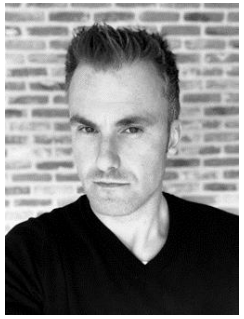
Modernize endpoint security with MEM

Speaker Intro



Tim De Keukelaere

Freelance Consultant

Tim.De.Keukelaere@IT-Essence.be

@Tim_DK

http://be.linkedin.com/in/timdekeukelaere/

http://www.dekeukelaere.com

Timdk_itpro

Ken Goossens

Sr. Program Manager

Ken.Goossens@microsoft.com

@Goosken

https://be.linkedin.com/in/kengoossens-ems/

http://mc2mc.be

N/A

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

Endpoint security | Overview

Search (Ctrl+/)

Overview

Overview
All devices
Security baselines
Security tasks

Manage

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

Setup

Microsoft Defender ATP

Help and support

Help and support

Protect and secure devices from one place

Enable, configure, and deploy Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) 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 recommended settings.

View Security Baselines

Simplified security policies

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

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

Remediate endpoint weaknesses

Remediate endpoint vulnerabilities reported by Microsoft Defender ATP and Threat and Vulnerability Management.

View security tasks

Enable Microsoft Defender ATP

Antivirus

Windows 10 Target versions:

- Windows 10 Professional
- Windows 10 Enterprise E3
- Windows 10 Enterprise E5

Antivirus policy for endpoint security

- Manage Antivirus Settings on managed devices
- Integrates with Defender ATP
- !!! Avoid Conflicts

Platform and supported profiles

- Requires ATP to be installed on device
- Antivirus profile replaces the need to configure the settings by using .plist files.
- Settings found in the Antivirus policy for macOS are unique and aren't available through the other policy types

- Manage Microsoft Defender Antivirus
- Manage Windows Security Experience

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

Create profile

Microsoft Defender Antivirus

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

Settings

Search for a setting

- Cloud protection
- Microsoft Defender Antivirus Exclusions
- Real-time protection
  - Turn on real-time protection: Not configured
  - Enable on access protection: Not configured
  - Monitoring for incoming and outgoing files: Monitor all files
  - Turn on behavior monitoring: Not configured
  - Turn on network protection: Not configured
  - Scan all downloaded files and attachments: Not configured
  - Scan scripts that are used in Microsoft browsers: Not configured
  - Scan network files: Not configured
  - Scan emails: Not configured
- 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
- Scan
- Updates
- User experience

Previous | Next

Summary

Basics

Name	Demo AV Profile
Description	--
Platform	Windows 10 and later

Configuration settings

Defender Processes To Exclude	1 items
Turn on real-time protection	Yes
Enable on access protection	Yes
Scan scripts that are used in Microsoft browsers	Yes
Scan emails	Yes
Scan all downloaded files and attachments	Yes
Turn on network protection	Yes

Scope tags

Default

Assignments

Included groups	--
Excluded groups	--

Also for on-prem scenarios

- Currently in preview
- Requires CB2006 and tenant attach devices
- Deploying antivirus policy to devices managed by ConfigMgr
- Platform: Windows 10 and Windows Server
  - Windows 10 and later (x86, x64, ARM64)
  - Windows 8.1 (x84, x64)
  - Windows Server 2019 and later (x64)
  - Windows server 2016 (x64)
  - Windows Server 2012 R2 (x64)
  - Windows Server 2008 R2 SP1 (x64)

Disk Encryption

Windows 10 Target versions:

- Windows 10 Professional
- Windows 10 Enterprise E3
- Windows 10 Enterprise E5

Disk encryption policy for endpoint security

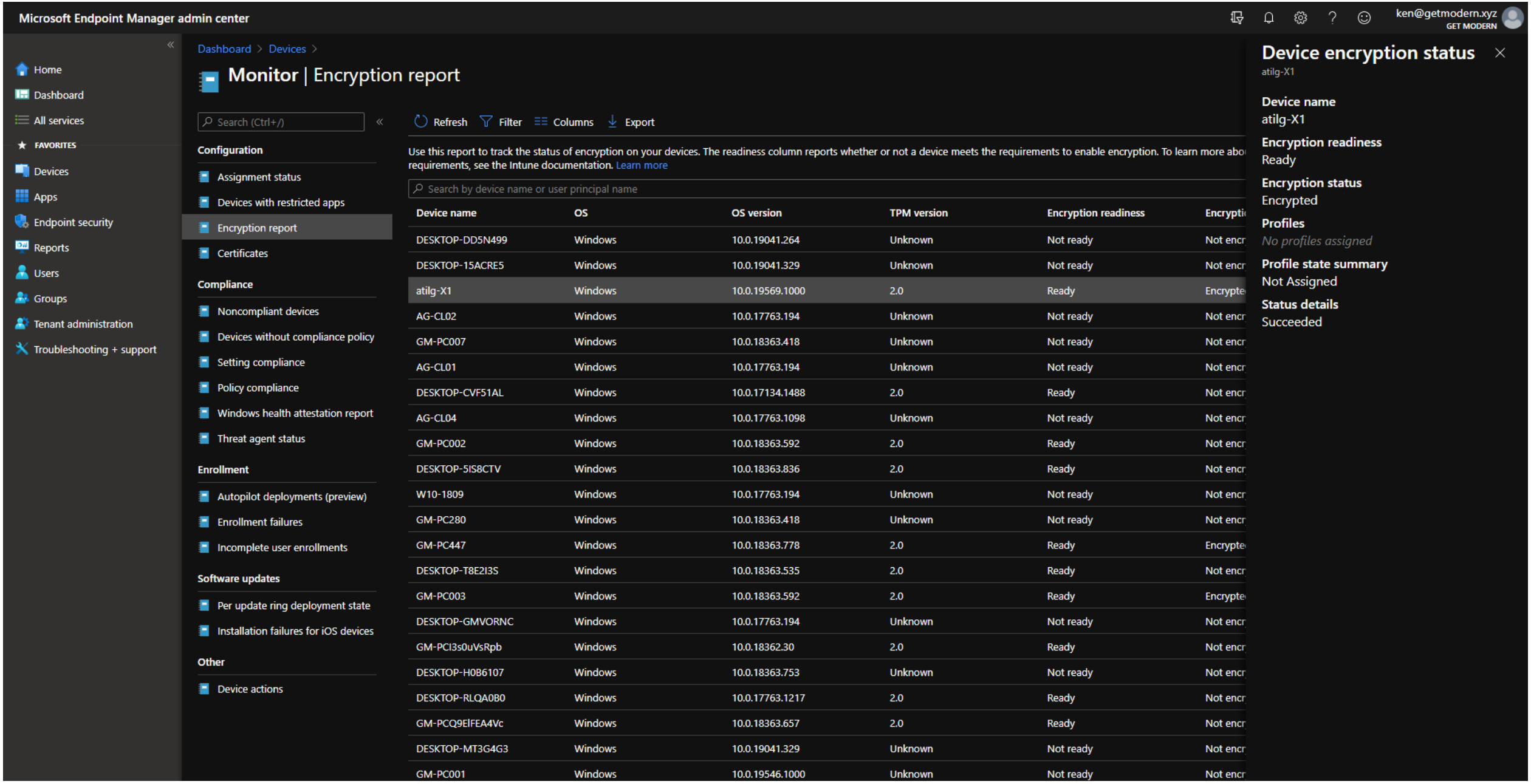
- Focus on relevant settings for a device built-in encryption method.
- This focus helps IT Admins to manage encryption settings more easily.

- Why not using Endpoint Protection Profiles?
  - Device Configuration Profiles include additional categories of settings.
  - These additional settings are unrelated to disk encryption.
  - Stay to the core and avoid complexity.

Platform and supported profiles

- macOS 10.13 or later
- Filevault

- Windows 10 or later
- BitLocker


Microsoft Endpoint Manager admin center
ken@getmodern.xyz
GET MODERN
Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Dashboard > Devices >
Monitor | Encryption report
Search (Ctrl+/)
Configuration
Assignment status
Devices with restricted apps
Encryption report
Certificates
Compliance
Noncompliant devices
Devices without compliance policy
Setting compliance
Policy compliance
Windows health attestation report
Threat agent status
Enrollment
Autopilot deployments (preview)
Enrollment failures
Incomplete user enrollments
Software updates
Per update ring deployment state
Installation failures for iOS devices
Other
Device actions
Refresh
Filter
Columns
Export
Use this report to track the status of encryption on your devices. The readiness column reports whether or not a device meets the requirements to enable encryption. To learn more abo
requirements, see the Intune documentation. Learn more
Search by device name or user principal name
Device name
OS
OS version
TPM version
Encryption readiness
Encrypti
DESKTOP-DD5N499 Windows 10.0.19041.264 Unknown Not ready Not encr
DESKTOP-15ACRE5 Windows 10.0.19041.329 Unknown Not ready Not encr
atilg-X1 Windows 10.0.19569.1000 2.0 Ready Encrypte
AG-CL02 Windows 10.0.17763.194 Unknown Not ready Not encr
GM-PC007 Windows 10.0.18363.418 Unknown Not ready Not encr
AG-CL01 Windows 10.0.17763.194 Unknown Not ready Not encr
DESKTOP-CVF51AL Windows 10.0.17134.1488 2.0 Ready Not encr
AG-CL04 Windows 10.0.17763.1098 Unknown Not ready Not encr
GM-PC002 Windows 10.0.18363.592 2.0 Ready Not encr
DESKTOP-5IS8CTV Windows 10.0.18363.836 2.0 Ready Not encr
W10-1809 Windows 10.0.17763.194 Unknown Not ready Not encr
GM-PC280 Windows 10.0.18363.418 Unknown Not ready Not encr
GM-PC447 Windows 10.0.18363.778 2.0 Ready Encrypte
DESKTOP-T8E2I3S Windows 10.0.18363.535 2.0 Ready Not encr
GM-PC003 Windows 10.0.18363.592 2.0 Ready Encrypte
DESKTOP-GMVORNC Windows 10.0.17763.194 Unknown Not ready Not encr
GM-PCI3s0uVsRpb Windows 10.0.18362.30 2.0 Ready Not encr
DESKTOP-H0B6107 Windows 10.0.18363.753 Unknown Not ready Not encr
DESKTOP-RLQA0B0 Windows 10.0.17763.1217 2.0 Ready Not encr
GM-PCQ9ElFEA4Vc Windows 10.0.18363.657 2.0 Ready Not encr
DESKTOP-MT3G4G3 Windows 10.0.19041.329 Unknown Not ready Not encr
GM-PC001 Windows 10.0.19546.1000 Unknown Not ready Not encr
Device encryption status
atilg-X1
Device name
atilg-X1
Encryption readiness
Ready
Encryption status
Encrypted
Profiles
No profiles assigned
Profile state summary
Not Assigned
Status details
Succeeded

