

# Deploy the Microsoft Defender for Endpoint environment

By: Ryan Stewart

As a Security Operations Analyst tasked with implementing Microsoft Defender for Endpoint at my company, my responsibilities include configuring our tenant, onboarding devices, and managing security team access.

Under the guidance of leadership, who aim to gain insights into necessary adjustments for our SecOps team's response procedures, I embark on the process.

Firstly, I kickstart the Defender for Endpoint environment setup. Then, I proceed to onboard the initial batch of devices by executing the onboarding script on each device. Once devices are onboarded, I focus on configuring security settings tailored to our environment. This involves creating device groups and ensuring each device is assigned to the appropriate group.

By the end of this module, I will have mastered the following skills:

- Establishing a Microsoft Defender for Endpoint environment
- Onboarding devices for monitoring through Microsoft Defender for Endpoint
- Configuring settings for the Microsoft Defender for Endpoint environment

# Create your environment

When accessing Microsoft Defender portal settings for Endpoints for the first time, you'll be able to configure many attributes. You must be a global administrator or security administrator for the tenant. On the Set-up preferences page, you can set the:



















**Data storage location** - Determine where you want to be primarily hosted: US, EU, or UK. You **can't** change the location after this set up and Microsoft won't transfer the data from the specified geolocation.

**Data retention** - The default is six months.








**Enable preview features** - The default is on, can be changed later.

To access the Microsoft Defender portal settings for Endpoints do the following action:

1. Go to (<https://security.microsoft.com>)
2. Select **Settings**.
3. Select **Endpoints**.

	Threat tracker
	Attack simulation training
	Policies & rules
<hr/>	
	Cloud apps 
	Cloud discovery
	Cloud app catalog
	OAuth apps
	App governance
	Files
	Activity log
	Governance log
	Policies 
<hr/>	
	Reports
	Health
	Permissions
	Settings

## Settings

Name	
	Security center
	Microsoft 365 Defender
	Endpoints
	Email & collaboration
	Identities
	Device discovery
	Cloud Apps

## Network configuration

If the organization doesn't require the endpoints to use a Proxy to access the Internet, the following configuration isn't required.

The Microsoft Defender for Endpoint sensor requires Microsoft Windows HTTP (WinHTTP) to report sensor data and communicate with the Microsoft Defender for Endpoint service. The embedded Microsoft Defender for Endpoint sensor runs in the system context using the LocalSystem account. The sensor uses Microsoft Windows HTTP Services (WinHTTP) to enable communication with the Microsoft Defender for Endpoint cloud service. The WinHTTP configuration setting is independent of the Windows Internet (WinINet) internet browsing proxy settings and can only discover a proxy server by using the following discovery methods:

Autodiscovery methods:

- Transparent proxy
- Web Proxy Autodiscovery Protocol (WPAD)

If a Transparent proxy or WPAD has been implemented in the network topology, there's no need for special configuration settings.