Endpoint Security

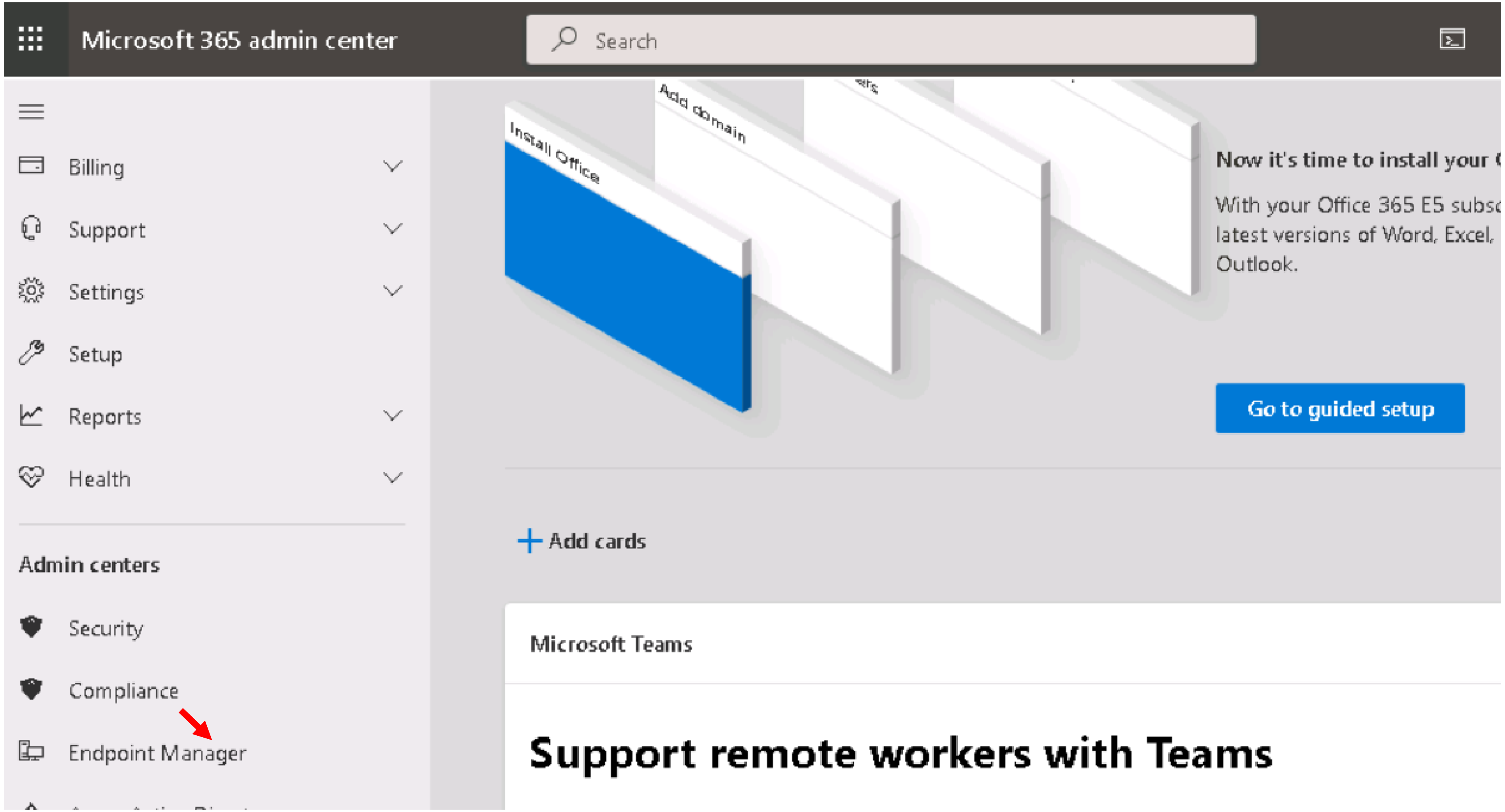
Managing Security in your Organization

With security threats multiplying and morphing daily, users expect you to keep them protected—which can be a challenge with a full-time roster of clients.

- Endpoints are one of the most common means of access for network breaches.
- How do we go about ensuring that each endpoint in your environment is protected
- To maintain effective security in your environment you need to use EDR tools. Microsoft provides Endpoint detection and response as part its Endpoint security service.

10. N- central
9. Cisco AMP for endpoints
8 Code 42
7 Paloalto network traps
6. FireEye endpoint security
5. Microsoft Endpoint for Security
4. Vmware Carbon Black
3. Sentinel One active edr
2. Envision Endpoint security
1. Sophos Intercept X

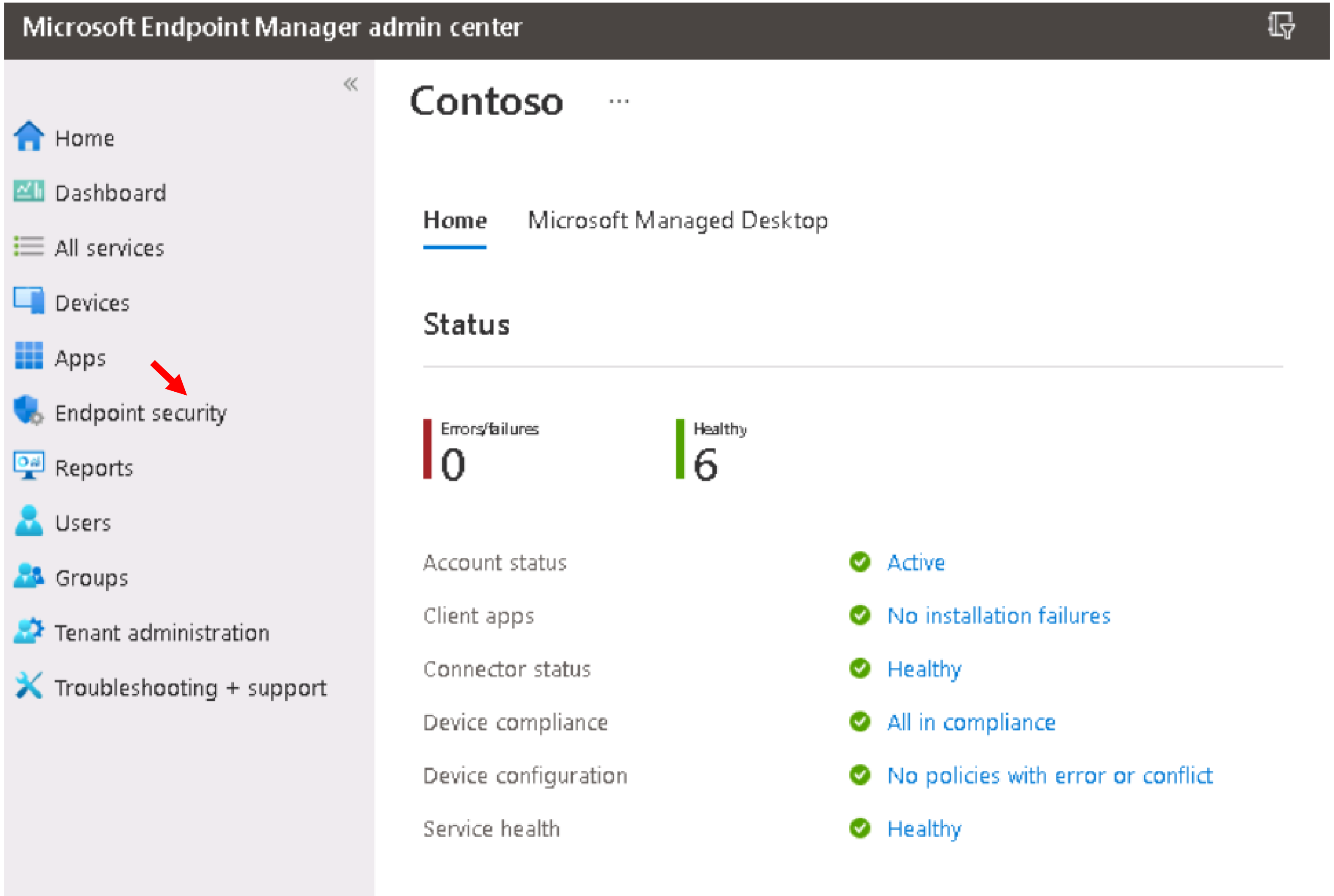
These services offers protection against a host of malware issues, ransomeware, exploits and viruses - signficant risks that companies face every day. These services range for threat hunting solutions that help you track the source of a problem remotely to exploit protection and deep learning technology. You can even set up your system to respond automatically to attacks.



Now it's time to install your (

With your Office 365 E5 subsc latest versions of Word, Excel, Outlook.

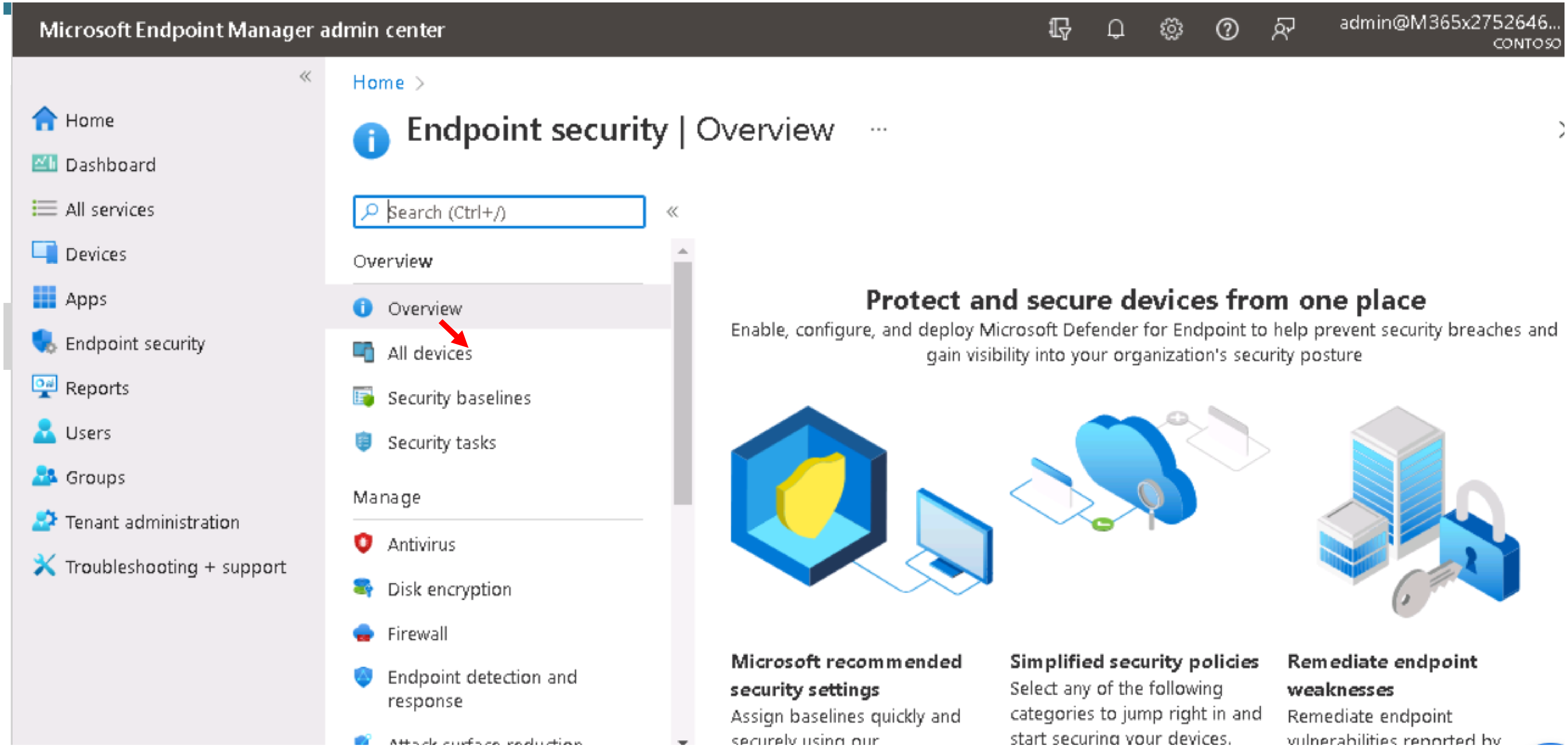
Support remote workers with Teams



Errors/failures 0

Healthy 6

Account status	Active
Client apps	No installation failures
Connector status	Healthy
Device compliance	All in compliance
Device configuration	No policies with error or conflict
Service health	Healthy



Endpoint security | Overview

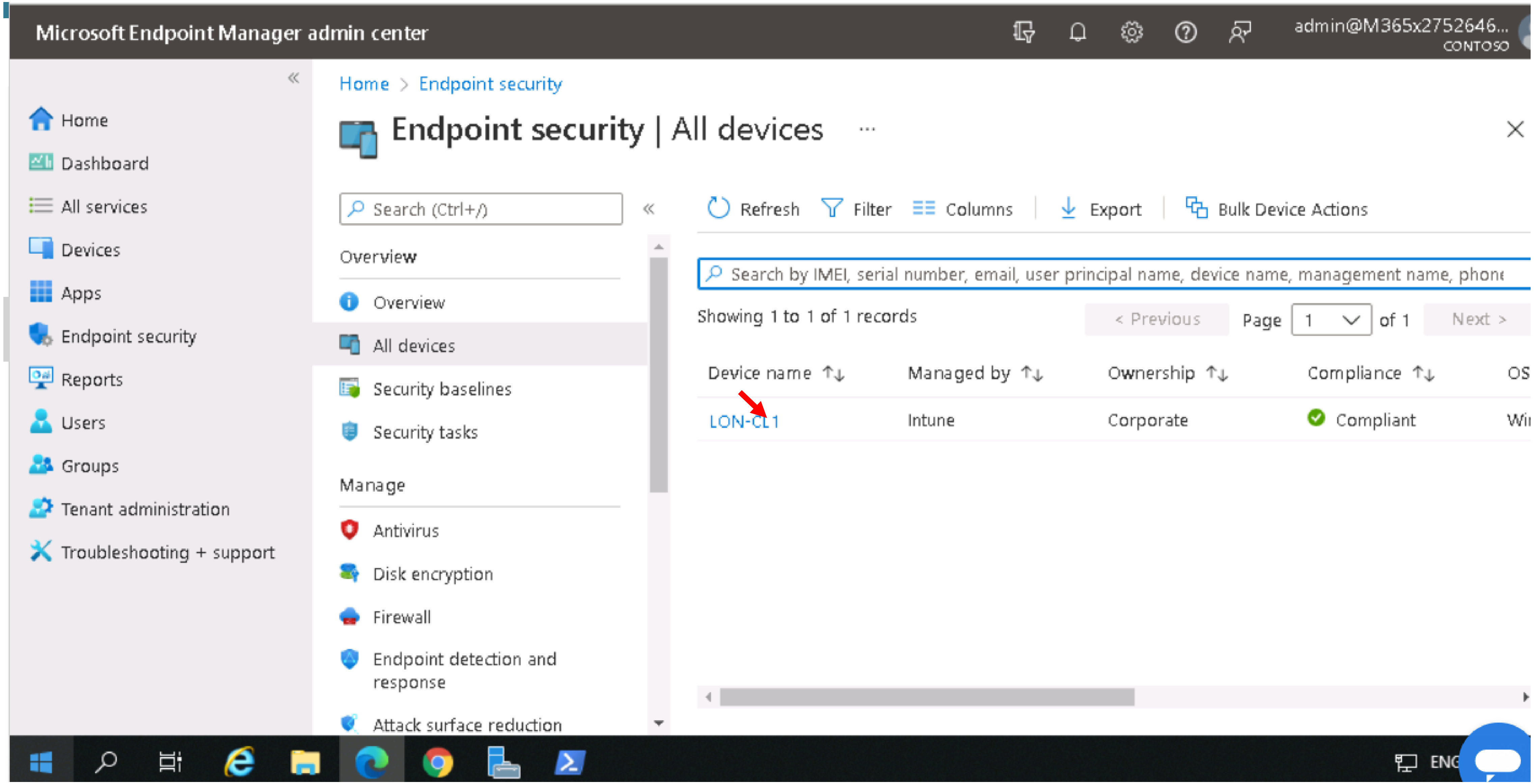
Protect and secure devices from one place

Enable, configure, and deploy Microsoft Defender for Endpoint to help prevent security breaches and 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

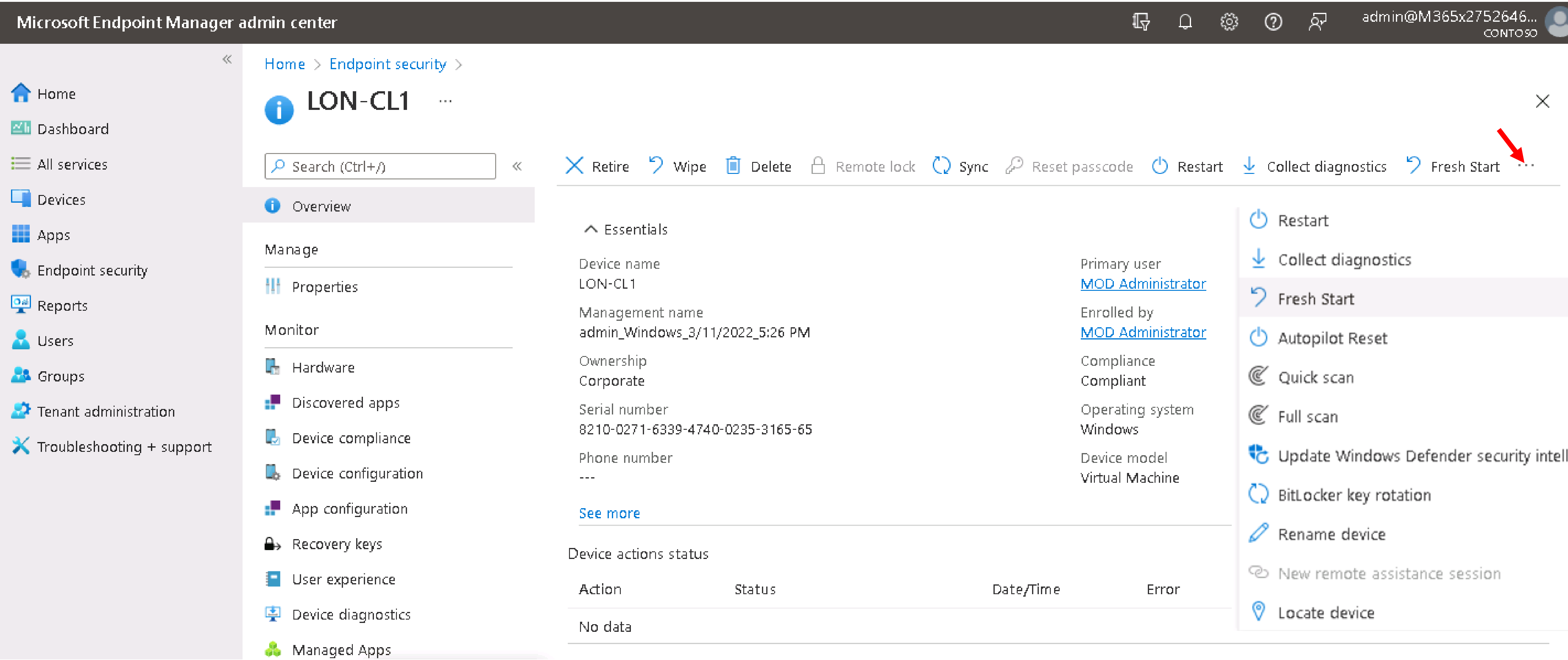


Endpoint security | All devices

Showing 1 to 1 of 1 records

Device name	Managed by	Ownership	Compliance	OS
LON-CL1	Intune	Corporate	✓ Compliant	Wi

Remote actions are actions you can start or apply to a device from the Microsoft Endpoint Manager admin center. Remote actions display across the top of the devices *Overview* page. Actions that can't display because of limited space on your screen are available by selecting the ellipsis on the right side:



Essentials

Device name
LON-CL1

Management name
admin_Windows_3/11/2022_5:26 PM

Ownership
Corporate

Serial number
8210-0271-6339-4740-0235-3165-65

Phone number

Primary user
MOD Administrator

Enrolled by
MOD Administrator

Compliance
Compliant

Operating system
Windows

Device model
Virtual Machine

Device actions status

Action	Status	Date/Time	Error
No data			

The remote actions that are available depend on how the device is managed:

- **Intune**: All Intune remote actions that apply to the device platform are available.
- **Configuration Manager**: You can use the following Configuration Manager actions:
  - Sync Machine Policy
  - Sync User Policy
  - App Evaluation Cycle
- **Co-management**: You can access both Intune remote actions and Configuration Manager actions.

Some of the Intune remote actions can help secure devices or safeguard data that might be on the device. With remote actions you can:

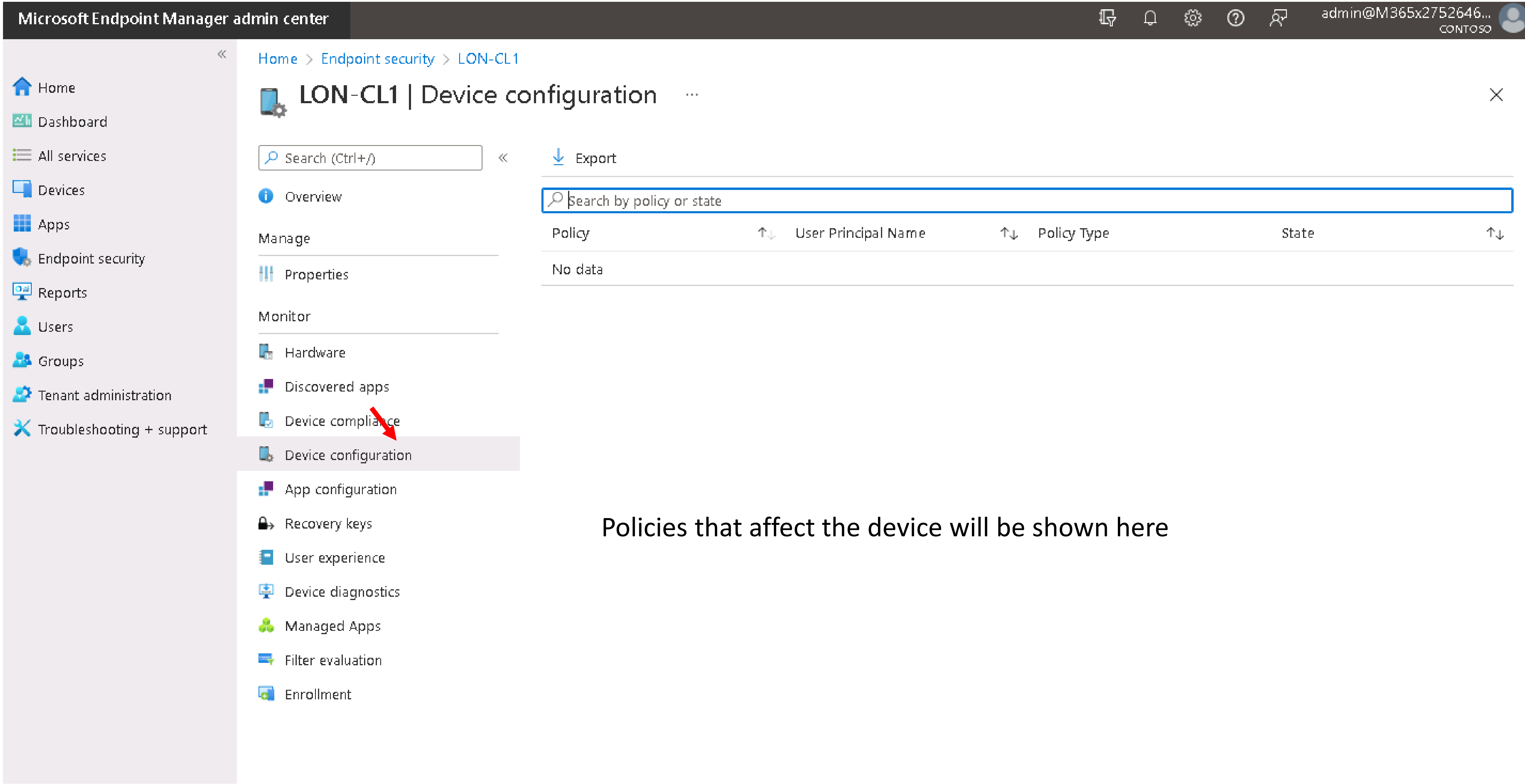
- Lock a device
- Reset a device
- Remove company data

- Scan for malware outside of a scheduled run
- Rotate BitLocker keys

The following Intune remote actions are of interest to the security admin, and are a subset of the full list. Not all actions are available for all device platforms. The links go to content that provides in-depth details for each action.

- Synchronize device – Have the device immediately check-in with Intune. When a device checks in, it receives any pending actions or policies that have been assigned to it.
- Restart – Force a Windows 10/11 device to restart, within five minutes. The device owner won't automatically be notified of the restart and might lose work.
- Quick Scan – Have Defender run a quick scan of the device for malware and then submit the results to Intune. A quick scan looks at common locations where there could be malware registered, such as registry keys and known Windows startup folders.
- Full scan – Have Defender run a scan of the device for malware and then submit the results to Intune. A full scan looks at common locations where there could be malware registered, and also scans every file and folder on the device.
- Update Windows Defender security intelligence – Have the device update its malware definitions for Microsoft Defender Antivirus. This action doesn’t start a scan.
- BitLocker key rotation – Remotely rotate the BitLocker recovery key of a device that runs Windows 10 version 1909 or later, or Windows 11.

You can also use **Bulk Device Actions** to manage some actions like *Retire* and *Wipe* for multiple devices at the same time. Bulk actions are available from the *All devices* view. You’ll select the platform, action, and then specify up to 100 devices.



