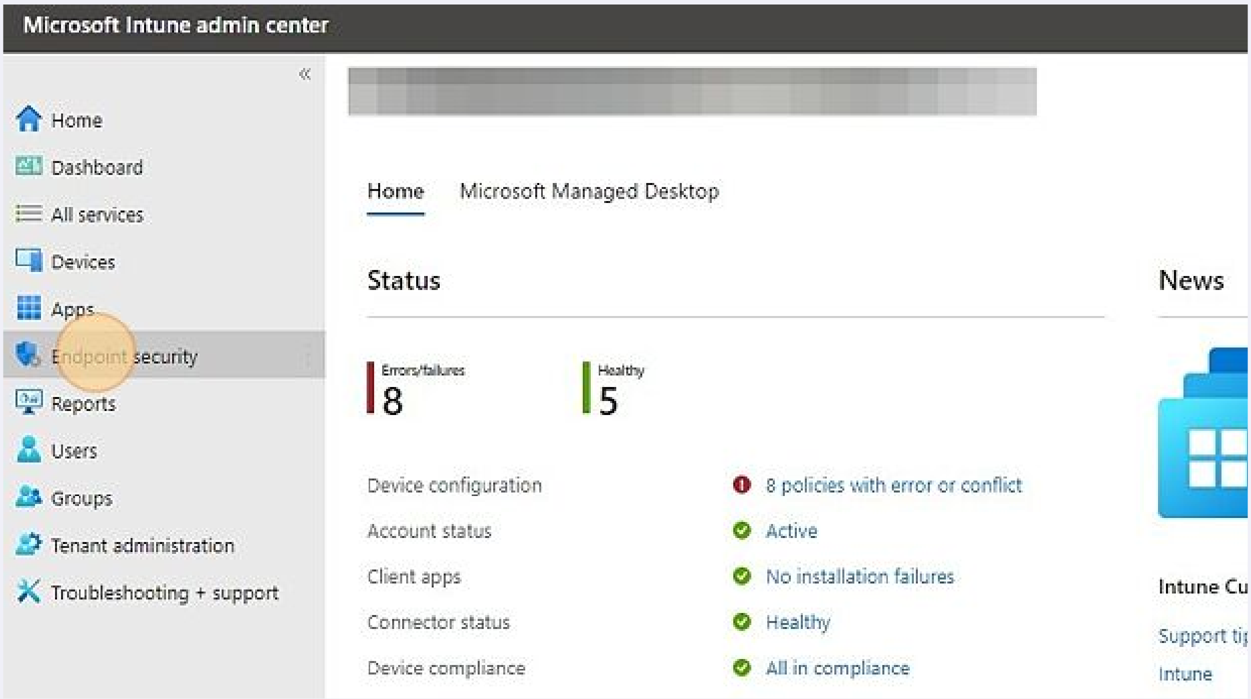
How to Create BitLocker Encryption Profile for Windows in Microsoft Endpoint Manager

petri.com/best-practices-for-deploying-bitlocke...

1 Navigate to endpoint.microsoft.com

2 Click "Endpoint security"



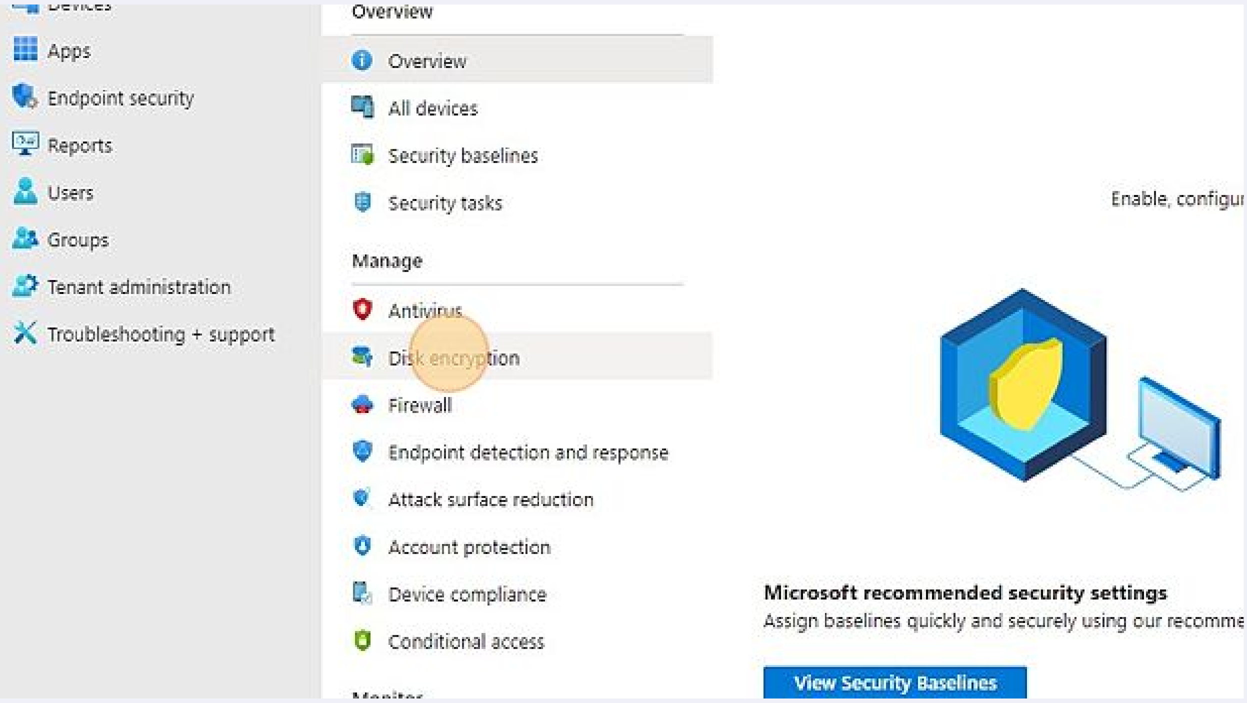
[redacted]

