

Contrôle de Bitlocker

Table des matières

Contrôle de Bitlocker.....	1
Présentation	1
Démarrage.....	1
Fonctionnement	2
Vérification sur l'AD.....	2
1 – Vérification Cryptage	3
2 – Vérification TPM + Mot de Passe	3
3 – Sauvegarde sur l'AD.....	3

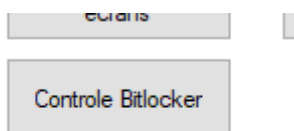
Présentation

Certains ordinateurs sont bien chiffrés par BitLocker mais la clé de déchiffrement ne remonte pas dans l'AD. Cet outil va, après avoir vérifié que les paramètres sont corrects forcer la sauvegarde de la clé sur les contrôleurs de domaine.

ATTENTION DE BIEN CONTROLER LES 2 PREMIERES ETAPES AVANT DE LANCER LA SAUVEGARDE SUR L'AD.

Démarrage

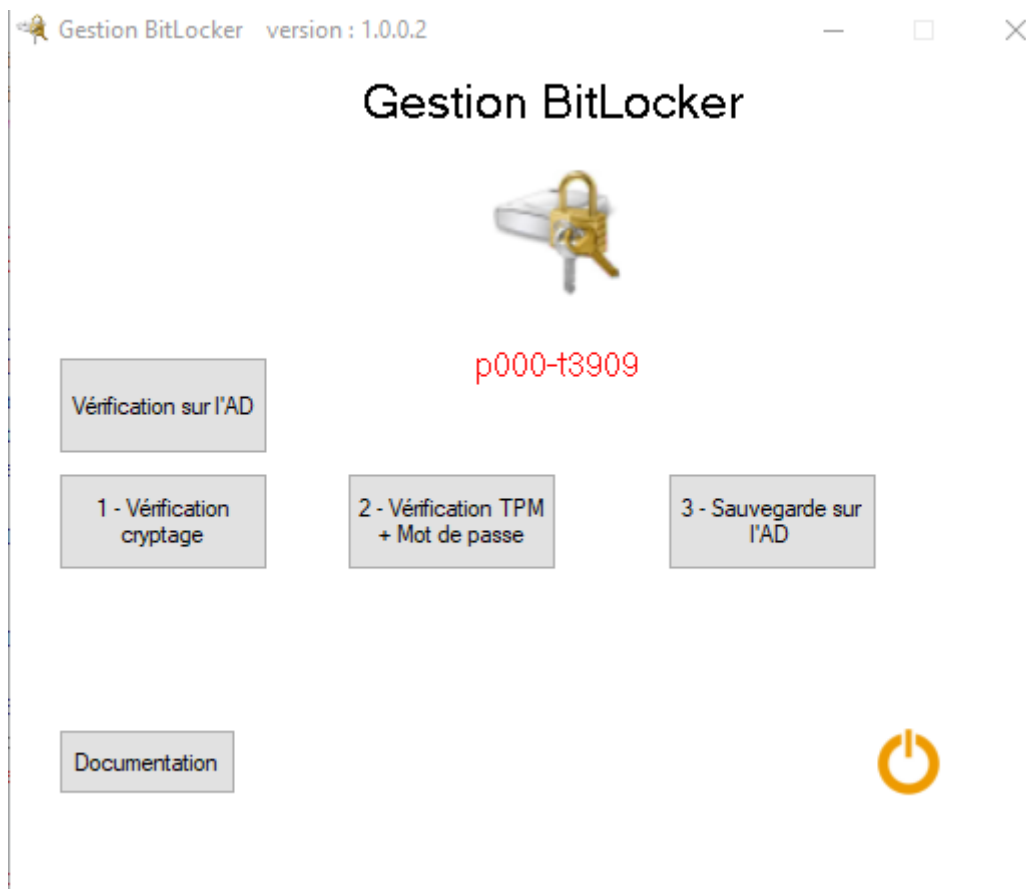
Sur outils Admin, après avoir saisi le nom de l'ordinateur, aller dans l'onglet « Gestion du PC » puis cliquer sur le bouton « Contrôle Bitlocker »



Alimentation

Confirmer ou modifier le nom de l'ordinateur à analyser puis cliquer sur OK

A screenshot of a small dialog box with a light gray background. At the top, it says 'saisir le nom de l'ordinateur a analyser'. Below this is a text input field containing the text 'p000-tpret22'. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.



