

Microsoft Defender for endpoint

[Securitycenter.windows.com](https://securitycenter.windows.com)



Microsoft Security Center

Set up

Welcome MyrlWhitney

Step 1

Set up permissions



Step 2

Get started



Step 3

Set up preferences



Step 4



This wizard will guide you through the steps to onboard your organization onto the Microsoft Defender for Endpoint service.

For more detailed help and information on the onboarding process, see the [Onboard devices and set up access](#) section in the [Microsoft Defender for Endpoint guide](#).

For more information about how Microsoft Defender for Endpoint stores and retains your data, see the [Data storage and privacy](#) section in the [Microsoft Defender for Endpoint guide](#).

You need to set aside 10 to 20 minutes to complete the process, although it might take longer before all onboarded devices appear in the Microsoft Defender for Endpoint portal.

Click 'Next' to start the onboarding process.

Set up preferences

Step 1



Set up permissions

Step 2



Get started

Step 3



Set up preferences

Step 4



Onboard a device

Select data storage location



This option cannot be changed without completely offboarding from Microsoft Defender for Endpoint and completing a new enrollment process.

For more information, see the [Data storage and privacy](#) section in the [Microsoft Defender for Endpoint guide](#).

US

UK

Europe

Select the data retention policy

This will determine the period of time we retain your data in your cloud instance.

Note this does not refer to expiration or cancellation of your Microsoft Defender for Endpoint contract.

For more information, see the [Data storage and privacy](#) section in the [Microsoft Defender for Endpoint guide](#).



Step 3

Set up preferences



Step 4

Onboard a device



Select the data retention policy

This will determine the period of time we retain your data in your cloud instance.
Note this does not refer to expiration or cancellation of your Microsoft Defender for Endpoint contract.
For more information, see the [Data storage and privacy](#) section in the [Microsoft Defender for Endpoint guide](#).

180 days



Select your organization size

Select the estimated number of devices you have in your organization.

Up to 1,000



Preview features

This section allows you to turn preview features on/off.
Turn on to be among the first to try upcoming features.
It is turned on by default to allow you to experience the latest features as they become available.



On



Back

Next



Step 3

Set up preferences

Step 4

Onboard a device

Select the data retention policy

This will determine the period of time we retain your data in your cloud instance.
Note this does not refer to expiration or cancellation of your Microsoft Defender for Endpoint contract.
For more information, see the [Data storage and privacy](#) section in the [Microsoft Defender for Endpoint guide](#).

180 da

Select

Select th

Up to

Preview features

This section allows you to turn preview features on/off.
Turn on to be among the first to try upcoming features.
It is turned on by default to allow you to experience the latest features as they become available.

On

Create your cloud instance

You won't be able to change some of your preferences (such as the data storage location) after clicking 'Continue'.
If you want to check or make any changes, click 'Back to preferences' and review your preferences. Click 'Continue' if you want to set up your account.



Microsoft
Security Center

Set up

Creating your Microsoft Defender for Endpoint account

Step 1



Set up permissions

Step 2

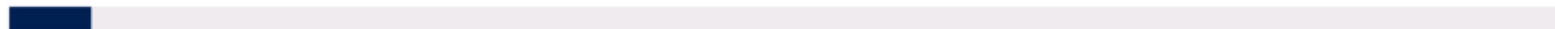


Get started

Step 3



Set up preferences





Microsoft Security Center

Set up

Step 1



Set up permissions

Step 2



Get started

Step 3



Set up preferences

Step 4



Microsoft Defender for Endpoint is almost ready

To start experiencing Microsoft Defender for Endpoint, you need to onboard at least one device and run a detection test on the device. Ensure you:

1. Onboard a device

First device onboarded: Incomplete

Onboard devices to Microsoft Defender for Endpoint using the onboarding configuration package that matches your [preferred deployment method](#). For other device preparation instructions, read [Onboard and set up](#).

Deployment method

Local Script (for up to 10 devices)

You can configure a single device by running a script locally.

Note: This script has been optimized for usage with a limited number of devices (1-10). To deploy at scale, please see other deployment options above.

For more information on how to configure and monitor Microsoft Defender for Endpoint devices, see [Configure devices using a local script](#) section in the [Microsoft Defender for Endpoint guide](#).

