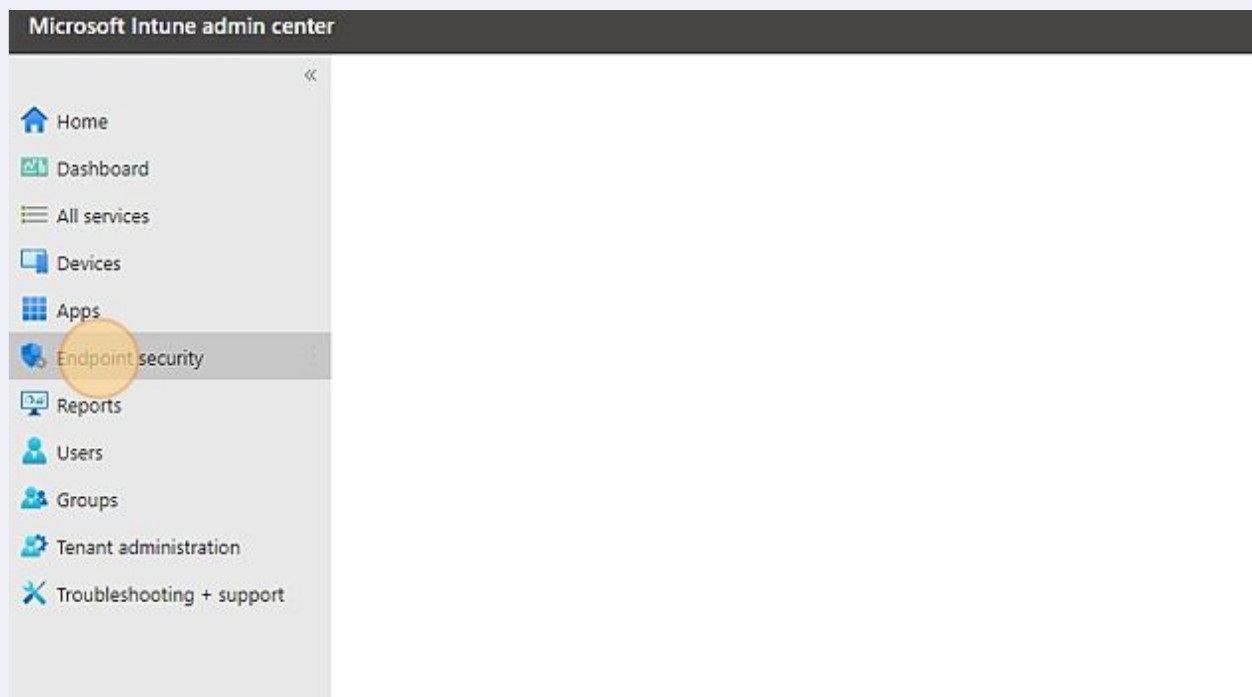


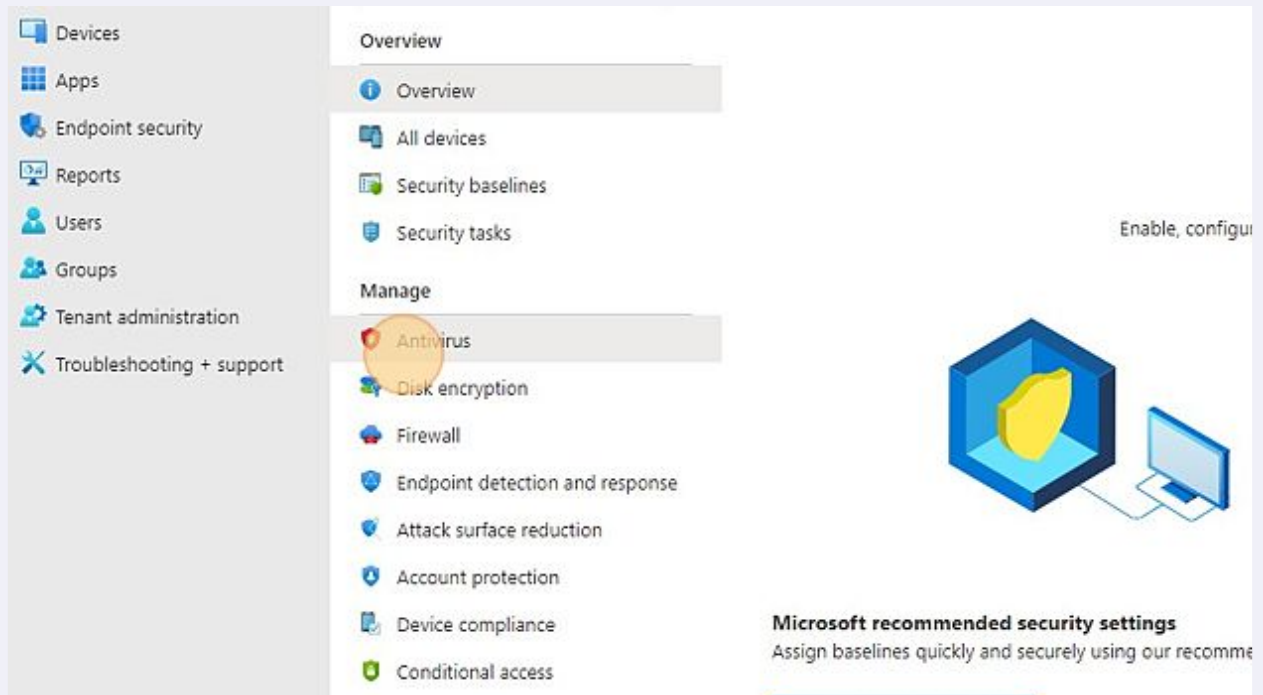
# How to Create a Defender for Endpoint Antivirus Profile for Windows in Microsoft 365

