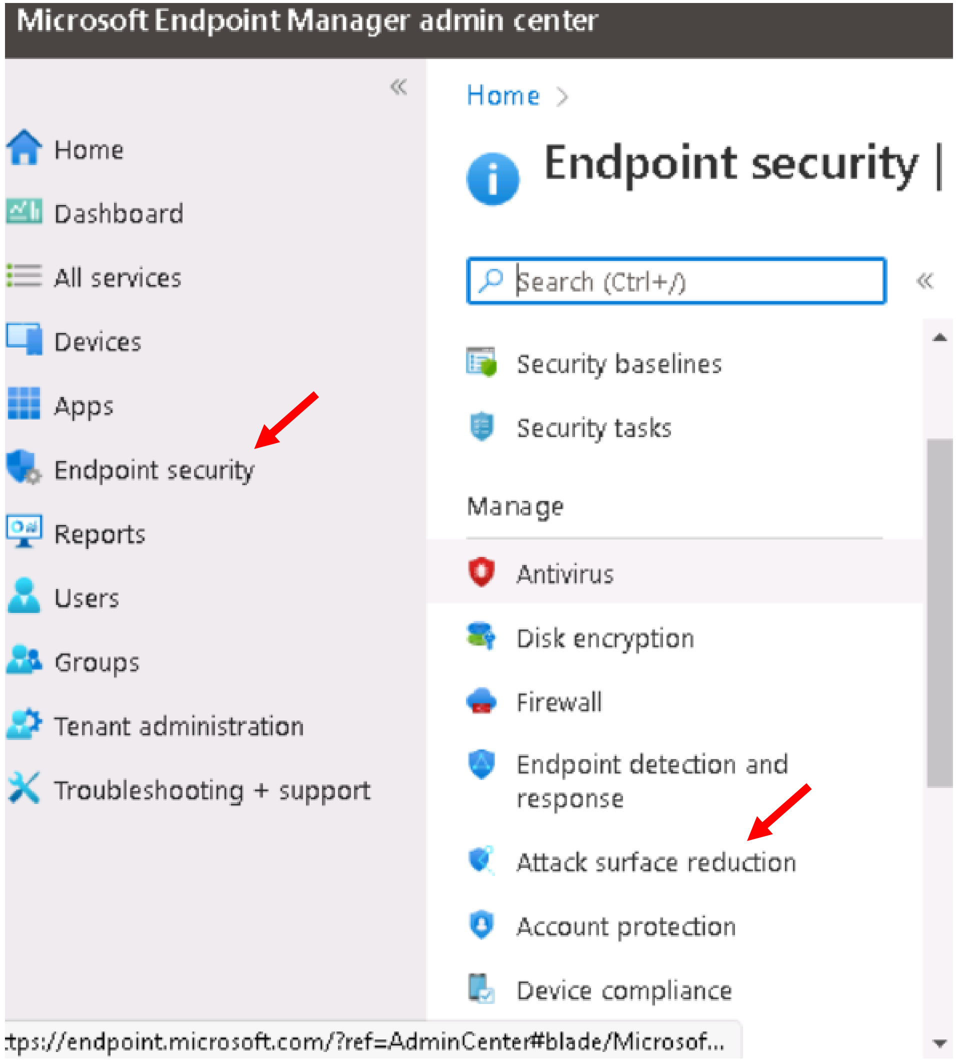
Device and Application protection

Application Guard, Application control, Exploit protection, windows device encryption, non-windows device encryption



Microsoft Endpoint Manager admin center

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

Home >

Endpoint security |

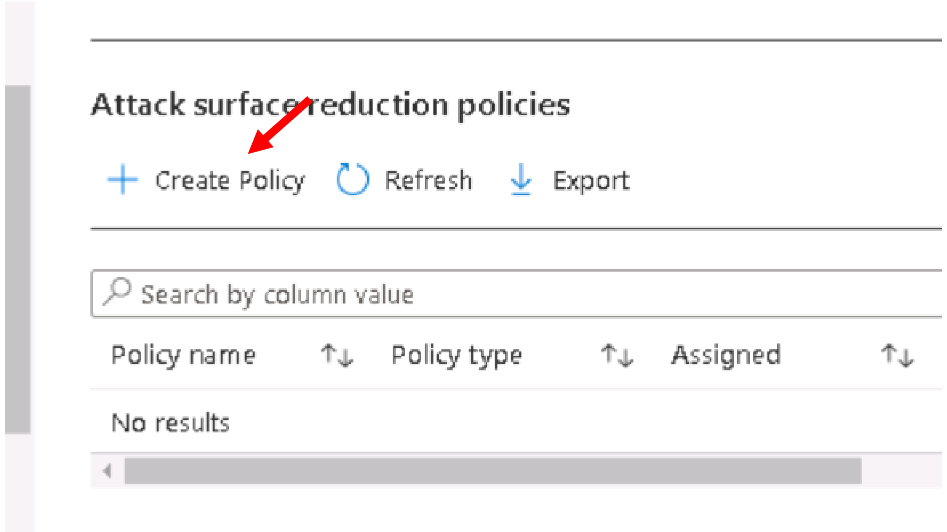
Search (Ctrl+/)

- Security baselines
- Security tasks

Manage

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

tps://endpoint.microsoft.com/?ref=AdminCenter#blade/Microsof...

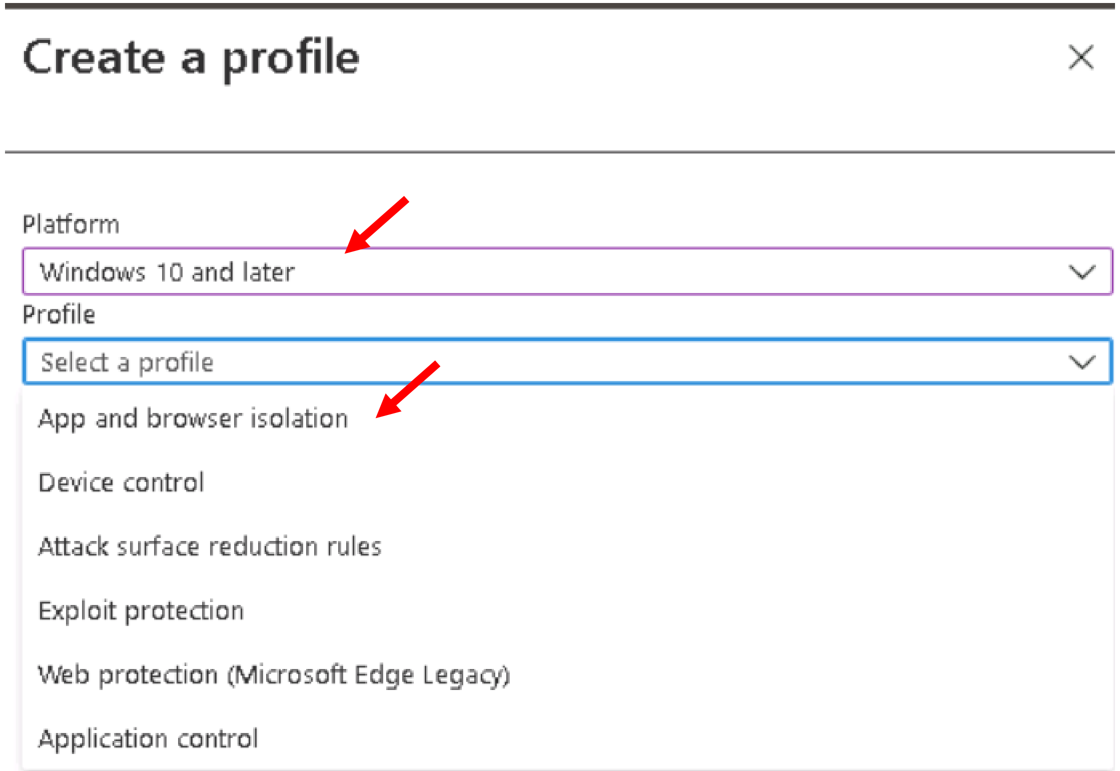


Attack surface reduction policies

+ Create Policy　Refresh　Export

Search by column value

Policy name ↑↓	Policy type ↑↓	Assigned ↑↓
No results		

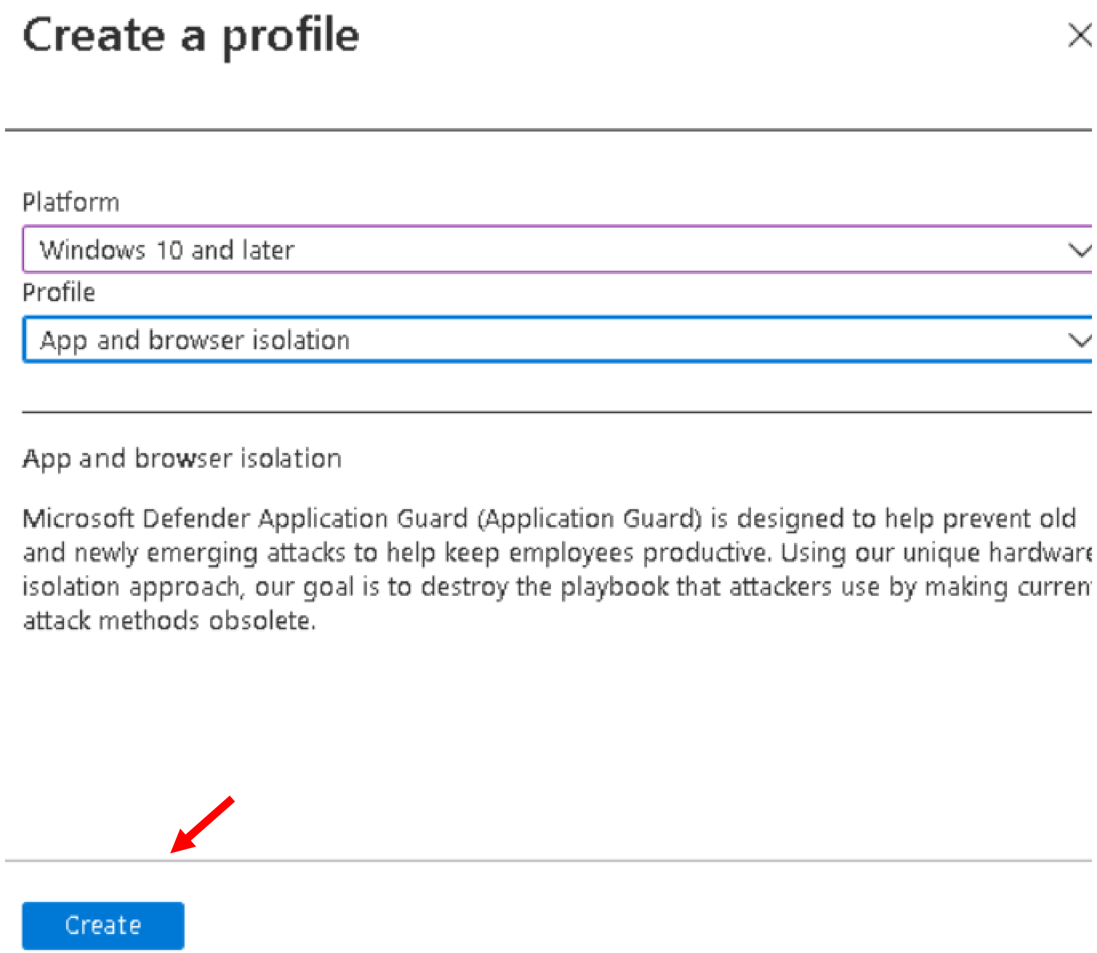


Create a profile

Platform: Windows 10 and later

Profile: Select a profile

App and browser isolation
Device control
Attack surface reduction rules
Exploit protection
Web protection (Microsoft Edge Legacy)
Application control



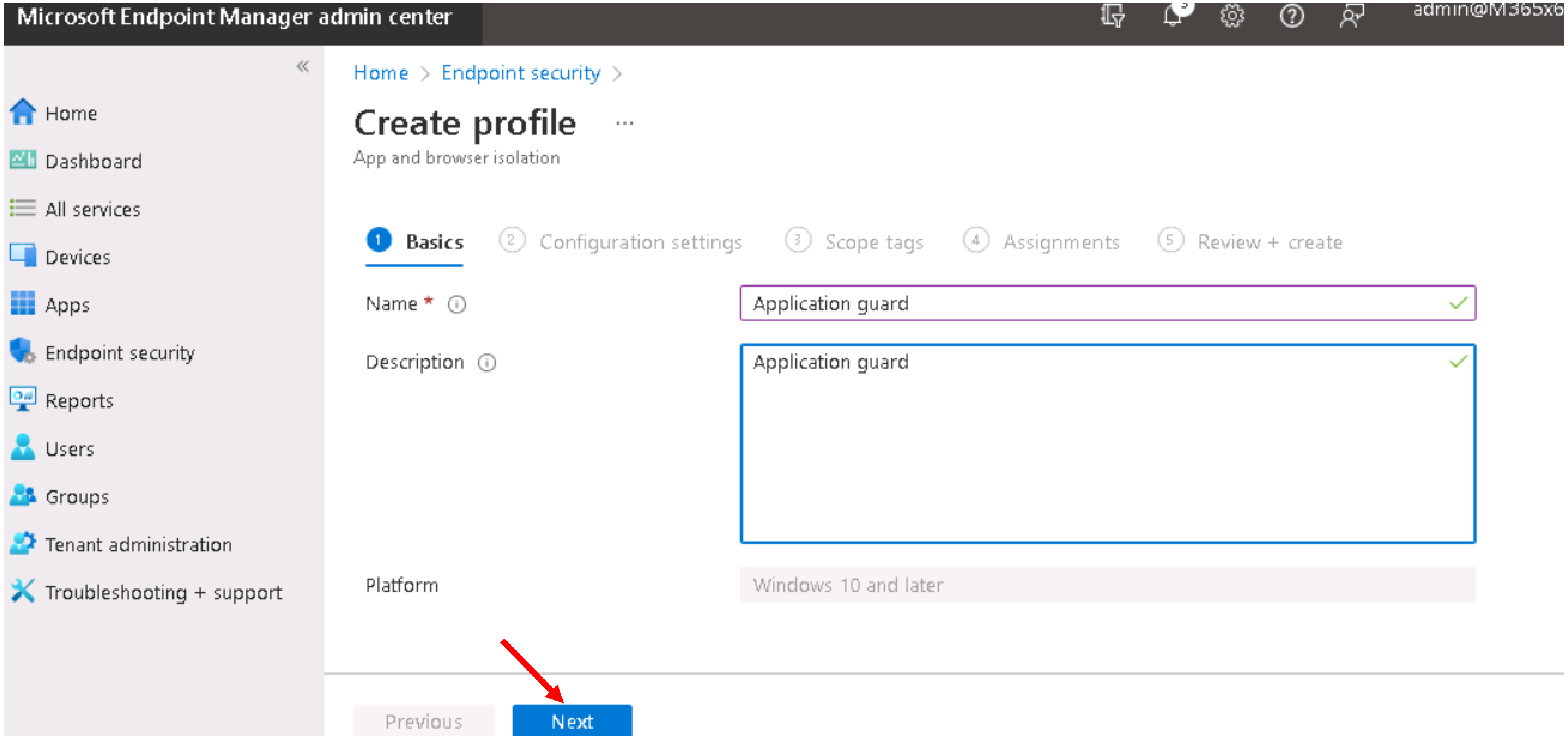
Create a profile

Platform: Windows 10 and later

Profile: App and browser isolation

App and browser isolation

Microsoft Defender Application Guard (Application Guard) is designed to help prevent old and newly emerging attacks to help keep employees productive. Using our unique hardware isolation approach, our goal is to destroy the playbook that attackers use by making curren attack methods obsolete.



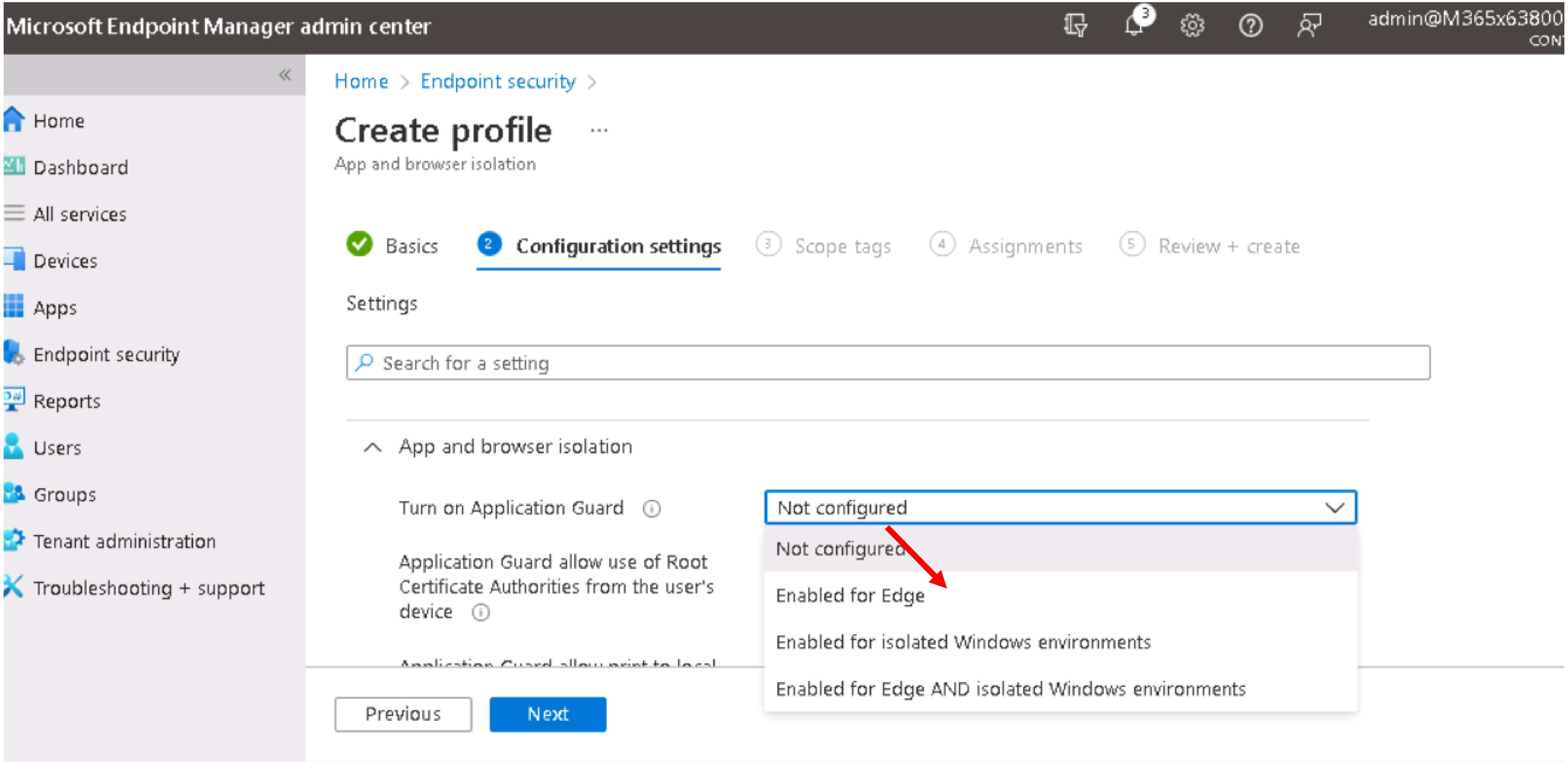
Create profile ...

App and browser isolation

Name * : Application guard

Description : Application guard

Platform : Windows 10 and later



Create profile ...

