Privileged Identity Management

Research Guide

Dr. Sibi Chakkaravarthy Sethuraman

Team

Tarun R

19BCN7122

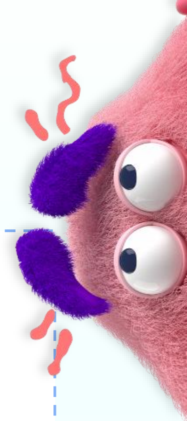
Praveen K

19BCE7595

Nikhil V

19BCE7130

Contents



1. Introduction
2. Problem Statement
3. Solution
4. Requirements
5. Methodology
6. Results
7. Conclusion and references

Introduction

Our Purpose

Organizations want to limit the number of individuals who have access to secure information or resources because it reduces the possibility of a malicious actor gaining access to an authorized user and inadvertently compromising a sensitive resource. As the number of work-from-home employees and interns grows, we want to address this by properly configuring **Privileged Identity Management** (PIM) **to provide time-based** and **approval-based role activation** to mitigate the risks of **excessive, unnecessary,** or **misused access permissions** on resources that you value.

Problem Statement

In today's world, Security has become an extreme necessity for almost every organization. On the other hand, **the usage of Azure AD in many companies has enabled them to manage user identities and roles, configure security settings** for the same. However, it is possible to **lose sight of the number of Global Admin accounts** which results in a **lack of permissions** to some of the administrators to perform their daily tasks. In addition to that, there is a higher chance of a serious breach or **privileged users inadvertently impacting a sensitive resource** if any privileged user is not rightly administered.

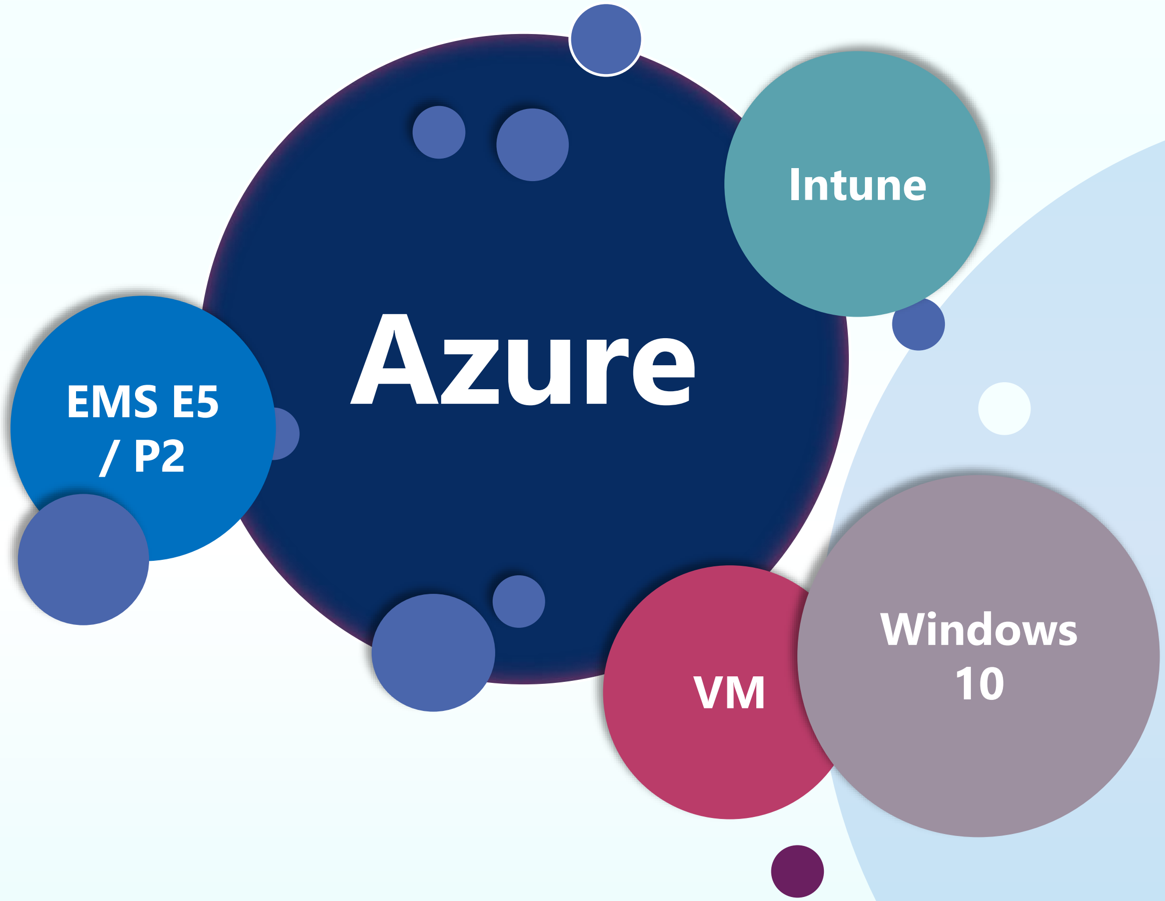
PIM (Privileged Identity Management), an Azure AD security component designed to administer access to privileged account provides the right solution to such issues.

The Solution

PIM (Privileged Identity Management), an Azure AD security component designed to administer access to privileged accounts, provides the right solution to such issues with key features such as:

- Provide Just-In-Time (JIT) access to resources
- Assign time-bound access to resources between firm dates
- Require approval to activate privileged roles
- Enforce Multi-Factor Authentication to activate any role
- Use justifications to understand why users need access
- Get notified when privileged roles are activated

Requirements



Azure

Intune

EMS E5 / P2

VM

Windows 10

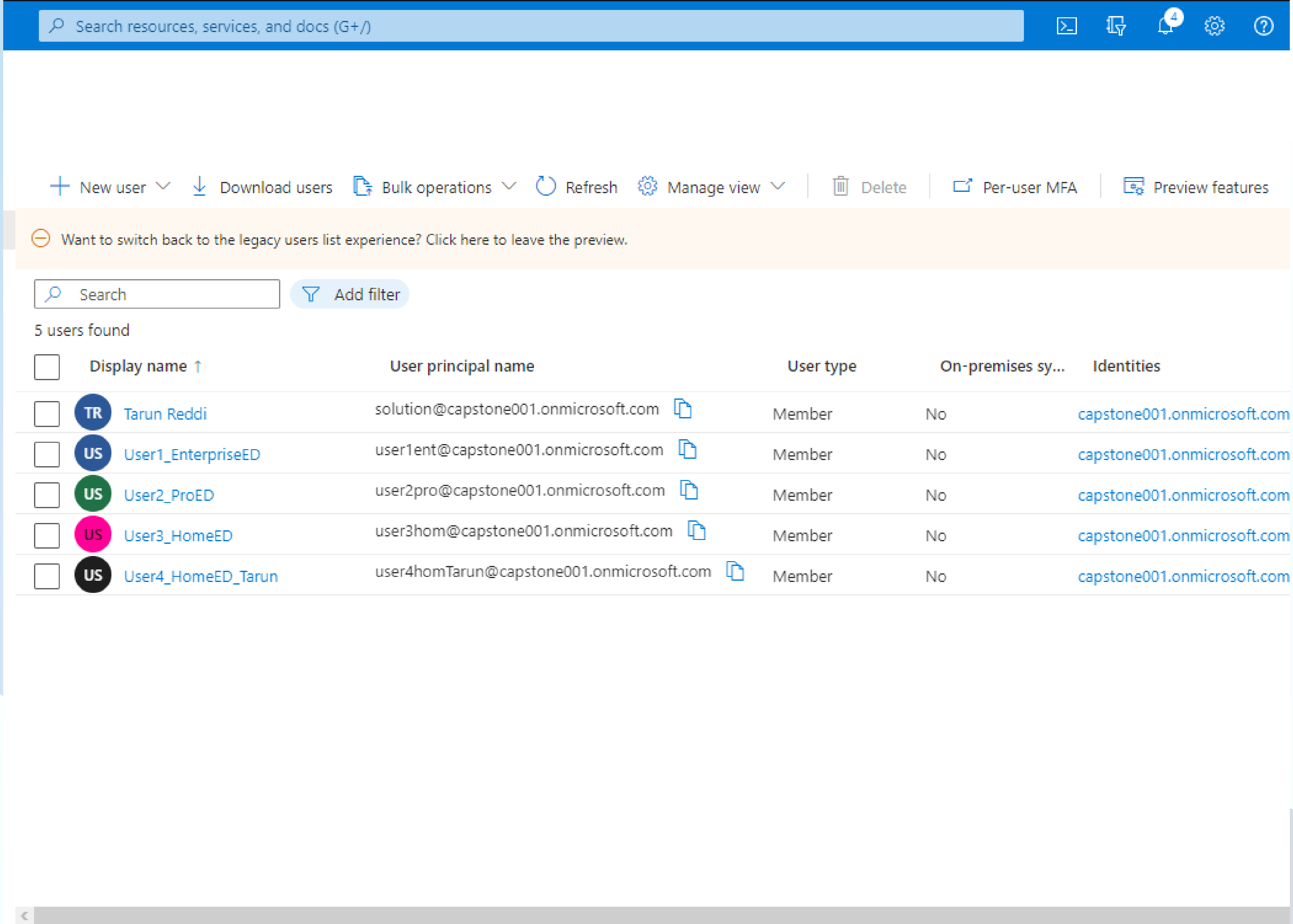
METHODOLOGY:

- **Environment Setup.**
  - Creating Users.
  - Prerequisites.
  - Device enrolment.
- **Compliance configured at the device level.**
  - Properties of the Compliance policies Configured through endpoint security in the MEAD.
  - Applying the established compliance security policies to the users and devices to simulate the workspace environment.

STEP – 1: Creating Users

- We begin with setting up the Intune account (solution@capstone001.onmicrosoft.com), followed by creating 4 users having different Windows 10 edition devices under the domain - **capstone001.onmicrosoft.com -** in the Azure Active Directory.

- Setting up devices into Intune is done by accessing the Microsoft Endpoint Admin Center (MEAD), where we configure the endpoint security through compliance policies to ensure the device and user/employee accounts are secure enough to access the organization’s resources.



