Need to Know Microsoft 365 Webinar July 2024

@directorcia

http://about.me/ciaops

Web cast has started

Web cast is being recorded

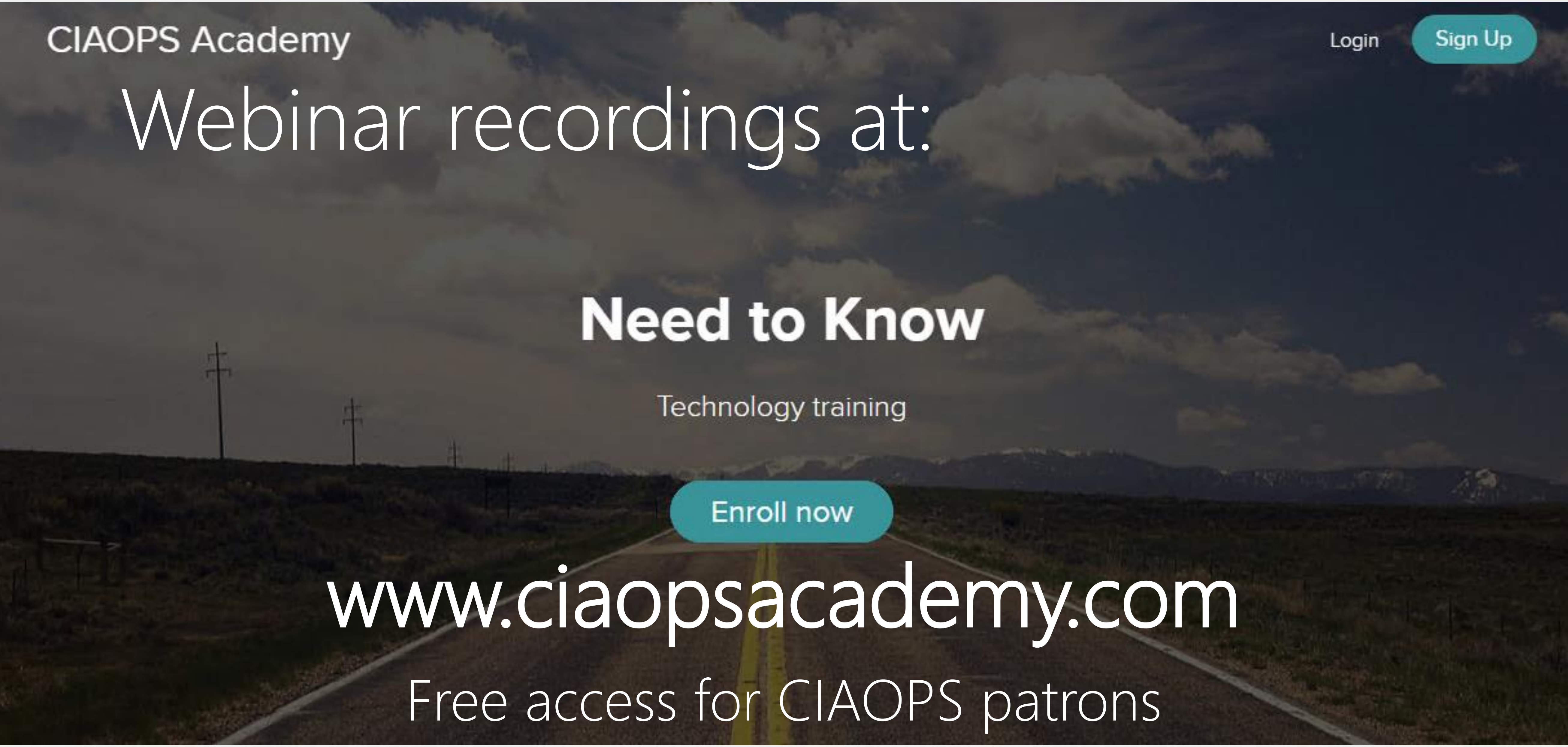
If you can’t hear anything check your speaker settings

For questions after the event:

Email : director@ciaops.com

Twitter : @directorcia

Webinar recordings at:



CIAOPS Academy

Need to Know

Technology training

www.ciaopsacademy.com

Free access for CIAOPS patrons

https://blog.ciaops.com/2022/07/29/join-my-teams-shared-channel/

Join my free shared Channel

Agenda

-Microsoft 365 Update

-Defender for Business

-Q & A

Microsoft 365 Update

News

- Try out the new Copilot in Planner (preview) today in the new Microsoft Planner in Teams
  - https://techcommunity.microsoft.com/t5/planner-blog/try-out-the-new-copilot-in-planner-preview-today-in-the-new/ba-p/4193042
- The Microsoft Copilot Dashboard is now included with Copilot for Microsoft 365
  - https://techcommunity.microsoft.com/t5/viva-insights-blog/the-microsoft-copilot-dashboard-is-now-included-with-copilot-for/ba-p/4198372
- Copilot Learning Hub: Your Gateway to Mastering Microsoft Copilot
  - https://techcommunity.microsoft.com/t5/microsoft-developer-community/copilot-learning-hub-your-gateway-to-mastering-microsoft-copilot/ba-p/4189618
- Preview of Inbound SMTP DANE with DNSSEC for Exchange Online
  - https://techcommunity.microsoft.com/t5/exchange-team-blog/announcing-public-preview-of-inbound-smtp-dane-with-dnssec-for/ba-p/4155257
- Guest sharing now available in Microsoft Loop
  - https://insider.microsoft365.com/en-us/blog/guest-sharing-now-available-in-microsoft-loop

Defender for Business

Microsoft Defender for Business

Elevate your security

Elevate your security with enterprise-grade endpoint protection specially built for businesses with up to 300 employees.

Enterprise-grade protection

Security for all your devices with next-gen protection, endpoint detection and response, and threat and vulnerability management.

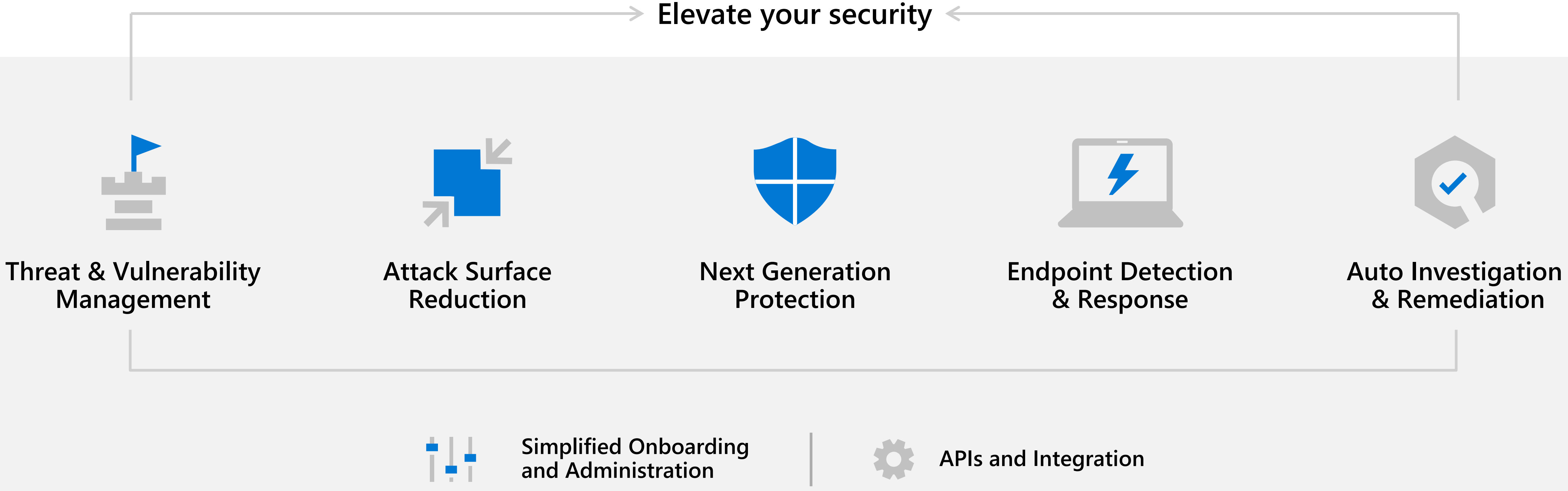
Easy to use

Streamline onboarding with wizard-driven set up and recommended security policies activated out-of-the-box to quickly secure devices.

Cost-effective

Endpoint security that keeps you productive and works with your IT without compromising budget.

Microsoft Defender
for Business



Elevate your security

Threat & Vulnerability Management

Attack Surface Reduction

Next Generation Protection

Endpoint Detection & Response

Auto Investigation & Remediation

Simplified Onboarding and Administration

APIs and Integration

Delivering endpoint security across platforms

Windows macOS

Endpoints

iOS

Mobile device OS

Windows 365

Azure Virtual Desktop

Virtual desktops

How to purchase Microsoft Defender for Business

Microsoft Defender Business ($3pupm)

Enterprise-grade endpoint security

Per user license

- ✓ Next generation protection
- ✓ Cross Platform support (iOS, Android, Windows, MacOS)
- ✓ Endpoint Detection and Response
- ✓ Threat and Vulnerability Management
- ✓ ...and more

Microsoft 365 Business Premium ($20pupm)

Comprehensive productivity and security solution

Per user license

Microsoft 365 Business Standard ($12.50)
Office apps and services, Teams

+

- Microsoft Defender for Business
- Microsoft Defender for Office 365 Plan 1
- Intune
- Azure AD Premium Plan 1
- Azure Information Protection Premium P1
- Exchange Online Archiving
- Autopilot
- Azure Virtual Desktop license
- Windows 10/11 Business
- Shared Computer Activation

1) As standalone SKU

Entitlement for use on up to 5 devices

Generally available H1 2022

2) Included as part of Microsoft 365 Business Premium

Microsoft Defender for Business will roll out to new and existing M365 Business Premium customers, post GA

Product comparison

Cross platform and enterprise grade protection with next-gen protection, endpoint detection and response, and threat and vulnerability management