App and browser isolation

Settings

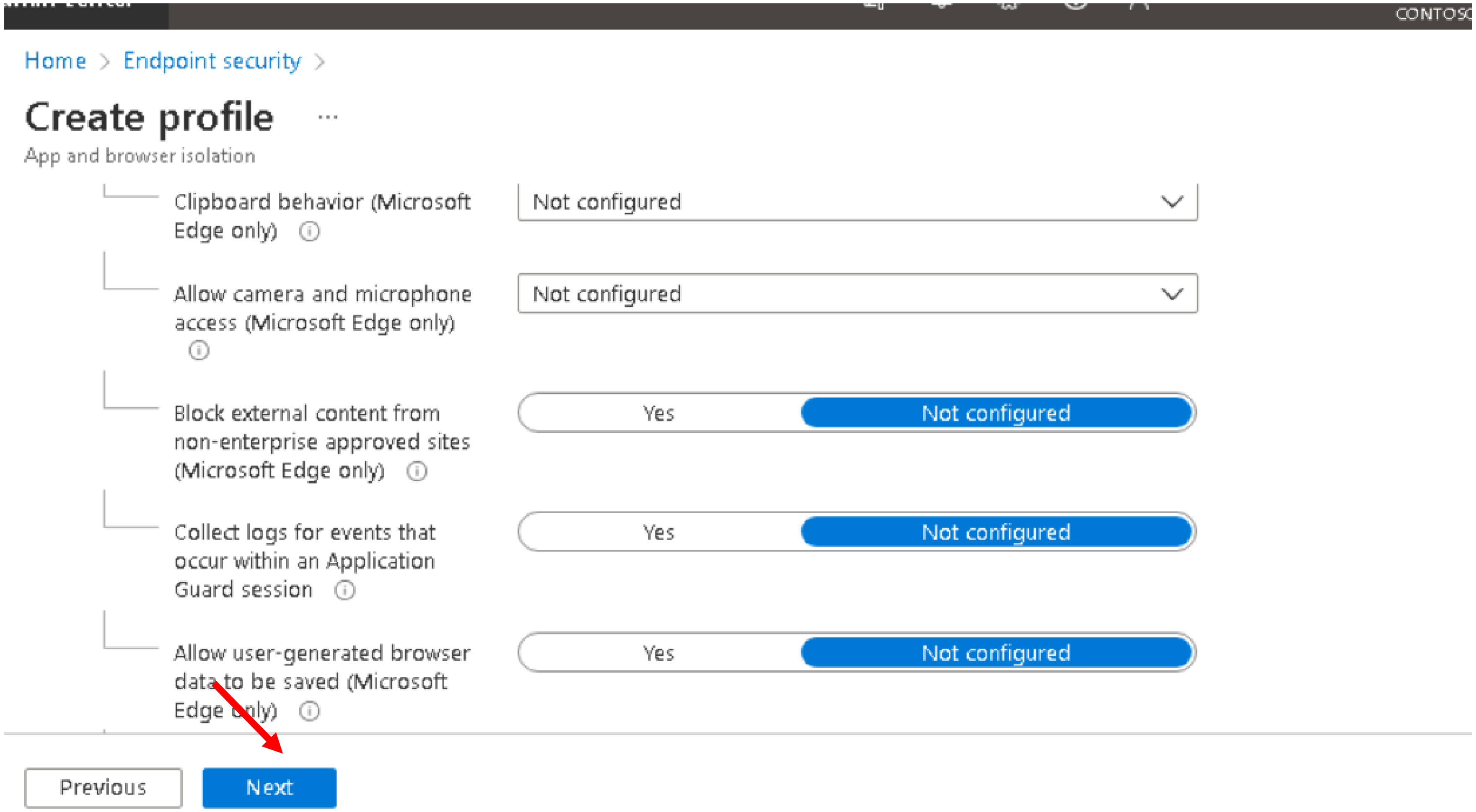
App and browser isolation

Turn on Application Guard ⓘ — Not configured

- Not configured
- Enabled for Edge
- Enabled for isolated Windows environments
- Enabled for Edge AND isolated Windows environments

Application Guard allow use of Root Certificate Authorities from the user's device ⓘ

Application Guard allow print to local

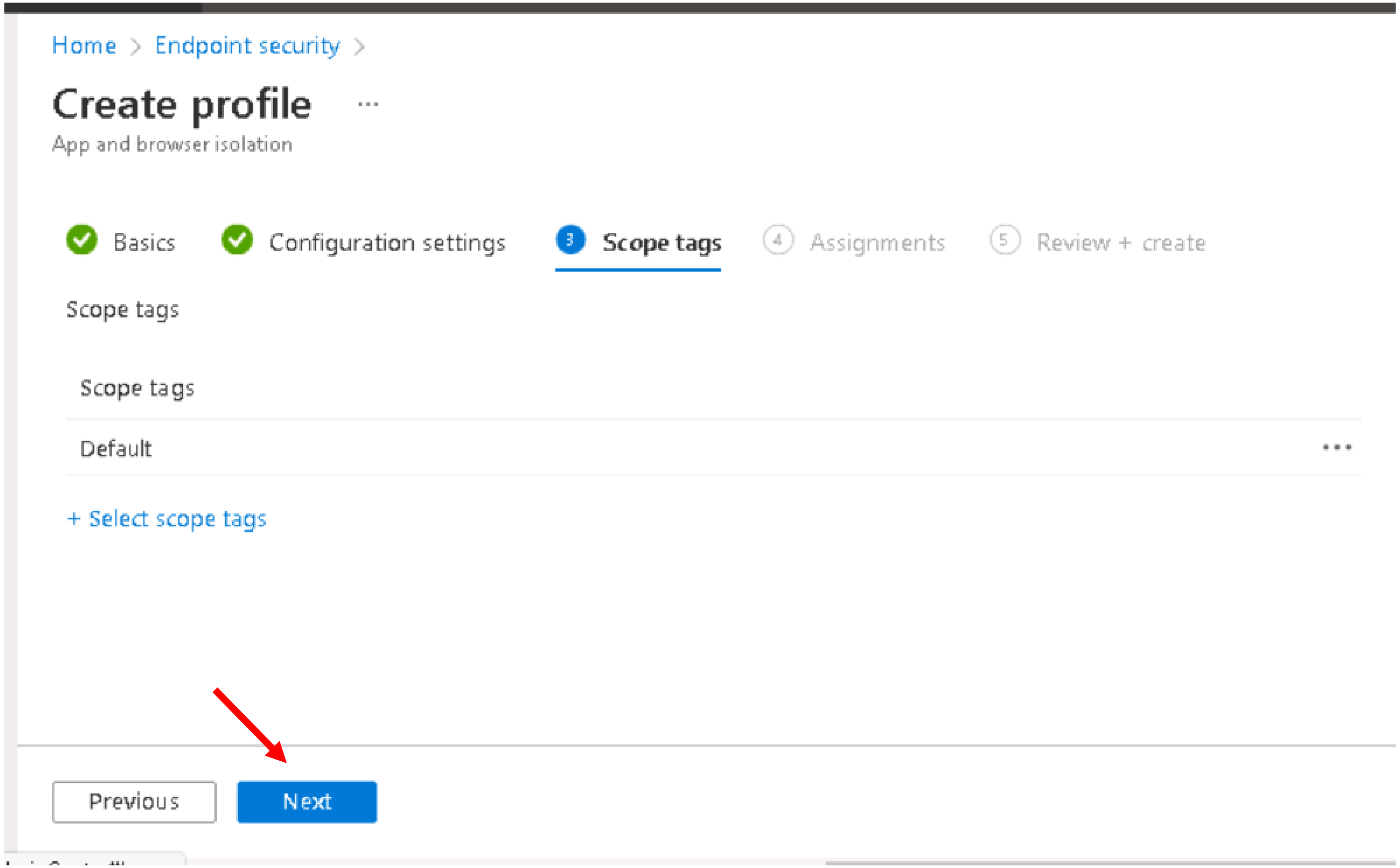


Create profile

App and browser isolation

- Clipboard behavior (Microsoft Edge only): Not configured
- Allow camera and microphone access (Microsoft Edge only): Not configured
- Block external content from non-enterprise approved sites (Microsoft Edge only): Yes [✓ Not configured]
- Collect logs for events that occur within an Application Guard session: Yes [✓ Not configured]
- Allow user-generated browser data to be saved (Microsoft Edge only): Yes [✓ Not configured]

Scroll down and look at all the options



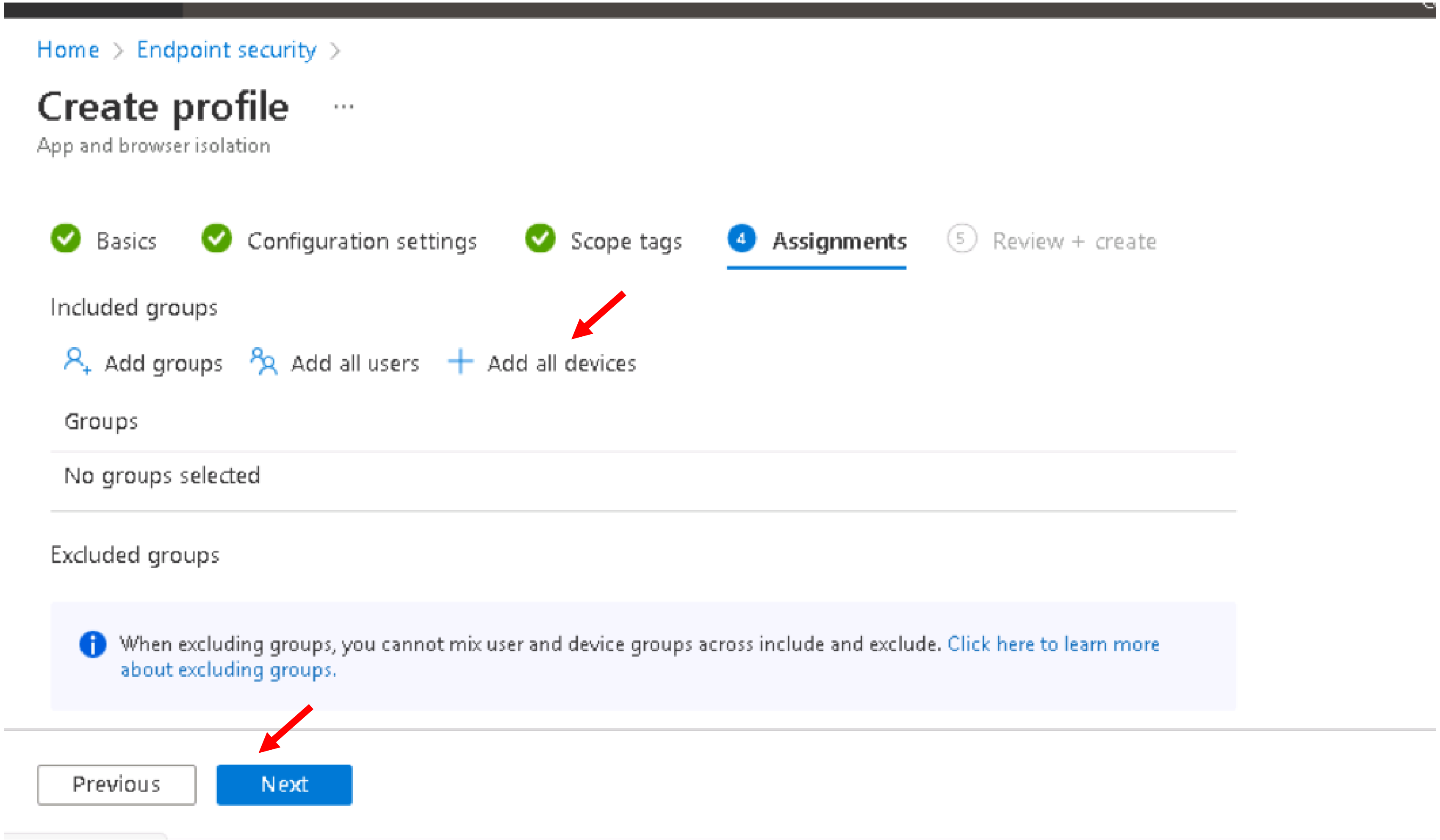
Create profile ...

App and browser isolation

Scope tags

Scope tags
Default

+ Select scope tags



Home > Endpoint security >

Create profile ...

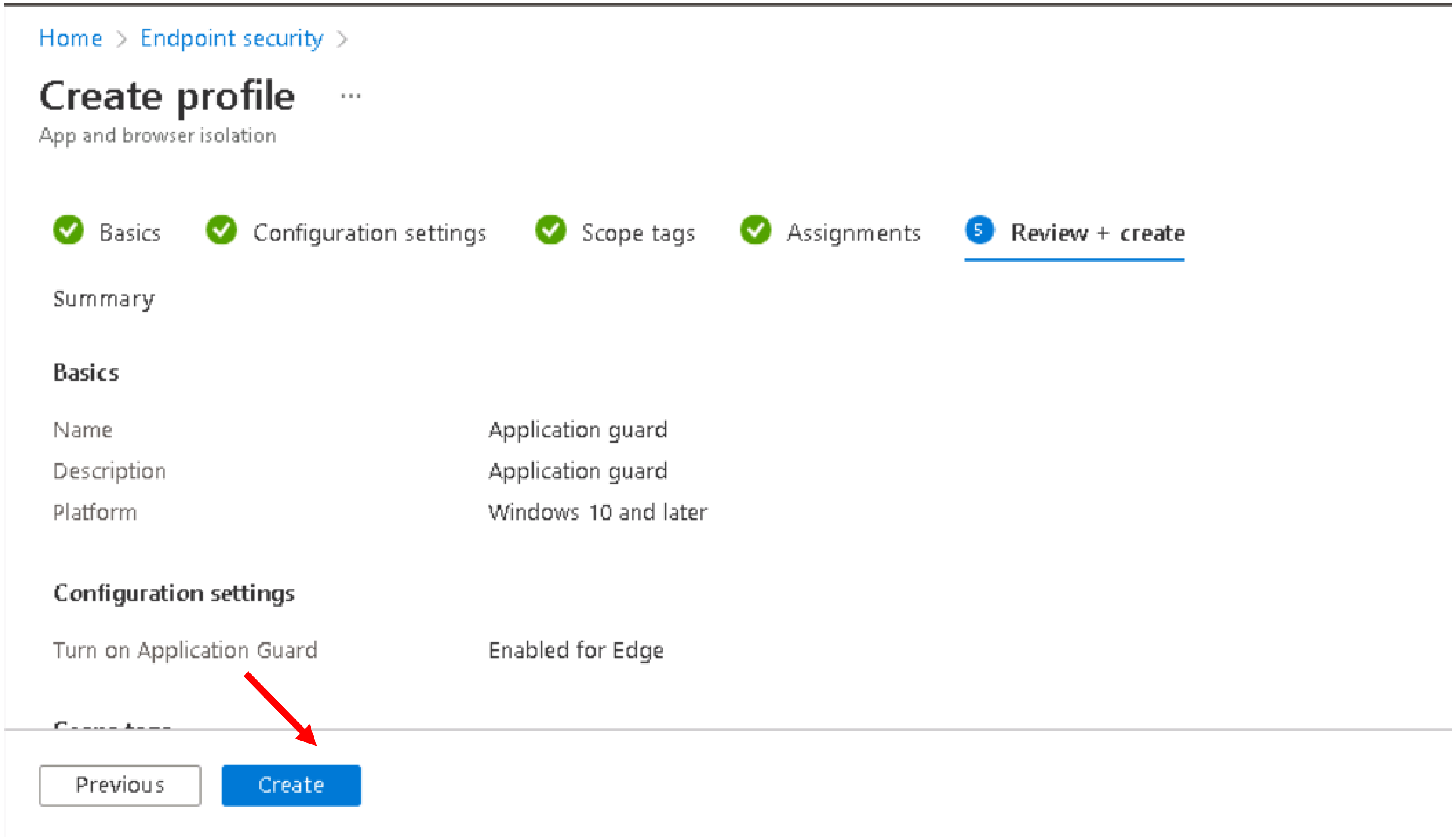
App and browser isolation

Included groups

Groups
No groups selected

Excluded groups

When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about excluding groups.



Create profile

App and browser isolation

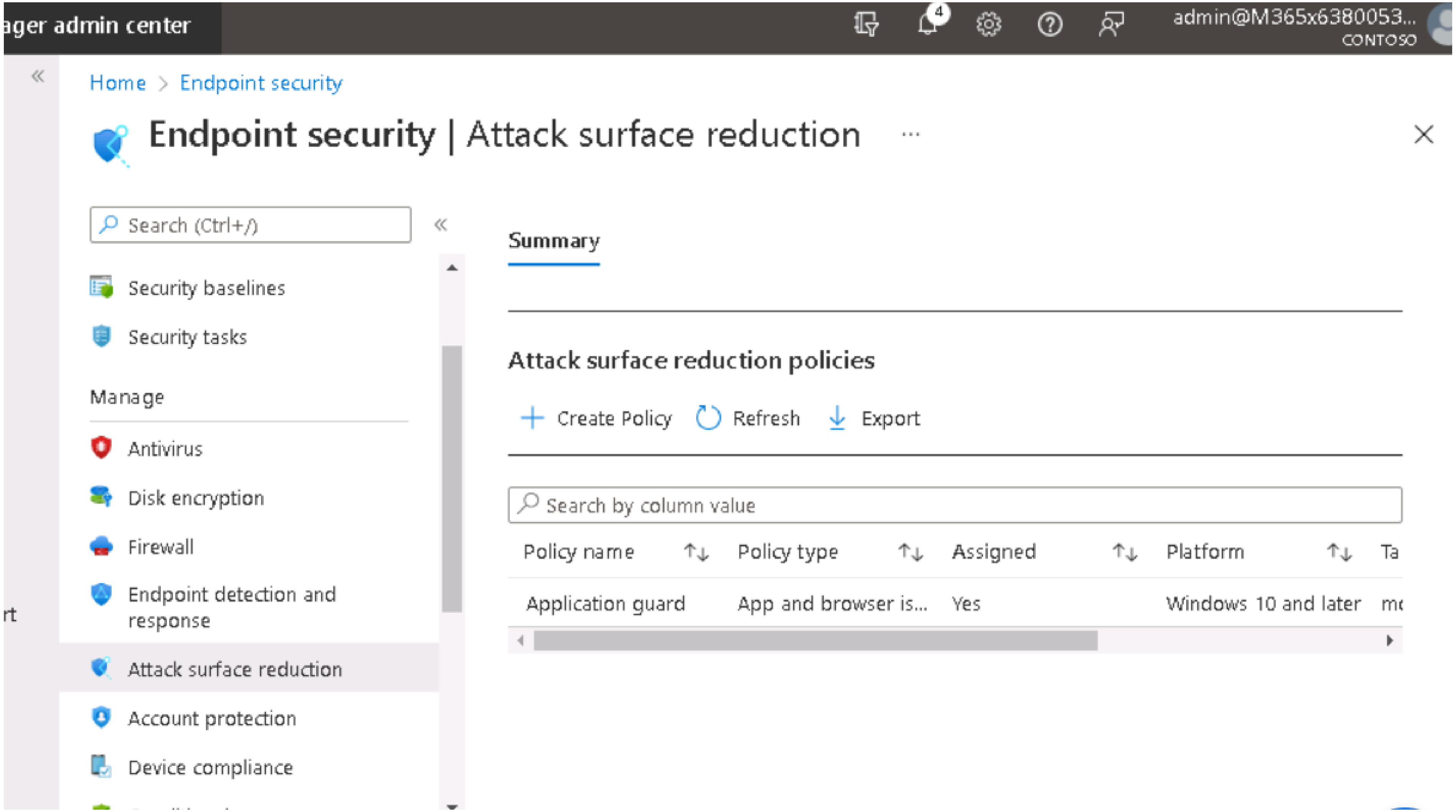
Summary

Basics

Name	Application guard
Description	Application guard
Platform	Windows 10 and later

Configuration settings

Turn on Application Guard	Enabled for Edge

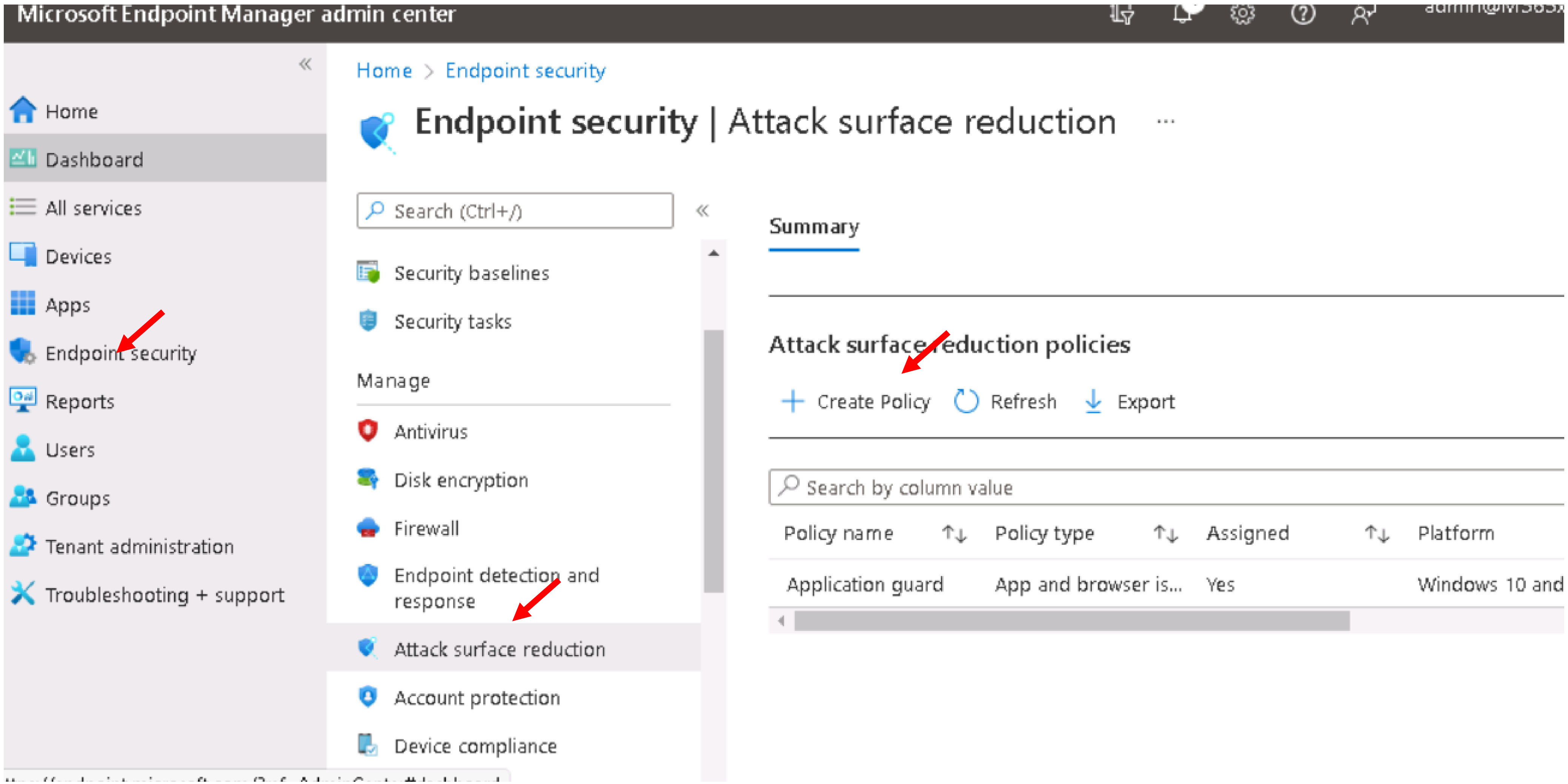


Endpoint security | Attack surface reduction

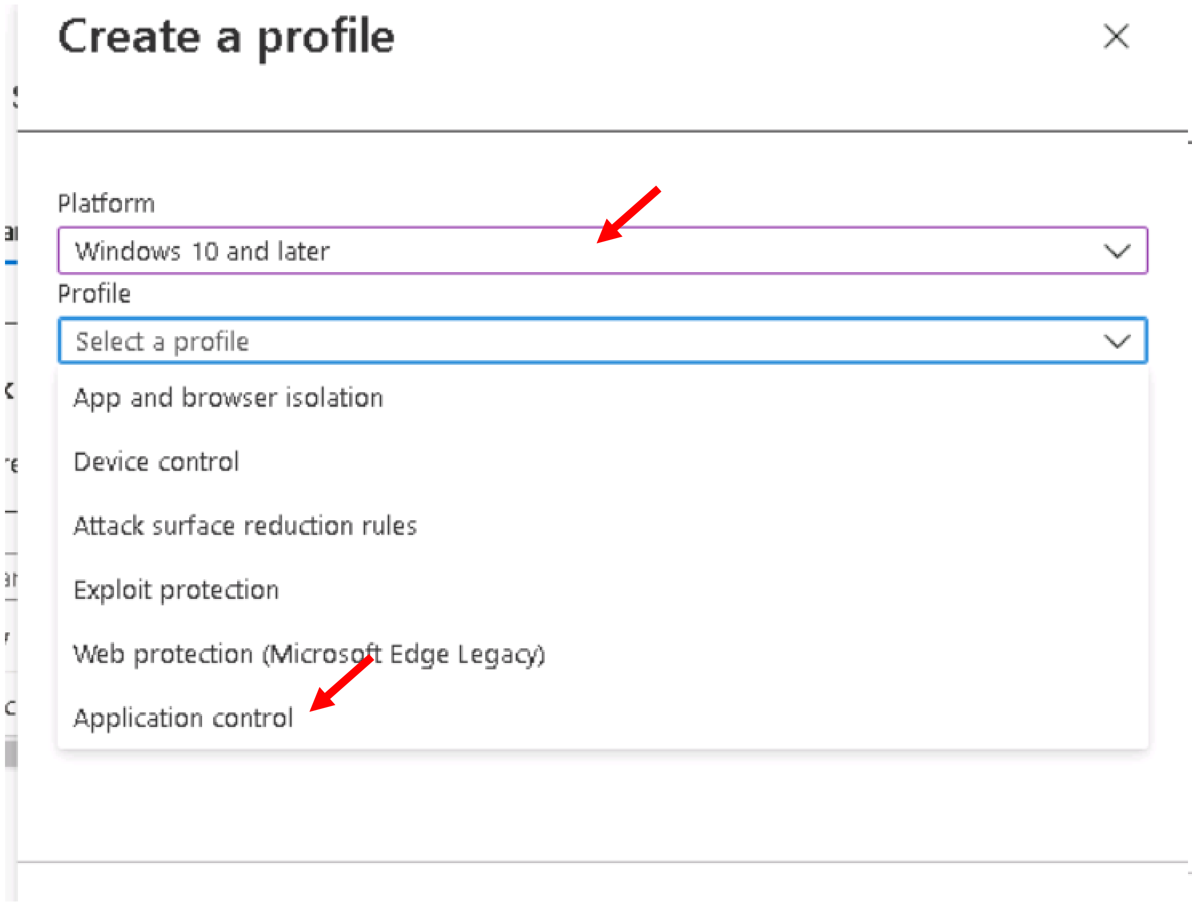
Attack surface reduction policies

Policy name	Policy type	Assigned	Platform	Ta
Application guard	App and browser is...	Yes	Windows 10 and later	m

