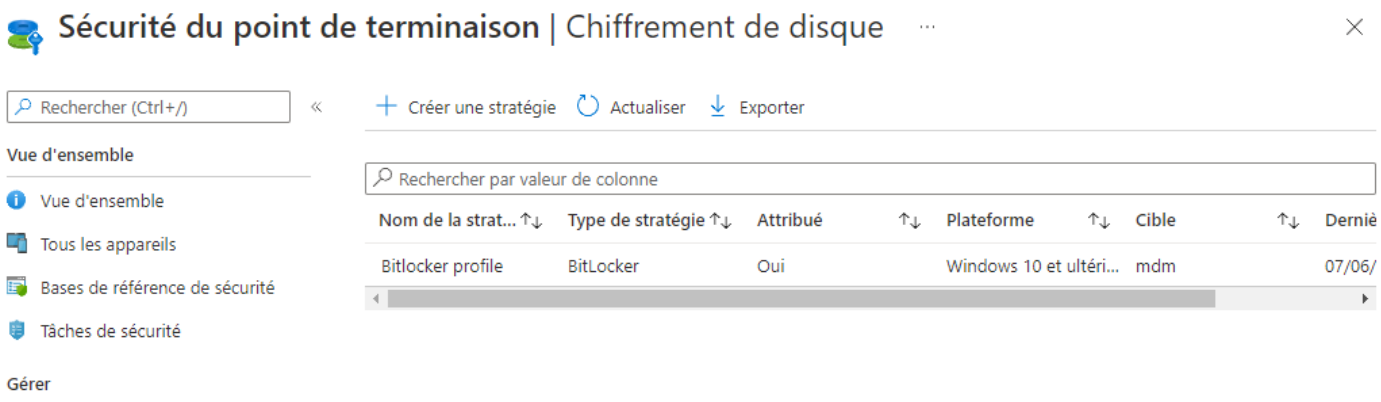
Activer silencieusement BitLocker

Pour activer silencieusement BitLocker, il est nécessaire d'avoir des paramètres précis.
Il existe deux manières de le faire :

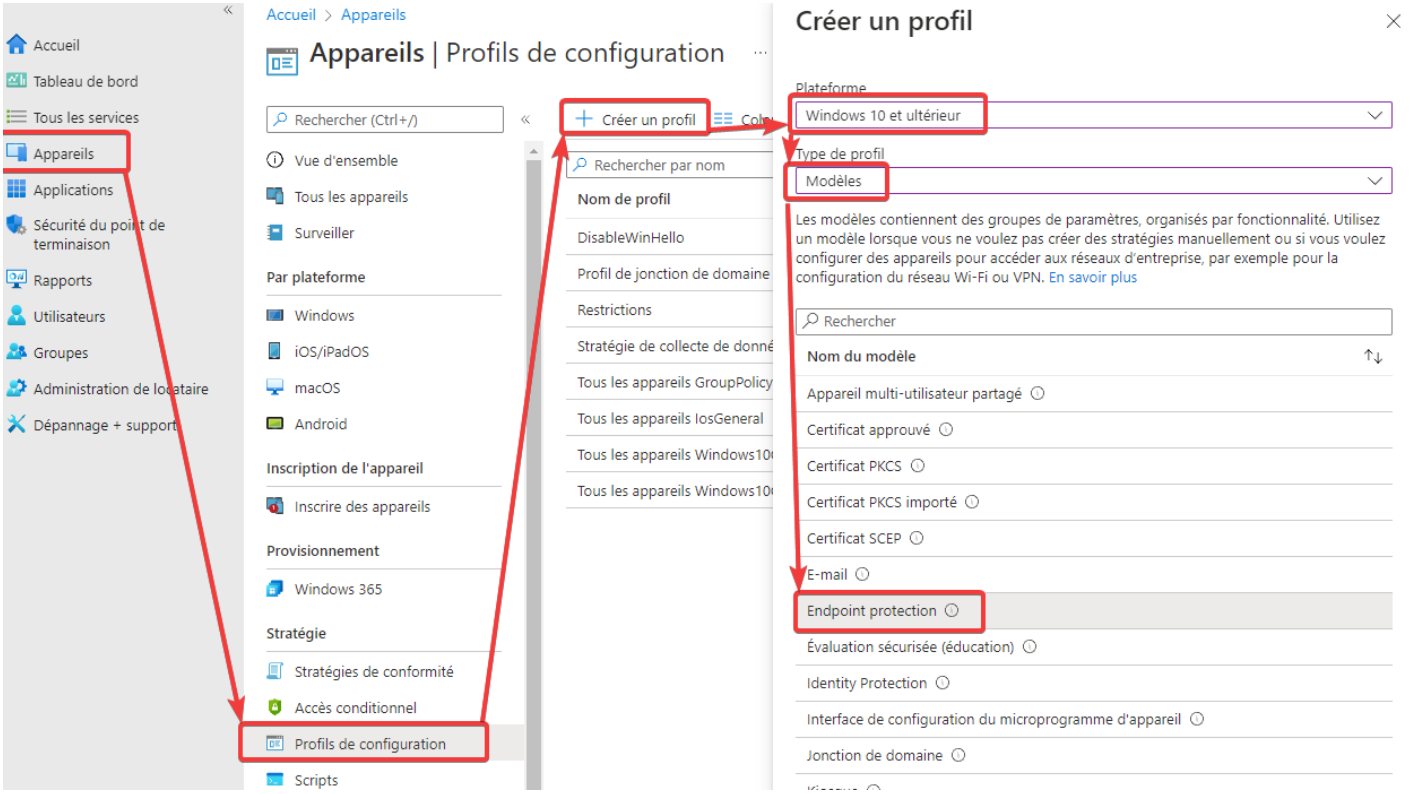
Dans le profil "Bitlocker" :

