

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

Chiffrement du disque système Windows à l'aide de Bitlocker.

L'objectif de ce document est de décrire étape par étape la méthode de chiffrement d'un système d'exploitation Windows 10 à l'aide du logiciel BITLOCKER

Postulat de départ : le chiffrement du disque système doit être réalisé uniquement par l'administrateur système et réseau du laboratoire, ceci dans un objectif de gestion pertinente des clefs de recouvrement.

Installez le logiciel ou demandez à l'administrateur de votre machine de le faire.



Direction Opérationnelle des Systèmes d'Information – Pôle proximité

TPM ou pas?

La plupart des machines récentes sont équipées d'une puce TPM (Trusted Platform Module). Celle-ci prend en charge le stockage de la clef de chiffrement du disque.

Par défaut, sous Windows 10, Bitlocker est configuré pour utiliser la puce TPM.

Or, vous pouvez être amené à intervenir sur des machines non munies de cette puce ou sur lesquelles elle a été désactivée.

Les étapes ci-dessous décrivent la configuration d'une machine avec et sans TPM.



Direction Opérationnelle des Systèmes d'Information – Pôle proximité

Chiffrement avec puce TPM.

Etape 1 : Activation de Bitlocker et chiffrement du système d'exploitation.

Par défaut, Bitlocker est désactivé. Il faut l'activer afin de pouvoir lancer le chiffrement de la machine.

1. Lancez l'outil de gestion de Bitlocker





Direction Opérationnelle des Systèmes d'Information – Pôle proximité

2. Dans la partie « Lecteur du système d'exploitation », cliquez sur « Activer Bitlocker ».



ATTENTION : l'objet de ce document est de chiffrer le lecteur du système d'exploitation. Il est possible de chiffrer un autre disque dur « interne » en utilisant la même méthode.

Concernant le chiffrement des périphériques de stockage « mobiles », un autre document décrit la marche à suivre.

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

3. Cliquez sur « Enregistrer dans un fichier ».

		\times
\leftarrow	R Chiffrement de lecteur BitLocker (C:)	
	Comment voulez-vous sauvegarder votre clé de récupération ?	
	 Certains paramètres sont gérés par votre administrateur système. 	
	Une clé de récupération vous permet d'accéder à vos fichiers et vos dossiers, si vous rencontrez des problèmes pour déverrouiller votre PC. Il est préférable d'en avoir plusieurs et de les conserver ailleurs que sur votre PC.	
\langle	→ Enregistrer dans un fichier	
	→ Imprimer la clé de récupération	
	Comment retrouver ma clé de récupération ultérieurement ?	
	Suivant Annule	,

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

- 4. La mise en place de la clef de recouvrement est une étape importante. Cette clef doit être stockée dans un endroit sûr et accessible uniquement aux personnes autorisées.
- 5. Bitlocker vous propose d'enregistrer cette clef au format « .txt ». Vous pouvez la stocker sur un périphérique de stockage mobile, mais il est recommandé de la stocker dans un gestionnaire de mot de passe, un logiciel type « coffre fort numérique » ou tout système de gestion de secret vous paraissant adapté à la protection de cette clef.

🎕 Enregistrer la clé (de récupé	ération BitLocker sous					×
← → • ↑ 🖡	> Kate	K (D:) > bitlocker		~ Ū	Rechercher dans : bi	tlocker	Q
Organiser 🔻 No	ouveau de	ossier				∎ = ▼	?
🔚 Images	* ^	Nom		Modifié le	Туре	Taille	
🐌 Musique 驞 Vidéos			Aucun élément ne c	orrespond à votre re	cherche.		
la OneDrive							
🍤 Ce PC							
🧹 KateK (D:)							
🅩 Réseau	~ <						>
Nom du fichier	Clé de	récupération BitLocker 7416E	DA1-C01D-41C3-A51	10-BB9F173F8734	>		~
Туре :	: Fichiers	texte (*.txt)					~
∧ Masquer les dossi	iers			\langle	Enregistrer	Annuler	

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

6. Cochez « chiffrer tout le lecteur » puis cliquez sur suivant

 \times

Representation of the sector of

Choisir dans quelle proportion chiffrer le lecteur

Si vous configurez BitLocker sur un nouveau lecteur ou un nouveau PC, il vous suffit de chiffrer la partie du lecteur en cours d'utilisation. BitLocker chiffre automatiquement les nouvelles données que vous ajoutez.

Si vous activez BitLocker sur un PC ou un lecteur en cours d'utilisation, chiffrez l'intégralité du lecteur. Le chiffrement de l'intégralité du lecteur garantit la protection de la totalité des données, même des données supprimées qui peuvent contenir des informations récupérables.

