Deploy the Microsoft Defender for Endpoint environment

# Creating your environment

* You must be a **global administrator or security administrator**
* On the set-up preferences page you can set the:
  + Data storage location – cannot change the location after this set up
  + Data retention – default is 6 months
  + Enable preview features – default is on
* To access the Microsoft 365 Defender portal settings for Endpoints do the following action:
  + Go to security.microsoft.com
  + Select **settings**
  + Select **Endpoints**

# Network configuration

Microsoft Defender for Endpoint sensor requires Microsoft Windows HTTP (WinHTTP) to report sensor data and communicate with defender for endpoint service. The embed sensor runs in the system context using the LocalSystem account. It also uses WinHTTP to enable communicate with defender for endpoint cloud service.

WinHTTP configuration setting can only discover a proxy server by using the following discovery methods:

Autodiscovery methods:

* Transparent proxy
* Web Proxy Autodiscovery Protocol (WPAD)

# Onboard Devices

Go to Microsoft 365 Defender portal to onboard any supported devices.

Steps that follow are:

* In Settings, Endpoints, Device management, Onboarding select operating system dropdown to see the supported options
* After selecting the operating system option, the supported deployment options are outlined.

Here is a list of windows 10 supported deployment options:

* Group Policy
* Microsoft endpoint Configuration Manager Current branch and later
* Mobile Device Management (including Microsoft Intune)
* Local Script (for up to 10 devices)
* VDI onboarding script for non-persistent devices
* System Centre Configuration Manager 2012/2012 R2/1511/1602

# Create and manage roles for role-based access control

* View data
  + Security operations - View all security operations data in the portal
  + Threat and vulnerability management - View threat and vulnerability management data in the portal
* Active remediation actions
  + Security operations - Take response actions, approve or dismiss pending remediation actions, manage allowed/blocked lists for automation and indicators
  + Threat and vulnerability management - Exception handling - Create new exceptions and manage active exceptions
  + Threat and vulnerability management - Remediation handling - Submit new remediation requests, create tickets, and manage existing remediation activities
* Alerts investigation - Manage alerts, start automated investigations, run scans, collect investigation packages, manage device tags, and download only portable executable (PE) files
* Manage security settings in Security Center - Configure alert suppression settings, manage folder exclusions for automation, onboard and offboard devices, and manage email notifications, manage evaluation lab
* Live response capabilities
  + Basic commands:
    - Start a live response session
    - Perform read-only live response commands on remote device (excluding file copy and execution
  + Advanced commands:
    - Download a file from the remote device via live response
    - Download PE and non-PE files from the file page
    - Upload a file to the remote device
    - View a script from the files library
    - Execute a script on the remote device from the files library

# Configure Device groups

In Microsoft defender for endpoint you can create device groups and use them to:

* Limit access based on RBAC
* Configure different auto-remediation settings for different sets of devices
* Assign specific remediation levels to apply during automated investigations
* Filter the devices list to just specific device groups using the group filter

As part of the process of creatin a device group you’ll:

* Set the automated remediation level for that group
* Select the Azure AD user group that should have access to the device group
* Rank the device group relative to other groups once created
* Specify the matching rule that determines which device group belongs to the group based on the device name, domain, tags and os platform.

# Create a device group

1. In navigation pane, select settings, select **Endpoints** and then under **Permissions** select **Device Groups**
2. Select + **Add device group**
3. Enter the group name and automation settings and specify the matching rule
4. Preview several devices that will be matched by this rule. If satisfied, select the User access tab.
5. Assign the user groups that can access the DG that’s been created. Can only grant access to AAD user groups that have been assigned RBAC roles.
6. Select **Close.** The configuration changes are applied