Errors/failures 8

Healthy 5

Device configuration	8 policies with error or conflict
Account status	Active
Client apps	No installation failures
Connector status	Healthy
Device compliance	All in compliance

3 Click "Disk encryption"



Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

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

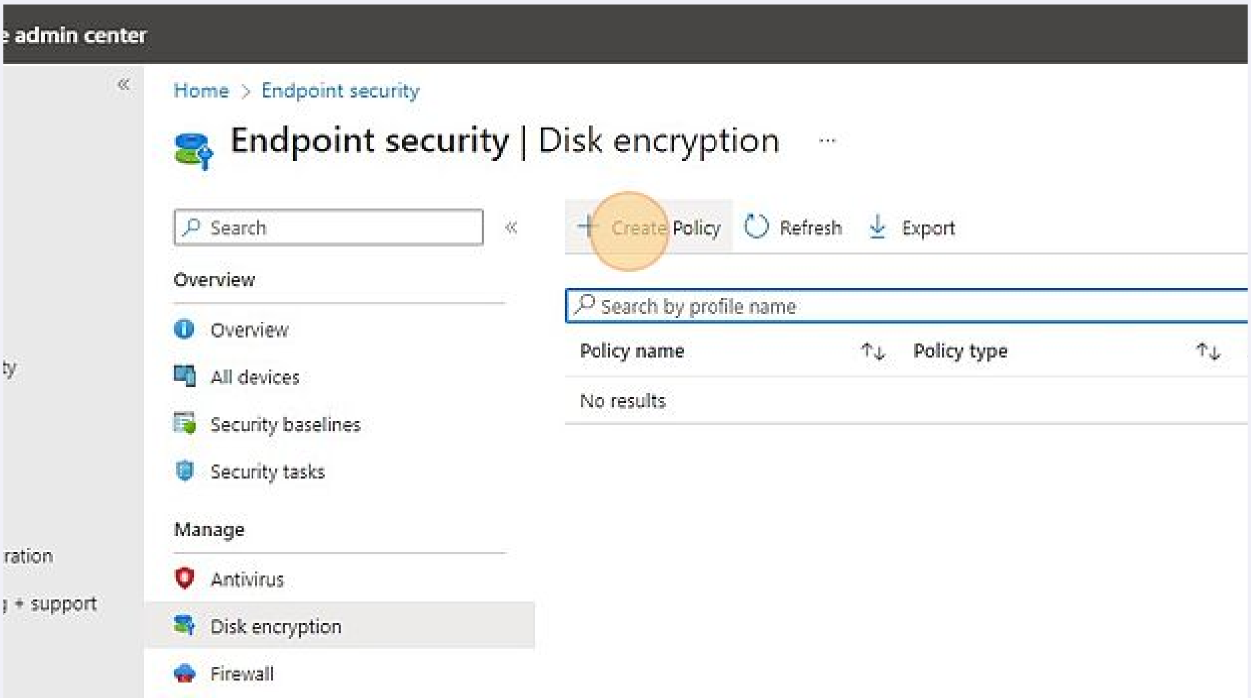
Monitor

Enable, configur

Microsoft recommended security settings
Assign baselines quickly and securely using our recomme