Available as a standalone offering and as part of Microsoft 365 Business Premium

Standalone offering will serve non-Microsoft 365 customers. No licensing prerequisites

Supports multi-customer viewing of security incidents with Microsoft 365 Lighthouse for partners in preview

Customer size	< 300 seats	> 300 seats	
Endpoint capabilities\SKU	**Microsoft Defender for Business**	**Microsoft Defender for Endpoint Plan 1**	**Microsoft Defender for Endpoint Plan 2**
Centralized management	✓	✓	✓
Simplified client configuration	✓		
Threat and Vulnerability Management	✓		✓
Attack Surface Reduction	✓	✓	✓
Next-Gen Protection	✓	✓	✓
Endpoint Detection and Response	✓[2]		✓
Automated Investigation and Response	✓[2]		✓
Threat Hunting and 6-months data retention			✓
Threat Analytics	✓[2]		✓
Cross platform support for Windows, MacOS, iOS, and Android	✓	✓	✓
Microsoft Threat Experts			✓
Partner APIs	✓	✓	✓
Microsoft 365 Lighthouse for viewing security incidents across customers	✓[3]		

[1]Limited. [2] Optimized for SMB. [3] Additional capabilities planned

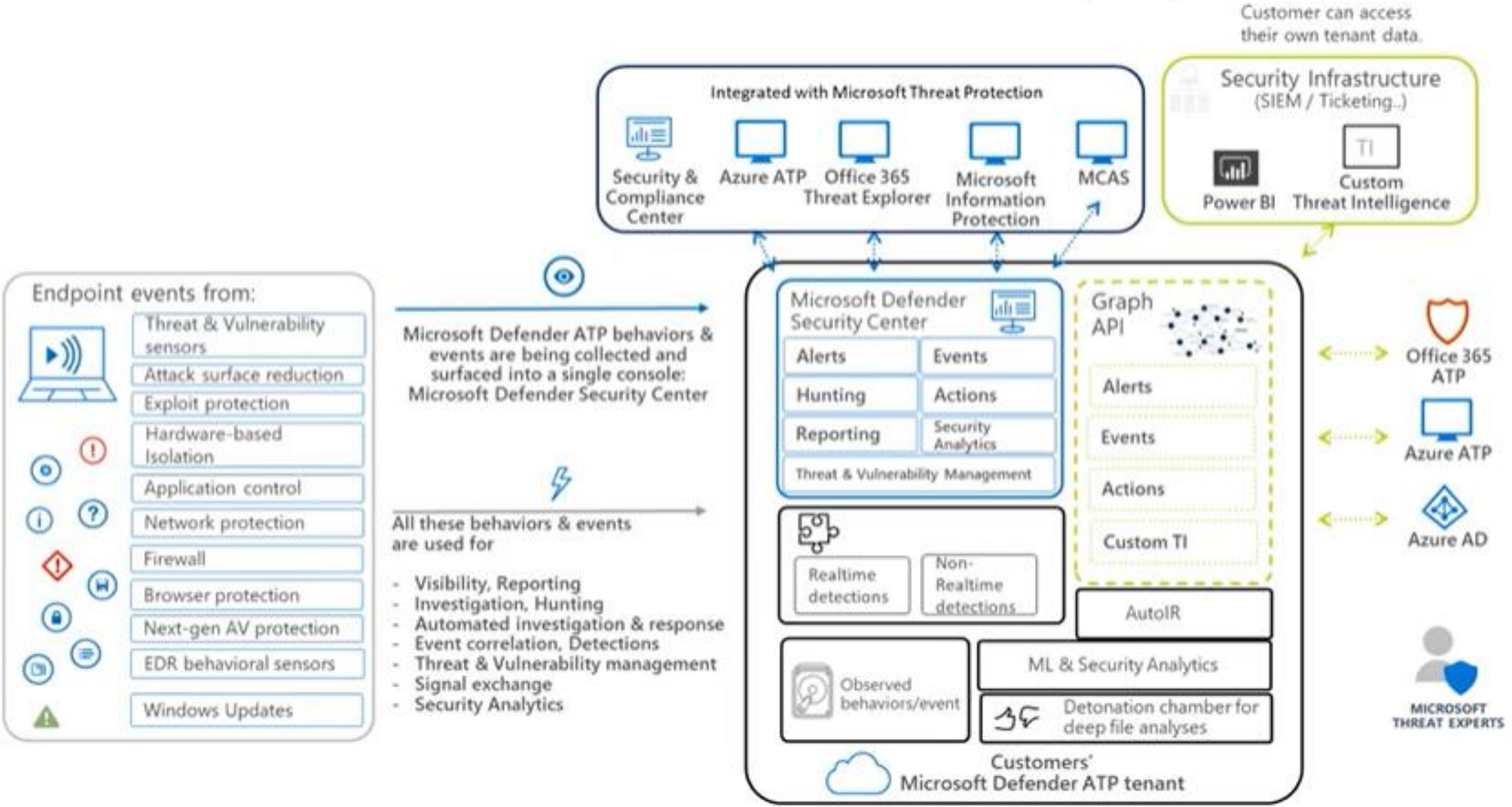
Detailed product comparison

Capabilities	MDB	MDE P1	MDE P2
Threat & Vulnerability			
Microsoft secure score	●		●
Vulnerability management (visibility into software and vulnerabilities)	●		●
Vulnerability remediation based on Intune integration	●		●
Attack Surface Reduction			
Advanced vulnerability and zero-day exploit mitigations	●	●	●
Attack Surface Reduction rules	●	●	●
Application Control	●	●	●
Network Firewall	●	●	●
Device Control (e.g.: USB)	●	●	●
Network protection	●	●	●
Device-based conditional access	●	●	●
Web Control / Category-based URL Blocking	●	●	●
Ransomware mitigation	●	●	●
Next Gen Protection			
Advanced cloud protection (deep inspection and detonation) BAFS	●	●	●
Monitoring, analytics and reporting for Next Generation Protection capabilities	●	●	●
Endpoint Detection and Response			
Behavioral-based detection (post-breach)	●		●
Rich investigation tools			●
Custom detections			●
6-month searchable data per endpoint			●
Advanced hunting			●
Evaluation Lab			●
Manual response actions - (Run AV scan, Machine isolation, File stop and quarantine)	●	●	●
Live response	●		●

Detailed product comparison

Capabilities	MDB	MDE P1	MDE P2
Automatic Investigation and Remediation			
Default automation levels	●		●
Customized automation levels			●
Centralized Management			
Role-based access control	●	●	●
Simplified client configuration	●		
Reporting	●	●	●
API's			
SIEM Connector		●	●
API's (Response, Data collection)		●	●
Partner applications		●	●
Threat Intelligence			
Threat Analytics	●		●
Custom Threat Intelligence	●	●	●
Sandbox			●
3rd party Threat Intelligence Connector			●
Partner Support			
APIs (For Partners)	●	●	●
RMM Integration	●		
MSP Support (Multi-tenant API, multi tenant authentication)	●	●	●
Microsoft Threat Expert			
Targeted attack notification			●
Collaborate with Experts, on demand			●
Platform support			
Windows Client	●	●	●
MacOS	●	●	●
Mobile (Android, iOS)	●	●	●

Microsoft Defender Advanced Threat Protection (ATP)



Endpoint events from:

- Threat & Vulnerability sensors
- Attack surface reduction
- Exploit protection
- Hardware-based Isolation
- Application control
- Network protection
- Firewall
- Browser protection
- Next-gen AV protection
- EDR behavioral sensors
- Windows Updates

Microsoft Defender ATP behaviors & events are being collected and surfaced into a single console: Microsoft Defender Security Center

All these behaviors & events are used for

- Visibility, Reporting
- Investigation, Hunting
- Automated investigation & response
- Event correlation, Detections
- Threat & Vulnerability management
- Signal exchange
- Security Analytics

Integrated with Microsoft Threat Protection

Security & Compliance Center

Azure ATP

Office 365 Threat Explorer

Microsoft Information Protection

MCAS

Customer can access their own tenant data.

Security Infrastructure (SIEM / Ticketing..)