[Download onboarding package](#)

2. Run a detection test

First device detection test: Incomplete

To verify that the device is properly onboarded and reporting to the service, run the detection script on the device.

Need help?

device:

- a. Open a Command Prompt window
- b. At the prompt, copy and run the command below. The Command Prompt window will close automatically.

```
powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden $ErrorActionPreference=
'silentlycontinue';(New-Object System.Net.WebClient).DownloadFile('http://127.0.0.1/1.exe',
'C:\\test-WDATP-test\\invoice.exe');Start-Process 'C:\\test-WDATP-test\\invoice.exe'
```



If successful, the detection test will be marked as completed and a new alert will appear in few minutes.

Start using Microsoft Defender for Endpoint 

 Need help?



Step 1

Set up permissions



Step 2

Get started



Step 3

Set up preferences



Step 4

Onboard a device



You can configure a single device by running a script locally.

Note: This script has been optimized for usage with a limited number of devices (1-10). To deploy at scale, please see other deployment options above.

For more information on how to configure and monitor Microsoft Defender for Endpoint devices, see [Configure devices a local script](#)

section in the [Microsoft Defender for Endpoint guide](#).

↓ Download onboarding package

Setup incomplete

To experience Microsoft Defender for Endpoint, you need to onboard and test at least one device. You can also onboard devices later.

Proceed anyway

Cancel

```
powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden $ErrorActionPreference='silentlycontinue';(New-Object System.Net.WebClient).DownloadFile('http://127.0.0.1/1.exe' 'C:\\test-WDATP-test\\invoice.exe');Start-Process 'C:\\test-WDATP-test\\invoice.exe'
```

If successful, the detection test will be marked as completed and a new alert will appear in few minutes.

Start using Microsoft Defender for Endpoint →

Need help

- ⚡
- 🏠
- 📄
- 📊
- 🔗
- 📁
- 📄
- 📄
- 📄
- 📄
- ⚙️

Settings

- Web content filtering
- Automation uploads
- Automation folder exclusions
- Device management**
- Onboarding
- Offboarding
- Network assessments**
- Assessment jobs

This section provides general settings that were previously defined as part of the onboarding process.

Data Storage



This option cannot be changed without completely offboarding from Microsoft Defender for Endpoint and starting a new enrollment process. For more information, see the [Data storage and privacy](#) section in the [Microsoft Defender for Endpoint](#) documentation.

- US
- UK
- Europe

Data Retention

This will determine the period of time we retain your data in your cloud instance. Note this does not refer to expiration or cancellation of your Microsoft Defender for Endpoint contract.



Settings



Web content filtering



Automation uploads



Automation folder exclusions



Device management



Onboarding



Offboarding



Network assessments



Assessment jobs



Select operating system to start onboarding process:

Windows 10 and 11

Onboard devices to Microsoft Defender for Endpoint using the onboarding configuration package that matches your [preferred deployment method](#). For other device preparation instructions, read [Onboard and set up](#).

Deployment method

Mobile Device Management / Microsoft Intune

You can use Mobile Device Management solutions, such as Microsoft Intune to configure and monitor your devices. For more information on how to configure and monitor Microsoft Defender for Endpoint devices, see [Configure devices using Mobile Device Management tools](#) section in the [Microsoft Defender for Endpoint guide](#).

↓ Download onboarding package

2. Run a detection test



Need help?



ENG

Click to go back (Alt+Left arrow), hold to see history

Downloads

WindowsDefenderATPOnboardingPackage.zip
[Open file](#)

Settings

- Web content filtering
- Automation uploads
- Automation folder exclusions

Device management

Onboarding

Offboarding

Network assessments

Assessment jobs

Select operating system to start onboarding process:

Windows 10 and 11

Onboard devices to Microsoft Defender for Endpoint using the onboarding configuration package that matches your [preferred deployment method](#). For other device preparation instructions, read [Onboard and set up](#).

Deployment method

Mobile Device Management / Microsoft Intune

You can use Mobile Device Management solutions, such as Microsoft Intune to configure and monitor your devices. For more information on how to configure and monitor Microsoft Defender for Endpoint devices, see [Configure devices u Device Management tools](#) section in the [Microsoft Defender for Endpoint guide](#).

