



Top Security Tips an Intune Admin Should Know

Petri Paavola

Panu Saukko

Panu Saukko

ProTrainIT Oy



Microsoft Certified Trainer



Intune

X@PanuSaukko

Panu.Saukko@protrainit.fi



Petri Paavola

Microsoft MVP –
Windows and Devices
Senior Modern Management Principal

Petri.Paavola@yodamiitti.fi



Skills

- › Windows Autopilot + Intune + Intune for Education
- › Windows 10&11 Deployment and Management
- › Powershell / Graph API
- › Traditional on-prem deployment and management
- › Consulting
- › Training



@petripaavola

<https://github.com/petripaavola>

[Intune.ninja](https://intune.ninja)

[Powershell.ninja](https://powershell.ninja)

Over 23 years of work experience

Current:

- › Yodamiitti Oy / Owner
Consulting / Training

Past:

- › Aalto university / IT-services
Responsible for Workstation service
(Windows, macOS and Linux)



Topics

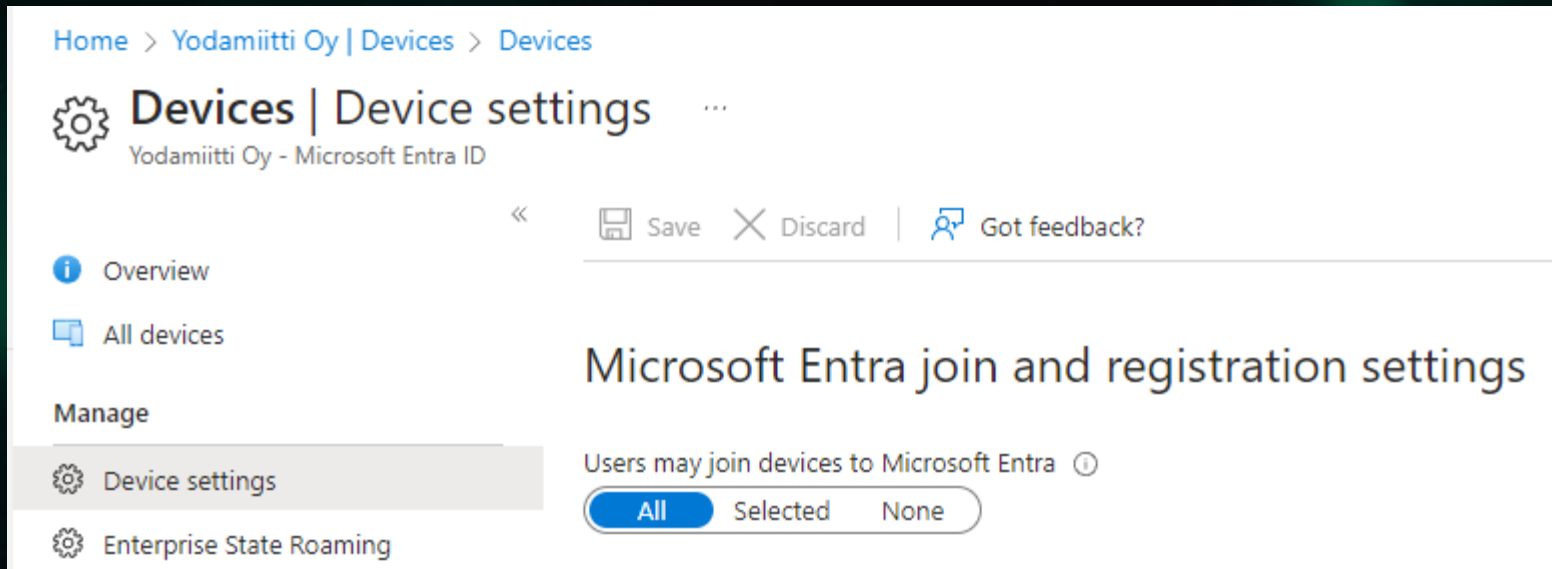
- Enrollment restrictions
- Admin permissions
- Windows LAPS
- Bitlocker
- Autopilot
- Intune logs
- Summary

Entra ID enrollment settings

1. Entra ID join
2. Automatic enrollment to Intune
3. Device enrollment restrictions

Entra ID enrollment settings

- Who can join device to Entra ID
- Add users who are doing Autopilot enrollments



Home > Yodamiitti Oy | Devices > Devices

Devices | Device settings ...
Yodamiitti Oy - Microsoft Entra ID

« Save Discard | Got feedback?

Microsoft Entra join and registration settings

Users may join devices to Microsoft Entra ⓘ

All Selected None

Manage

- Overview
- All devices
- Device settings**
- Enterprise State Roaming




Entra ID enrollment settings

- Automatic enrollment to Intune management after Entra ID join
- Entra ID Premium P1 license
- Add users who are doing Autopilot enrollments

Home > Devices | Windows > Windows | Windows enrollment >

Configure

Microsoft Intune

 Save  Discard  Delete

MDM user scope ⓘ	None Some All
MDM terms of use URL ⓘ	<input type="text" value="https://portal.manage.microsoft.com/TermsOfUse.aspx"/> ✓
MDM discovery URL ⓘ	<input type="text" value="https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc"/> ✓
MDM compliance URL ⓘ	<input type="text" value="https://portal.manage.microsoft.com/?portalAction=Compliance"/> ✓

[Restore default MDM URLs](#)

Entra ID enrollment settings

- Block Personal devices enrollment to Intune

Home > Devices | Enrollment device platform restrictions > All Users | Properties >

Edit restriction

Device type restriction

- 1 Platform settings 2 Review + save

Specify the platform configuration restrictions that must be met for a device to enroll. Use compliance policies to restrict devices after enrollment. Define versions as major.minor.build. Version restrictions only apply to devices enrolled with the Company Portal. Intune classifies devices as personally-owned by default. Additional action is required to classify devices as corporate-owned. [Learn more.](#)

Type	Platform	versions	Personally owned	Device manufacturer
Android Enterprise (work profile)	<input checked="" type="radio"/> Allow <input type="radio"/> Block	Allow min/max range: <input type="text"/> Min <input type="text"/> Max	<input checked="" type="radio"/> Allow <input type="radio"/> Block	<input type="text"/> Manufacturer name
Android device administrator	<input type="radio"/> Allow <input checked="" type="radio"/> Block	Allow min/max range: <input type="text"/> Min <input type="text"/> Max	<input type="radio"/> Allow <input checked="" type="radio"/> Block	<input type="text"/> Manufacturer name
iOS/iPadOS	<input checked="" type="radio"/> Allow <input type="radio"/> Block	Allow min/max range: <input type="text"/> Min <input type="text"/> Max	<input checked="" type="radio"/> Allow <input type="radio"/> Block	Restriction not supported
macOS	<input checked="" type="radio"/> Allow <input type="radio"/> Block	Restriction not supported	<input checked="" type="radio"/> Allow <input type="radio"/> Block	Restriction not supported
Windows (MDM) ⓘ	<input checked="" type="radio"/> Allow <input type="radio"/> Block	Allow min/max range: <input type="text"/> Min <input type="text"/> Max	<input type="radio"/> Allow <input checked="" type="radio"/> Block	Restriction not supported

Stay signed in to all your apps

Windows will remember your account and automatically sign you in to your apps and websites on this device. This will reduce the number of times you are asked to login.



Allow my organization to manage my device

① Selecting this option means your administrator can install apps, control settings, and reset your device remotely. Your organization may require you to enable this option to access data and apps on this device.

[No, sign in to this app only](#)

OK

Enrollment restrictions: Block personal devices

Trying to enroll a new device during OOBЕ with a company account

No Entra ID device exists even if the user had rights to join devices to Entra ID

How would you like to set up this device?



Set up for personal use

Use a personal Microsoft account to get set up and have full control over this device.



Set up for work or school

Get access to your organization's resources like email, network, apps, and services. Your organization will have full control over this device.

Next



Something went wrong.



This feature is not supported. Contact your system administrator with the error code 80180014.