Application control



Policy name	Policy type	Assigned	Platform
Application guard	App and browser is...	Yes	Windows 10 and



Create a profile

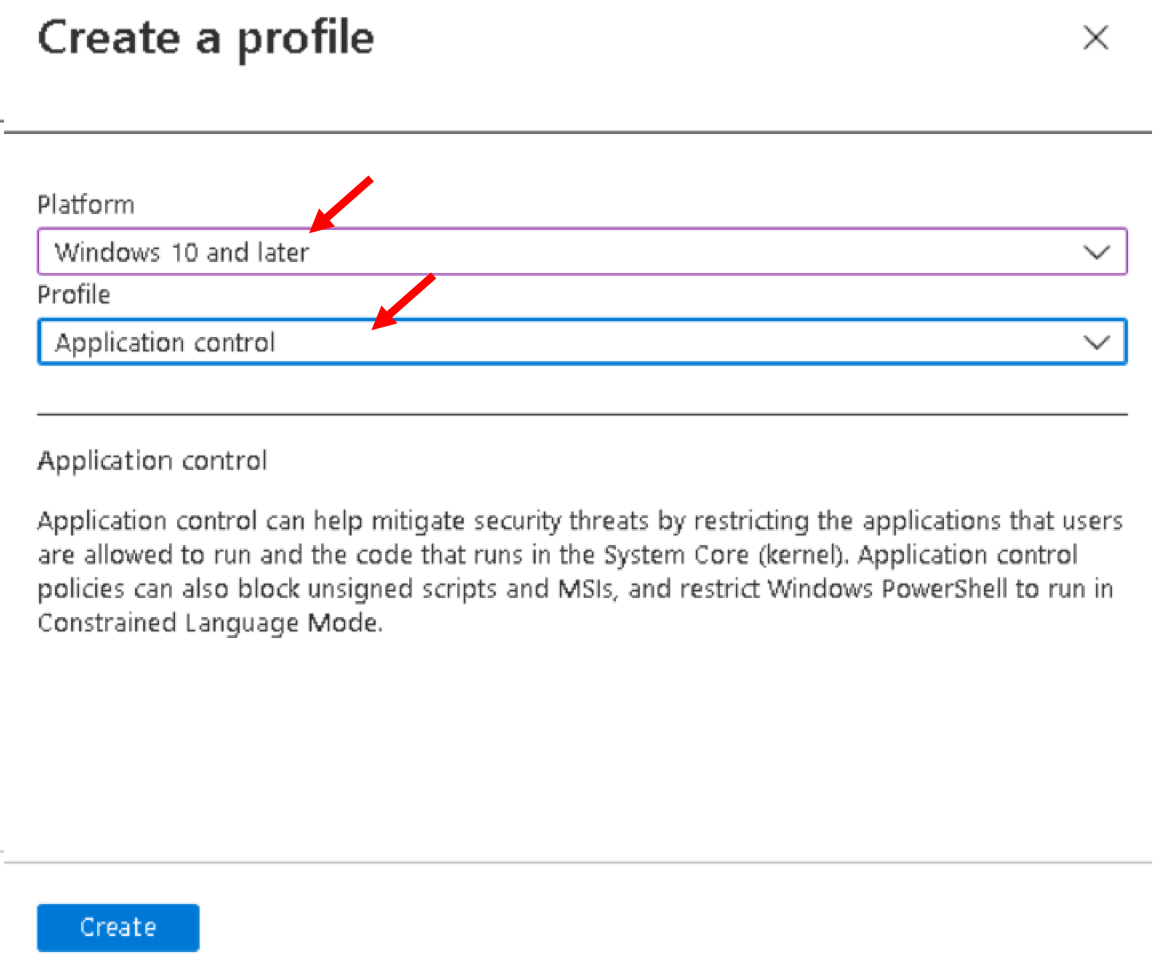
Platform

Windows 10 and later

Profile

Select a profile

- App and browser isolation
- Device control
- Attack surface reduction rules
- Exploit protection
- Web protection (Microsoft Edge Legacy)
- Application control



Create a profile

Platform

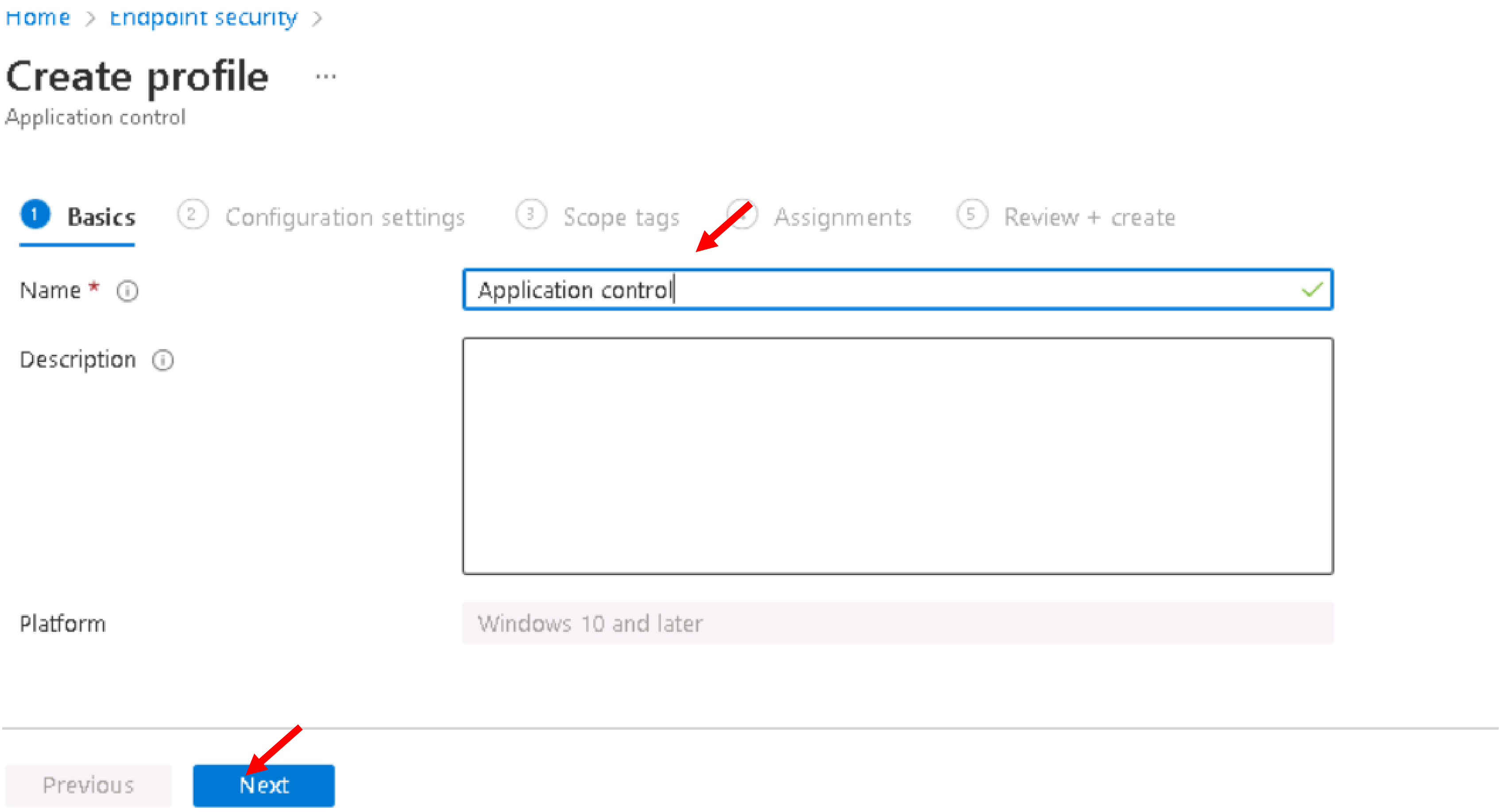
Windows 10 and later

Profile

Application control

Application control

Application control can help mitigate security threats by restricting the applications that users are allowed to run and the code that runs in the System Core (kernel). Application control policies can also block unsigned scripts and MSIs, and restrict Windows PowerShell to run in Constrained Language Mode.



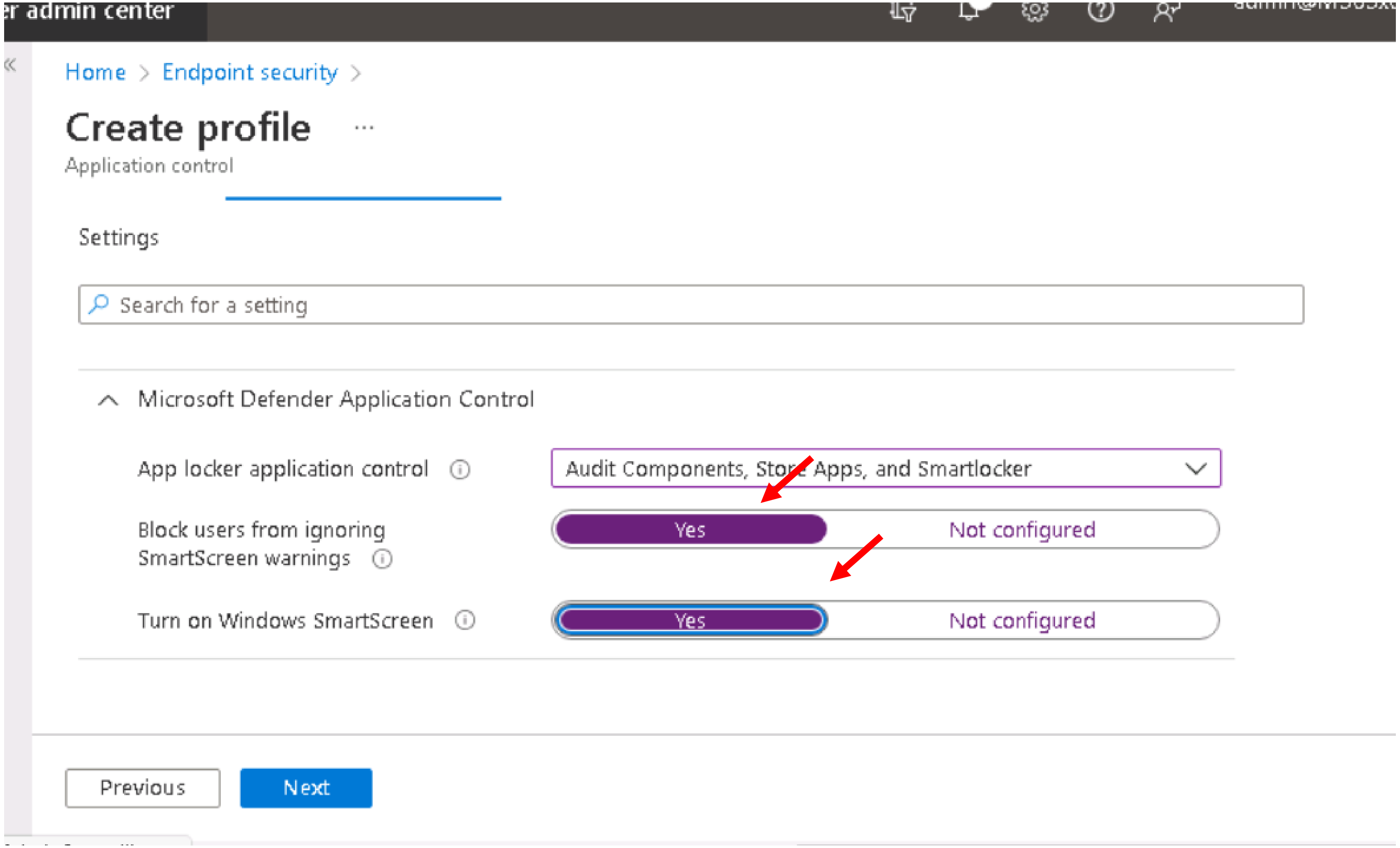
Create profile ...

Application control

Name * ⓘ Application control ✓

Description ⓘ

Platform Windows 10 and later



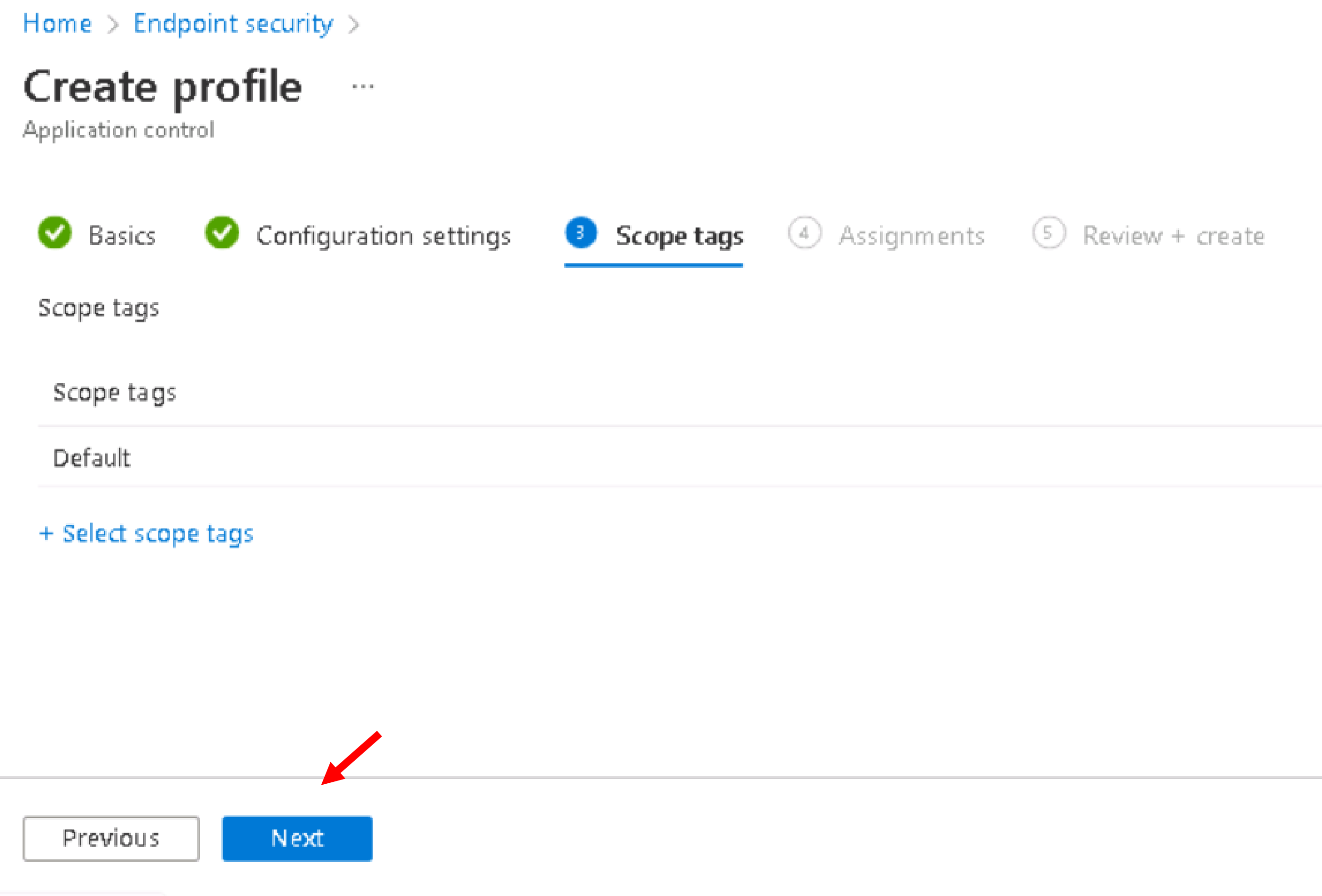
Create profile

Application control

Settings

Microsoft Defender Application Control

App locker application control	Audit Components, Store Apps, and Smartlocker
Block users from ignoring SmartScreen warnings	[✓ Yes] Not configured
Turn on Windows SmartScreen	[✓ Yes] Not configured



Home > Endpoint security >

Create profile ...

Application control

✓ Basics ✓ Configuration settings ③ Scope tags ④ Assignments ⑤ Review + create

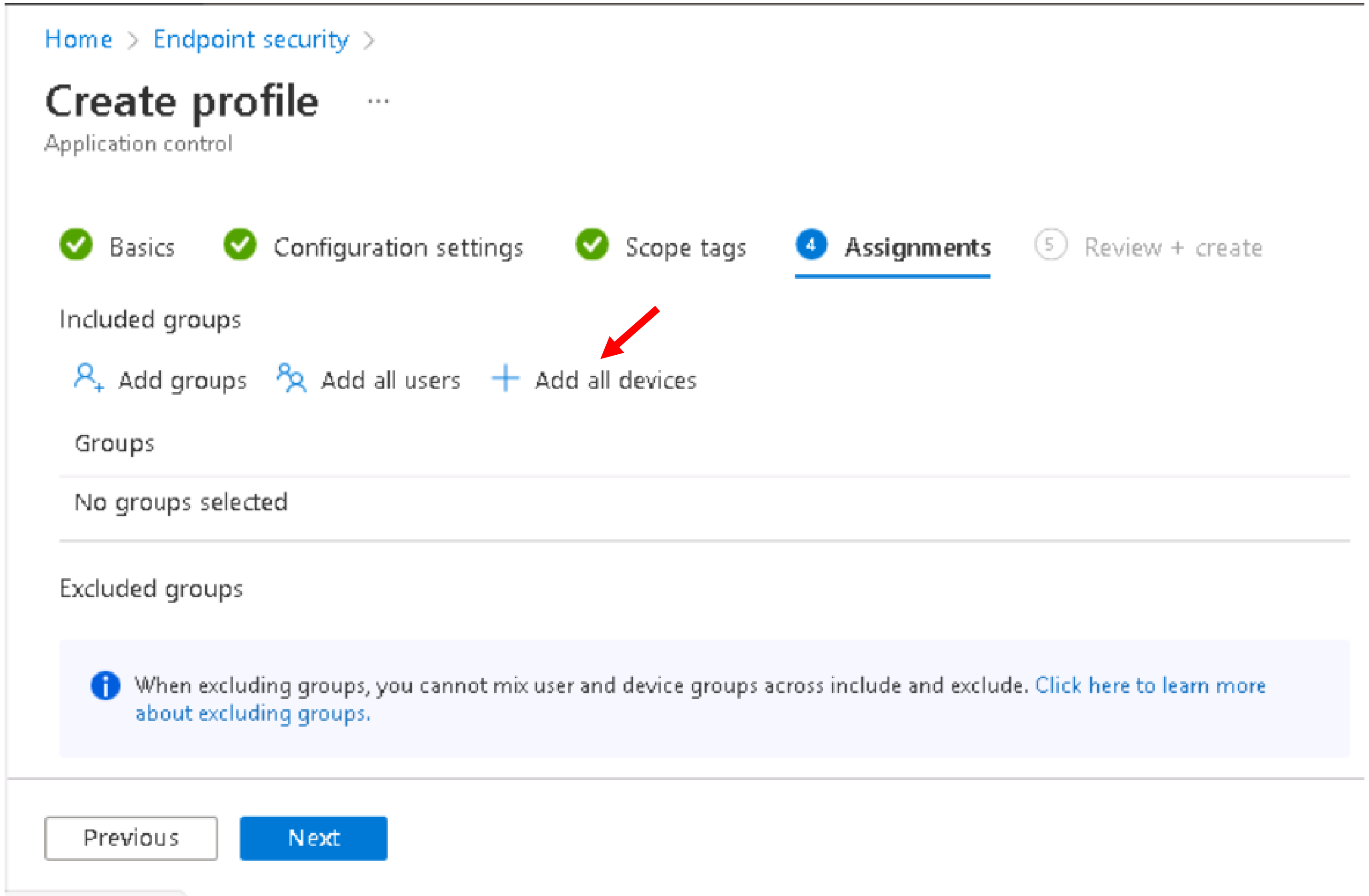
Scope tags

Scope tags

Default

+ Select scope tags

Previous Next



Create profile ...

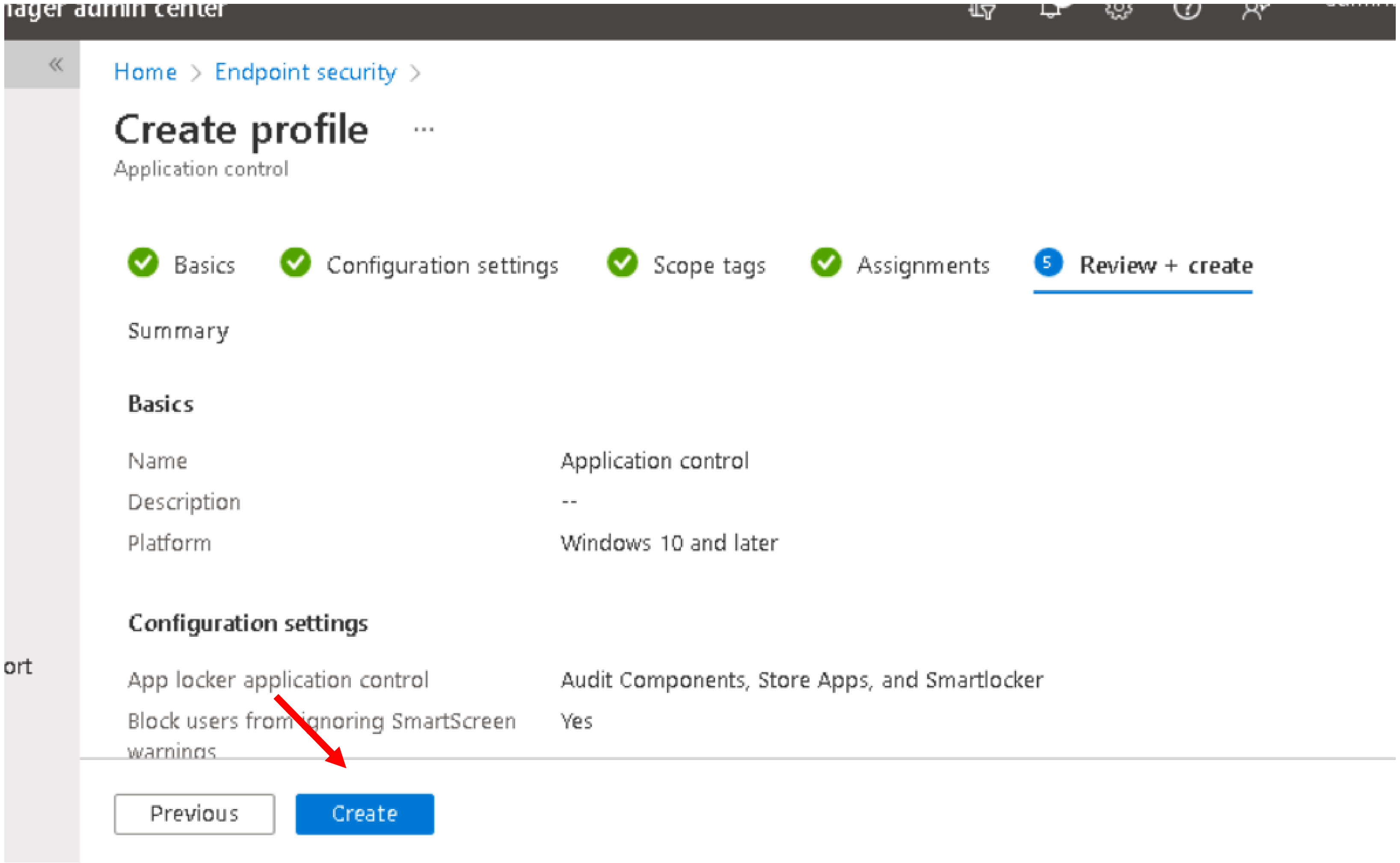
Application control

Included groups

Groups
No groups selected

Excluded groups

When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about excluding groups.