1 Navigate to [endpoint.microsoft.com](https://endpoint.microsoft.com)

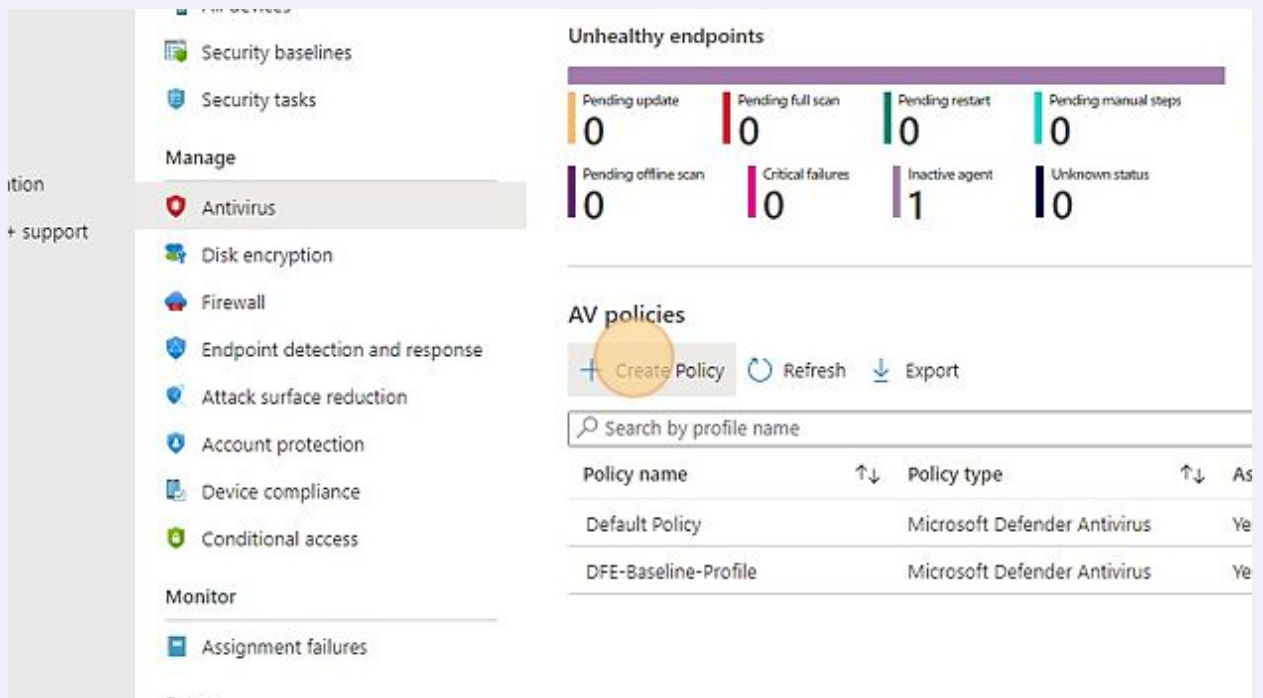
2 Click "Endpoint security"



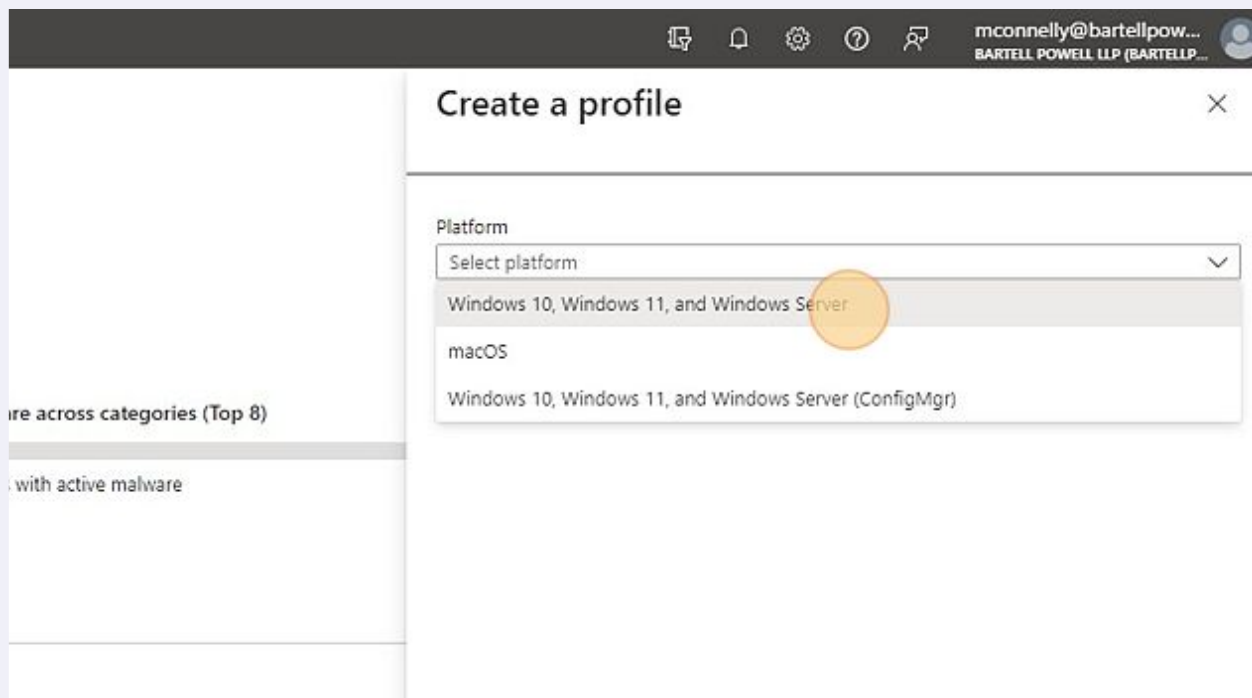
### 3 Click "Antivirus"