Additional problem information:

Server error code: 80180014

Correlation ID: Not available

Timestamp: 2024-01-31T08:46:10Z

Server message: Not available

More information: <https://www.microsoft.com/mdmerrors>

Try again



Manage local administrators

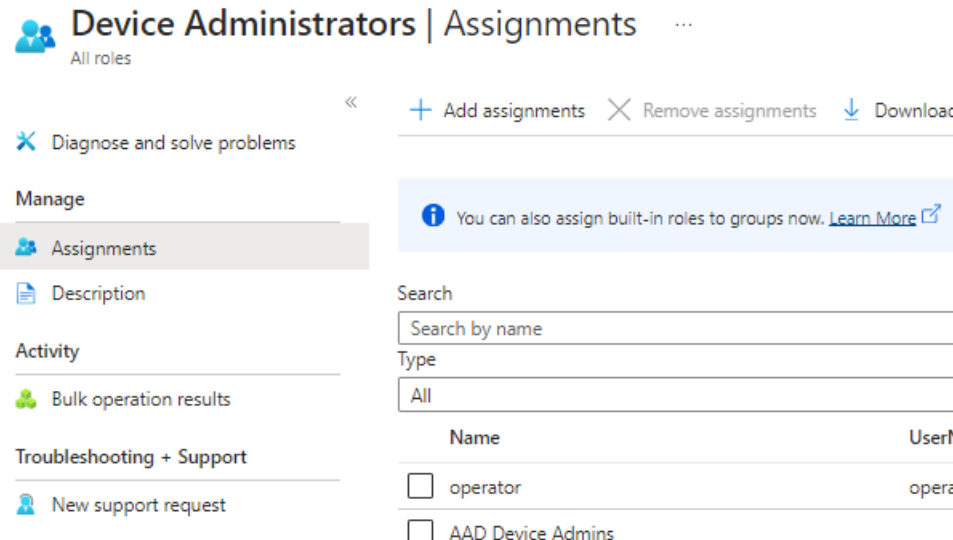
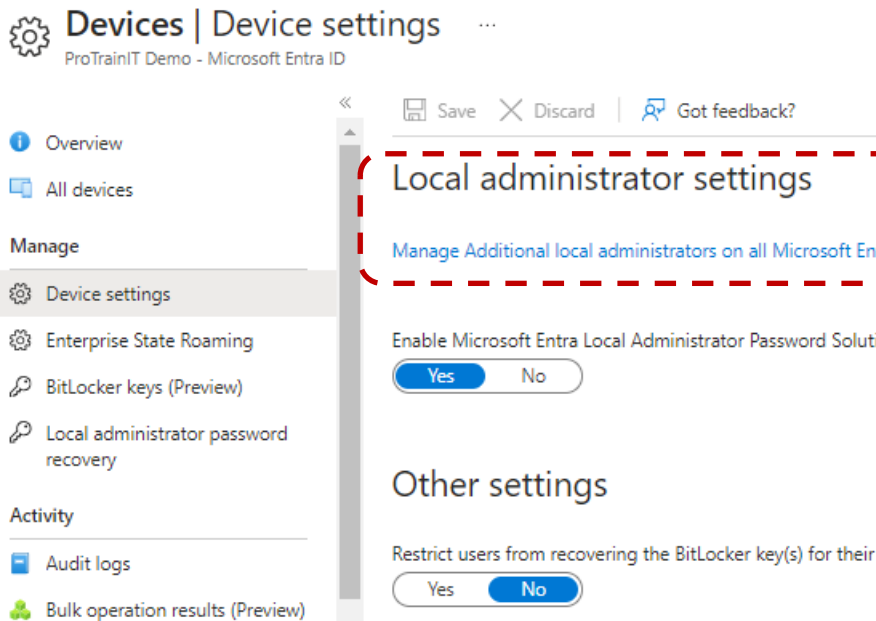
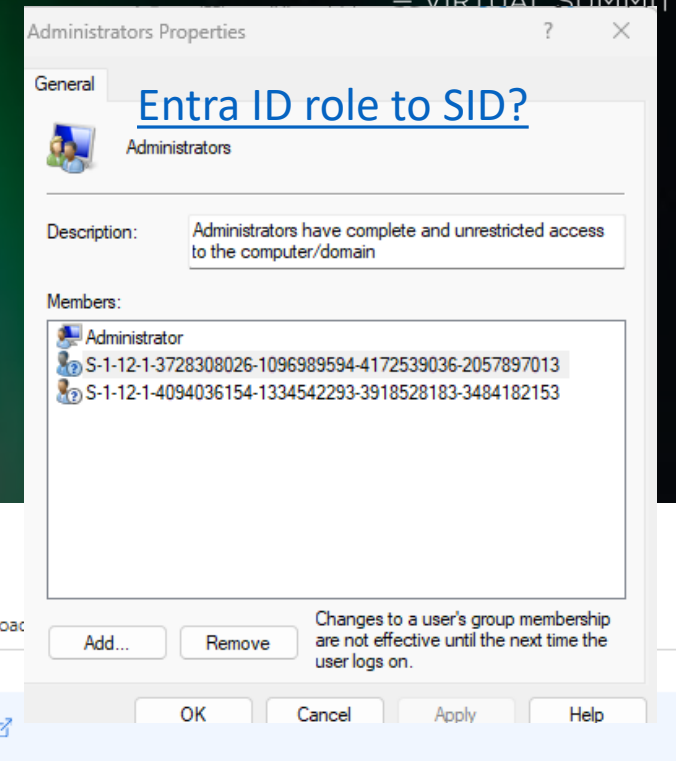
Default local admin rights on Entra ID joined devices

- Local Administrator account (disabled by default)
- Global admin **role** owners
- Microsoft Entra Joined Device Local Administrator **role**
 - No members by default
- The user who enrolled the device?
 - Autopilot device: if allowed by Autopilot profile
 - Non-autopilot device: if personal devices are allowed to enroll

Local Admin Rights on Entra ID joined devices

NORDIC
— VIRTUAL SUMMIT —

- Local admin rights on ALL devices
 - Global admins **role**
 - Microsoft Entra Joined Device Local Administrator **role** assigned to a group/user
 - Who can modify group members?



DEMO

Local admins rights

Device Admin Rights

- Configure admin rights to subset of devices

Home > Endpoint security | Account protection >

Create profile ...

Local user group membership

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

Local Users And Groups

Update or replace?

+ Add Delete

<input type="checkbox"/> Local group ⓘ	Group and user action ⓘ	User selection type ⓘ	Selected users/groups
<input type="checkbox"/> Administrators ▾	<div><div>Add (Update) ▾</div><div>Add (Update)</div><div>Remove (Update)</div><div>Add (Replace)</div></div>	Users/Groups ▾	Users selected: 1

Most secure →

Can I apply more than one LocalUserAndGroups policy/XML to the same device?