Create profile

Application control

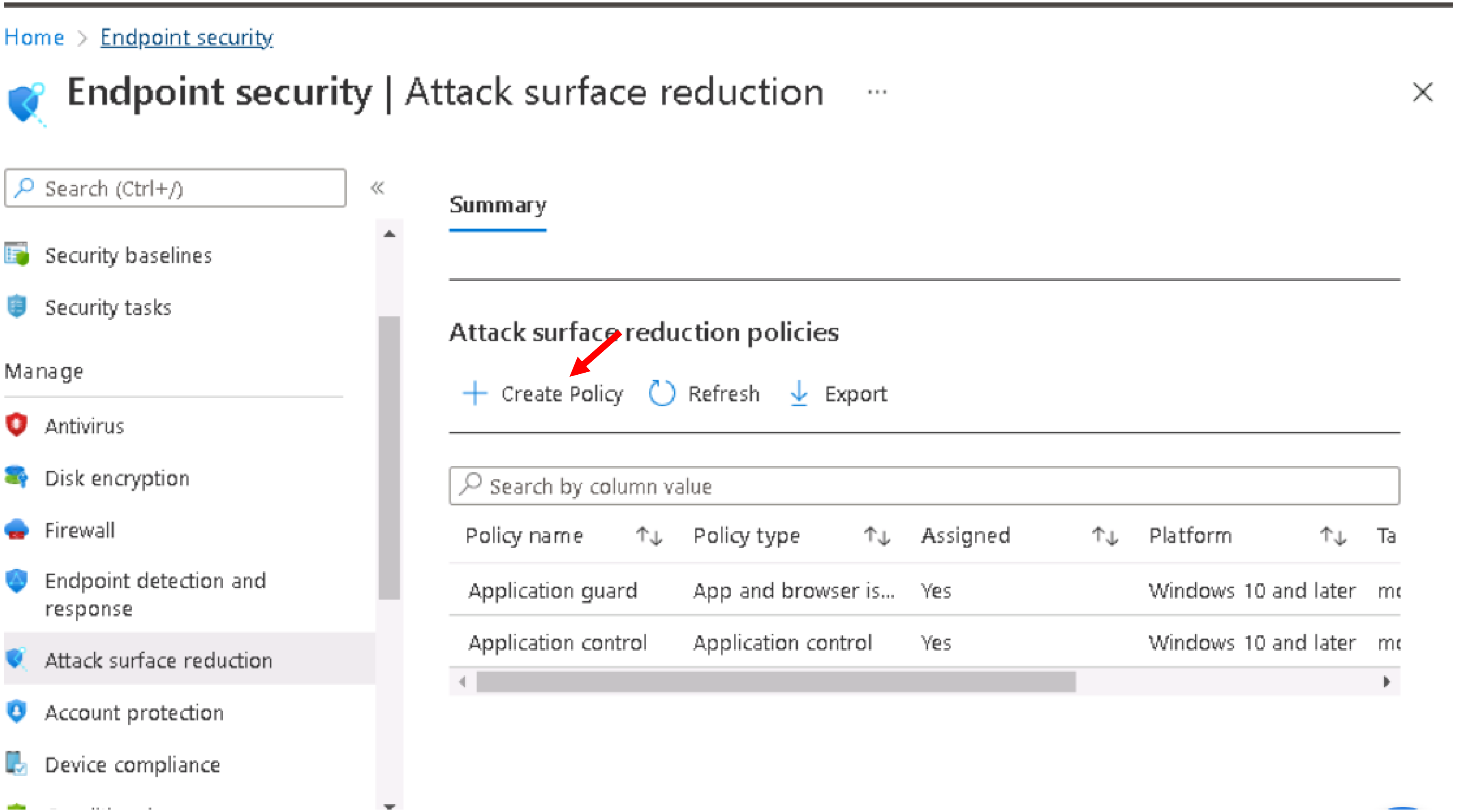
Summary

Basics

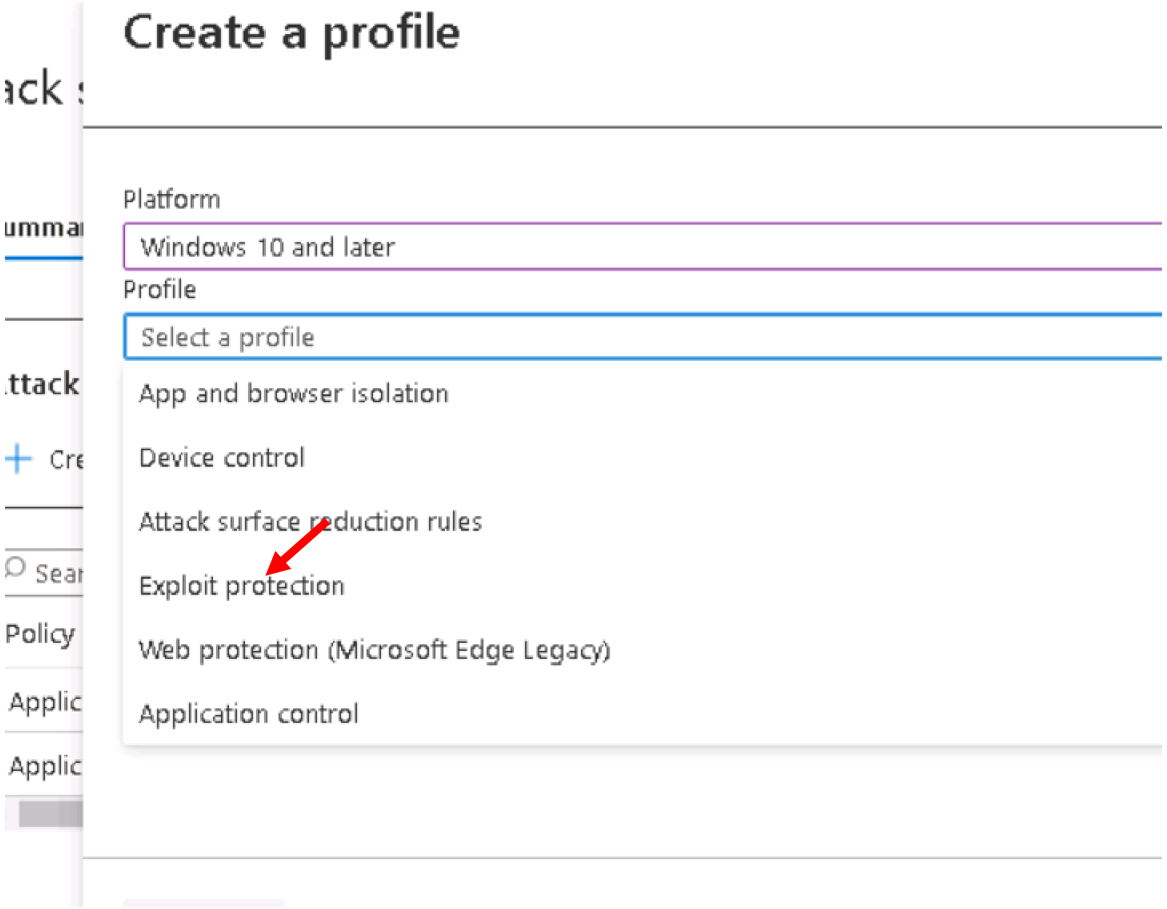
Name	Application control
Description	--
Platform	Windows 10 and later

Configuration settings

App locker application control	Audit Components, Store Apps, and Smartlocker
Block users from ignoring SmartScreen warnings	Yes



Policy name	Policy type	Assigned	Platform	Ta
Application guard	App and browser is...	Yes	Windows 10 and later	m
Application control	Application control	Yes	Windows 10 and later	m



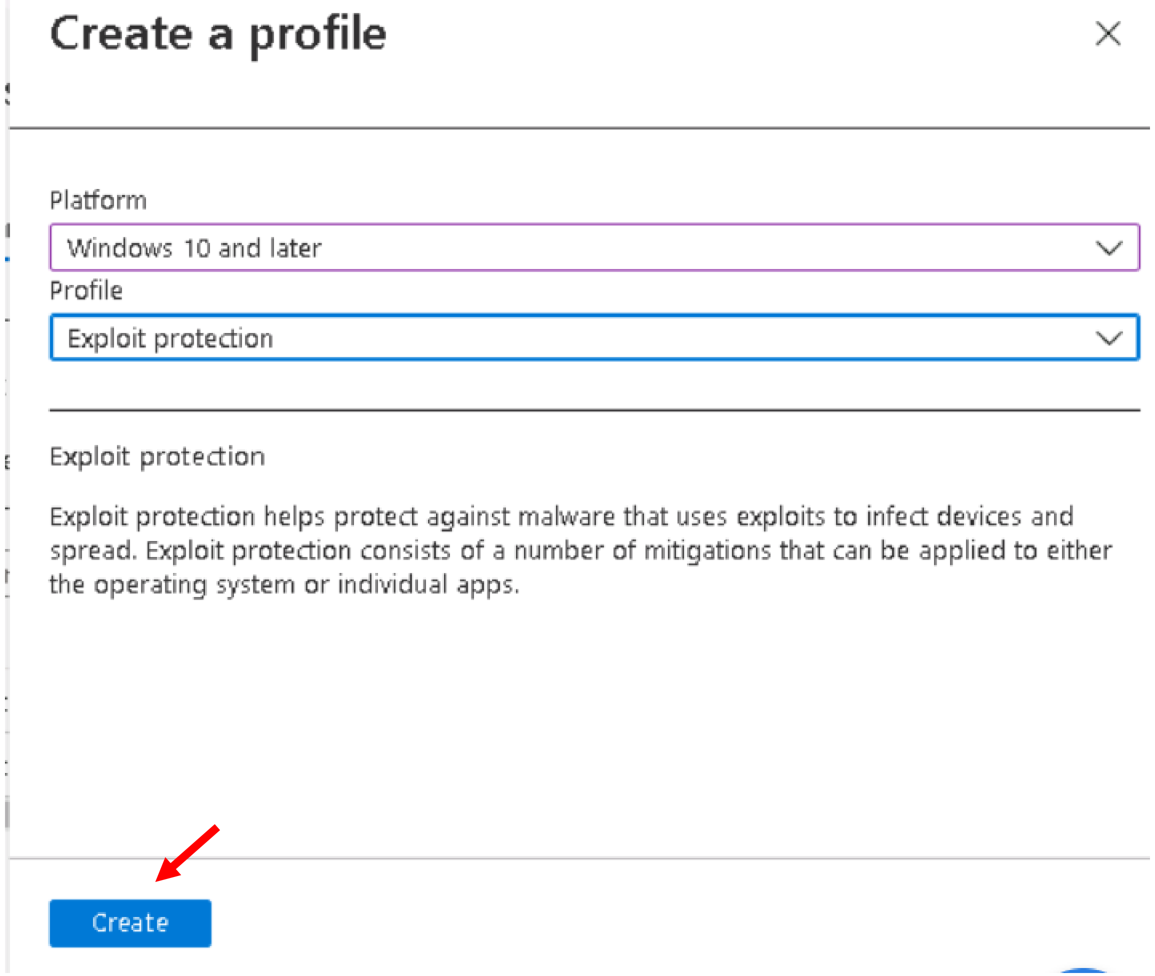
ack s
umma
ttack
+ Cre
Sear
Policy
Applic
Applic

Create a profile

Platform
Windows 10 and later

Profile
Select a profile

App and browser isolation
Device control
Attack surface reduction rules
Exploit protection
Web protection (Microsoft Edge Legacy)
Application control



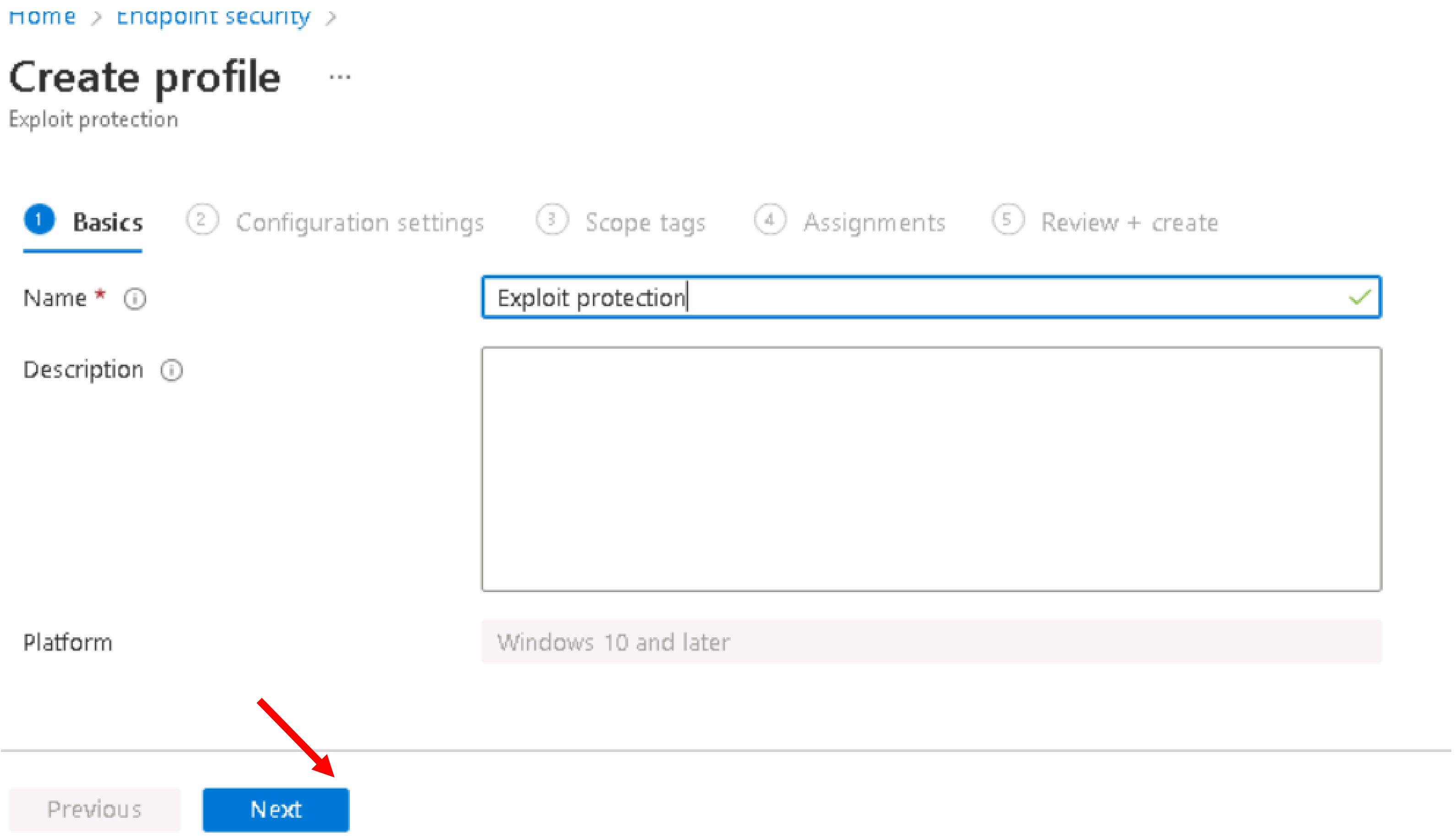
Create a profile

Platform: Windows 10 and later

Profile: Exploit protection

Exploit protection

Exploit protection helps protect against malware that uses exploits to infect devices and spread. Exploit protection consists of a number of mitigations that can be applied to either the operating system or individual apps.


Home > Endpoint security >

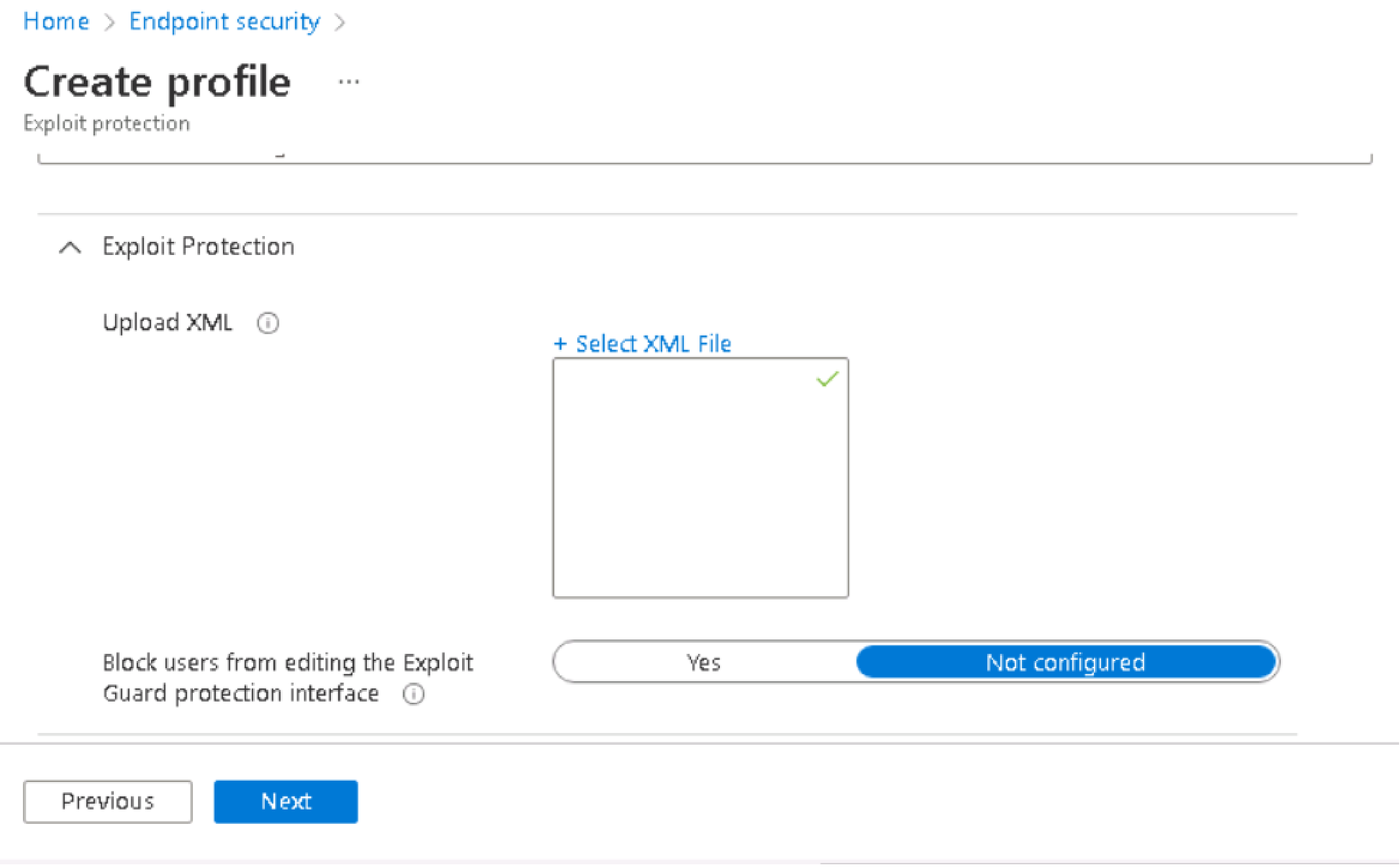
Create profile ...

Exploit protection

Name * Exploit protection

Description

Platform Windows 10 and later



Home > Endpoint security >

Create profile ...

Exploit protection

Exploit Protection

Upload XML ⓘ

+ Select XML File

Block users from editing the Exploit Guard protection interface ⓘ Yes [✓ Not configured]

Instructions for getting the xml file.

