|  |
| --- |
| Setting up Microsoft Defender for Endpoint |

# Setting up Microsoft Defender for Endpoint

## Background and benefit

Microsoft Defender for Endpoint provides a centralised security management solution for your devices. This allows you to remotely monitor and respond to cyber security events on your staff’s devices.

## Prerequisites

### Licensing

Microsoft Defender for Endpoint (MDE) comes in two versions: a standard capability (P1) and a premium capability (P2). Microsoft 365 E3 or A3 licensing includes MDE P1, and Microsoft 365 E5 or A5 licensing includes MDE P2. You can also purchase MDE as a stand-alone product.

For the purposes of these instructions, you only need MDE P1.

### Deployment methods

MDE requires devices to be “onboarded”. This means that you need a configuration for each device (see instructions below). For a large number of devices, it will be impractical to do this manually, so a device management capability is recommended (eg, Intune).

## What you need to do as an organisation

**Configure your Microsoft 365 environment**

MDE is part of Microsoft Defender XDR. If you haven’t already done the first-time set-up of Microsoft Defender XDR, do this first.

1. Navigate to the [Defender admin portal](https://security.microsoft.com).
2. Select **Assets**.
3. Select **Devices.**
4. A welcome to Defender for Business screen will appear. Click **Get Started** and follow the instructions on screen.

**Important:** If asked where you want to store your data, choose Australia (or New Zealand once this becomes available).

### Onboarding devices (manual)

If you have a small number of devices (fewer than about 10), you can manually onboard them.

1. Go to the [Defender admin portal](https://security.microsoft.com) > **Settings** > **Endpoints**.
2. Select **Onboarding** under the Device management menu.
3. Select your operating system, set the Connectivity type to **Standard**, and choose the **Local Script** as the deployment method.
4. Download the onboarding package and run this on every device.
5. On the page where you downloaded the onboarding package, a sample script is provided to generate a fake alert for testing purposes (see **Incidents** and **Alerts** > **Alerts**).

### Onboarding devices (Intune)

If you have a larger number of devices, you can use Intune to onboard them.

1. Go to the [Defender admin portal](https://security.microsoft.com) > **Settings** > **Endpoints**.
2. Under **General**, go to **Advanced features** and make sure the **Microsoft Intune Connection** option is turned on. It’s also a good idea to turn on **Enable EDR in block mode**. Enabling Endpoint Detection and Response (EDR) in block mode using Microsoft Intune can help enhance the security of your organisation's endpoints by blocking malicious artifacts that are detected by EDR, even if the primary antivirus (Microsoft Defender Antivirus) has not detected them.
3. Go to the [Intune Management portal](https://intune.microsoft.com) > **Tenant** **administration** > **Connectors and tokens** > **Microsoft Defender for Endpoint**.
4. Make sure the **Connection Status** is **Enabled** (this is controlled via the setting in the Defender XDR portal).
5. Go to **Endpoint security** (on the left main menu)> **Endpoint detection and response** > **Create Policy**.
6. For **Platform**, select **Windows 10, Windows 11, and Windows Servers.**
7. For **Profile type**, select **Endpoint detection and response**, and then select **Create**.
8. Enter a name and description and click **Next**.
9. Under the **Configuration Settings**:
	1. MDE client configuration package type – **Auto from connector**
	2. Sample Sharing – **Not configured**
	3. Telemetry Reporting Frequency – **Expedite**
	4. Click **Next** and **Next**.
10. Click through to **Assignments** and search for and add **all devices** (or a preconfigured target group).
11. Click **Next** and **Save**.

[Microsoft Defender for Endpoint – Configuration Manager | Microsoft Learn](https://learn.microsoft.com/en-us/mem/configmgr/protect/deploy-use/defender-advanced-threat-protection)

### What to expect as an administrator within your organisation

MDE will give you visibility of your devices and provide additional actions within the Defender XDR portal. Any security events on your staff’s devices will generate an alert and corresponding incident under Incidents & Alerts. You can respond to these events through actions such as triggering an antivirus scan.

You can get a view of all your devices under the **Assets** > **Devices** menu item. Clicking into a device will give you detailed information about that device and its security status (the details are different depending on whether you have a P1 or a P2 license).

### Change and adoption

Your staff shouldn’t notice any change. However, it may be a good opportunity to remind them about acceptable use and that their devices are monitored.