

Configurer et déployer BitLocker via Intune

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

The screenshot shows the Microsoft Intune dashboard. On the left, a sidebar lists various management categories: Accueil, Tableau de bord, Tous les services, Appareils, Applications, Sécurité du point de terminaison (which is highlighted with a red box), Rapports, Utilisateurs, Groupes, Administration de locataire, and Dépannage + support. The main content area is titled "Sécurité du point de terminaison". It features a search bar labeled "Rechercher (Ctrl+ /)" and a back arrow. Below the search bar, there are two main sections: "Vue d'ensemble" (which is also highlighted with a red box) and "Gérer". Under "Vue d'ensemble", there are links to "Tous les appareils", "Bases de référence de sécurité", and "Tâches de sécurité". Under "Gérer", there are links to "Antivirus", "Chiffrement de disque" (which is highlighted with a red box), "Pare-feu", "Détection de point de terminaison et réponse", "Réduction de la surface d'attaque", and "Désactivation de l'antivirus".

On crée une nouvelle stratégie.

Créer un profil

X

Plateforme

Windows 10 et ultérieur



Profil

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

↖ BitLocker - Removable Drive Settings

BitLocker removable drive policy	<input type="radio"/> Configurer	<input type="radio"/> Non configuré
Configure encryption method for removable data-drives	<input type="radio"/> AES 256bit CBC	<input checked="" type="radio"/> ▾
Block write access to removable data-drives not protected by BitLocker	<input type="radio"/> Oui	<input type="radio"/> Non configuré
Block write access to devices configured in another organization	<input type="radio"/> Oui	<input type="radio"/> Non configuré

Revision #1

Created 10 June 2022 21:03:20 by Khroners

Updated 10 June 2022 21:07:30 by Khroners