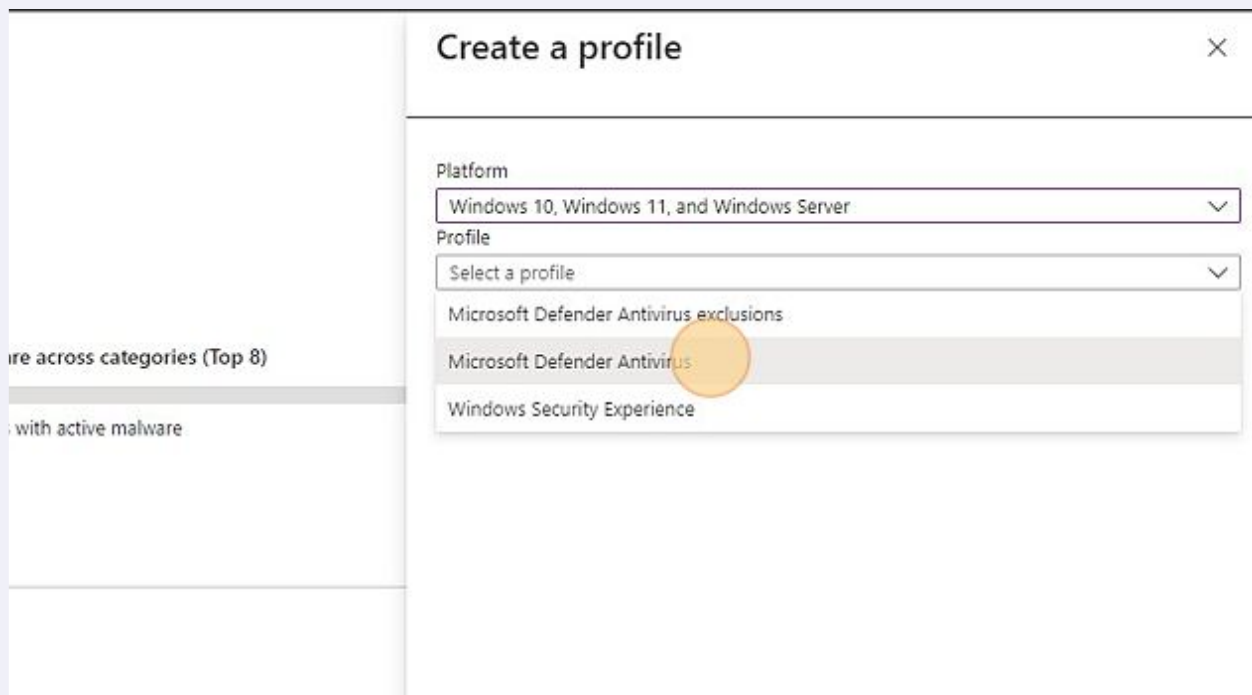
### 4 Click "Create Policy"



- 5 Select "Windows 10, Windows 11, Windows Server" for the "Platform"



- 6 Select "Microsoft Defender Antivirus" for the "Profile"



## 7 Click "Create"

Assigned	↑↓	Platform
Yes		Windows 10 and later
Yes		Windows 10 and later

Create

## 8 Name: DFE-Security-Baseline Description: This AV profile is used as a security baseline for all endpoints.

tion  
support

1 Basics2 Configuration settings3 Scope tags4 Assignments5 Review + create

Name \*

DFE-Security-Baseline

Description

This AV profile is used as a security baseline for all endpoints.