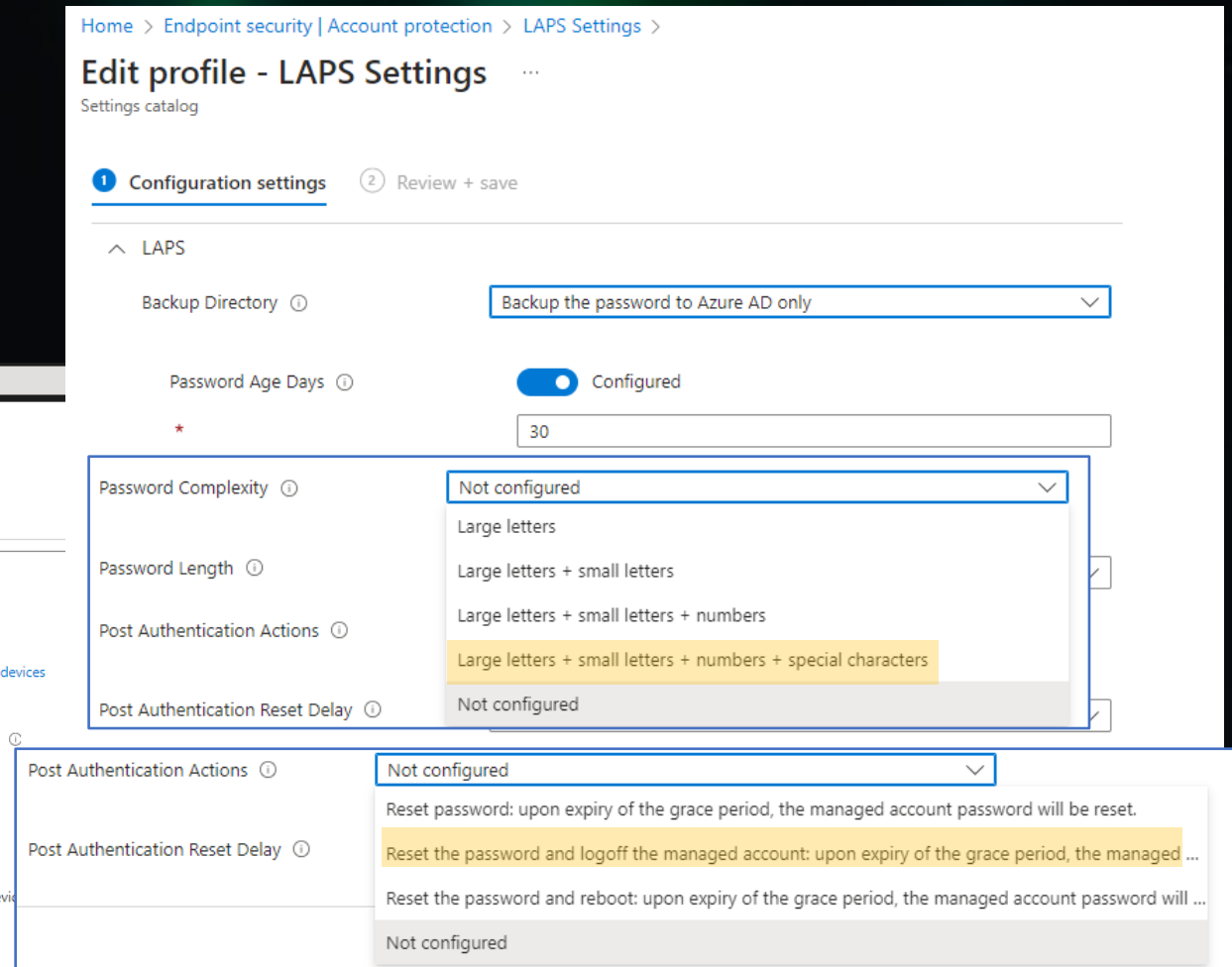
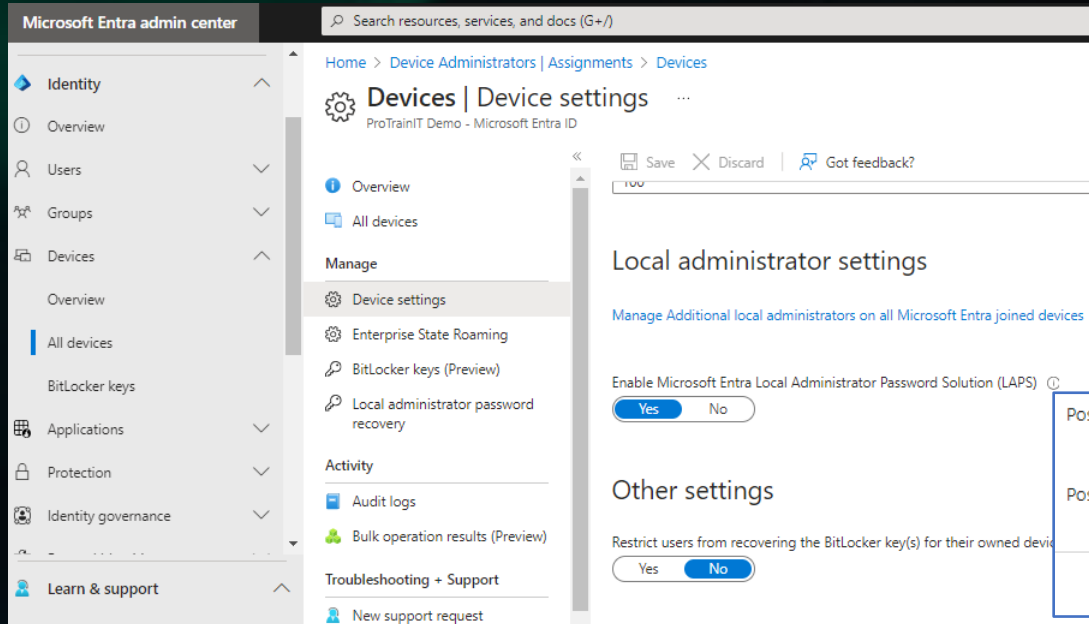
No, this is not allowed. Attempting to do so will result in a conflict in Intune.

[LocalUsersAndGroups Policy CSP](#)

Windows LAPS

Windows LAPS

- Enable Windows LAPS for Entra ID joined devices
- Very simple to configure Windows LAPS settings
- Passwords are in Entra ID (and accessible from Intune)
- Just need Windows 10/11 with at least April 2023 CU



Windows LAPS debugging

Microsoft-Windows-LAPS/Operational

Event Properties - Event 10003, LAPS

General Details

LAPS policy processing is now starting.
See <https://go.microsoft.com/fwlink/?linkid=2220550> for more information.

Log Name: Microsoft-Windows-LAPS/Operational
Source: LAPS Logged: 24/01/2024 14.27.41
Event ID: 10003 Task Category: None

↑
↓

Level	Id	Description
User:		
OpCo	10000	The Local Administrator Password feature was successfully loaded and initialized.
More	10003	LAPS policy processing is now starting.
Co	10004	LAPS policy processing succeeded.
	10022	The current LAPS policy is configured as follows: ...
	10010	LAPS is configured to backup passwords to Azure Active Directory.
	10067	The configured local account is currently disabled. The account must be enabled before it can be used.

Windows LAPS

- Enable/disable local admin account via remediation

Home > Devices | Windows > Windows | Windows devices > SANTAPC950 >

Run remediation (preview) ...

SANTAPC950

Deploy a remediation script package to this device using both a detection and remediation scripts. [Learn more about the remediation script packages.](#) [To manage the script packages available on this screen, go to Proactive remediations.](#)

ⓘ

Script package name	Description
<input type="checkbox"/> Disable local Administrator account	
<input checked="" type="checkbox"/> Enable local Administrator account	

```
# Enable Built-in Administrator account
#
# Petri.Paavola@yodamiitti.fi
# Microsoft MVP - Windows and Devices

# Get the Administrator account name
$adminAccount = Get-LocalUser | Where-Object { $_.SID -like 'S-1-5-*-500' }
$adminName = $adminAccount.Name
#Write-Output "Administrator account name: $adminName"

# Enable the Administrator account
Enable-LocalUser -Name $adminName
$Success = $?

if($Success) {
    Write-Output "Administrator account enabled: $adminName"
    Exit 0
} else {
    Write-Output "Error enabling local administrator account: $adminName"
    Exit 1
}
```

Disable account: Disable-LocalUser

Need to run as 64-bit!

Non-default admin account

- Need to be created manually
 - Automatically in the upcoming Windows release?
- Autopilot enrollment
 - Create the new admin account in your Autopilot branding process
 - LAPS policy fails until the account exists
 - Policy is rerun every 60 min
- Or use remediation/PowerShell scripts

Windows LAPS permissions

- Entra ID custom role

<input type="checkbox"/>	<code>microsoft.directory/deviceLocalCredentials/password/read</code>	Read all properties of the backed up local administrator account credentials for Microsoft Entra joined devices, including the password
<input type="checkbox"/>	<code>microsoft.directory/deviceLocalCredentials/standard/read</code>	Read all properties of the backed up local administrator account credentials for Microsoft Entra joined devices, except the password

- By default:
 - Cloud Device Administrator
 - Intune Administrator
 - Global Admin
- Not within Intune custom roles 😞

