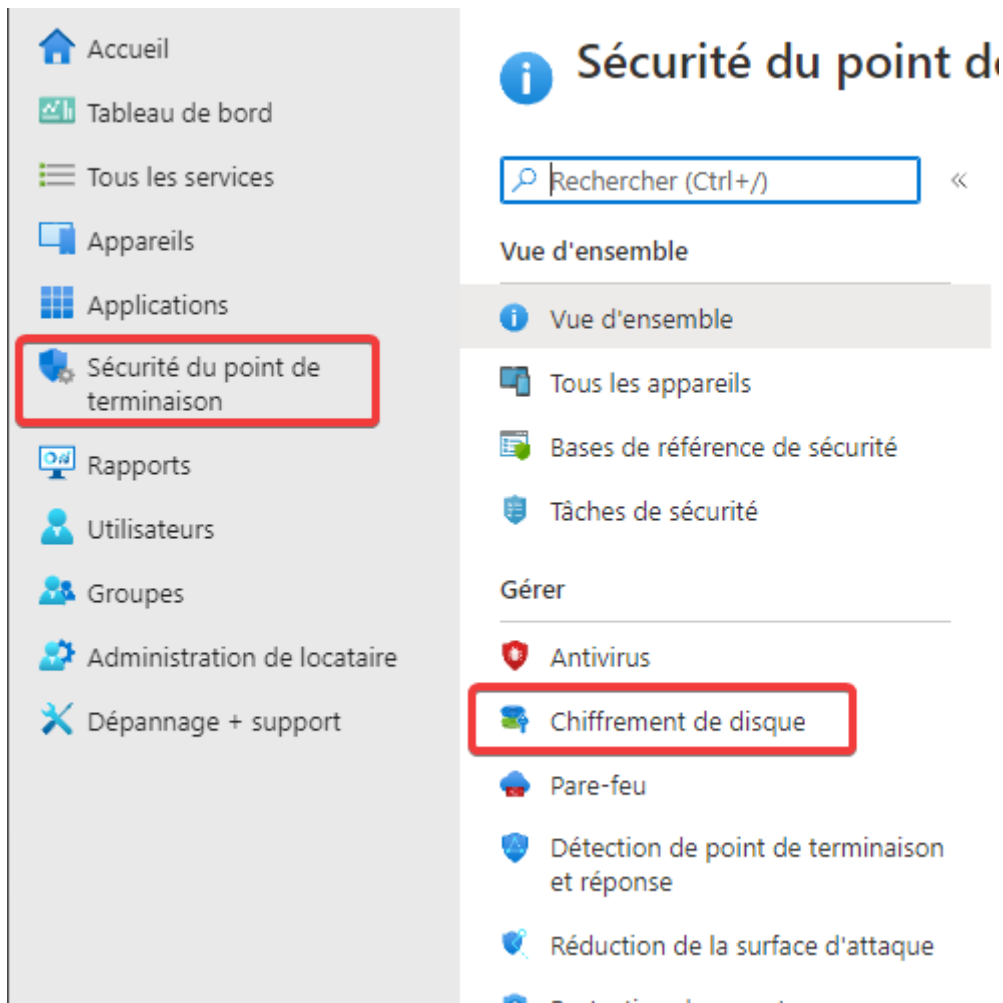


Configurer et déployer BitLocker via Intune

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



On crée une nouvelle stratégie.

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.

Créer

^ 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 ⓘ	<div>Configurer</div> <div>Non configuré</div>
Startup authentication required ⓘ	<div>Oui</div> <div>Non configuré</div>
Compatible TPM startup ⓘ	<div>Required</div> <div>▼</div>
Compatible TPM startup PIN ⓘ	<div>Blocked</div> <div>▼</div>
Compatible TPM startup key ⓘ	<div>Blocked</div> <div>▼</div>
Compatible TPM startup key and PIN ⓘ	<div>Blocked</div> <div>▼</div>
Disable BitLocker on devices where TPM is incompatible ⓘ	<div>Oui</div> <div>Non configuré</div>
Enable preboot recovery message and url ⓘ	<div>Oui</div> <div>Non configuré</div>
System drive recovery ⓘ	<div>Configurer</div> <div>Non configuré</div>
Recovery key file creation ⓘ	<div>Allowed</div> <div>▼</div>
Configure BitLocker recovery package ⓘ	<div>Password and key</div> <div>▼</div>
Require device to back up recovery information to Azure AD ⓘ	<div>Oui</div> <div>Non configuré</div>
Recovery password creation ⓘ	<div>Allowed</div> <div>▼</div>
Hide recovery options during BitLocker setup ⓘ	<div>Oui</div> <div>Non configuré</div>
Enable BitLocker after recovery information to store ⓘ	<div>Oui</div> <div>Non configuré</div>
Block the use of certificate-based data recovery agent (DRA) ⓘ	<div>Oui</div> <div>Non configuré</div>
Minimum PIN length ⓘ	<div>8</div> <div>✓</div>
Configure encryption method for Operating System drives ⓘ	<div>AES 128bit XTS</div> <div>▼</div>

^ 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