O Ne chiffrer que l'espace disque utilisé (plus rapide et plus efficace pour les nouveaux PC et lecteurs)

Ochiffrer tout le lecteur (opération plus lente recommandée pour les PC et les lecteurs en service)

Suivant

Annuler

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

7. Cochez « nouveau mode de chiffrement » puis cliquez sur suivant

 \times

A the second seco

Choisir le mode de chiffrement à utiliser

La mise à jour Windows 10 (Version 1511) présente un nouveau mode de chiffrement de disque (XTS-AES). Ce mode fournit une prise en charge supplémentaire de l'intégrité, mais il n'est pas compatible avec les versions antérieures de Windows.

S'il s'agit d'un lecteur amovible que vous allez utiliser sur une version antérieure de Windows, vous devez choisir le mode Compatible.

S'il s'agit d'un lecteur fixe ou si ce lecteur ne va être utilisé que sur des appareils exécutant au moins Windows 10 (Version 1511) ou version ultérieure, vous devez choisir le nouveau mode de chiffrement

Nouveau mode de chiffrement (recommandé pour les lecteurs fixes sur ce périphérique)

O Mode Compatible (recommandé pour les lecteurs pouvant être déplacés à partir de ce périphérique)

Suivant

Annuler

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

- 8. Cochez « Exécuter la vérification du système », puis cliquez sur « continuer »

Êtes-vous prêt à chiffrer ce lecteur ?

Le chiffrement peut prendre un moment, selon la taille du lecteur.

Vous pouvez continuer à travailler pendant le chiffrement du lecteur, bien que les performances de votre ordinateur puissent être affectées.

×

Exécuter la vérification du système BitLocker

La vérification du système permet de s'assurer que BitLocker peut lire correctement les clés de récupération et de chiffrement avant de chiffrer le lecteur.

BitLocker redémarrera votre ordinateur avant d'effectuer le chiffrement.

Remarque : cette vérification peut être longue, mais elle est recommandée pour vous assurer que la méthode de déverrouillage sélectionnée fonctionne sans devoir entrer la clé de récupération.

	Continuer Annuler
9. Redémarrez l'ordinateur	
Real Chiffrement de lecteur BitLocker	
L'ordinateur doit être redémarré	
Redémarrer maintenant Redémarrer ultérieurement	
<u>Gérer BitLocker</u>	

10. Au démarrage de la machine vous serez invité à saisir le code PIN que vous avez défini plus haut. Attention : à la saisie du code PIN, le clavier sera en QWERTY.

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

11. Pour connaitre l'état d'avancement de la procédure de chiffrement du disque, cliquez sur l'icone cachée à droite de la barre des tâches.

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

Chiffrement sans puce TPM ou puce TPM désactivée.

Etape 1: autoriser Bitlocker à ne pas utiliser TPM

1. Lancez l'éditeur de stratégie de groupe « gpedit.msc »

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

 Placez-vous dans « Modèles d'administration > Composants Windows > Chiffrement de lecteur BitLocker > Lecteurs du système d'information », double-cliquez sur « Exiger une authentification supplémentaire au démarrage ».

Х

Éditeur de stratégie de groupe locale

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

- 3. Cochez « Activé ».
- 4. Cochez la case « Autoriser Bitlocker sans un module de plateforme sécurisée compatible ».

	Exiger une authentification supplémentaire au démarrage											
	📷 Exiger une authe	entification supplémen	taire au dém	arrage	Paramètre précédent	Paramètr	e suivant					
$\left(\right)$	O Non configuré	Commentaire :						· · · · · · · · · · · · · · · · · · ·	^			
	O Désactivé	Pris en charge sur :	Au minimu	um Windows	Server 2008 R2 ou Windo	ows 7						
	Options :			Aide :								
\langle	Autoriser BitLock mot de passe ou Paramètres pour les Configurer le démar Autoriser le module Configurer le code P	er sans un module de une clé de démarrage ordinateurs avec un m rage du module de pla de plateforme sécurise PIN de démarrage de m	lateform ^ sur un di: nodule de teforme s se nodule de	 Ce parametre de strategie vous permet de configurer si bitLocker exige une authentification supplémentaire à chaque démarrage de l'ordinateur et si vous utilisez BitLocker avec ou sans module de plateforme sécurisée. Ce paramètre de stratégie est appliqué lorsque vous activez BitLocker. Remarque : une seule des options d'authentification supplémentaire peut être exigée au démarrage, sans générer d'erreur de stratégie. Si vous voulez utiliser BitLocker sur un ordinateur sans un module de plateforme sécurisée, activez la case à cocher « Autoriser BitLocker sans un module de plateforme autorisée compatible ». Dans ce mode, un mot de passe ou un lecteur USB 								
	Autoriser un code P Configurer la clé de	IN de démarrage avec démarrage de module	le module de platef									
	Autoriser une clé de Configurer le code P	Autoriser une clé de démarrage avec le module de p Configurer le code PIN et la clé de démarrage de m			est requis pour le démarrage. Si une clé de démarrage est utilisé les informations de clé utilisées pour chiffrer le lecteur sont stockées sur ce lecteur USB, créant une clé USB. Lorsque la clé USB est insérée, l'accès au lecteur est authentifié et le lecteur est							
	<		>	 accessible, of a cle obblest perdue ou non disponible, ou ble encore si vous oubliez le mot de passe, vous devez utiliser l'u des options de récupération BitLocker pour accéder au lecter 								