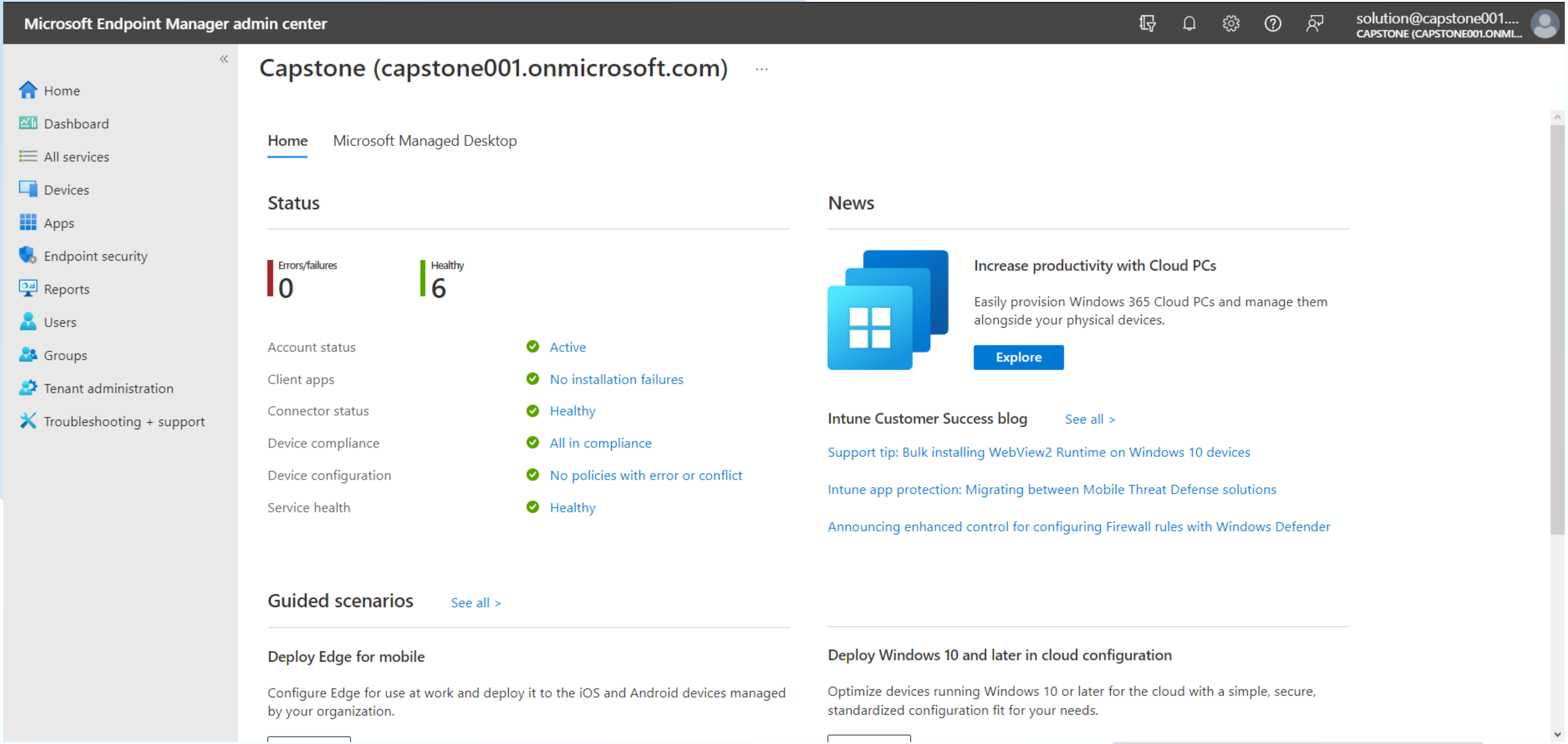
Want to switch back to the legacy users list experience? Click here to leave the preview.

5 users found

Display name ↑	User principal name	User type	On-premises sy...	Identities
TR Tarun Reddi	solution@capstone001.onmicrosoft.com	Member	No	capstone001.onmicrosoft.com
US User1_EnterpriseED	user1ent@capstone001.onmicrosoft.com	Member	No	capstone001.onmicrosoft.com
US User2_ProED	user2pro@capstone001.onmicrosoft.com	Member	No	capstone001.onmicrosoft.com
US User3_HomeED	user3hom@capstone001.onmicrosoft.com	Member	No	capstone001.onmicrosoft.com
US User4_HomeED_Tarun	user4homTarun@capstone001.onmicrosoft.com	Member	No	capstone001.onmicrosoft.com

STEP – 2: Prerequisites

A glance into the MEAD:



Microsoft Endpoint Manager admin center

solution@capstone001....
CAPSTONE (CAPSTONE001.ONMI...

Capstone (capstone001.onmicrosoft.com) ...

Home | Microsoft Managed Desktop

Status

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

News

Increase productivity with Cloud PCs

Easily provision Windows 365 Cloud PCs and manage them alongside your physical devices.

Explore

Intune Customer Success blog See all >

Support tip: Bulk installing WebView2 Runtime on Windows 10 devices

Intune app protection: Migrating between Mobile Threat Defense solutions

Announcing enhanced control for configuring Firewall rules with Windows Defender

Guided scenarios See all >

Deploy Edge for mobile

Configure Edge for use at work and deploy it to the iOS and Android devices managed by your organization.

Deploy Windows 10 and later in cloud configuration

Optimize devices running Windows 10 or later for the cloud with a simple, secure, standardized configuration fit for your needs.

There are certain prerequisites to be completed before device enrolment into Intune.

1. All users must have the EMS E5 / AD Premium P2 Licenses assigned to be eligible for device enrollment.
2. Mobility (MDM and MAM) should be configured by opting ‘NONE’ option for the MDM and MAM user scope.
3. Individual user usage locations must be assigned to apply the above Licenses for the users.

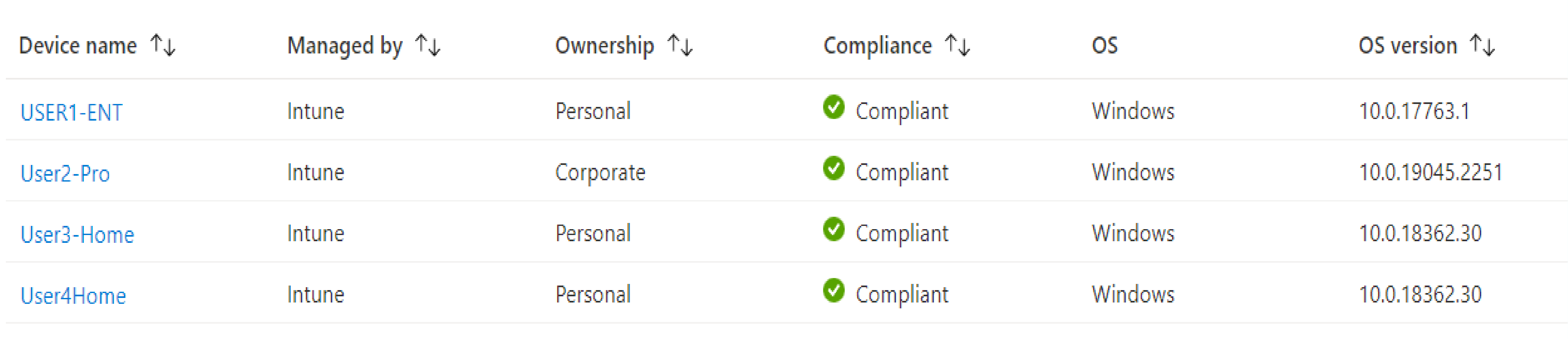
Once the prerequisites are completed, we can proceed further to add devices one by one.

There are two ways a device can be enrolled:

a) **Personal:** A device logged in with a personal Email ID but only the **Company Portal App (Intune app)** is logged in with the corporate Email ID.

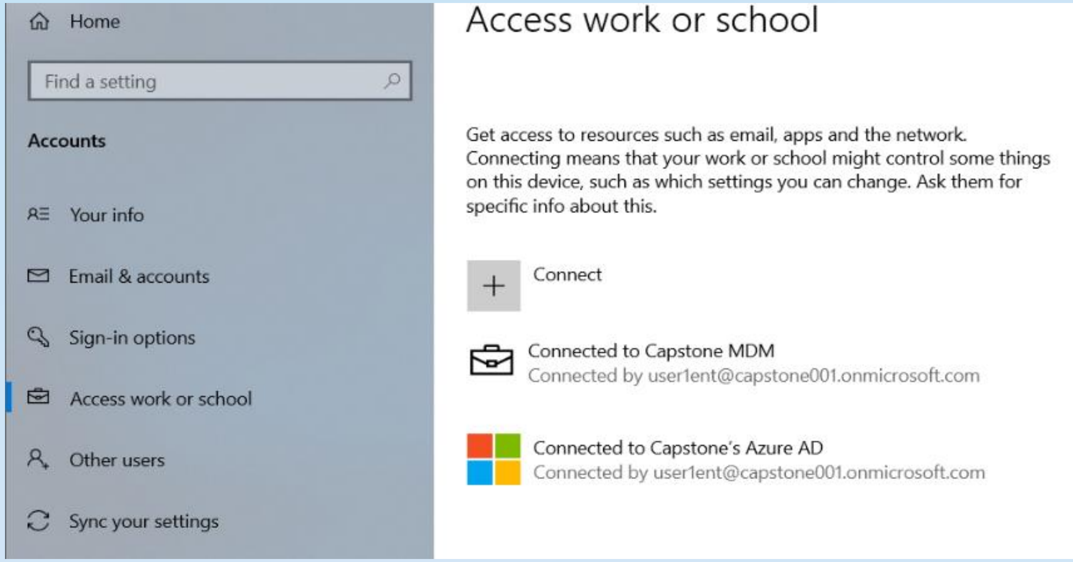
b) **Corporate:** The device is **Azure Joined to the Active Directory** via the work or school account option in the device settings with the corporate Email ID

The following image tells us the type of user’s device enrolled in Intune



Device name ↑↓	Managed by ↑↓	Ownership ↑↓	Compliance ↑↓	OS	OS version ↑↓
USER1-ENT	Intune	Personal	✓ Compliant	Windows	10.0.17763.1
User2-Pro	Intune	Corporate	✓ Compliant	Windows	10.0.19045.2251
User3-Home	Intune	Personal	✓ Compliant	Windows	10.0.18362.30
User4Home	Intune	Personal	✓ Compliant	Windows	10.0.18362.30

STEP – 3: Device Enrollment

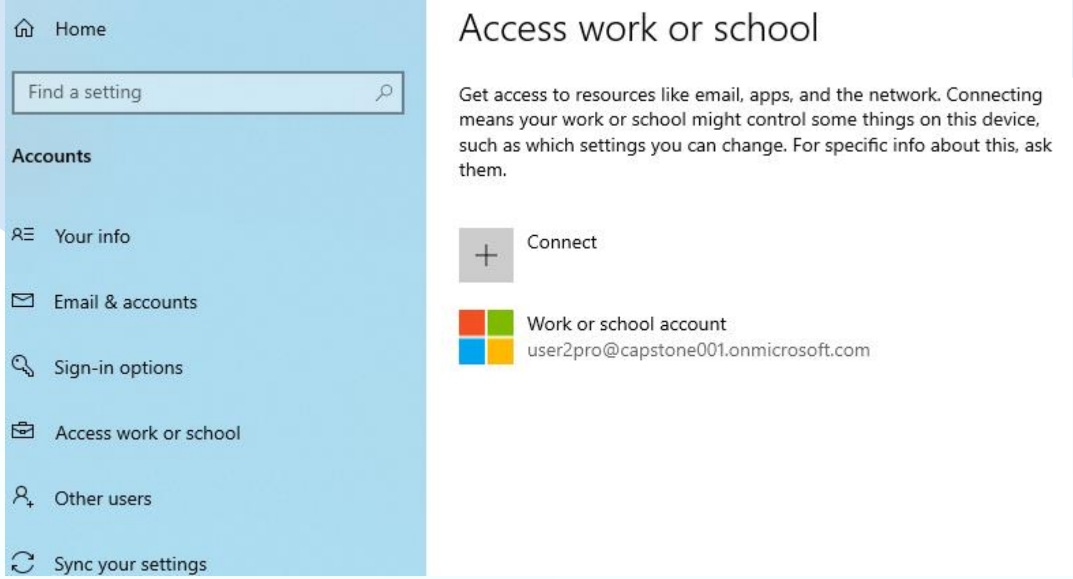


Access work or school

Get access to resources such as email, apps and the network. Connecting means that your work or school might control some things on this device, such as which settings you can change. Ask them for specific info about this.