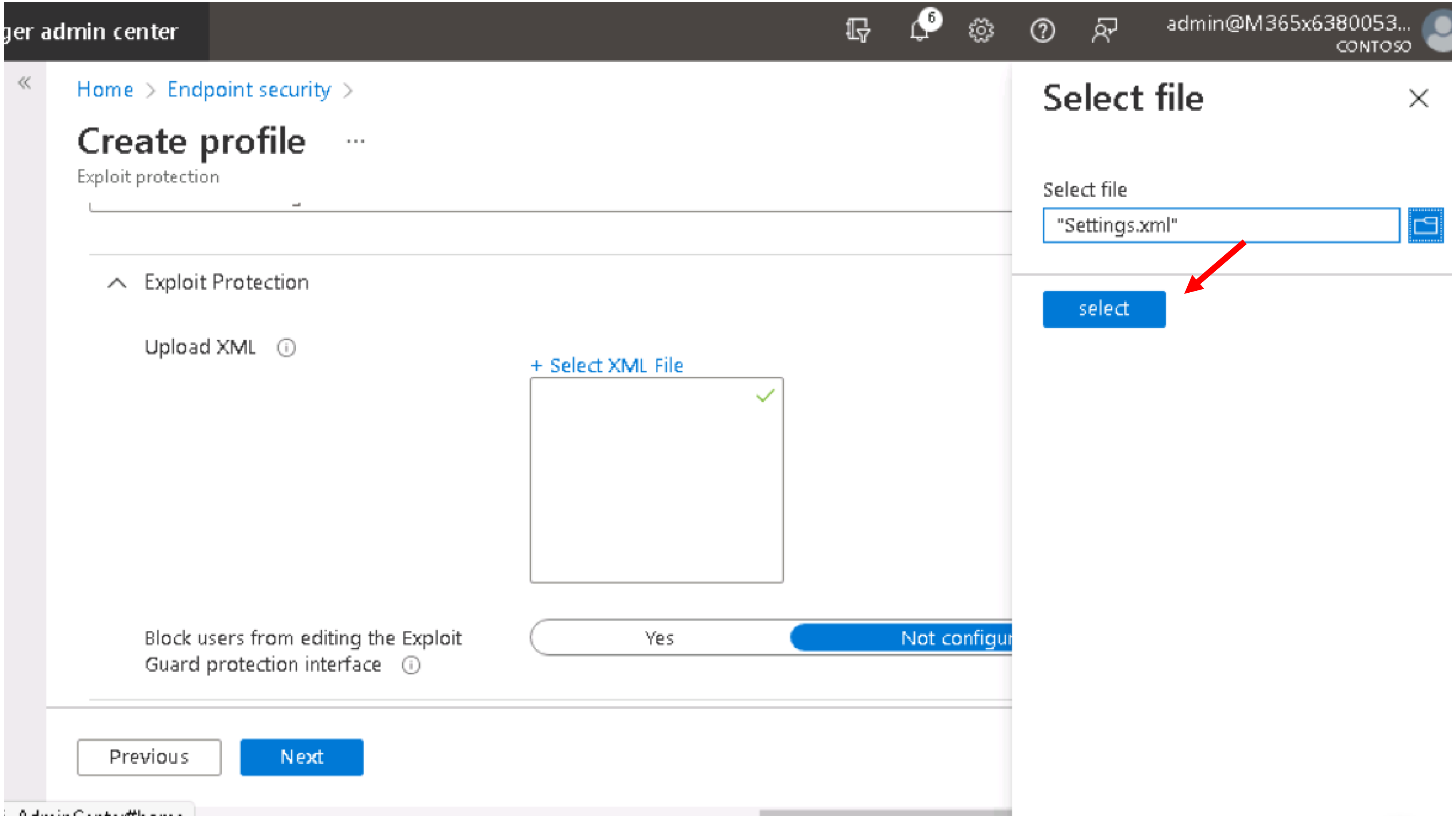
1.Open the Windows Security app by selecting the shield icon in the task bar or searching the start menu for **Windows Security**.
2.Select the **App & browser control** tile (or the app icon on the left menu bar) and then select **Exploit protection**.
3.Go to **Program settings** and choose the app you want to apply mitigations to.

1. If the app you want to configure is already listed, select it, and then select **Edit**.
2. If the app is not listed, at the top of the list select **Add program to customize** and then choose how you want to add the app.

    1. Use **Add by program name** to have the mitigation applied to any running process with that name. Specify a file with an extension. You can enter a full path to limit the mitigation to only the app with that name in that location.
    2. Use **Choose exact file path** to use a standard Windows Explorer file picker window to find and select the file you want.

4.After selecting the app, you'll see a list of all the mitigations that can be applied.
Choosing **Audit** will apply the mitigation in audit mode only. You will be notified if you need to restart the process or app, or if you need to restart Windows.
5.Repeat steps 3-4 for all the apps and mitigations you want to configure.

6.Export the settings. This will be the xml file you will import.



Create profile ···

Exploit protection

Exploit Protection

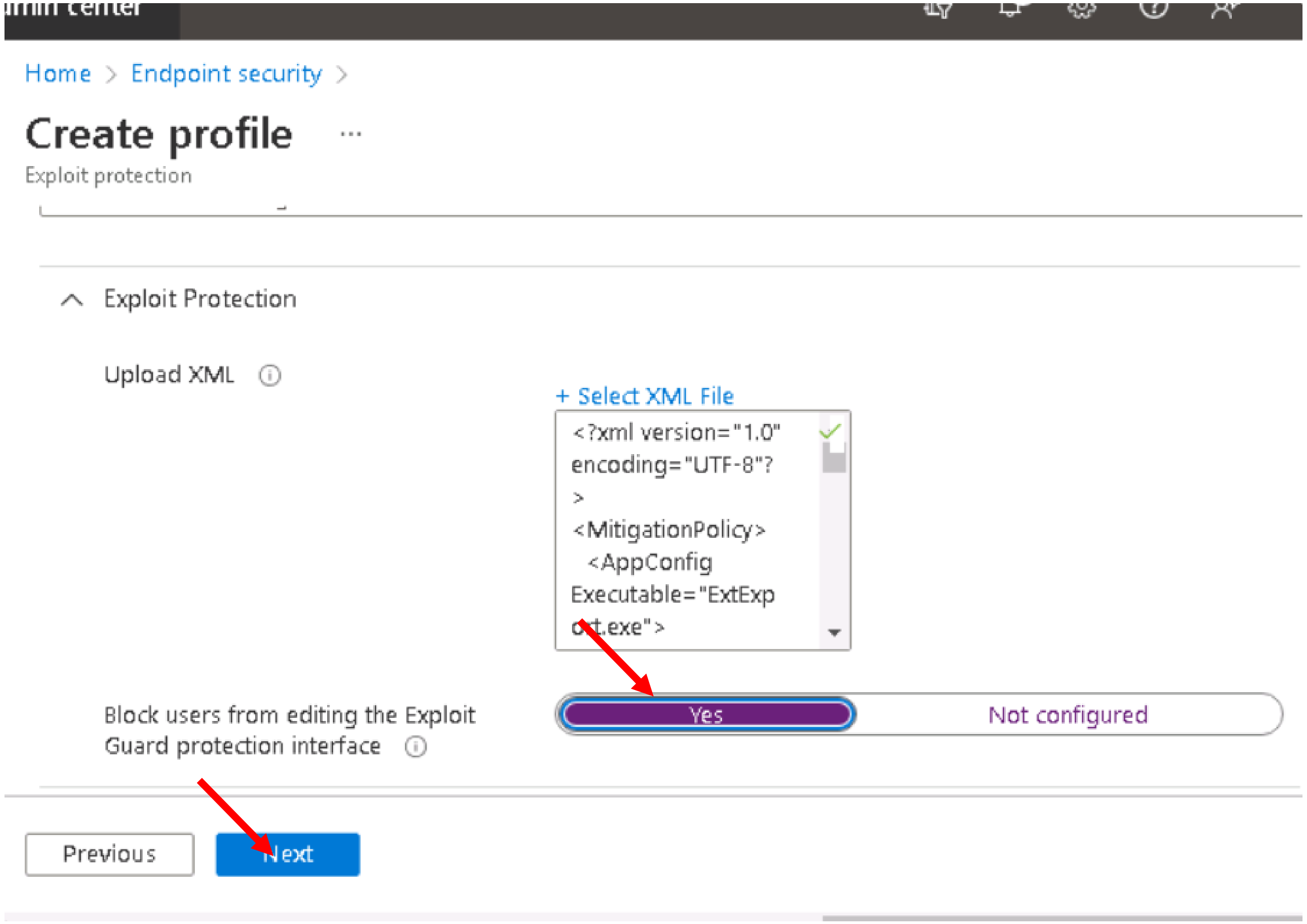
Upload XML ⓘ

+ Select XML File

Block users from editing the Exploit Guard protection interface ⓘ: Yes [✓ Not configu]

Select file

Select file: "Settings.xml"



Create profile ...

Exploit protection

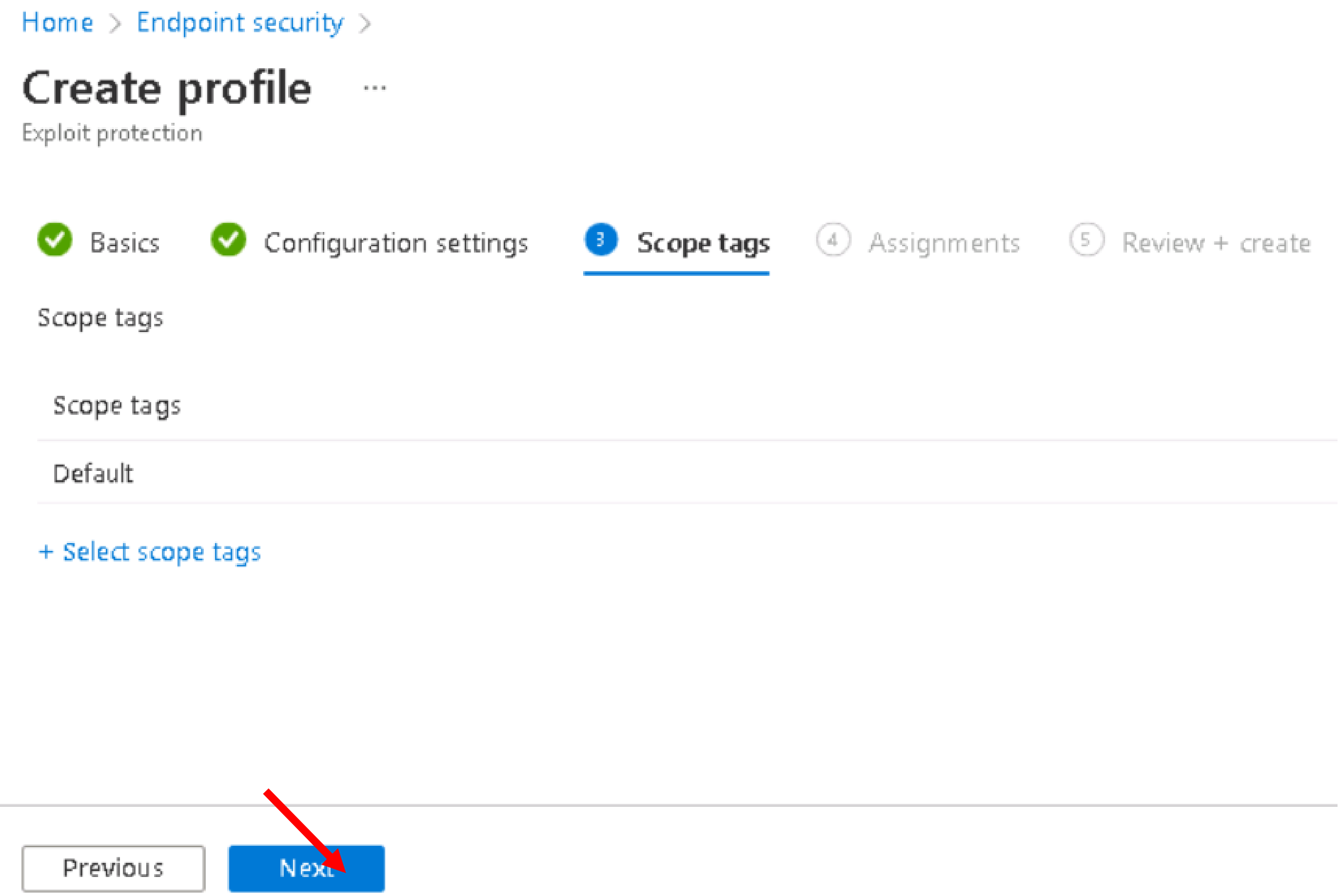
Exploit Protection

Upload XML ⓘ

+ Select XML File

```
<?xml version="1.0"
encoding="UTF-8"?
>
<MitigationPolicy>
  <AppConfig
Executable="ExtExp
ort.exe">
```

Block users from editing the Exploit Guard protection interface ⓘ [✓ Yes] Not configured



Home > Endpoint security >

Create profile ...

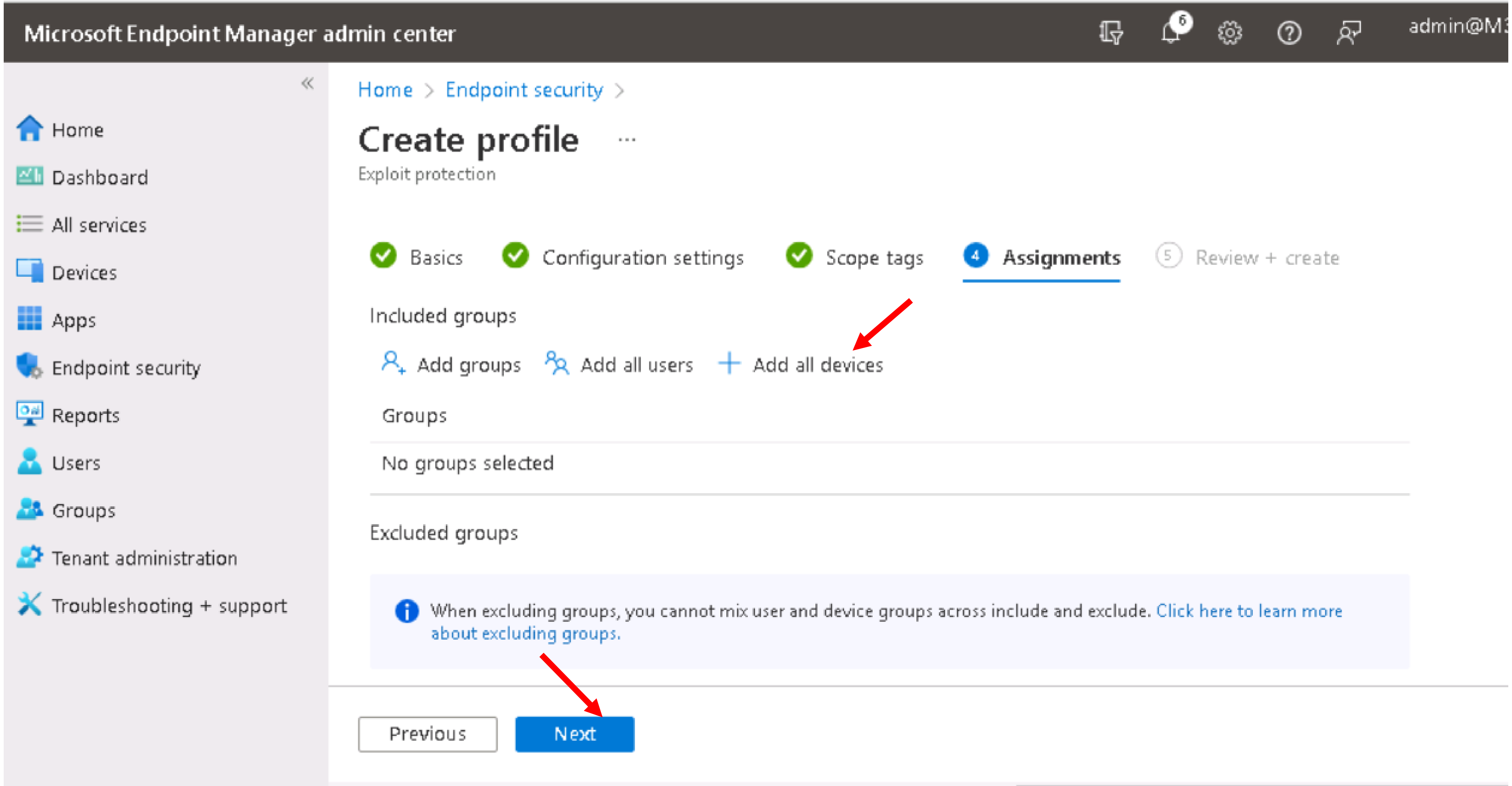
Exploit protection

✓ Basics ✓ Configuration settings ③ Scope tags ④ Assignments ⑤ Review + create

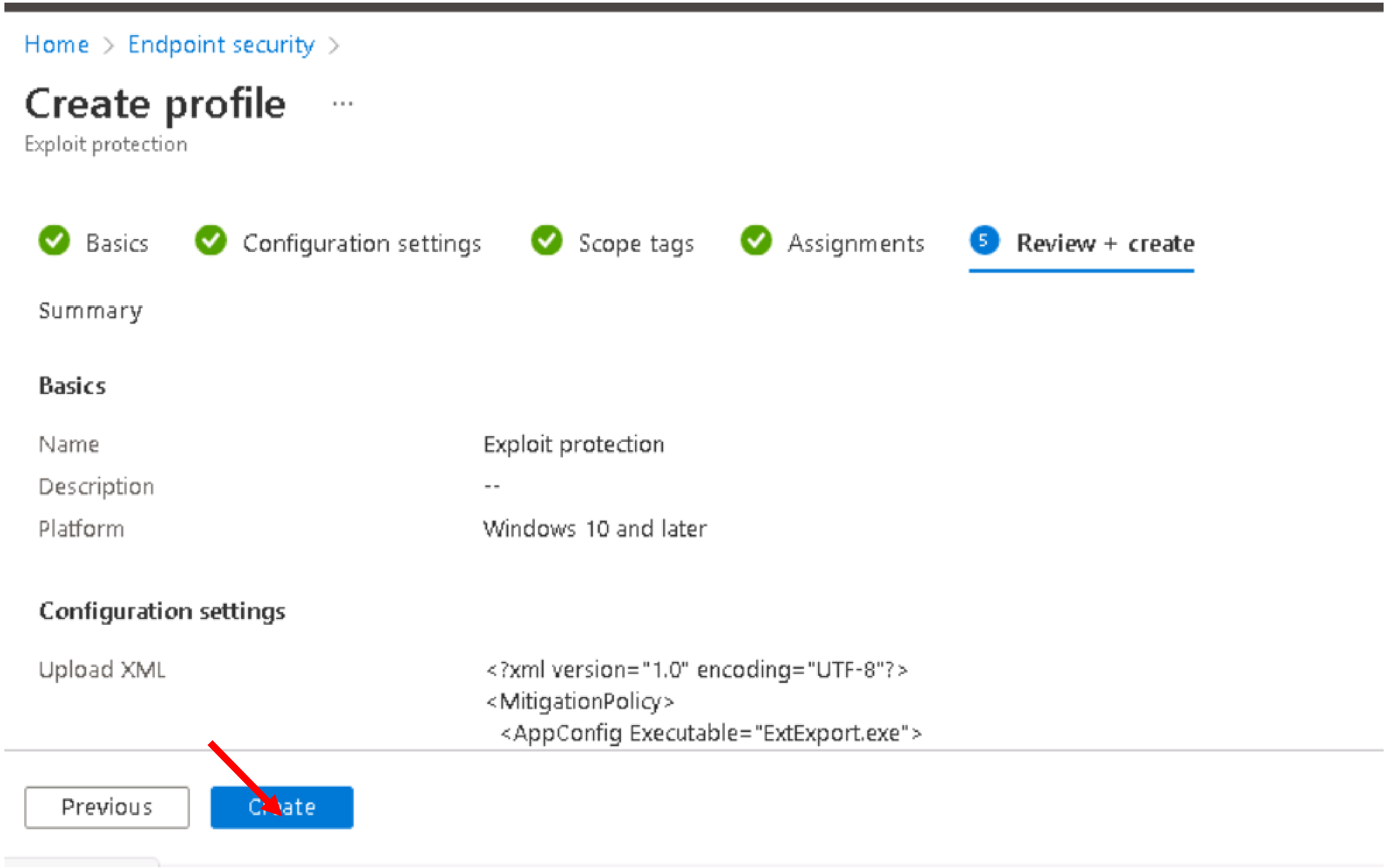
Scope tags

Scope tags
Default

+ Select scope tags



When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about excluding groups.