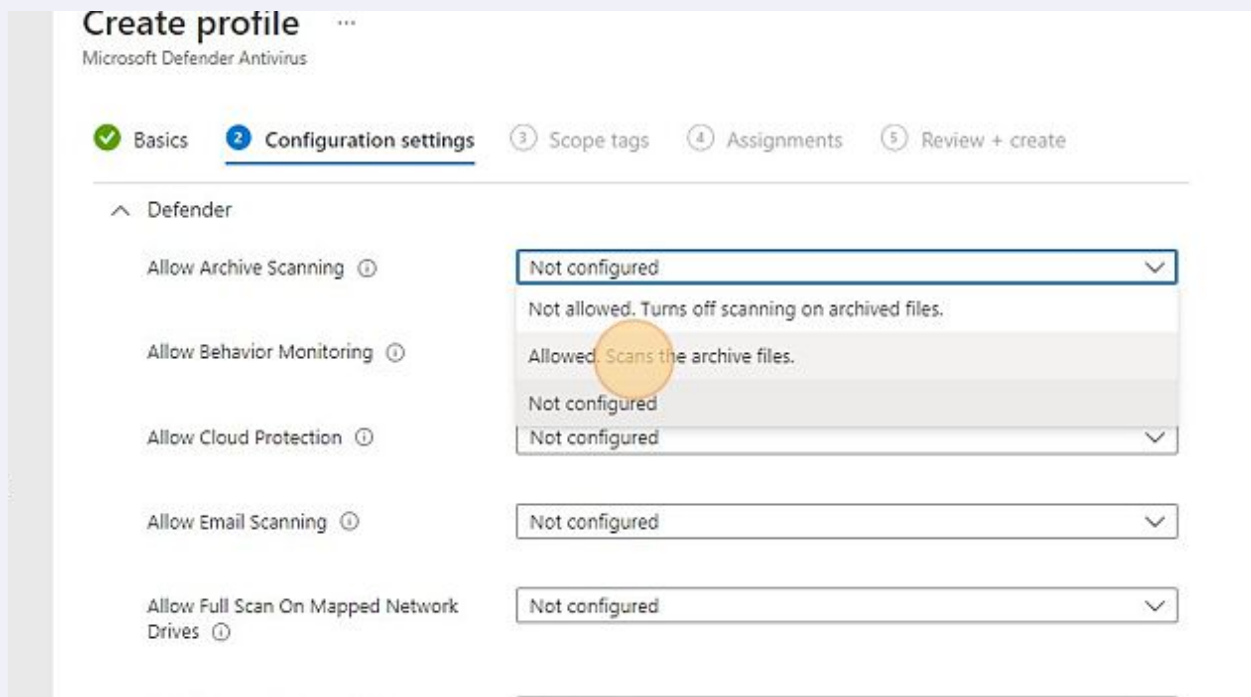
Platform

Windows 10 and later

9 Click "Next"



10 Click "Allowed. Scans the archive files."



11 Click "Allowed. Turns on real-time behavior monitoring."

Defender

Allow Archive Scanning ⓘ	Allowed. Scans the archive files.
Allow Behavior Monitoring ⓘ	Not configured
Allow Cloud Protection ⓘ	Not allowed. Turns off behavior monitoring.
Allow Email Scanning ⓘ	Allowed. Turns on real-time behavior monitoring.
Allow Full Scan On Mapped Network Drives ⓘ	Not configured
Allow Full Scan Removable Drive Scanning ⓘ	Not configured

12 Click "Allowed. Turns on Cloud Protection."

Defender

Allow Archive Scanning ⓘ	Allowed. Scans the archive files.
Allow Behavior Monitoring ⓘ	Allowed. Turns on real-time behavior monitoring.
Allow Cloud Protection ⓘ	Not configured
Allow Email Scanning ⓘ	Not allowed. Turns off Cloud Protection.
Allow Full Scan On Mapped Network Drives ⓘ	Allowed. Turns on Cloud Protection.
Allow Full Scan Removable Drive Scanning ⓘ	Not configured
Allow Intrusion Prevention System ⓘ	Not configured

13 Click "Allowed. Turns on email scanning."

A screenshot of the Windows Security settings window. The 'Allow Email Scanning' dropdown menu is open, showing four options: 'Not configured', 'Not allowed. Turns off email scanning.', 'Allowed. Turns on email scanning.' (which is highlighted with a yellow circle), and 'Not configured'. Other settings visible include 'Allow Archive Scanning' (Allowed), 'Allow Behavior Monitoring' (Allowed), 'Allow Cloud Protection' (Allowed), 'Allow Full Scan On Mapped Network Drives' (Not configured), 'Allow Full Scan Removable Drive Scanning' (Not configured), 'Allow Intrusion Prevention System' (Not configured), and 'Allow scanning of all downloaded files and attachments' (Not configured).

Setting	Value
Allow Archive Scanning ⓘ	Allowed. Scans the archive files. ▼
Allow Behavior Monitoring ⓘ	Allowed. Turns on real-time behavior monitoring. ▼
Allow Cloud Protection ⓘ	Allowed. Turns on Cloud Protection. ▼
Allow Email Scanning ⓘ	Not configured ▼ Not allowed. Turns off email scanning. Allowed. Turns on email scanning. (selected) Not configured
Allow Full Scan On Mapped Network Drives ⓘ	Not configured ▼
Allow Full Scan Removable Drive Scanning ⓘ	Not configured ▼
Allow Intrusion Prevention System ⓘ	Not configured ▼
Allow scanning of all downloaded files and attachments ⓘ	Not configured ▼

14 Click "Allowed. Scans mapped network drives."

A screenshot of the Windows Security settings window. The 'Allow Full Scan On Mapped Network Drives' dropdown menu is open, showing four options: 'Not configured', 'Not allowed. Disables scanning on mapped network drives.', 'Allowed. Scans mapped network drives.' (which is highlighted with a yellow circle), and 'Not configured'. Other settings visible include 'Allow Behavior Monitoring' (Allowed), 'Allow Cloud Protection' (Allowed), 'Allow Email Scanning' (Allowed), 'Allow Full Scan Removable Drive Scanning' (Not configured), 'Allow Intrusion Prevention System' (Not configured), 'Allow scanning of all downloaded files and attachments' (Not configured), and 'Allow Realtime Monitoring' (Not configured).

Setting	Value
Allow Behavior Monitoring ⓘ	Allowed. Turns on real-time behavior monitoring. ▼
Allow Cloud Protection ⓘ	Allowed. Turns on Cloud Protection. ▼
Allow Email Scanning ⓘ	Allowed. Turns on email scanning. ▼
Allow Full Scan On Mapped Network Drives ⓘ	Not configured ▼ Not allowed. Disables scanning on mapped network drives. Allowed. Scans mapped network drives. (selected) Not configured
Allow Full Scan Removable Drive Scanning ⓘ	Not configured ▼
Allow Intrusion Prevention System ⓘ	Not configured ▼
Allow scanning of all downloaded files and attachments ⓘ	Not configured ▼
Allow Realtime Monitoring ⓘ	Not configured ▼

## 15 Click "Allowed. Scans removable drives."

Allow Email Scanning ⓘ	Allowed. Turns on email scanning. ▼
Allow Full Scan On Mapped Network Drives ⓘ	Allowed. Scans mapped network drives. ▼
Allow Full Scan Removable Drive Scanning ⓘ	Not configured ▼
Allow Intrusion Prevention System ⓘ	Not allowed. Turns off scanning on removable drives. Allowed. Scans removable drives. Not configured
Allow scanning of all downloaded files and attachments ⓘ	Not configured ▼
Allow Realtime Monitoring ⓘ	Not configured ▼
Allow Scanning Network Files ⓘ	Not configured ▼

## 16 Click Allow Intrusion Prevention

Allow Full Scan On Mapped Network Drives ⓘ	Allowed. Scans mapped network drives. ▼
Allow Full Scan Removable Drive Scanning ⓘ	Allowed. Scans removable drives. ▼
Allow Intrusion Prevention System ⓘ	Not configured ▼
Allow scanning of all downloaded files and attachments ⓘ	Not allowed. Allowed. Not configured
Allow Realtime Monitoring ⓘ	Not configured ▼
Allow Scanning Network Files ⓘ	Not configured ▼
Allow Script Scanning ⓘ	Not configured ▼



## 17 Click Allow scanning of all downloaded files and attachments

This screenshot shows the Windows Security settings window. The 'Allow scanning of all downloaded files and attachments' dropdown menu is open, displaying three options: 'Not configured', 'Not allowed', and 'Allowed'. The 'Allowed' option is highlighted with a yellow circle, indicating it is the correct selection for step 17.