Power BI

TI

Custom Threat Intelligence

Microsoft Defender Security Center

Alerts | Events

Hunting | Actions

Reporting | Security Analytics

Threat & Vulnerability Management

Realtime detections

Non-Realtime detections

Observed behaviors/event

Graph API

Alerts

Events

Actions

Custom TI

AutoIR

ML & Security Analytics

Detonation chamber for deep file analyses

Customers' Microsoft Defender ATP tenant

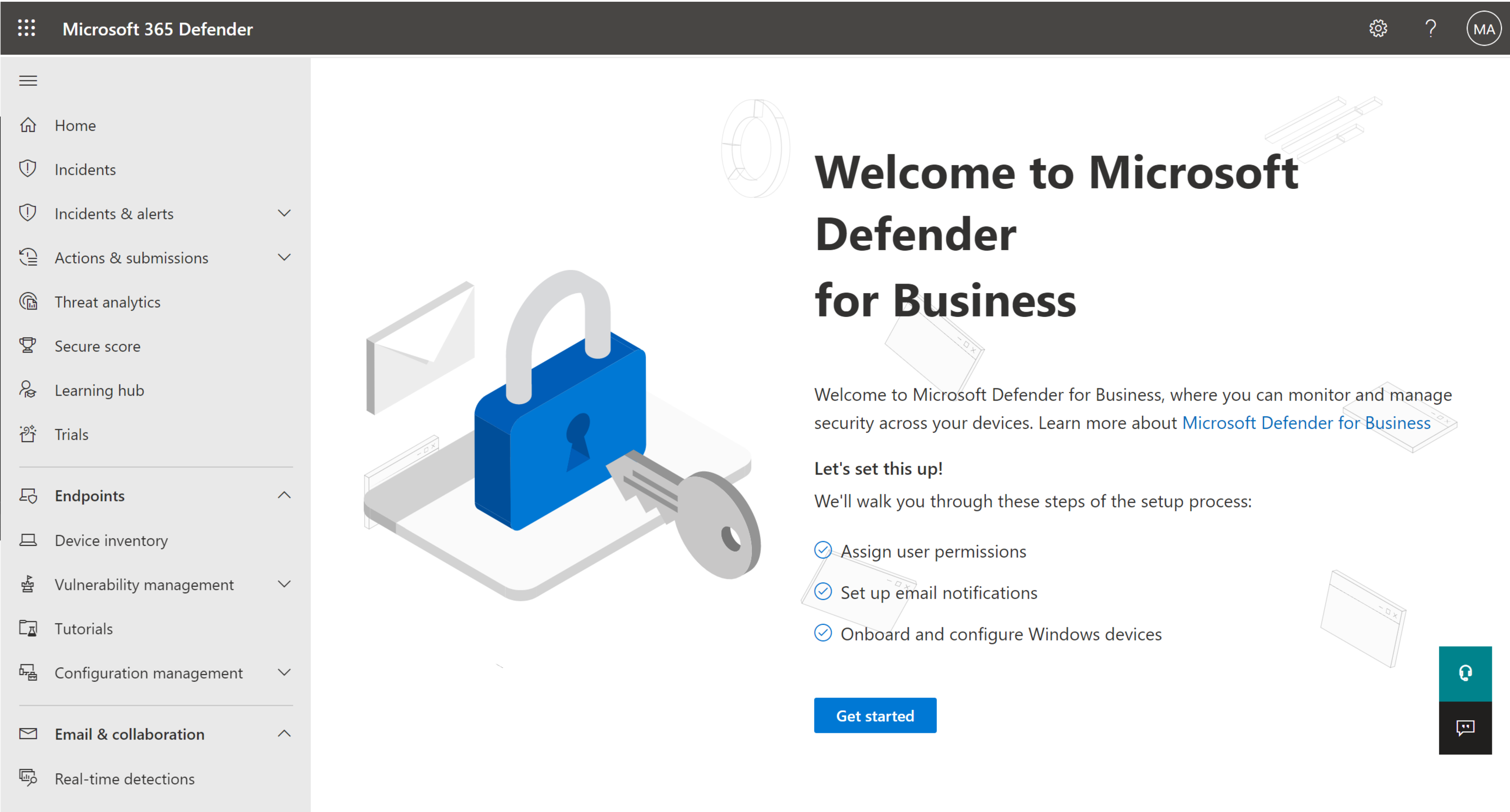
Office 365 ATP

Azure ATP

Azure AD

MICROSOFT THREAT EXPERTS

Initial setup



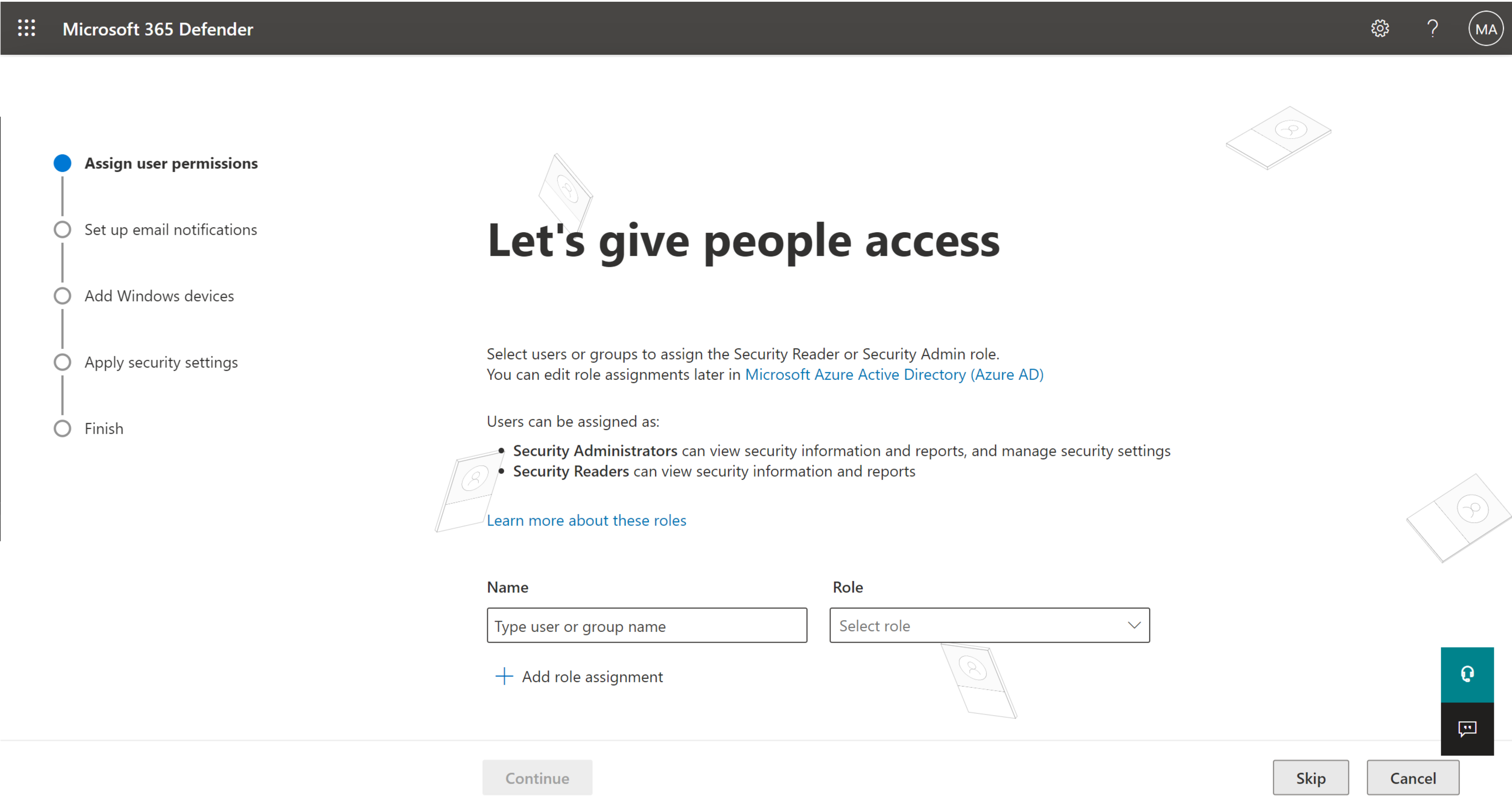
Welcome to Microsoft Defender for Business

Welcome to Microsoft Defender for Business, where you can monitor and manage security across your devices. Learn more about Microsoft Defender for Business

Let's set this up!

We'll walk you through these steps of the setup process:

- ✓ Assign user permissions
- ✓ Set up email notifications
- ✓ Onboard and configure Windows devices



● **Assign user permissions**

○ Set up email notifications

○ Add Windows devices

○ Apply security settings

○ Finish

Let's give people access

Select users or groups to assign the Security Reader or Security Admin role.
You can edit role assignments later in Microsoft Azure Active Directory (Azure AD)

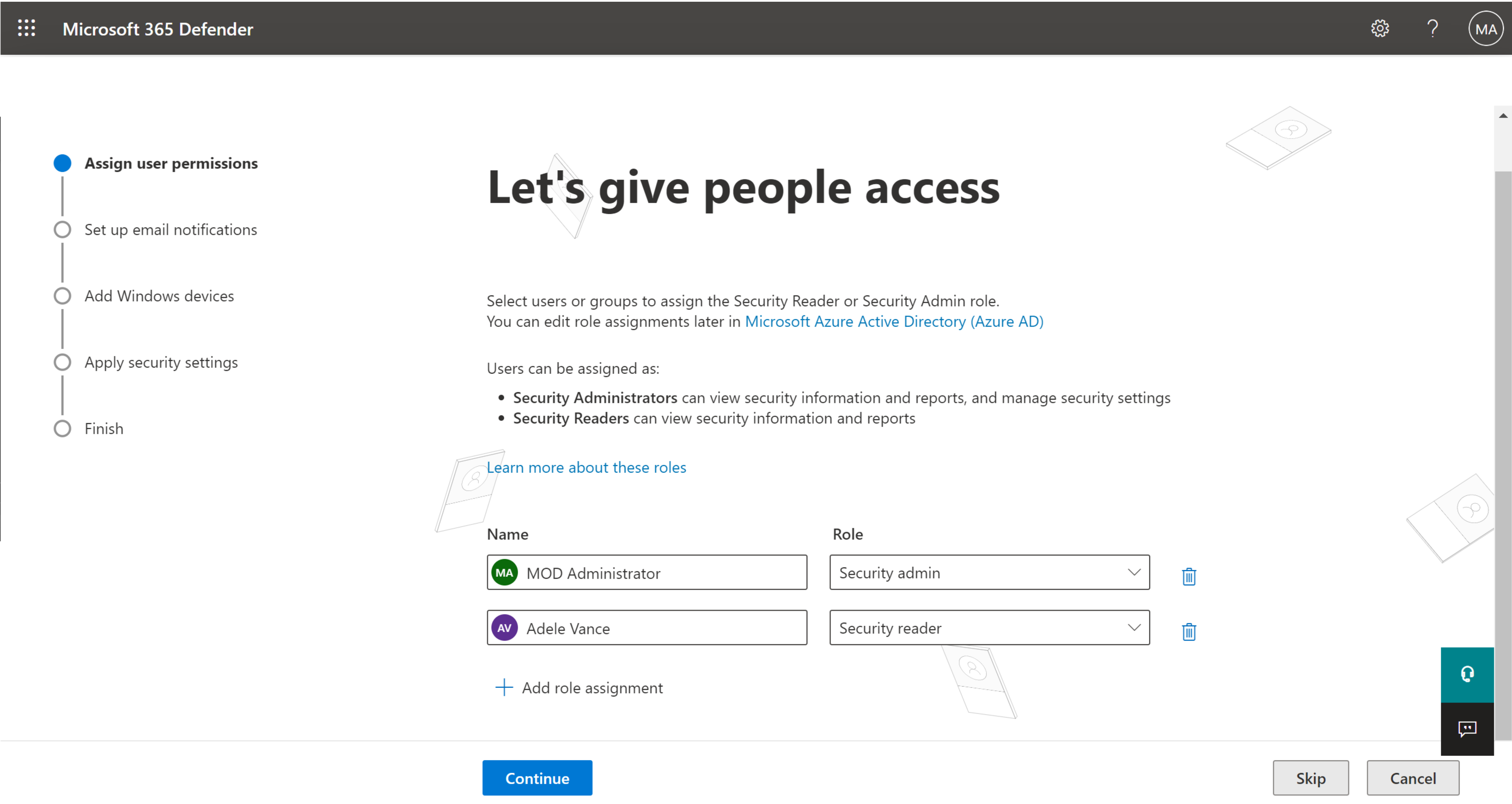
Users can be assigned as:

- **Security Administrators** can view security information and reports, and manage security settings
- **Security Readers** can view security information and reports

Learn more about these roles

Name	Role
Type user or group name	Select role

+ Add role assignment



- ● **Assign user permissions**
- ○ Set up email notifications
- ○ Add Windows devices
- ○ Apply security settings
- ○ Finish

Let's give people access

Select users or groups to assign the Security Reader or Security Admin role.
You can edit role assignments later in Microsoft Azure Active Directory (Azure AD)

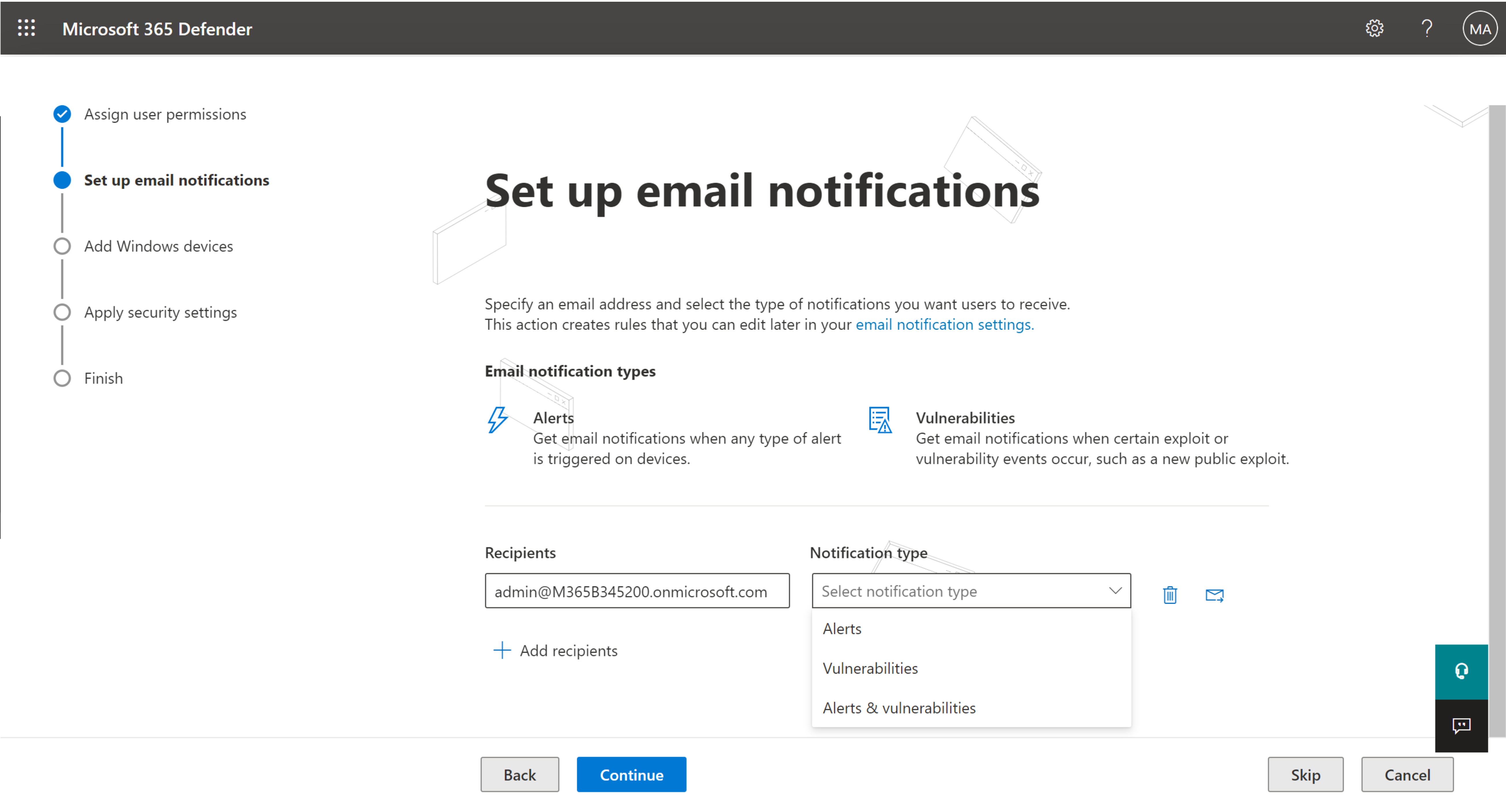
Users can be assigned as:

- **Security Administrators** can view security information and reports, and manage security settings
- **Security Readers** can view security information and reports

Learn more about these roles

Name	Role
MA MOD Administrator	Security admin
AV Adele Vance	Security reader

+ Add role assignment



Microsoft 365 Defender
MA
✓ Assign user permissions
● Set up email notifications
○ Add Windows devices
○ Apply security settings
○ Finish

Set up email notifications

Specify an email address and select the type of notifications you want users to receive.
This action creates rules that you can edit later in your email notification settings.

Email notification types

Alerts
Get email notifications when any type of alert is triggered on devices.

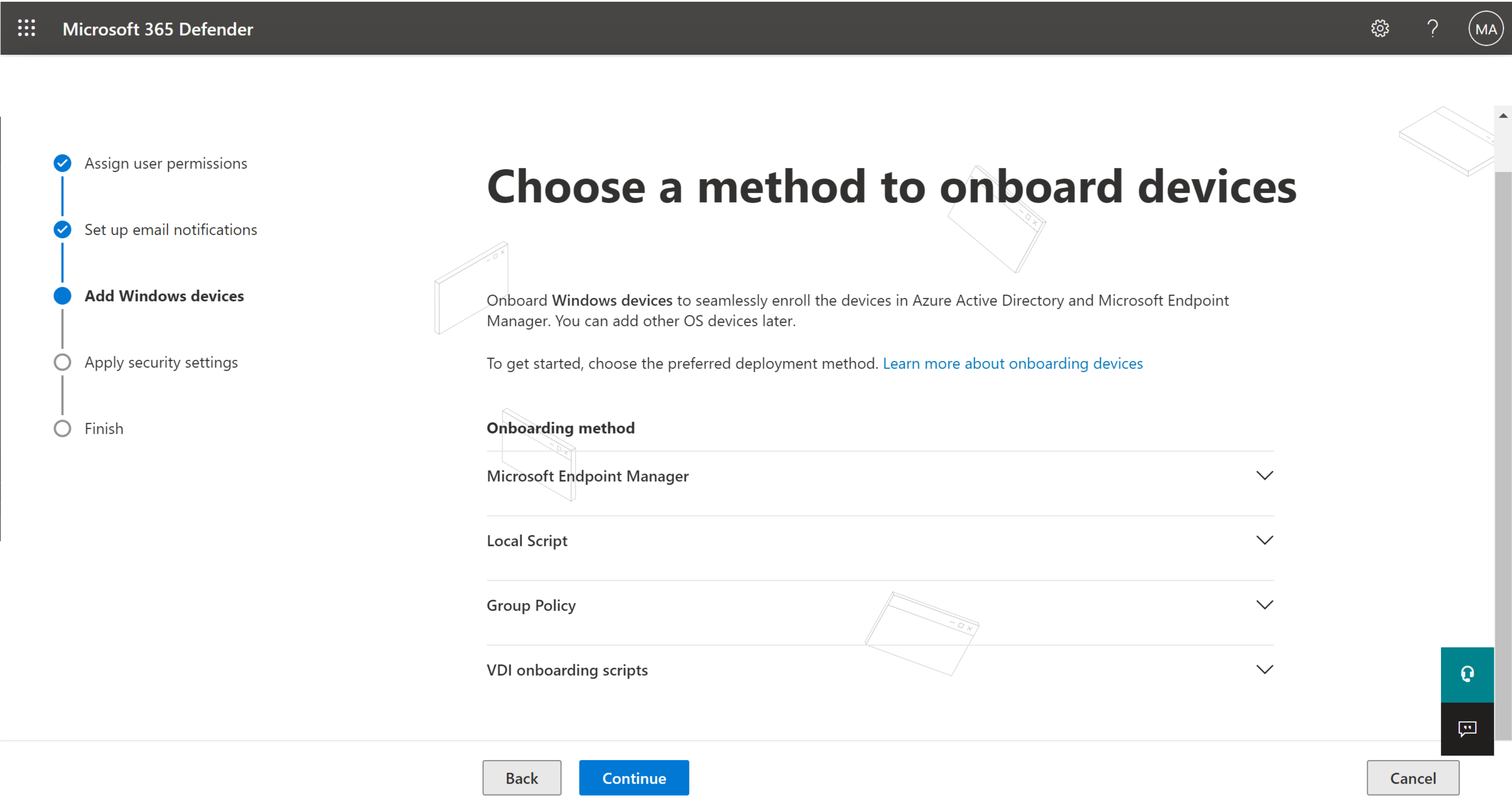
Vulnerabilities
Get email notifications when certain exploit or vulnerability events occur, such as a new public exploit.

Recipients

admin@M365B345200.onmicrosoft.com

Notification type

Select notification type



- ✓ Assign user permissions
- ✓ Set up email notifications
- ● **Add Windows devices**
- ○ Apply security settings
- ○ Finish

Choose a method to onboard devices

Onboard **Windows devices** to seamlessly enroll the devices in Azure Active Directory and Microsoft Endpoint Manager. You can add other OS devices later.