Microsoft Endpoint Manager admin center

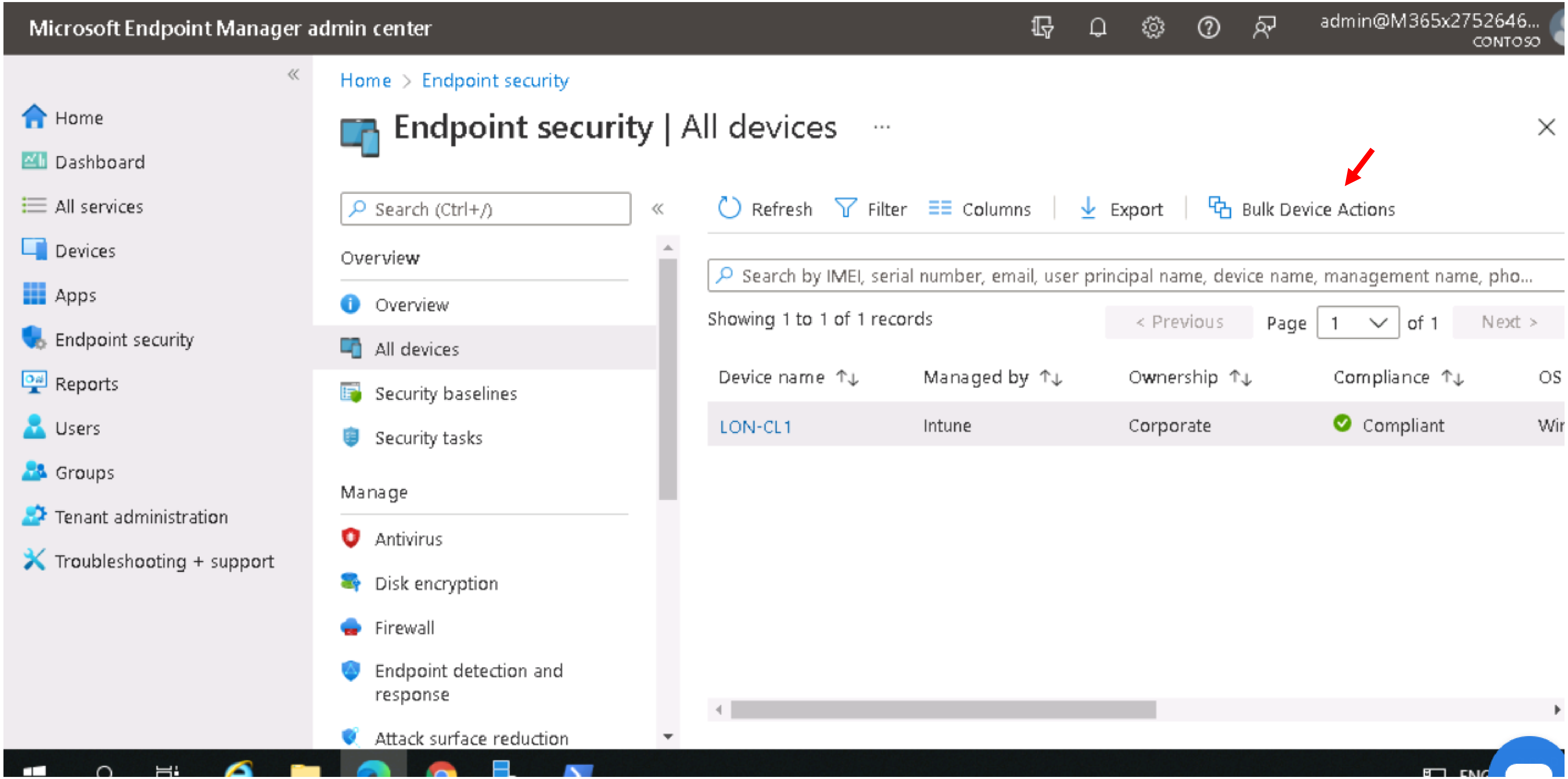
admin@M365x2752646...
CONTOSO

Home > Endpoint security > LON-CL1

LON-CL1 | Device configuration

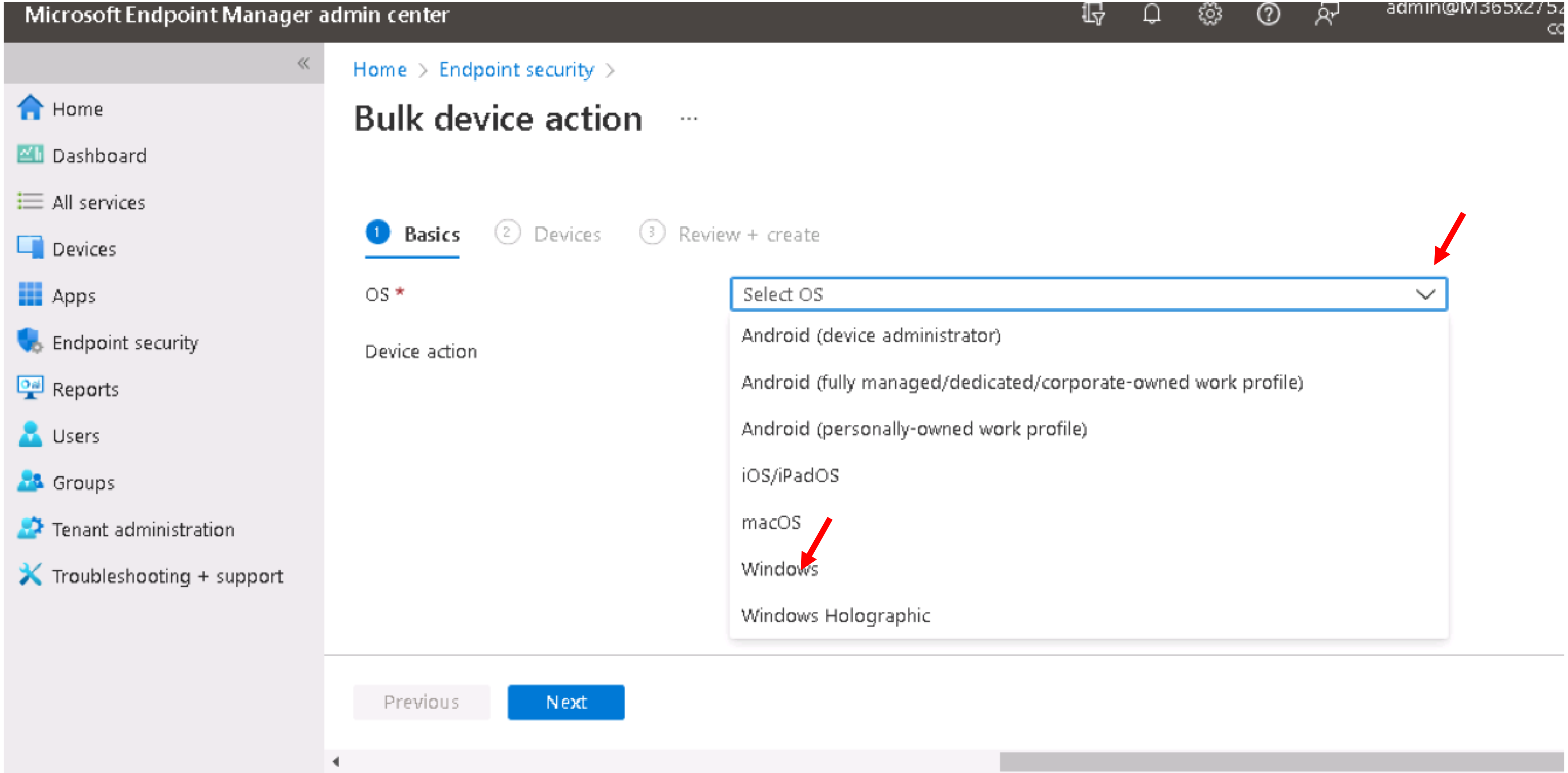
Policy	User Principal Name	Policy Type	State
No data			

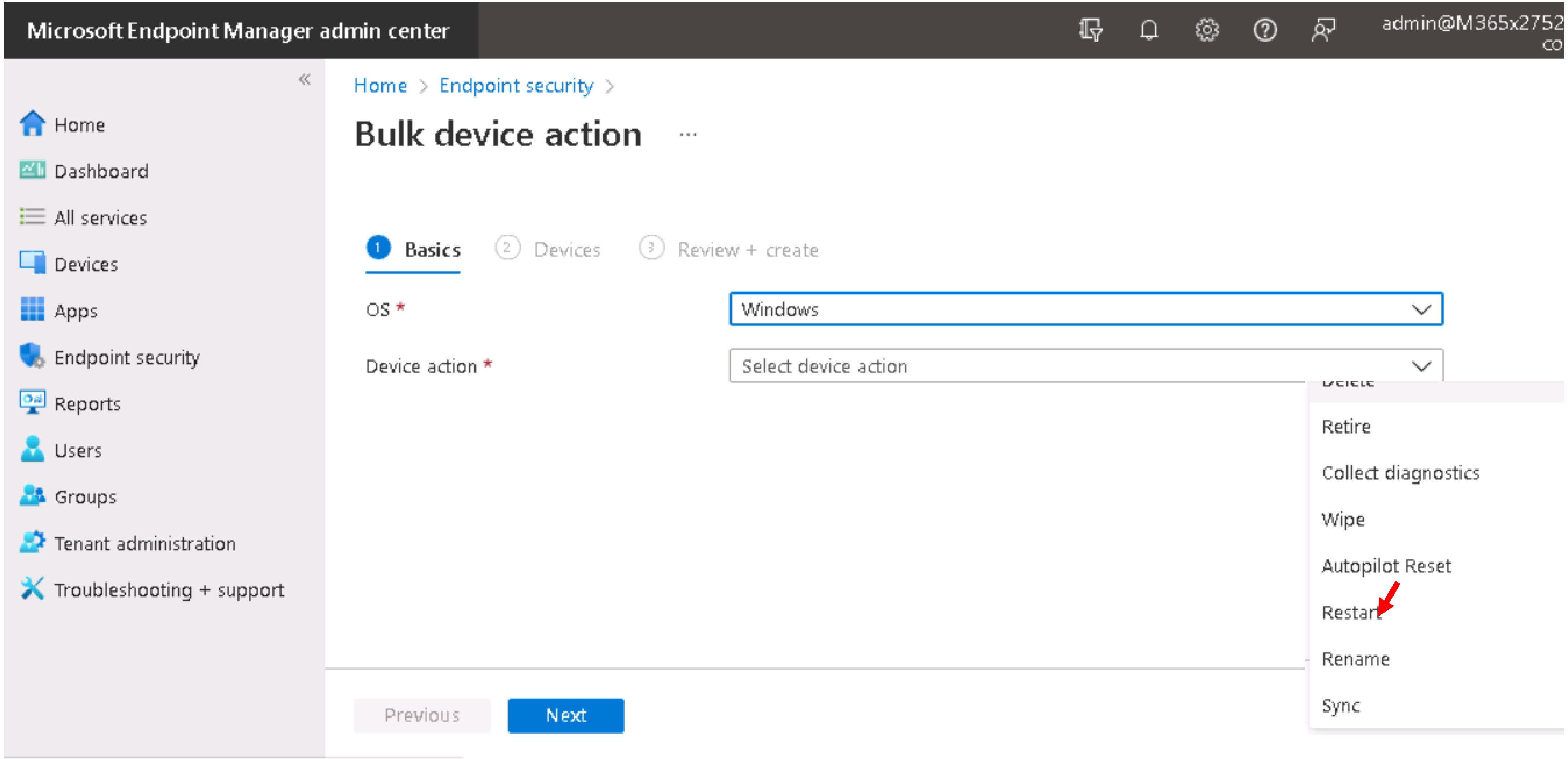
Policies that affect the device will be shown here



Showing 1 to 1 of 1 records

Device name	Managed by	Ownership	Compliance	OS
LON-CL1	Intune	Corporate	✓ Compliant	Wir


Microsoft Endpoint Manager admin center
admin@M365x2752
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security >
Bulk device action ...
1 Basics
2 Devices
3 Review + create
OS *
Select OS
Device action
Android (device administrator)
Android (fully managed/dedicated/corporate-owned work profile)
Android (personally-owned work profile)
iOS/iPadOS
macOS
Windows
Windows Holographic
Previous
Next



Microsoft Endpoint Manager admin center

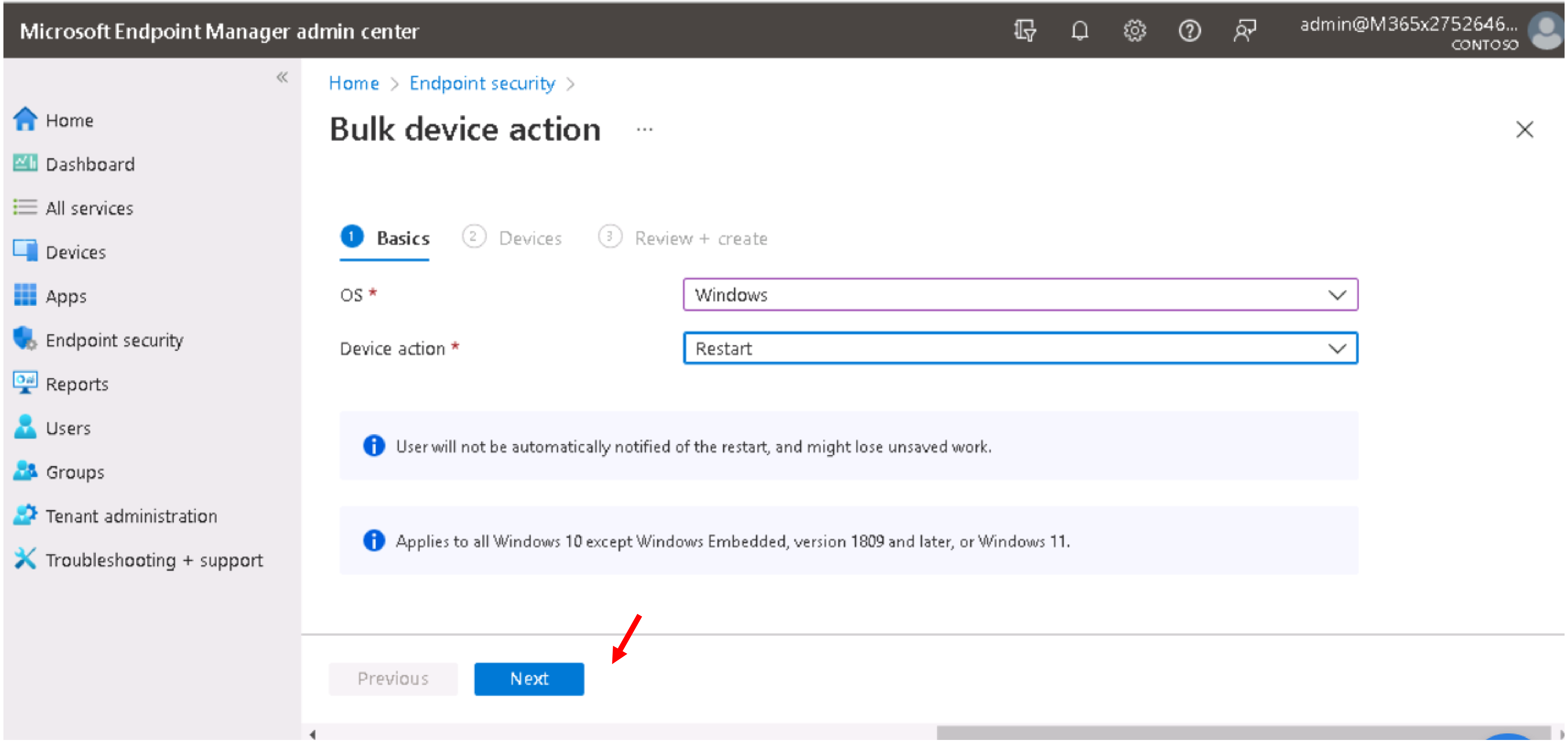
admin@M365x2752
co

Home > Endpoint security >

Bulk device action ...

OS * Windows

Device action * Select device action



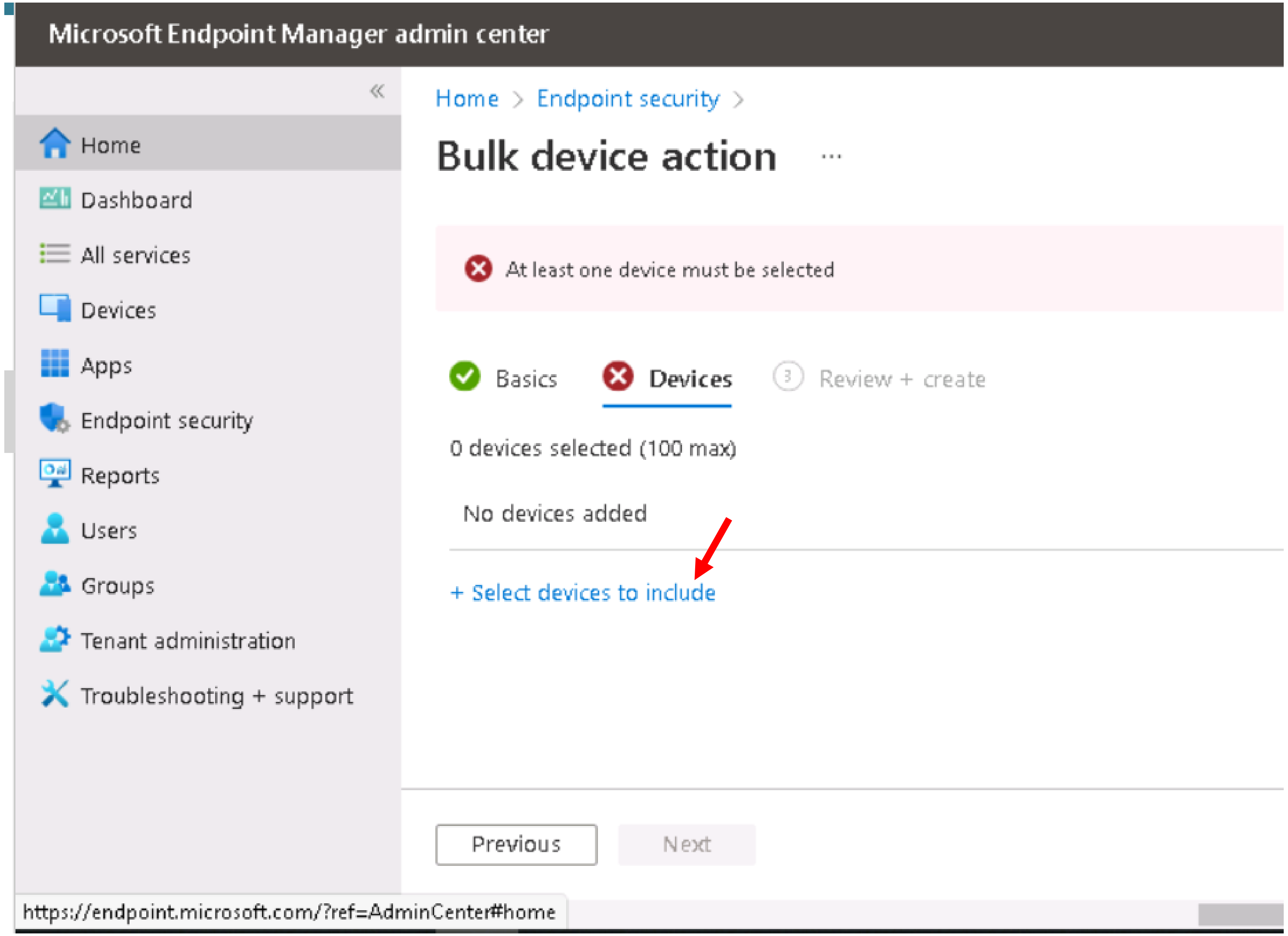
Bulk device action

OS * Windows

Device action * Restart

User will not be automatically notified of the restart, and might lose unsaved work.

Applies to all Windows 10 except Windows Embedded, version 1809 and later, or Windows 11.

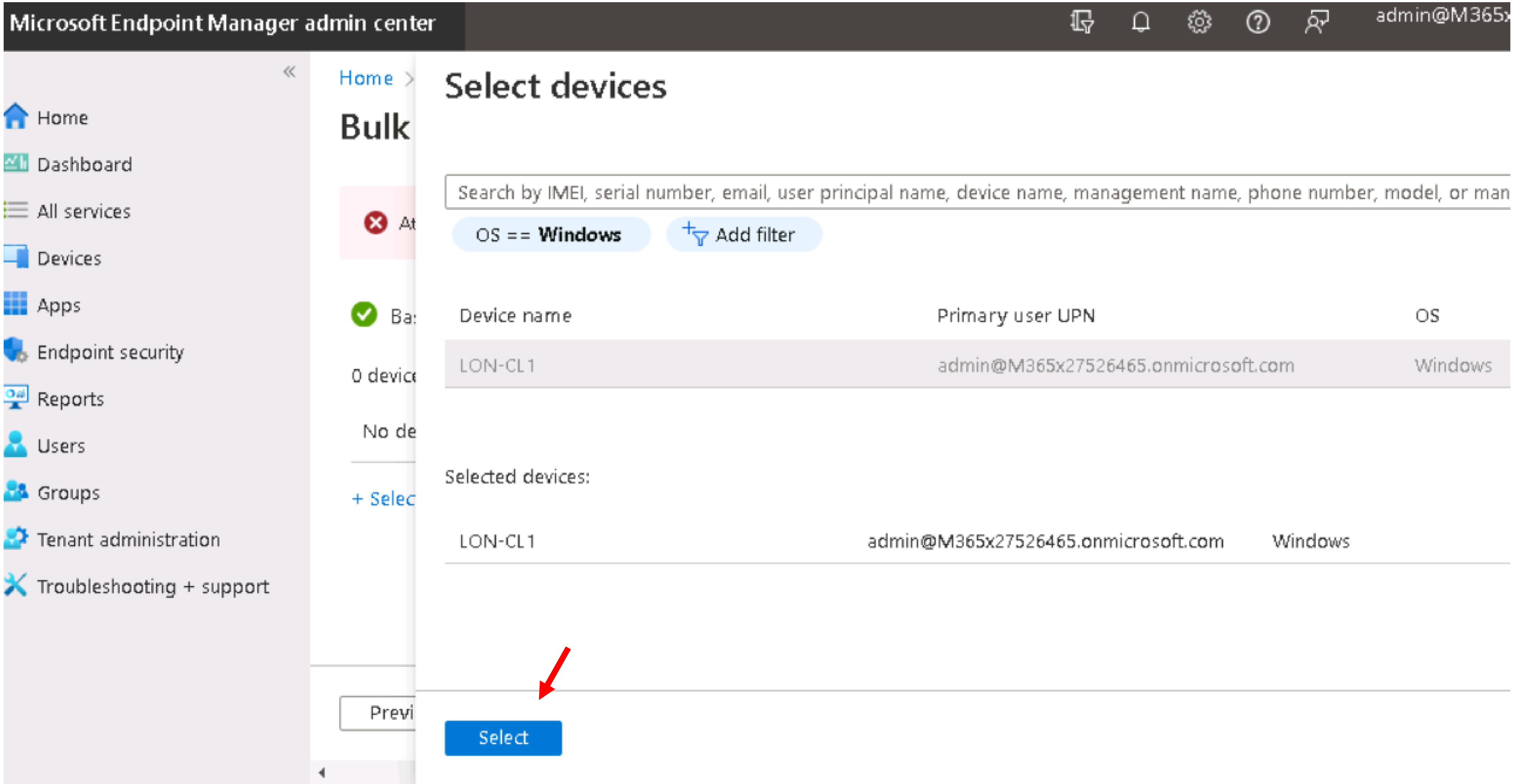


At least one device must be selected

0 devices selected (100 max)

No devices added

https://endpoint.microsoft.com/?ref=AdminCenter#home



Select devices

Search by IMEI, serial number, email, user principal name, device name, management name, phone number, model, or man

OS == **Windows**

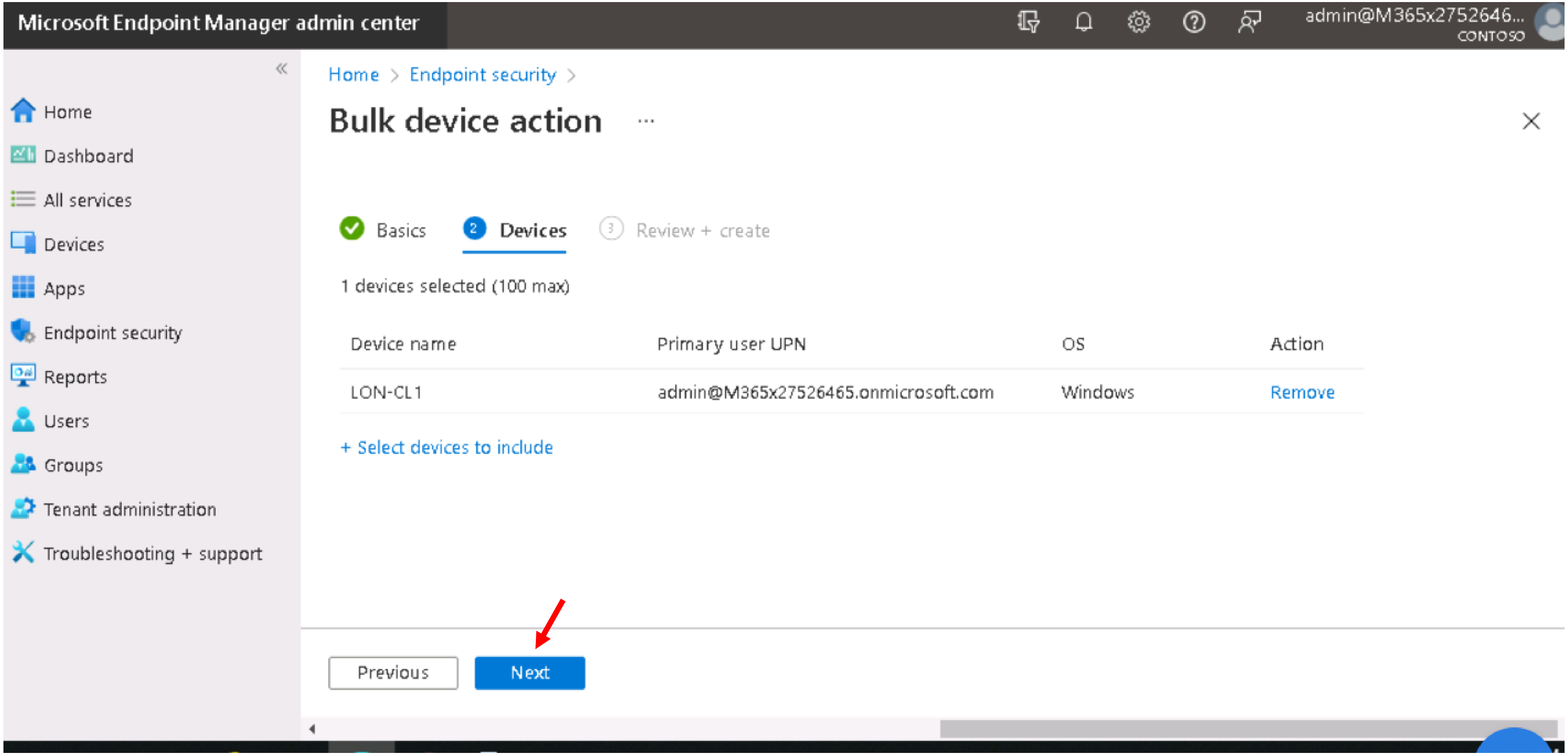
Add filter

Device name	Primary user UPN	OS
LON-CL1	admin@M365x27526465.onmicrosoft.com	Windows

Selected devices:

LON-CL1	admin@M365x27526465.onmicrosoft.com	Windows

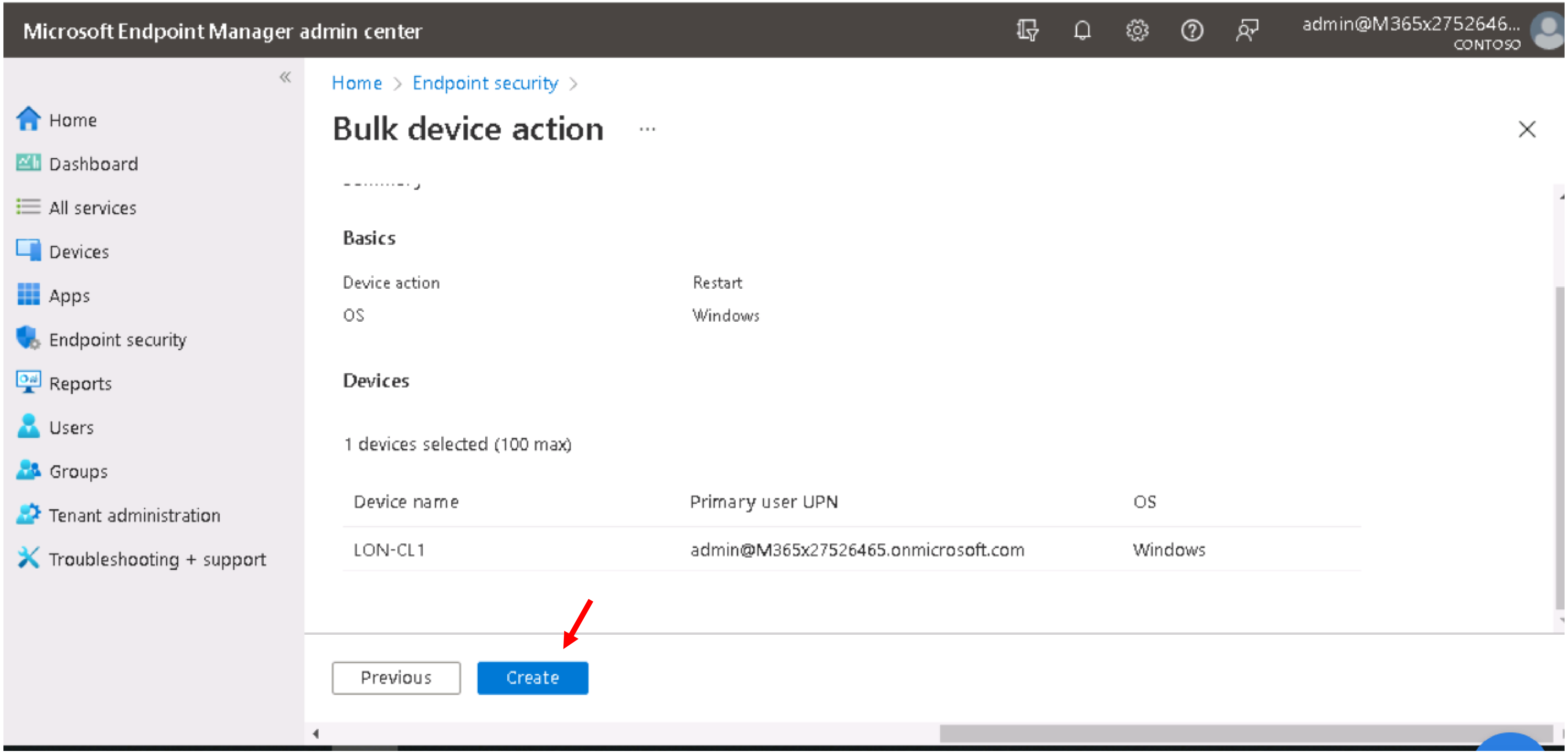
Select



Bulk device action ...

1 devices selected (100 max)

Device name	Primary user UPN	OS	Action
LON-CL1	admin@M365x27526465.onmicrosoft.com	Windows	Remove



Bulk device action

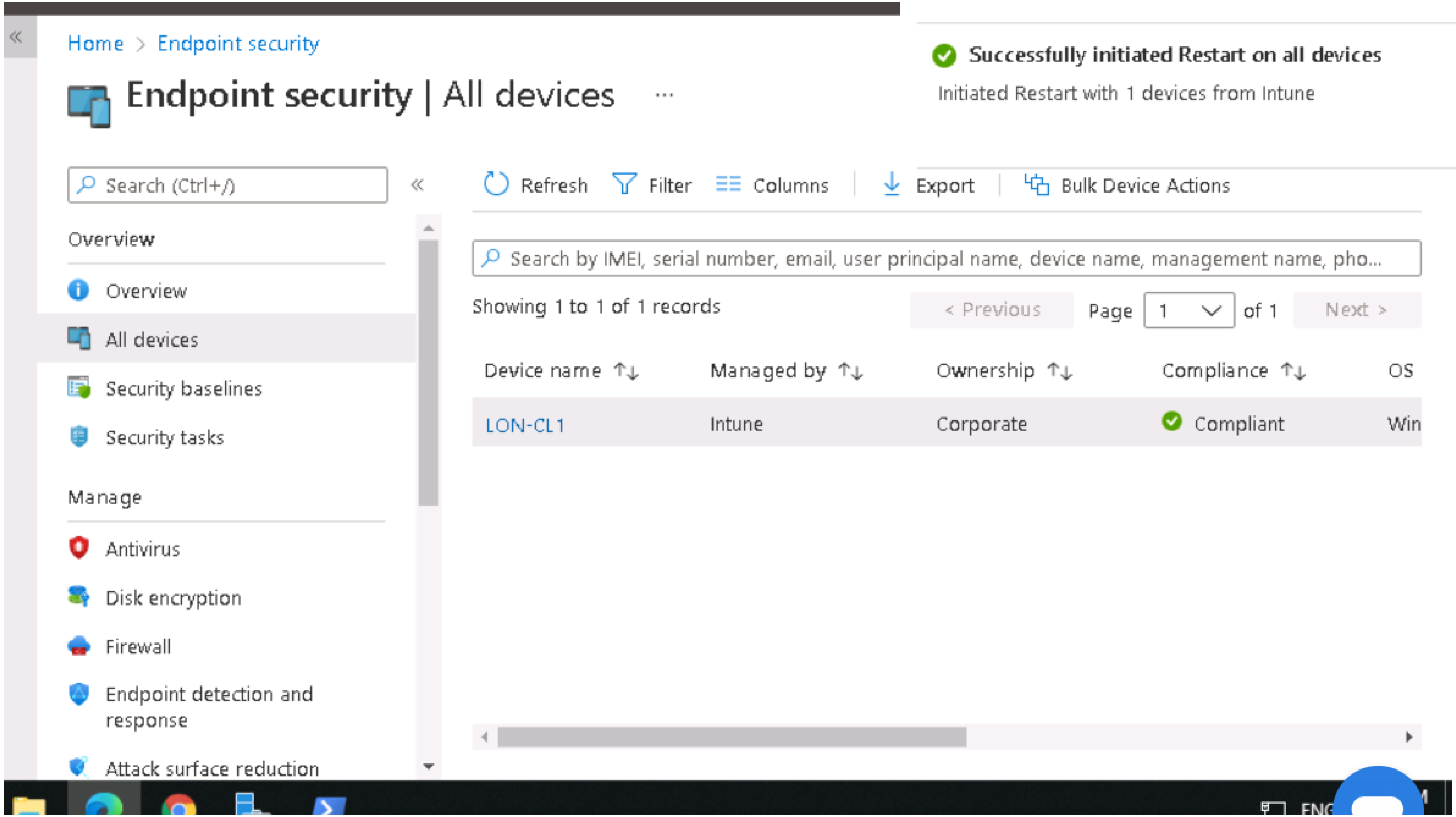
Basics

Device action	Restart
OS	Windows

Devices

1 devices selected (100 max)

Device name	Primary user UPN	OS
LON-CL1	admin@M365x27526465.onmicrosoft.com	Windows



Endpoint security | All devices ...