Firewall

Windows 10 Target versions:

- Windows 10 Professional
- Windows 10 Enterprise E3
- Windows 10 Enterprise E5

Firewall policy for endpoint security

- Focus on relevant settings for a device built-in firewall
- This focus helps IT Admins to manage firewall settings more easily.

- Why not use Endpoint Protection Profiles?
  - Device Configuration Profiles include additional categories of settings.
  - These additional settings are unrelated to disk encryption.
  - Stay to the core and avoid complexity.

Platform and supported profiles

- macOS any supported version
- macOS firewall

- Windows 10 or later
- Windows Defender Firewall
- Windows Defender Firewall rules (Preview)

Firewall Rule mergers and Policy conflicts

- **Mergers:**
  - Two firewall policies with different settings targeting same device = **Merger**

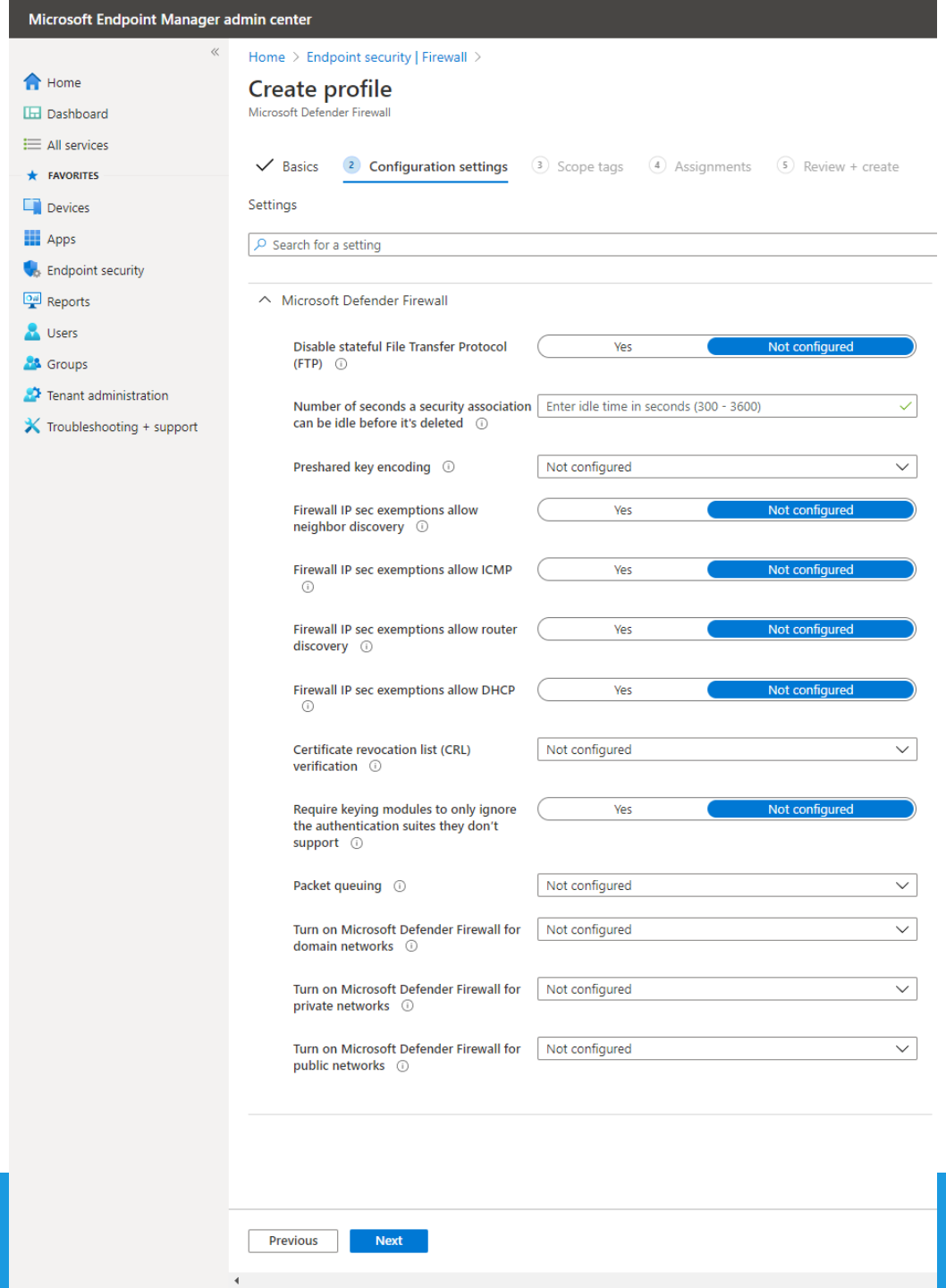
- **Conflicts:**
  - Two firewall rules with same settings targeting same device = **Conflicting**

Important: When a conflict exists between two policy instances or types of policy that manage the same setting with different values, the setting isn't sent to the device.