Connected to Capstone MDM
Connected by user1ent@capstone001.onmicrosoft.com

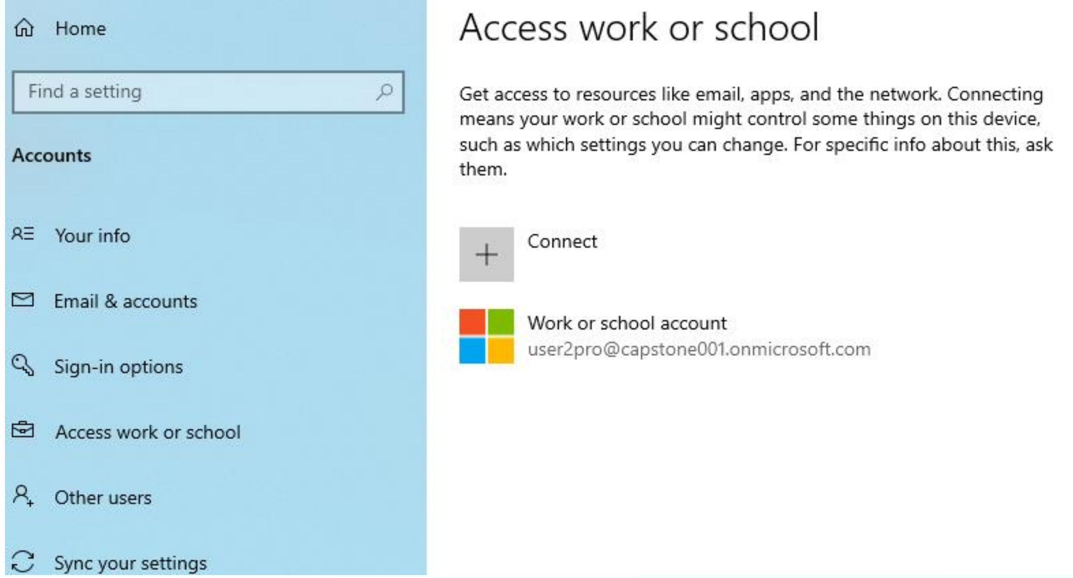
Connected to Capstone's Azure AD
Connected by user1ent@capstone001.onmicrosoft.com



Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

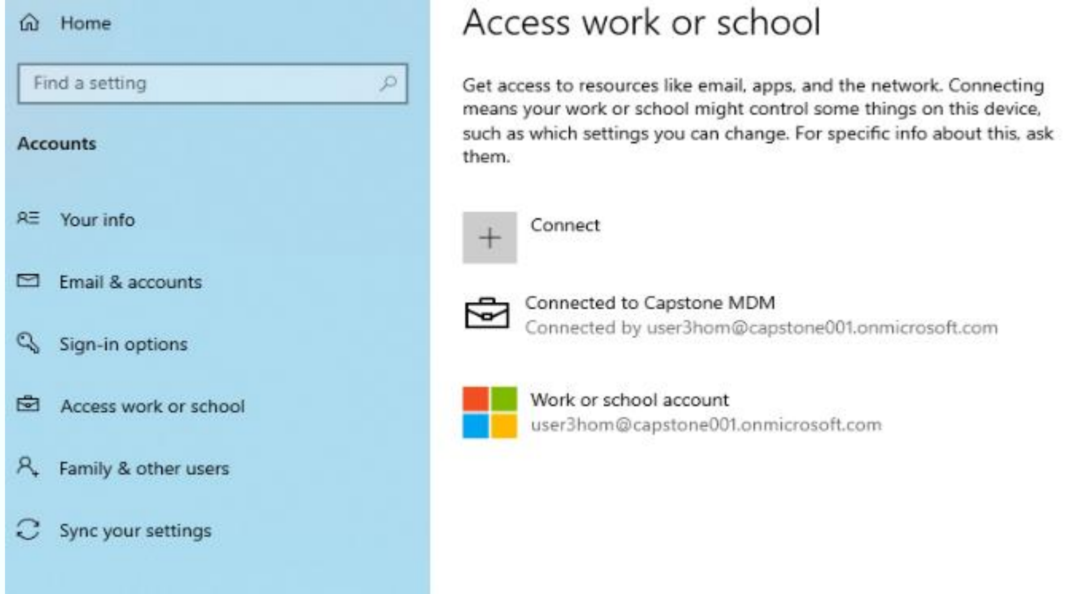
Work or school account
user2pro@capstone001.onmicrosoft.com



Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Work or school account
user2pro@capstone001.onmicrosoft.com



Access work or school

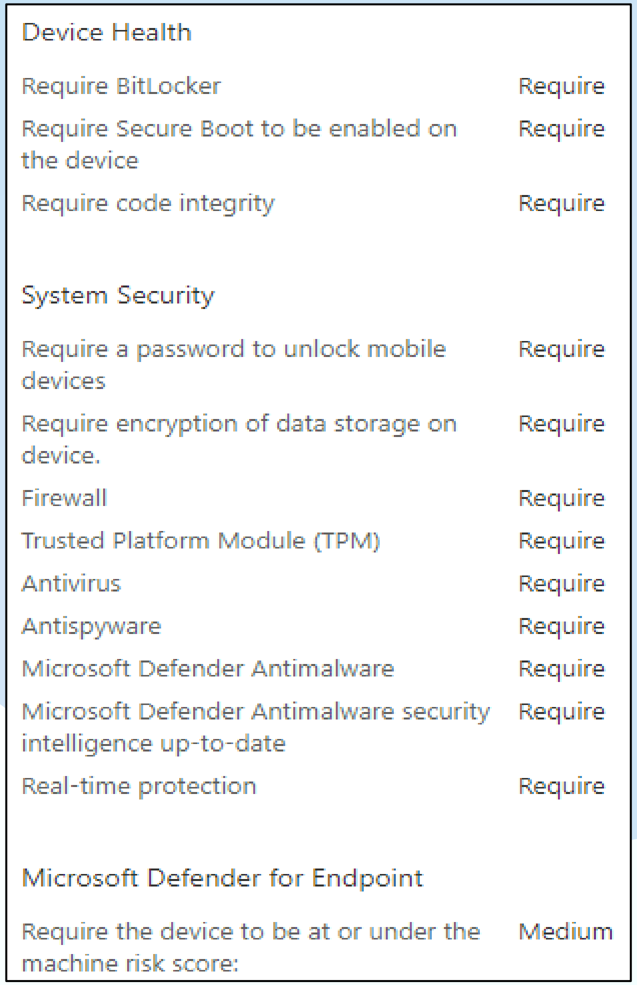
Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Connected to Capstone MDM
Connected by user3hom@capstone001.onmicrosoft.com

Work or school account
user3hom@capstone001.onmicrosoft.com

Compliance Configured at the device level

Properties:



Device Health

Require BitLocker	Require
Require Secure Boot to be enabled on the device	Require
Require code integrity	Require

System Security

Require a password to unlock mobile devices	Require
Require encryption of data storage on device.	Require
Firewall	Require
Trusted Platform Module (TPM)	Require
Antivirus	Require
Antispyware	Require
Microsoft Defender Antimalware	Require
Microsoft Defender Antimalware security intelligence up-to-date	Require
Real-time protection	Require

Microsoft Defender for Endpoint

Require the device to be at or under the machine risk score:	Medium

Properties of the Compliance policies Configured through endpoint security in the MEAD.

Endpoint Security – Device Compliance

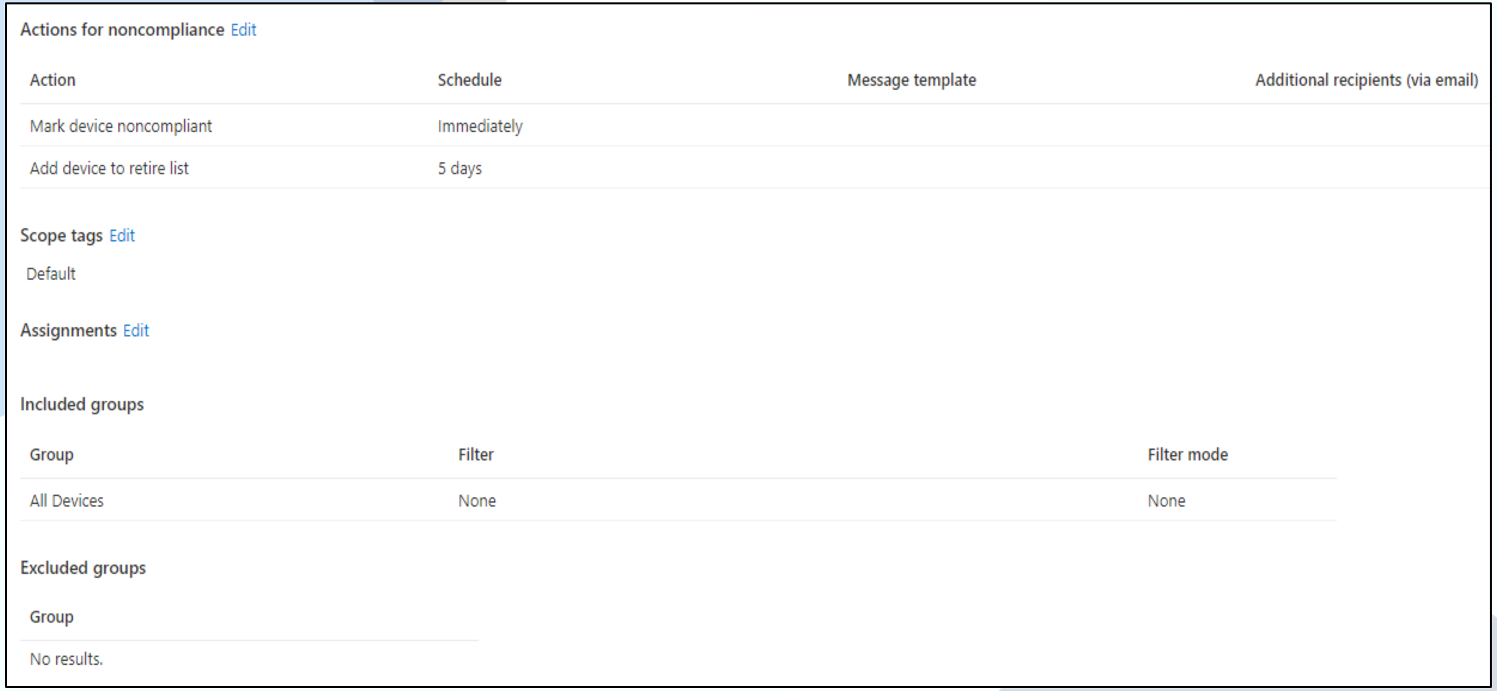
Name: Basic Device Compliance

Profile type: Windows 10/11 compliance policy

Assigned: Yes**Platform supported:** Windows 10 and later

Groups assigned: 1

Other Properties:



Actions for noncompliance Edit

Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	Immediately		
Add device to retire list	5 days		

Scope tags Edit

Default

Assignments Edit

Included groups

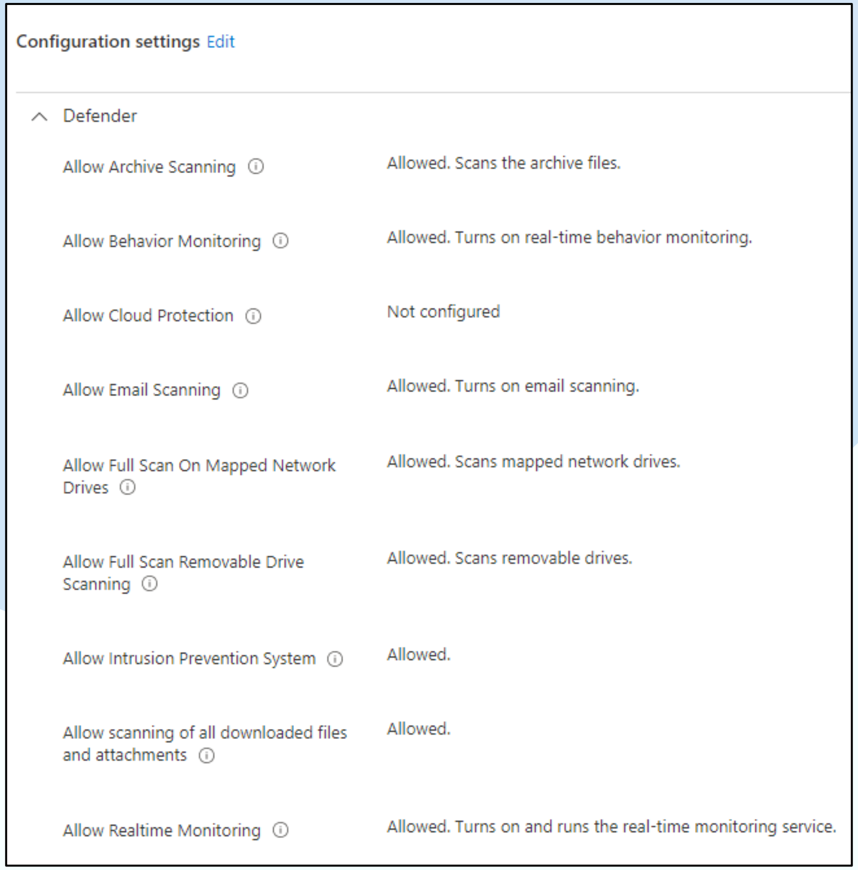
Group	Filter	Filter mode
All Devices	None	None

Excluded groups

Group
No results.

Endpoint Security | Antivirus

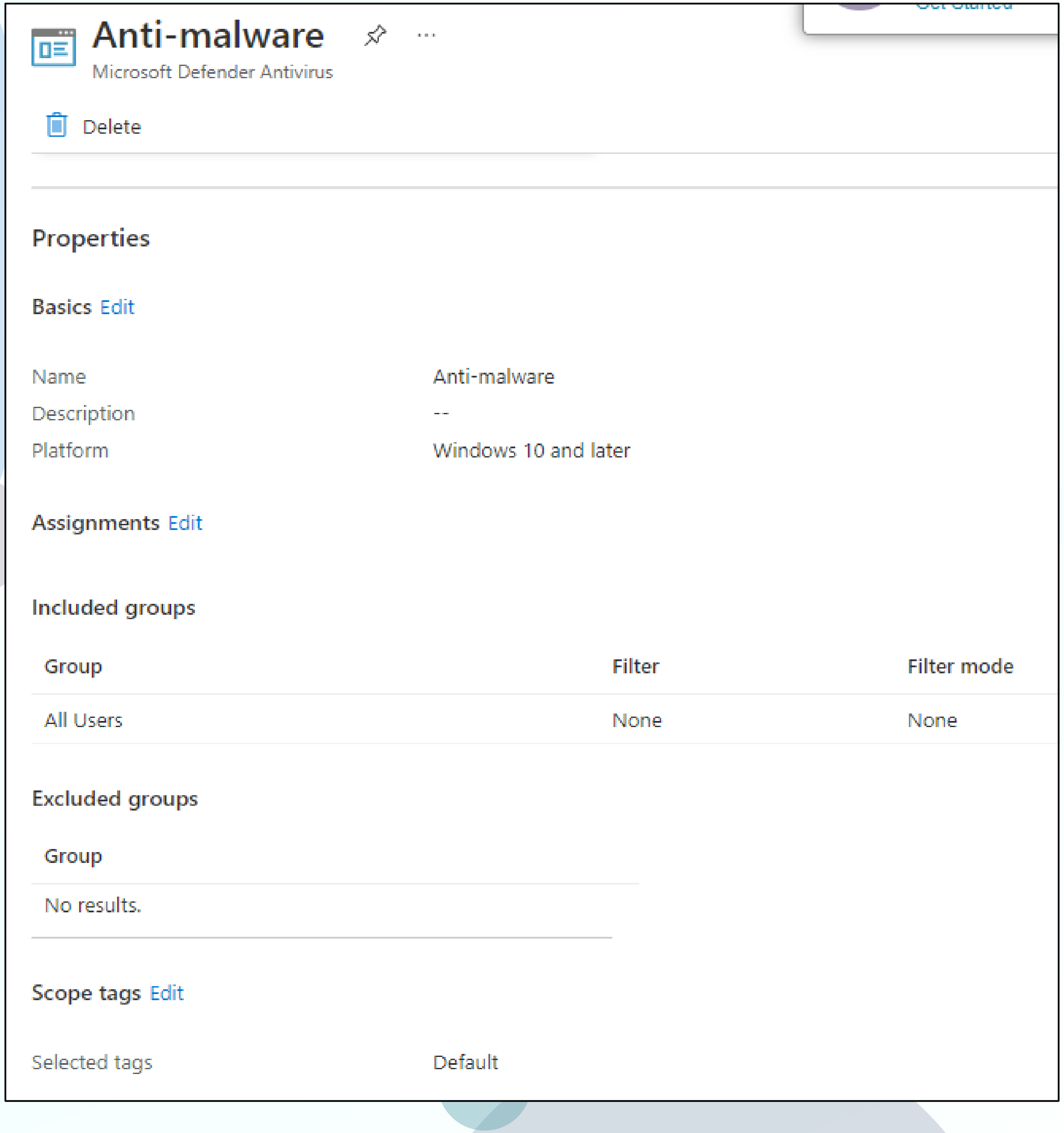
After enabling basic compliance for the devices, we also created Antivirus policy for every user to enhance the protection, by enabling various configurations we are available with, which can be seen below.



Configuration settings Edit

Defender

Allow Archive Scanning ⓘ	Allowed. Scans the archive files.
Allow Behavior Monitoring ⓘ	Allowed. Turns on real-time behavior monitoring.
Allow Cloud Protection ⓘ	Not configured
Allow Email Scanning ⓘ	Allowed. Turns on email scanning.
Allow Full Scan On Mapped Network Drives ⓘ	Allowed. Scans mapped network drives.
Allow Full Scan Removable Drive Scanning ⓘ	Allowed. Scans removable drives.
Allow Intrusion Prevention System ⓘ	Allowed.
Allow scanning of all downloaded files and attachments ⓘ	Allowed.
Allow Realtime Monitoring ⓘ	Allowed. Turns on and runs the real-time monitoring service.



Anti-malware

Microsoft Defender Antivirus

Properties

Basics Edit

Name	Anti-malware
Description	--
Platform	Windows 10 and later

Assignments Edit

Included groups

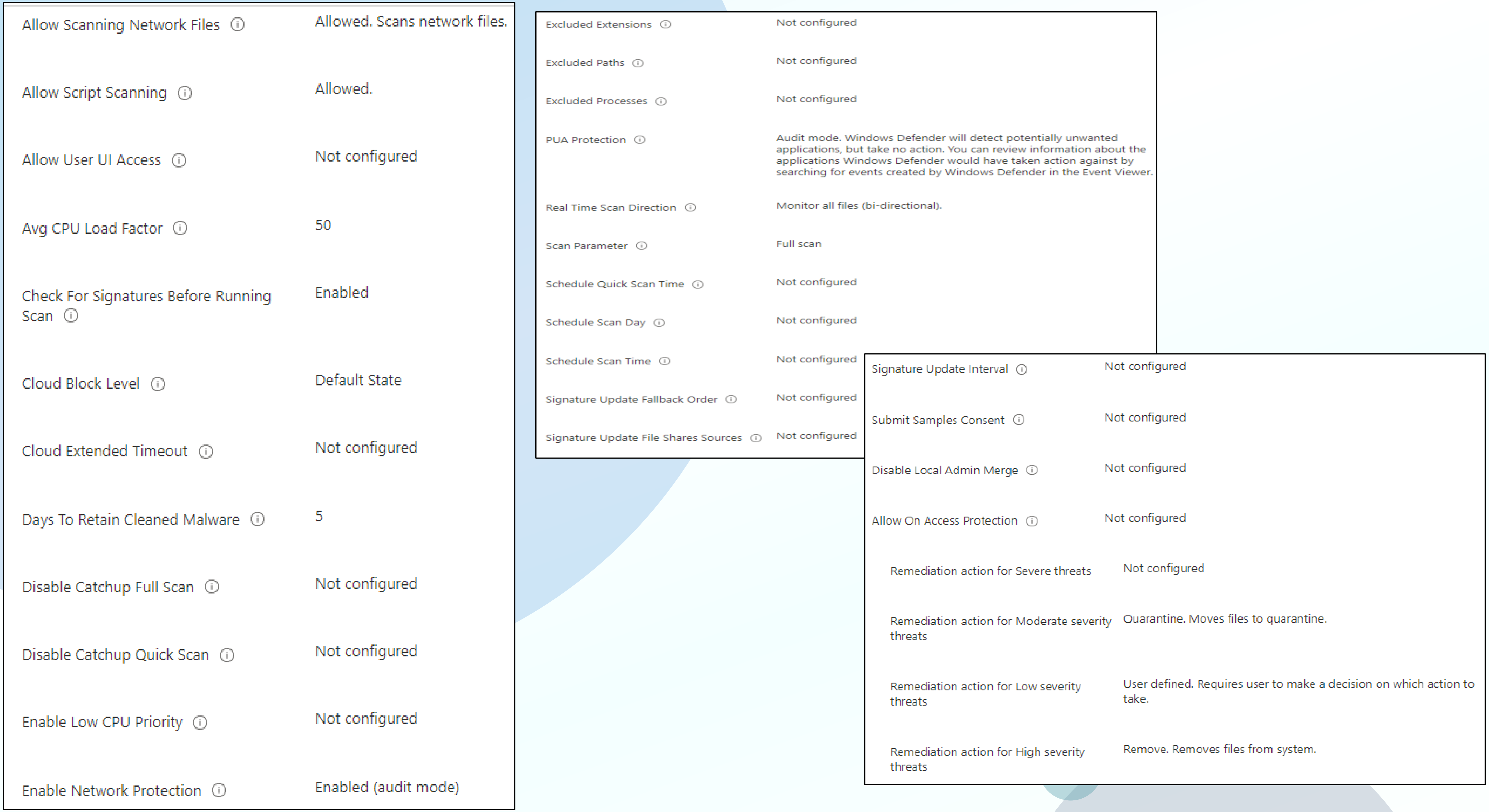
Group	Filter	Filter mode
All Users	None	None

Excluded groups

Group
No results.