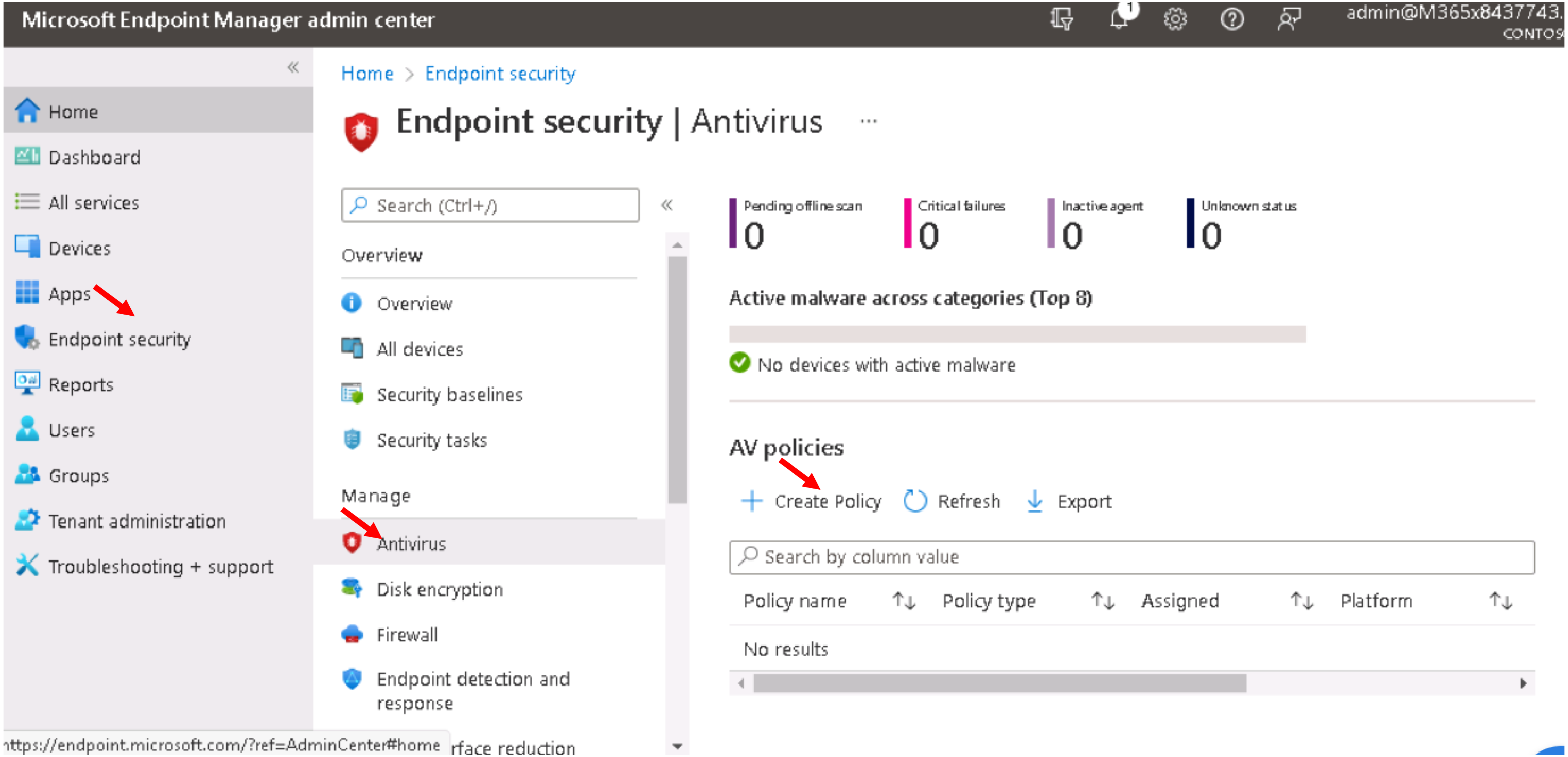
✓ **Successfully initiated Restart on all devices**

Initiated Restart with 1 devices from Intune

Showing 1 to 1 of 1 records

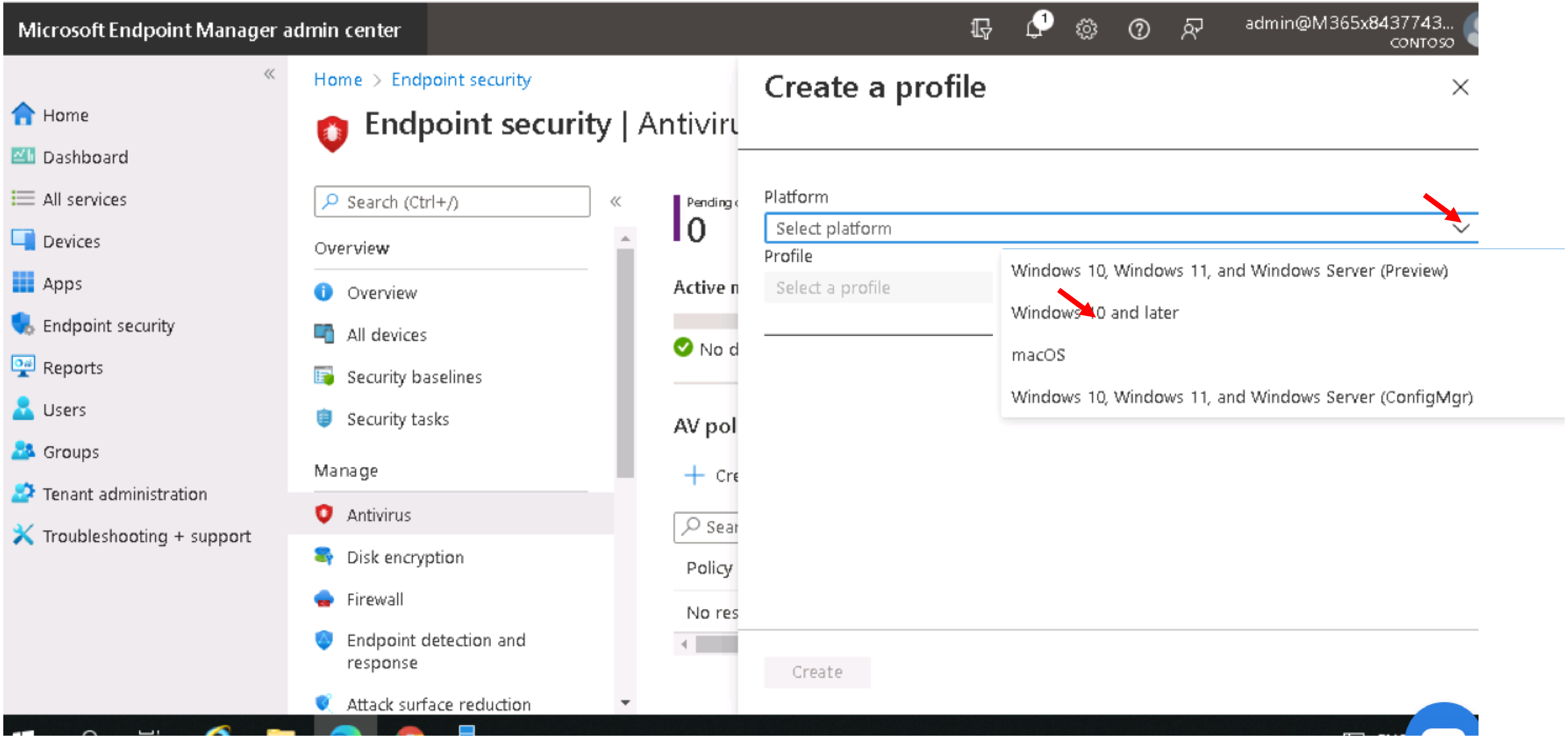
Device name ↑↓	Managed by ↑↓	Ownership ↑↓	Compliance ↑↓	OS
LON-CL1	Intune	Corporate	✓ Compliant	Win

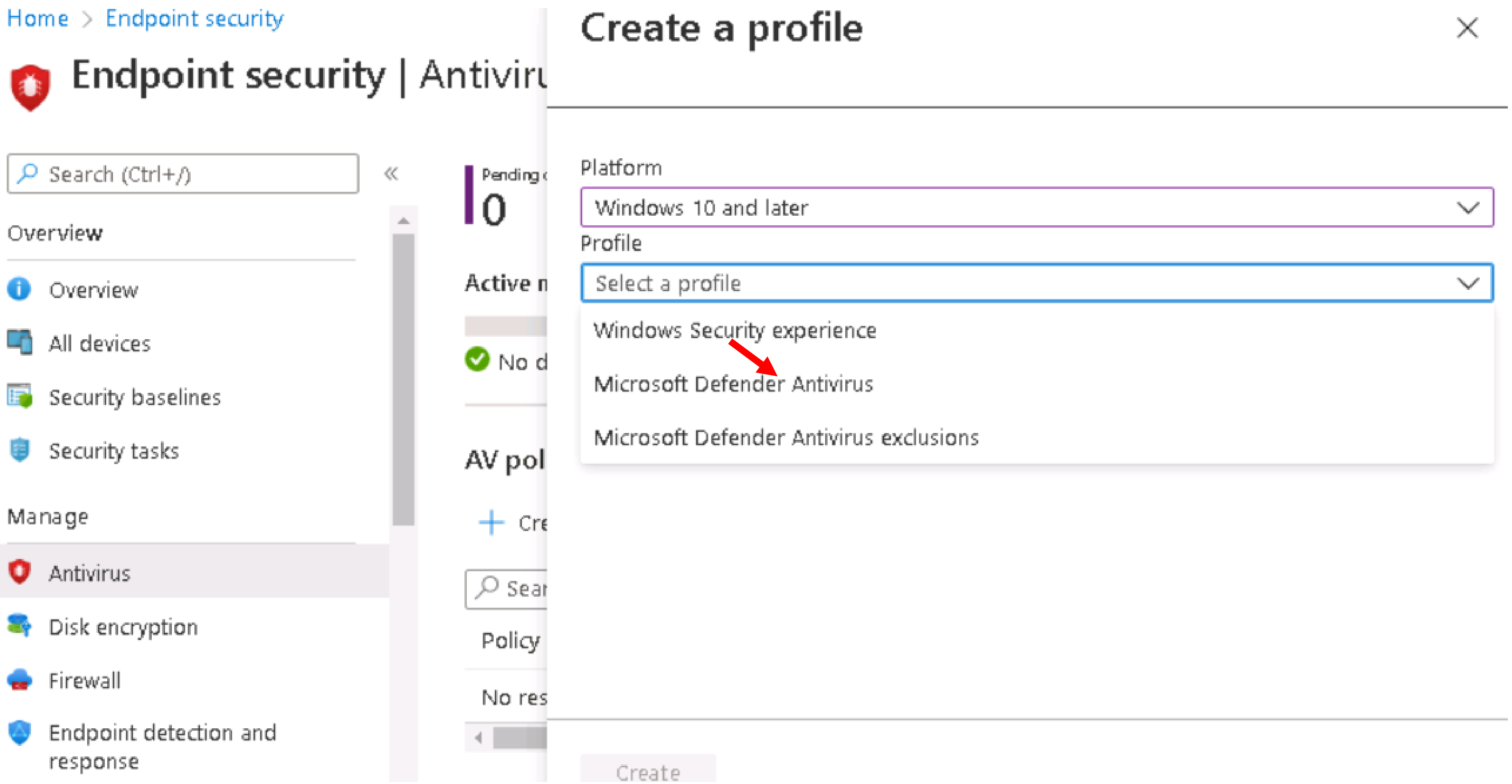
Antivirus



No devices with active malware

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


Microsoft Endpoint Manager admin center
admin@M365x8437743...
CONTOSO
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Antiviru
Search (Ctrl+/)
Overview
Overview
All devices
Security baselines
Security tasks
Manage
Antivirus
Disk encryption
Firewall
Endpoint detection and response
Attack surface reduction
Pending
0
Active m
No d
AV pol
Cre
Sear
Policy
No res
Create a profile
Platform
Select platform
Profile
Select a profile
Windows 10, Windows 11, and Windows Server (Preview)
Windows 10 and later
macOS
Windows 10, Windows 11, and Windows Server (ConfigMgr)
Create



Home > Endpoint security

Endpoint security | Antiviru

Search (Ctrl+/)

Overview

- Overview
- All devices
- Security baselines
- Security tasks

Manage

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

Pending
0

Active n

No d

AV pol

Cre

Sear

Policy

No res

Create a profile

Platform

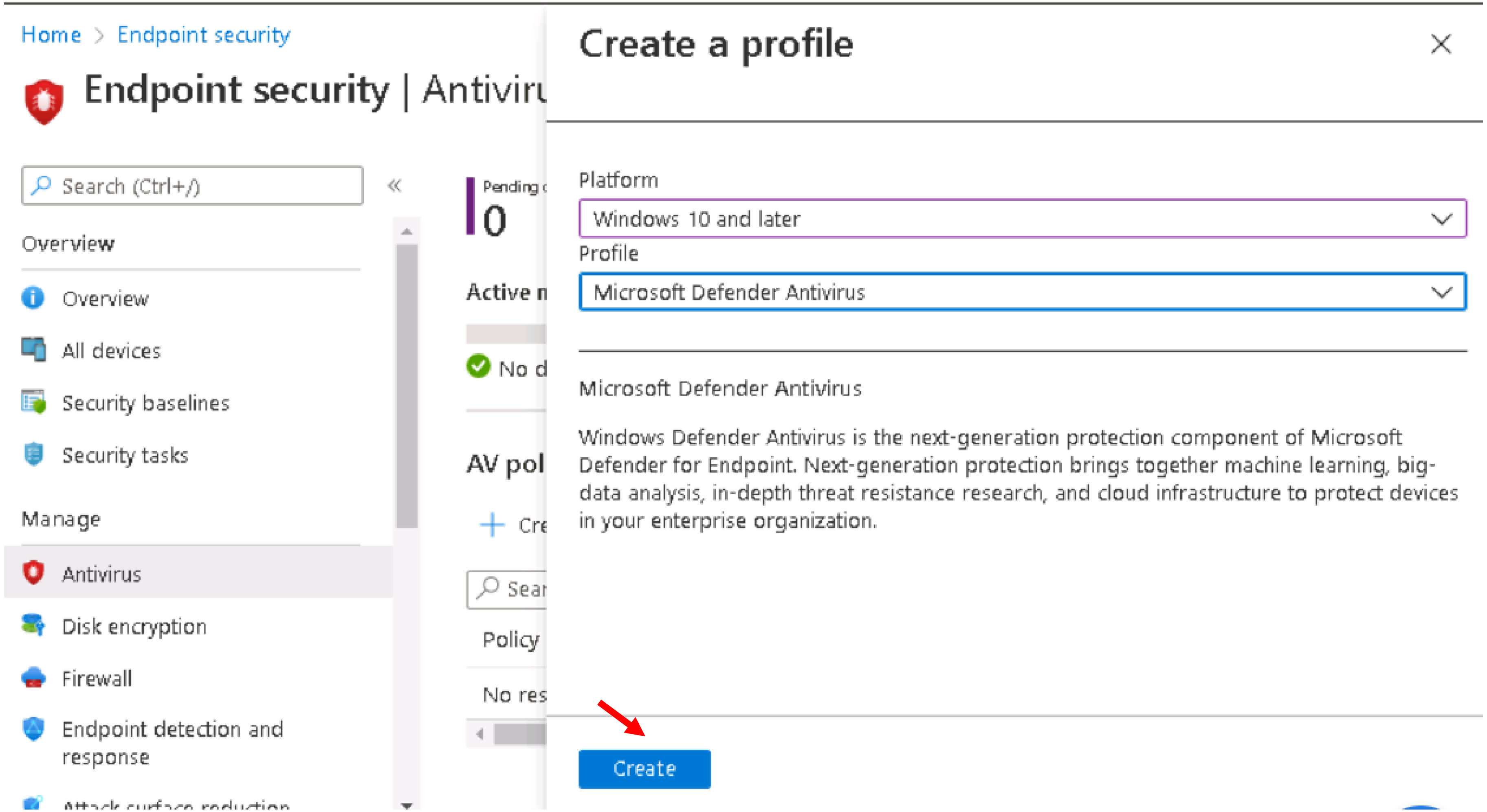
Windows 10 and later

Profile

Select a profile

- Windows Security experience
- Microsoft Defender Antivirus
- Microsoft Defender Antivirus exclusions

Create



Create a profile

Platform

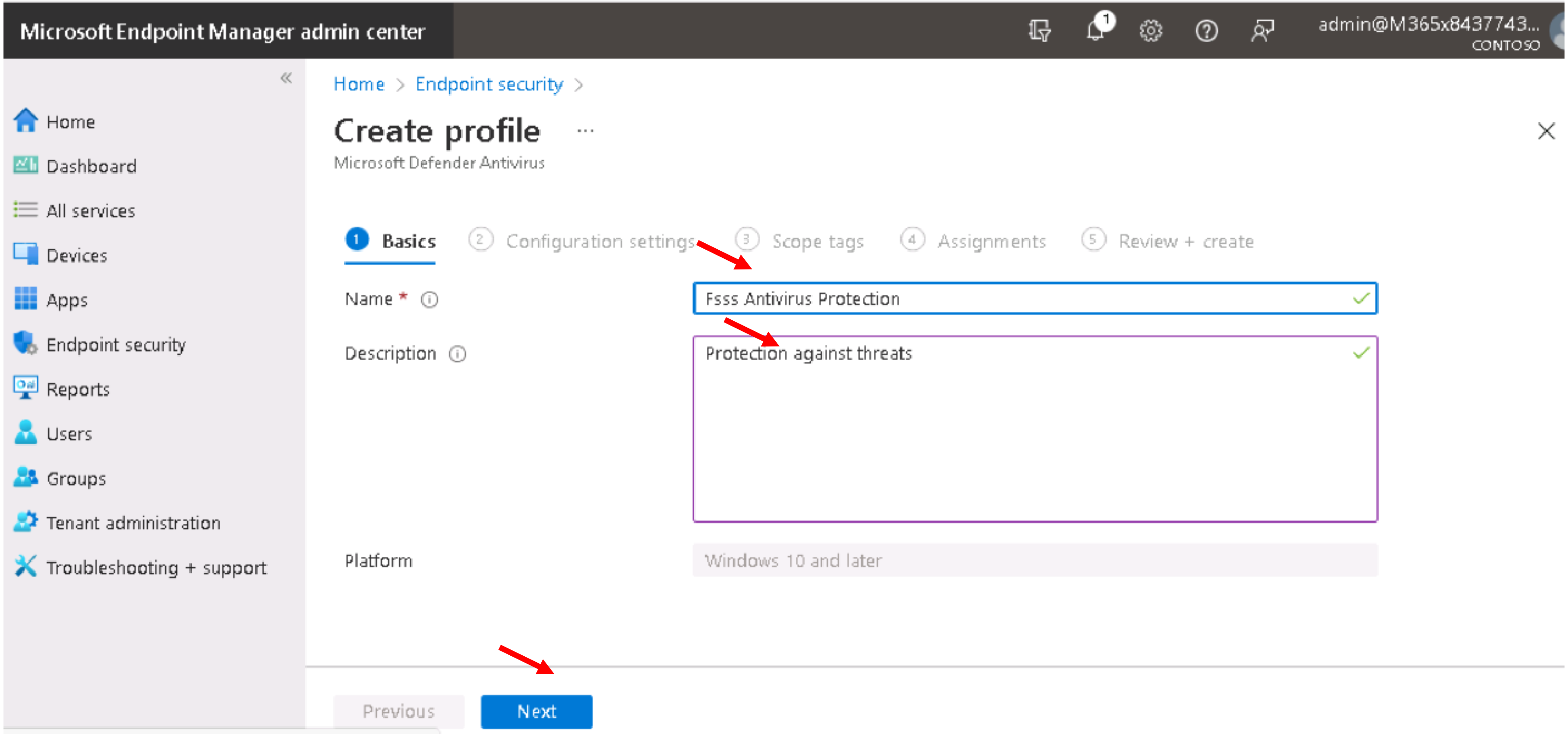
Windows 10 and later

Profile

Microsoft Defender Antivirus

Microsoft Defender Antivirus

Windows Defender Antivirus is the next-generation protection component of Microsoft Defender for Endpoint. Next-generation protection brings together machine learning, big-data analysis, in-depth threat resistance research, and cloud infrastructure to protect devices in your enterprise organization.



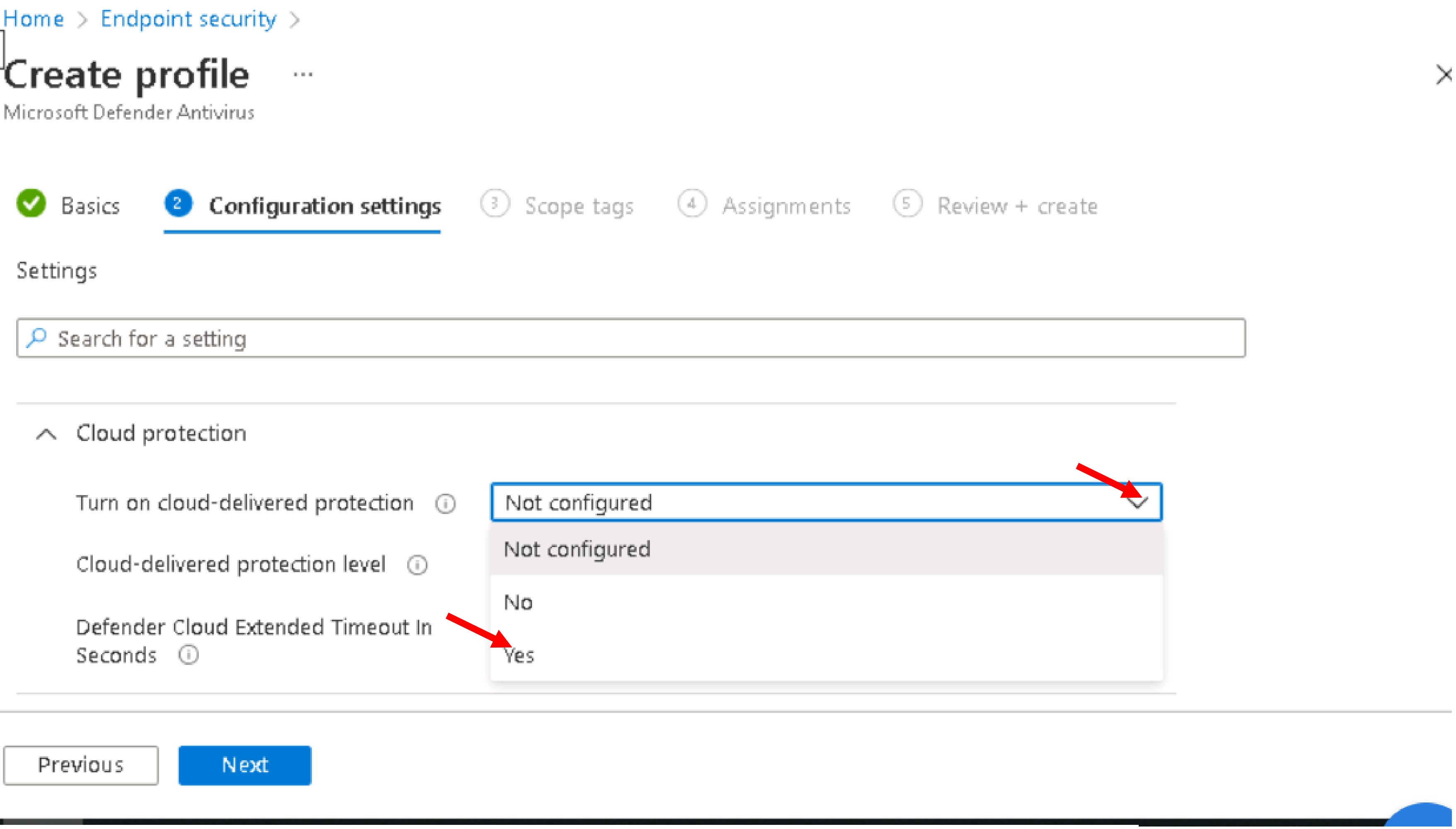
Create profile

Microsoft Defender Antivirus

Name * : Fsss Antivirus Protection

Description: Protection against threats

Platform: Windows 10 and later



Home > Endpoint security >

Create profile

Microsoft Defender Antivirus

Settings

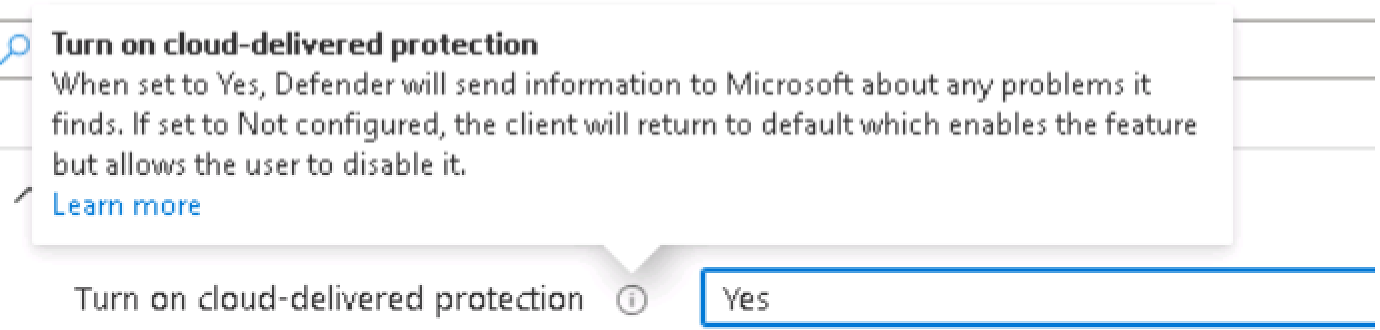
Cloud protection

Turn on cloud-delivered protection: Not configured

- Not configured
- No
- Yes

Cloud-delivered protection level

Defender Cloud Extended Timeout In Seconds

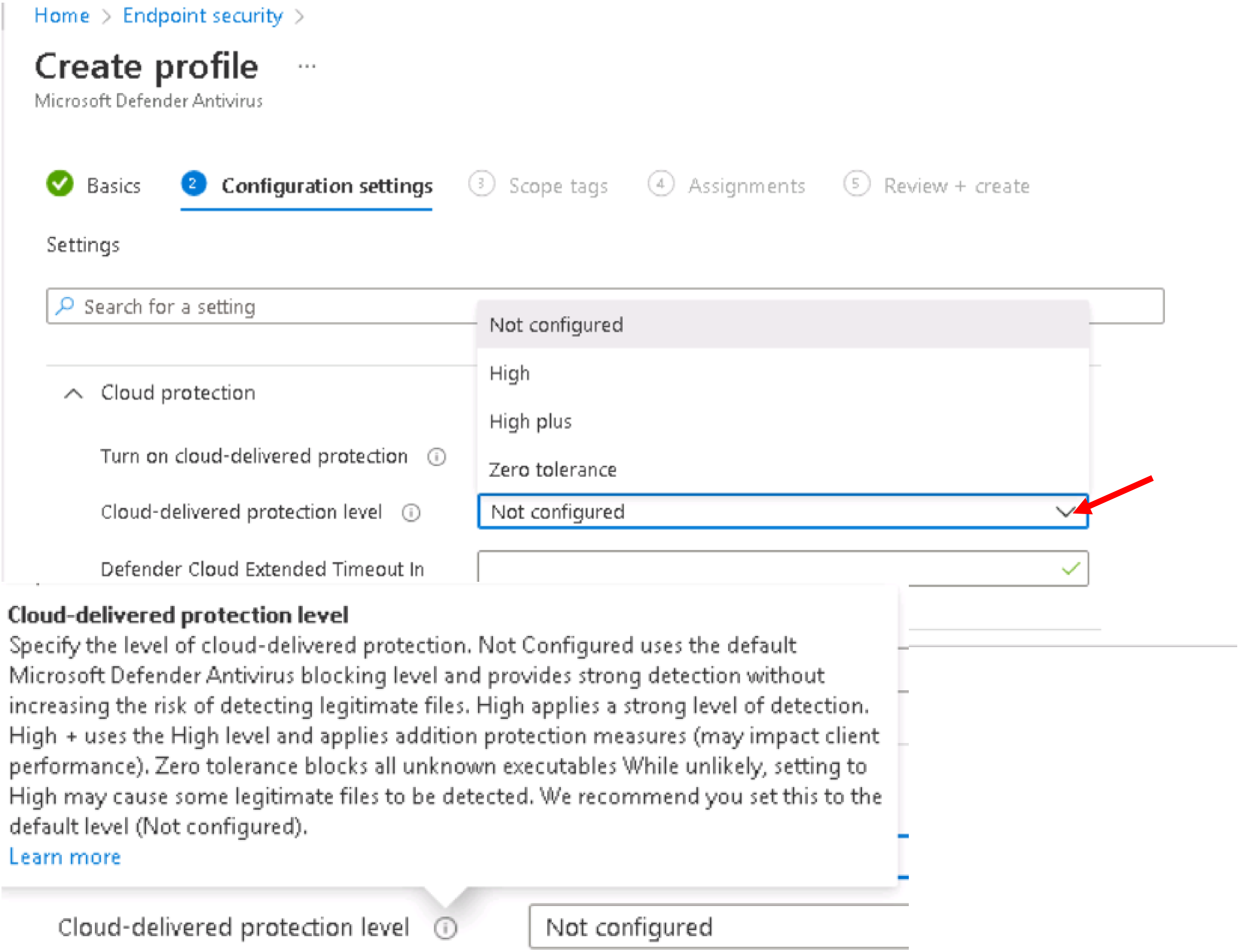


Turn on cloud-delivered protection

When set to Yes, Defender will send information to Microsoft about any problems it finds. If set to Not configured, the client will return to default which enables the feature but allows the user to disable it.