Policy conflict applies to the Microsoft Defender Firewall profile, which can conflict with other Microsoft Defender Firewall profiles, or a firewall configuration that’s delivered by a different policy type, like device configuration.

Microsoft Defender Firewall profiles don't conflict with Microsoft Defender Firewall rules profiles.

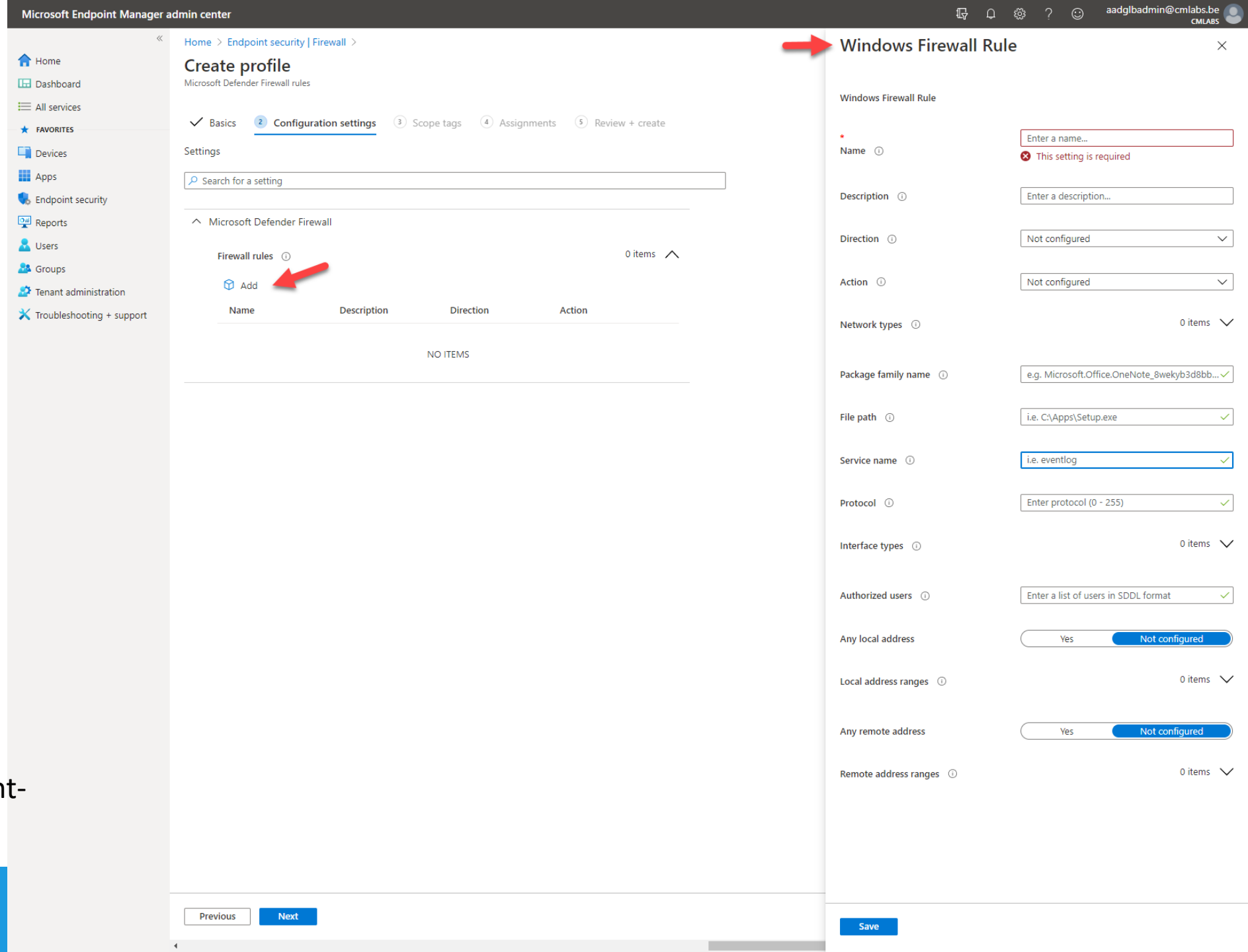
Defender Firewall



Full details on all settings:

https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-firewall-profile-settings

Defender Firewall Rules



Full details on all settings:

https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-firewall-profile-settings

Detection & Response

Windows 10 Target versions:

- Windows 10 Enterprise E5

Endpoint detection and response policy for endpoint security

- Advanced Attack Detections nearly real-time and actionable.
- SecOps can prioritize alerts.
- SecOps can see the full scope of a breach.
- SecOps can take response actions to remediate.