View Security Baselines

4 Click "Create Policy"



admin center

Home > Endpoint security

Endpoint security | Disk encryption ···

Search

Overview
Overview
All devices
Security baselines
Security tasks

Manage
Antivirus
Disk encryption
Firewall

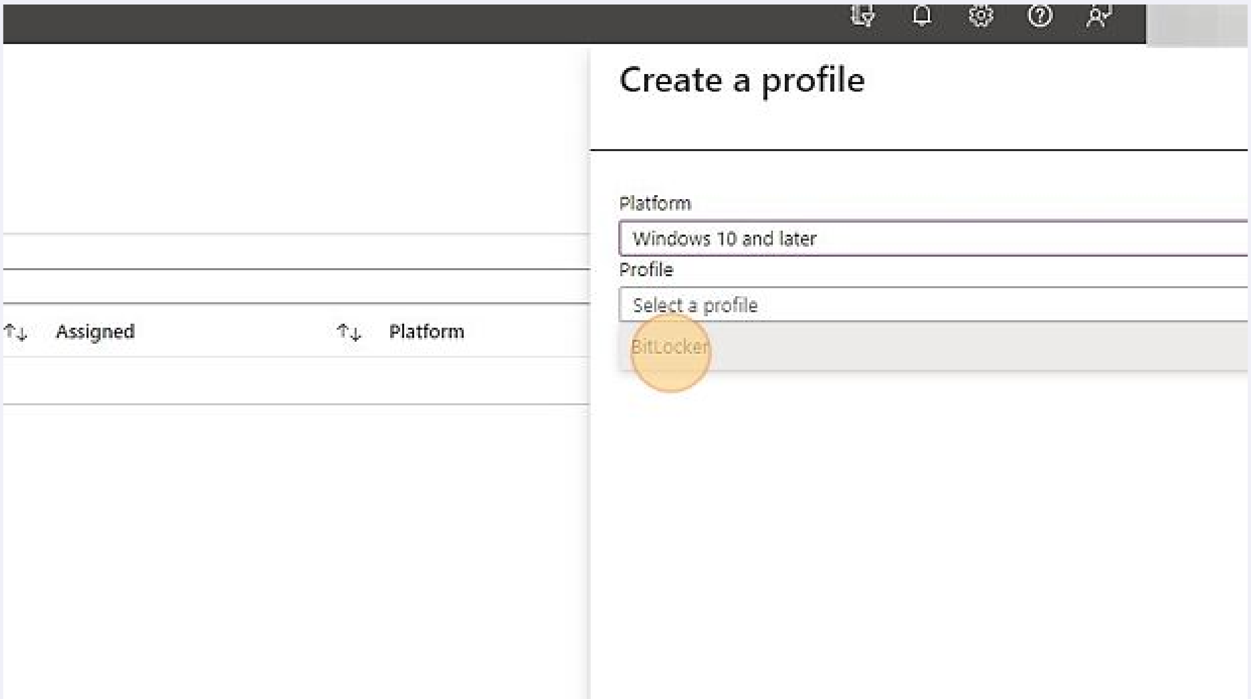
ty
ration
+ support

+ Create Policy   Refresh   Export

Search by profile name

Policy name ↑↓	Policy type ↑↓
No results	

5 Platform: Windows 10
Profile: BitLocker

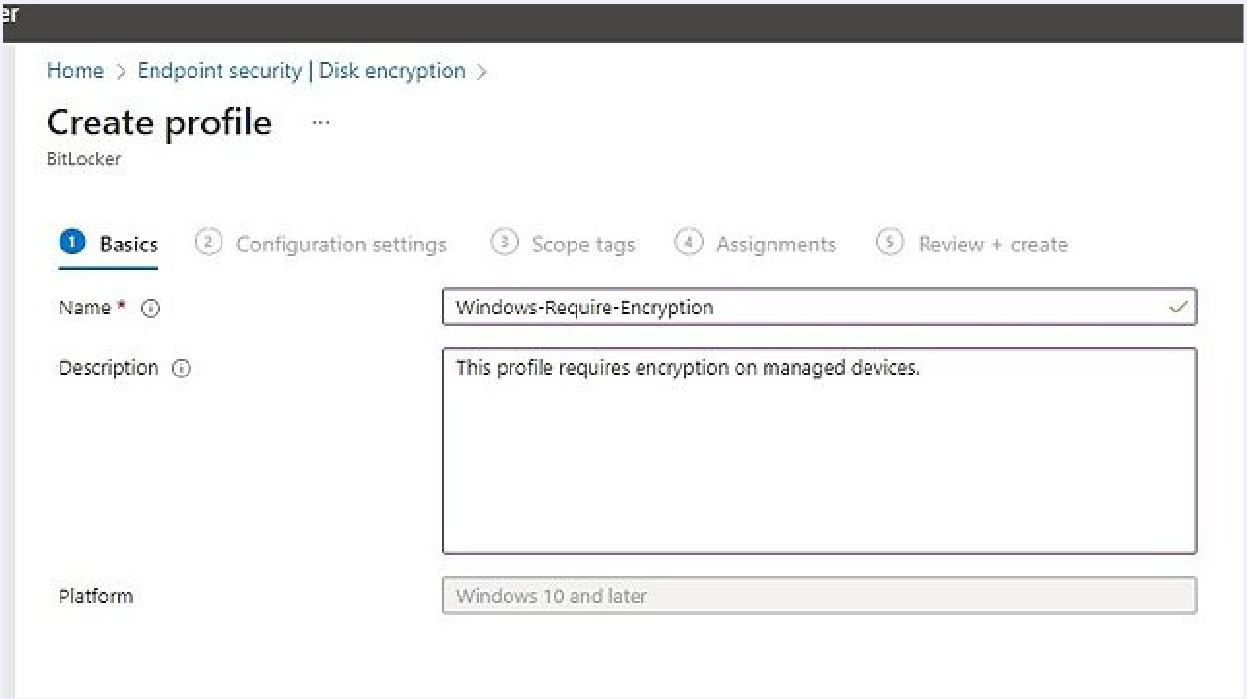


Create a profile

Platform: Windows 10 and later

Profile: Select a profile

6 Create Profile:
Name: Windows-Require-Encryption
Description: This profile requires encryption on managed devices.