Learn more

Turn on cloud-delivered protection: Yes



Turn on cloud-delivered protection ⓘ

Cloud-delivered protection level ⓘ

- Not configured
- High
- High plus
- Zero tolerance

Not configured

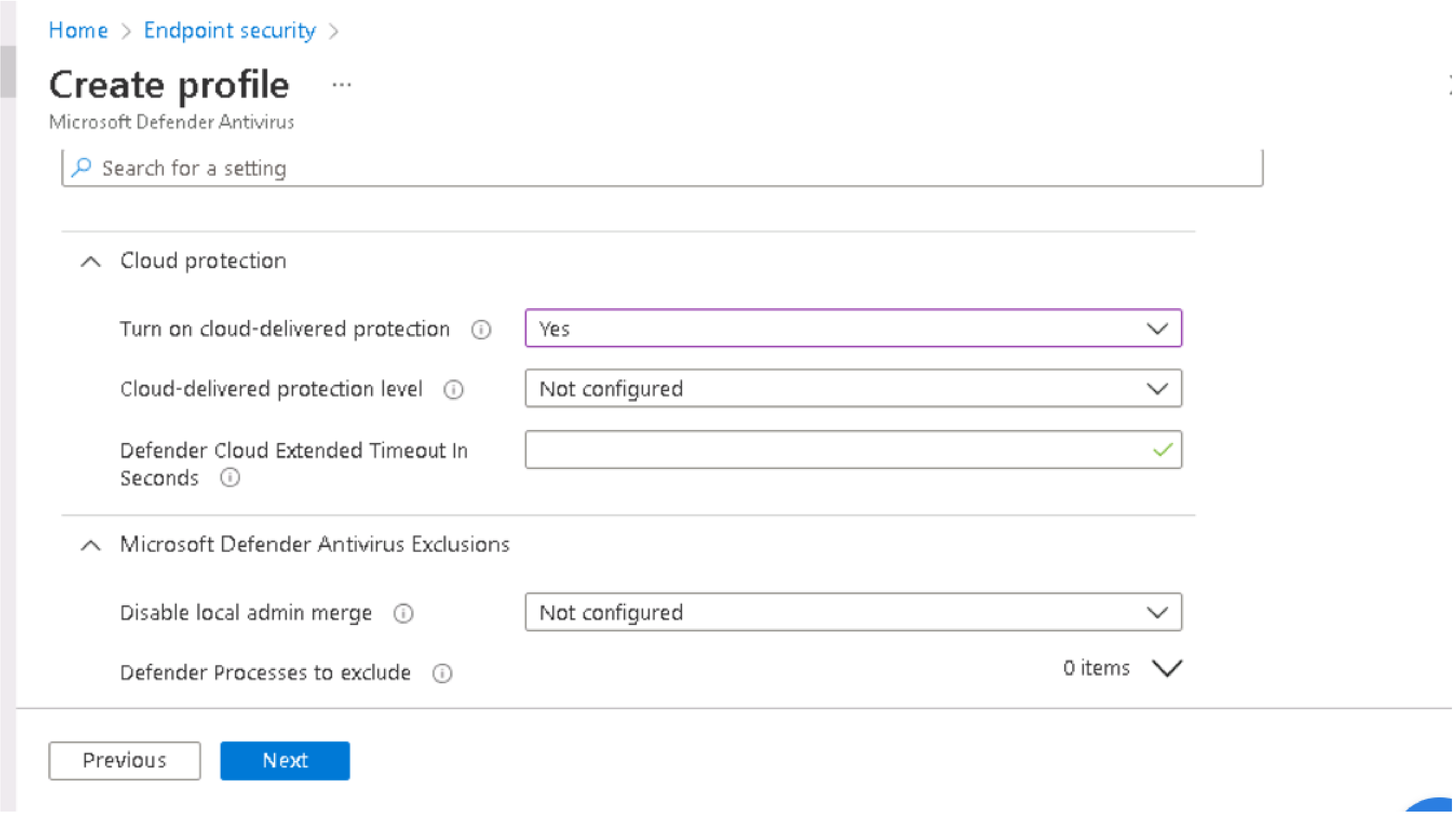
Defender Cloud Extended Timeout In ✓

Cloud-delivered protection level

Specify the level of cloud-delivered protection. Not Configured uses the default Microsoft Defender Antivirus blocking level and provides strong detection without increasing the risk of detecting legitimate files. High applies a strong level of detection. High + uses the High level and applies addition protection measures (may impact client performance). Zero tolerance blocks all unknown executables While unlikely, setting to High may cause some legitimate files to be detected. We recommend you set this to the default level (Not configured).

Learn more

Cloud-delivered protection level ⓘ Not configured



Create profile

Microsoft Defender Antivirus

Cloud protection

Turn on cloud-delivered protection: Yes

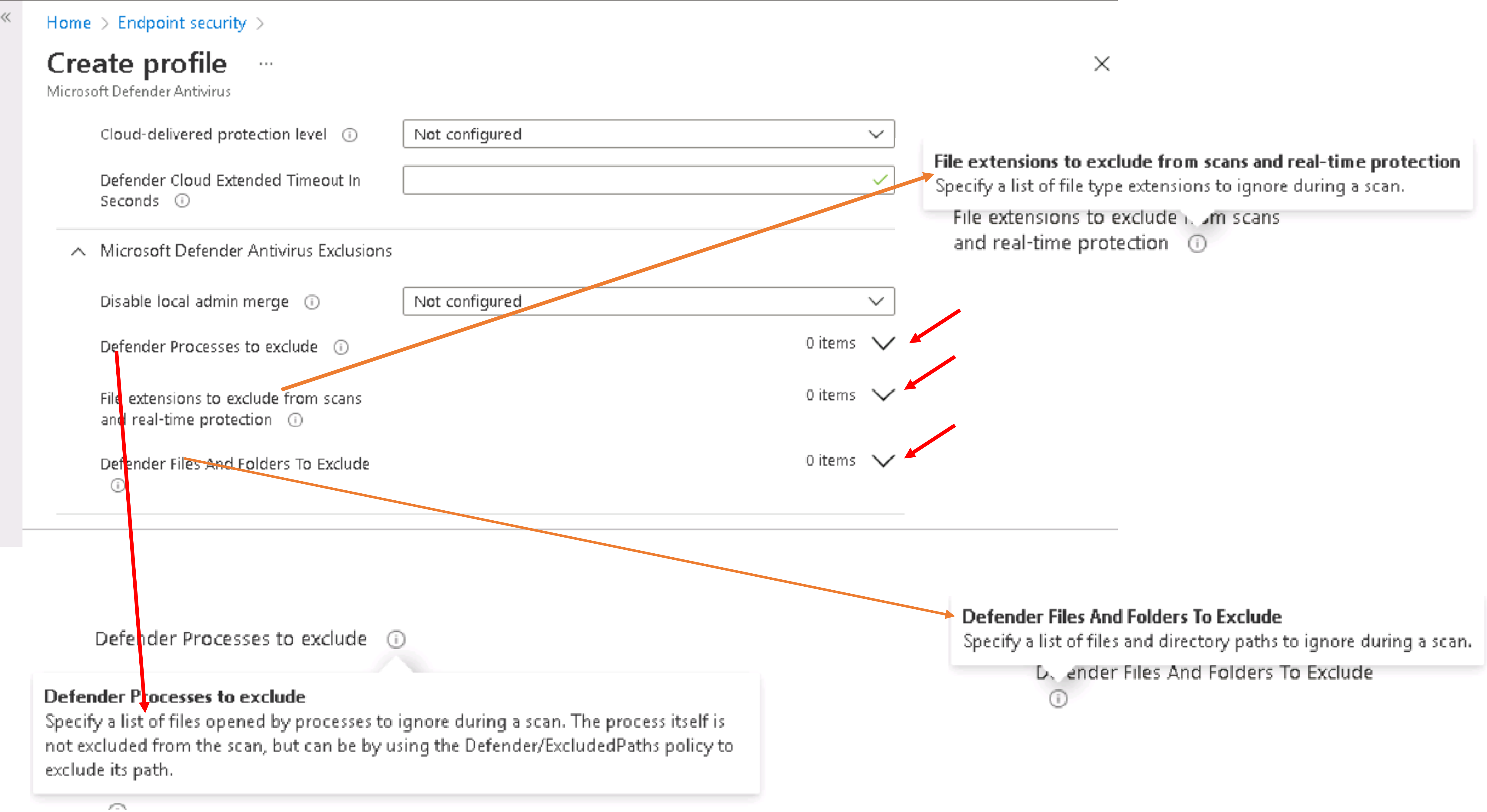
Cloud-delivered protection level: Not configured

Defender Cloud Extended Timeout In Seconds: ✓

Microsoft Defender Antivirus Exclusions

Disable local admin merge: Not configured

Defender Processes to exclude: 0 items



Home > Endpoint security >

Create profile ...

Microsoft Defender Antivirus

Cloud-delivered protection level ⓘ Not configured

Defender Cloud Extended Timeout In Seconds ⓘ

Microsoft Defender Antivirus Exclusions

Disable local admin merge ⓘ Not configured

Defender Processes to exclude ⓘ 0 items

File extensions to exclude from scans and real-time protection ⓘ 0 items

Defender Files And Folders To Exclude ⓘ 0 items

File extensions to exclude from scans and real-time protection
Specify a list of file type extensions to ignore during a scan.

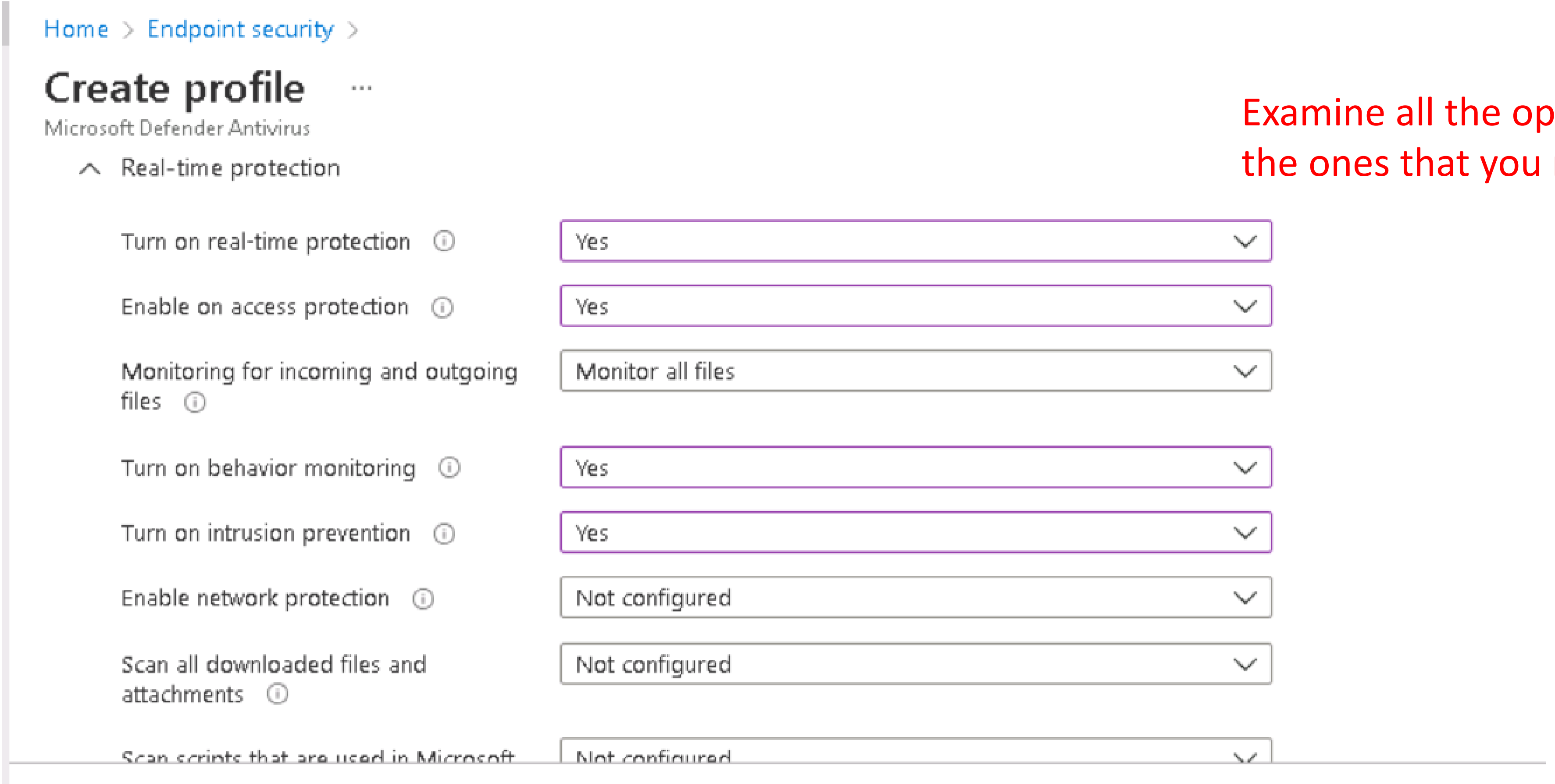
File extensions to exclude ı. ɔm scans and real-time protection ⓘ

Defender Files And Folders To Exclude
Specify a list of files and directory paths to ignore during a scan.

D. ender Files And Folders To Exclude ⓘ

Defender Processes to exclude ⓘ

Defender Processes to exclude
Specify a list of files opened by processes to ignore during a scan. The process itself is not excluded from the scan, but can be by using the Defender/ExcludedPaths policy to exclude its path.



Home > Endpoint security >

Create profile ...

Microsoft Defender Antivirus

Real-time protection

Turn on real-time protection: Yes

Enable on access protection: Yes

Monitoring for incoming and outgoing files: Monitor all files

Turn on behavior monitoring: Yes

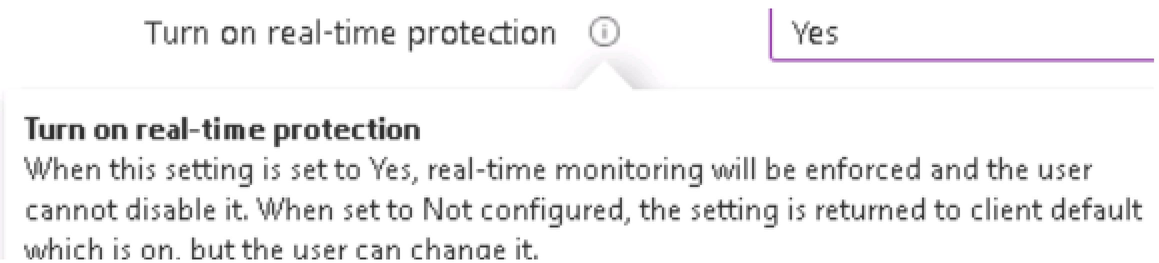
Turn on intrusion prevention: Yes

Enable network protection: Not configured

Scan all downloaded files and attachments: Not configured

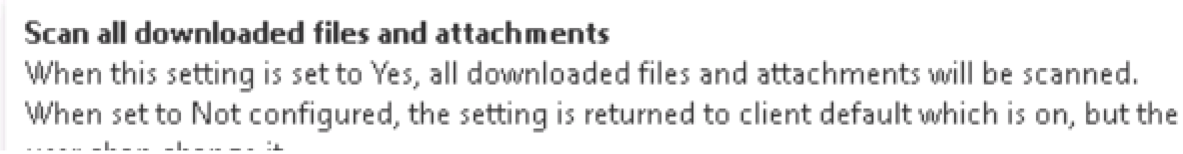
Scan scripts that are used in Microsoft: Not configured

Examine all the options for Real-time turning on the ones that you need

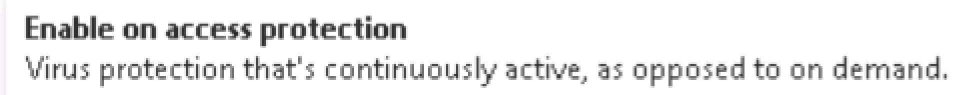


Turn on real-time protection Yes

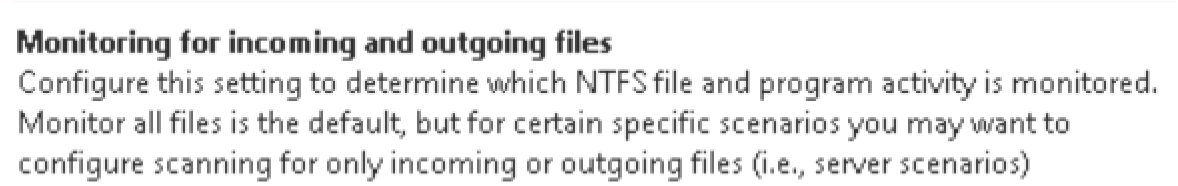
Turn on real-time protection
When this setting is set to Yes, real-time monitoring will be enforced and the user cannot disable it. When set to Not configured, the setting is returned to client default which is on. but the user can change it.



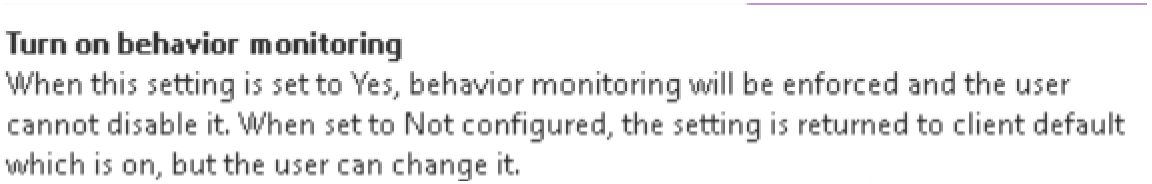
Scan all downloaded files and attachments
When this setting is set to Yes, all downloaded files and attachments will be scanned. When set to Not configured, the setting is returned to client default which is on, but the user can change it.



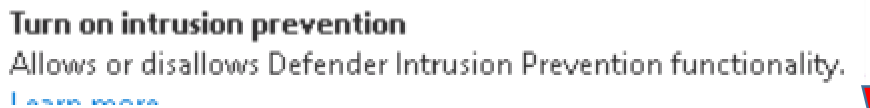
Enable on access protection
Virus protection that's continuously active, as opposed to on demand.



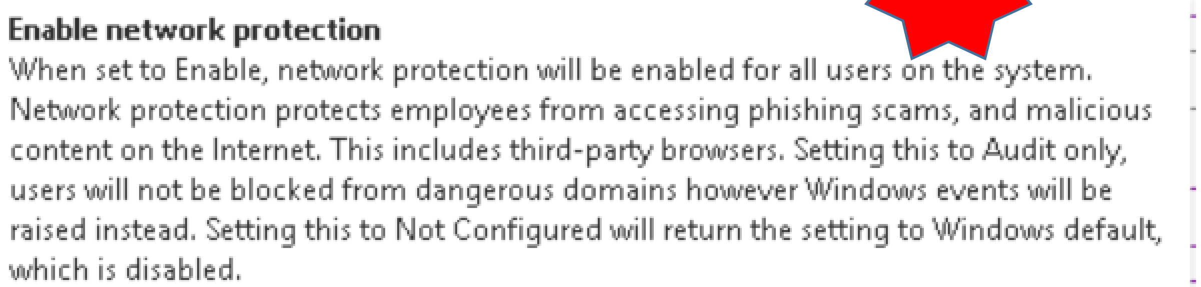
Monitoring for incoming and outgoing files
Configure this setting to determine which NTFS file and program activity is monitored. Monitor all files is the default, but for certain specific scenarios you may want to configure scanning for only incoming or outgoing files (i.e., server scenarios)



Turn on behavior monitoring
When this setting is set to Yes, behavior monitoring will be enforced and the user cannot disable it. When set to Not configured, the setting is returned to client default which is on, but the user can change it.

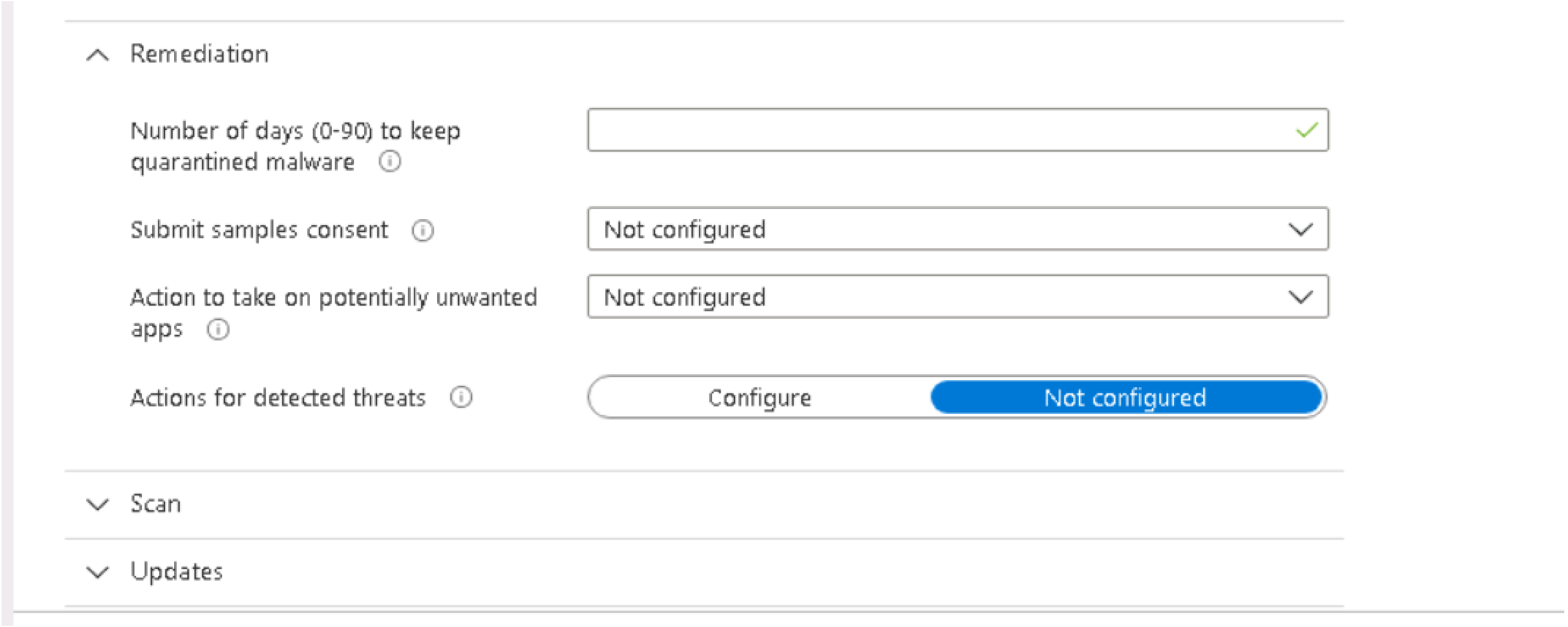


Turn on intrusion prevention
Allows or disallows Defender Intrusion Prevention functionality.
Learn more



Enable network protection
When set to Enable, network protection will be enabled for all users on the system. Network protection protects employees from accessing phishing scams, and malicious content on the Internet. This includes third-party browsers. Setting this to Audit only, users will not be blocked from dangerous domains however Windows events will be raised instead. Setting this to Not Configured will return the setting to Windows default, which is disabled.

Examine all the options for Remediation turning on the ones that you need



Remediation

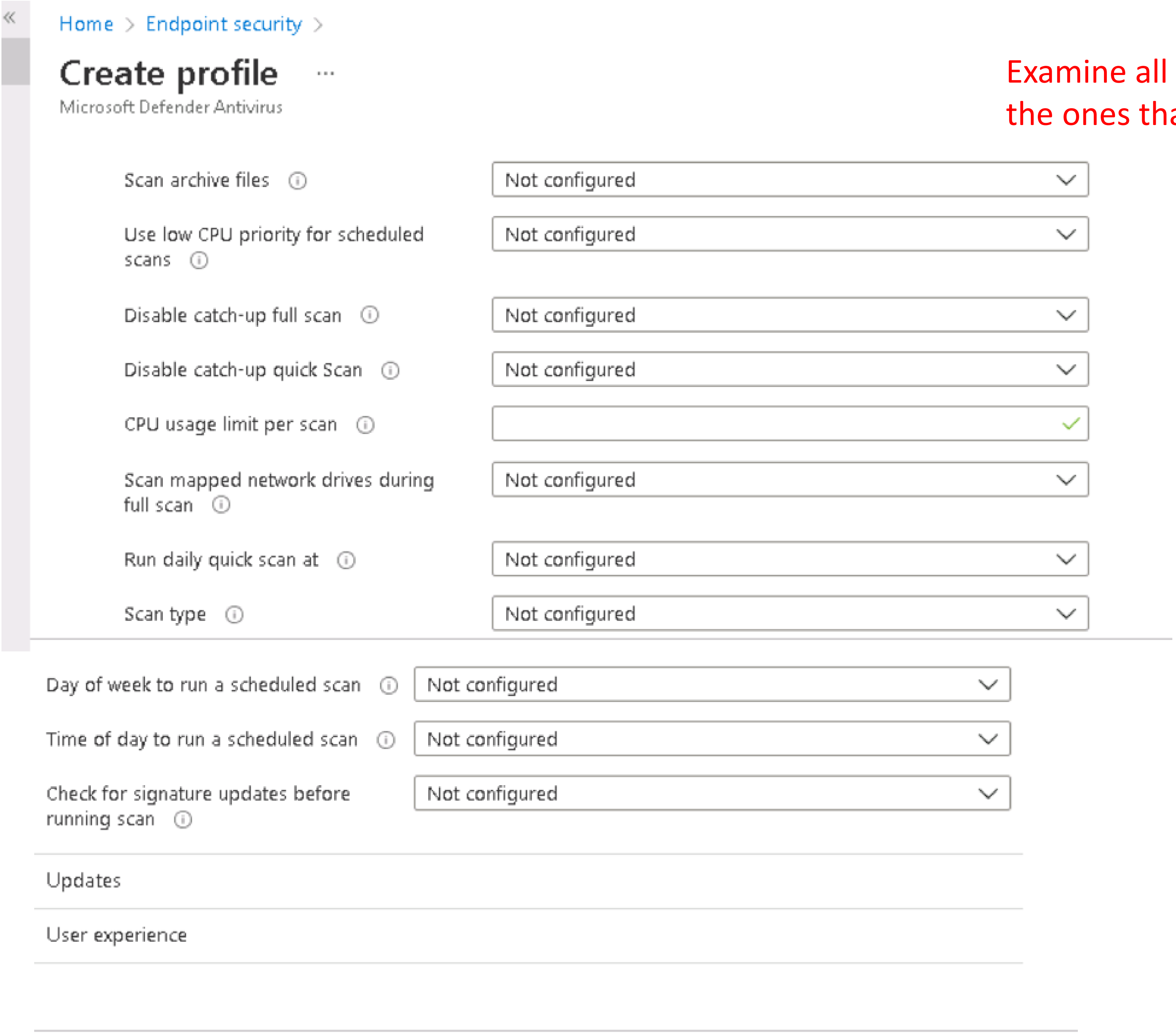
Number of days (0-90) to keep quarantined malware ✓

Submit samples consent: Not configured

Action to take on potentially unwanted apps: Not configured

Actions for detected threats: Configure | Not configured

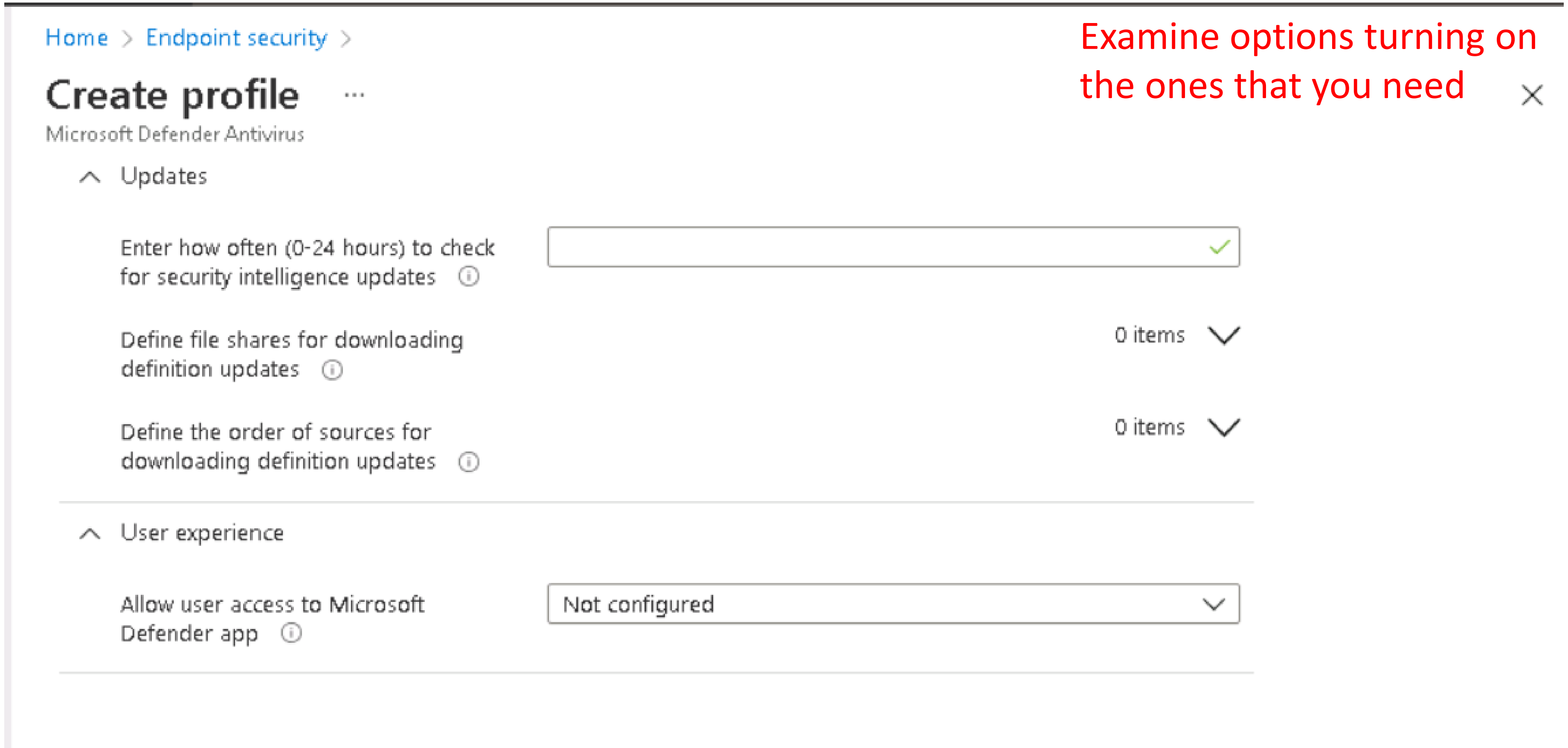
Examine all the options for scan turning on the ones that you need



Create profile ...