To get started, choose the preferred deployment method. Learn more about onboarding devices

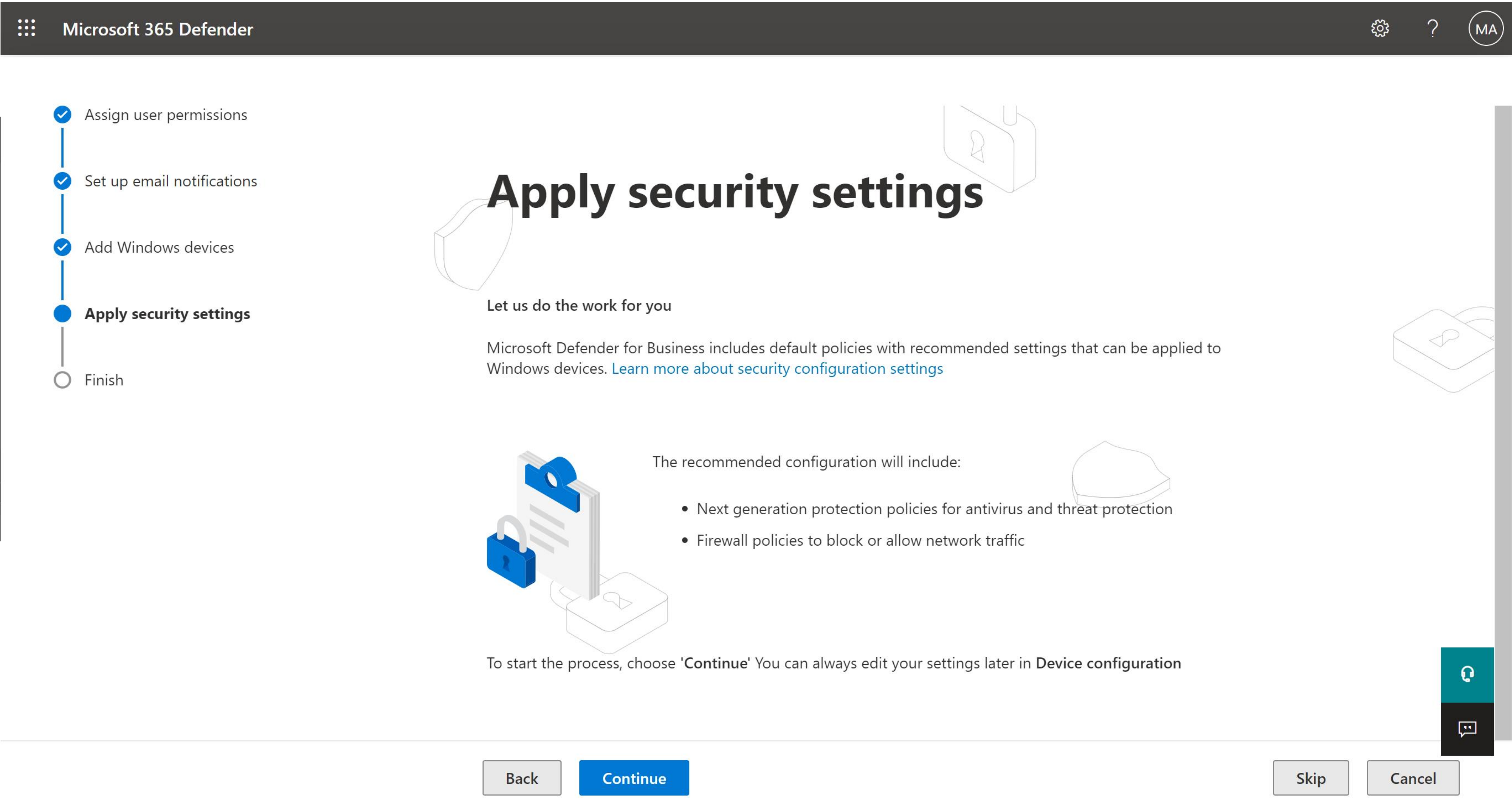
Onboarding method

Microsoft Endpoint Manager

Local Script

Group Policy

VDI onboarding scripts



Apply security settings

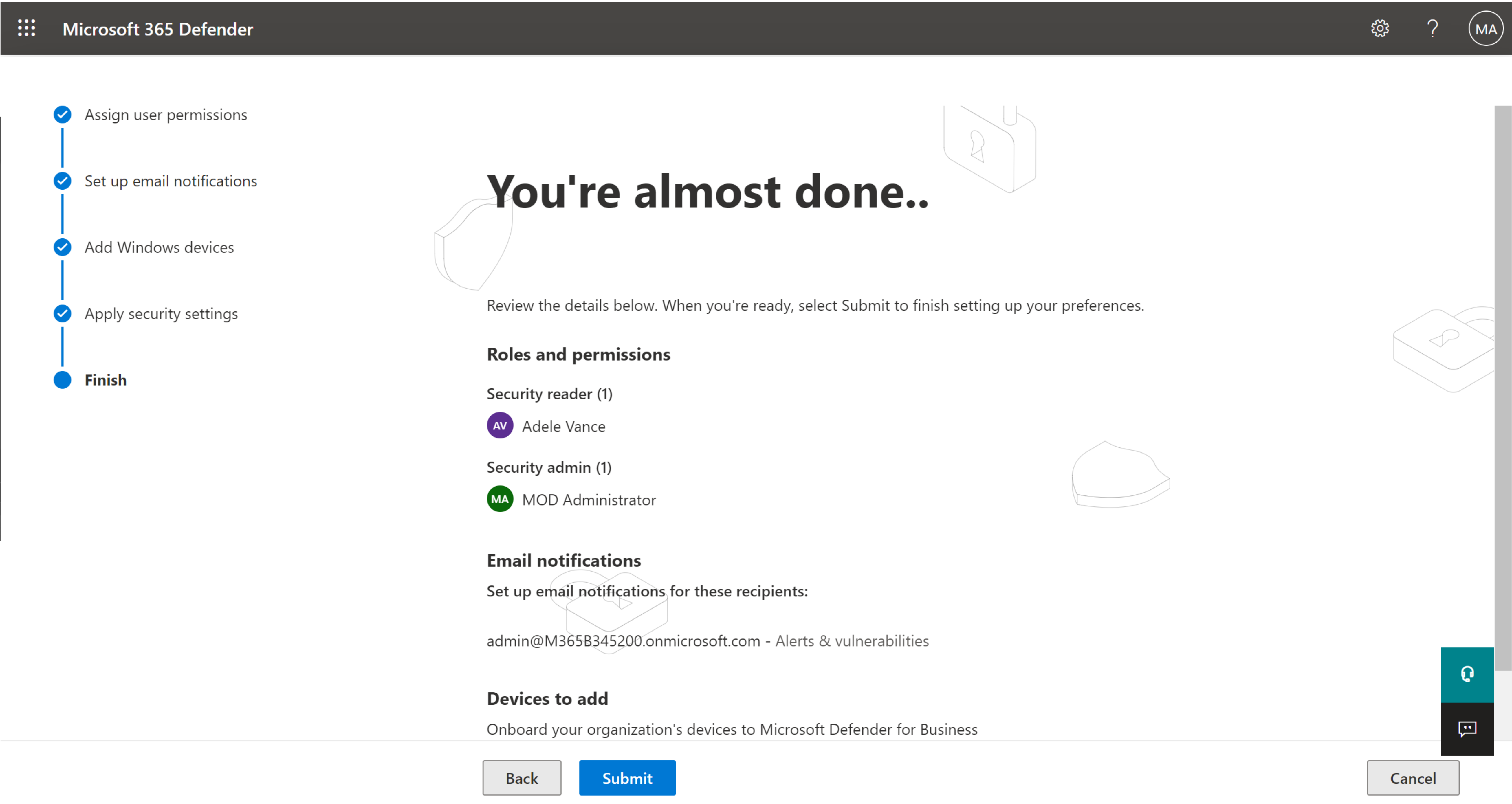
Let us do the work for you

Microsoft Defender for Business includes default policies with recommended settings that can be applied to Windows devices. Learn more about security configuration settings

The recommended configuration will include:

- Next generation protection policies for antivirus and threat protection
- Firewall policies to block or allow network traffic

To start the process, choose '**Continue**' You can always edit your settings later in **Device configuration**



You're almost done..

Review the details below. When you're ready, select Submit to finish setting up your preferences.

Roles and permissions

Security reader (1)

AV Adele Vance

Security admin (1)