↓ Download onboarding package

← → ↻ 🔒 https://admin.mic

Microsoft 365 admin center

- ☰
- Billing
- Support
- Settings
- Setup
- Reports
- Health

Admin centers

- Security
- Compliance
- Endpoint Manager
- Azure Active Directory

Microsoft Endpoint Manager admin center

etech ...

Home Microsoft Managed Desktop

Status

Errors/failures	0	Healthy	6
-----------------	---	---------	---

- Account status ✔ Active
- Client apps ✔ No ins
- Connector status ✔ Health
- Device compliance ✔ All in c
- Device configuration ✔ No po
- Service health ✔ Health

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home >

Endpoint security | Overview

Search (Ctrl+/)

Overview

- Overview
 - All devices
 - Security baselines
 - Security tasks
-
- Manage
- Antivirus
 - Disk encryption
 - Firewall
 - Endpoint detection and response
 - Attack surface reduction

Protect and secure devices from one place

Enable, configure, and deploy Microsoft Defender for Endpoint to help prevent security breaches gain visibility into your organization's security posture



Microsoft recommended security settings
Assign baselines quickly and securely using our



Simplified security policies
Select any of the following categories to jump right in and start securing your devices.



Remediate endpoint weaknesses
Remediate endpoint vulnerabilities reported by

- 🏠 Home
- 📊 Dashboard
- ☰ All services
- 📁 Devices
- 🗃️ Apps
- 🛡️ Endpoint security
- 📄 Reports
- 👤 Users
- 👥 Groups
- ⚙️ Tenant administration
- 🔧 Troubleshooting + support

Home > Endpoint security

Endpoint security | Endpoint detection and response

🔍 Search (Ctrl+f)

+ Create Policy 🔄 Refresh ⬇️ Export

Overview

- 📘 Overview
- 📄 All devices
- 📄 Security baselines
- 🛡️ Security tasks

Manage

- 🛡️ Antivirus
- 📁 Disk encryption
- 🛡️ Firewall
- 🛡️ Endpoint detection and response

🔍 Search by column value

Policy name	↕	Policy type	↕	Assigned
-------------	---	-------------	---	----------

No results

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Endpoint security

Endpoint security | Endpoi

Search (Ctrl+/)

Overview

- Overview
- All devices
- Security baselines
- Security tasks

Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and response

+ Create

Search

Policy n

No resu

Create a profile

Platform

Windows 10 and later

Profile

Endpoint detection and response

Endpoint detection and response

Microsoft Defender for Endpoint endpoint detection and response capabilities provide advanced attack detections that are near real-time and actionable. Security analysts can prioritize alerts effectively, gain visibility into the full scope of a breach, and take response actions to remediate threats.

Create

Home > Endpoint security >

Create profile ...

Endpoint detection and response

- 1 Basics
- 2 Configuration settings
- 3 Scope tags
- 4 Assignments
- 5 Review + create

Name * ⓘ

testonboarding ✓

Description ⓘ

Empty text area for description

Platform

Windows 10 and later

Previous

Next

Create profile

Endpoint detection and response

✖ One or more settings in following categories have invalid input:

- ✔ Basics
- ✖ **Configuration settings**
- ③ Scope tags
- ④ Assignments
- ⑤ Review + create

Settings

Endpoint Detection and Response

Microsoft Defender for Endpoint client configuration package type ⓘ

Microsoft Defender for Endpoint offboarding blob ⓘ

Select offboarding file

Remove

Microsoft Defender for Endpoint offboarding filename

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Microsoft Defender for Endpoint onboarding blob ⓘ

Select onboarding file

Remove

Microsoft Defender for Endpoint onboarding filename

Previous

Next

Select file

Select file

"WindowsDefenderATP.onboarding" 

select

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Endpoint security >

Create profile ...

Endpoint detection and response

❌ One or more settings in following categories have invalid input:

Microsoft Defender for Endpoint onboarding blob ⓘ

Select onboarding file

```
{ "body": { "previousOrgIds":  
[], "orgId": "5a71dc03-df33-415a-aa3b-  
f2c1261f1b3a", "geoLocationUrl": "https://  
winatp-gw-  
cus3.microsoft.com/", "datacenter": "CentralUs3",  
"vortexGeoLocation": "US", "version": "1.35"}, "sig": "FLvmpmKXDj7aiom/VZ
```

Remove

Microsoft Defender for Endpoint onboarding filename

WindowsDefenderATP.onboarding ✓

Previous

Next

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Endpoint security >

Create profile ...