Home > Endpoint security | Disk encryption >

Create profile

BitLocker

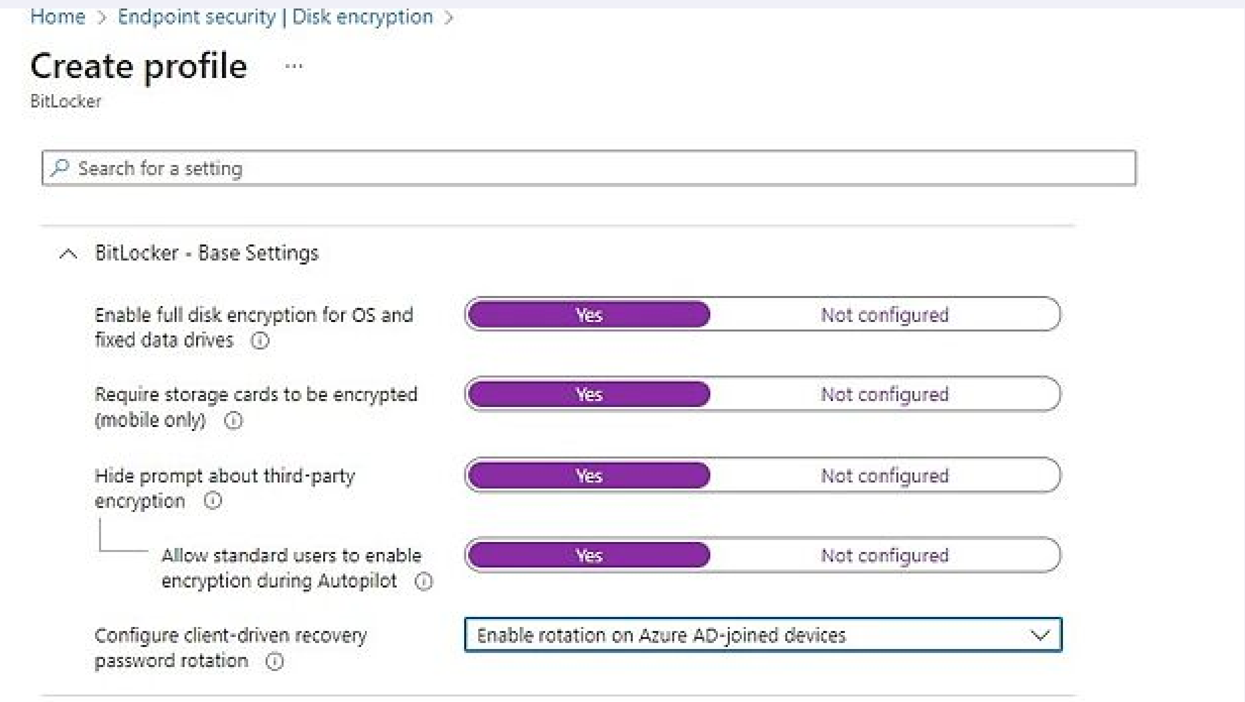
Name * : Windows-Require-Encryption

Description: This profile requires encryption on managed devices.

Platform: Windows 10 and later

7

BitLocker - Base Settings
- Enable full disk encryption for OS and fixed data drive = Yes
- Require storage cards to be encrypted = Yes
-Hide prompt about third-party encryption = Yes
-Allow standard users to enable encryption during Autopilot = Yes
-Configure client driven recovery password rotation = Azure AD Devices



Home > Endpoint security | Disk encryption >

Create profile ...