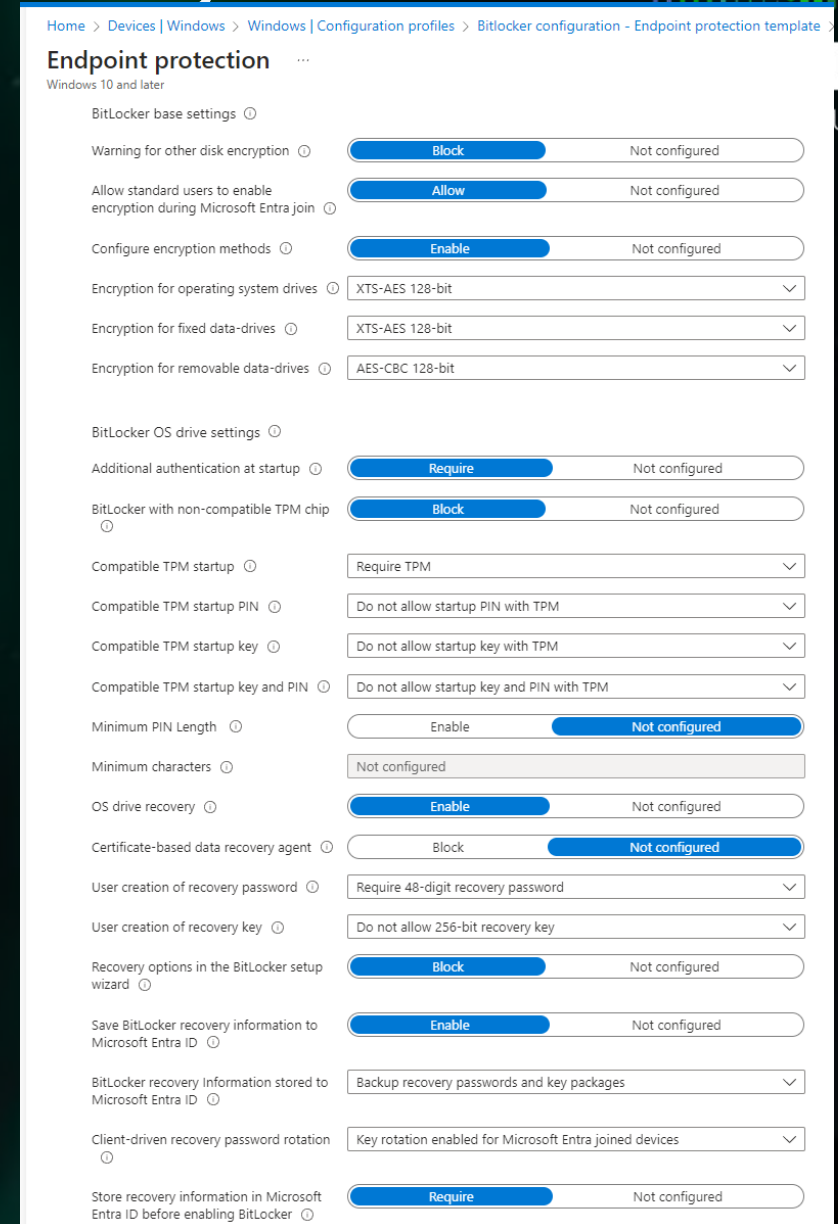
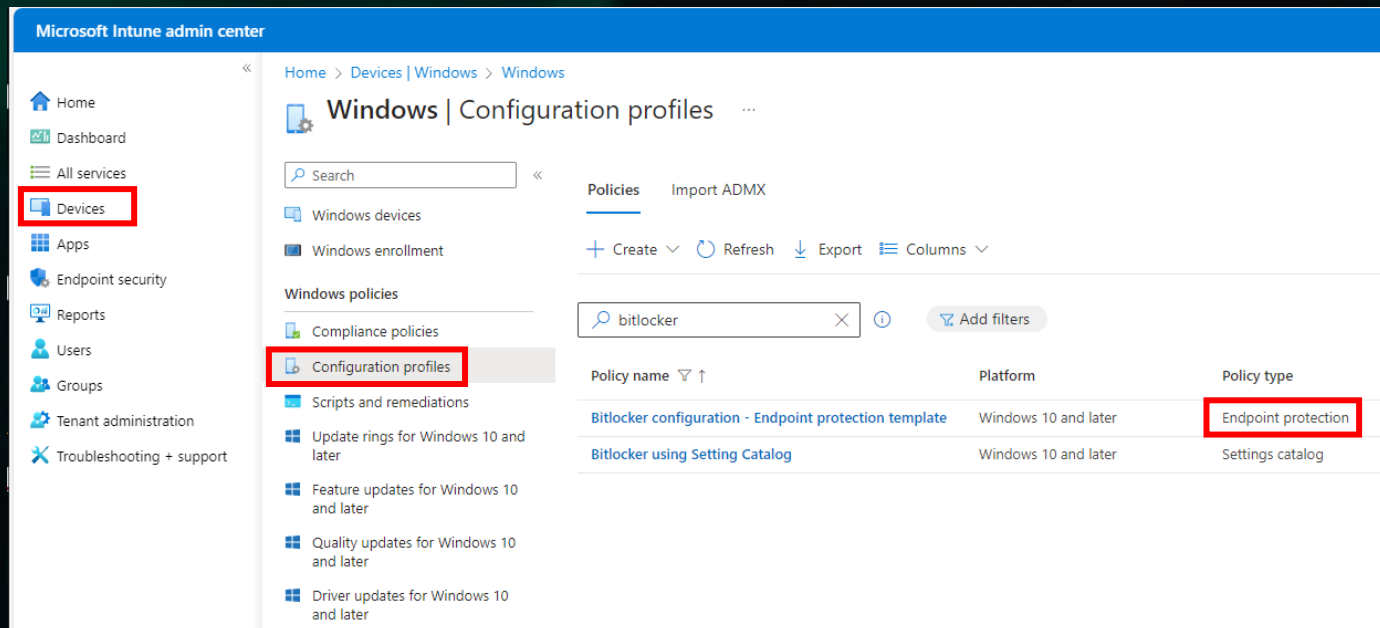
Bitlocker

Bitlocker

- Enable Bitlocker on your devices!
- Multiple ways to set. Which one to use?
 - Configuration profiles → Endpoint protection policy type
 - Setting catalog → create your own template
 - Endpoint security
 - **Old & New template!**
- Change your current policy to new template?
- What to use for new profiles?
 - New Endpoint security template vs Settings catalog

Bitlocker - Endpoint protection policy

- Configuration profiles -> Endpoint protection policy
- First template which may still be in use



Bitlocker - Setting Catalog

- Settings Catalog
- Create your own policy settings

Microsoft Intune admin center

Home > Devices | Windows > Windows

Windows | Configuration profiles

Search

Windows devices

Windows enrollment

Windows policies

Compliance policies

Configuration profiles

Scripts and remediations

Update rings for Windows 10 and later

Feature updates for Windows 10 and later

Quality updates for Windows 10 and later

Driver updates for Windows 10 and later

Policies Import ADMX

Create Refresh Export Columns

bitlocker

Add filters

Policy name	Platform	Policy type
Bitlocker configuration - Endpoint protection template	Windows 10 and later	Endpoint protection
Bitlocker using Setting Catalog	Windows 10 and later	Settings catalog

Home > Devices | Windows > Windows | Configuration profiles > Bitlocker using Setting Catalog

Edit profile - Bitlocker using Setting Catalog

Settings catalog

Configuration settings Review + save

+ Add settings

Administrative Templates Remove category

Windows Components > BitLocker Drive Encryption > Operating System Drives Remove subcategory

4 of 26 settings in this subcategory are not configured

Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive) ☐ False

Configure TPM startup key and PIN: * Do not allow startup key and PIN with TPM

Configure TPM startup key: * Do not allow startup key with TPM

Configure TPM startup PIN: * Do not allow startup PIN with TPM

Configure TPM startup: * Require TPM

Allow devices compliant with InstantGo or HSTI to opt out of pre-boot PIN. ☐ Disabled

Allow enhanced PINs for startup ☐ Disabled

Choose how BitLocker-protected operating system drives can be recovered ☒ Enabled

Do not allow 256-bit recovery key

Configure user storage of BitLocker recovery information: * Require 48-digit recovery password