- Profiles contains automatically a Microsoft Defender ATP onboarding package.
  - As soon as the device is onboarded, you can start to use threat data.
  - You can deploy the EDR Policy to:
    - Azure Active Directory Groups
    - ConfigMgr Collections (incl. Servers Collections)

Prerequisites for EDR Policies

Microsoft Defender ATP Tenant

ConfigMgr Deployment

- ConfigMgr 2002 or later
- ConfigMgr 2002 Hotfix KB4563473
- Configure Tenant Attach
- Sync ConfigMgr Collections to Admin Center
- Enable Collections for use with MDATP
- Require Global Admin on the Subscription to setup

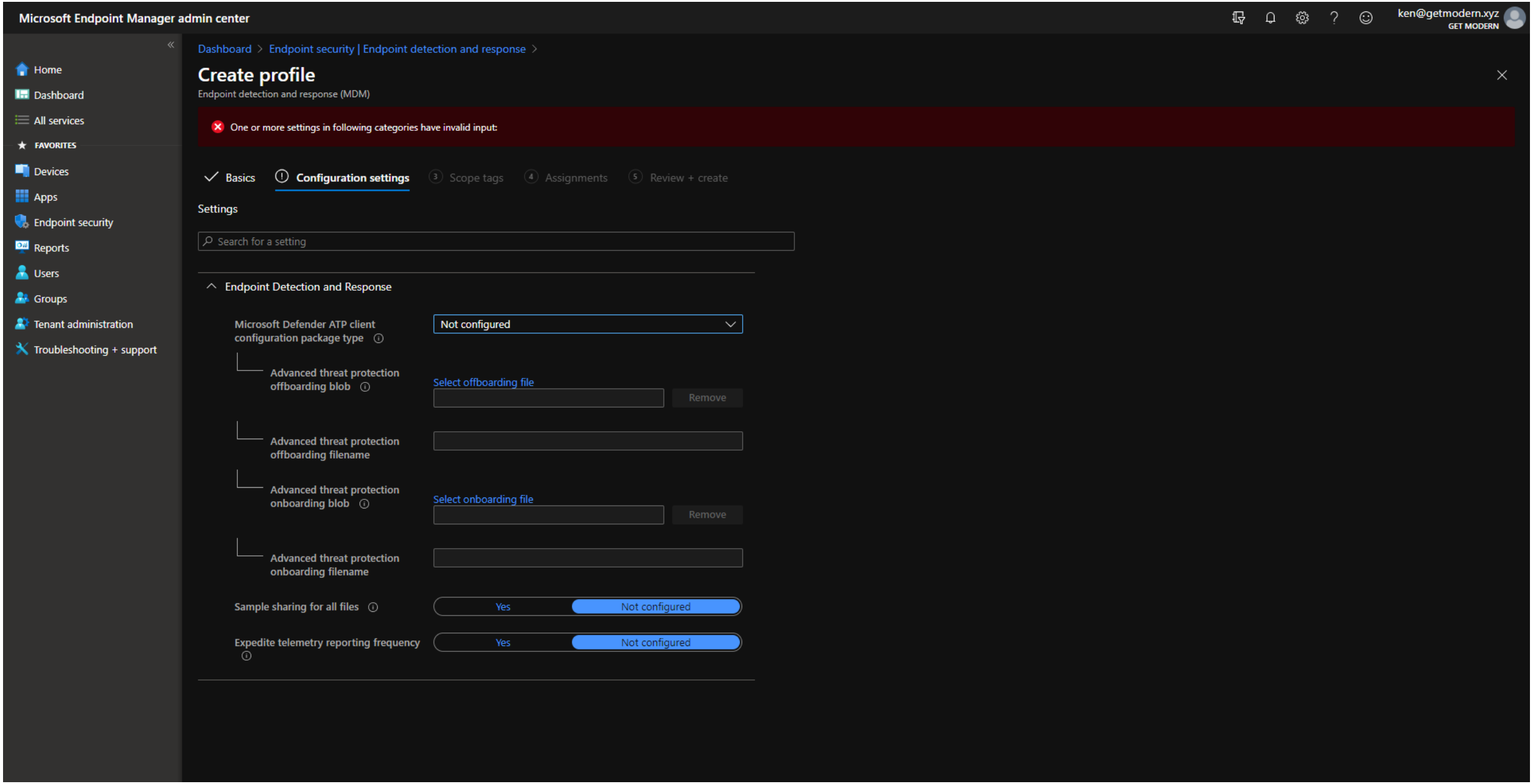
Intune Deployment

- Create and Assign your EDR Policy

EDR policy reports

- For policies that target the Windows 10 and later platform (Intune), you'll see an overview of compliance to the policy.
- The Devices with ATP sensor chart displays only devices that successfully onboard to Microsoft Defender ATP through use of the Windows 10 and later profile.