BitLocker

Search for a setting

BitLocker - Base Settings

Enable full disk encryption for OS and fixed data drives: Yes

Require storage cards to be encrypted (mobile only): Yes

Hide prompt about third-party encryption: Yes

Allow standard users to enable encryption during Autopilot: Yes

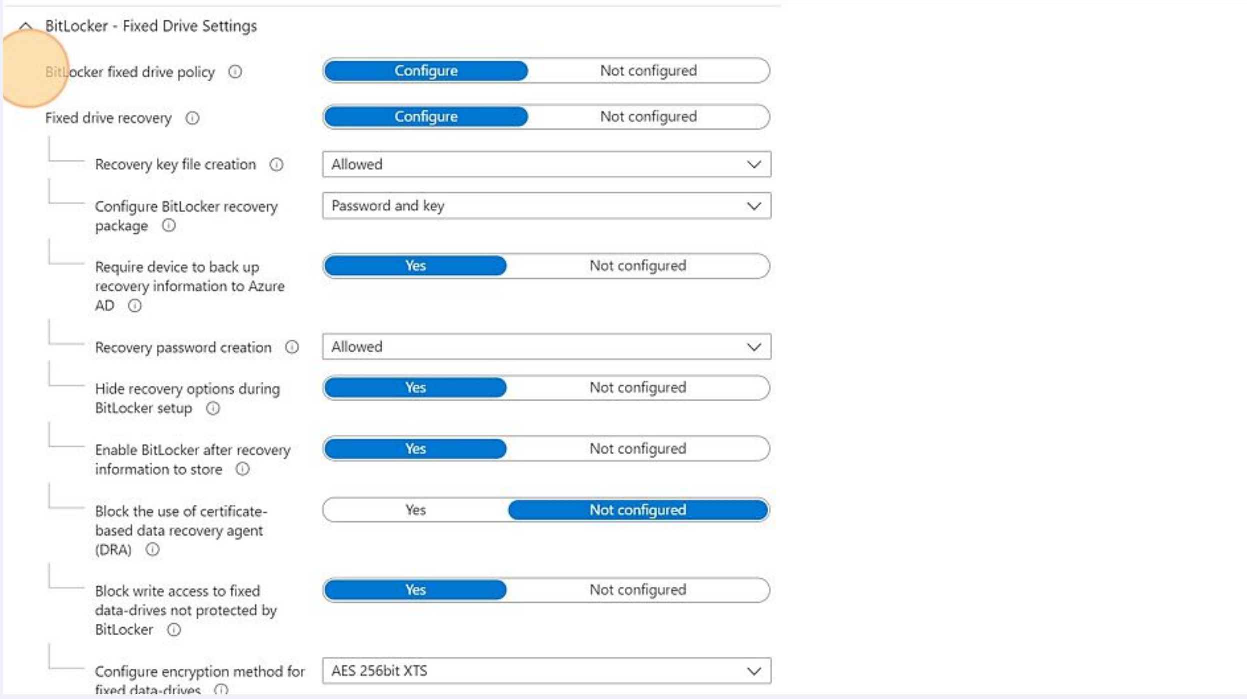
Configure client-driven recovery password rotation: Enable rotation on Azure AD-joined devices

!

Hiding prompts is a pre-requisite to silent encryption
Allowing standard users to enable encryption is required for Autopilot
Password rotation changes the keys each time they are used

8

BotLocker Fixed Drive Settings:
- BitLocker Fixed Drive Policy = Configured
- Fixed Drive Recovery = Configured
-Recovery Key File Creation = Allowed
- Configure BitLocker Recovery Package = Password and Key
- Require device to back up recovery information to Azure AD = Yes
- Recovery Password Creation = Yes
-Hide Recovery Options During BitLocker Setup = Yes
-Enable BitLocker After Recovery Information to Store = Yes
-Block the Use of Certificates = Not Configured
- Block Write Access to Fixed Data Drive Not Protected = Yes
-Configure Encryption Method = AES 256bit XTS