Microsoft Defender Antivirus

Scan archive files ⓘ	Not configured
Use low CPU priority for scheduled scans ⓘ	Not configured
Disable catch-up full scan ⓘ	Not configured
Disable catch-up quick Scan ⓘ	Not configured
CPU usage limit per scan ⓘ	✓
Scan mapped network drives during full scan ⓘ	Not configured
Run daily quick scan at ⓘ	Not configured
Scan type ⓘ	Not configured
Day of week to run a scheduled scan ⓘ	Not configured
Time of day to run a scheduled scan ⓘ	Not configured
Check for signature updates before running scan ⓘ	Not configured



Examine options turning on the ones that you need

Home > Endpoint security >

Create profile

Microsoft Defender Antivirus

Updates

Enter how often (0-24 hours) to check for security intelligence updates ⓘ ✓

Define file shares for downloading definition updates ⓘ 0 items

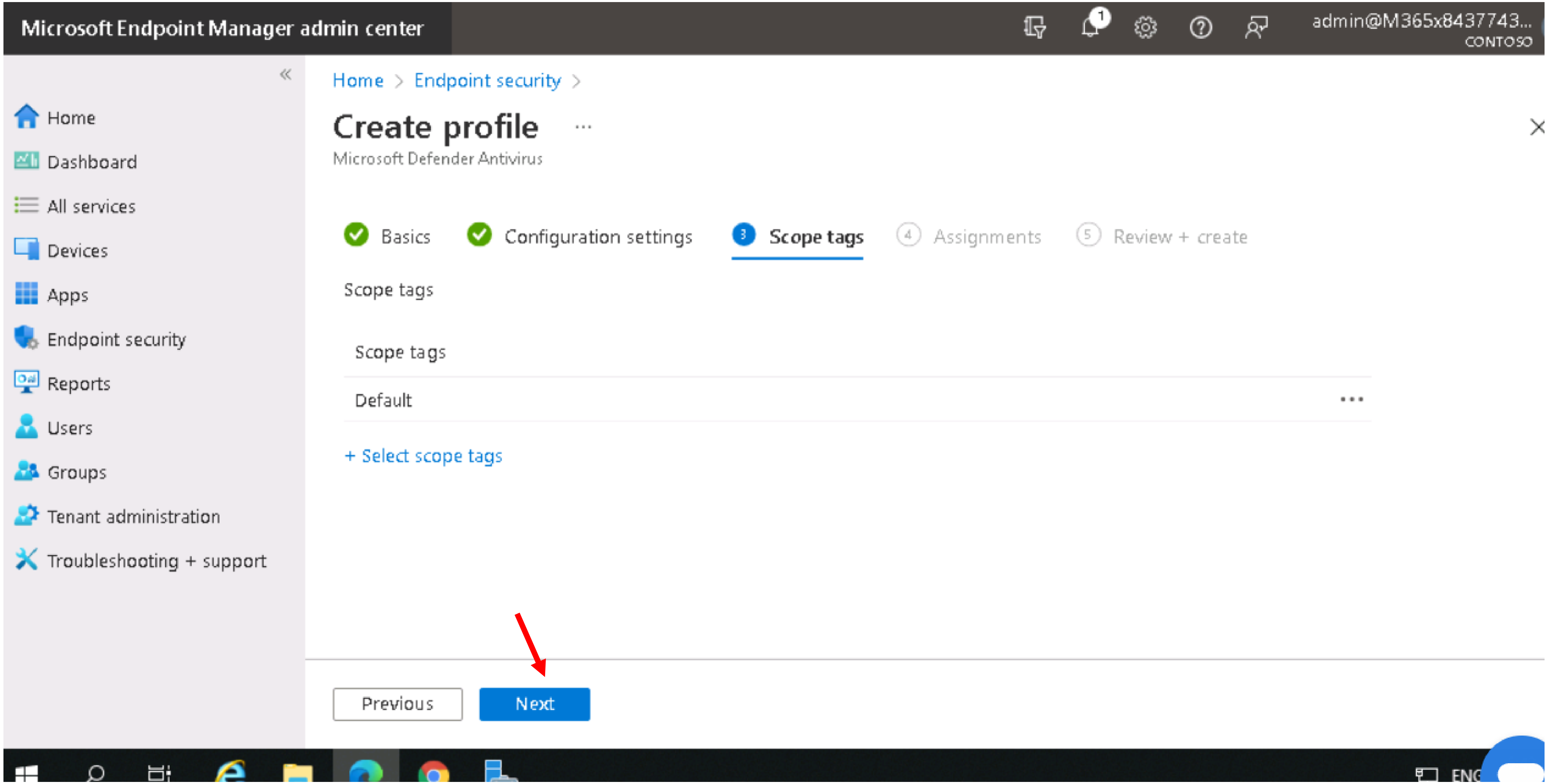
Define the order of sources for downloading definition updates ⓘ 0 items

User experience

Allow user access to Microsoft Defender app ⓘ Not configured

User experience

Allow user access to Microsoft Defender app ⓘ Not configured

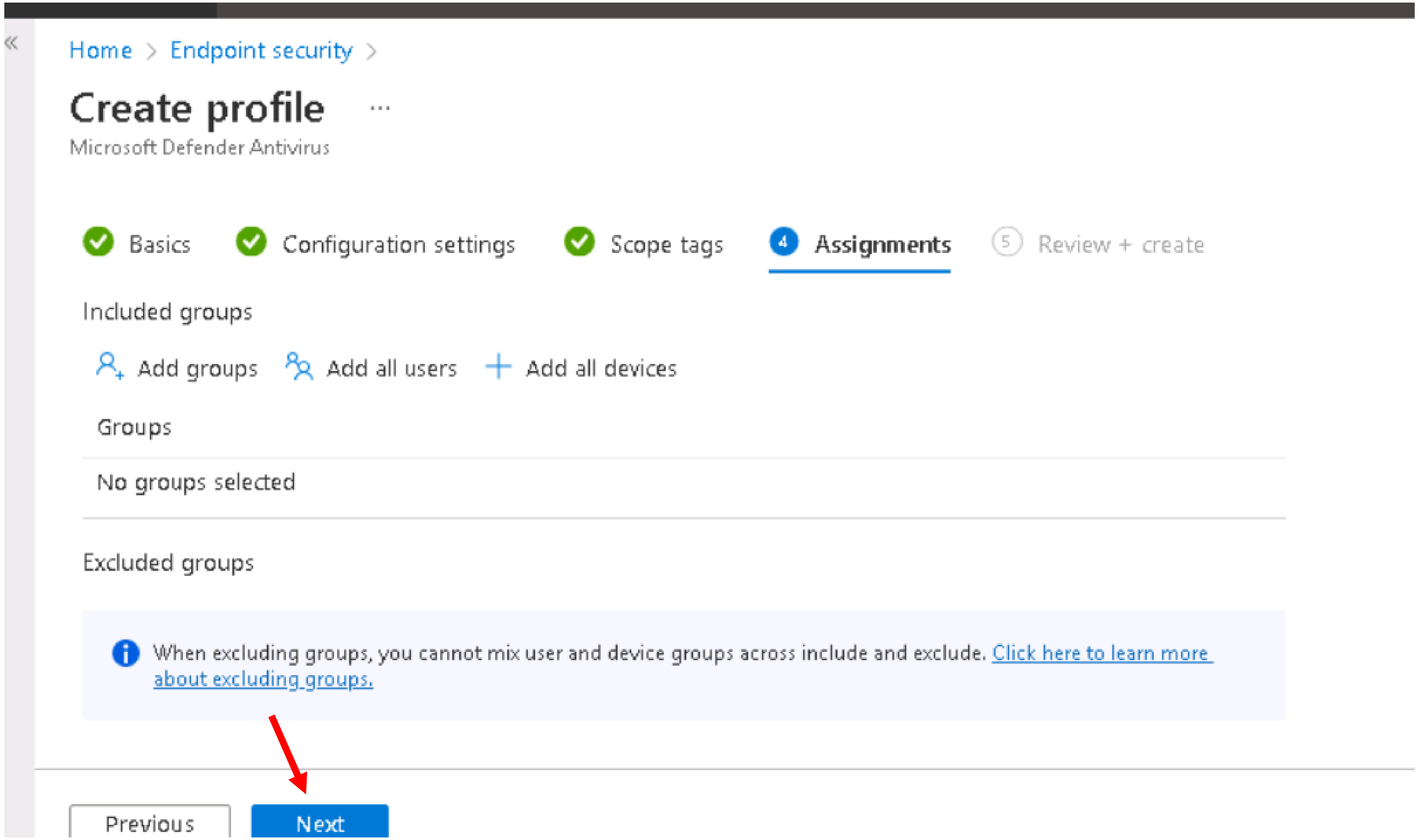


Create profile

Microsoft Defender Antivirus

Scope tags

Scope tags
Default



Home > Endpoint security >

Create profile ...

Microsoft Defender Antivirus

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

Included groups

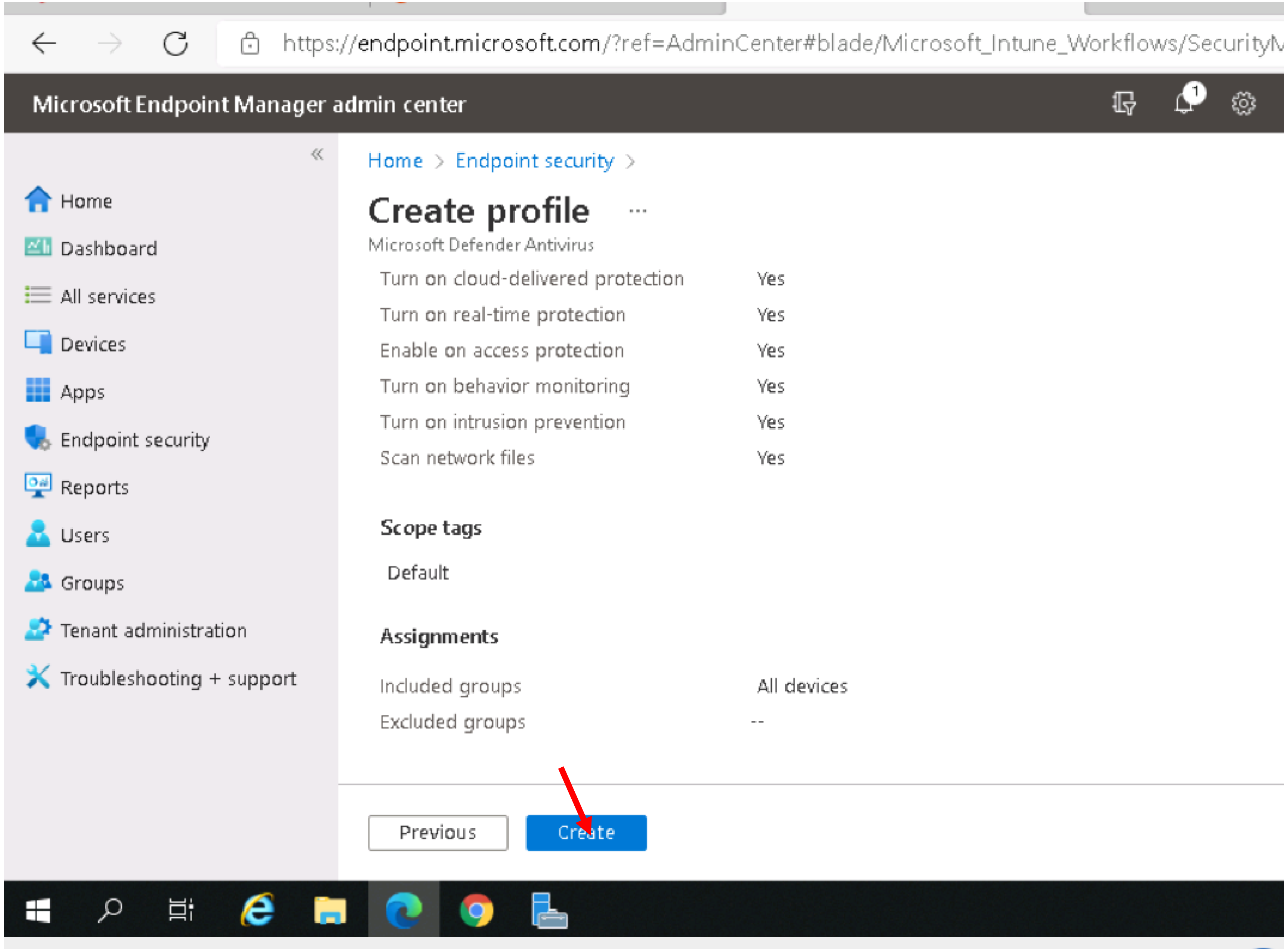
Add groups Add all users + Add all devices

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



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

Create profile

Microsoft Defender Antivirus

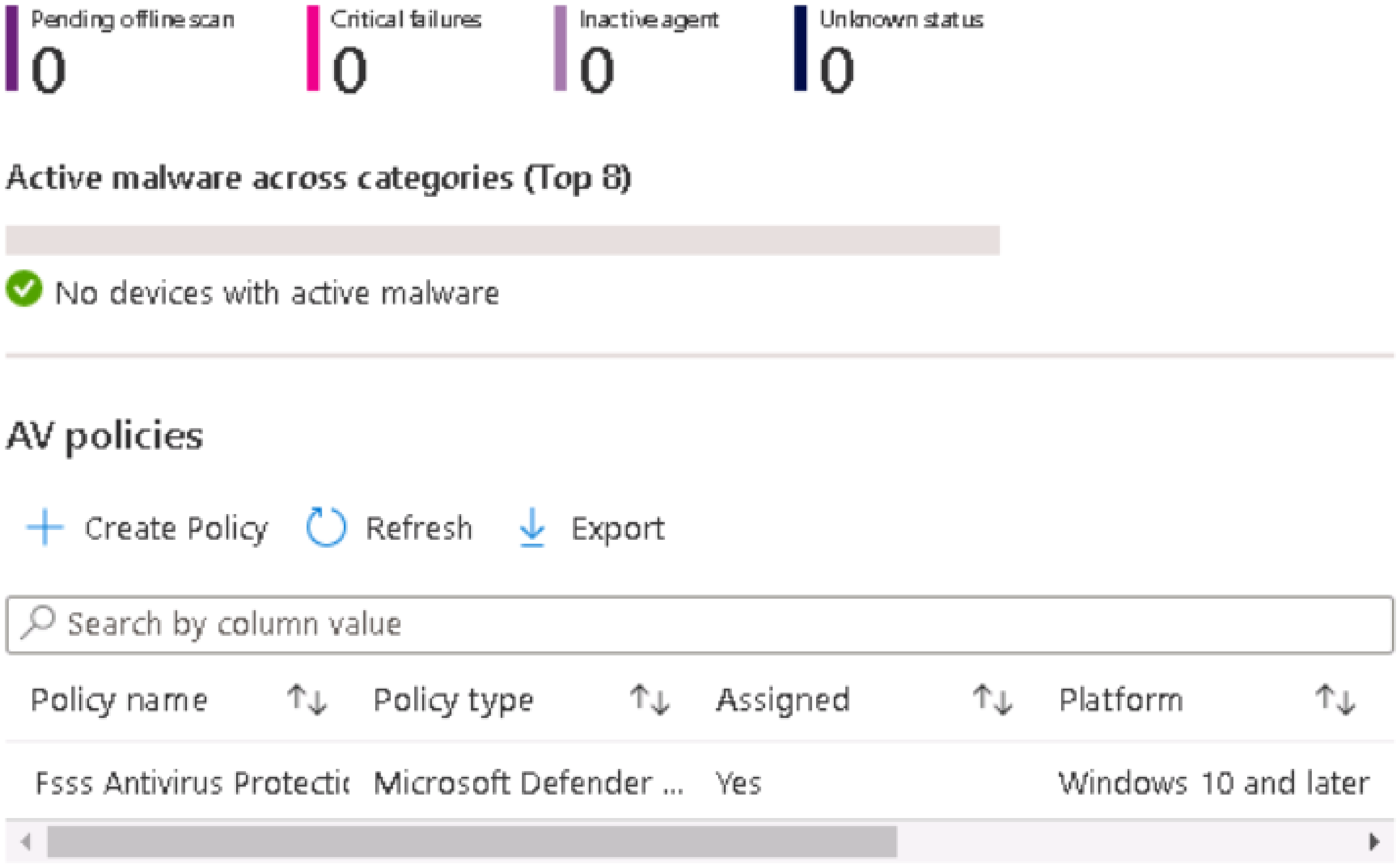
Turn on cloud-delivered protection	Yes
Turn on real-time protection	Yes
Enable on access protection	Yes
Turn on behavior monitoring	Yes
Turn on intrusion prevention	Yes
Scan network files	Yes

Scope tags

Default

Assignments

Included groups	All devices
Excluded groups	--



Pending offline scan 0

Critical failures 0

Inactive agent 0

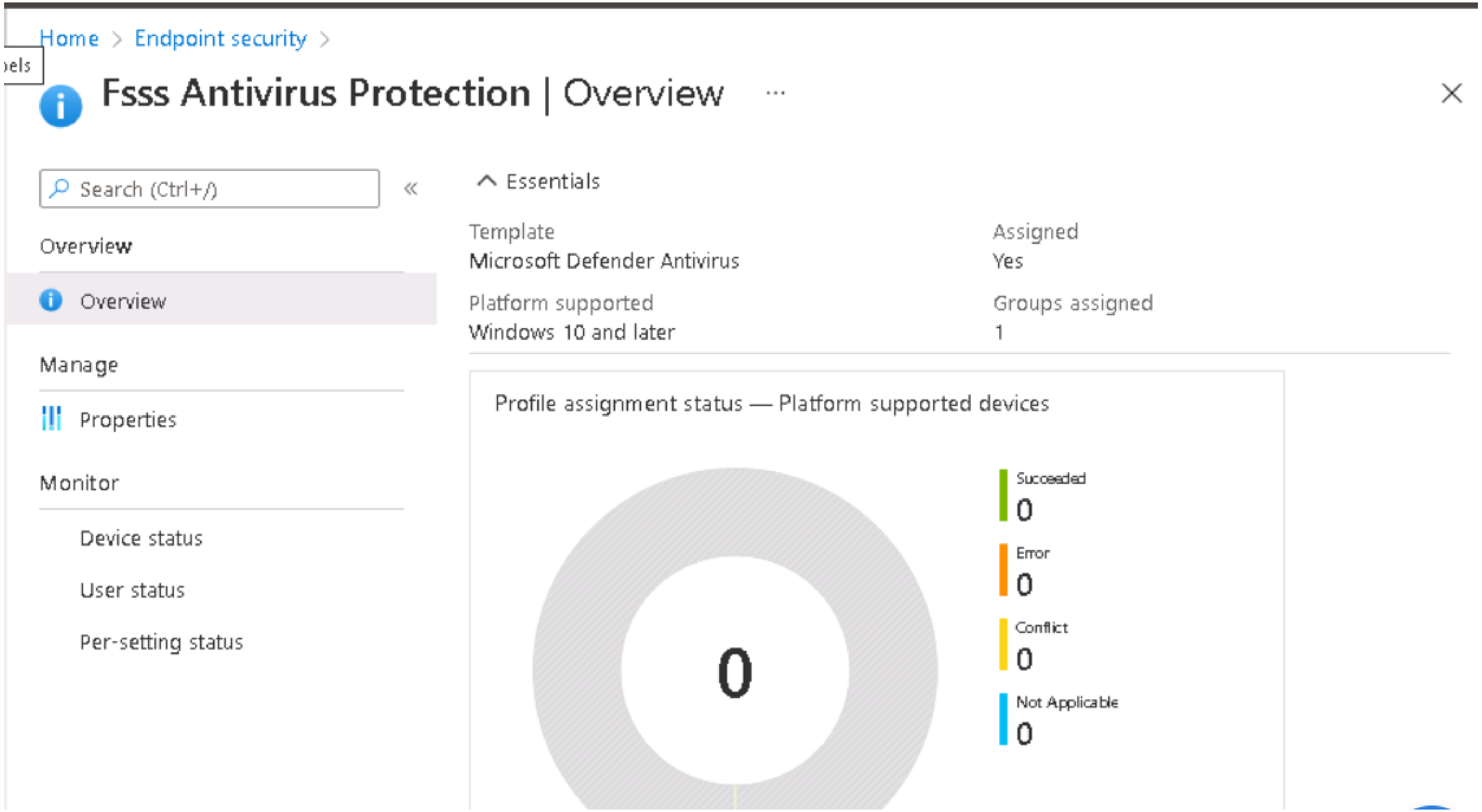
Unknown status 0

Active malware across categories (Top 8)

✓ No devices with active malware

AV policies

Policy name	Policy type	Assigned	Platform
Fsss Antivirus Protecti	Microsoft Defender ...	Yes	Windows 10 and later



