and Uninstallation Commands**

For **Win32 Apps (.intunewin)**:

1. Enter the **install command** (silent installation):
   - **Example for MSI:**

   ```
   msiexec /i "AppName.msi" /qn /norestart
   ```

   - **Example for EXE:**

   ```
   setup.exe /silent /install
   ```

2. Enter the **uninstall command**:
   - **Example for MSI:**

   ```
   msiexec /x "AppName.msi" /qn /norestart
   ```

3. Select the appropriate **restart behavior** (e.g., "No specific action").
4. Click **Next**.

### Step 5: Assign Deployment Settings

1. Under **Assignments**, select one of the following options:
    - **Required** → Installs automatically on assigned devices.
    - **Available for enrolled devices** → Users can manually install via **Company Portal**.
    - **Uninstall** → Removes the app from assigned devices.
2. Choose the **user or device group** to deploy the app to.
3. Click **Next**.

### Step 6: Configure Detection Rules

To verify if the application is installed correctly:

1. Select **Manually configure detection rules**.
2. Click **+ Add Rule** and choose one of the following methods:
    - **MSI Product Code** (for MSI-based apps).
    - **File or Folder Existence** (to check if a specific file exists after installation).
    - **Registry Key** (to check for application installation in the registry).
3. Click **OK**, then **Next**.

### Step 7: Configure Requirements (Optional)

1. Specify **Minimum OS version** (e.g., Windows 10 21H2 or later).
2. Define **disk space, RAM, and processor requirements** if needed.
3. Click **Next**.

**Step 8: Review and Deploy the Application**

1. Review all configuration settings.
2. Click **Create** to finalize the deployment.
3. The application will now be **processed and deployed** to the assigned Windows devices.

## 5.2 Verifying Application Installation

### *5.2.1 Method 1: Using Company Portal*

**Step 1: Open Company Portal on the Windows device.**

**Step 2: Navigate to Apps.**

**Step 3: Check if the application appears under Installed Apps or Available Apps.**

### *5.2.2 Method 2: Using Microsoft Endpoint Manager*

**Step 1: In MEM, go to Apps > Monitor.**

**Step 2: Check the Device Install Status to verify deployment.**

## 5.3. Removing an Application Using Intune

To uninstall an application:

1. In MEM, navigate to **Apps** > **All Apps**.
2. Select the application.
3. Modify the **Assignment type** to **Uninstall**.
4. Click **Save** and allow time for the policy to apply.

# 6. Configuring Endpoint Security in Microsoft Intune

## 6.1 Accessing Endpoint Security Settings

**Step 1: Log into Microsoft Endpoint Manager**

- Open a web browser and navigate to https://endpoint.microsoft.com.
- Sign in using your **Intune administrator** account.

**Step 2: Navigate to Endpoint Security**

- In the **left-hand menu**, click on **Endpoint Security**.
- You will see multiple security configuration categories, such as:
  - **Antivirus** – Configure and enforce Microsoft Defender Antivirus settings.
  - **Disk Encryption** – Enable and enforce BitLocker (Windows) and FileVault (macOS).
  - **Firewall** – Manage Windows Defender Firewall rules and settings.
  - **Endpoint Detection & Response (EDR)** – Integrate with Microsoft Defender for Endpoint.
  - **Attack Surface Reduction (ASR)** – Reduce exposure to cyber threats through security controls.
  - **Security Baselines** – Apply recommended security settings for Windows and Microsoft Defender.

## 6.2 Configuring Antivirus Protection (Microsoft Defender for Endpoint)

**Step 1: Go to Endpoint Security > Antivirus**.

**Step 2: Click + Create Policy and select:**

- **Platform**: Windows 10/11 or macOS.
- **Profile Type**: Microsoft Defender Antivirus.

**Step 3: Configure Antivirus Settings, including:**

- **Real-time protection** – Ensures files are scanned upon access.
- **Cloud-delivered protection** – Enables Microsoft Defender to receive the latest threat intelligence.
- **Automatic sample submission** – Allows suspicious files to be sent for analysis.
- **Scan settings** – Set scheduled scan times and quick/full scan options.