Setting	Value
Allow Full Scan Removable Drive Scanning ⓘ	Allowed. Scans removable drives.
Allow Intrusion Prevention System ⓘ	Allowed.
Allow scanning of all downloaded files and attachments ⓘ	Allowed.
Allow Realtime Monitoring ⓘ	Not configured
Allow Scanning Network Files ⓘ	Not configured
Allow Script Scanning ⓘ	Not configured
Allow User UI Access ⓘ	Not configured

## 18 Click "Allowed. Turns on and runs the real-time monitoring service."

This screenshot shows the Windows Security settings window. The 'Allow Realtime Monitoring' dropdown menu is open, displaying four options: 'Not configured', 'Not allowed. Turns off the real-time monitoring service.', 'Allowed. Turns on and runs the real-time monitoring service.', and 'Not configured'. The 'Allowed. Turns on and runs the real-time monitoring service.' option is highlighted with a yellow circle, indicating it is the correct selection for step 18.

Setting	Value
Allow Intrusion Prevention System ⓘ	Allowed.
Allow scanning of all downloaded files and attachments ⓘ	Allowed.
Allow Realtime Monitoring ⓘ	Allowed. Turns on and runs the real-time monitoring service.
Allow Scanning Network Files ⓘ	Not configured
Allow Script Scanning ⓘ	Not configured
Allow User UI Access ⓘ	Not configured
Avg CPU Load Factor ⓘ	Not configured
Check For Signatures Before Running Scan ⓘ	Not configured

## 19 Click "Allowed. Scans network files."

ort

Allow scanning of all downloaded files and attachments ⓘ	Allowed. ▾
Allow Realtime Monitoring ⓘ	Allowed. Turns on and runs the real-time monitoring service. ▾
Allow Scanning Network Files ⓘ	Not configured ▾
Allow Script Scanning ⓘ	Not allowed. Turns off scanning of network files.
Allow User UI Access ⓘ	Allowed. Scans network files.
	Not configured
	Not configured ▾
Avg CPU Load Factor ⓘ	<input checked="" type="radio"/> Not configured
Check For Signatures Before Running Scan ⓘ	Not configured ▾
Cloud Block Level ⓘ	Not configured ▾

## 20 Click Allow script scanning

rt

and attachments ⓘ	
Allow Realtime Monitoring ⓘ	Allowed. Turns on and runs the real-time monitoring service. ▾
Allow Scanning Network Files ⓘ	Allowed. Scans network files. ▾
Allow Script Scanning ⓘ	Not configured ▾
Allow User UI Access ⓘ	Not allowed.
	Allowed.
	Not configured
Avg CPU Load Factor ⓘ	<input checked="" type="radio"/> Not configured
Check For Signatures Before Running Scan ⓘ	Not configured ▾
Cloud Block Level ⓘ	Not configured ▾
Cloud Extended Timeout ⓘ	<input checked="" type="radio"/> Not configured

## 21 Click "Allowed. Lets users access UI."

Allow Realtime Monitoring ⓘ Allowed. Turns on and runs the real-time monitoring service. ▼

Allow Scanning Network Files ⓘ Allowed. Scans network files. ▼

Allow Script Scanning ⓘ Allowed. ▼

Allow User UI Access ⓘ Not configured ▼

Avg CPU Load Factor ⓘ Not allowed. Prevents users from accessing UI. Allowed. Lets users access UI. Not configured

Check For Signatures Before Running Scan ⓘ Not configured

Cloud Block Level ⓘ Not configured ▼

Cloud Extended Timeout ⓘ ☐ Not configured

Days To Retain Cleaned Malware ⓘ ☐ Not configured

## 22 Enable Check for signatures before running scan

Allow User UI Access ⓘ Allowed. Lets users access UI. ▼

Avg CPU Load Factor ⓘ ☒ Configured

\* 50

Check For Signatures Before Running Scan ⓘ Not configured ▼

Cloud Block Level ⓘ Disabled Enabled Not configured

Cloud Extended Timeout ⓘ ☐ Not configured

Days To Retain Cleaned Malware ⓘ ☐ Not configured

Disable Catchup Full Scan ⓘ Not configured ▼

Disable Catchup Quick Scan ⓘ Not configured ▼

## 23 Set Cloud Block Level to High

A screenshot of the Windows Security application, specifically the 'Windows Defender Security Center' settings page. The 'Cloud Block Level' setting is highlighted with a yellow circle. The dropdown menu is open, showing the following options: 'Not configured', 'Default State', 'High', 'High Plus', 'Zero Tolerance', and 'Not configured'. The 'High' option is selected and highlighted in grey. Other settings visible include 'Avg CPU Load Factor' (50), 'Check For Signatures Before Running Scan' (Enabled), 'Cloud Extended Timeout' (Not configured), 'Days To Retain Cleaned Malware' (Not configured), 'Disable Catchup Full Scan' (Not configured), 'Disable Catchup Quick Scan' (Not configured), and 'Enable Low CPU Priority' (Not configured).