Endpoint detection and response

- Basics
- 2 Configuration settings**
- 3 Scope tags
- 4 Assignments
- 5 Review + create

Settings

Search for a setting

Endpoint Detection and Response

Microsoft Defender for Endpoint client configuration package type ⓘ

Onboarding blob

Microsoft Defender for Endpoint onboarding blob ⓘ

Select onboarding file

`{"body":{"previousOrgIds":["orgId":"5a71dc03-df33-415a-aa3b-`

Remove

Previous

Next

onboarding filename

Block sample sharing for all files ⓘ

 Yes Not configured

Expedite telemetry reporting frequency ⓘ

 Yes Not configured

Previous

Next

ninCenter#allservices/cate...

- ⏪
- 🏠 Home
- 📊 Dashboard
- ☰ All services
- 🖥️ Devices
- 📱 Apps
- 🛡️ Endpoint security
- 📄 Reports
- 👤 Users
- 👥 Groups
- ⚙️ Tenant administration
- 🔧 Troubleshooting + support

Home > Endpoint security >

Create profile ...

Endpoint detection and response

- ✅ Basics
- ✅ Configuration settings
- 3** Scope tags
- ④ Assignments
- ⑤ Review + create

Scope tags

Scope tags

Default

[+ Select scope tags](#)

Previous **Next**



- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Endpoint security >

Create profile

Endpoint detection and response

- ✓ Basics
- ✓ Configuration settings
- ✓ Scope tags
- 4** Assignments
- 5 Review + create

Included groups

- 👤 Add groups
- 👤 Add all users
- + Add all devices

Groups

No groups selected

Excluded groups

i When excluding groups, you cannot mix user and device groups across include and exclude. [Click here to learn more about excluding groups.](#)

- Previous
- Next**

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Endpoint security >

Create profile ...

Endpoint detection and response

- Basics
- Configuration settings
- Scope tags
- Assignments
- 5 Review + create**

Summary

Basics

Name	onboarding test
Description	--
Platform	Windows 10 and later

Configuration settings

Auto populate Microsoft Defender for Endpoint onboarding blob	Not configured
Microsoft Defender for Endpoint	!\"body\": \"&\"previousOrOlds\": !\\\"orOld\\\" \\\"5a71dc03-df33-415a-aa3b-

Previous Create

Microsoft Endpoint Manager admin center

Home > Endpoint security

Endpoint security | Endpoint detection and response

Search (Ctrl+/)

Overview

- Overview
- All devices
- Security baselines
- Security tasks

Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and response

+ Create Policy Refresh Export

Search by column value

Policy name	Policy type	Assigned	Platform	Target
onboarding test	Endpoint detection a...	Yes	Windows 10 and later	mdm

This creates the onboarding package to enable and enroll your Windows devices into the defender for endpoint solution.

Settings

- General
 - Data retention
 - Licenses
 - Email notifications
 - Advanced features
 - Auto remediation
 - Portal redirection
- Permissions
 - Roles

https://securitycenter.windows.com/dashboards_junction

- On Download quarantined files
Backup quarantined files in a secure and compliant location so they can be downloaded directly from quarantine.
- Off Share endpoint alerts with Microsoft Compliance Center
Forwards endpoint security alerts and their triage status to Microsoft Compliance Center, allowing enhance [insider risk management](#) policies with alerts and remediate internal risks before they cause harm. Forwarded data is processed and stored in the same location as your Office 365 data.
- On Microsoft Intune connection
Connects to [Microsoft Intune](#) to enable sharing of device information and enhanced policy enforcement. Intune provides additional information about managed devices for secure score. It can use risk information to enforce [conditional access](#) and other security policies.

[Save preferences](#) [New](#)

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home >

Endpoint security | C

Search (Ctrl+/)

- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and response
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access

Monitor

- Assignment failures (preview)

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration

Home > Endpoint security >

Compliance policies | Policies

Search (Ctrl+I)

- Policies
- Notifications
- Retire Noncompliant Devices
- Compliance policy settings
- Scripts

+ Create Policy Columns Filter Refresh Export

Search by name

Policy Name	Platform	Policy Type	Last modified
-------------	----------	-------------	---------------

No compliance policy profiles.