Summary

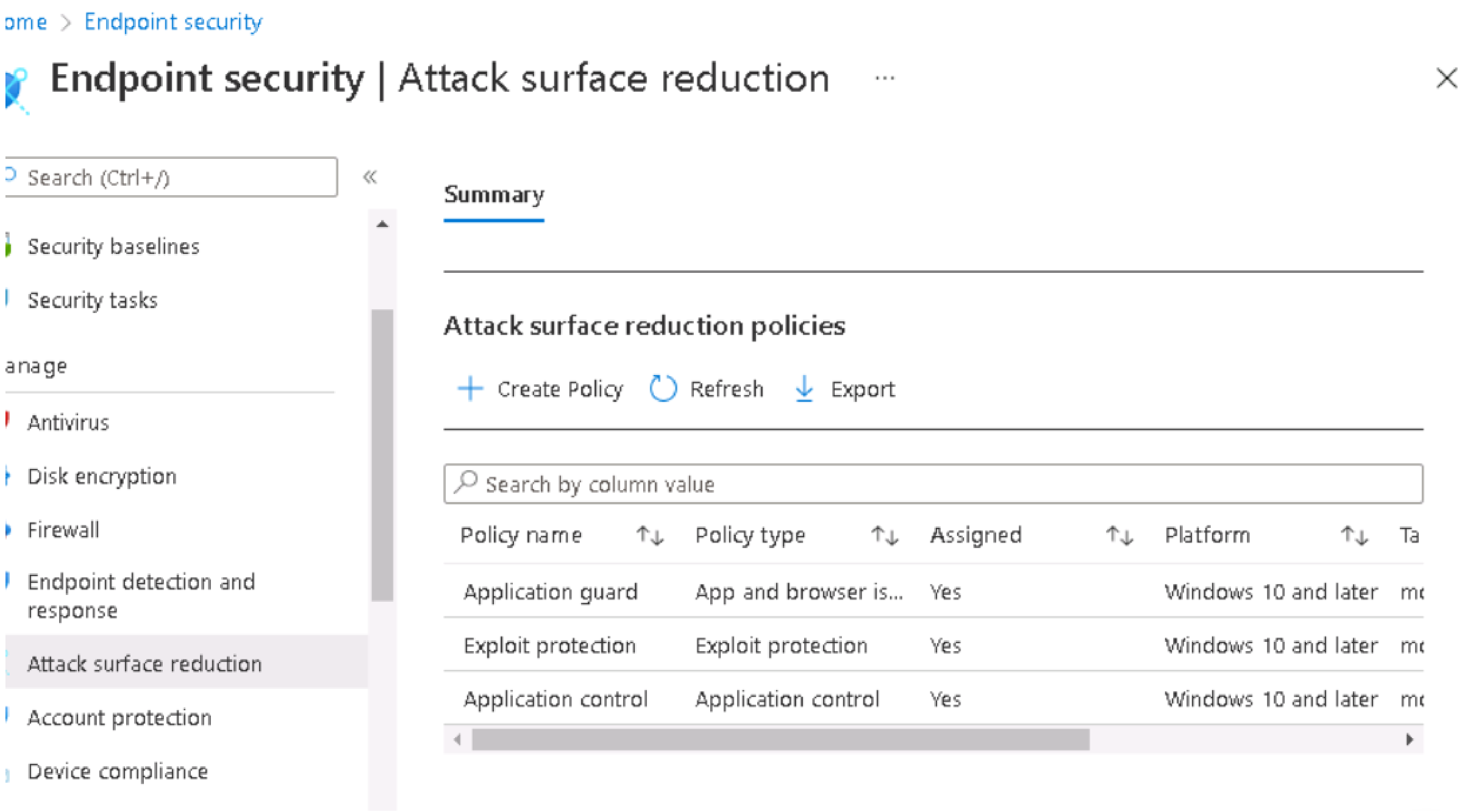
Basics

Name	Exploit protection
Description	--
Platform	Windows 10 and later

Configuration settings

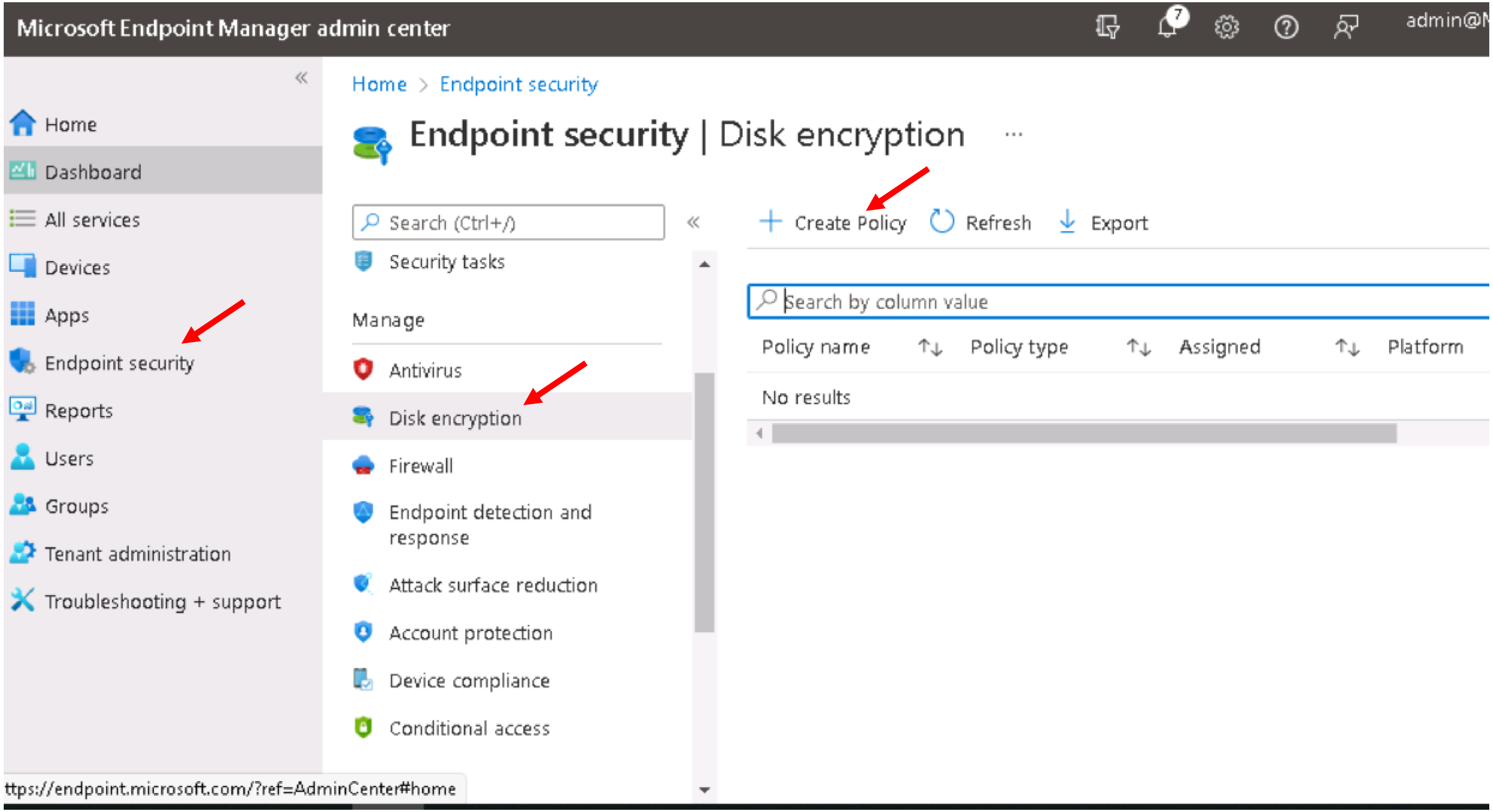
Upload XML

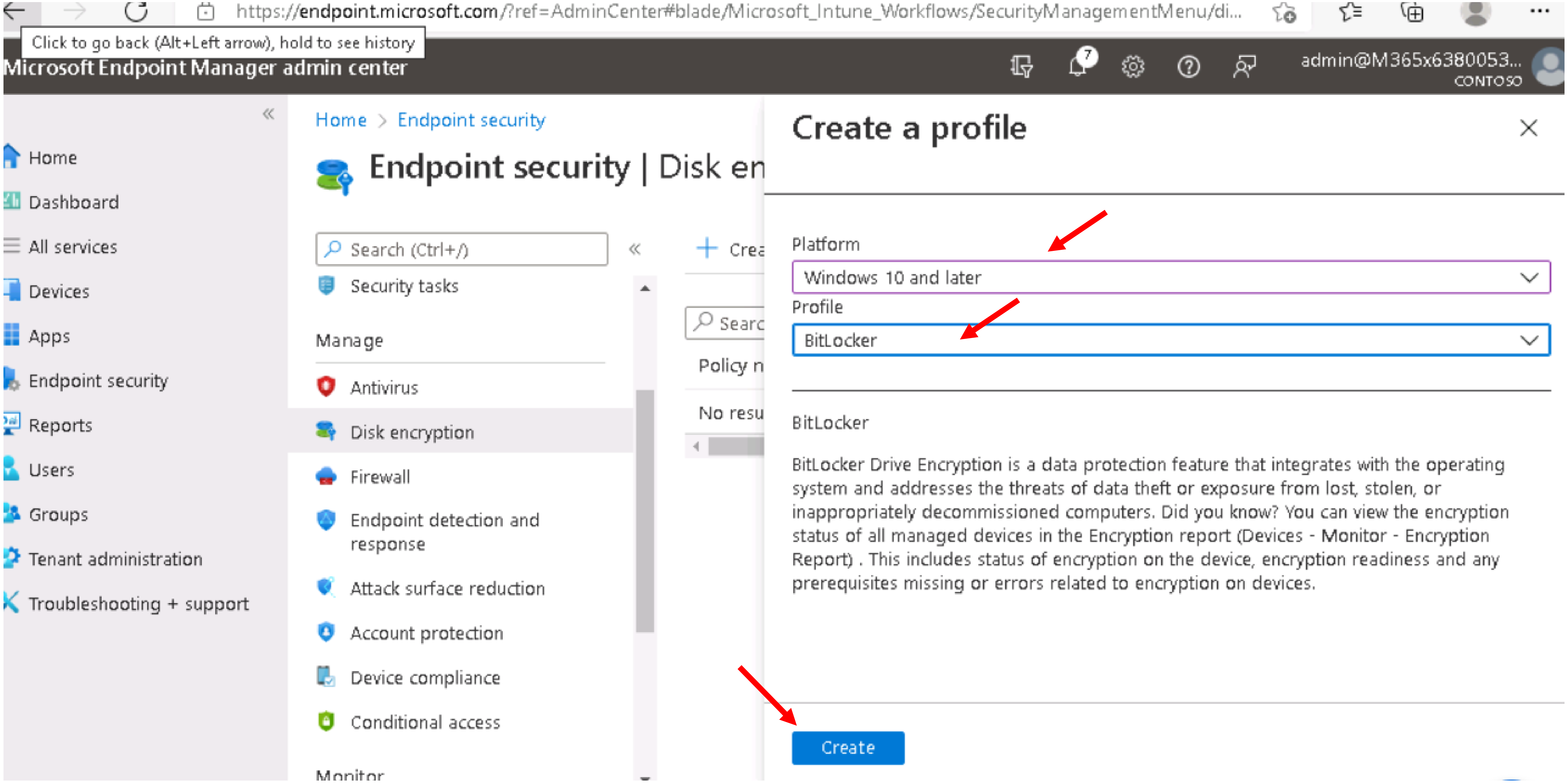
```
<?xml version="1.0" encoding="UTF-8"?>
<MitigationPolicy>
  <AppConfig Executable="ExtExport.exe">
```



Policy name	Policy type	Assigned	Platform	Ta
Application guard	App and browser is...	Yes	Windows 10 and later	m
Exploit protection	Exploit protection	Yes	Windows 10 and later	m
Application control	Application control	Yes	Windows 10 and later	m

Windows device encryption





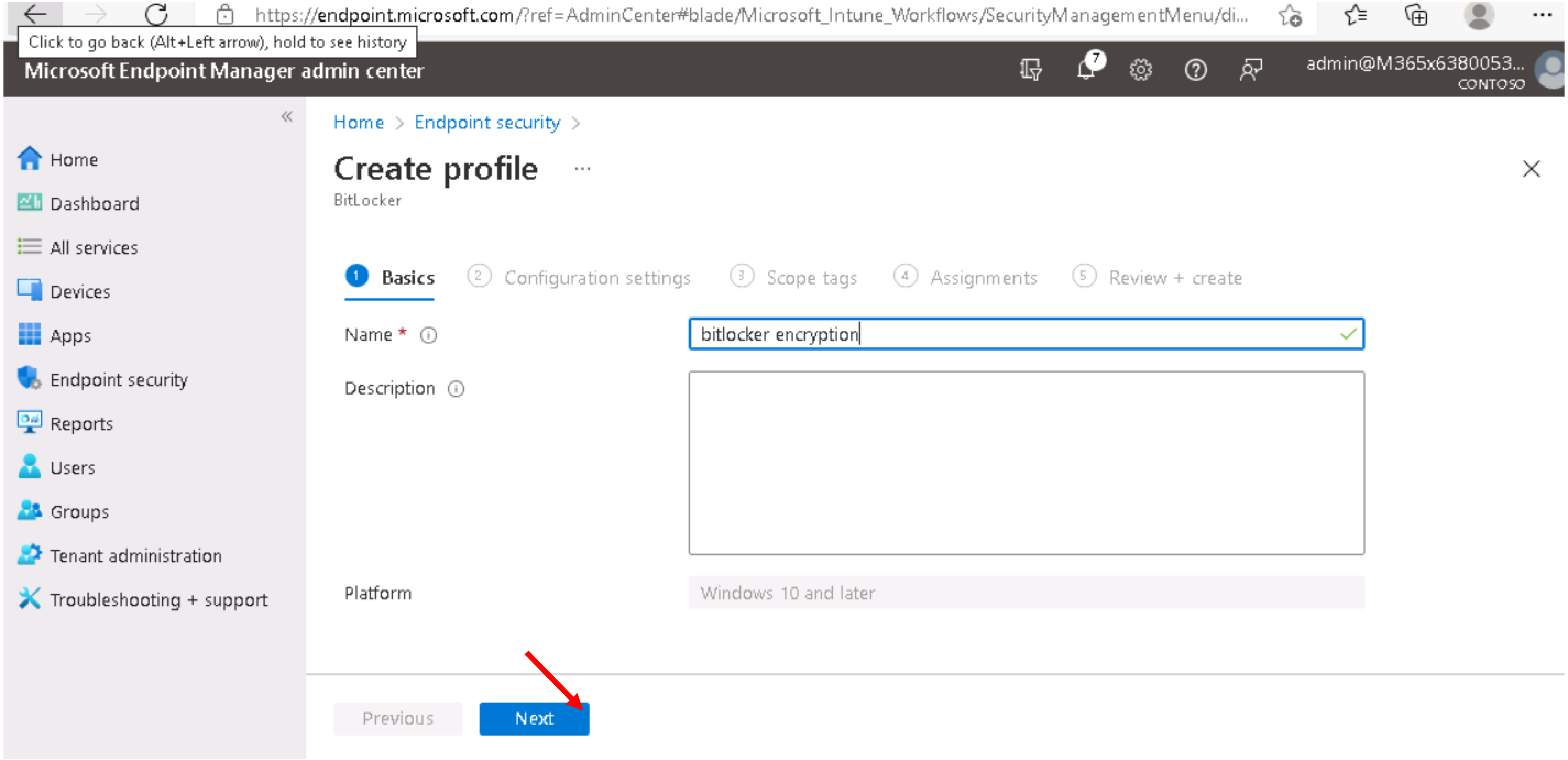
Create a profile

Platform: Windows 10 and later

Profile: BitLocker

BitLocker

BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers. Did you know? You can view the encryption status of all managed devices in the Encryption report (Devices - Monitor - Encryption Report) . This includes status of encryption on the device, encryption readiness and any prerequisites missing or errors related to encryption on devices.

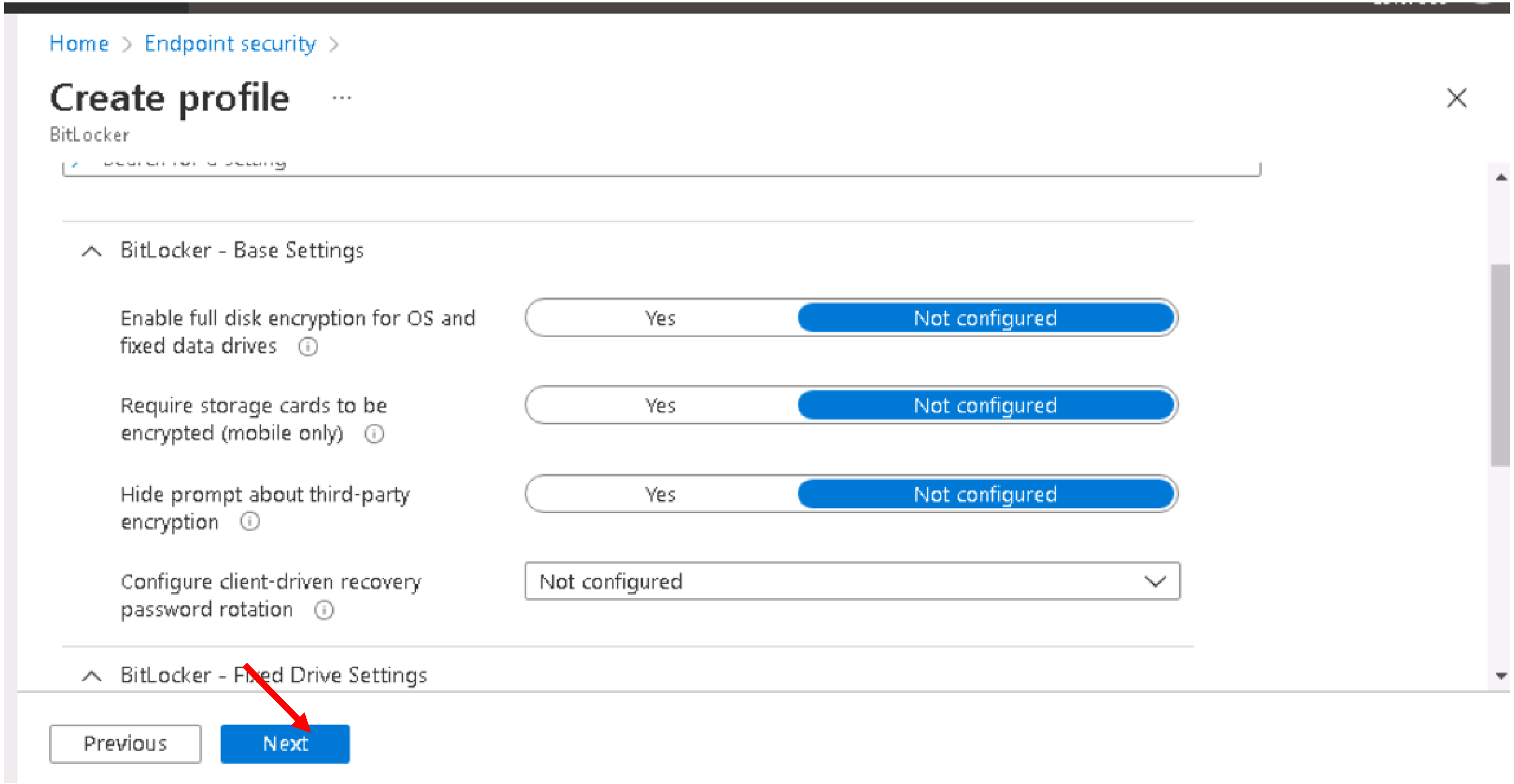


https://endpoint.microsoft.com/?ref=AdminCenter#blade/Microsoft_Intune_Workflows/SecurityManagementMenu/di...
Click to go back (Alt+Left arrow), hold to see history
Microsoft Endpoint Manager admin center
7
admin@M365x6380053...
CONTOSO
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security >
Create profile ...
BitLocker
1 Basics
2 Configuration settings
3 Scope tags
4 Assignments
5 Review + create
Previous
Next

Name * bitlocker encryption

Description

Platform Windows 10 and later



Home > Endpoint security >

Create profile ...

BitLocker

BitLocker - Base Settings

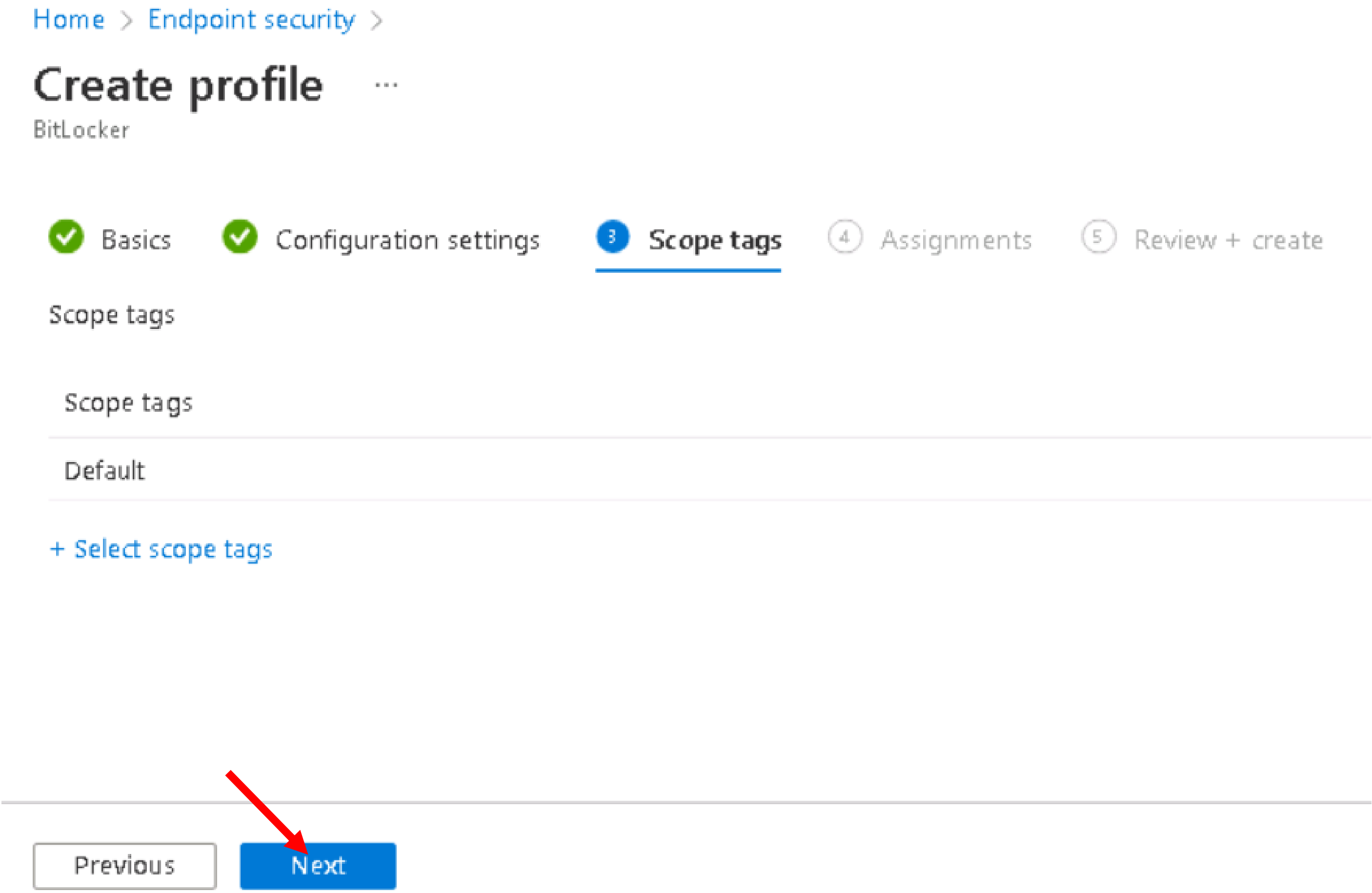
Enable full disk encryption for OS and fixed data drives ⓘ: Yes [✓ Not configured]

Require storage cards to be encrypted (mobile only) ⓘ: Yes [✓ Not configured]

Hide prompt about third-party encryption ⓘ: Yes [✓ Not configured]

Configure client-driven recovery password rotation ⓘ: Not configured

BitLocker - Fixed Drive Settings



Home > Endpoint security >

Create profile ...

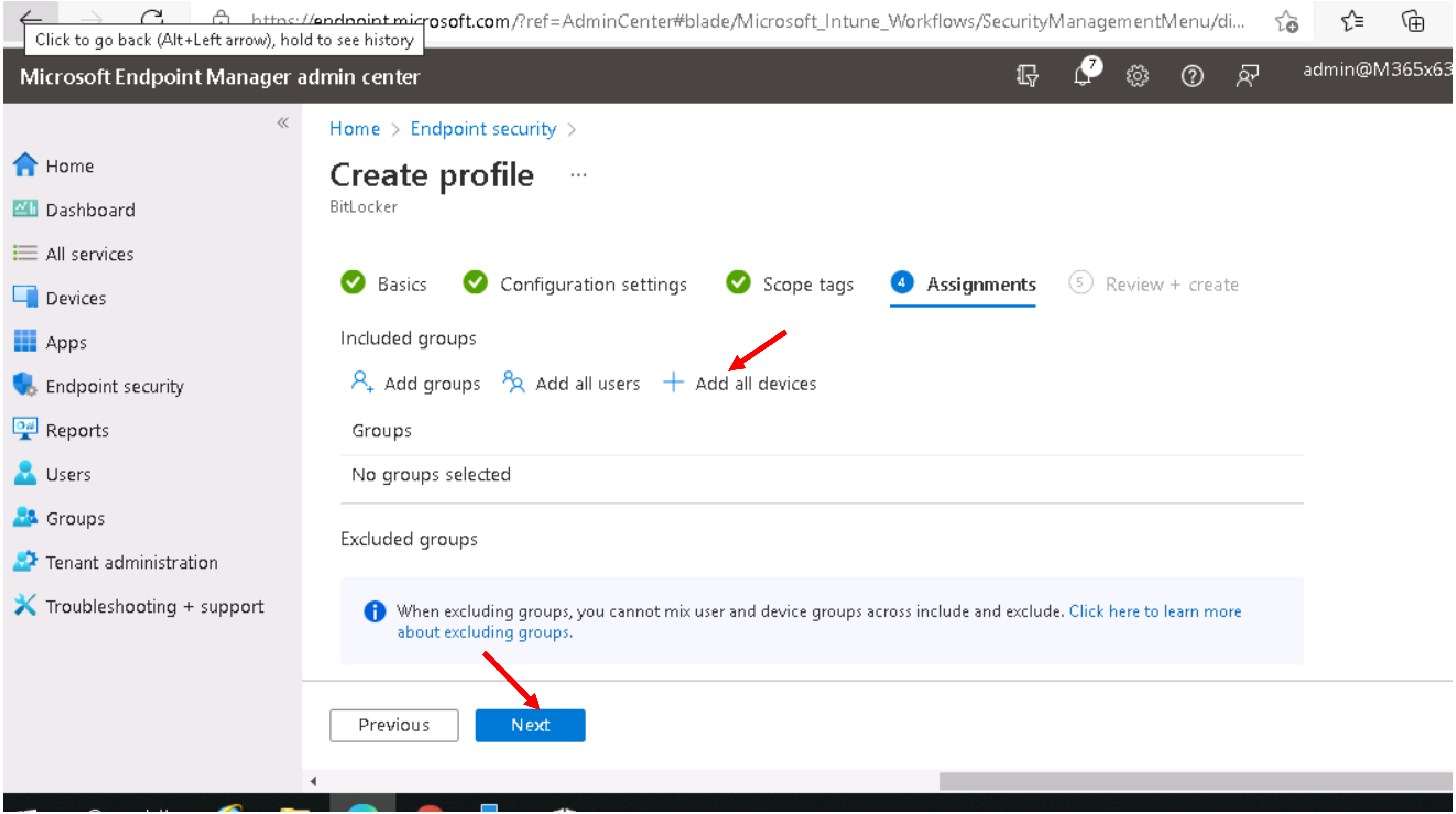
BitLocker

✓ Basics ✓ Configuration settings ③ Scope tags ④ Assignments ⑤ Review + create

Scope tags

Scope tags
Default

+ Select scope tags



https://endpoint.microsoft.com/?ref=AdminCenter#blade/Microsoft_Intune_Workflows/SecurityManagementMenu/di...