Setting	Value
Avg CPU Load Factor	50
Check For Signatures Before Running Scan	Enabled
Cloud Block Level	High
Cloud Extended Timeout	Not configured
Days To Retain Cleaned Malware	Not configured
Disable Catchup Full Scan	Not configured
Disable Catchup Quick Scan	Not configured
Enable Low CPU Priority	Not configured

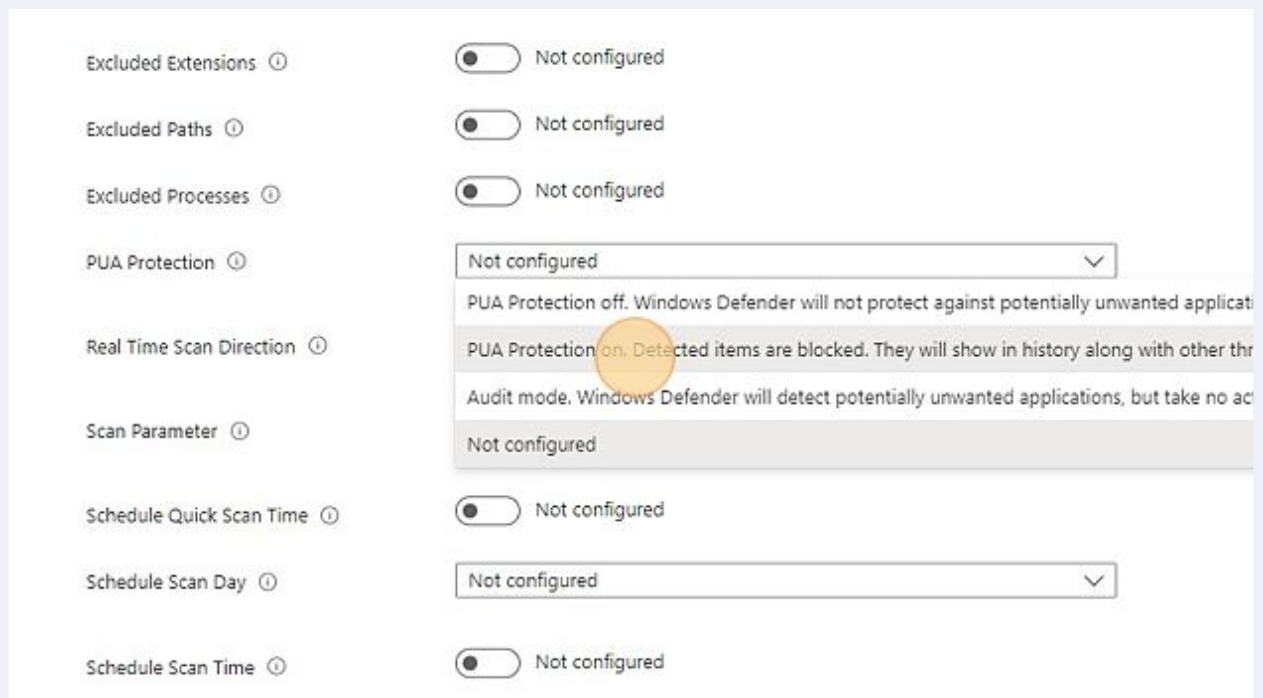
## 24 Enable Network Protection: Enabled (block mode)

A screenshot of the Windows Security application, specifically the 'Windows Defender Security Center' settings page. The 'Enable Network Protection' setting is highlighted with a yellow circle. The dropdown menu is open, showing the following options: 'Not configured', 'Disabled', 'Enabled (block mode)', 'Enabled (audit mode)', and 'Not configured'. The 'Enabled (block mode)' option is selected and highlighted in grey. Other settings visible include 'Days To Retain Cleaned Malware' (Not configured), 'Disable Catchup Full Scan' (Not configured), 'Disable Catchup Quick Scan' (Not configured), 'Enable Low CPU Priority' (Not configured), 'Excluded Extensions' (Not configured), 'Excluded Paths' (Not configured), 'Excluded Processes' (Not configured), 'PUA Protection' (Not configured), 'Real Time Scan Direction' (Not configured), 'Scan Parameter' (Not configured), and 'Schedule Quick Scan Time' (Not configured).

Setting	Value
Days To Retain Cleaned Malware	Not configured
Disable Catchup Full Scan	Not configured
Disable Catchup Quick Scan	Not configured
Enable Low CPU Priority	Not configured
Enable Network Protection	Enabled (block mode)
Excluded Extensions	Not configured
Excluded Paths	Not configured
Excluded Processes	Not configured
PUA Protection	Not configured
Real Time Scan Direction	Not configured
Scan Parameter	Not configured
Schedule Quick Scan Time	Not configured