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Endpoint security >

Compliance policies | Policies

Search (Ctrl+/)

- Policies
- Notifications
- Retire Noncompliant Devices
- Compliance policy settings
- Scripts

Create a policy

Platform
Windows 10 and later

Profile type
Windows 10/11 compliance policy

Create

- 🏠 Home
- 📊 Dashboard
- ☰ All services
- 🖨️ Devices
- 🗃️ Apps
- 🛡️ Endpoint security
- 📄 Reports
- 👤 Users
- 👥 Groups
- ⚙️ Tenant administration
- 🔧 Troubleshooting + support

⏪ [Home](#) > [Endpoint security](#) > [Compliance policies](#) >

Windows 10/11 compliance policy ...

Windows 10 and later

- ✅ Basics
- 2** Compliance settings
- ③ Actions for noncompliance
- ④ Assignments
- ⑤ Review + create

- ∨ Custom Compliance
- ∨ Device Health
- ∨ Device Properties
- ∨ Configuration Manager Compliance
- ∨ System Security
- ∨ Microsoft Defender for Endpoint

Previous

Next

Device Health

Windows Health Attestation Service evaluation rules

Require BitLocker ⓘ	Require	Not configured
Require Secure Boot to be enabled on the device ⓘ	Require	Not configured
Require code integrity ⓘ	Require	Not configured

Device Properties

Operating System Version ⓘ

Minimum OS version ⓘ	Not configured
Maximum OS version ⓘ	Not configured
Minimum OS version for mobile devices ⓘ	Not configured
Maximum OS version for mobile devices ⓘ	Not configured

System Security

Password

Require a password to unlock mobile devices ⓘ	Require	Not configured
Simple passwords ⓘ	Block	Not configured
Password type ⓘ	Device default	▼
Minimum password length ⓘ	4	
Maximum minutes of inactivity before password is required ⓘ	Not configured	▼
Password expiration (days) ⓘ	41	

^ Microsoft Defender for Endpoint

Microsoft Defender for Endpoint rules

Require the device to be at or under the machine risk score: ⓘ

Previous

Next

If my device in Microsoft for endpoint is either medium or high I want my device in intune to be listed as non compliant

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Endpoint security > Compliance policies >

Windows 10/11 compliance policy

Windows 10 and later

- Basics
- Compliance settings
- 3 Actions for noncompliance**
- 4 Assignments
- 5 Review + create

Specify the sequence of actions on noncompliant devices

Action	Schedule (days after noncompliance) ⓘ	Message template	Additional recipients (...)
Mark device noncompliant	Immediately		
<input type="text" value=""/>	<input type="text" value="0"/>		

Previous Next

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Endpoint security > Compliance policies >

Windows 10/11 compliance policy

Windows 10 and later

- Basics
- Compliance settings
- Actions for noncompliance
- 4 Assignments**
- 5 Review + create

Included groups

- Add groups
- Add all users

Groups	Filter	Filter mode
--------	--------	-------------

No groups selected

Excluded groups

i When excluding groups, you cannot mix user and device groups across include and exclude. [Click here to learn more about excluding groups.](#)

Previous

Next

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Endpoint security > Compliance policies >

Windows 10/11 compliance policy

Windows 10 and later

- Basics
- Compliance settings
- Actions for noncompliance
- Assignments
- 5 Review + create**

Summary

Basics

Name	windows 10 compliance policy
Description	--
Platform	Windows 10 and later
Profile type	Windows 10/11 compliance policy

Compliance settings

System Security

Previous Create

Click to go back (Alt+Left arrow), hold to see history

MICROSOFT Endpoint Manager admin center


Home > Endpoint security > Compliance policies >

windows 10 compliance policy ...

Device compliance policy

 Delete

 Overview

 Assign profile to at least one group. Click Properties and then Assignments.

Manage

^ Essentials

 Properties

Profile type	Assigned
Windows 10/11 compliance policy	No
Platform supported	Groups assigned
Windows 10 and later	0
Groups excluded	
0	

Monitor

 Device status

 User status

 Per-setting status

Policy assignment status — Windows 10 and later devices



- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support