- For policies that target the Windows 10 and Windows Server platform (Configuration Manager), you'll see an overview of compliance to the policy **but can't drill-in to view additional details.**
- The view is limited because the admin center receives limited status details from Configuration Manager, which manages the deployment of the policy to Configuration Manager devices.


Microsoft Endpoint Manager admin center
ken@getmodern.xyz
GET MODERN
Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Dashboard > Endpoint security | Endpoint detection and response >
Create profile
Endpoint detection and response (MDM)
One or more settings in following categories have invalid input:
Basics
Configuration settings
3 Scope tags
4 Assignments
5 Review + create
Settings
Search for a setting
Endpoint Detection and Response
Microsoft Defender ATP client configuration package type
Not configured
Advanced threat protection offboarding blob
Select offboarding file
Remove
Advanced threat protection offboarding filename
Advanced threat protection onboarding blob
Select onboarding file
Remove
Advanced threat protection onboarding filename
Sample sharing for all files
Yes
Not configured
Expedite telemetry reporting frequency
Yes
Not configured

Attack Surface Reduction

Windows 10 Target versions:

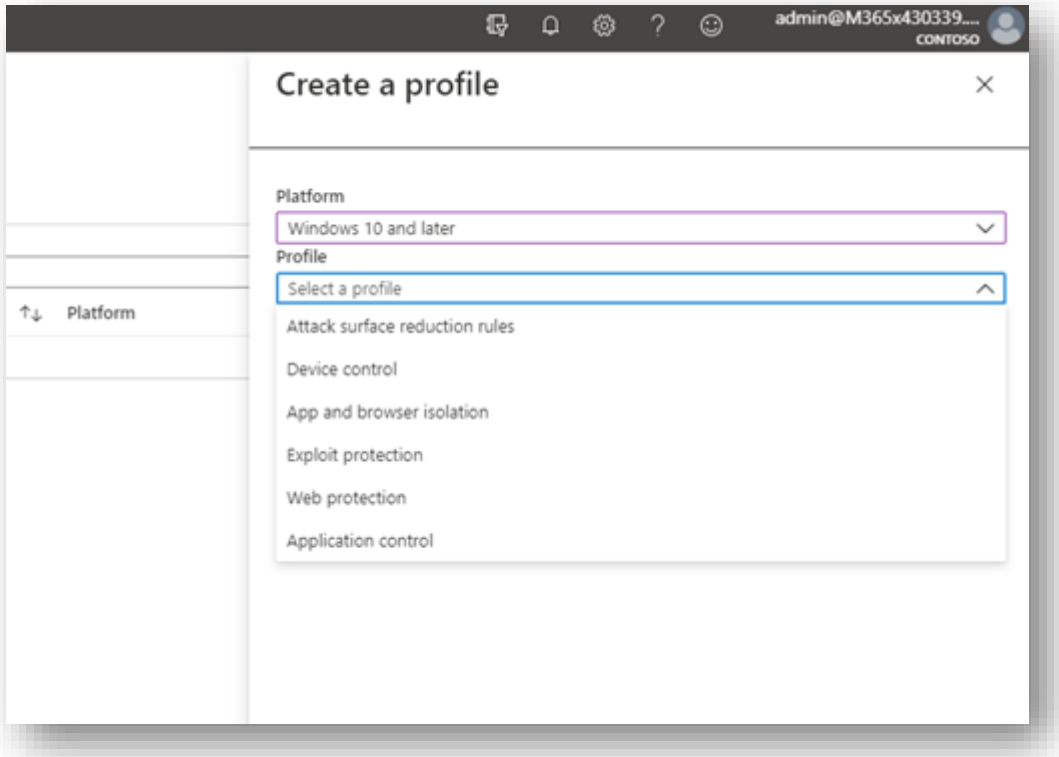
- Windows 10 Professional
- Windows 10 Enterprise E3
- Windows 10 Enterprise E5

Attack surface reduction policy for endpoint security

- ASR was originally a feature of the suite of exploit guard.
- Full ASR Set only with Windows 10 Enterprise E3/E5
  - E5 add Monitoring and review analytics on alerts in real-time.
- Reduce your attack surfaces, by minimizing the places where your organization is vulnerable to cyberthreats and attacks.

- Requires Defender AV as primary AV on the device

Different Profile Types



- Application control
- App and browser isolation
- Web protection
- Attack surface reduction rules
- Exploit protection
- Device control

Tip : Audit your profile settings before implementing them !