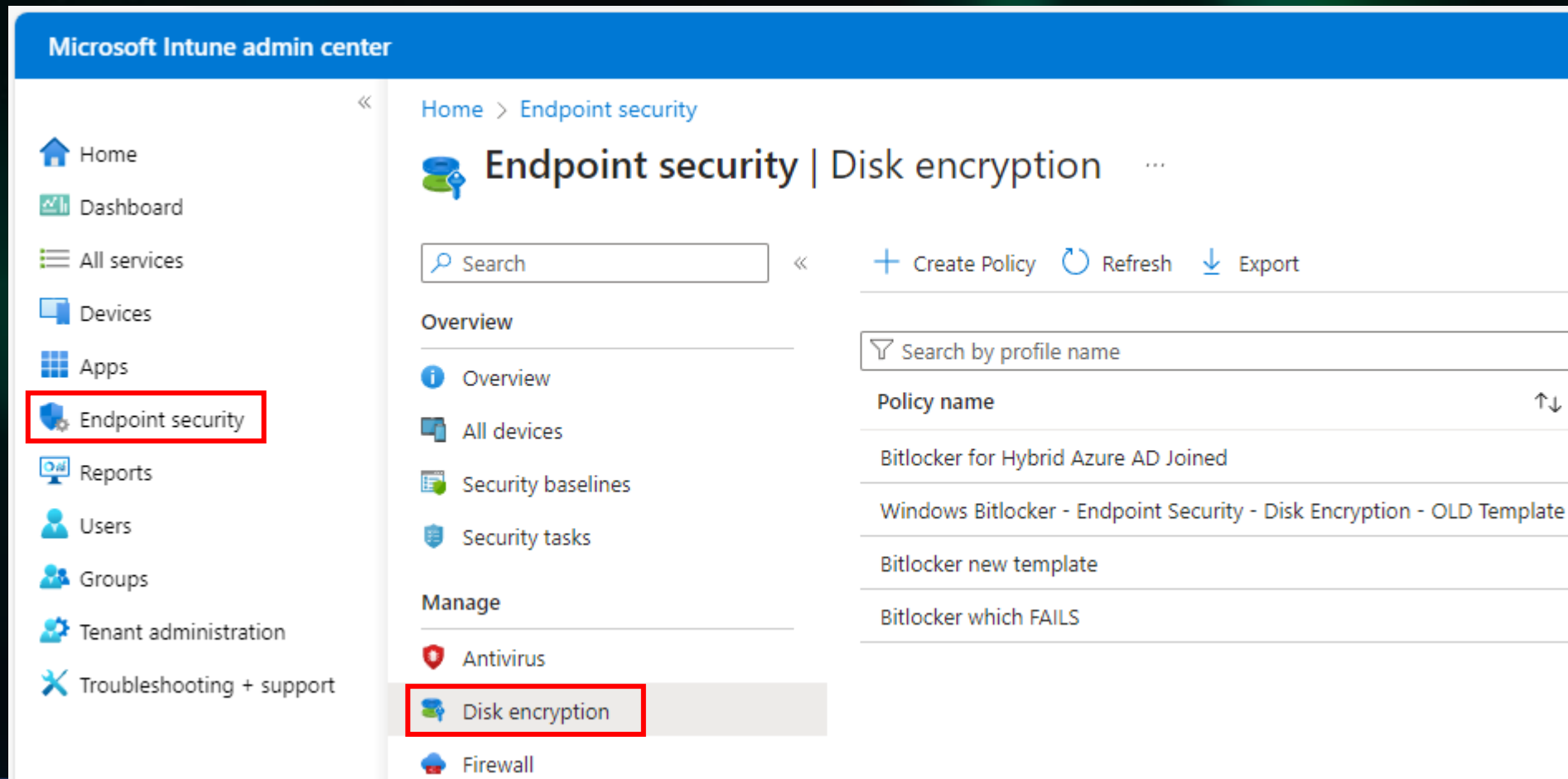
Allow data recovery agent ☐ False

Configure storage of BitLocker recovery information to AD DS: * Store recovery passwords and key packages

Do not enable BitLocker until recovery information is stored to AD DS for operating system drives ☒ True

Bitlocker - Endpoint Security templates

- Endpoint Security -> Disk encryption
- Newest templates



The screenshot displays the Microsoft Intune admin center interface. The left-hand navigation pane includes links to Home, Dashboard, All services, Devices, Apps, Endpoint security (highlighted with a red box), Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Endpoint security | Disk encryption' and features a search bar, 'Create Policy', 'Refresh', and 'Export' buttons. Below this, there are sections for 'Overview' (with links to Overview, All devices, Security baselines, and Security tasks) and 'Manage' (with links to Antivirus, Disk encryption (highlighted with a red box), and Firewall). A table on the right lists policies, with a search bar 'Search by profile name' and a table with columns 'Policy name' and a sort icon. The table contains three entries: 'Bitlocker for Hybrid Azure AD Joined', 'Windows Bitlocker - Endpoint Security - Disk Encryption - OLD Template', and 'Bitlocker new template'. Below the table, there is a link 'Bitlocker which FAILS'.

Policy name
Bitlocker for Hybrid Azure AD Joined
Windows Bitlocker - Endpoint Security - Disk Encryption - OLD Template
Bitlocker new template

Bitlocker - Endpoint Security - old template

Home > Endpoint security | Disk encryption > Windows BitLocker - Endpoint Security - Disk Encryption - OLD Template | Properties >

Edit profile ...

1 Configuration settings 2 Review + save

Settings

Search for a setting

BitLocker - Base Settings

Enable Full disk or Used Space only encryption for OS and fixed data drives ⓘ

Yes

Not configured

Require storage cards to be encrypted (mobile only) ⓘ

Yes

Not configured

Hide prompt about third-party encryption ⓘ

Yes

Not configured

Allow standard users to enable encryption during Autopilot ⓘ

Yes

Not configured

Configure client-driven recovery password rotation ⓘ

Enable rotation on Azure AD-joined devices



BitLocker - Fixed Drive Settings

BitLocker fixed drive policy ⓘ

Configure

Not configured

BitLocker - OS Drive Settings

BitLocker system drive policy ⓘ

Configure

Not configured

Startup authentication required ⓘ

Yes

Not configured

Compatible TPM startup ⓘ

Required



Compatible TPM startup PIN ⓘ

Blocked



Compatible TPM startup key ⓘ

Blocked



Compatible TPM startup key and PIN ⓘ

Blocked



Disable BitLocker on devices where TPM is incompatible ⓘ

Yes

Not configured

Enable preboot recovery message and url ⓘ

Yes

Not configured

Preboot recovery message ⓘ

Something went wrong. Unplug all USB-devices and docks and restart computer.

If problem continues contact IT-Support +35840xxxxxxx

Preboot recovery url ⓘ

<https://portal.manage.microsoft.com/>



System drive recovery ⓘ

Configure

Not configured

Recovery key file creation ⓘ

Blocked



Configure BitLocker recovery package ⓘ

Password and key



Require device to back up recovery information to Azure AD ⓘ

Yes

Not configured

Recovery password creation ⓘ

Required



Hide recovery options during BitLocker setup ⓘ

Yes

Not configured

Enable BitLocker after recovery information to store ⓘ

Yes

Not configured

Block the use of certificate-based data recovery agent (DRA) ⓘ

Yes

Not configured

Minimum PIN length ⓘ



Configure encryption method for Operating System drives ⓘ

Not configured



BitLocker - Removable Drive Settings

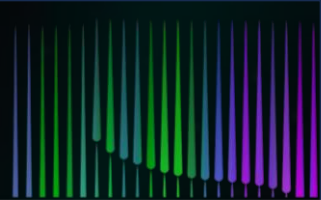
BitLocker removable drive policy ⓘ

Configure

Not configured

NORDIC
- VIRTUAL SUMMIT -

Bitlocker - Endpoint Security - current template



[Home](#) > [Endpoint security | Disk encryption](#) > [Bitlocker new template](#) >

Edit profile - Bitlocker new template

Settings catalog

1 Configuration settings 2 Review + save

BitLocker

- Require Device Encryption ☒ Enabled
- Allow Warning For Other Disk Encryption ☐ Disabled
- Allow Standard User Encryption ☒ Enabled
- Configure Recovery Password Rotation ☐ Refresh on for Azure AD-joined devices

Administrative Templates

Windows Components > BitLocker Drive Encryption

- Choose drive encryption method and cipher strength (Windows 10 [Version 1511] and later) ☒ Enabled
- Select the encryption method for removable data drives: * AES-CBC 128-bit (default)
- Select the encryption method for operating system drives: * XTS-AES 128-bit (default)
- Select the encryption method for fixed data drives: * XTS-AES 128-bit (default)
- Provide the unique identifiers for your organization ☐ Not configured

Windows Components > BitLocker Drive Encryption > Operating System Drives

- Enforce drive encryption type on operating system drives ☒ Enabled
- Select the encryption type: (Device) * Full encryption
- Require additional authentication at startup ☒ Enabled
- Configure TPM startup key: * Do not allow startup key with TPM
- Configure TPM startup key and PIN: * Do not allow startup key and PIN with TPM
- Configure TPM startup: * Require TPM
- Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive) ☐ False
- Configure TPM startup PIN: * Do not allow startup PIN with TPM
- Configure minimum PIN length for startup ☐ Not configured
- Allow enhanced PINs for startup ☐ Not configured
- Disallow standard users from changing the PIN or password ☐ Not configured
- Allow devices compliant with InstantGo or HSTI to opt out of pre-boot PIN. ☐ Not configured
- Enable use of BitLocker authentication requiring preboot keyboard input on slates ☐ Not configured
- Choose how BitLocker-protected operating system drives can be recovered ☒ Enabled

Omit recovery options from the BitLocker setup wizard ☒ True

Do not allow 256-bit recovery key

Save BitLocker recovery information to AD DS for operating system drives ☒ True

Do not enable BitLocker until recovery information is stored to AD DS for operating system drives ☒ True

