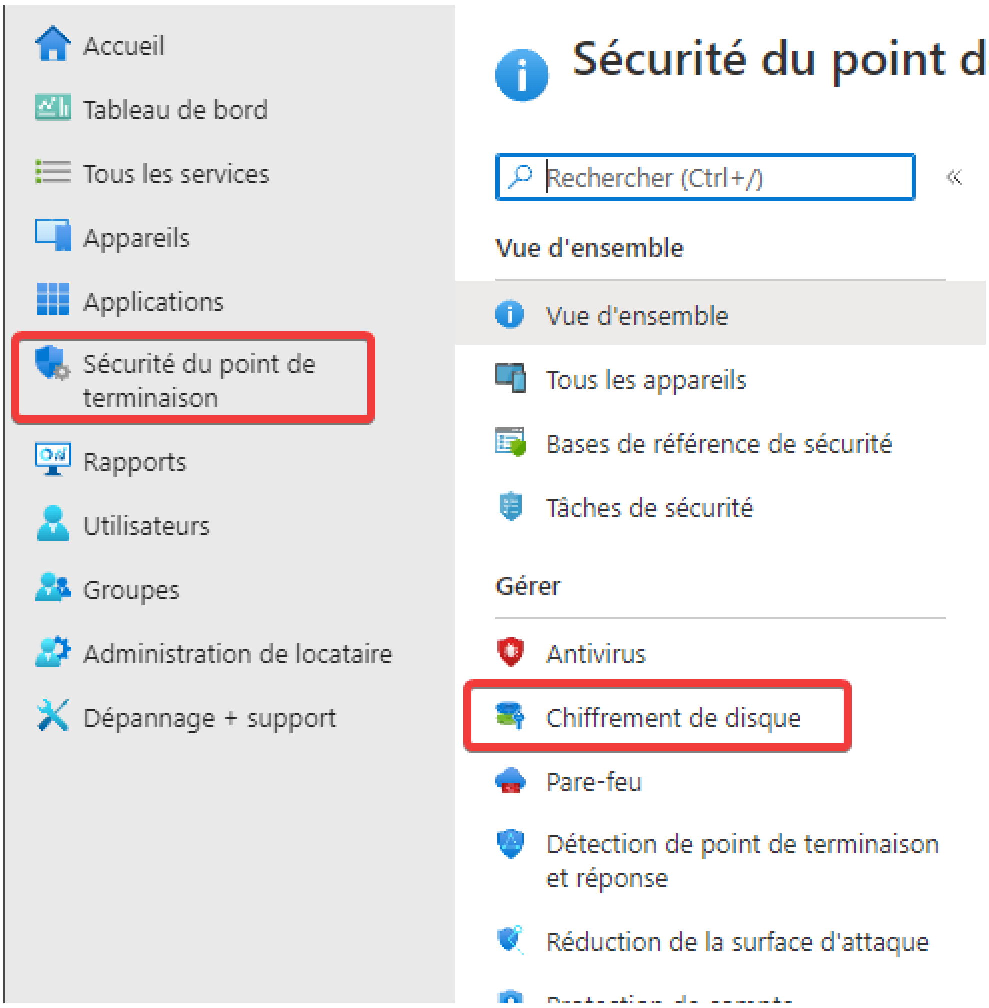
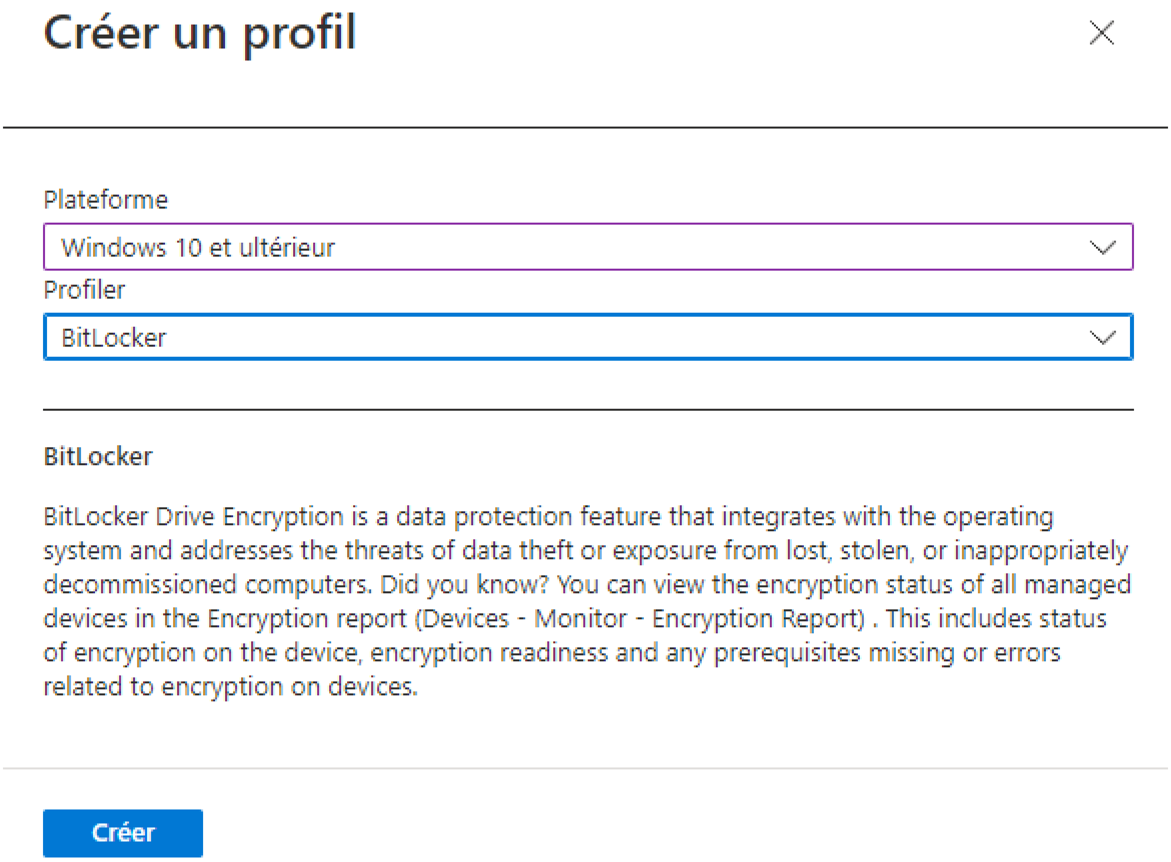
Configurer et déployer BitLocker via Intune