Fsss Antivirus Protection | Overview

Template
Microsoft Defender Antivirus

Assigned
Yes

Platform supported
Windows 10 and later

Groups assigned
1

Profile assignment status — Platform supported devices

0

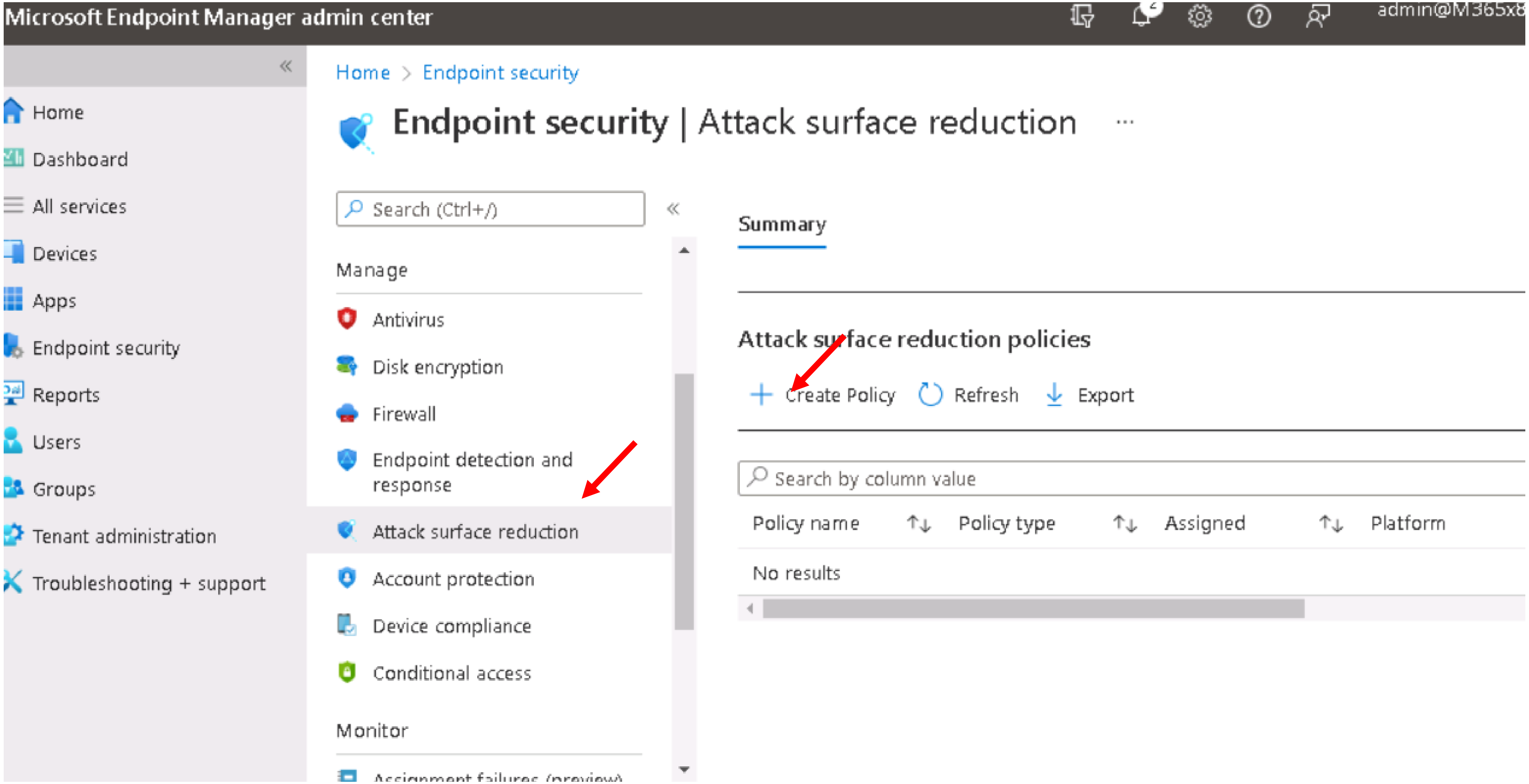
Succeeded
0

Error
0

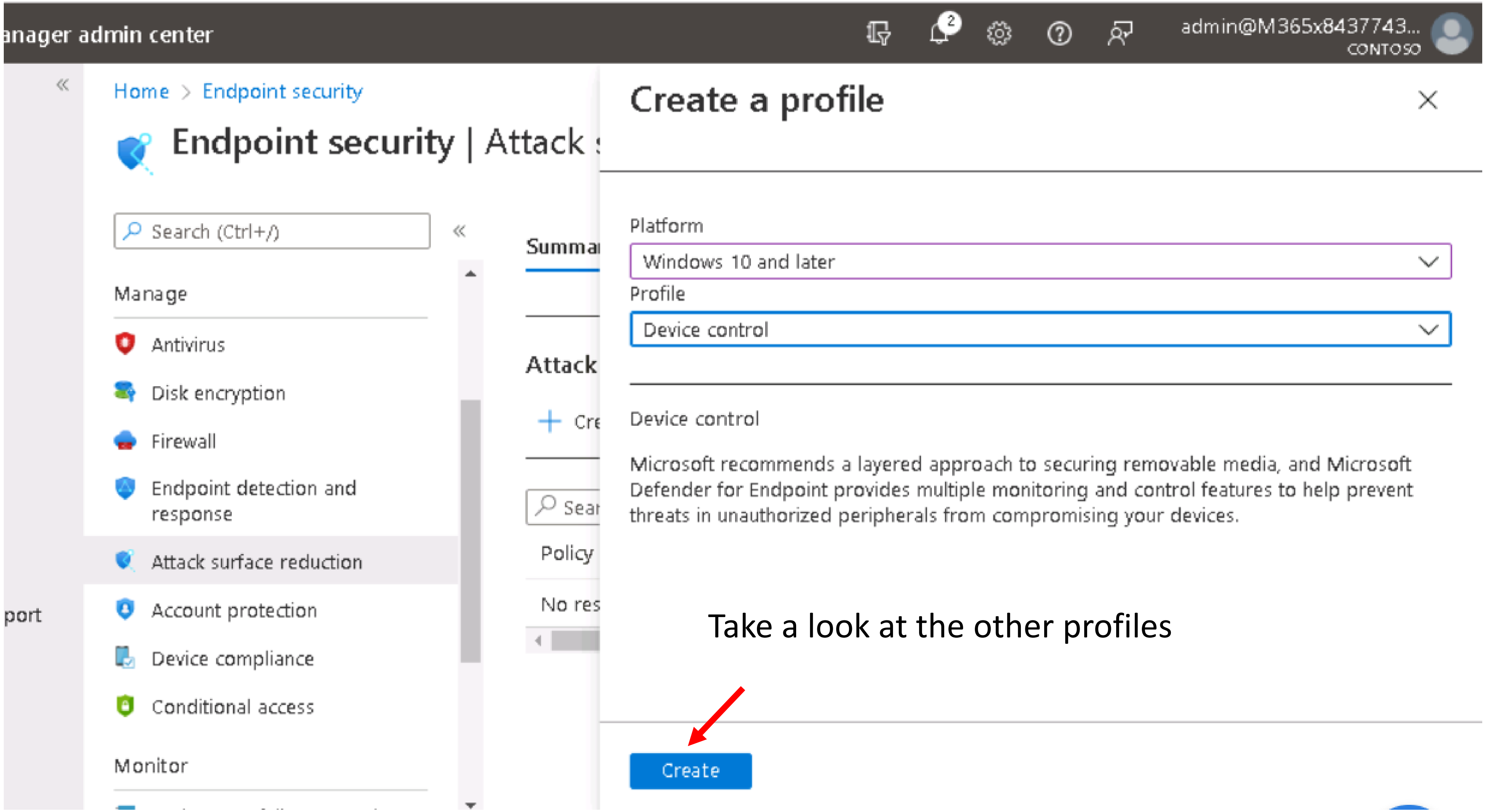
Conflict
0

Not Applicable
0

Attack Surface Reduction



Policy name	Policy type	Assigned	Platform
No results			



Create a profile

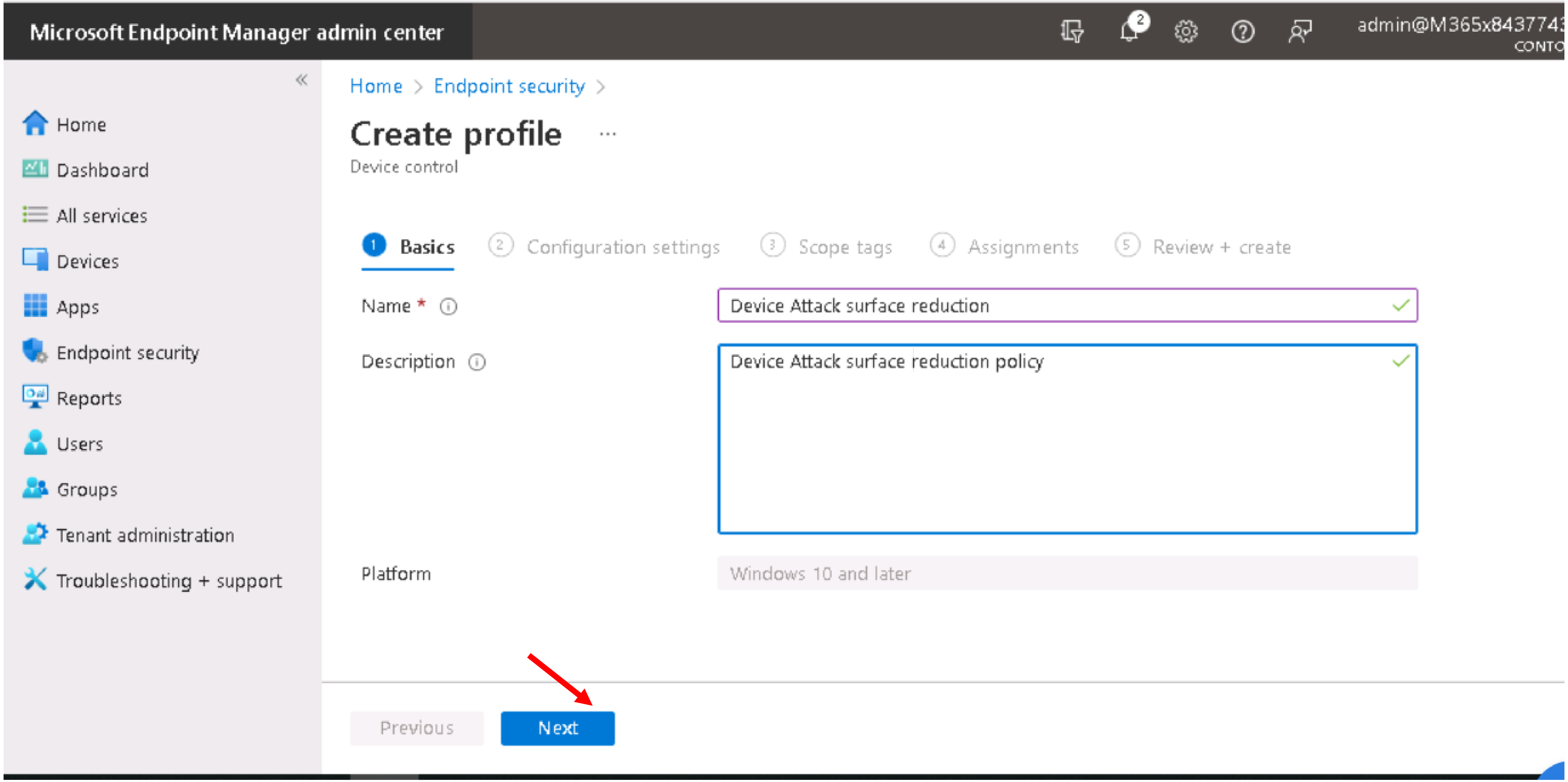
Platform: Windows 10 and later

Profile: Device control

Device control

Microsoft recommends a layered approach to securing removable media, and Microsoft Defender for Endpoint provides multiple monitoring and control features to help prevent threats in unauthorized peripherals from compromising your devices.

Take a look at the other profiles



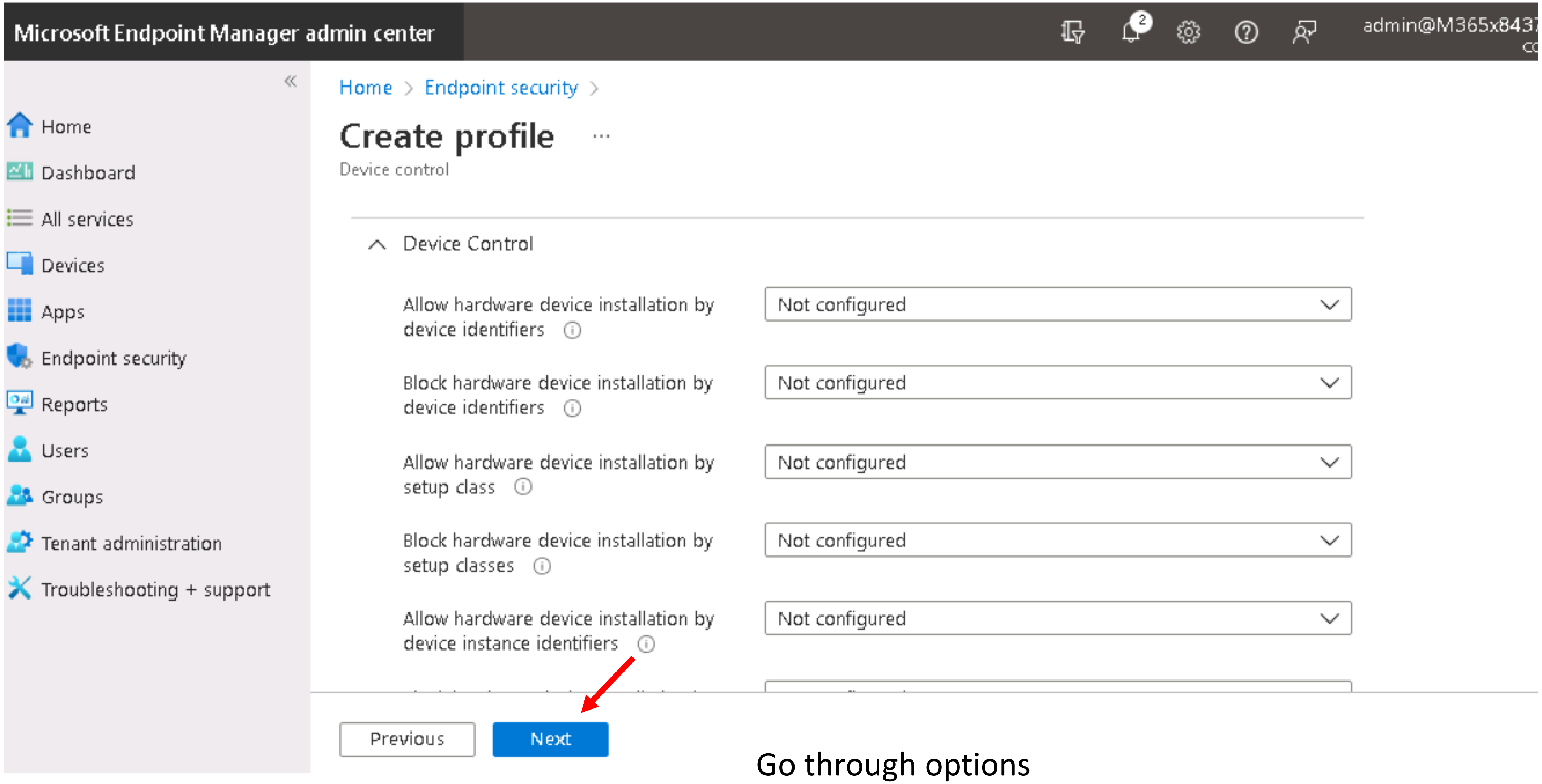
Create profile

Device control

Name * Device Attack surface reduction

Description Device Attack surface reduction policy

Platform Windows 10 and later



Create profile

Device control

Device Control

Allow hardware device installation by device identifiers: Not configured

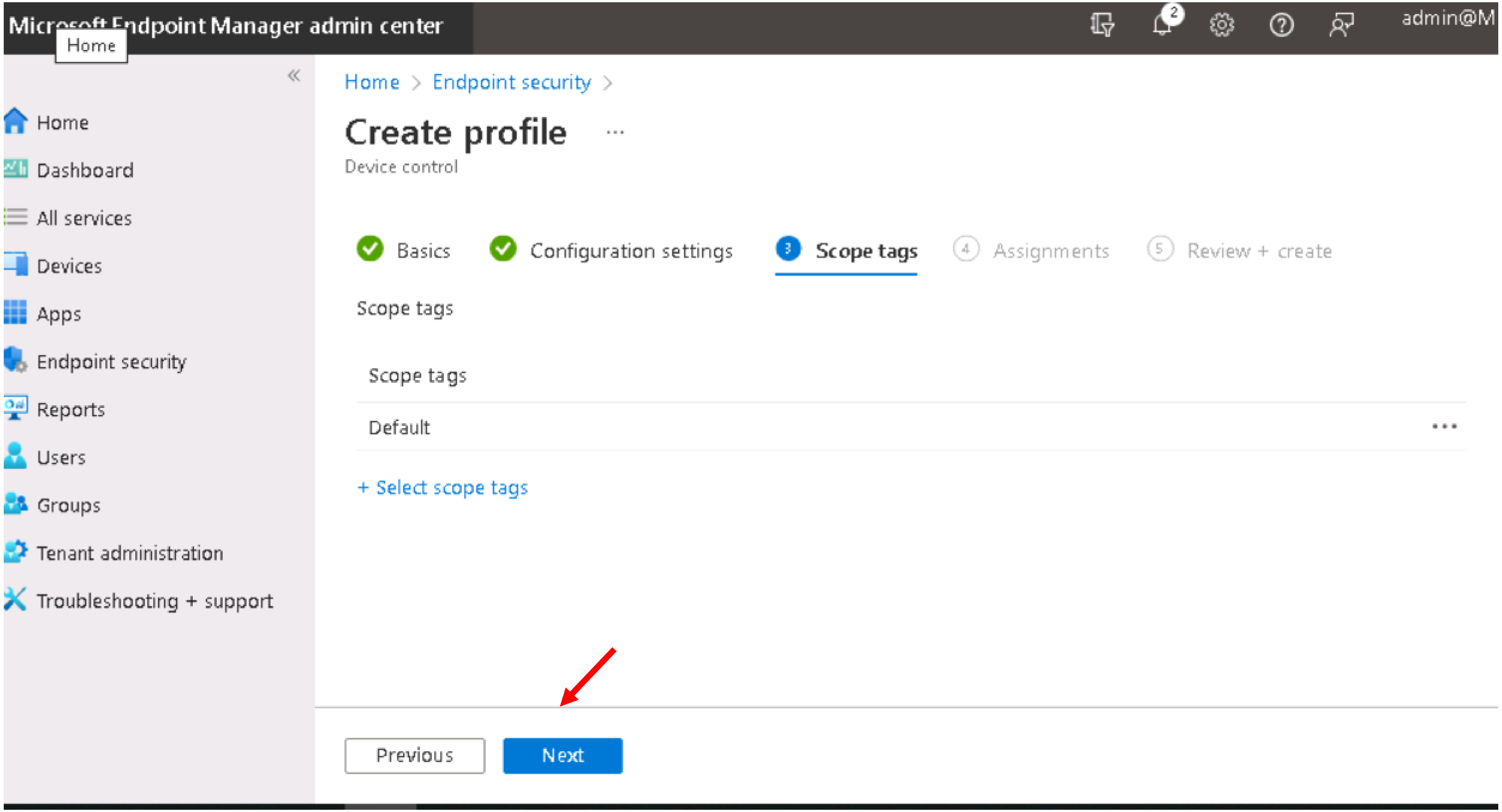
Block hardware device installation by device identifiers: Not configured

Allow hardware device installation by setup class: Not configured

Block hardware device installation by setup classes: Not configured

Allow hardware device installation by device instance identifiers: Not configured

Go through options

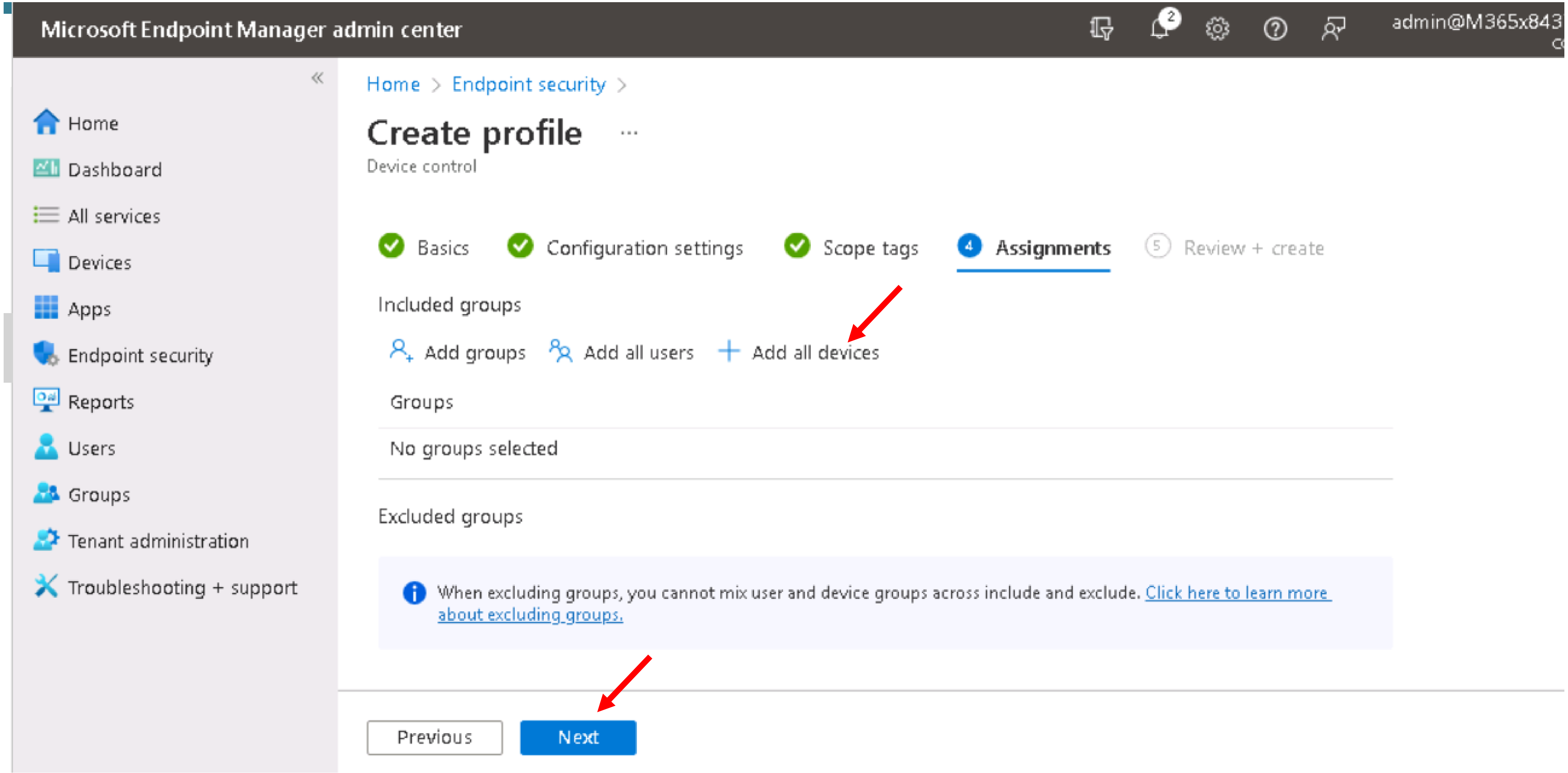


Create profile

Device control

Scope tags

Scope tags
Default



Create profile ...

Device control

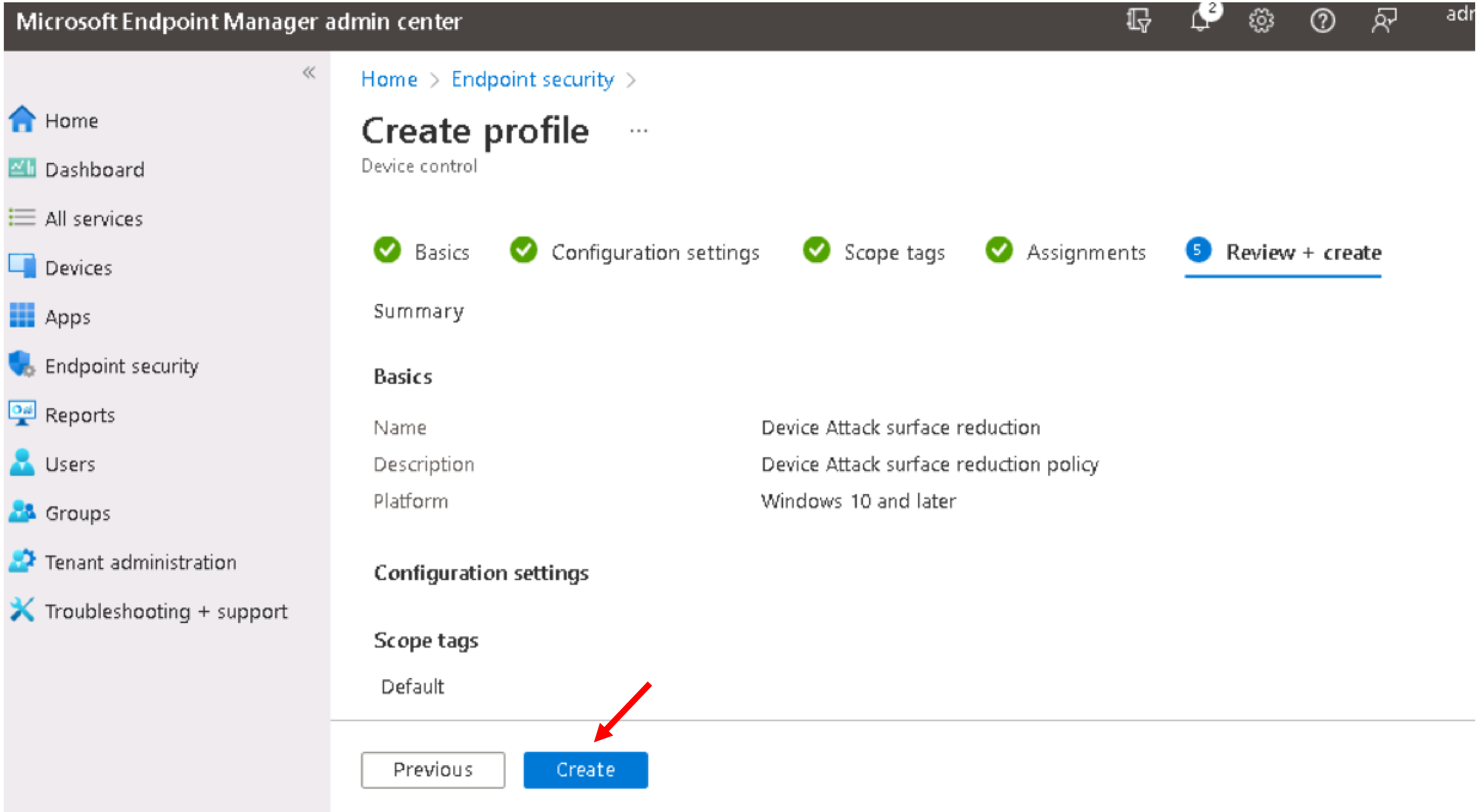
Included groups

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 ...

Device control

Summary

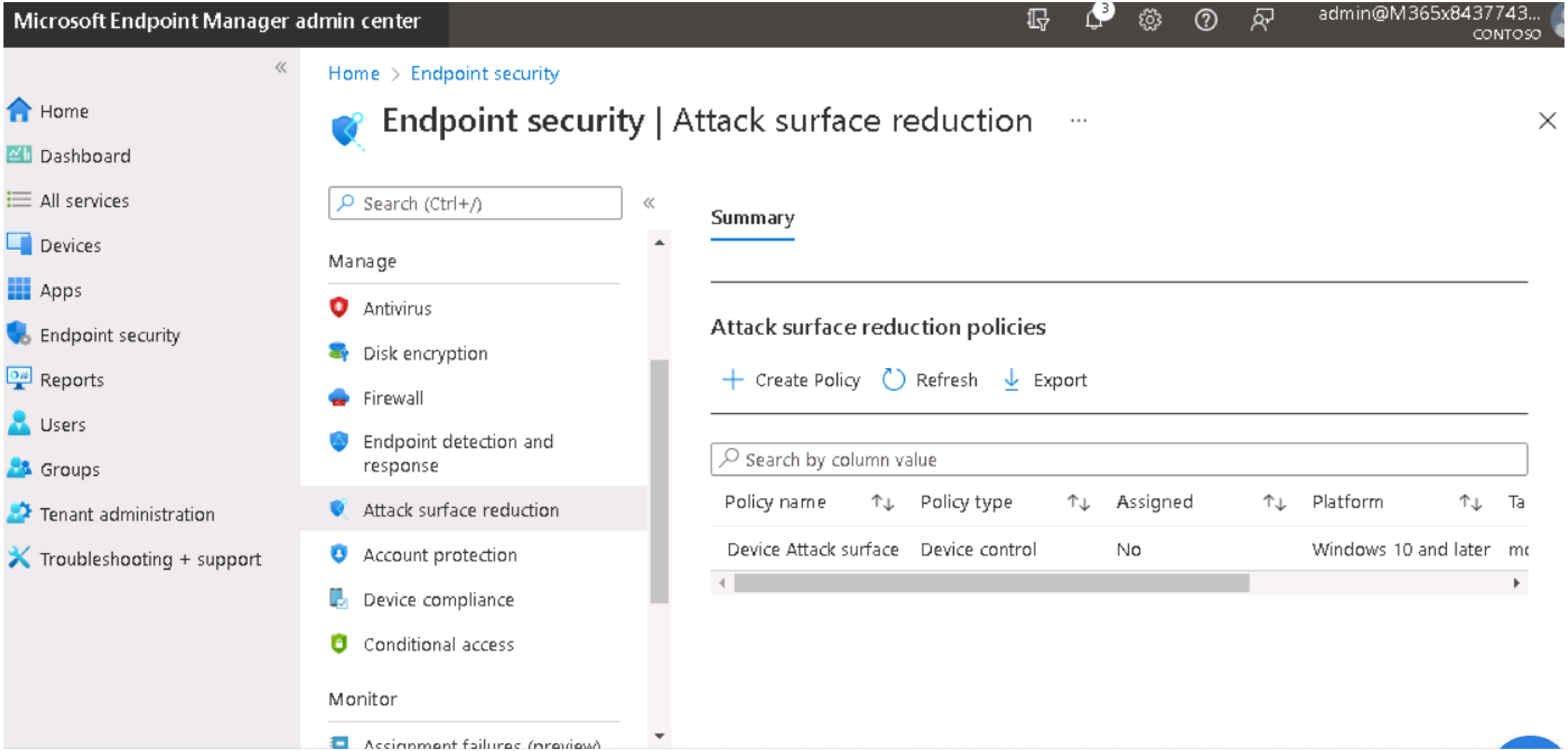
Basics

Name	Device Attack surface reduction
Description	Device Attack surface reduction policy
Platform	Windows 10 and later

Configuration settings

Scope tags

Default

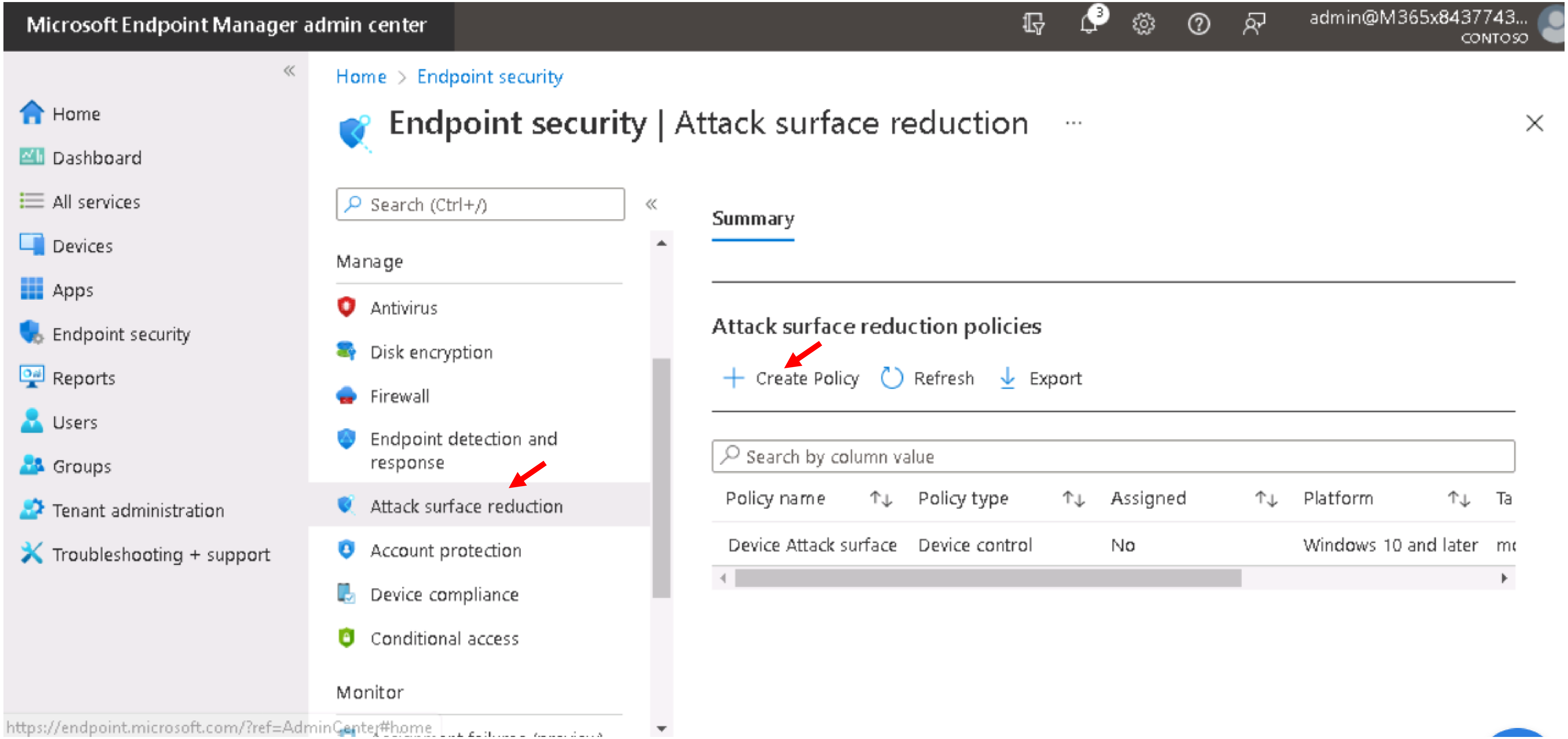


Endpoint security | Attack surface reduction

Attack surface reduction policies

Policy name	Policy type	Assigned	Platform	Ta
Device Attack surface	Device control	No	Windows 10 and later	mo