Configure user storage of BitLocker recovery information: * Require 48-digit recovery password

Allow data recovery agent ☐ False

Configure storage of BitLocker recovery information to AD DS: * Store recovery passwords and key packages

Configure pre-boot recovery message and URL ☒ Enabled

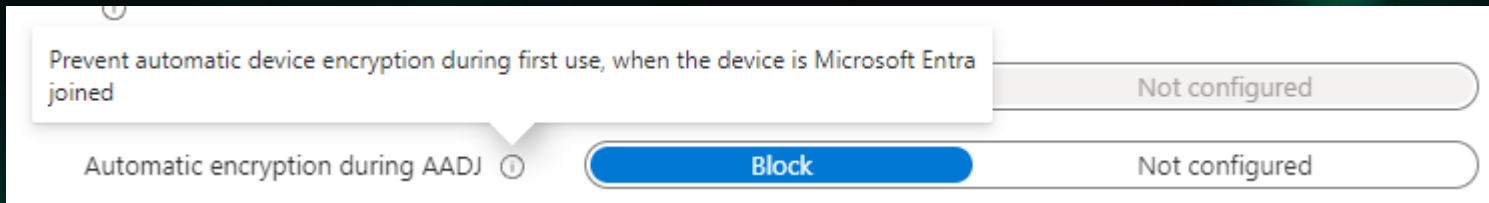
Select an option for the pre-boot recovery message: * Use custom recovery message

Custom recovery URL option:

Custom recovery message option: Something went wrong! Unplug all USB-device and docks and re

Bitlocker - Automatic Encryption during Entra Join

- (Bitlocker /) **Device encryption** can be enabled automatically after Entra Join and after user sign in **without Bitlocker policy**
- You may want to prevent this with policy setting



- Or deploy Bitlocker policy during Enrollment Status Page phase

BitLocker automatic device encryption

BitLocker automatic device encryption uses BitLocker drive encryption technology to automatically encrypt internal drives after the user completes the Out Of Box Experience (OOBE) on [Modern Standby](#) or HSTI-compliant hardware.

ⓘ Note

BitLocker automatic device encryption starts during Out-of-box (OOBE) experience. However, protection is enabled (armed) only after users sign in with a **Microsoft Account** or an **Azure Active Directory** account. Until that, protection is suspended and data is not protected. BitLocker automatic device encryption is not enabled with local accounts, in which case BitLocker can be manually enabled using the BitLocker Control Panel.

Bitlocker - Recovery key

- Stored in Entra ID
- Also shown in Intune console

Microsoft Intune admin center

Home > Devices | Windows > Windows | Windows devices > APVM-8726300880

APVM-8726300880 | Recovery keys

Search

Got feedback?

Overview

Manage

- Properties

Monitor

- Hardware
- Discovered apps
- Device compliance
- Device configuration
- App configuration
- Local admin password
- Recovery keys**

Recovery Key (Preview)

Device Name
APVM-8726300880

BitLocker Key Id
86ec5886-05e2-4a85-8ccd-f170d6f6992c

BitLocker Recovery Key
375419-699479-641245-092587-

Drive Type
Operating system drive

Backed up
1/31/2024, 12:37:03 PM

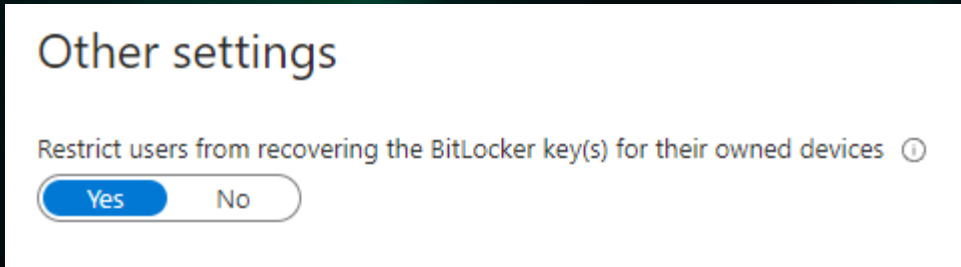
BitLocker Key Id	BitLocker Recovery Key (Preview)	Drive Type
86ec5886-05e2-4a85-8ccd-f170d6f6992c	Show Recovery Key	Operating system drive
f9c8aa1c-a2e1-4396-8f69-6024d046591f	Show Recovery Key	Operating system drive

Bitlocker - Recovery key

- Who can view recovery keys?
 - Entra ID permissions
 - By default: Cloud Device Administrator, Intune Administrator, Global Administrator, Global Reader, Helpdesk Administrator, Security Administrator, Security Reader
 - For custom roles: `microsoft.directory/bitlockerKeys/key/read`

Bitlocker - Recovery key

- Prevent users seeing their device's Bitlocker Recovery Key?
 - If/When users don't have Administrative rights then they should not be able to read Bitlocker Recovery keys either?
 - This is security, process and usability question
-
- Entra ID -> Devices -> Device Settings



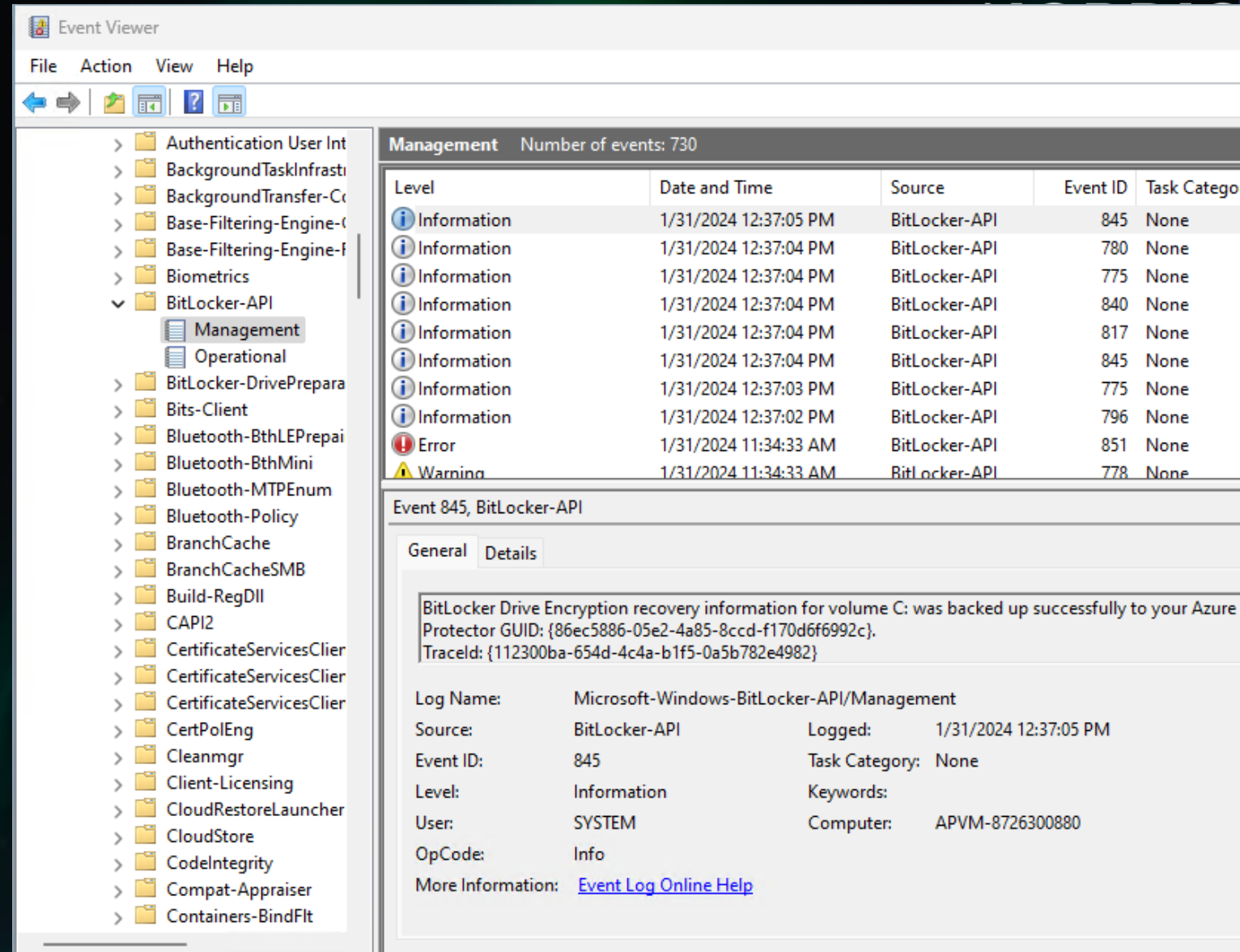
Other settings

Restrict users from recovering the BitLocker key(s) for their owned devices ⓘ

☒ Yes ☐ No

Bitlocker eventlogs

- Application and Service Logs → Microsoft → Windows → Bitlocker-API → Management



The screenshot displays the Windows Event Viewer application. The left-hand pane shows the 'Event Viewer' tree with 'BitLocker-API' expanded, and 'Management' selected. The right-hand pane shows a list of 730 events. The table below represents the data shown in the 'Management' log.