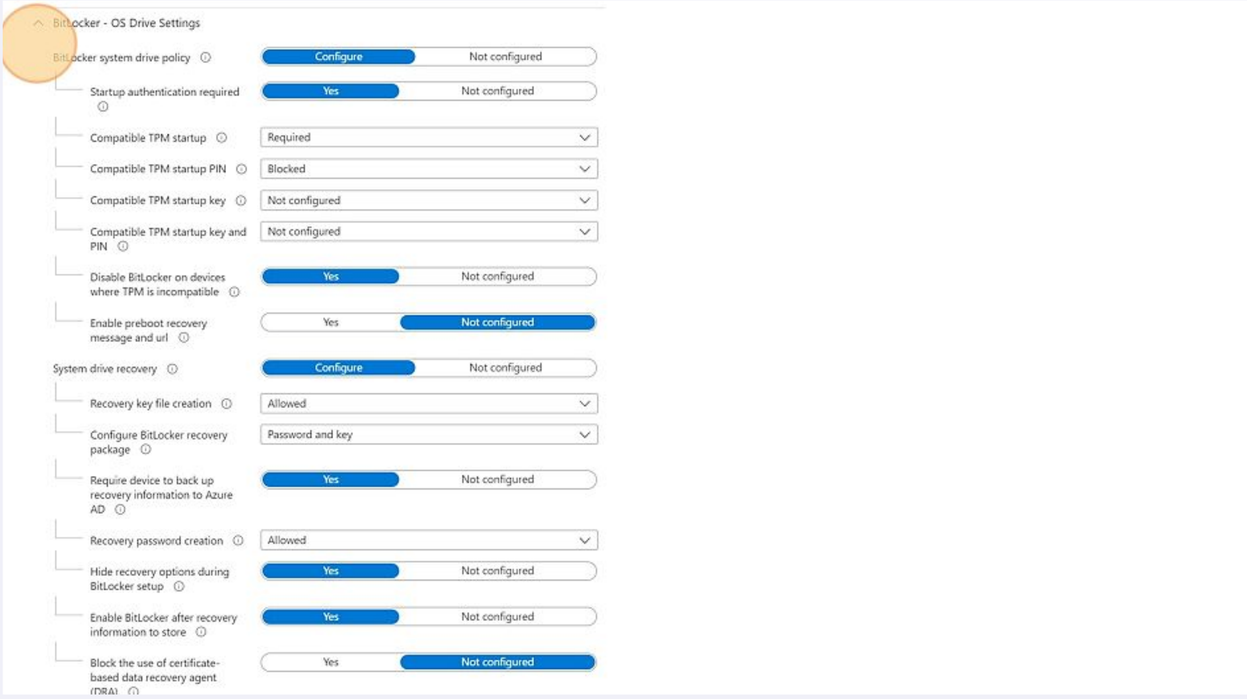
BitLocker - Fixed Drive Settings

BitLocker fixed drive policy ⓘ	**Configure** / Not configured
Fixed drive recovery ⓘ	**Configure** / Not configured
Recovery key file creation ⓘ	Allowed
Configure BitLocker recovery package ⓘ	Password and key
Require device to back up recovery information to Azure AD ⓘ	**Yes** / Not configured
Recovery password creation ⓘ	Allowed
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**
Block write access to fixed data-drives not protected by BitLocker ⓘ	**Yes** / Not configured
Configure encryption method for fixed data-drives ⓘ	AES 256bit XTS

These settings support silent encryption
Keys are safeguarded in Azure AD
Blocks writing to unencrypted storage

9

BitLocker OS Drive Settings:
- BitLocker System Drive Policy = Configure
-Startup Authentication Required = Yes
- Compatible TPM startup = Required
- Compatible TPM startup PIN = Not Configured
- Compatible TPM startup key = Not Configured
- Compatible TPM startup key and PIN = Not Configured
- Disable BitLocker on devices Where TPM is Incompatible = Yes
-Enable Preboot Message and URL = Not Configured
-System Drive Recovery = Configure
- Recovery Key File Creation = Allowed
- Configure BitLocker Recovery Package = Password and Key
-Require Device to Backup to Azure AD = Yes
-Recovery Password Creation = Allowed
-Hide Recovery Options During BitLocker Setup = Yes
-Enable BitLocker After Recovery Information Store = Yes
-Block the Use of Certificates = Not Configured
-Minimum PIN Length = 8
-Configure Encryption Method = AES 256bit XTS