Fonctionnement

ATTENTION DE BIEN CONTROLER LES 2 PREMIERES ETAPES AVANT DE LANCER LA SAUVEGARDE SUR L'AD.

Vérification sur l'AD

Permet de contrôler si la clé BitLocker est enregistrée sur l'AD

```
C:\windows\system32>powershell -ExecutionPolicy Bypass -File C:\ProgramData\DSIAN\utilsAdmin\Bin\CheckBitLocker.ps1 -ComputerName p000-t3909
Appuyer sur entree pour continuer
C:\windows\system32>
```

La clé **n'est pas** enregistrée sur l'AD

```
C:\windows\system32>powershell -ExecutionPolicy Bypass -File C:\ProgramData\DSIAN\utilsAdmin\Bin\CheckBitLocker.ps1 -ComputerName p000-t3909
Appuyer sur entree pour continuer
DistinguishedName      : CN=2024-03-15T10:37:33\+01:00{[redacted]},CN=P000-t3909,OU=CONTENEUR
                        PAR DEFALT,OU=Ordinateurs,OU=W10,OU=CLIENTS CG47,DC=dptlg,DC=fr
msFVE-RecoveryPassword : 690932-510961-483494-[redacted]
Name                   : 2024-03-15T10:37:33+01:00{[redacted]}
ObjectClass             : msFVE-RecoveryInformation
ObjectGUID             : f2f97a[redacted]
Appuyer sur entree pour continuer
C:\windows\system32>
```

La clé **est** enregistrée sur l'AD

1 – Vérification Cryptage

Permet de vérifier si le disque dur est chiffré ou pas.

Une fenêtre DOS s'ouvre en lançant le script. Patienter quelques instants pour avoir le résultat.

```
C:\windows\system32>powershell
*****
crypte
*****
C:\windows\system32>
```

Le disque est chiffré

```
C:\windows\system32>powershell
*****
Decrypte
*****
C:\windows\system32>
```

Le disque n'est pas chiffré

NE PAS CONTINUER SI LE DISQUE N'EST PAS CHIFFRÉ

2 – Vérification TPM + Mot de Passe

Pour fonctionner et déchiffrer le disque dur au démarrage, Bitlocker utilise 2 méthode : la puce TPM intégrée à la carte mère de l'ordinateur et une clé (mot de passe) sauvegardée sur l'AD. Ce bouton permet de contrôler l'existence de ces 2 modes d'authentification.

```
Chiffrement de lecteur BitLocker : outil de configuration version 10.0.19041
Copyright (C) 2013 Microsoft Corporation. Tous droits réservés.

Volume C: [Windows]
Tous les protecteurs de clés

1 TPM :
  ID : {0D4B5C20-0DD9-4ABB-98C6-86E215A74082}
  Profil de validation PCR :
    0, 2, 4, 11

2 Mot de passe numérique :
  ID : {5F000000-6D000000-437D-0000-5F000000}
  Mot de passe :
    01500000-03100000-21600000-39800000-19400000-101739-38000000-62700000
```

Ici la puce TPM et le mot de passe numérique sont bien activés.

SI L'UNE DE CES 2 VALEURS N'APPARAÎT PAS NE PAS CONTINUER

3 – Sauvegarde sur l'AD

Toutes les étapes étant correcte, nous allons pouvoir forcer la sauvegarde de la clé sur l'AD.

```
ComputerName : P00-  
VolumeType      Mount Point CapacityGB VolumeStatus Encryption Percentage KeyProtector AutoUnlock Protection  
-----  
OperatingSystem C:          460,50 FullyEncrypted 100 {Tpm, RecoveryPassword} On  
C:\windows\system32>
```

La clé est sauvegardée sur l'AD. Patienter quelques minutes pour lancer le contrôle via le SSI.