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

Microsoft Endpoint Manager admin center

admin@M365x63

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

Home > Endpoint security >

Create profile ...

BitLocker

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

Included groups

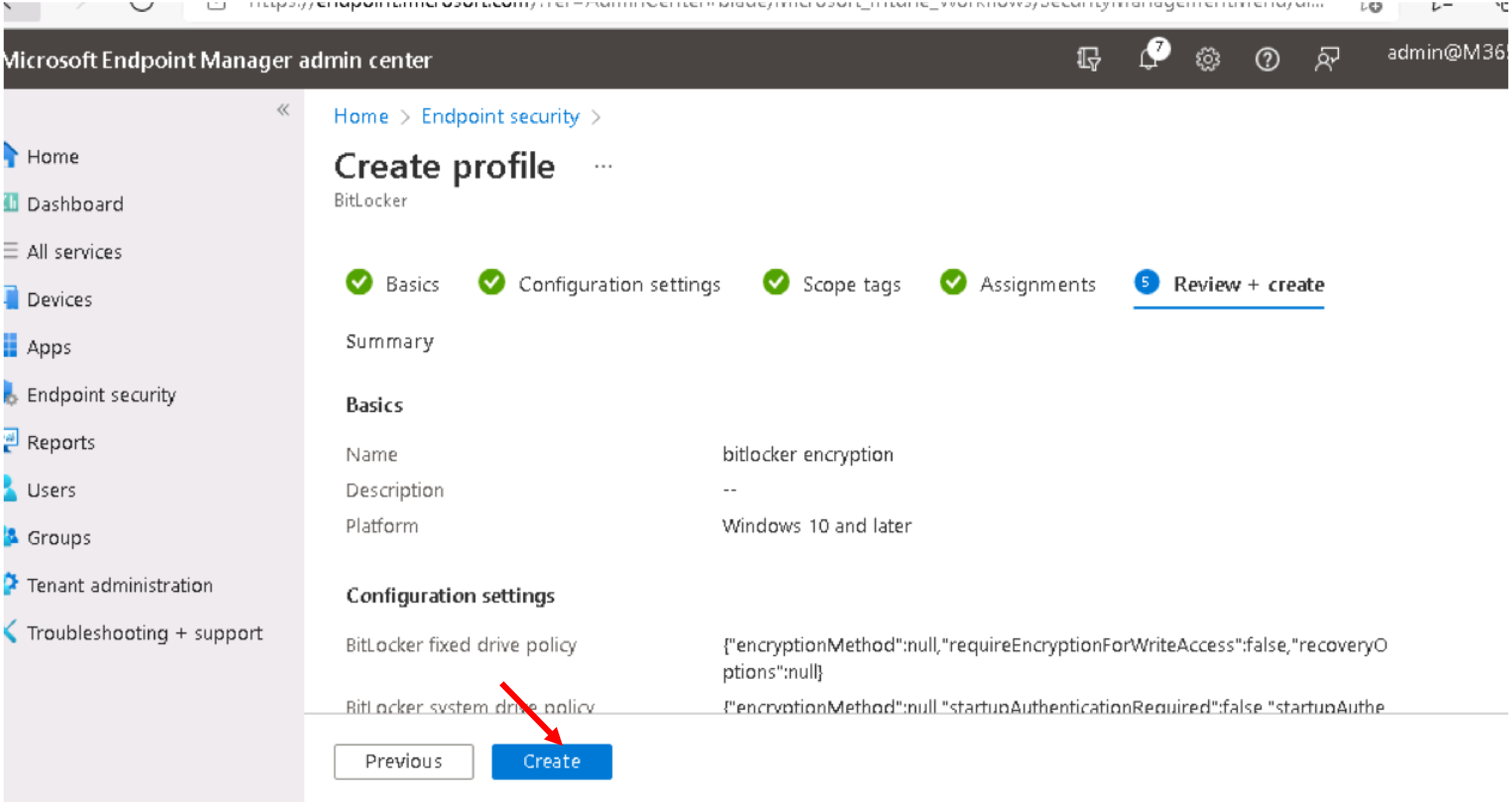
Add groups Add all users + Add all devices

Groups
No groups selected

Excluded groups

When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about excluding groups.

Previous Next



Create profile

BitLocker

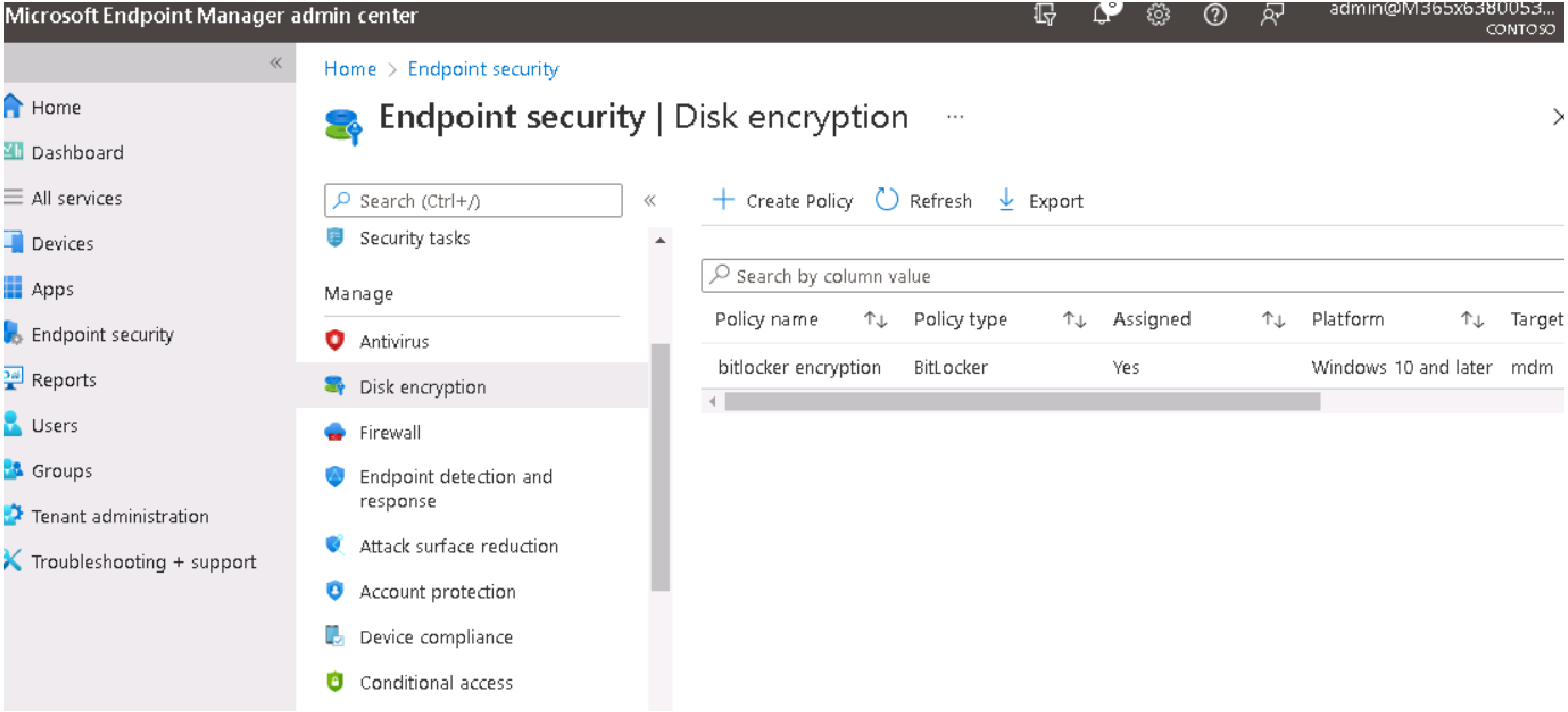
Summary

Basics

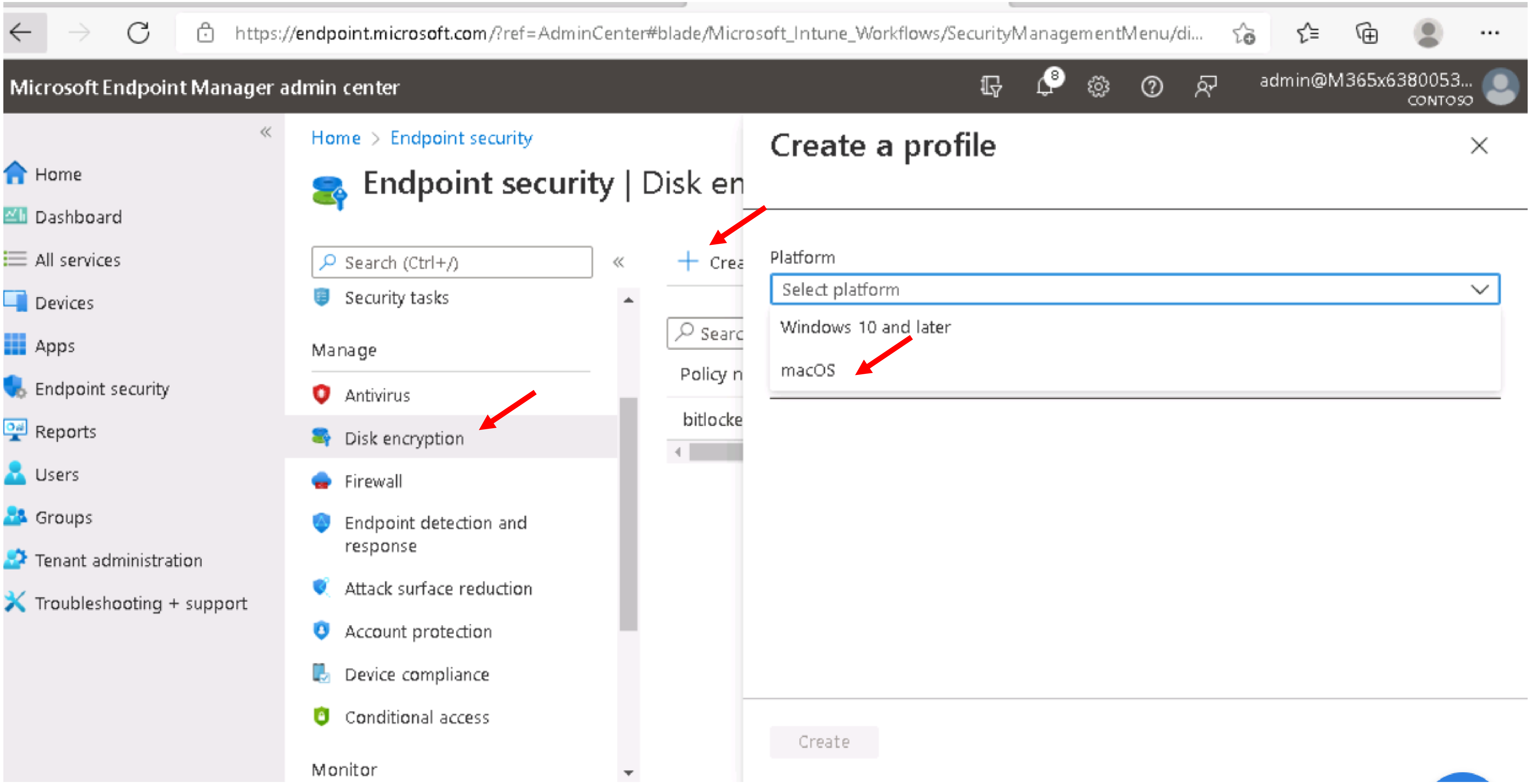
Name	bitlocker encryption
Description	--
Platform	Windows 10 and later

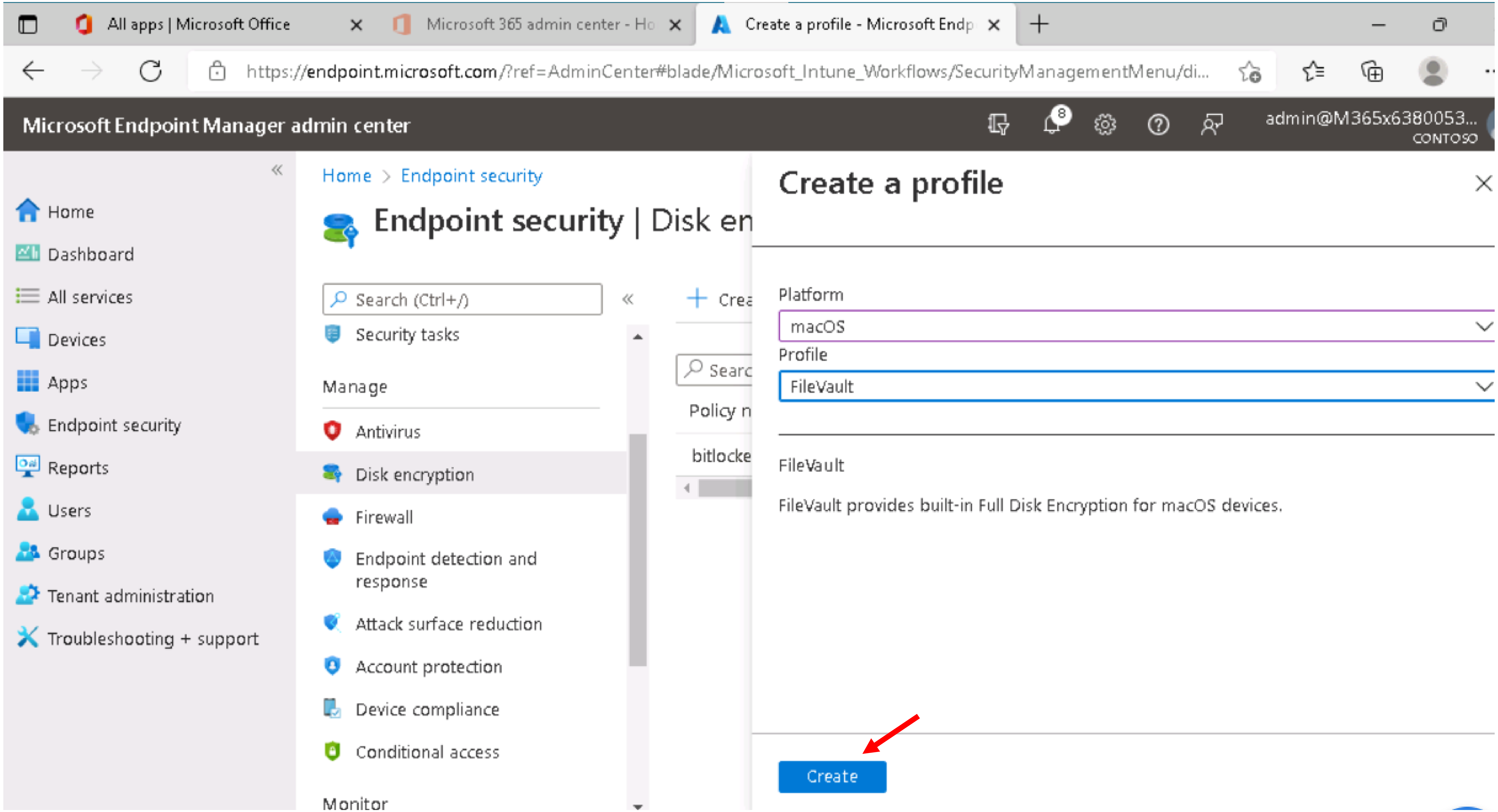
Configuration settings

BitLocker fixed drive policy	{"encryptionMethod":null,"requireEncryptionForWriteAccess":false,"recoveryOptions":null}
BitLocker system drive policy	{"encryptionMethod":null,"startupAuthenticationRequired":false,"startupAuthe



Policy name	Policy type	Assigned	Platform	Target
bitlocker encryption	BitLocker	Yes	Windows 10 and later	mdm


https://endpoint.microsoft.com/?ref=AdminCenter#blade/Microsoft_Intune_Workflows/SecurityManagementMenu/di...
Microsoft Endpoint Manager admin center
admin@M365x6380053...
CONTOSO
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Disk en
Search (Ctrl+/)
Security tasks
Manage
Antivirus
Disk encryption
Firewall
Endpoint detection and response
Attack surface reduction
Account protection
Device compliance
Conditional access
Monitor
+ Crea
Searc
Policy n
bitlocke
Create a profile
Platform
Select platform
Windows 10 and later
macOS
Create



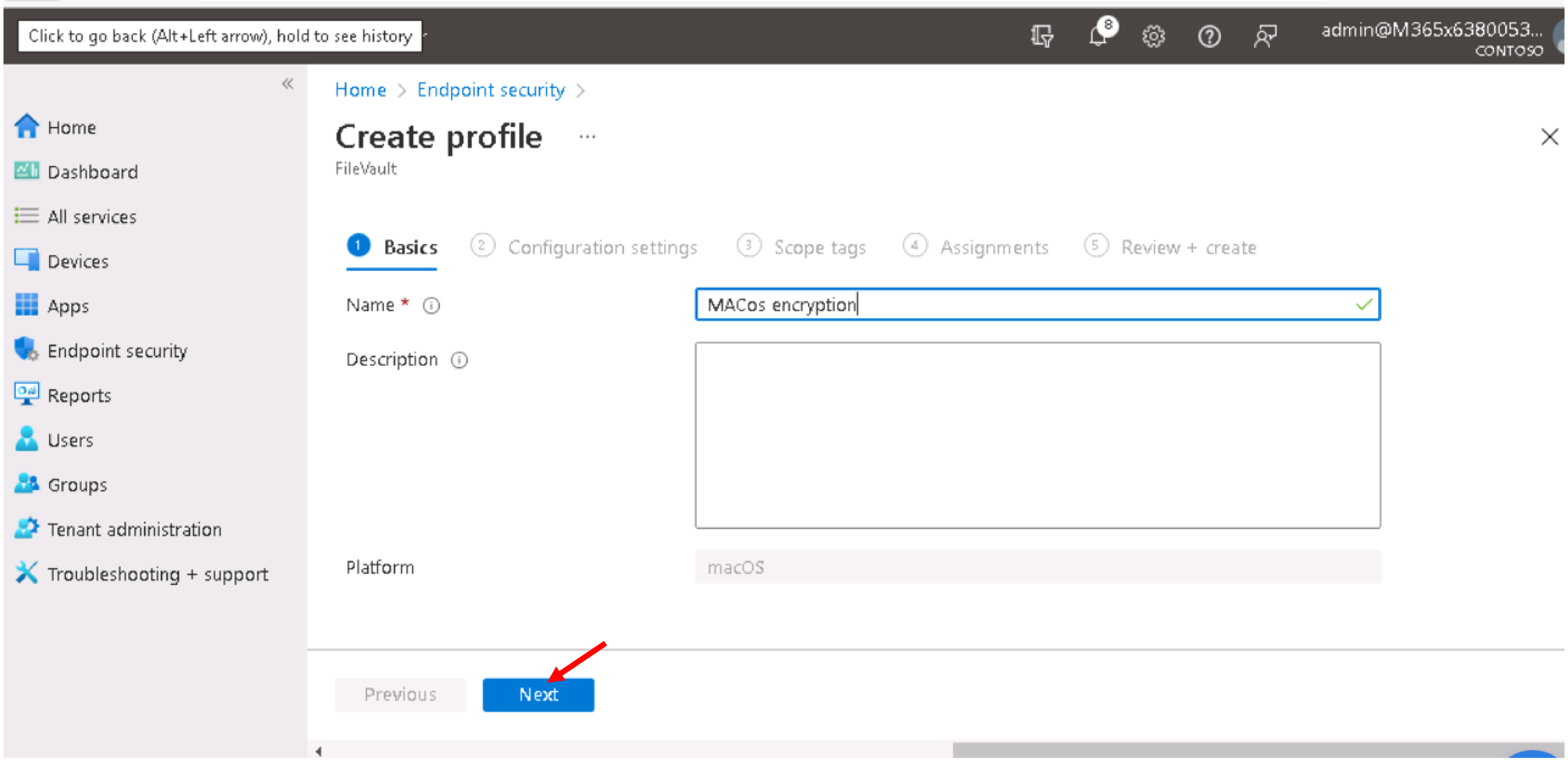
Create a profile

Platform
macOS

Profile
FileVault

FileVault

FileVault provides built-in Full Disk Encryption for macOS devices.