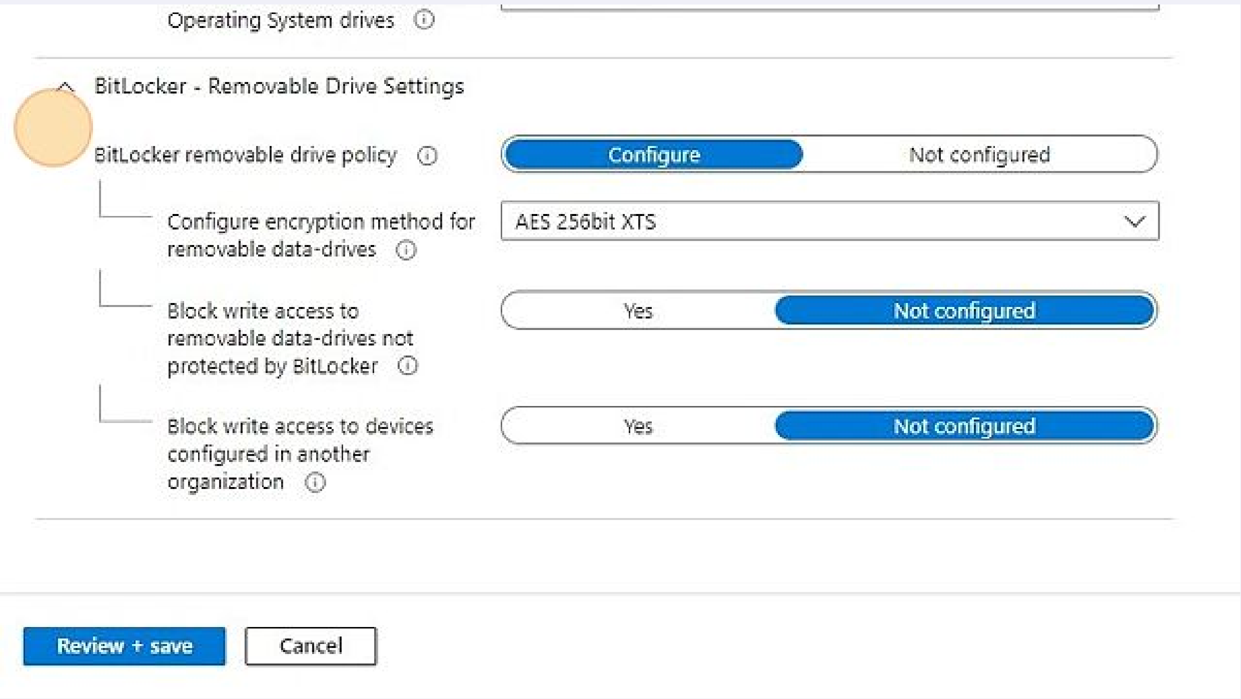


BitLocker - OS Drive Settings

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 ⓘ	Not configured
Compatible TPM startup key and PIN ⓘ	Not configured
Disable BitLocker on devices where TPM is incompatible ⓘ	[✓ Yes] Not configured
Enable preboot recovery message and url ⓘ	Yes [✓ Not configured]
System drive recovery ⓘ	[✓ Configure] Not configured
Recovery key file creation ⓘ	Allowed
Configure BitLocker recovery package ⓘ	Password and key
Require device to back up recovery information to Azure AD ⓘ	[✓ Yes] Not configured
Recovery password creation ⓘ	Allowed
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]

Keys are stored on the TPM
TPM supports silent encryption
Non TPM devices are excluded

10 BitLocker - Removable Drive Settings:
-BitLocker Removable Drive Policy = Configure
-Configure Encryption Method = AES 256bit XTS
-Block Write Access to Non-Encrypted Drives = Not Configured
-Block Write Access to Devices Configured in Another Org = Not Configured



Operating System drives ⓘ

BitLocker - Removable Drive Settings

BitLocker removable drive policy ⓘ — [✓ Configure] Not configured

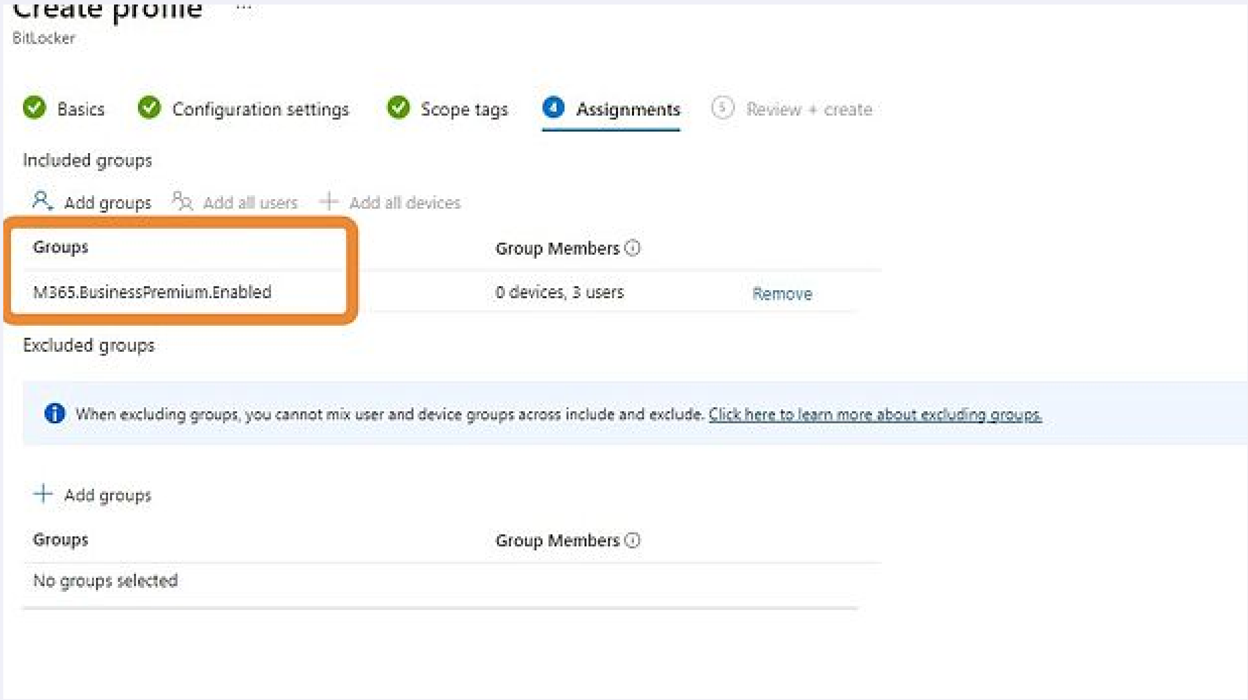
Configure encryption method for removable data-drives ⓘ — AES 256bit XTS

Block write access to removable data-drives not protected by BitLocker ⓘ — Yes [✓ Not configured]

Block write access to devices configured in another organization ⓘ — Yes [✓ Not configured]

This allows the option for encryption using the set method only
It does not block other removable drives

11 Target the required groups



Create profile ...