**Step 4: Assign the Policy** to user or device groups.

**Step 5: Click Create to deploy the policy.**

**Verification:**

- Navigate to **Reports > Antivirus Reports** to check policy enforcement.
- Run **Get-MpPreference** on a Windows device to verify Defender settings.

## 6.3 Configuring Disk Encryption (BitLocker & FileVault)

Disk encryption ensures that sensitive data is protected against unauthorized access in case of device loss or theft.

**Step 1: Go to Endpoint Security > Disk Encryption.**

**Step 2: Click + Create Policy and select:**

- **Platform**: Windows 10/11.
- **Profile Type**: BitLocker.

**Step 3: Configure BitLocker settings, including:**

- **Require encryption for fixed drives**.
- **Enforce startup PINs for additional security**.
- **Backup BitLocker recovery keys to Azure AD**.

**Step 4: Assign the policy to Windows device groups and click Create.**

**Verification:**

- Navigate to **Reports > Encryption Reports** to ensure compliance.
- On a Windows device, run manage-bde -status to check BitLocker status.

## 6.4 Configuring Firewall Protection

**Step 1: Go to Endpoint Security > Firewall.**

**Step 2: Click + Create Policy and select:**

- **Platform**: Windows 10/11.
- **Profile Type**: Windows Defender Firewall.

**Step 3: Configure Firewall rules, including:**

- **Enable Windows Defender Firewall**.
- **Define inbound and outbound rules**.
- **Allow/block specific applications and ports**.

**Step 4: Assign the policy to Windows devices and click Create.**

**Verification:**

- Navigate to **Reports > Firewall Reports**.
- On a Windows device, check firewall settings with Get-NetFirewallProfile.

## 6.5 Configuring Attack Surface Reduction (ASR) Rules

**Step 1: Navigate to Endpoint Security > Attack Surface Reduction.**

**Step 2: Click + Create Policy and select:**

- **Platform**: Windows 10/11.
- **Profile Type**: Attack Surface Reduction Rules.

**Step 3: Configure ASR settings, such as:**

- **Block Office applications from creating child processes** (prevents macro-based attacks).
- **Block executable content from email and webmail**.
- **Use advanced ransomware protection**.

**Step 4: Assign the policy to device groups and click Create.**

**Verification:**

- Navigate to **Reports > Attack Surface Reduction Reports**.
- Use PowerShell command:

```
Get-MpPreference | Select-Object AttackSurfaceReductionRules_Ids
```

## 6.6 Configuring Endpoint Detection & Response (EDR) with Microsoft Defender

Step 1: Go to **Endpoint Security > Endpoint Detection & Response**.

Step 2: Click **+ Create Policy** and select:

  - **Platform**: Windows 10/11 or macOS.
  - **Profile Type**: Microsoft Defender for Endpoint.

Step 3: Enable the following settings:

  - **Cloud-based protection** for threat intelligence.
  - **Automated incident response** to contain threats.
  - **Behavior monitoring** for anomaly detection.

**Step 4:** Assign the policy to **devices enrolled in Defender for Endpoint**.

**Step 5:** Click **Create** to deploy the policy.

**Verification:**

- Navigate to **Reports > Endpoint Detection & Response Reports**.
- Use **Microsoft Defender Security Center** for detailed threat insights.

### 6.7 Responding to Security Incidents in Intune

If a device is compromised, administrators can take immediate action.

**Step 1: Go to Devices > Windows/macOS/iOS/Android > Select Device**.

**Step 2 : Choose from the following remote actions:**

- **Remote Lock** – Lock the device to prevent unauthorized access.
- **Reset Passcode** – Force a password reset on mobile devices.
- **Wipe Device** – Erase all data (used for lost/stolen devices).
- **Retire Device** – Remove company data while keeping personal data intact.

**Step 3: Confirm the action and monitor security reports for further analysis.**

## 7. Conclusion

By following the steps outlined in this SOP, IT administrators can effectively enroll, configure, and monitor devices, ensuring that security policies and applications are properly deployed. Whether managing Windows, macOS, iOS, or Android devices, Intune offers the tools necessary to maintain a secure and efficient device ecosystem. With the ability to enforce security settings such as antivirus protection, disk encryption, and firewall management, as well as responding swiftly to security incidents, Intune empowers organizations to safeguard their data and resources while maintaining seamless device operations.