MA MOD Administrator

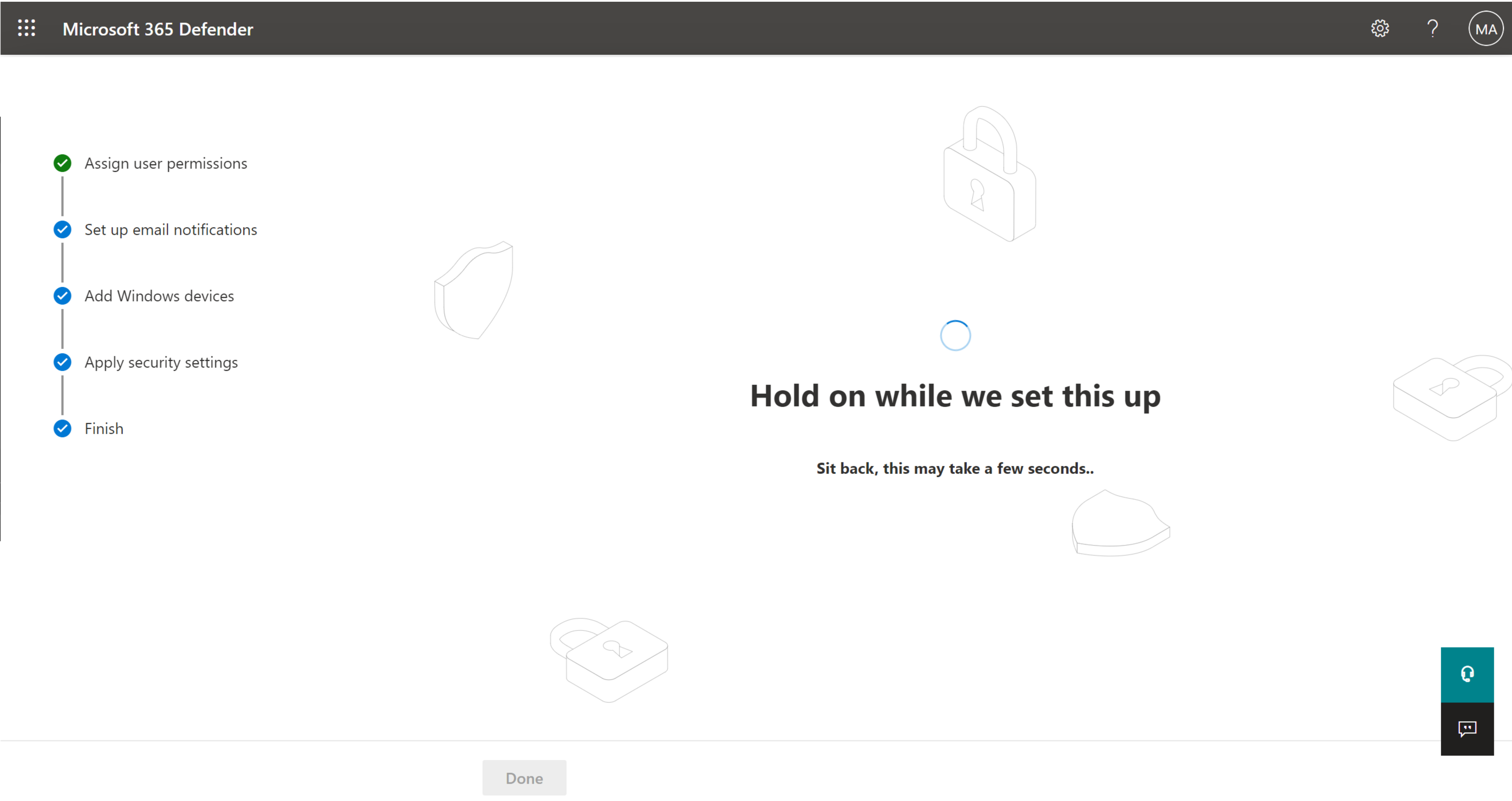
Email notifications

Set up email notifications for these recipients:

admin@M365B345200.onmicrosoft.com - Alerts & vulnerabilities

Devices to add

Onboard your organization's devices to Microsoft Defender for Business



✓ Assign user permissions

✓ Set up email notifications

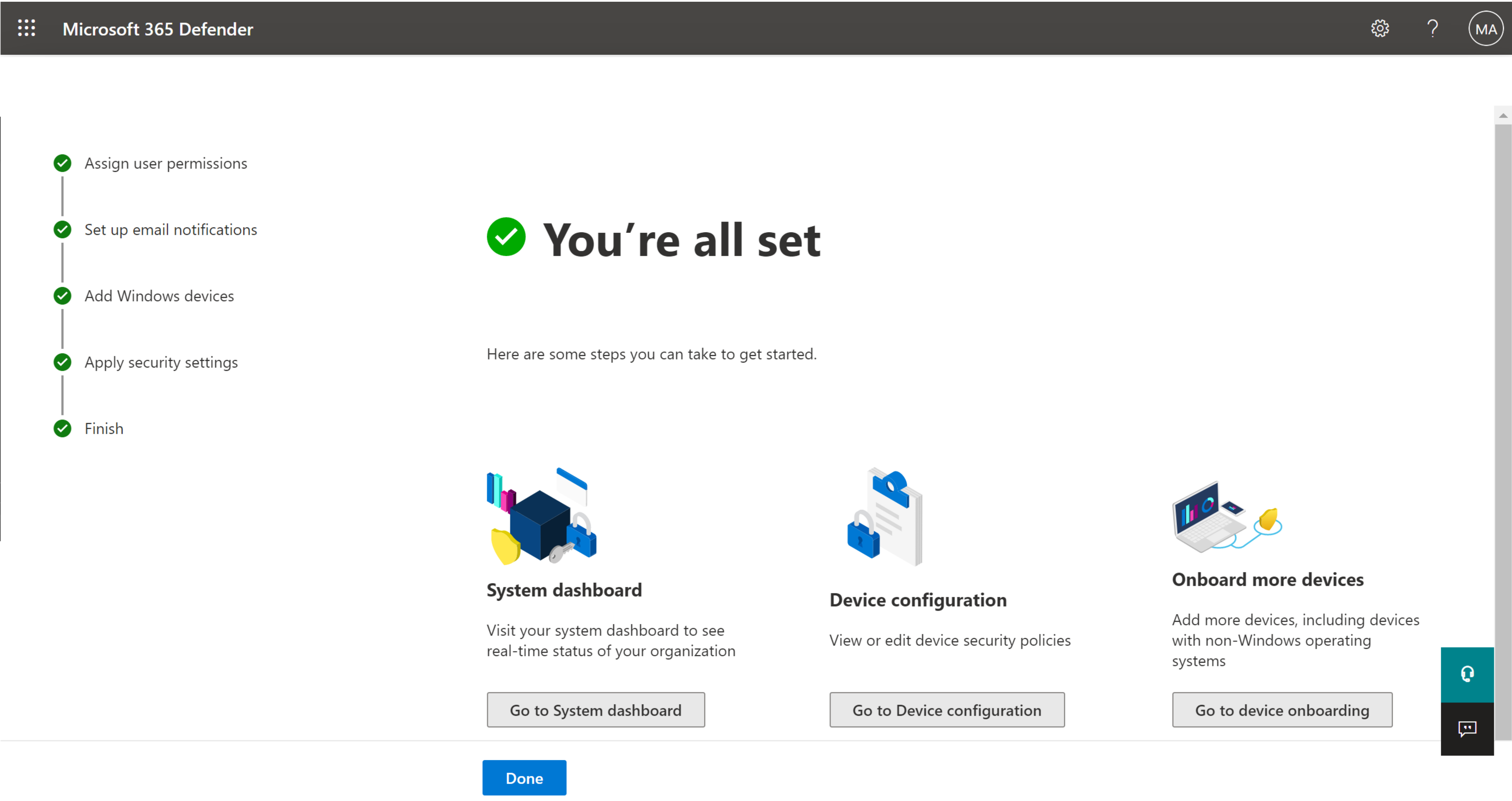
✓ Add Windows devices

✓ Apply security settings

✓ Finish

Hold on while we set this up

Sit back, this may take a few seconds..



- ✓ Assign user permissions
- ✓ Set up email notifications
- ✓ Add Windows devices
- ✓ Apply security settings
- ✓ Finish

✓ You're all set

Here are some steps you can take to get started.