- **Hide prompt about third-party encryption** = *Yes*
- **Alow standard users to enable encryption during Autopilot** = *Yes*



Dans le profil "Endpoint Protection" :

- **Warning for other disk encryption** = *Block*.
- **Allow standard users to enable encryption during Azure AD Join** = *Allow*


Accueil
Tableau de bord
Tous les services
Appareils
Applications
Sécurité du point de terminaison
Rapports
Utilisateurs
Groupes
Administration de locataire
Dépannage + support
Accueil > Appareils
Appareils | Profils de configuration
Rechercher (Ctrl+/)
Vue d'ensemble
Tous les appareils
Surveiller
Par plateforme
Windows
iOS/iPadOS
macOS
Android
Inscription de l'appareil
Inscrire des appareils
Provisionnement
Windows 365
Stratégie
Stratégies de conformité
Accès conditionnel
Profils de configuration
Scripts
Créer un profil
Rechercher par nom
Nom de profil
DisableWinHello
Profil de jonction de domaine
Restrictions
Stratégie de collecte de donné
Tous les appareils GroupPolicy
Tous les appareils IosGeneral
Tous les appareils Windows10
Tous les appareils Windows10
Créer un profil
Plateforme
Windows 10 et ultérieur
Type de profil
Modèles
Les modèles contiennent des groupes de paramètres, organisés par fonctionnalité. Utilisez un modèle lorsque vous ne voulez pas créer des stratégies manuellement ou si vous voulez configurer des appareils pour accéder aux réseaux d'entreprise, par exemple pour la configuration du réseau Wi-Fi ou VPN. En savoir plus
Rechercher
Nom du modèle
Appareil multi-utilisateur partagé
Certificat approuvé
Certificat PKCS
Certificat PKCS importé
Certificat SCEP
E-mail
Endpoint protection
Évaluation sécurisée (éducation)
Identity Protection
Interface de configuration du microprogramme d'appareil
Jonction de domaine

Endpoint protection

Windows 10 et ultérieur

De base | 2 Paramètres de configuration | 3 Balises d'étendue | 4 Affectations | 5 Règles d'applicabilité

Microsoft Defender Application Guard

Pare-feu Microsoft Defender

Microsoft Defender SmartScreen

Chiffrement Windows

Paramètres Windows

Chiffrer les appareils	Exiger	Non configuré
Chiffrer la carte de stockage (mobile uniquement)	Exiger	Non configuré

Paramètres de base de BitLocker

Avertissement pour tout autre chiffrement de disque	Bloquer	Non configuré
Autoriser les utilisateurs standard à activer le chiffrement pendant une jonction Azure AD	Accorder	Non configuré
Configurer les méthodes de chiffrement	Activer	Non configuré
Chiffrement pour les lecteurs du système d'exploitation	XTS-AES 128 bits	
Chiffrement pour les lecteurs de données fixes	XTS-AES 128 bits	
Chiffrement pour les lecteurs de données amovibles	AES-CBC 128 bits	

Paramètres des lecteurs de système d'exploitation BitLocker

Authentification supplémentaire au démarrage	Exiger	Non configuré
BitLocker avec puce TPM non compatible	Bloquer	Non configuré
Démarrage du module TPM compatible	Autoriser TPM	
Code PIN de démarrage du module TPM compatible	Autoriser un code PIN de démarrage avec TPM	

Précédent | Suivant

Revision #1
Created 10 June 2022 21:07:39 by Khroners
Updated 10 June 2022 21:16:26 by Khroners