On se rend dans l'onglet "Sécurité du point de terminaison" et "Chiffrement du disque".



On crée une nouvelle stratégie.



Créer un profil

Plateforme

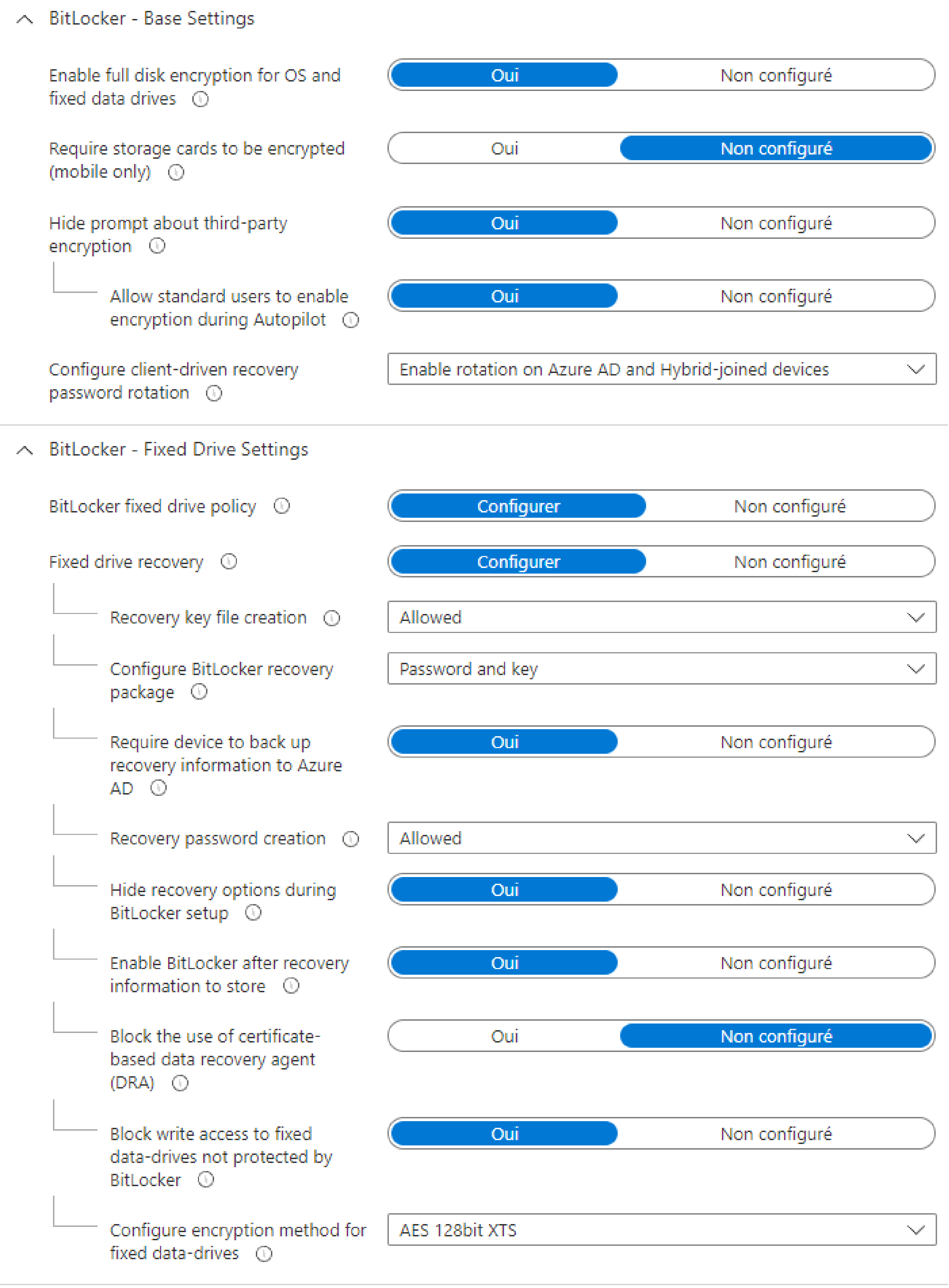
Windows 10 et ultérieur

Profiler

BitLocker

BitLocker

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



BitLocker - Base Settings

Enable full disk encryption for OS and fixed data drives: [✓ Oui] Non configuré

Require storage cards to be encrypted (mobile only): Oui [✓ Non configuré]

Hide prompt about third-party encryption: [✓ Oui] Non configuré

- Allow standard users to enable encryption during Autopilot: [✓ Oui] Non configuré