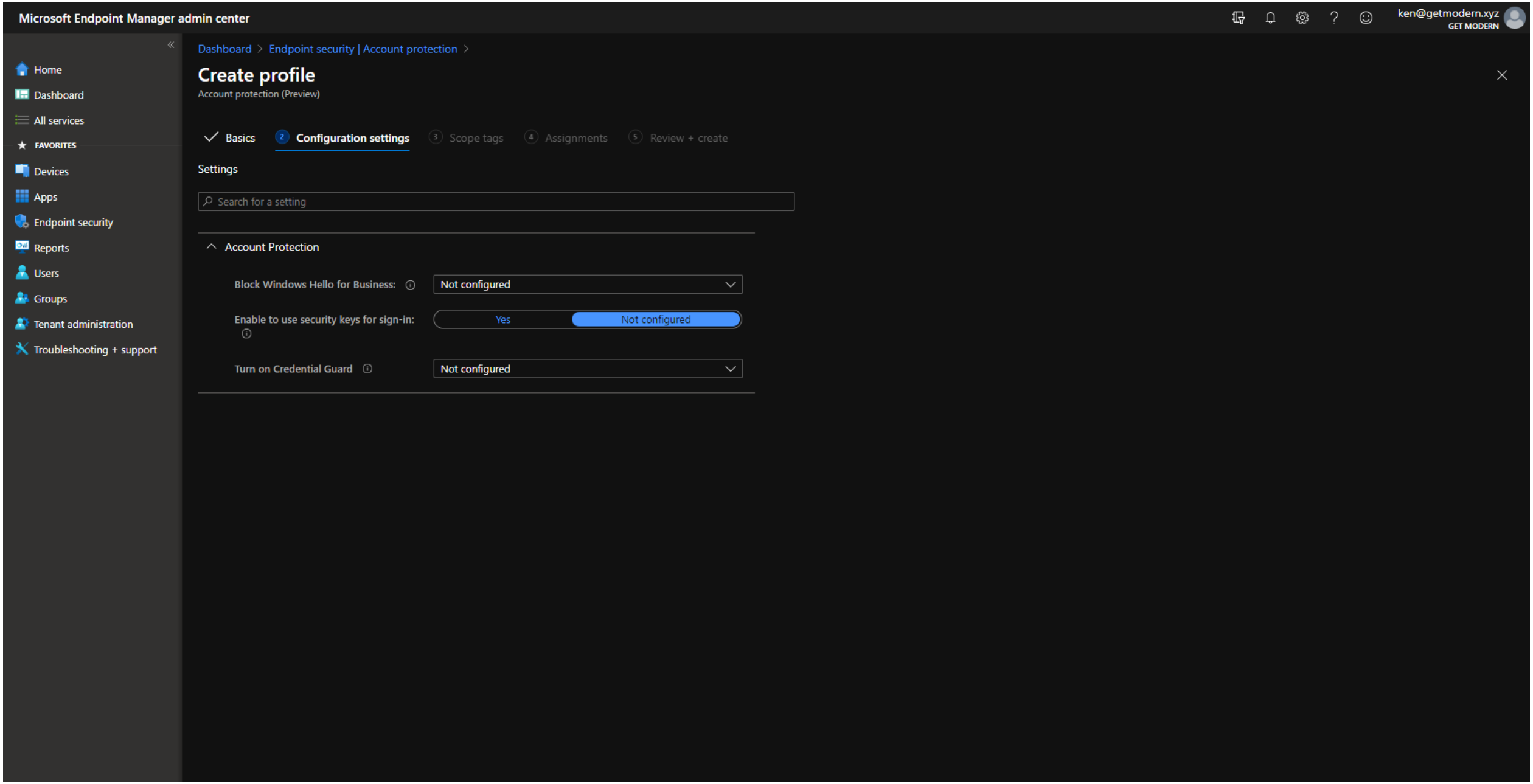
Account Protection

Windows 10 Target versions:

- Windows 10 Enterprise E3
- Windows 10 Enterprise E5

Account protection policy for endpoint security

- **Protect Identities and Accounts**
- **Account Protection is focused on 2 areas:**
  - Windows Hello for Business
    - Block Windows Hello for Business
    - Enable to use security keys for sign-in
  - Credential Guard
    - Turn CG on/off