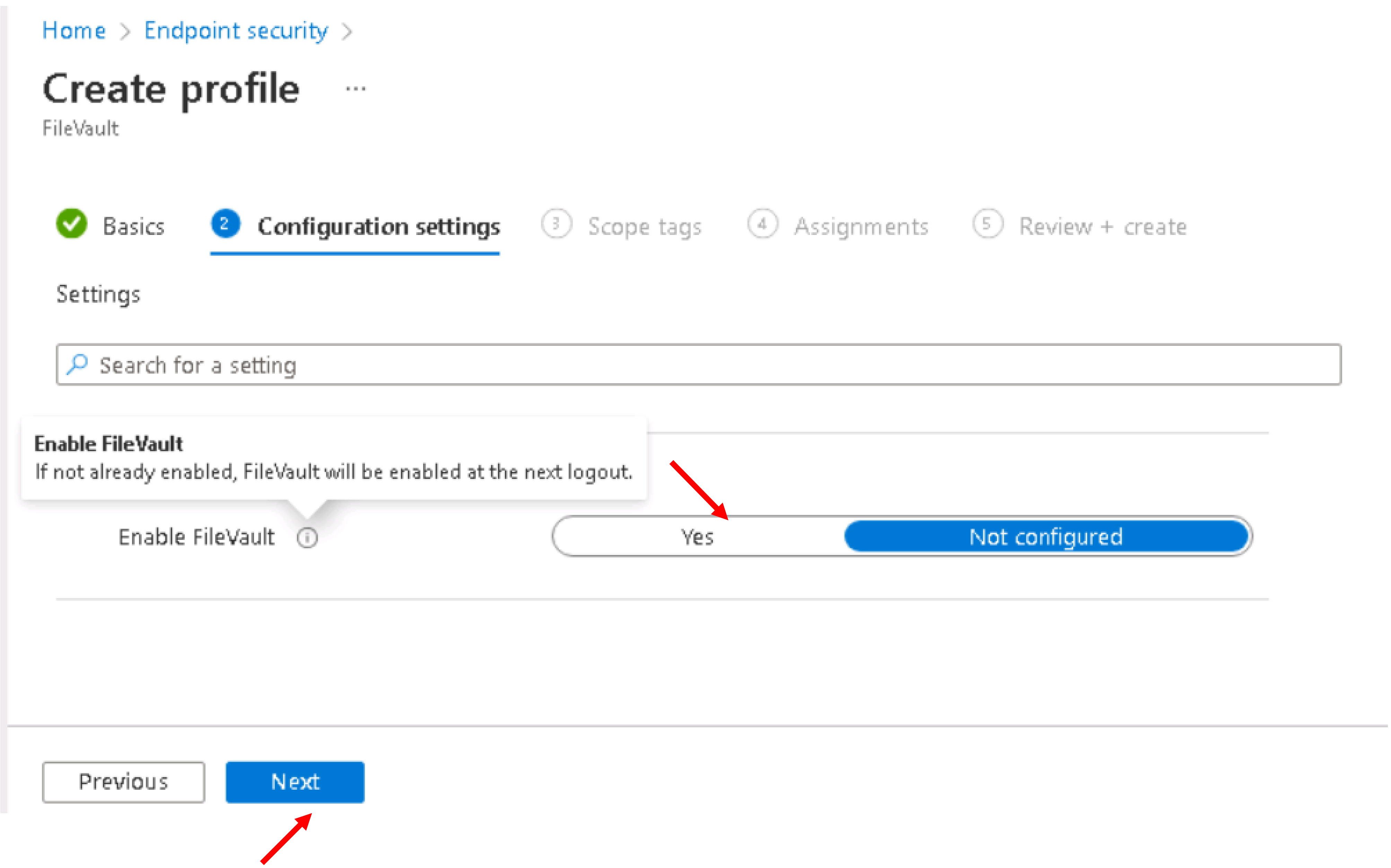
Create profile

FileVault

Name * ⓘ MACos encryption

Description ⓘ

Platform macOS



Home > Endpoint security >

Create profile ...

FileVault

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

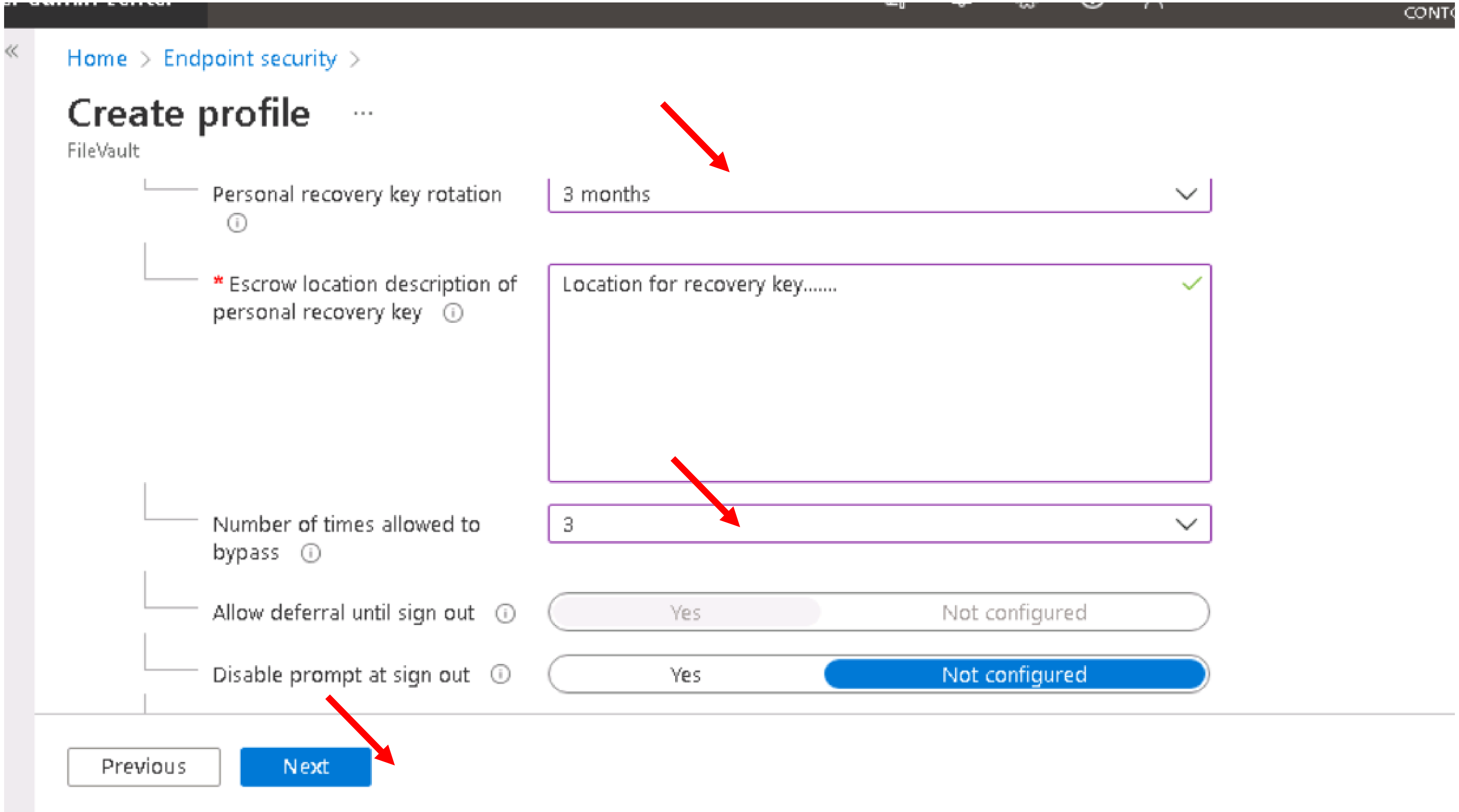
Settings

Search for a setting

Enable FileVault
If not already enabled, FileVault will be enabled at the next logout.

Enable FileVault ⓘ Yes [✓ Not configured]

Previous Next



Home > Endpoint security >

Create profile ...

FileVault

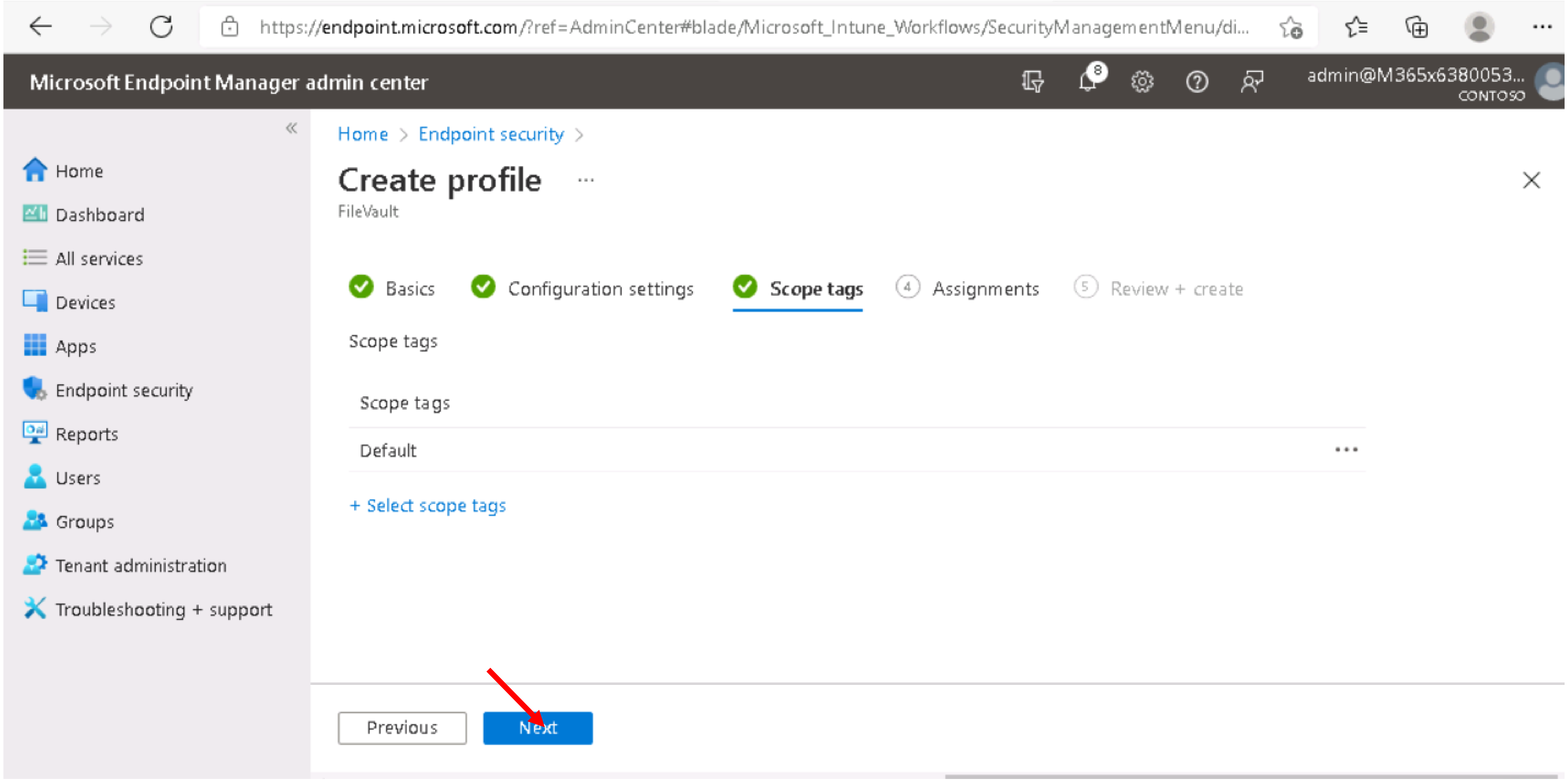
Personal recovery key rotation ⓘ: 3 months

* Escrow location description of personal recovery key ⓘ: Location for recovery key.......

Number of times allowed to bypass ⓘ: 3

Allow deferral until sign out ⓘ: Yes / Not configured

Disable prompt at sign out ⓘ: Yes [✓ Not configured]

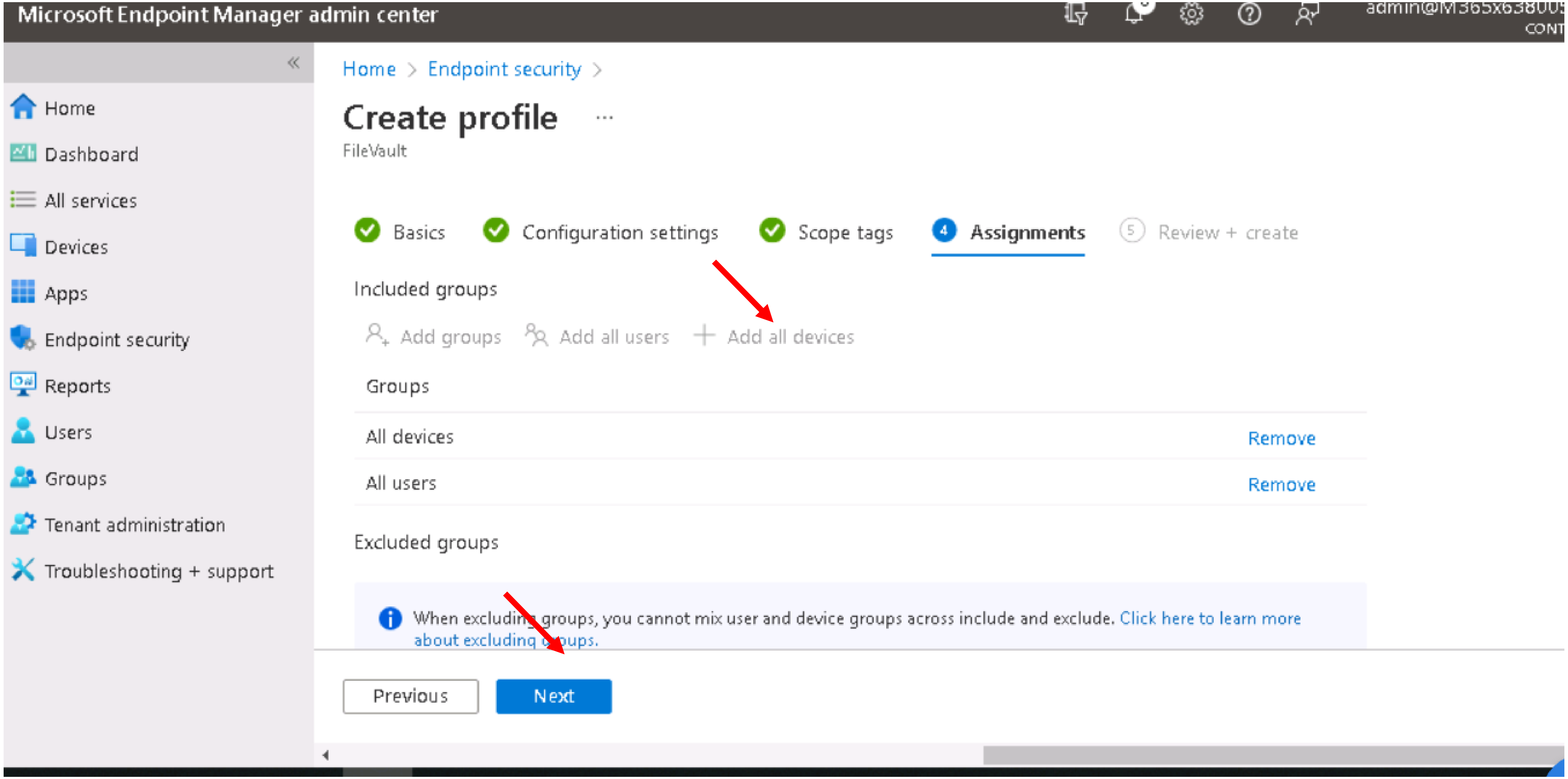


Create profile ...

FileVault

Scope tags

Scope tags
Default

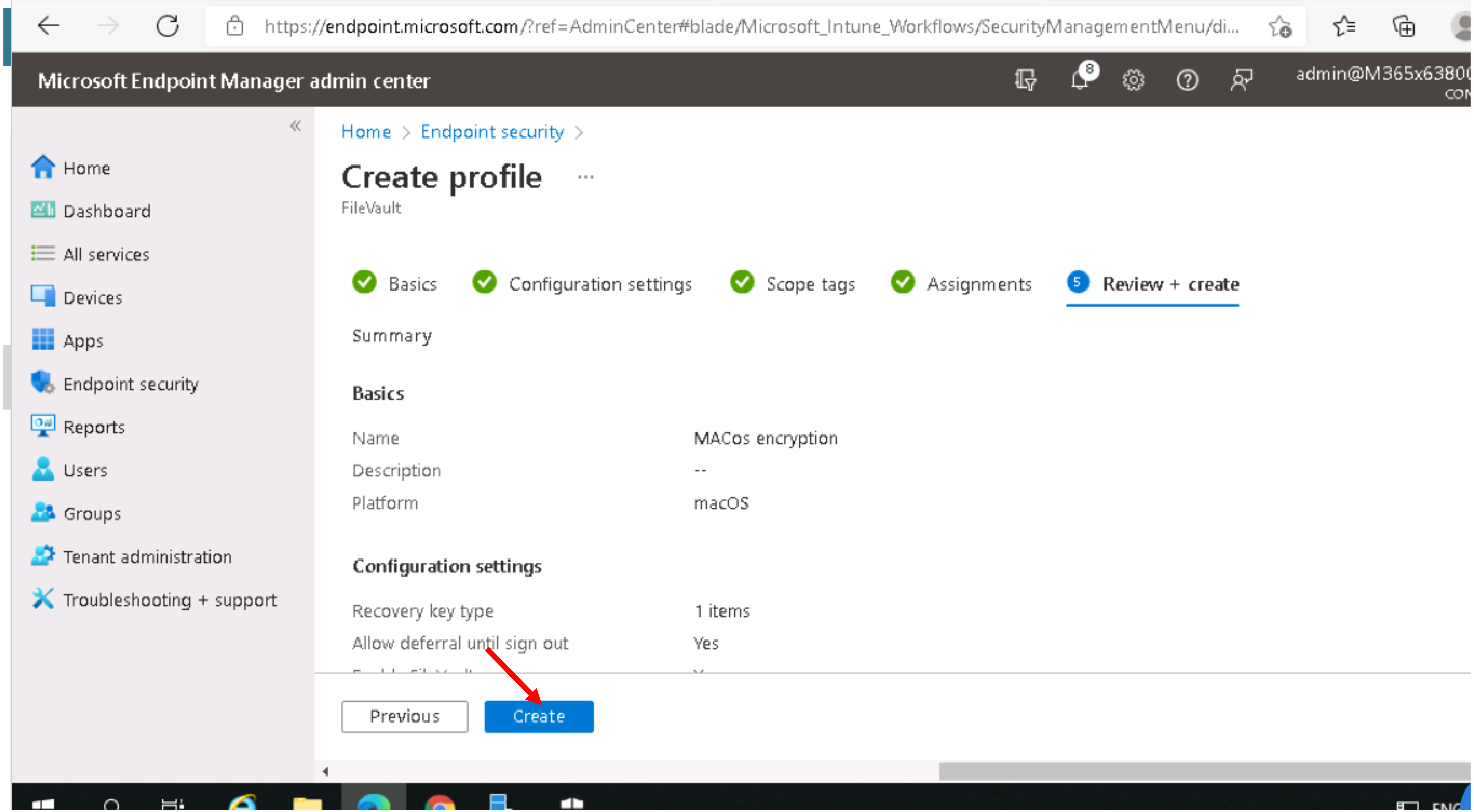


Included groups

Groups	
All devices	Remove
All users	Remove

Excluded groups

When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about excluding groups.


https://endpoint.microsoft.com/?ref=AdminCenter#blade/Microsoft_Intune_Workflows/SecurityManagementMenu/di...
Microsoft Endpoint Manager admin center
admin@M365x6380
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security >

Create profile

FileVault

✓ Basics
✓ Configuration settings
✓ Scope tags
✓ Assignments
5 Review + create

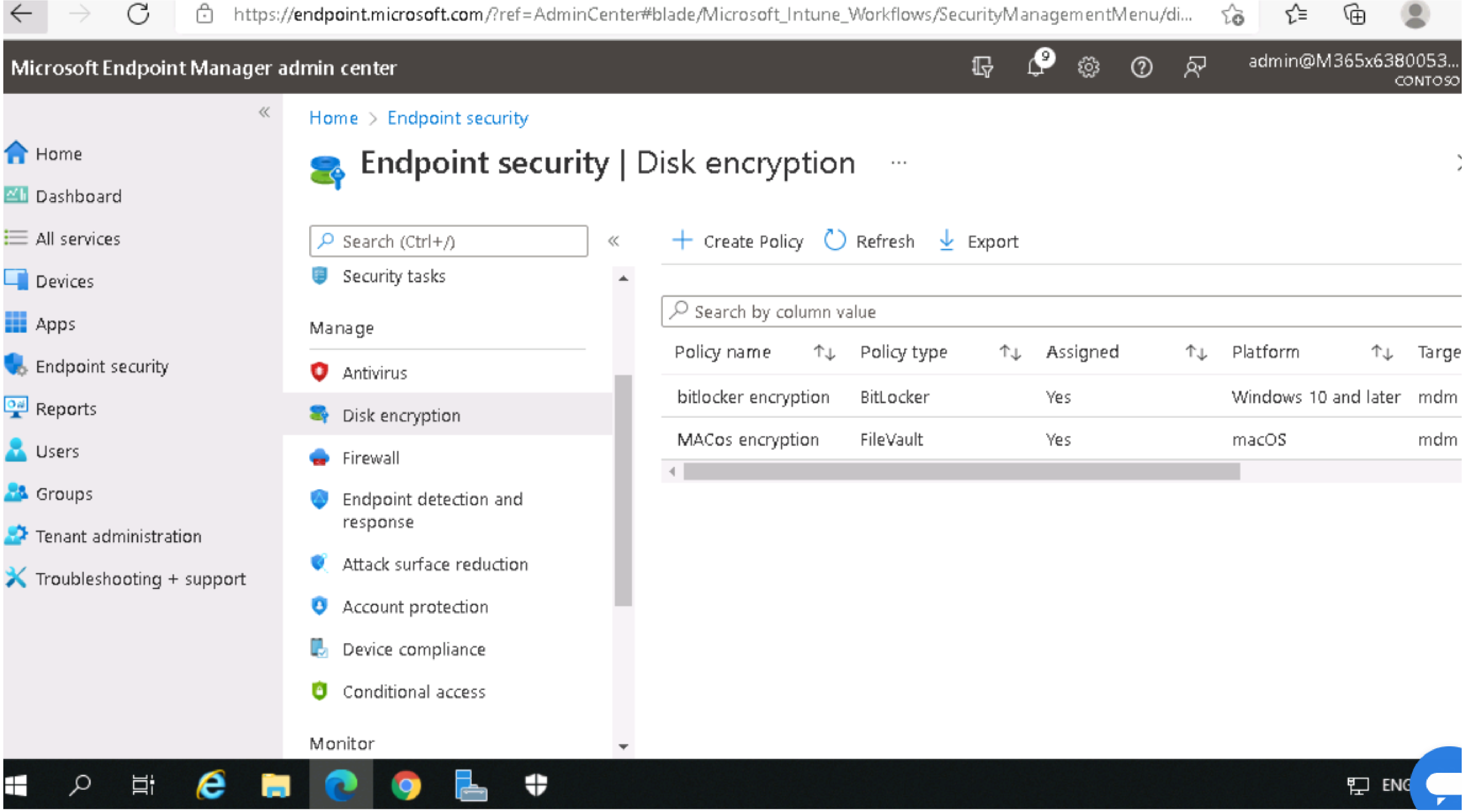
Summary

Basics

Name	MACos encryption
Description	--
Platform	macOS

Configuration settings

Recovery key type	1 items
Allow deferral until sign out	Yes



Policy name	Policy type	Assigned	Platform	Targe
bitlocker encryption	BitLocker	Yes	Windows 10 and later	mdm
MACos encryption	FileVault	Yes	macOS	mdm