Scope tags Edit

Selected tags	Default



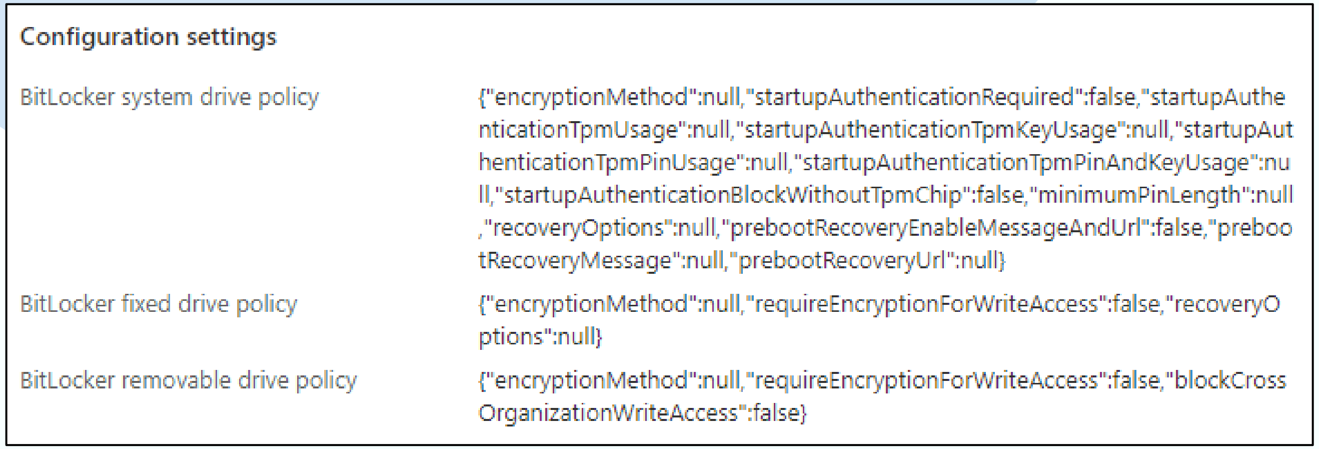
Allow Scanning Network Files	Allowed. Scans network files.
Allow Script Scanning	Allowed.
Allow User UI Access	Not configured
Avg CPU Load Factor	50
Check For Signatures Before Running Scan	Enabled
Cloud Block Level	Default State
Cloud Extended Timeout	Not configured
Days To Retain Cleaned Malware	5
Disable Catchup Full Scan	Not configured
Disable Catchup Quick Scan	Not configured
Enable Low CPU Priority	Not configured
Enable Network Protection	Enabled (audit mode)

Excluded Extensions	Not configured
Excluded Paths	Not configured
Excluded Processes	Not configured
PUA Protection	Audit mode. Windows Defender will detect potentially unwanted applications, but take no action. You can review information about the applications Windows Defender would have taken action against by searching for events created by Windows Defender in the Event Viewer.
Real Time Scan Direction	Monitor all files (bi-directional).
Scan Parameter	Full scan
Schedule Quick Scan Time	Not configured
Schedule Scan Day	Not configured
Schedule Scan Time	Not configured
Signature Update Fallback Order	Not configured
Signature Update File Shares Sources	Not configured

Signature Update Interval	Not configured
Submit Samples Consent	Not configured
Disable Local Admin Merge	Not configured
Allow On Access Protection	Not configured
Remediation action for Severe threats	Not configured
Remediation action for Moderate severity threats	Quarantine. Moves files to quarantine.
Remediation action for Low severity threats	User defined. Requires user to make a decision on which action to take.
Remediation action for High severity threats	Remove. Removes files from system.

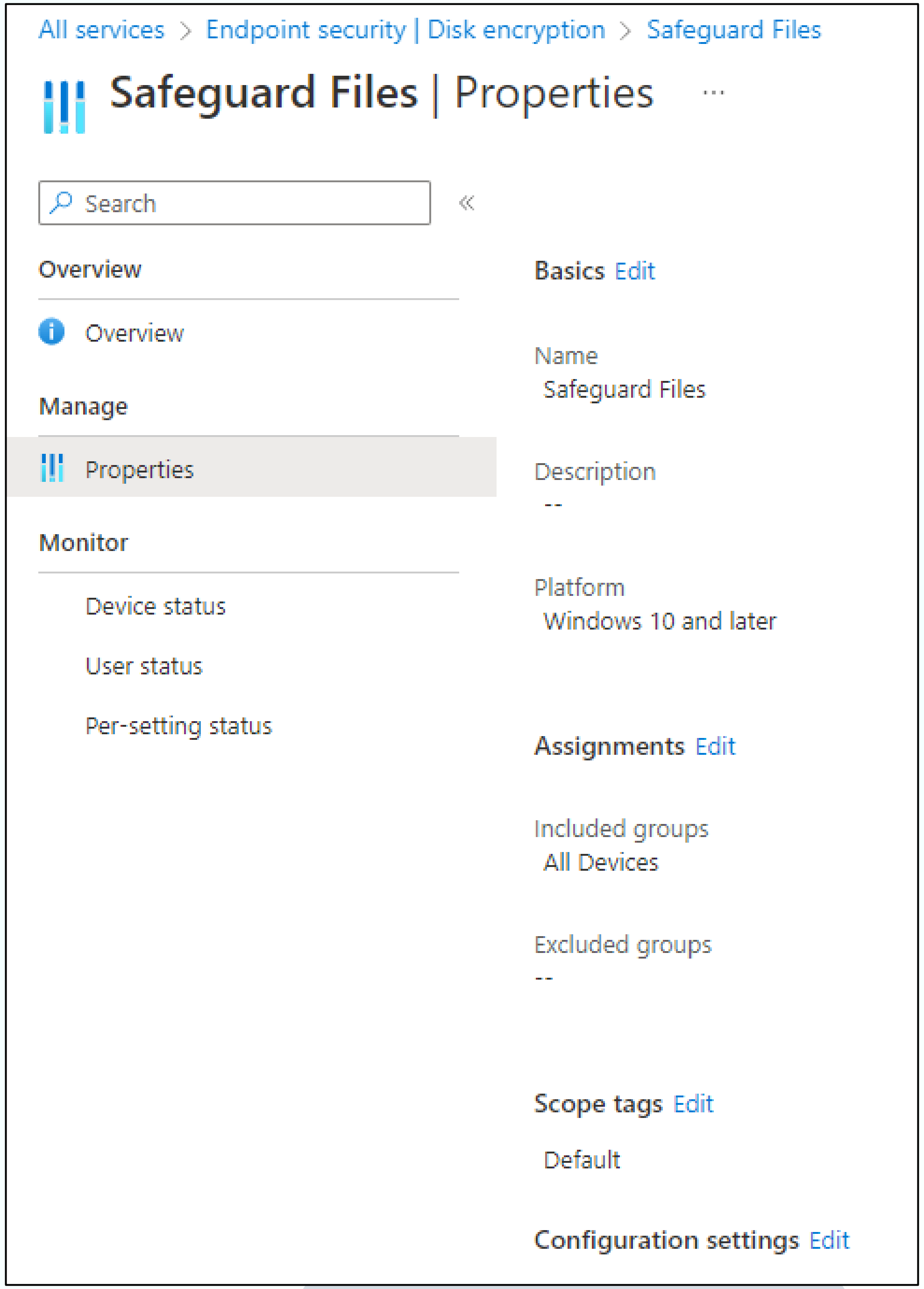
Endpoint security | Disk encryption

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 the status of encryption on the device, encryption readiness, and any prerequisites missing or errors related to encryption on devices.



Configuration settings

BitLocker system drive policy	{"encryptionMethod":null,"startupAuthenticationRequired":false,"startupAuthenticationTpmUsage":null,"startupAuthenticationTpmKeyUsage":null,"startupAuthenticationTpmPinUsage":null,"startupAuthenticationTpmPinAndKeyUsage":null,"startupAuthenticationBlockWithoutTpmChip":false,"minimumPinLength":null,"recoveryOptions":null,"prebootRecoveryEnableMessageAndUrl":false,"prebootRecoveryMessage":null,"prebootRecoveryUrl":null}
BitLocker fixed drive policy	{"encryptionMethod":null,"requireEncryptionForWriteAccess":false,"recoveryOptions":null}
BitLocker removable drive policy	{"encryptionMethod":null,"requireEncryptionForWriteAccess":false,"blockCrossOrganizationWriteAccess":false}



All services > Endpoint security | Disk encryption > Safeguard Files
Safeguard Files | Properties ...
Search
«
Overview
Overview
Manage
Properties
Monitor
Device status
User status
Per-setting status