Level	Date and Time	Source	Event ID	Task Category
Information	1/31/2024 12:37:05 PM	BitLocker-API	845	None
Information	1/31/2024 12:37:04 PM	BitLocker-API	780	None
Information	1/31/2024 12:37:04 PM	BitLocker-API	775	None
Information	1/31/2024 12:37:04 PM	BitLocker-API	840	None
Information	1/31/2024 12:37:04 PM	BitLocker-API	817	None
Information	1/31/2024 12:37:04 PM	BitLocker-API	845	None
Information	1/31/2024 12:37:03 PM	BitLocker-API	775	None
Information	1/31/2024 12:37:02 PM	BitLocker-API	796	None
Error	1/31/2024 11:34:33 AM	BitLocker-API	851	None
Warning	1/31/2024 11:34:33 AM	BitLocker-API	778	None

Below the table, the details for 'Event 845, BitLocker-API' are shown. The 'General' tab is active, displaying the following information:

BitLocker Drive Encryption recovery information for volume C: was backed up successfully to your Azure
Protector GUID: {86ec5886-05e2-4a85-8ccd-f170d6f6992c}.
TracId: {112300ba-654d-4c4a-b1f5-0a5b782e4982}

Log Name: Microsoft-Windows-BitLocker-API/Management
Source: BitLocker-API
Event ID: 845
Level: Information
User: SYSTEM
OpCode: Info
More Information: [Event Log Online Help](#)

Bitlocker eventlogs

- Ensure that the Bitlocker startup options are unambiguous

Configure TPM startup key and PIN: *

Allow startup key and PIN with TPM

Configure TPM startup: *

Require TPM

Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)

☐ False

Conflict

Configure TPM startup PIN: *

Require startup PIN with TPM

Configure TPM startup key: *

Do not allow startup key with TPM

> Base-Filtering-Engine-Connections
> Base-Filtering-Engine-Resource-Flo
> Biometrics
▼ BitLocker-API
 Management
 Operational
> BitLocker-DrivePreparationTool
> Bits-Client
> Bluetooth-BthLEPrepairing
> Bluetooth-BthMini
> Bluetooth-MTPEnum
> Bluetooth-Policy
> BranchCache
> BranchCacheSMB
> Build-RegDll
> CAPI

Management Number of events: 698

Level	Date and Time	Source	Event ID	Task Category
Error	1/31/2024 10:06:47 AM	BitLocker-API	851	None
Warning	1/31/2024 10:06:47 AM	BitLocker-API	778	None
Error	1/31/2024 9:13:03 AM	BitLocker-API	853	None
Error	1/31/2024 5:22:53 AM	BitLocker-API	853	None
Error	1/31/2024 5:13:02 AM	BitLocker-API	853	None

Event 851, BitLocker-API

General Details

Failed to enable Silent Encryption.
Error: The Group Policy settings for BitLocker startup options are in conflict and cannot be applied. Contact your system administrator for more information.

Event Properties - Event 851, BitLocker-API

General Details

Failed to enable Silent Encryption.

Error: The Group Policy settings for BitLocker startup options are in conflict and cannot be applied. Contact your system administrator for more information.

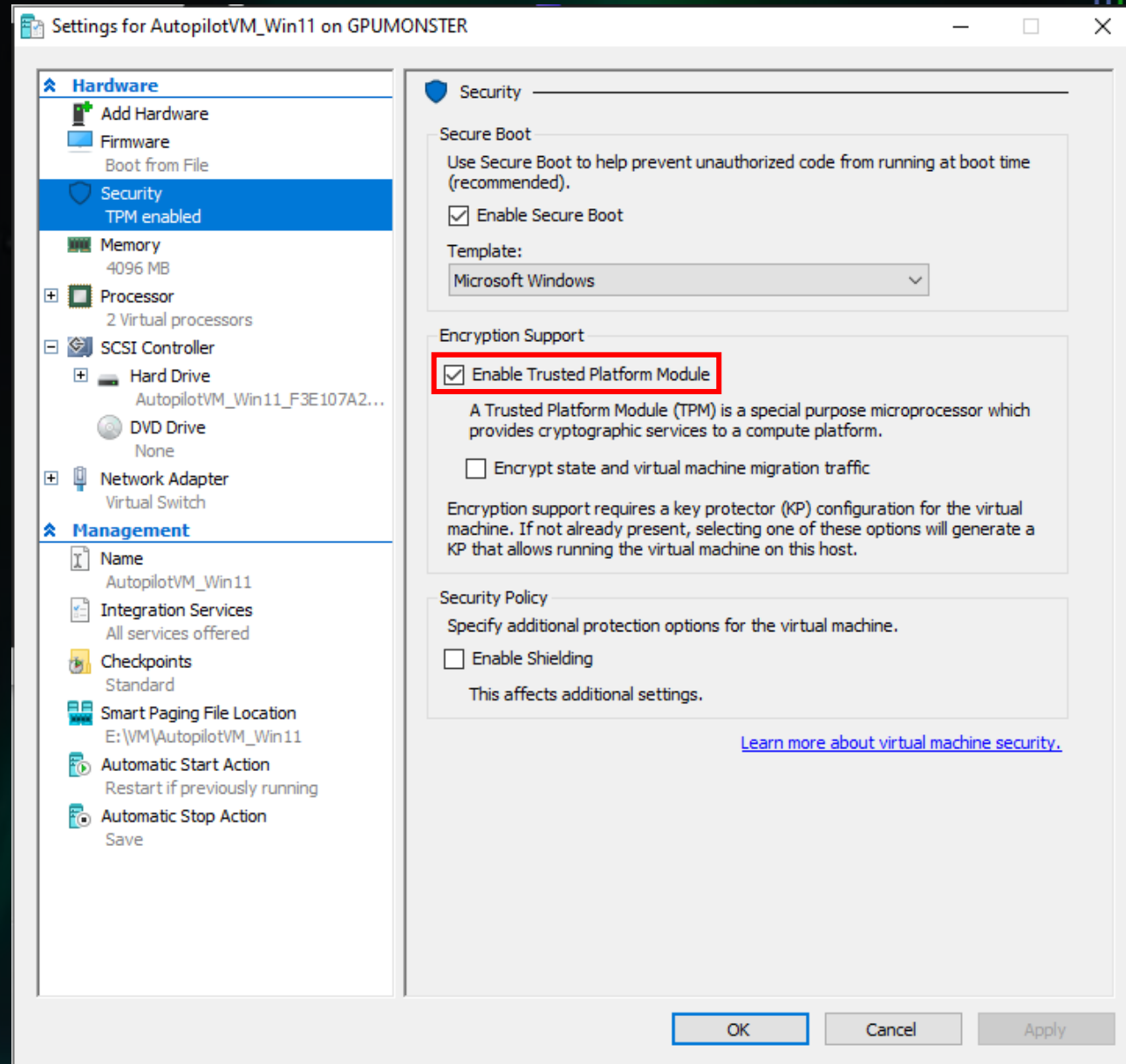
Log Name: Microsoft-Windows-BitLocker-API/Management
Source: BitLocker-API Logged: 1/31/2024 10:06:47 AM
Event ID: 851 Task Category: None
Level: Error Keywords:
User: SYSTEM Computer: APVM-8726300880
OpCode: Info
More Information: [Event Log Online Help](#)

Copy

Close

Bitlocker - Virtual Machines

- Test Bitlocker with Virtual Machines
- Virtual machine Settings
- **Enable Trusted Platform Module**



Bitlocker - Virtual Machines

- You will forget to remove DVD-drive from VM settings to enable Bitlocker silent encryption 😊

The image shows a composite of three screenshots illustrating a common issue with BitLocker encryption in virtual machines.