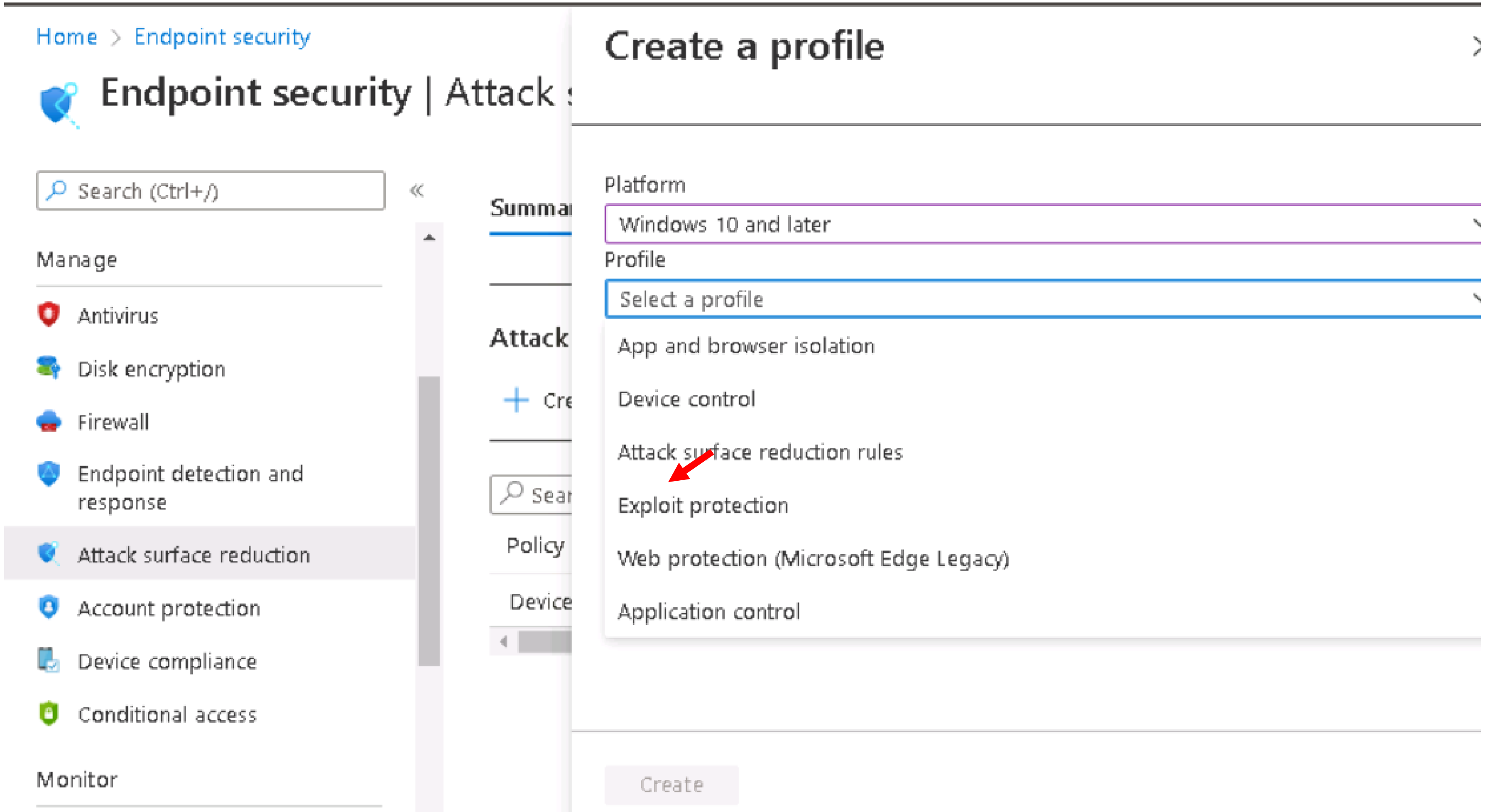
Exploit protection



Endpoint security | Attack surface reduction

Attack surface reduction policies

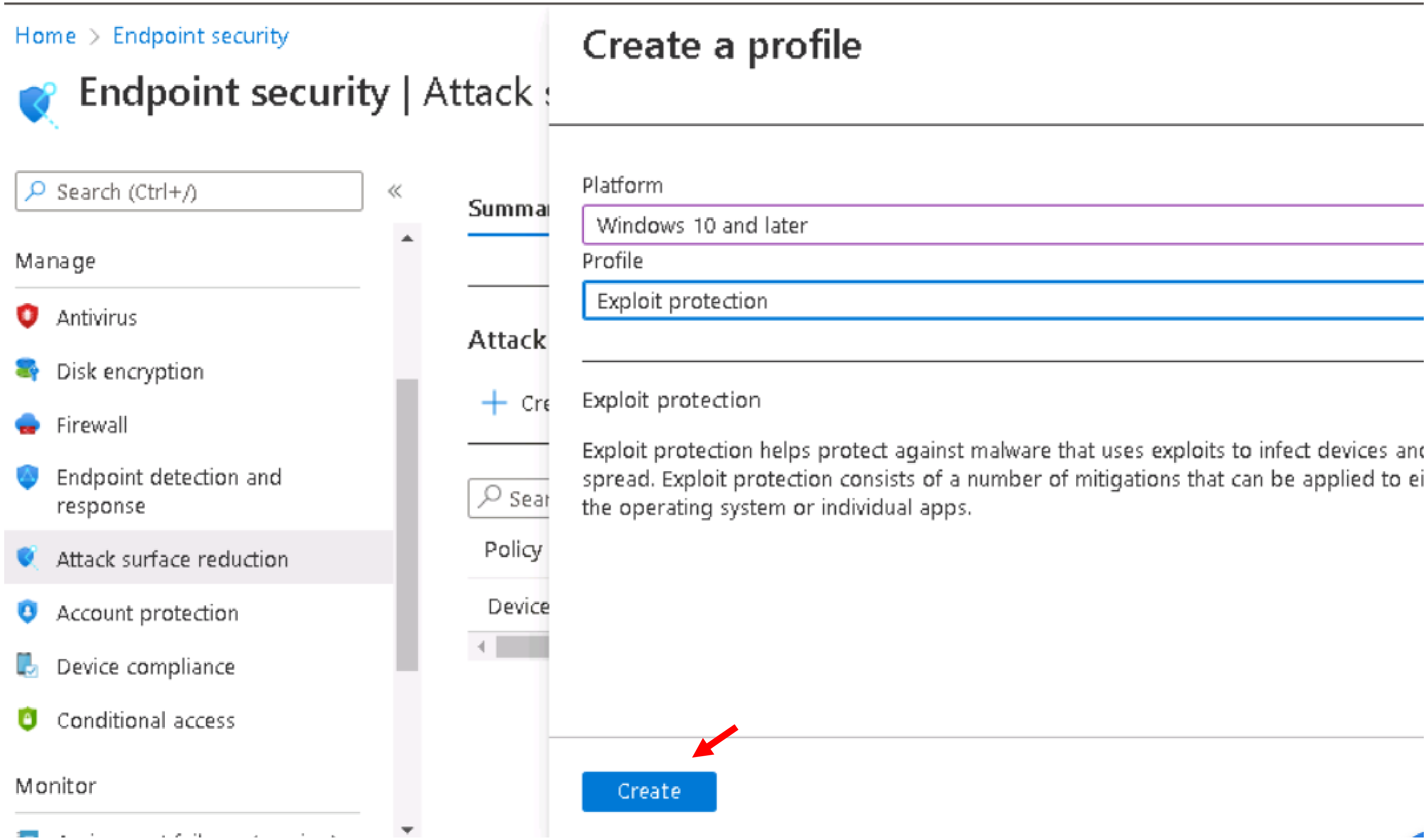
Policy name	Policy type	Assigned	Platform	Ta
Device Attack surface	Device control	No	Windows 10 and later	m



Create a profile

Platform: Windows 10 and later

Profile: Select a profile



Create a profile

Platform

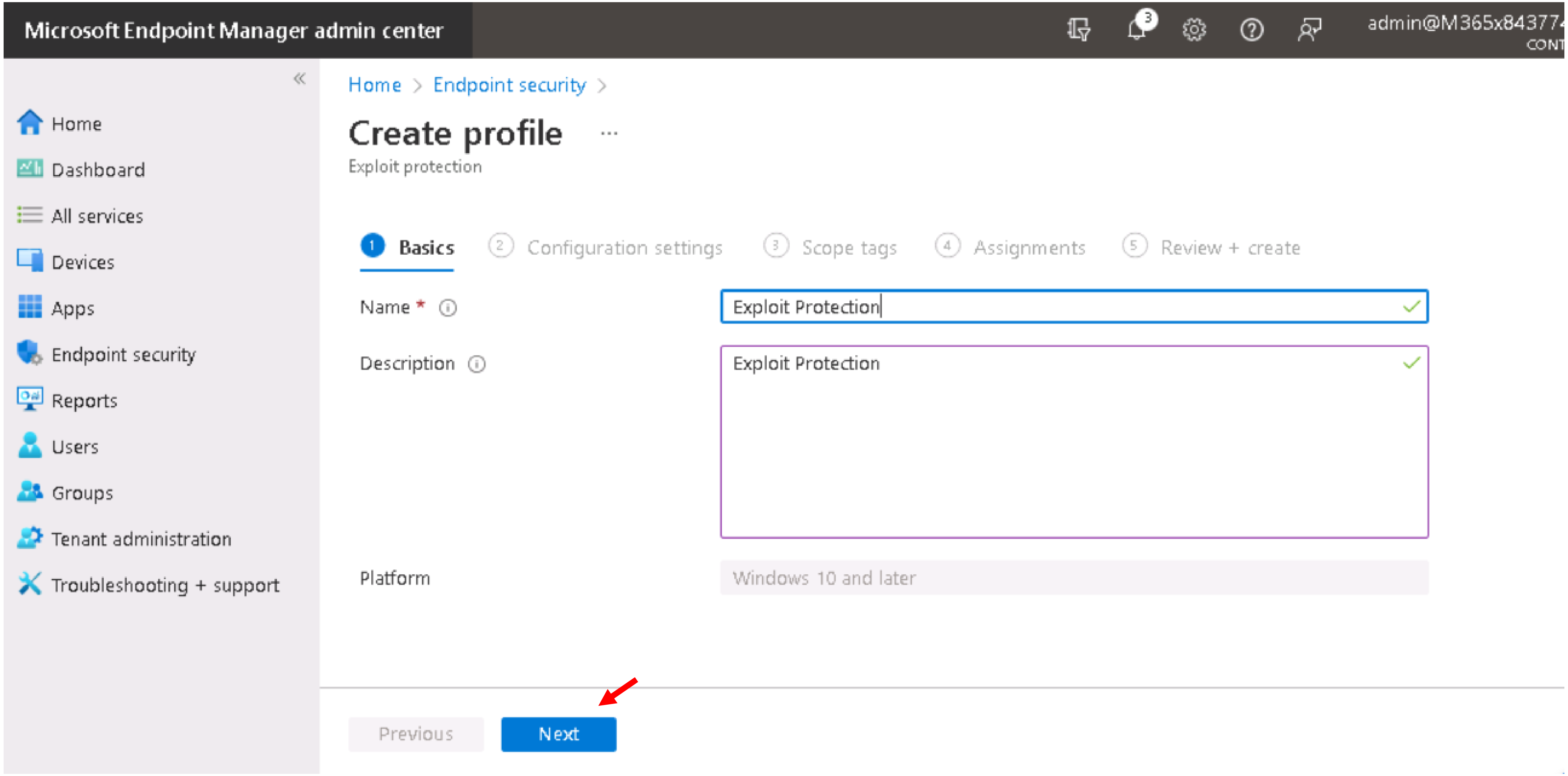
Windows 10 and later

Profile

Exploit protection

Exploit protection

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



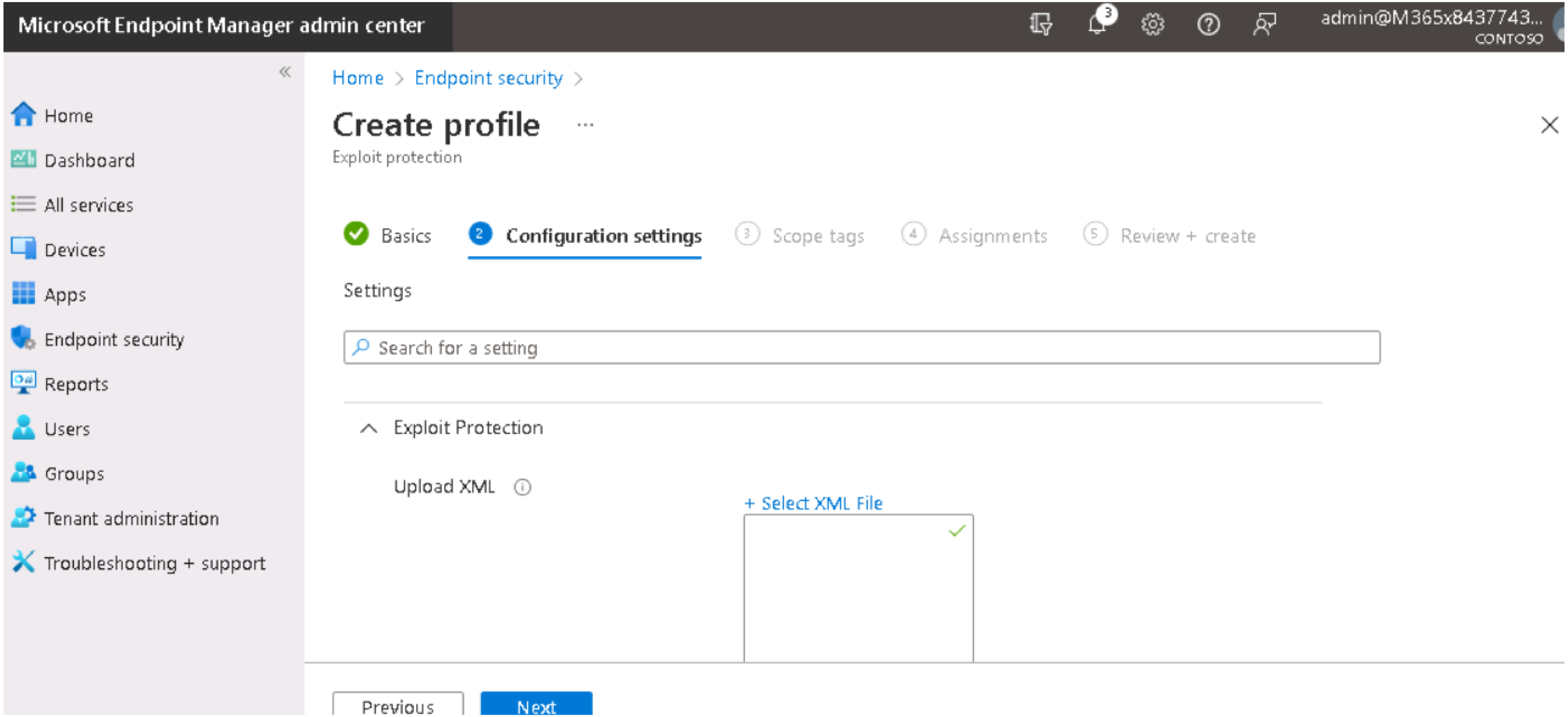
Create profile ...

Exploit protection

Name * : Exploit Protection

Description: Exploit Protection

Platform: Windows 10 and later



Create profile ...

Exploit protection

Settings

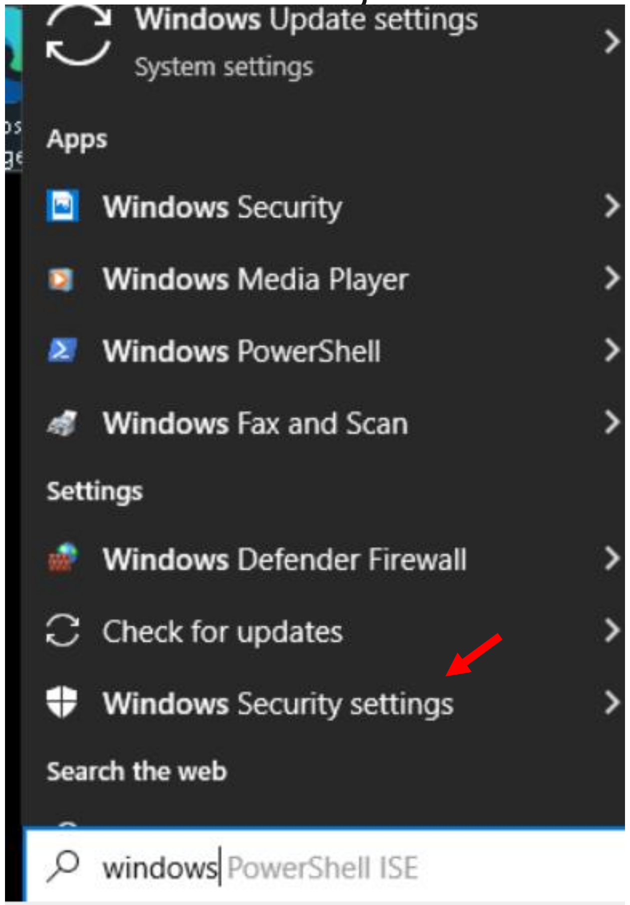
Exploit Protection

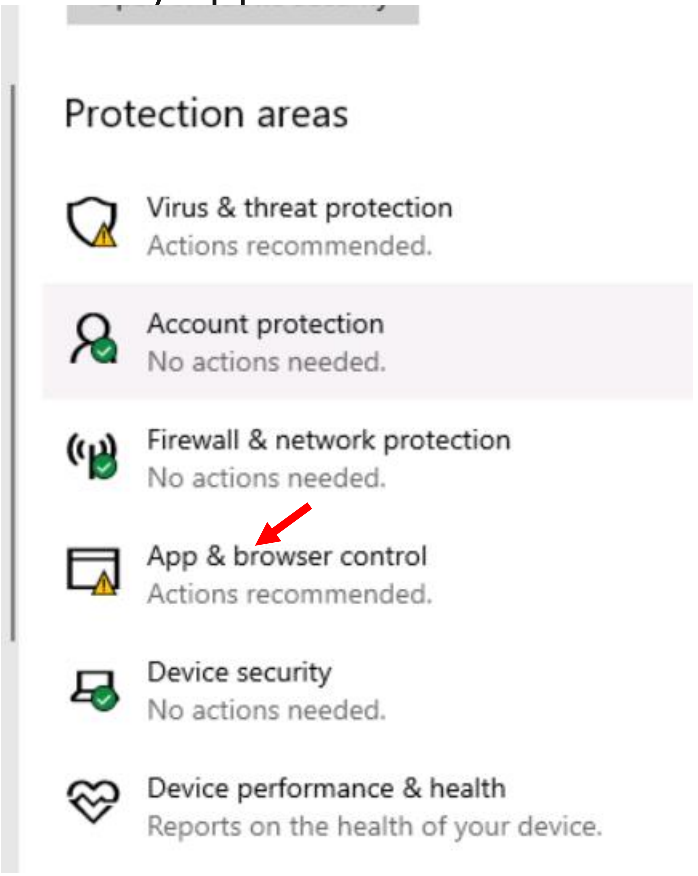
Upload XML ⓘ

Create and export a configuration file

Before you export a configuration file, you need to ensure you have the correct settings. First, configure exploit protection on a single, dedicated device. See [Customize exploit protection]() for more information about configuring mitigations.

When you've configured exploit protection to your desired state (including both system-level and app-level mitigations), you can export the file using either the Windows Security app or PowerShell.




Protection areas

Virus & threat protection
Actions recommended.

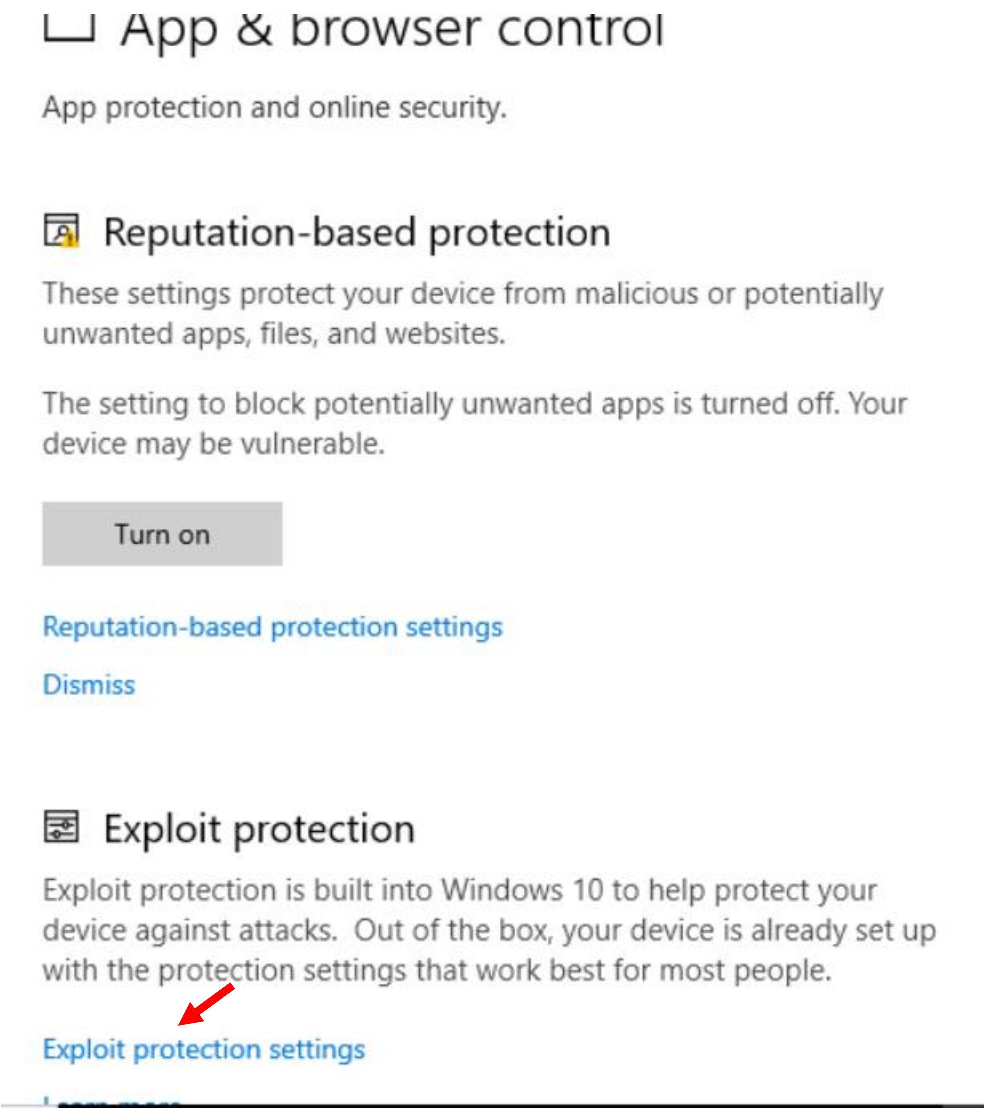
Account protection
No actions needed.

Firewall & network protection
No actions needed.

App & browser control
Actions recommended.

Device security
No actions needed.

Device performance & health
Reports on the health of your device.



App & browser control

App protection and online security.

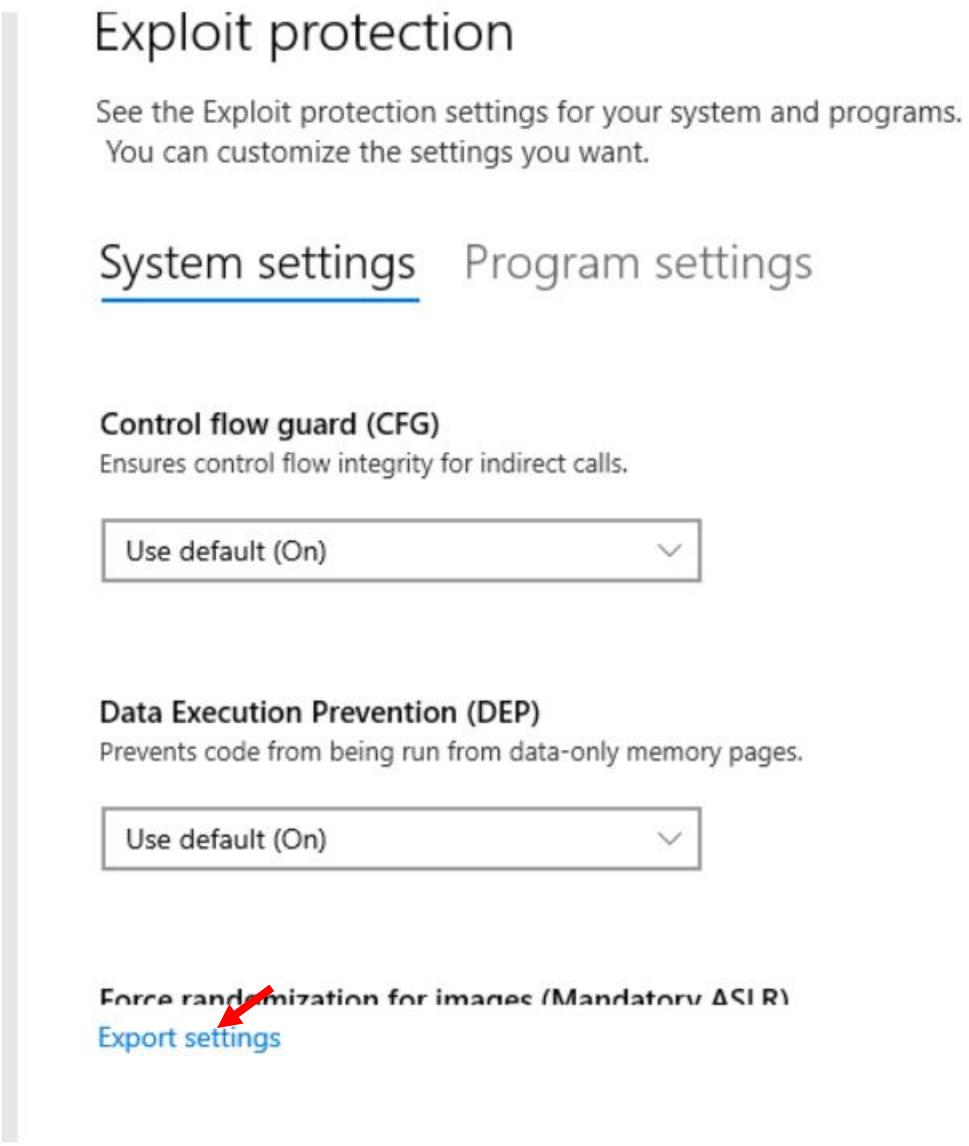
Reputation-based protection

These settings protect your device from malicious or potentially unwanted apps, files, and websites.

The setting to block potentially unwanted apps is turned off. Your device may be vulnerable.

Exploit protection

Exploit protection is built into Windows 10 to help protect your device against attacks. Out of the box, your device is already set up with the protection settings that work best for most people.



Exploit protection

See the Exploit protection settings for your system and programs. You can customize the settings you want.

Control flow guard (CFG)
Ensures control flow integrity for indirect calls.

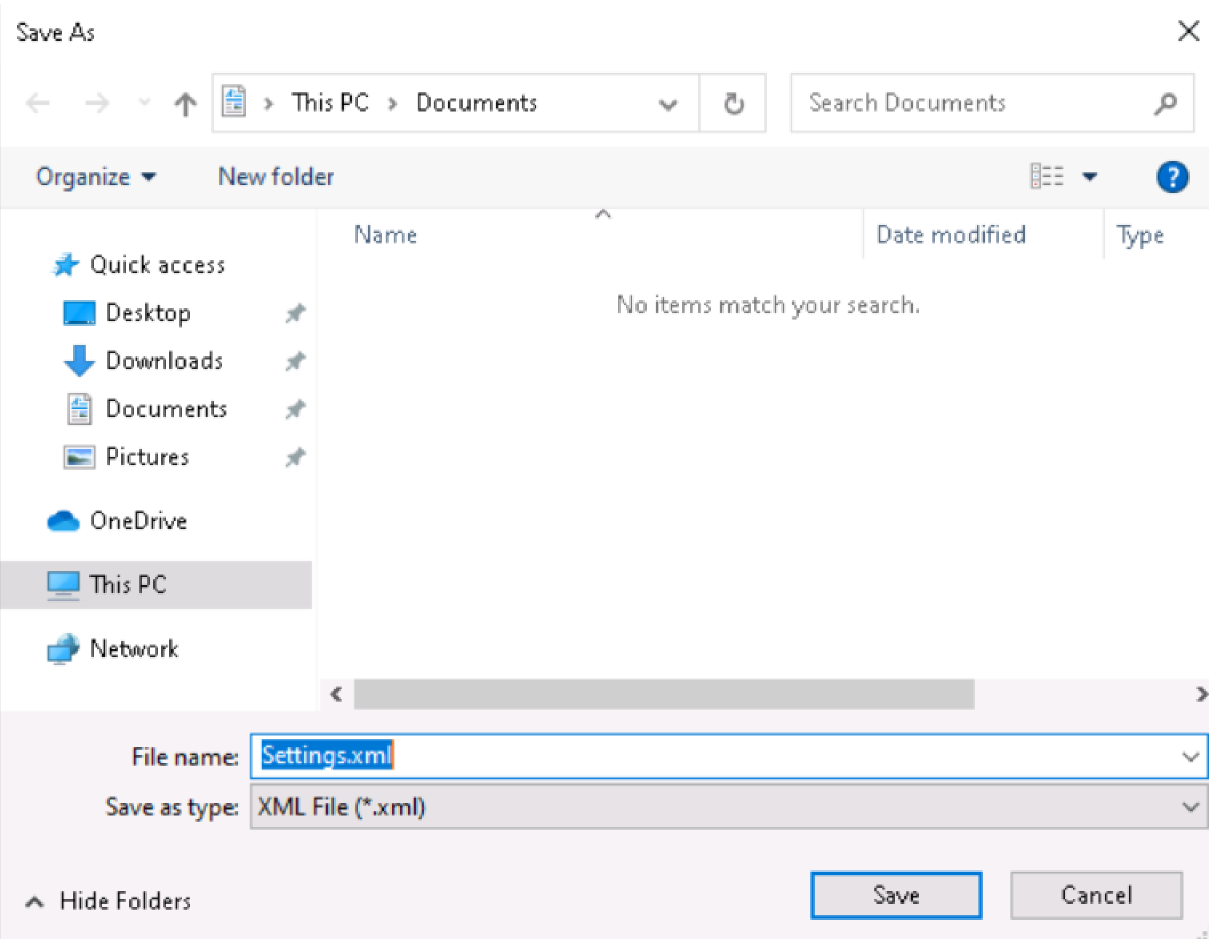
Use default (On)

Data Execution Prevention (DEP)
Prevents code from being run from data-only memory pages.