Basics Edit

Name
Safeguard Files

Description
--

Platform
Windows 10 and later

Assignments Edit

Included groups
All Devices

Excluded groups
--

Scope tags Edit

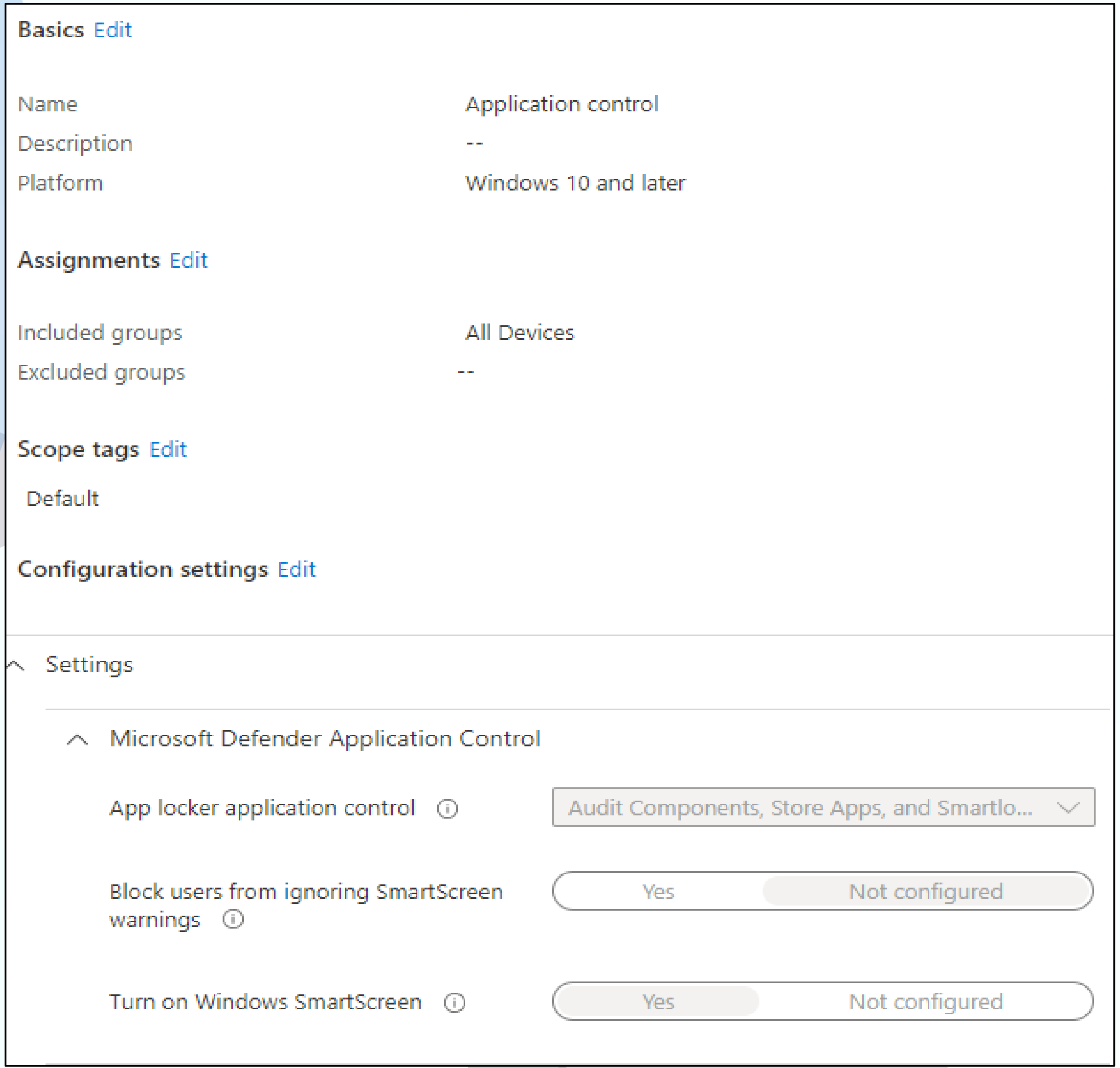
Default

Configuration settings Edit

Endpoint Security | Attack surface reduction

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.



Basics Edit

Name	Application control
Description	--
Platform	Windows 10 and later

Assignments Edit

Included groups	All Devices
Excluded groups	--

Scope tags Edit

Default

Configuration settings Edit

Settings

Microsoft Defender Application Control

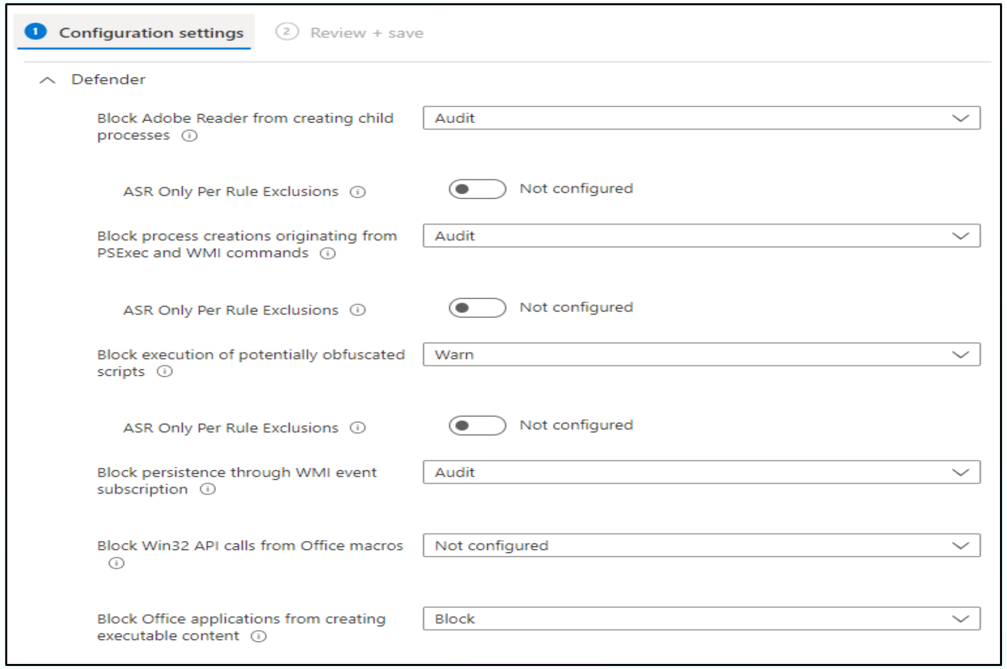
App locker application control: Audit Components, Store Apps, and Smartlo...

Block users from ignoring SmartScreen warnings: Yes [✓ Not configured]

Turn on Windows SmartScreen: [✓ Yes] Not configured

Attack Surface Reduction Rules

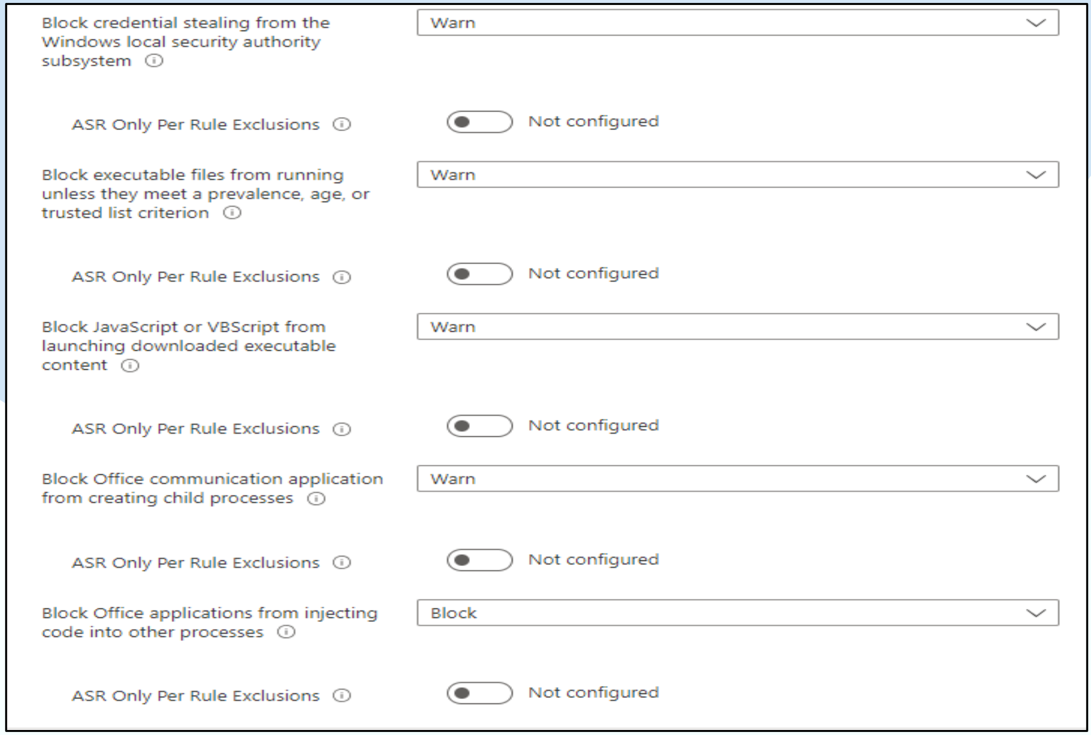
Attack surface reduction rules target behaviors that malware and malicious apps typically use to infect computers, including: Executable files and scripts used in Office apps or web mail that attempt to download or run files Obfuscated or otherwise suspicious scripts Behaviors that apps don't usually initiate during normal day-to-day work



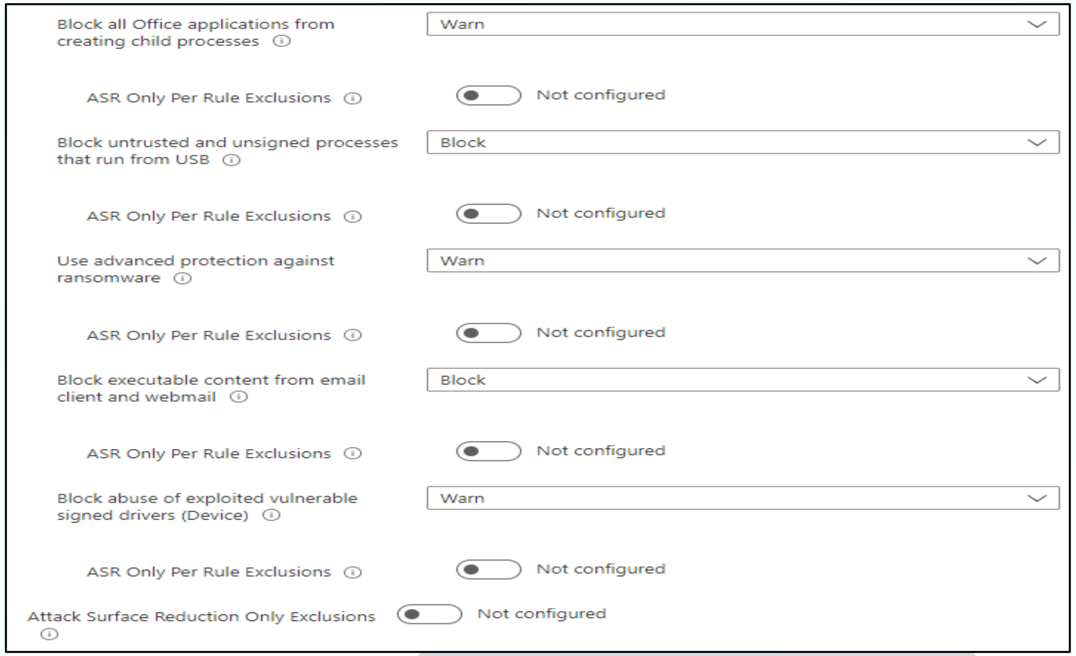
1 Configuration settings   2 Review + save