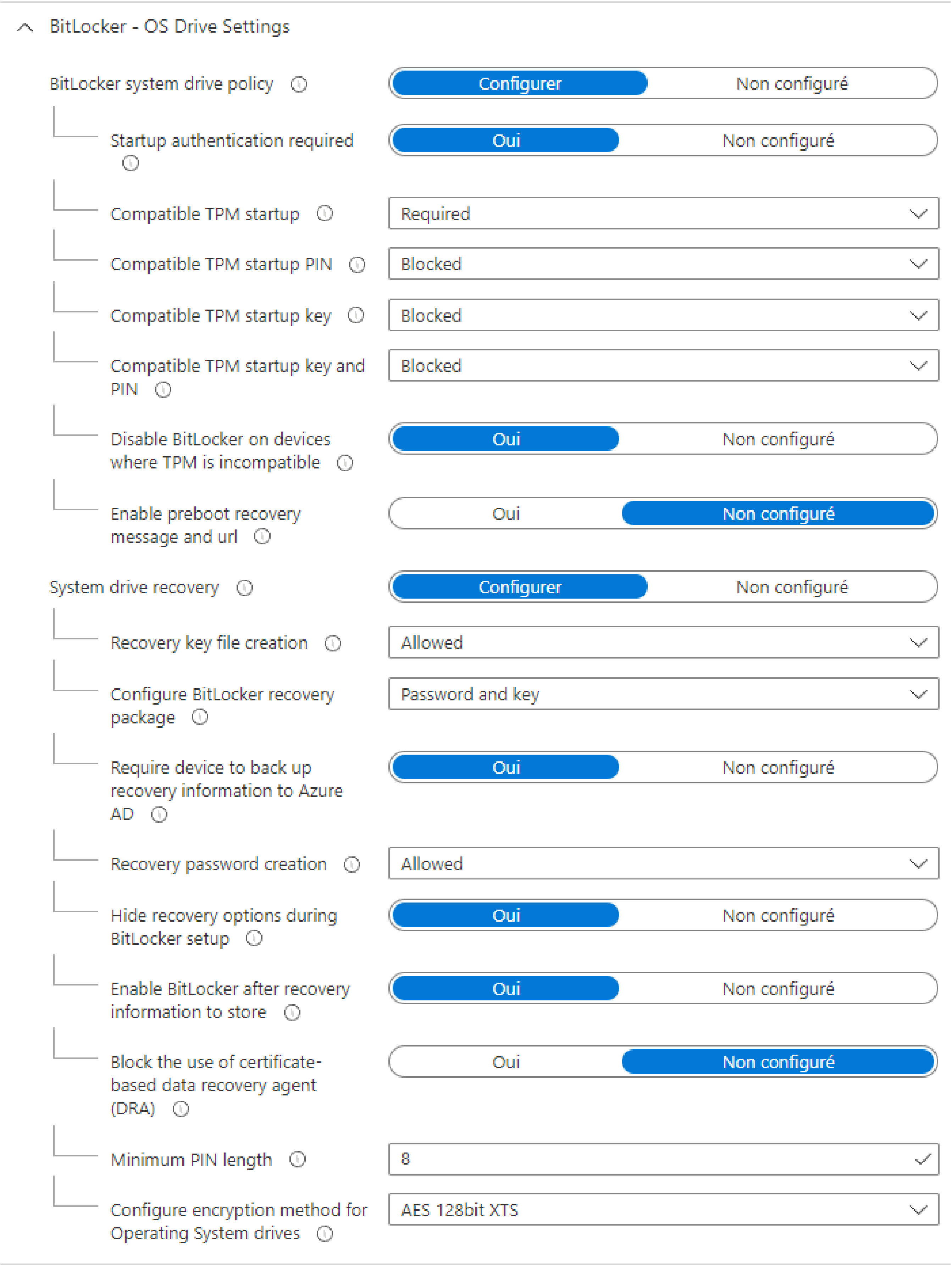
Configure client-driven recovery password rotation: Enable rotation on Azure AD and Hybrid-joined devices