Top Left: VM Settings (AutopilotVM_Win11 on GPUMONSTER)

- The **Hardware** tab is selected.
- The **DVD Drive** section shows a virtual CD/DVD drive attached to the **SCSI Controller** at **Location: 1 (in use)**.
- The **Media** section has **Image file:** selected, with the path **F:\ISO\windows 11_23H2\SW_DVD9_Win_Pro_11_23H2_64BIT_English_Pro_Er** entered.
- A red arrow points to the **Image file:** radio button, and a large red 'X' is drawn over the entire DVD Drive section, indicating it should be removed.

Top Right: Windows Event Viewer (Management)

Level	Date and Time	Source	Event...	Task Category
Error	1/31/2024 9:13:03 AM	BitLocker-API	853	None
Error	1/31/2024 5:22:53 AM	BitLocker-API	853	None
Error	1/31/2024 5:13:02 AM	BitLocker-API	853	None
Error	1/31/2024 4:37:02 AM	BitLocker-API	853	None
Error	1/31/2024 1:13:03 AM	BitLocker-API	853	None
Error	1/30/2024 9:13:02 PM	BitLocker-API	853	None
Error	1/30/2024 8:37:58 PM	BitLocker-API	853	None
Error	1/30/2024 8:37:02 PM	BitLocker-API	853	None
Error	1/30/2024 6:55:34 PM	BitLocker-API	853	None

Bottom Left: Windows Event Viewer (Details)

Event 853, BitLocker-API

Failed to enable Silent Encryption. TPM is not available.

Error: BitLocker Drive Encryption detected bootable media (CD or DVD) in the computer. Remove the media and restart the computer before configuring BitLocker..

Log Name: Microsoft-Windows-BitLocker-API/Management
Source: BitLocker-API
Event ID: 853
Level: Error
User: SYSTEM
OpCode: Info
More Information: [Event Log Online Help](#)

Bottom Right: Event Properties - Event 853, BitLocker-API

General Details

Failed to enable Silent Encryption. TPM is not available.

Error: BitLocker Drive Encryption detected bootable media (CD or DVD) in the computer. Remove the media and restart the computer before configuring BitLocker..

Log Name: Microsoft-Windows-BitLocker-API/Management
Source: BitLocker-API
Event ID: 853
Level: Error
User: SYSTEM
OpCode: Info
More Information: [Event Log Online Help](#)

Logged: 1/31/2024 9:13:03 AM
Task Category: None
Keywords: None
Computer: APVM-8726300880

Administrative units

Limit permissions to subset of users/group/devices e.g. BitLocker recovery keys

Identity

Overview

Users

Groups

Devices

Overview

All devices

BitLocker keys

Applications

Roles & admins

Roles & admins

Admin units

Delegated admin partners

Administrative units

Learn more

+ Add

🗑 Delete

🔄 Refresh

🔍 Preview features

🗨 Got feedback?

🔍 Search administrative units

+ Add filters

Name	Description	Restricted management	Membership type
<input type="checkbox"/> Hi-sec workstations		Yes	Assigned
<input type="checkbox"/> Kiosk devices		No	Dynamic

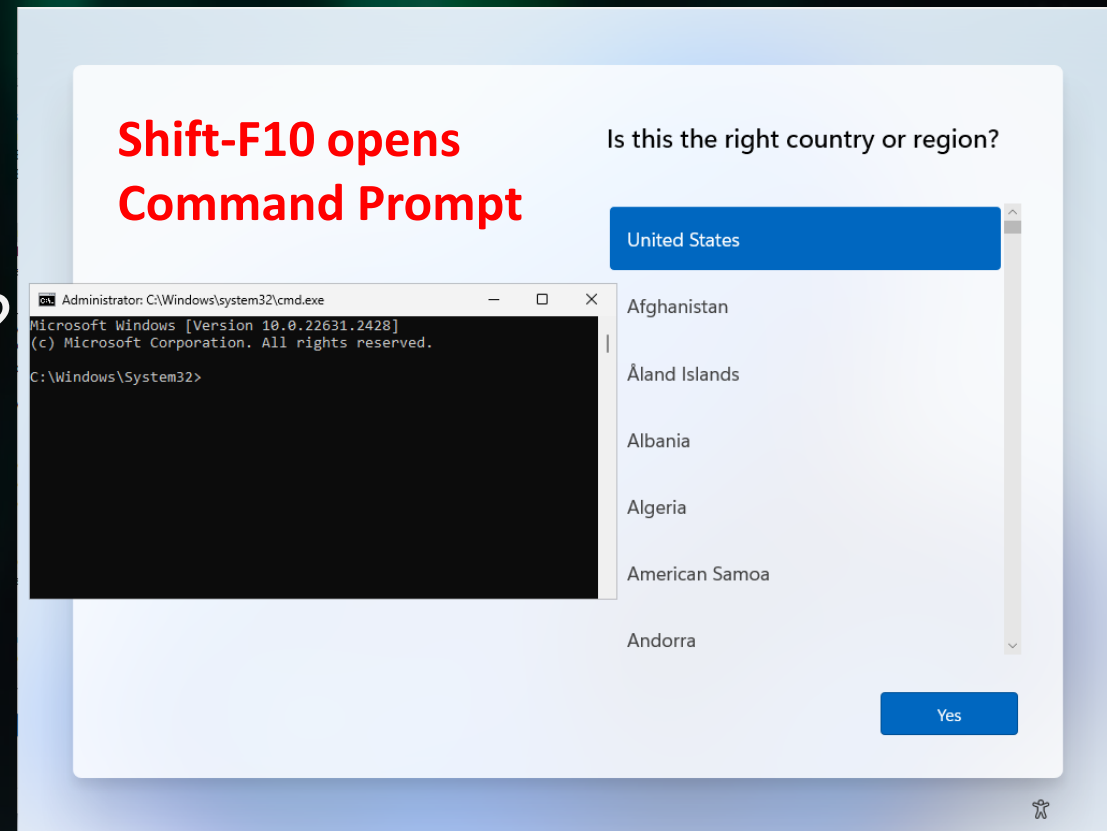
Work in progress...

Autopilot

Disable Shift-F10 Command Prompt in OOB/E and
in Enrollment Status Page

Autopilot

- By default anyone who can access the device during the OOB and Autopilot process can get local admin rights to the device
 - Shift-F10 (opens a command prompt with admin rights)
- How to disable Shift-F10?
 - Need to add the following file:
`C:\windows\setup\scripts\DisableCMDRequest.tag`
- How to add the file to the new devices?
 - Autopilot Pre-Provisioning
 - Custom image
- •How about wipe?
 - <https://call4cloud.nl/2022/01/the-oobe-massacre-the-beginning-of-shift-f10/>
 - <https://call4cloud.nl/2022/03/2022-03-update-the-search-for-sp-uhh-shiftf10/>



Intune deployments

Assume nothing is kept secret

Intune deployments

- Be aware of sensitive/secrets within
 - **Win32 app installation commands**
 - **Powershell scripts**
 - Remediation scripts ???
- Normal user can read Intune log files where the data is available
 - C:\ProgramData\Microsoft\IntuneManagementExtension\Logs
 - IntuneManagementExtension.log
 - AgentExecutor.log
- Intune rights
 - Who can create scripts/remediations/apps can run anything with system rights

DEMO

Intune log files secrets

Tools used in demo:

<https://github.com/petripaavola/Get-IntuneManagementExtensionDiagnostics>

<https://github.com/petripaavola/ClipboardTools>

Check also the following topics

- Windows Hello for Business
 - Check passwordless session: Passwordless; No One Wants To Go Back by Jóhannes Geir Kristjánsson & Martin Himken
- Microsoft Defender for Endpoint
 - Check session: Managing Your Risk of Vulnerabilities with MDE by Jörgen Nilsson & Stefan Schörling
- Firewall (on by default on Windows)
- Antivirus (on by default on Windows)
- Attack Surface Reduction rules
- Security baselines
- ConfigRefresh
- Query local admin group membership with PowerShell [issues](#)

Summary

- Control who has admin rights to your cloud devices
 - Active Directory & Entra ID behave similarly (Domain Admins vs Global admins)
- Windows LAPS is easy to implement. Highly recommended!
- Implement Bitlocker on your devices
 - Can end users see recovery keys?
- Think who has access to admin passwords/Bitlocker keys
 - Entra ID permissions!
 - Administrative units?
- Use remediations instead of PowerShell scripts
- Note potential secrets within apps/scripts