Defender

Block Adobe Reader from creating child processes	Audit
ASR Only Per Rule Exclusions	Not configured
Block process creations originating from PSExec and WMI commands	Audit
ASR Only Per Rule Exclusions	Not configured
Block execution of potentially obfuscated scripts	Warn
ASR Only Per Rule Exclusions	Not configured
Block persistence through WMI event subscription	Audit
Block Win32 API calls from Office macros	Not configured
Block Office applications from creating executable content	Block



Block credential stealing from the Windows local security authority subsystem	Warn
ASR Only Per Rule Exclusions	Not configured
Block executable files from running unless they meet a prevalence, age, or trusted list criterion	Warn
ASR Only Per Rule Exclusions	Not configured
Block JavaScript or VBScript from launching downloaded executable content	Warn
ASR Only Per Rule Exclusions	Not configured
Block Office communication application from creating child processes	Warn
ASR Only Per Rule Exclusions	Not configured
Block Office applications from injecting code into other processes	Block
ASR Only Per Rule Exclusions	Not configured

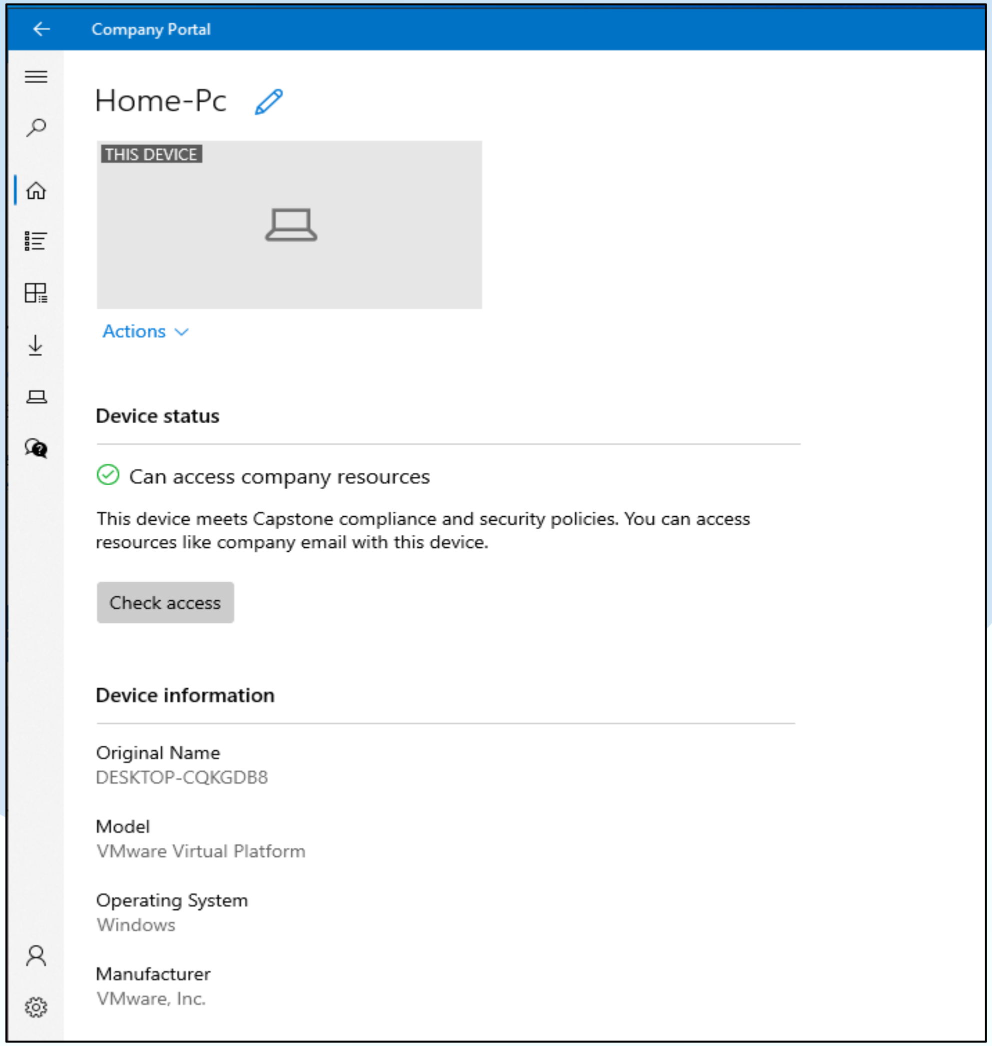


Block all Office applications from creating child processes	Warn
ASR Only Per Rule Exclusions	Not configured
Block untrusted and unsigned processes that run from USB	Block
ASR Only Per Rule Exclusions	Not configured
Use advanced protection against ransomware	Warn
ASR Only Per Rule Exclusions	Not configured
Block executable content from email client and webmail	Block
ASR Only Per Rule Exclusions	Not configured
Block abuse of exploited vulnerable signed drivers (Device)	Warn
ASR Only Per Rule Exclusions	Not configured
Attack Surface Reduction Only Exclusions	Not configured

Applying the established compliance security policies to the users and devices to simulate the workspace environment.

userPrincipalName	displayName	userType	identityIssuer
solution@capstone001.onmicrosoft.com	Tarun Reddi	Admin	capstone001.onmicrosoft.com
user2pro@capstone001.onmicrosoft.com	User2_ProED	Member	capstone001.onmicrosoft.com
user4hom@capstone001.onmicrosoft.com	User4_HomeED_Tarun	Member	capstone001.onmicrosoft.com
user1ent@capstone001.onmicrosoft.com	User1_EnterpriseED	Member	capstone001.onmicrosoft.com
user3hom@capstone001.onmicrosoft.com	User3_HomeED_Praveen	Member	capstone001.onmicrosoft.com

To assign the device to the endpoint manager we need to install the “Company Portal” app in the Microsoft windows store and log in using created user credentials. As shown in the snapshots below.



Home-Pc

Device status

✓ Can access company resources

This device meets Capstone compliance and security policies. You can access resources like company email with this device.

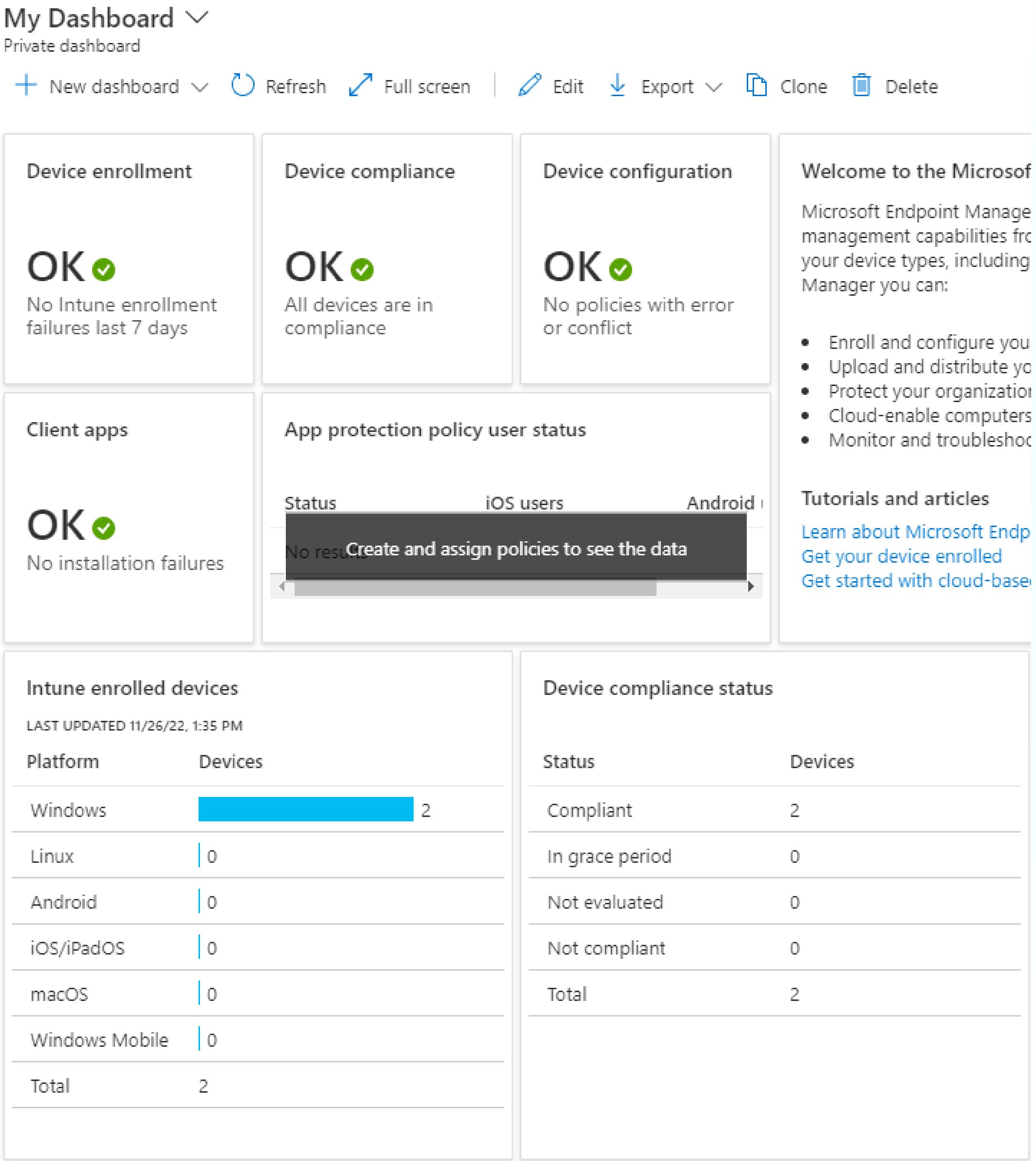
Device information

Original Name
DESKTOP-CQKGDB8

Model
VMware Virtual Platform

Operating System
Windows

Manufacturer
VMware, Inc.