BitLocker

Included groups

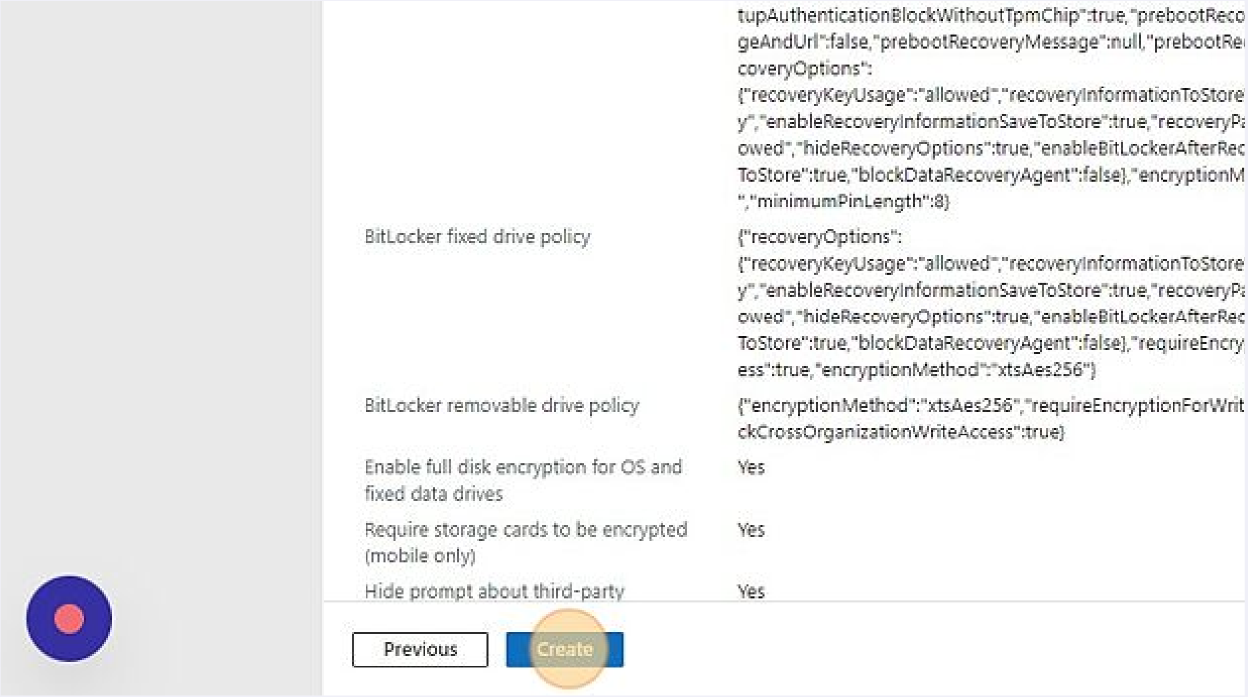
Groups	Group Members ⓘ	
M365.BusinessPremium.Enabled	0 devices, 3 users	Remove

Excluded groups

ⓘ When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about excluding groups.

Groups	Group Members ⓘ
No groups selected	

12 Click "Create"



	tupAuthenticationBlockWithoutTpmChip":true,"prebootReco geAndUrl":false,"prebootRecoveryMessage":null,"prebootRe coveryOptions": {"recoveryKeyUsage":"allowed","recoveryInformationToStore y","enableRecoveryInformationSaveToStore":true,"recoveryP owed","hideRecoveryOptions":true,"enableBitLockerAfterRec ToStore":true,"blockDataRecoveryAgent":false},"encryptionM ","minimumPinLength":8}
BitLocker fixed drive policy	{"recoveryOptions": {"recoveryKeyUsage":"allowed","recoveryInformationToStore y","enableRecoveryInformationSaveToStore":true,"recoveryP owed","hideRecoveryOptions":true,"enableBitLockerAfterRec ToStore":true,"blockDataRecoveryAgent":false},"requireEncry ess":true,"encryptionMethod":"xtsAes256"}
BitLocker removable drive policy	{"encryptionMethod":"xtsAes256","requireEncryptionForWrit ckCrossOrganizationWriteAccess":true}
Enable full disk encryption for OS and fixed data drives	Yes
Require storage cards to be encrypted (mobile only)	Yes
Hide prompt about third-party	Yes