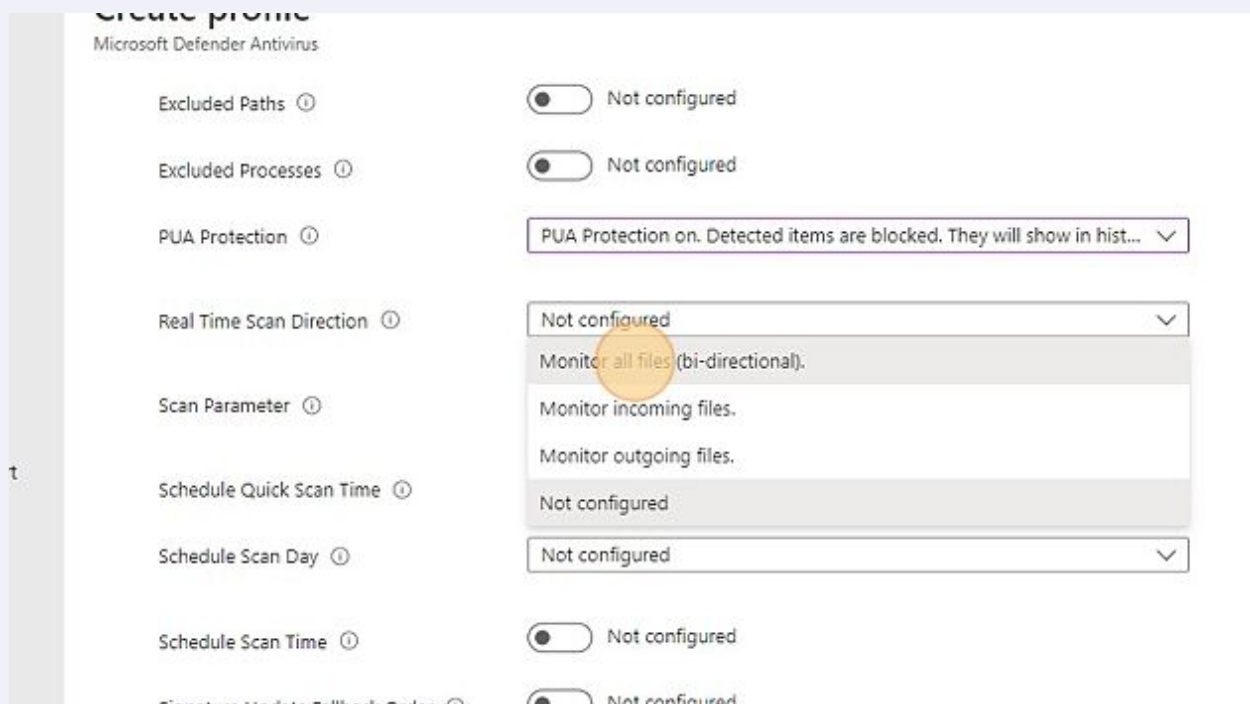
25

Click "PUA Protection on. Detected items are blocked. They will show in history along with other threats."



26

Click "Monitor all files (bi-directional)."



## 27 Set Signature update interval to 1 hour

Support

Schedule Scan Day ⓘ Every day ▼

Schedule Scan Time ⓘ ☐ Not configured

Signature Update Fallback Order ⓘ ☐ Not configured

Signature Update File Shares Sources ⓘ ☐ Not configured

Signature Update Interval ⓘ ☒ Configured

\*  ▼

Submit Samples Consent ⓘ Not configured ▼

Disable Local Admin Merge ⓘ Not configured ▼

Allow On Access Protection ⓘ Not configured ▼

Remediation action for Severe threats ⓘ Not configured ▼

## 28 Click "Send all samples automatically."

Signature Update Interval ⓘ ☒ Configured

\*  ▼

Submit Samples Consent ⓘ Not configured ▼

Disable Local Admin Merge ⓘ Not configured ▼

Allow On Access Protection ⓘ Not configured ▼

Remediation action for Severe threats ⓘ Not configured ▼

Remediation action for Moderate severity threats ⓘ Not configured ▼

Previous Next

## 29 Click "Disable Local Admin Merge"

Signature Update Interval ⓘ ☒ Configured

\*  ✓

Submit Samples Consent ⓘ  ▼

Disable Local Admin Merge ⓘ  ▼

Allow On Access Protection ⓘ  ▼

Remediation action for Severe threats  ▼

Remediation action for Moderate severity threats  ▼

Remediation action for Low severity threats  ▼

## 30 Allow on access protection

\*  ✓

Submit Samples Consent ⓘ  ▼

Disable Local Admin Merge ⓘ  ▼

Allow On Access Protection ⓘ  ▼

Remediation action for Severe threats  ▼

Remediation action for Moderate severity threats  ▼

Remediation action for Low severity threats  ▼

Remediation action for High severity threats  ▼



31

Set "Remediation action for Severe threats" to "Remove. Removes files from system."

The screenshot shows the Windows Security settings window. The 'Remediation action for Severe threats' dropdown menu is open, displaying the following options: 'Block. Blocks file execution.', 'Clean. Service tries to recover files and try to disinfect.', 'Quarantine. Moves files to quarantine.', 'Remove. Removes files from system.' (highlighted with an orange circle), 'Allow. Allows file/does none of the above actions.', 'User defined. Requires user to make a decision on which action to take.', and 'Block. Blocks file execution.'.

32

Set "Remediation action for High severity threats" to "Block. Blocks file execution."

The screenshot shows the Windows Security settings window. The 'Remediation action for High severity threats' dropdown menu is open, displaying the following options: 'Remove. Removes files from system.', 'Clean. Service tries to recover files and try to disinfect.', 'Quarantine. Moves files to quarantine.', 'Remove. Removes files from system.', 'Allow. Allows file/does none of the above actions.', 'User defined. Requires user to make a decision on which action to take.', and 'Block. Blocks file execution.' (highlighted with an orange circle). The 'Previous' and 'Next' buttons are visible at the bottom.



33

Set "Remediation action for Moderate severity threats" to "Quarantine. Moves files to quarantine."

The screenshot shows the Windows Security Settings window. The 'Remediation action for Moderate severity threats' dropdown menu is open, displaying the following options: 'Clean. Service tries to recover files and try to disinfect.', 'Quarantine. Moves files to quarantine.', 'Remove. Removes files from system.', 'Allow. Allows file/does none of the above actions.', 'User defined. Requires user to make a decision on which action to take.', and 'Block. Blocks file execution.' The 'Quarantine. Moves files to quarantine.' option is highlighted with a yellow circle. The other settings are: 'Disable Local Admin Merge' (set to 'Disable Local Admin Merge'), 'Allow On Access Protection' (set to 'Allowed'), 'Remediation action for Severe threats' (set to 'Remove. Removes files from system.'), 'Remediation action for Low severity threats' (set to 'Remove. Removes files from system.'), and 'Remediation action for High severity threats' (set to 'User defined. Requires user to make a decision on which action to take.'). The 'Previous' and 'Next' buttons are at the bottom.