My Dashboard

Private dashboard

Device enrollment

OK ✓
No Intune enrollment failures last 7 days

Device compliance

OK ✓
All devices are in compliance

Device configuration

OK ✓
No policies with error or conflict

Welcome to the Microsof

Microsoft Endpoint Manage
management capabilities fro
your device types, including
Manager you can:

- Enroll and configure you
- Upload and distribute yo
- Protect your organizatio
- Cloud-enable computers
- Monitor and troublesho

Client apps

OK ✓
No installation failures

App protection policy user status

Status	iOS users	Android
No resu		

Create and assign policies to see the data

Tutorials and articles

Learn about Microsoft Endp
Get your device enrolled
Get started with cloud-base

Intune enrolled devices

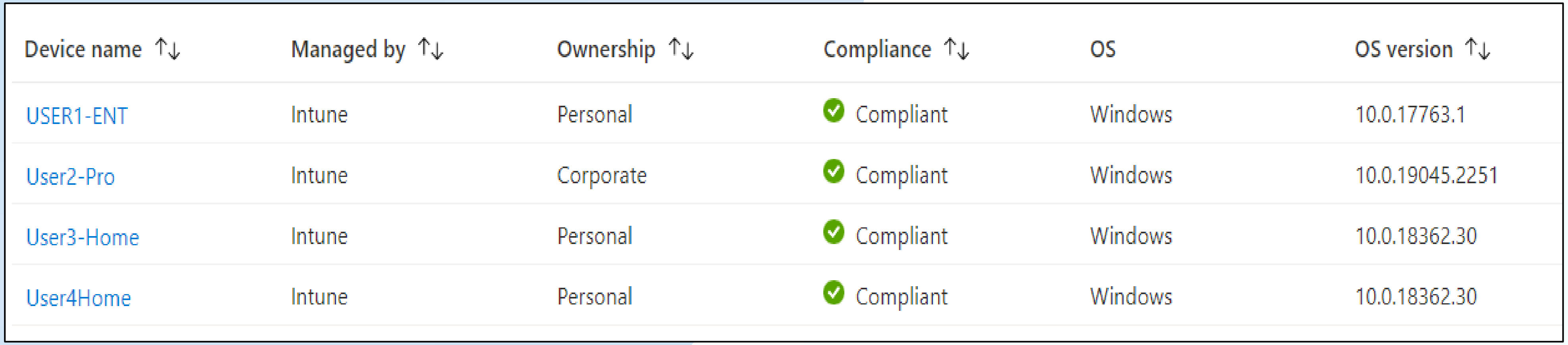
LAST UPDATED 11/26/22, 1:35 PM

Platform	Devices
Windows	2
Linux	0
Android	0
iOS/iPadOS	0
macOS	0
Windows Mobile	0
Total	2

Device compliance status

Status	Devices
Compliant	2
In grace period	0
Not evaluated	0
Not compliant	0
Total	2

We ensured all devices met the security standards we created.

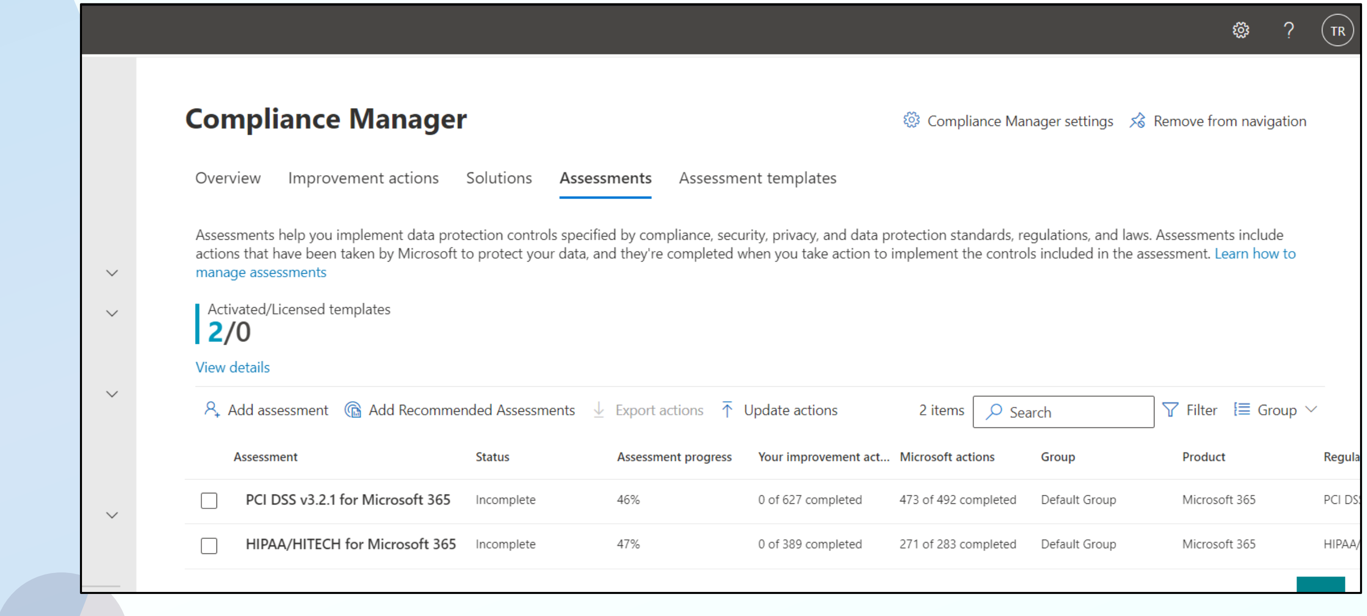


Device name ↑↓	Managed by ↑↓	Ownership ↑↓	Compliance ↑↓	OS	OS version ↑↓
USER1-ENT	Intune	Personal	✓ Compliant	Windows	10.0.17763.1
User2-Pro	Intune	Corporate	✓ Compliant	Windows	10.0.19045.2251
User3-Home	Intune	Personal	✓ Compliant	Windows	10.0.18362.30
User4Home	Intune	Personal	✓ Compliant	Windows	10.0.18362.30

Now we'd like to create a compliance policy based on the PCI DSS, HIPAA standards.
That can be done from the Microsoft preview portal
https://compliance.microsoft.com/homepage

Compliance At Resource Level

Microsoft Azure – Policy | Assessment



Compliance Manager

Compliance Manager settings   Remove from navigation

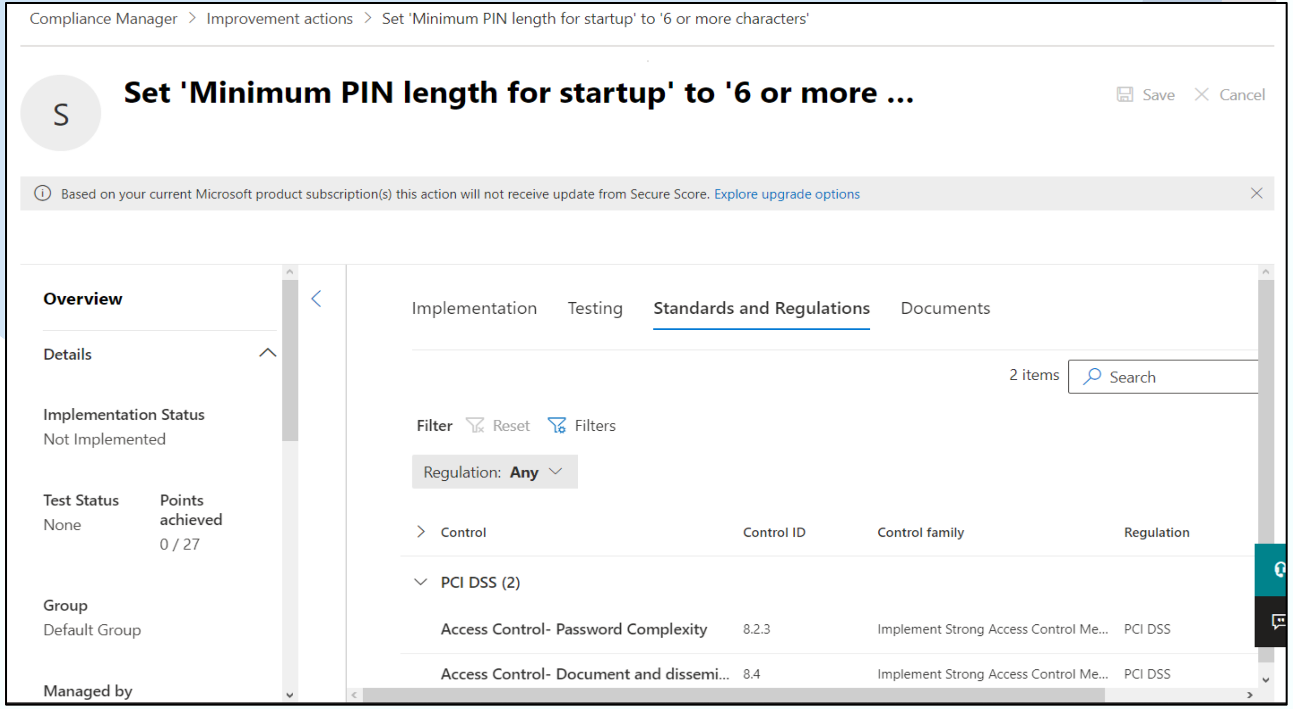
Overview   Improvement actions   Solutions   **Assessments**   Assessment templates

Assessments help you implement data protection controls specified by compliance, security, privacy, and data protection standards, regulations, and laws. Assessments include actions that have been taken by Microsoft to protect your data, and they're completed when you take action to implement the controls included in the assessment. Learn how to manage assessments

Activated/Licensed templates
2/0
View details

Add assessment   Add Recommended Assessments   Export actions   Update actions   2 items   Search   Filter   Group

	Assessment	Status	Assessment progress	Your improvement act...	Microsoft actions	Group	Product	Regula
□	PCI DSS v3.2.1 for Microsoft 365	Incomplete	46%	0 of 627 completed	473 of 492 completed	Default Group	Microsoft 365	PCI DS
□	HIPAA/HITECH for Microsoft 365	Incomplete	47%	0 of 389 completed	271 of 283 completed	Default Group	Microsoft 365	HIPAA/



Compliance Manager > Improvement actions > Set 'Minimum PIN length for startup' to '6 or more characters'

S **Set 'Minimum PIN length for startup' to '6 or more ...**

Save   Cancel

Based on your current Microsoft product subscription(s) this action will not receive update from Secure Score. Explore upgrade options

Overview

Details

Implementation Status
Not Implemented

Test Status
None

Points achieved
0 / 27

Group
Default Group

Managed by

Implementation   Testing   **Standards and Regulations**   Documents

2 items   Search

Filter   Reset   Filters

Regulation: **Any**

Control	Control ID	Control family	Regulation
PCI DSS (2)			
Access Control- Password Complexity	8.2.3	Implement Strong Access Control Me...	PCI DSS
Access Control- Document and dissemi...	8.4	Implement Strong Access Control Me...	PCI DSS

An example policy of the PCI DSS | Set 'Minimum PIN length for startup' to '6 or more characters'

References

- Buchan, J. (2022, August 2). ***Azure Privileged Identity Management. Here's why you need it.*** Performanta. https://www.performanta.com/post/azure-privileged-identity-management-here-s-why-you-need-it

- ***What is Privileged Identity Management?*** *- Azure AD - Microsoft entra*. (n.d.). Microsoft.com. Retrieved October 21, 2022, from https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

- Wrieden, O. (2022, May 3). ***What is Privileged Identity Management and why use it?*** Medium. https://medium.com/@olafwrieden/what-is-privileged-identity-management-and-why-use-it-7f383b3b797a