Use default (On)

Force randomization for images (Mandatory ASLR)

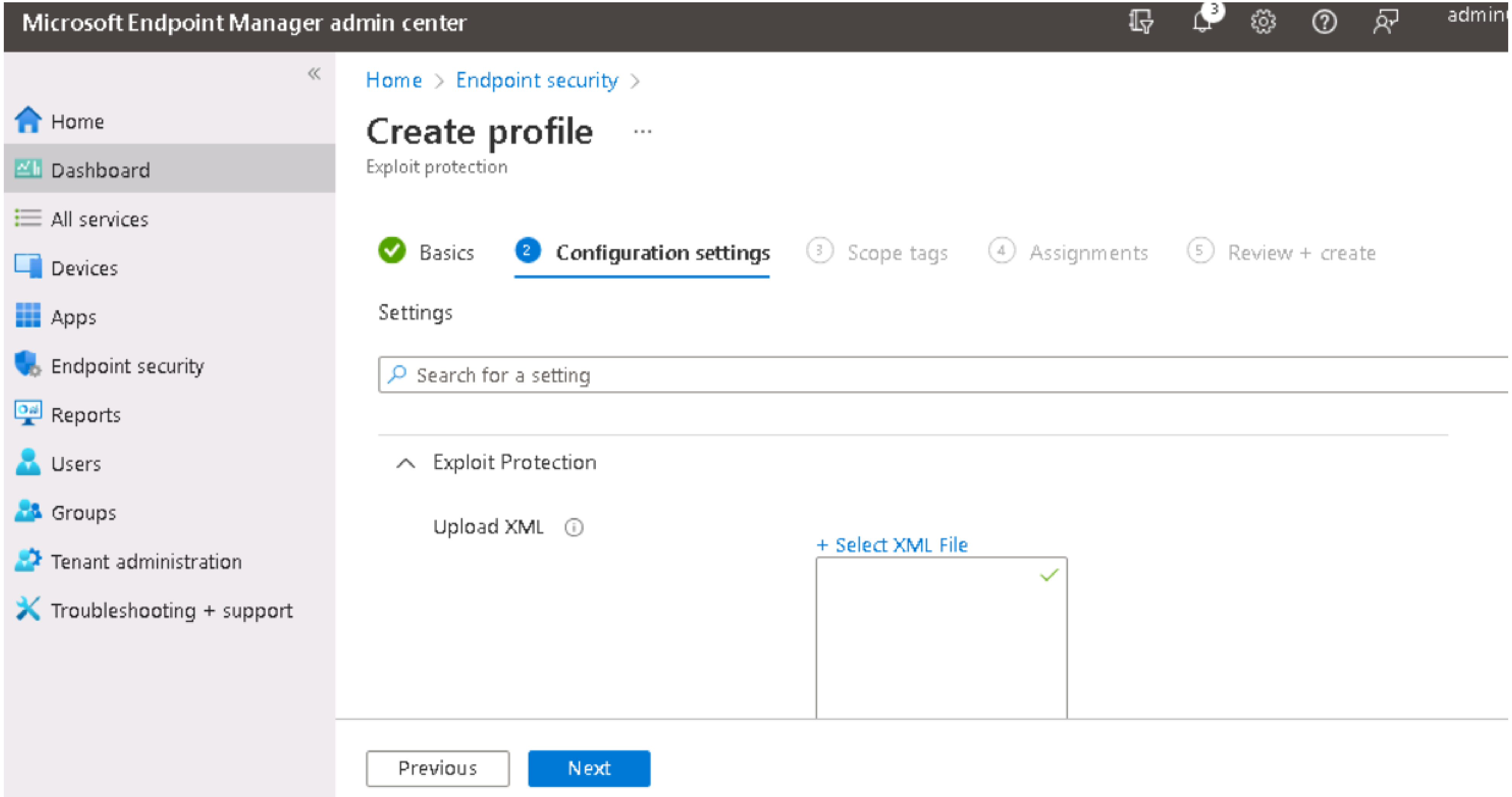
You can make changes to you system settings and your program settings then export the settings as an XML file.

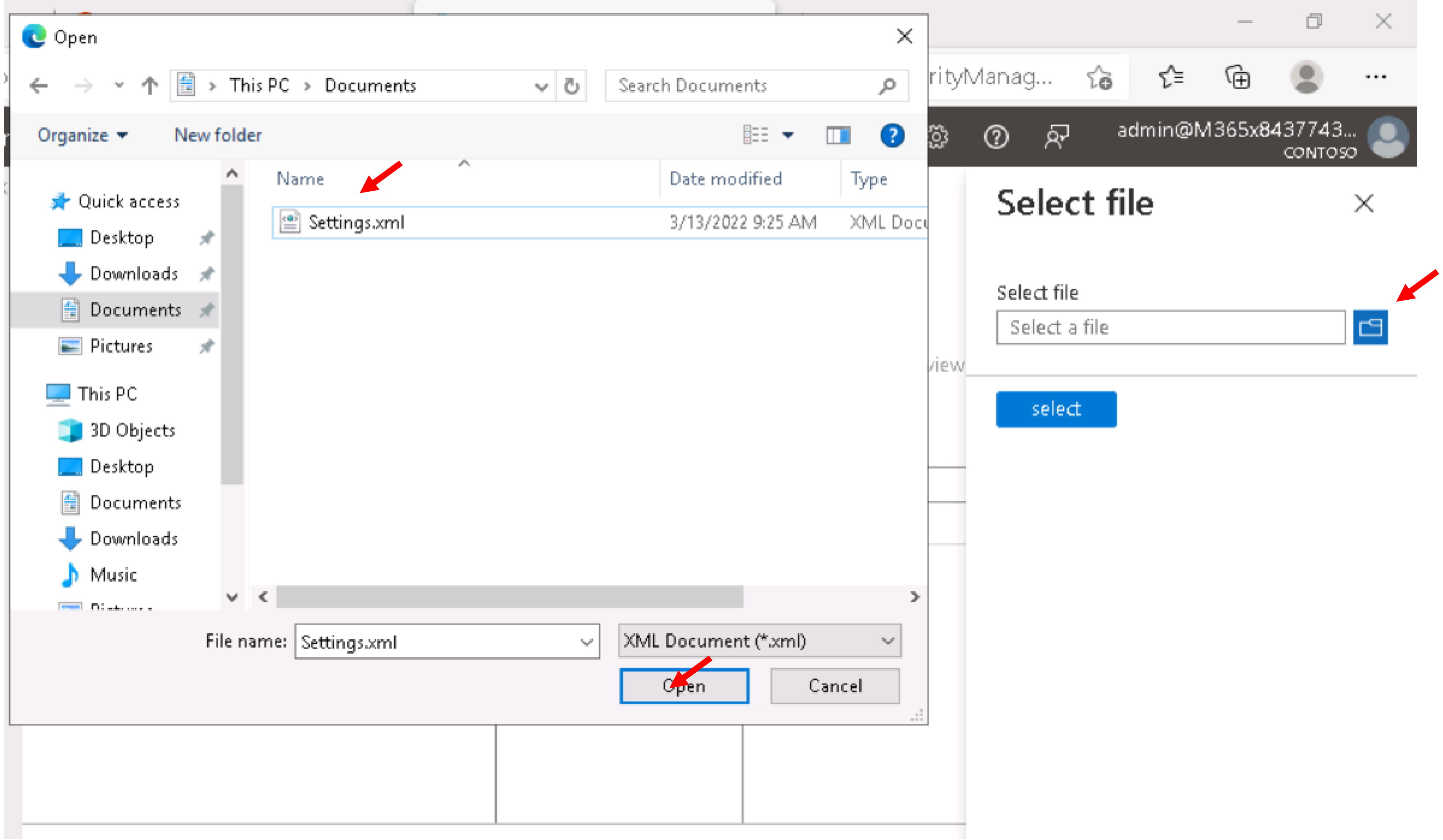


No items match your search.

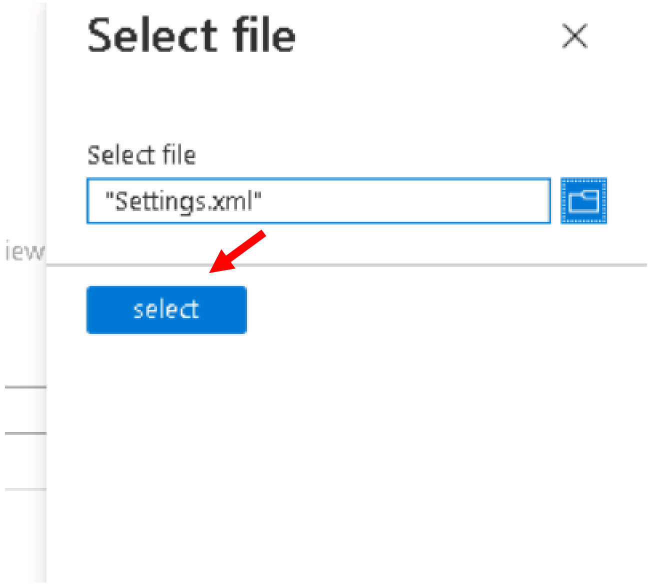
File name: Settings.xml

Save as type: XML File (*.xml)


Microsoft Endpoint Manager admin center
3
admin
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security >
Create profile ...
Exploit protection
Basics
2 Configuration settings
3 Scope tags
4 Assignments
5 Review + create
Settings
Search for a setting
Exploit Protection
Upload XML
+ Select XML File
Previous
Next

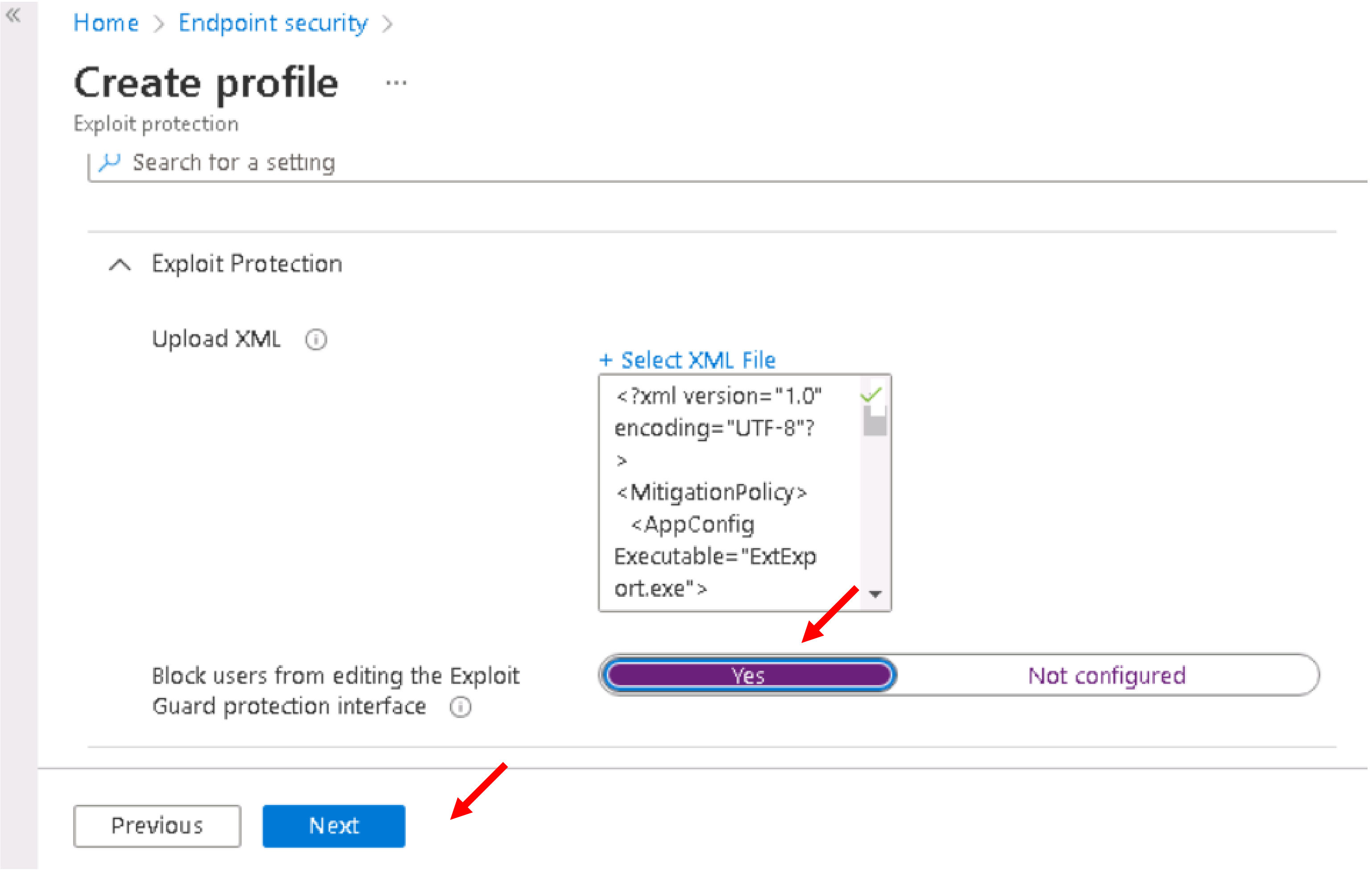


Open
This PC › Documents
Search Documents
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
This PC
3D Objects
Desktop
Documents
Downloads
Music
Name
Date modified
Type
Settings.xml
3/13/2022 9:25 AM
XML Docu
File name:
Settings.xml
XML Document (*.xml)
Open
Cancel
rityManag...
admin@M365x8437743...
CONTOSO
Select file
Select file
Select a file
select



Select file

Select file: "Settings.xml"



Home > Endpoint security >

Create profile ...

Exploit protection

Search for a setting

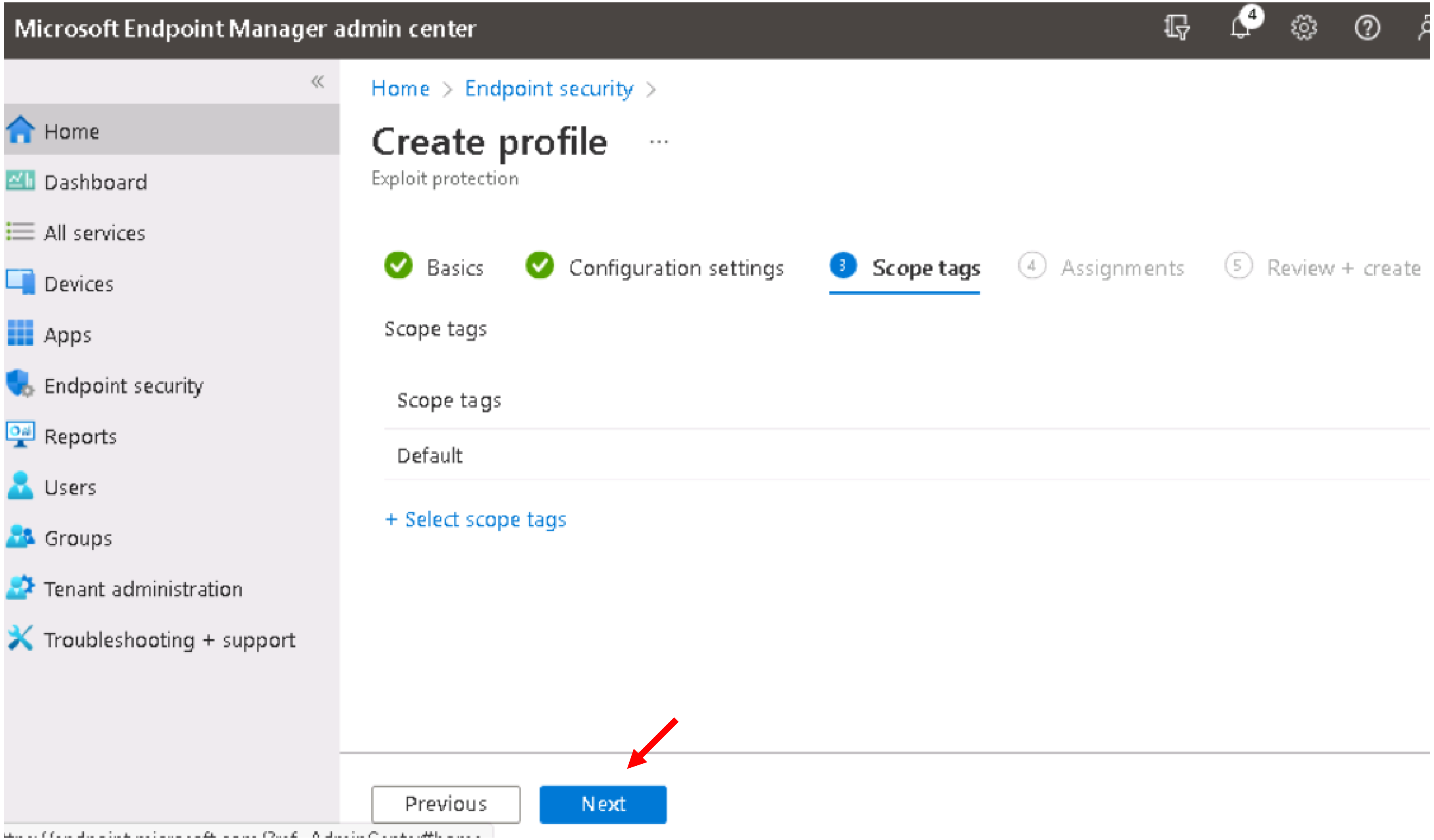
Exploit Protection

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 ···

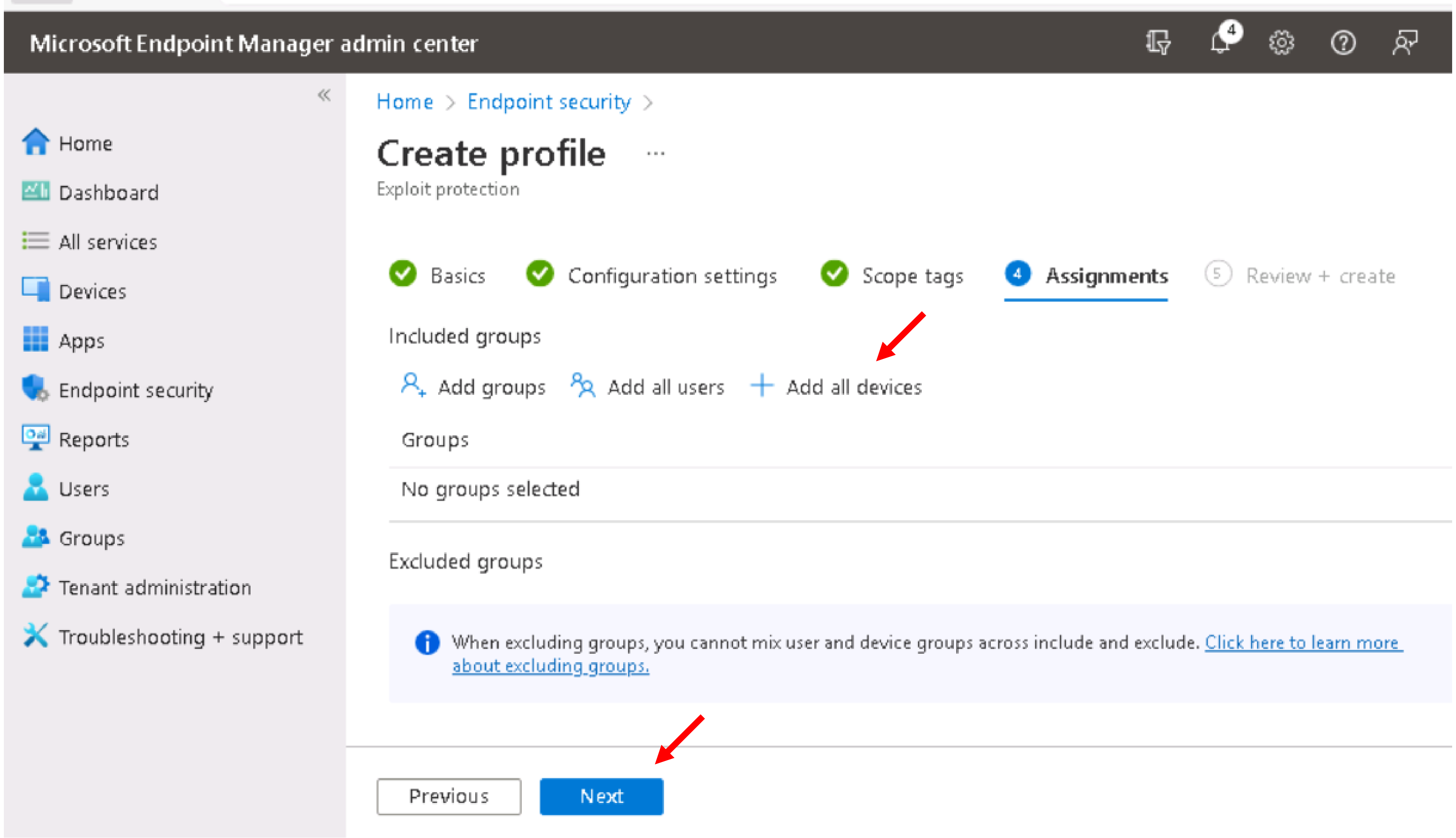
Exploit protection

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

Scope tags

Scope tags
Default

+ Select scope tags



Create profile ...

Exploit protection

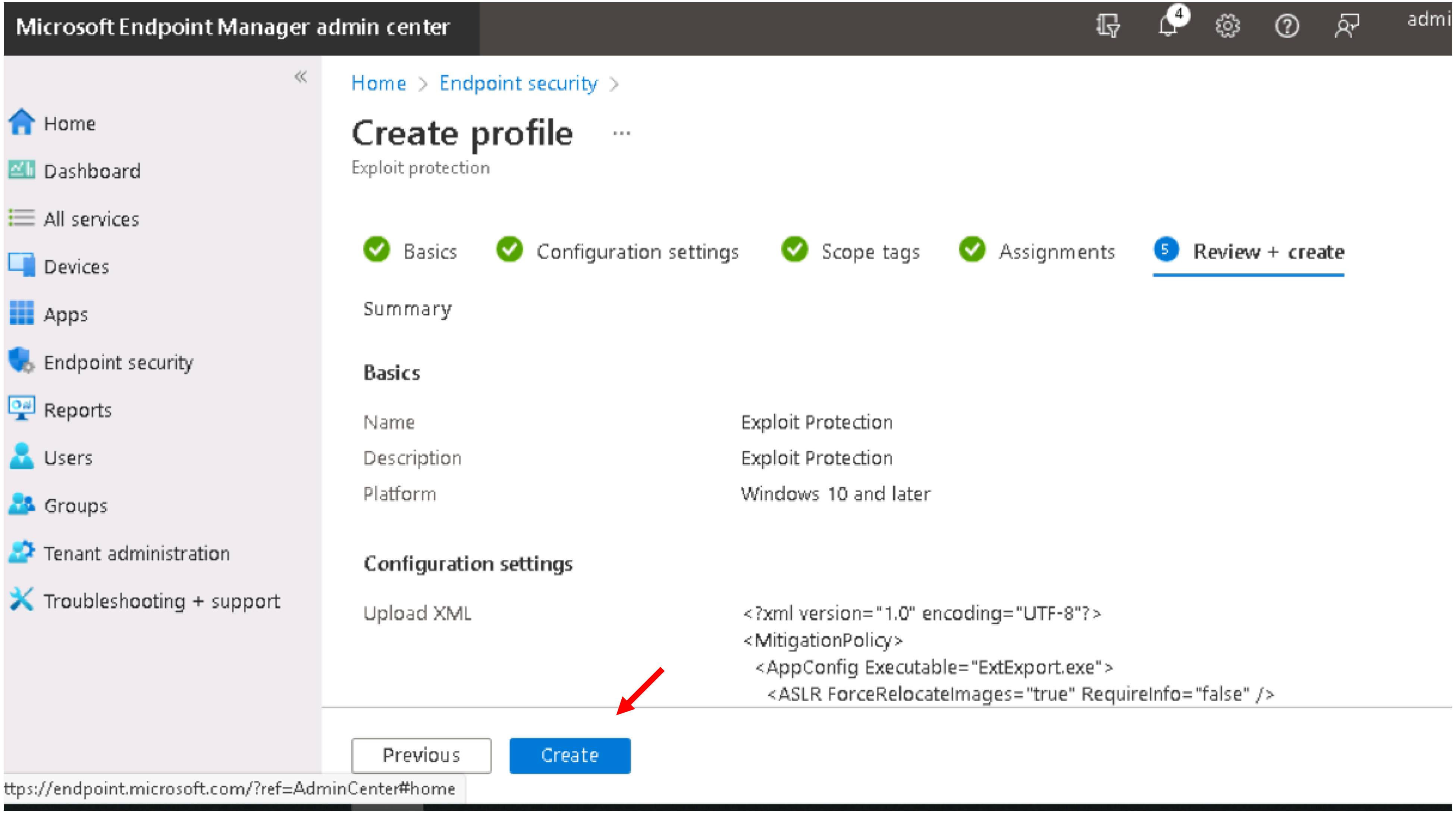
Included groups

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 ...

Exploit protection

Summary

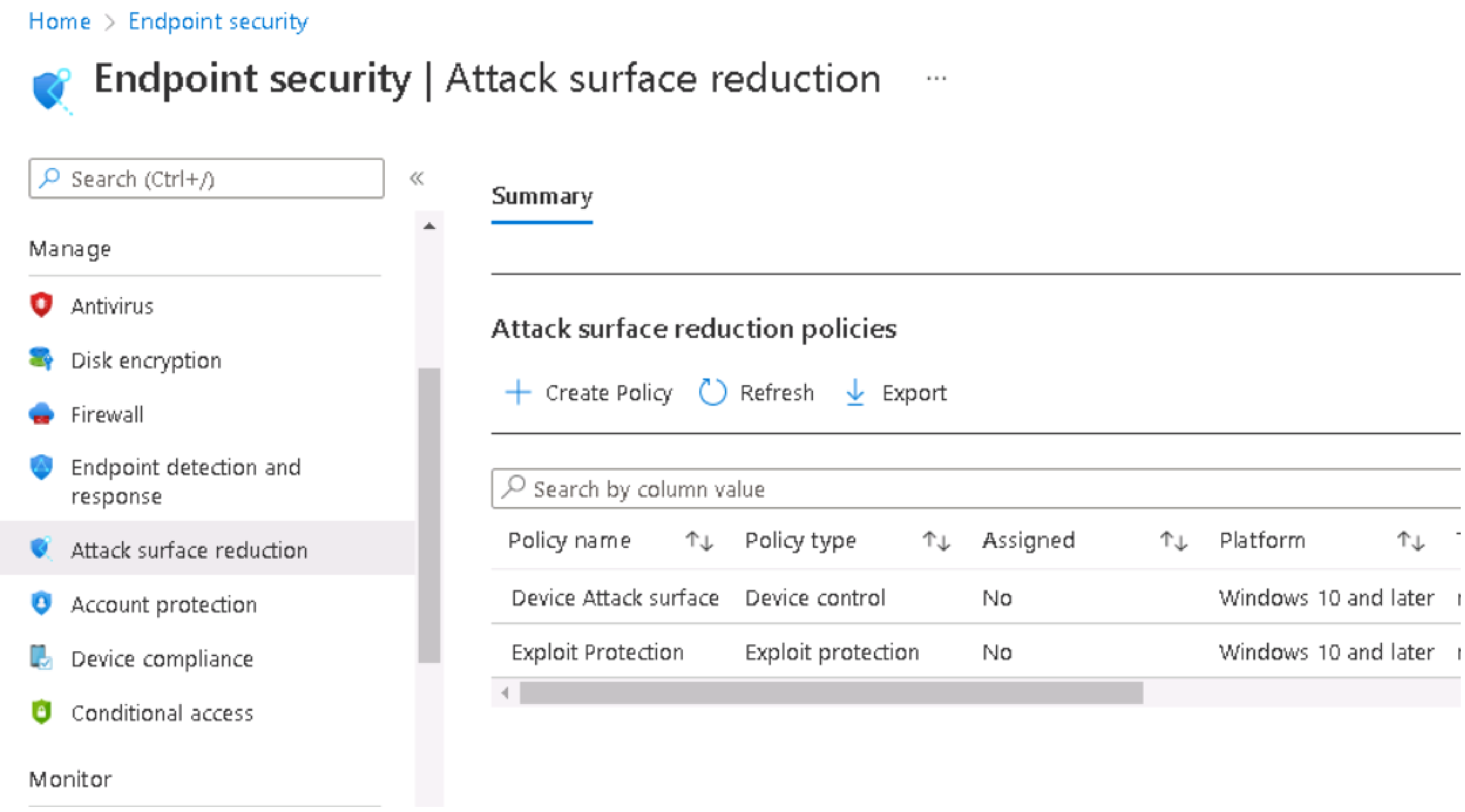
Basics

Name	Exploit Protection
Description	Exploit Protection
Platform	Windows 10 and later

Configuration settings

Upload XML

```
<?xml version="1.0" encoding="UTF-8"?>
<MitigationPolicy>
  <AppConfig Executable="ExtExport.exe">
    <ASLR ForceRelocateImages="true" RequireInfo="false" />
```



Attack surface reduction policies

Policy name	Policy type	Assigned	Platform
Device Attack surface	Device control	No	Windows 10 and later
Exploit Protection	Exploit protection	No	Windows 10 and later