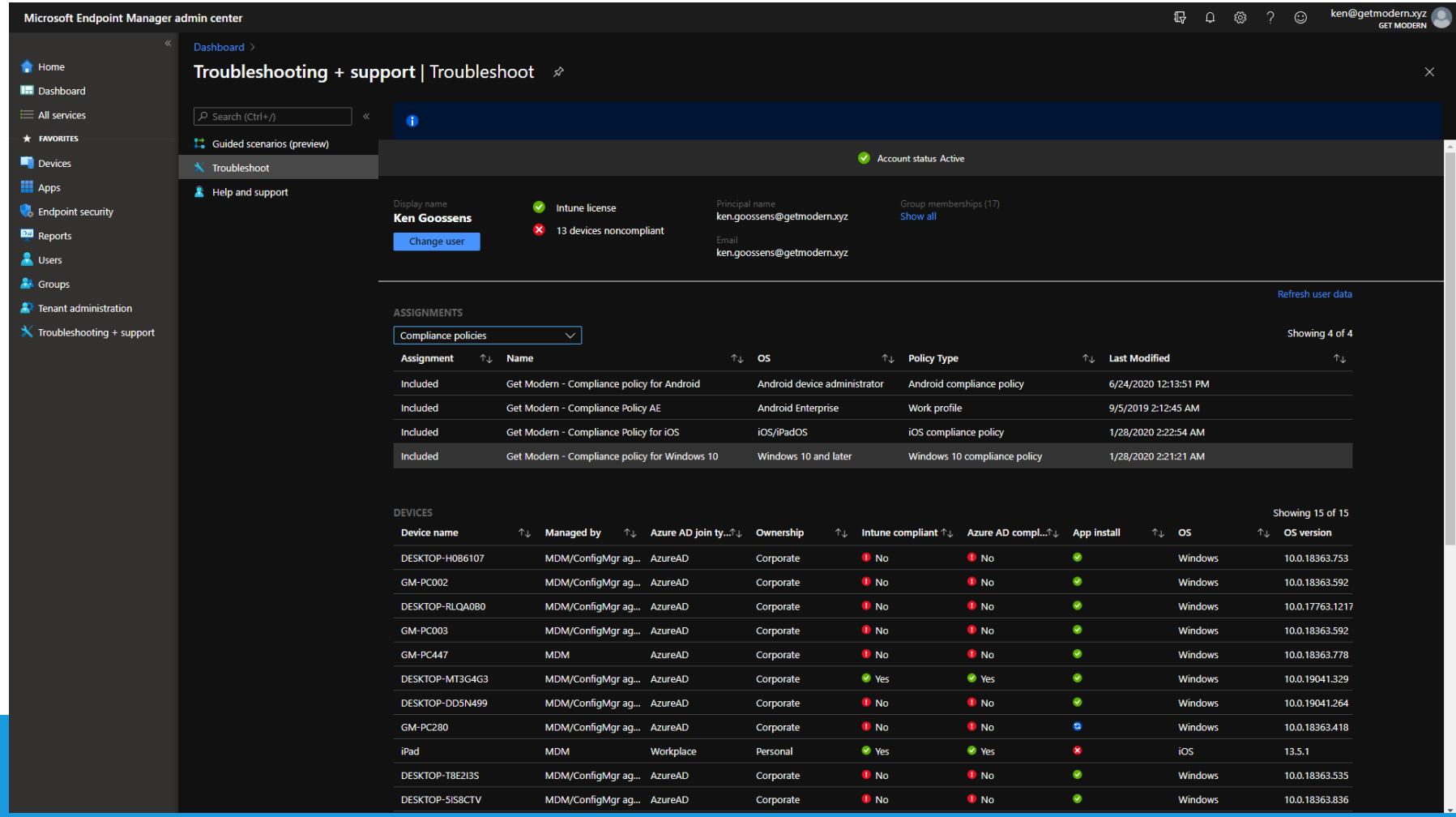

Microsoft Endpoint Manager admin center
ken@getmodern.xyz
GET MODERN
Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Dashboard > Endpoint security | Account protection >
Create profile
Account protection (Preview)
Basics
2 Configuration settings
3 Scope tags
4 Assignments
5 Review + create
Settings
Search for a setting
Account Protection
Block Windows Hello for Business:
Not configured
Enable to use security keys for sign-in:
Yes
Not configured
Turn on Credential Guard
Not configured

How to manage conflicts?

Troubleshooting Conflicts

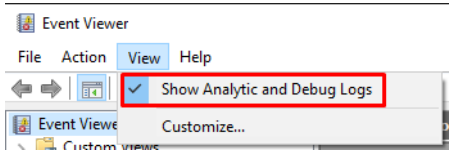
- Endpoint Manager Built-in Troubleshooting and Support node.

- Client Apps
- Compliance Policies
- Configuration Profiles
- App Protection Policies
- Windows 10 update rings
- Enrollment restrictions

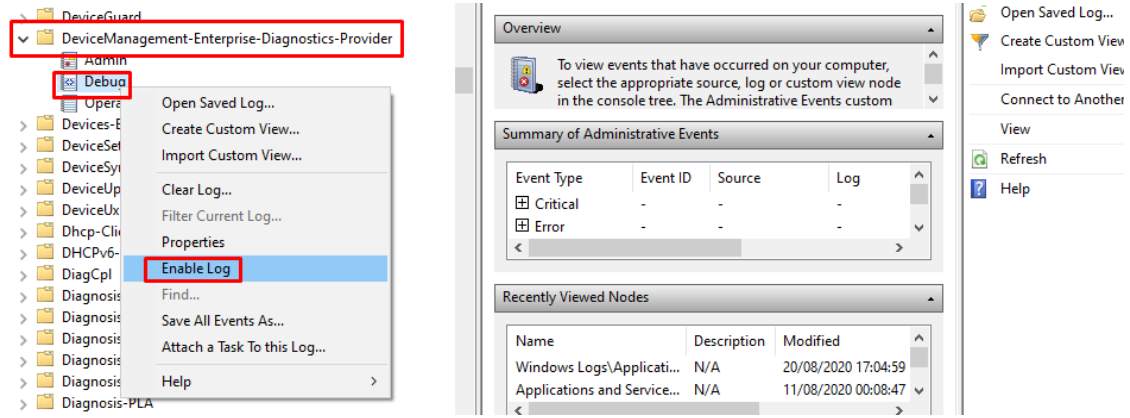


Troubleshooting Conflicts

- Enable verbose logging in Eventvwr.
  1. Show Analytics & Debug Logs



  2. Enable Debug Log



Key Takeaways

- MEM is powerful tool to help you manage security policies
- Approach implementing policies from a security persona perspective to avoid conflicts and complexity