Disable Local Admin Merge ① Disable Local Admin Merge ▼

Allow On Access Protection ① Allowed. ▼

Remediation action for Severe threats Remove. Removes files from system. ▼

Remediation action for Moderate severity threats Clean. Service tries to recover files and try to disinfect. ▼  
Quarantine. Moves files to quarantine.  
Remove. Removes files from system.  
Allow. Allows file/does none of the above actions.  
User defined. Requires user to make a decision on which action to take.  
Block. Blocks file execution.

Remediation action for Low severity threats Remove. Removes files from system. ▼

Remediation action for High severity threats User defined. Requires user to make a decision on which action to take. ▼

Previous Next

34

Set "Remediation action for Low severity threats" to "User defined. Requires user to make a decision on which action to take."

The screenshot shows the Windows Security Settings window. The 'Remediation action for Low severity threats' dropdown menu is open, displaying the following options: 'Clean. Service tries to recover files and try to disinfect.', 'Quarantine. Moves files to quarantine.', 'Remove. Removes files from system.', 'Allow. Allows file/does none of the above actions.', 'User defined. Requires user to make a decision on which action to take.', and 'Block. Blocks file execution.' The 'User defined. Requires user to make a decision on which action to take.' option is highlighted with a yellow circle. The other settings are: 'Allow On Access Protection' (set to 'Allowed'), 'Remediation action for Severe threats' (set to 'Remove. Removes files from system.'), 'Remediation action for Moderate severity threats' (set to 'Quarantine. Moves files to quarantine.'), and 'Remediation action for High severity threats' (set to 'User defined. Requires user to make a decision on which action to take.'). The 'Previous' and 'Next' buttons are at the bottom.

Allow On Access Protection ① Allowed. ▼

Remediation action for Severe threats Remove. Removes files from system. ▼

Remediation action for Moderate severity threats Quarantine. Moves files to quarantine. ▼

Remediation action for Low severity threats Clean. Service tries to recover files and try to disinfect. ▼  
Quarantine. Moves files to quarantine.  
Remove. Removes files from system.  
Allow. Allows file/does none of the above actions.  
User defined. Requires user to make a decision on which action to take.  
Block. Blocks file execution.

Remediation action for High severity threats User defined. Requires user to make a decision on which action to take. ▼

Previous Next

### 35 Click "Next"

Allow On Access Protection ⓘ Allowed.

Remediation action for Severe threats Remove. Removes files from system.

Remediation action for Moderate severity threats Quarantine. Moves files to quarantine.

Remediation action for Low severity threats User defined. Requires user to make a decision on

Remediation action for High severity threats Block. Blocks file execution.

Previous Next

### 36 Assign the profile to your security group

Microsoft Intune admin center

Home > Endpoint security | Antivirus >

## Create profile ...

Microsoft Defender Antivirus

✓ Basics ✓ Configuration settings ✓ Scope tags 4 Assignments 5 Review

Included groups

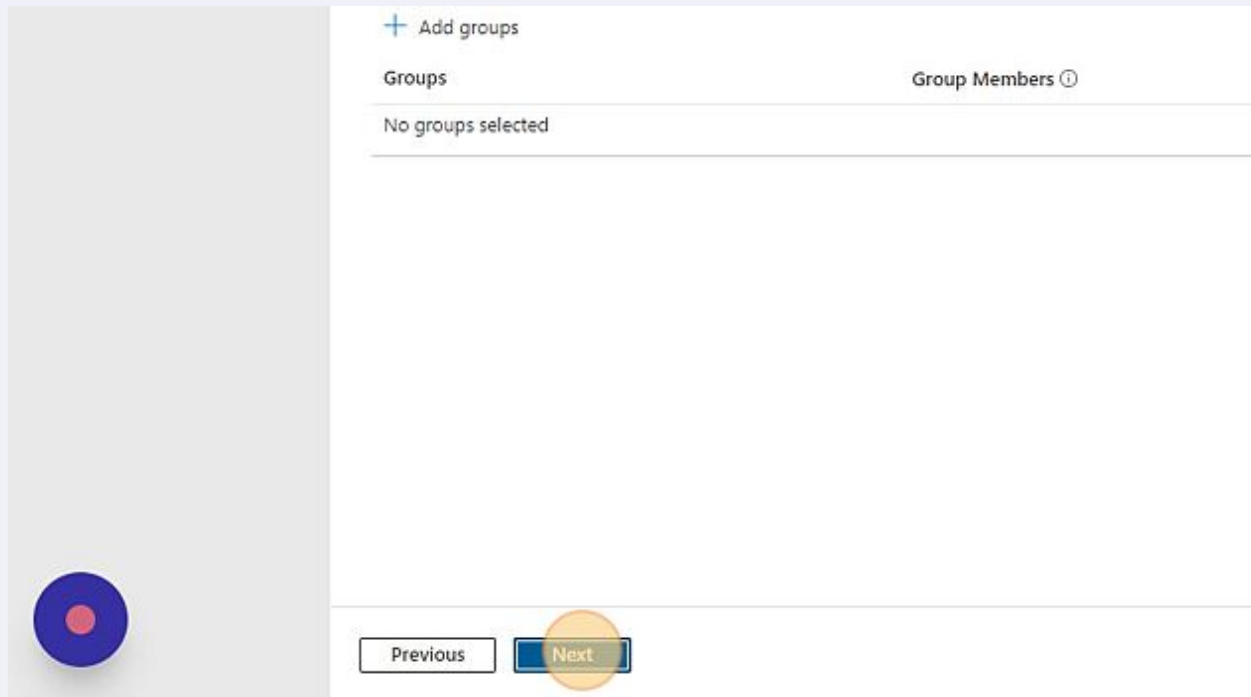
+ Add groups + Add all users + Add all devices

Groups	Group Members ⓘ	Filter
No groups selected		

Excluded groups

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

### 37 Click "Next"



### 38 Review your settings and click "Create"