System dashboard

Visit your system dashboard to see real-time status of your organization

Go to System dashboard

Device configuration

View or edit device security policies

Go to Device configuration

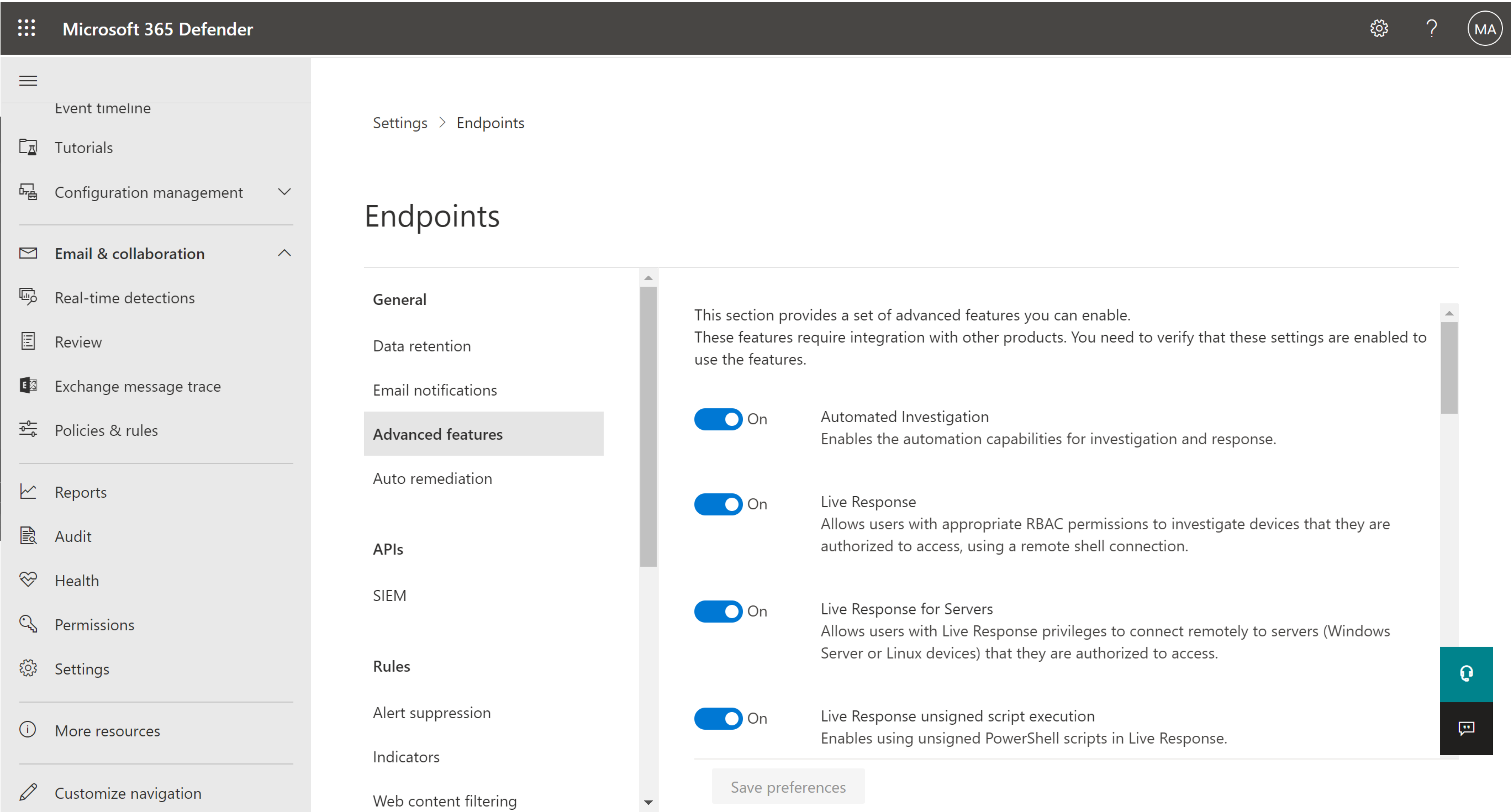
Onboard more devices

Add more devices, including devices with non-Windows operating systems

Go to device onboarding

Done

Enable features



Endpoints

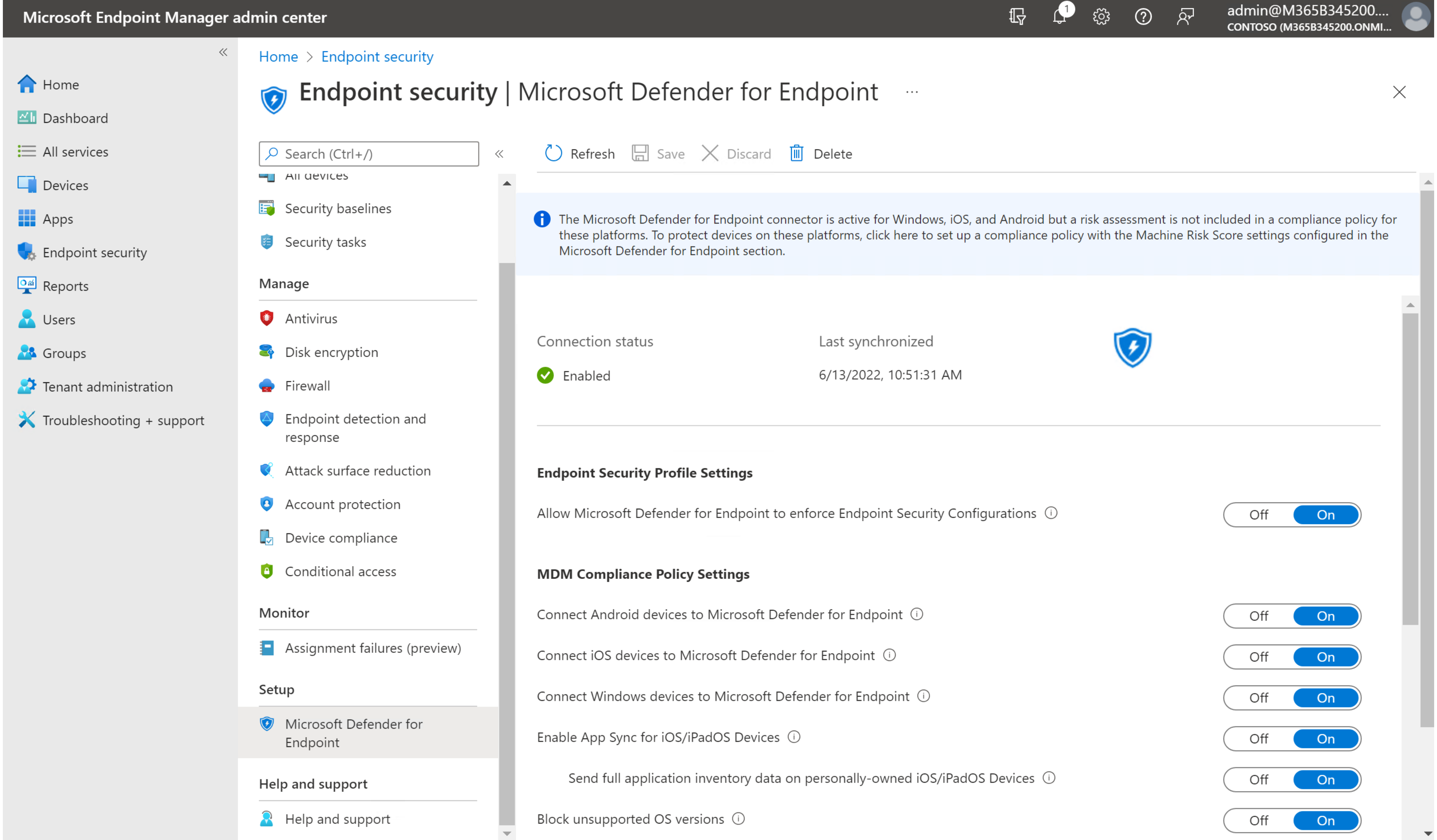
This section provides a set of advanced features you can enable.
These features require integration with other products. You need to verify that these settings are enabled to use the features.

On — **Automated Investigation**
Enables the automation capabilities for investigation and response.

On — **Live Response**
Allows users with appropriate RBAC permissions to investigate devices that they are authorized to access, using a remote shell connection.

On — **Live Response for Servers**
Allows users with Live Response privileges to connect remotely to servers (Windows Server or Linux devices) that they are authorized to access.

On — **Live Response unsigned script execution**
Enables using unsigned PowerShell scripts in Live Response.



Endpoint security | Microsoft Defender for Endpoint

The Microsoft Defender for Endpoint connector is active for Windows, iOS, and Android but a risk assessment is not included in a compliance policy for these platforms. To protect devices on these platforms, click here to set up a compliance policy with the Machine Risk Score settings configured in the Microsoft Defender for Endpoint section.

Connection status	Last synchronized
✓ Enabled	6/13/2022, 10:51:31 AM

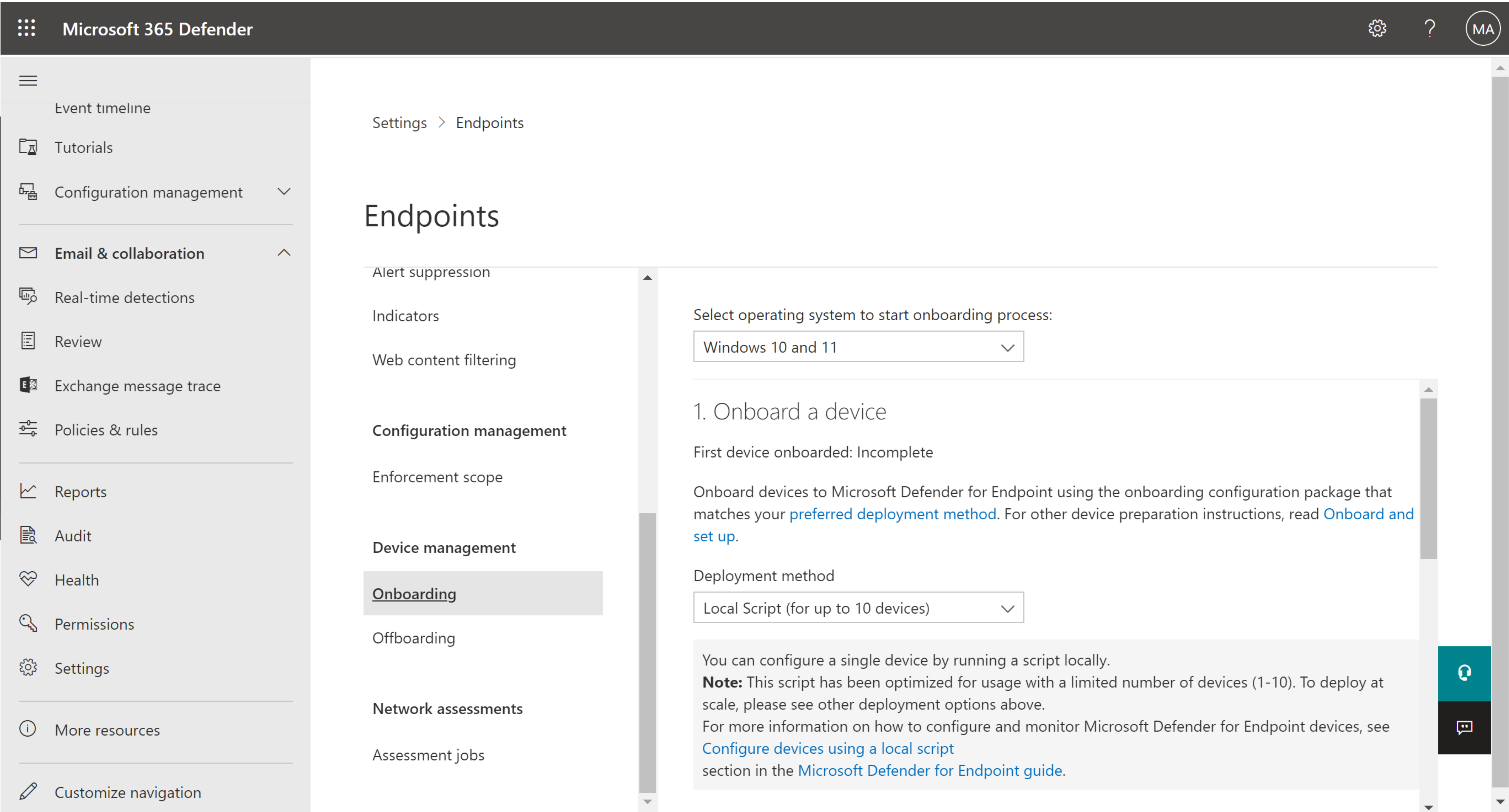
Endpoint Security Profile Settings

Allow Microsoft Defender for Endpoint to enforce Endpoint Security Configurations ⓘ	Off [✓ On]

MDM Compliance Policy Settings

Connect Android devices to Microsoft Defender for Endpoint ⓘ	Off [✓ On]
Connect iOS devices to Microsoft Defender for Endpoint ⓘ	Off [✓ On]
Connect Windows devices to Microsoft Defender for Endpoint ⓘ	Off [✓ On]
Enable App Sync for iOS/iPadOS Devices ⓘ	Off [✓ On]
Send full application inventory data on personally-owned iOS/iPadOS Devices ⓘ	Off [✓ On]
Block unsupported OS versions ⓘ	Off [✓ On]