BitLocker - Fixed Drive Settings

BitLocker fixed drive policy: [✓ Configurer] Non configuré

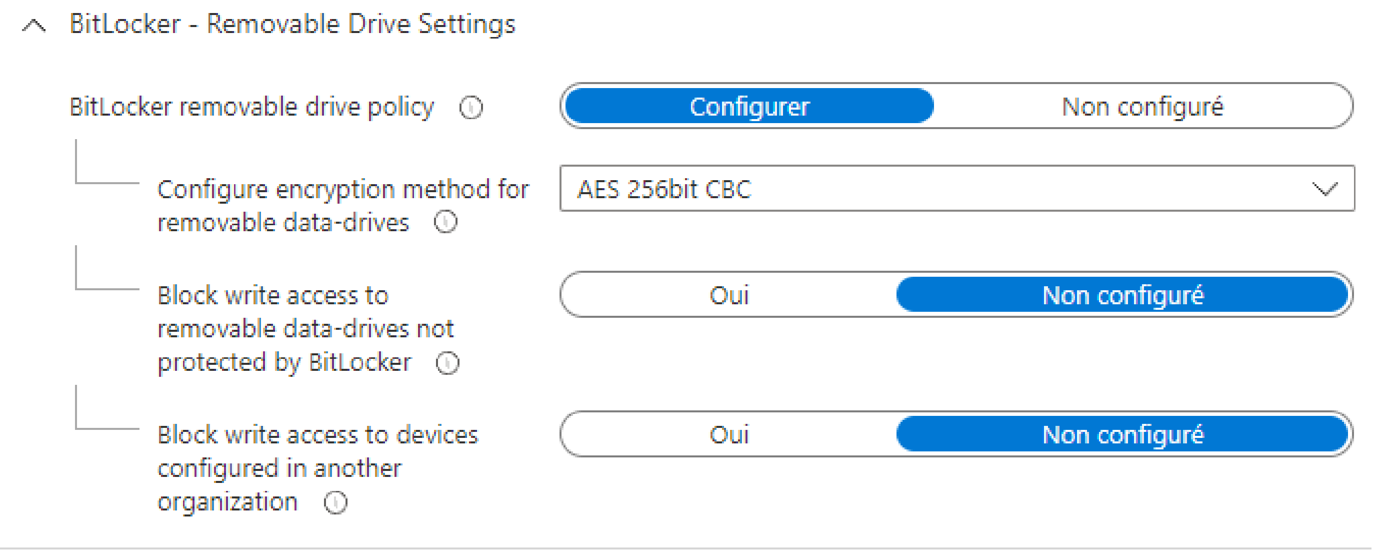
Fixed drive recovery: [✓ Configurer] Non configuré

- Recovery key file creation: Allowed
- Configure BitLocker recovery package: Password and key
- Require device to back up recovery information to Azure AD: [✓ Oui] Non configuré
- Recovery password creation: Allowed
- Hide recovery options during BitLocker setup: [✓ Oui] Non configuré
- Enable BitLocker after recovery information to store: [✓ Oui] Non configuré
- Block the use of certificate-based data recovery agent (DRA): Oui [✓ Non configuré]
- Block write access to fixed data-drives not protected by BitLocker: [✓ Oui] Non configuré
- Configure encryption method for fixed data-drives: AES 128bit XTS



BitLocker - OS Drive Settings

BitLocker system drive policy ⓘ	[✓ Configurer] Non configuré
Startup authentication required ⓘ	[✓ Oui] Non configuré
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 ⓘ	[✓ Oui] Non configuré
Enable preboot recovery message and url ⓘ	Oui [✓ Non configuré]
System drive recovery ⓘ	[✓ Configurer] Non configuré
Recovery key file creation ⓘ	Allowed
Configure BitLocker recovery package ⓘ	Password and key
Require device to back up recovery information to Azure AD ⓘ	[✓ Oui] Non configuré
Recovery password creation ⓘ	Allowed
Hide recovery options during BitLocker setup ⓘ	[✓ Oui] Non configuré
Enable BitLocker after recovery information to store ⓘ	[✓ Oui] Non configuré
Block the use of certificate-based data recovery agent (DRA) ⓘ	Oui [✓ Non configuré]
Minimum PIN length ⓘ	8
Configure encryption method for Operating System drives ⓘ	AES 128bit XTS



BitLocker - Removable Drive Settings

BitLocker removable drive policy ⓘ — [✓ Configurer] Non configuré

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

Block write access to removable data-drives not protected by BitLocker ⓘ — Oui [✓ Non configuré]

Block write access to devices configured in another organization ⓘ — Oui [✓ Non configuré]

Revision #1
Created 10 June 2022 21:03:20 by Khroners
Updated 10 June 2022 21:07:30 by Khroners