Onboarding



Endpoints

Select operating system to start onboarding process: Windows 10 and 11

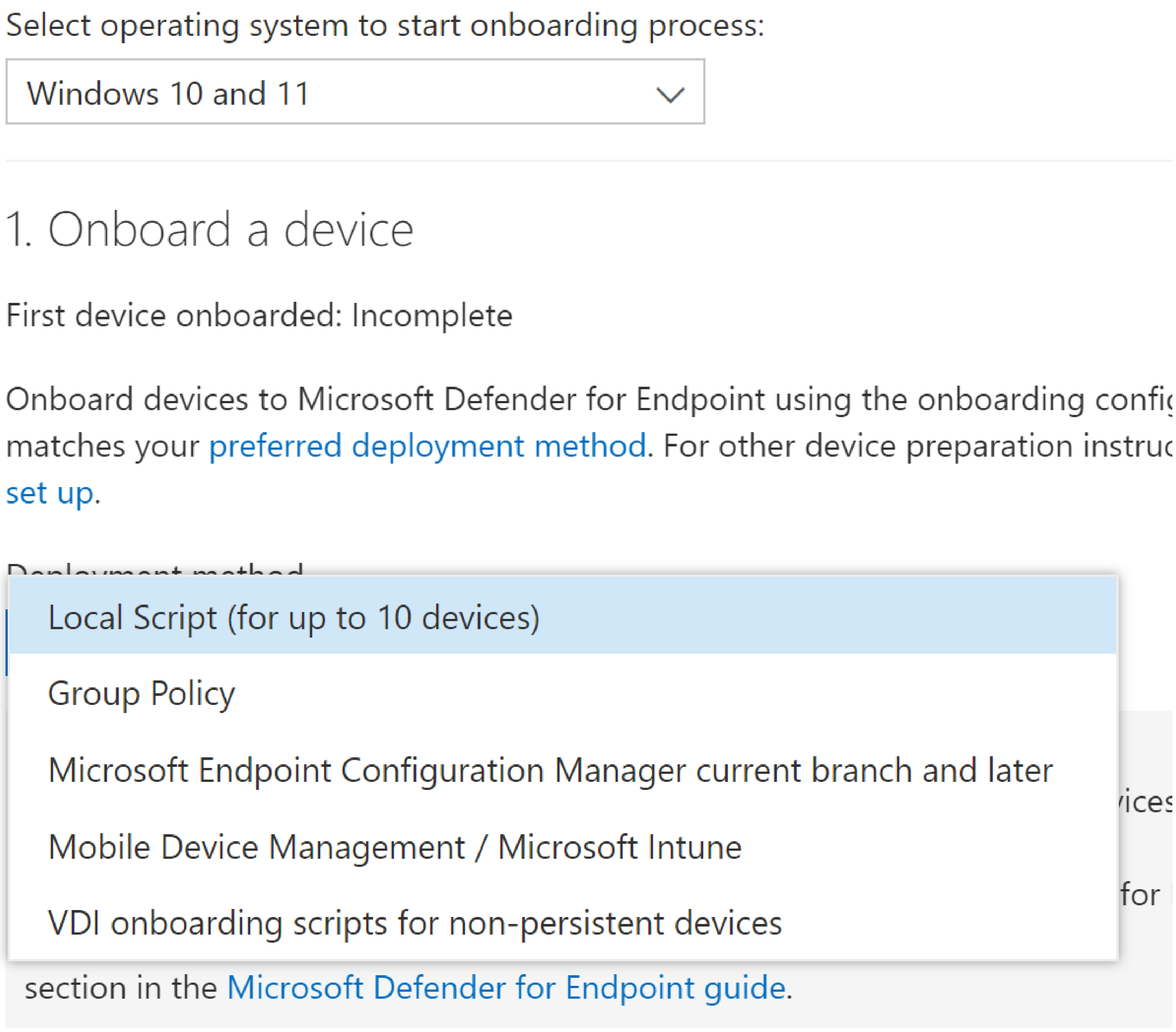
1. Onboard a device

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.



Select operating system to start onboarding process:

Windows 10 and 11

1. Onboard a device

First device onboarded: Incomplete

Onboard devices to Microsoft Defender for Endpoint using the onboarding confi matches your preferred deployment method. For other device preparation instruc set up.

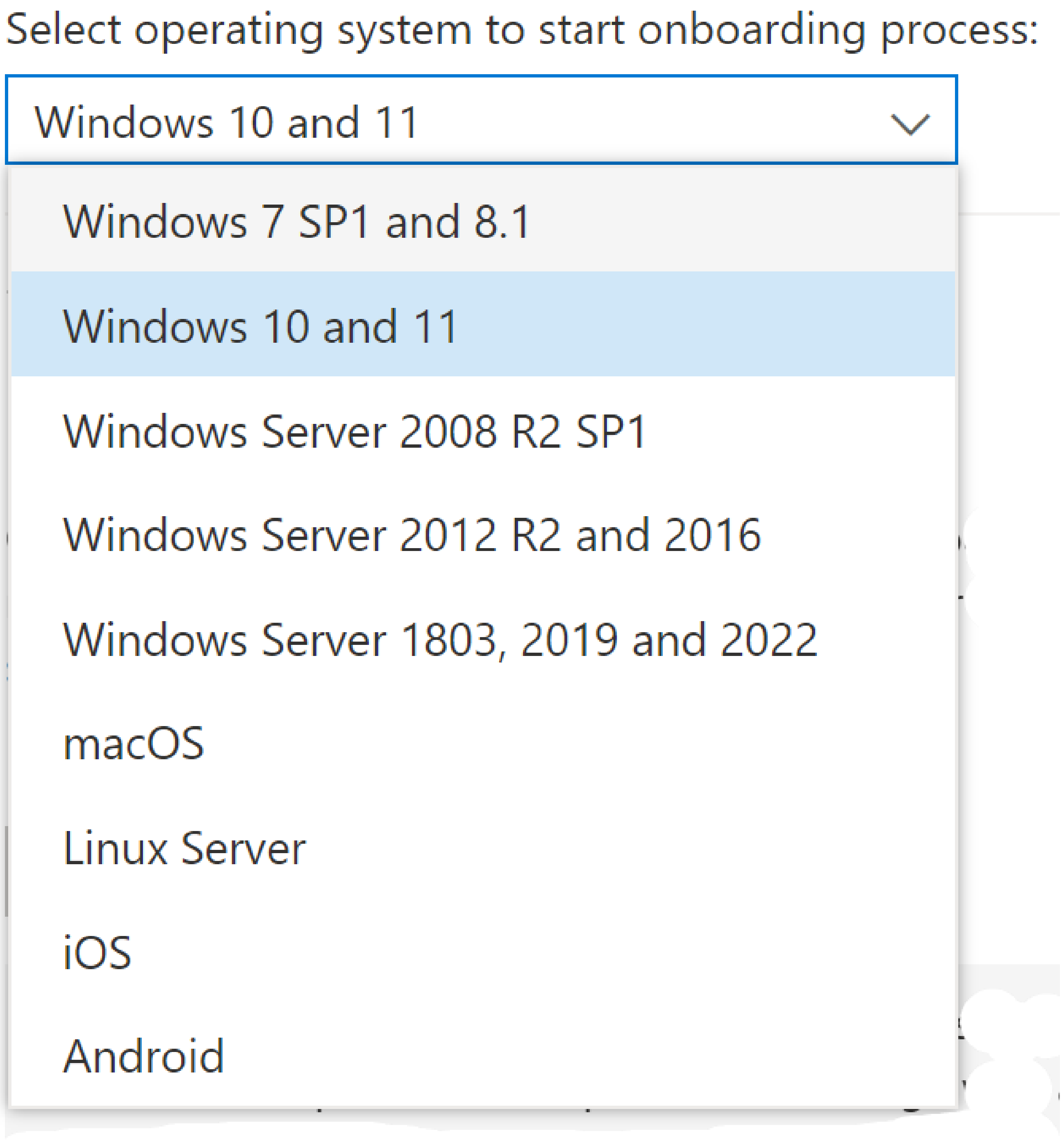
Deployment method

Local Script (for up to 10 devices)
Group Policy
Microsoft Endpoint Configuration Manager current branch and later
Mobile Device Management / Microsoft Intune
VDI onboarding scripts for non-persistent devices

ices

for

section in the Microsoft Defender for Endpoint guide.



Select operating system to start onboarding process: Windows 10 and 11

Windows 7 SP1 and 8.1
Windows 10 and 11
Windows Server 2008 R2 SP1
Windows Server 2012 R2 and 2016
Windows Server 1803, 2019 and 2022
macOS
Linux Server
iOS
Android

Resources

- What is Defender for Endpoint? - https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide
- Defender for Endpoint documentation - https://learn.microsoft.com/en-us/defender-endpoint/
- Defender for Business documentation – https://docs.microsoft.com/en-us/microsoft-365/security/defender-business/?view=o365-worldwide
- Compare Defender plans – https://docs.microsoft.com/en-us/microsoft-365/security/defender-business/compare-mdb-m365-plans?view=o365-worldwide
- Defender for Business integration with M365 Lighthouse - https://docs.microsoft.com/en-us/microsoft-365/security/defender-business/mdb-lighthouse-integration?view=o365-worldwide
- Defender for Business Trial playbook - https://docs.microsoft.com/en-us/microsoft-365/security/defender-business/trial-playbook-defender-business?view=o365-worldwide

CIAOPS Resources

- Blog – http://blog.ciaops.com
- Free Office 365, Azure video tutorials – http://www.youtube.com/directorciaops
- Free documents, presentations, eBooks – http://slideshare.net/directorcia
- Office 365, Azure, Cloud podcast – http://ciaops.podbean.com
- Office 365, Azure online training courses – http://www.ciaopsacademy.com
- Office 365 and Azure community – http://www.ciaopspatron.com
- CIAOPS Github – https://github.com/directorcia
- CIAOPS Best Practices Github – https://github.com/directorcia/bp

Twitter/X	Facebook	Email	Teams
@directorcia	https://www.facebook.com/ciaops	director@ciaops.com	director@ciaops.com

Get access to the latest information by becoming a Patron

http://www.ciaopspatron.com

Questions

That’s all folks!

Thanks for attending