OK Annuler

Appliquer

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

5. Double-cliquez sur « Autoriser les codes confidentiels améliorés au démarrage »

- 🗆 X

🧾 Éditeur de stratégie de groupe locale

Fichier	Action	Affichage ?				
🗢 🄿	2					
		Antivirus Windows Defender Appareil photo Assistance en ligne Biométrie Calendrier Windows Carte à puce Cartes Centre de mobilité Windows Centre de sécurité Chiffrement de lecteur BitLocker Chiffrement de lecteur BitLocker Lecteurs de données amovibles Lecteurs de données fixes Lecteurs de données fixes Lecteurs de système d'exploitation Collecte des données et versions d'évaluatio Compatibilité des applications Compte Microsoft Confidentialité de l'application Connexion Contenu cloud Déploiement de package Appx	^	Paramètre Autoriser le déverrouillage réseau au démarrage Autoriser le démarrage sécurisé pour la validation de l'intégr Exiger une authentification supplémentaire au démarrage Autoriser les autilisateurs standard à modifier le code Autoriser les appareils compatibles avec InstantGo ou HSTI Autoriser les confidentiels améliorés au démarrage Configurer l'utilisation de l'authentification BitLocker exigeantur. Configurer l'utilisation du chiffrement au niveau matériel po Configurer l'utilisation de crécupération des lecteurs du s Configurer la méthode de récupération des lecteurs du s Configurer le profil de validation de plateforme du module Configurer le profil de validation de plateforme du module Configurer le profil de validation de plateforme du module Configurer les données de validation de plateforme après u	État Non configuré Activé Non configuré Non configuré	Cor ^
<		Dossiers de travail		Étendu) Standard		

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

6. Cochez «	6. Cochez « Activé » puis validez en cliquant sur « OK »								
🕵 Autoriser les coo	des confidentiels améli	rés au démarrage — 🛛	×						
Autoriser les co	des confidentiels améli	rés au démarrage Paramètre précédent Paramètre suivant							
O Non configuré	Commentaire :		^						
Activé Désactivé			~						
	Pris en charge sur :	Au minimum Windows Server 2008 R2 ou Windows 7	< >						
Options :		Aide :							
		Ce paramètre de stratégie permet de configurer si les codes confidentiels améliorés peuvent être utilisés avec BitLocker au démarrage. Les codes confidentiels de démarrage améliorés permettent l'utilisation de caractères comme les majuscules et les minuscules, les symboles, les chiffres et les espaces. Ce paramètre de stratégie est appliqué lorsque vous activez BitLocker. Si vous activez ce paramètre de stratégie, tous les nouveaux codes confidentiels de démarrage BitLocker seront des codes améliorés. Remarque : tous les ordinateurs ne prennent pas en charge les codes confidentiels améliorés dans l'environnement préalable au démarrage. Il est fortement conseillé que les utilisateurs réalisent une vérification système pendant l'installation de BitLocker. Si vous désactivez ce paramètre de stratégie ou ne le configurez pas, les codes confidentiels améliorés ne sont pas autorisés.							
		OK Annuler Appliqu	ier						

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

7. Double-cliquez sur « Configurer la longueur minimale du code PIN de démarrage »

Éditeur de stratégie de groupe locale							
Fichier Action Affichage ?							
🔶 🏕 🔝 🗟 🖬 🔻							
Image: Stratégie Ordinateur local Image: Stratégie Ordinateur local Image: Configuration ordinateur Image: Paramètres du logiciel Image: Paramètres Windows Image: Pa	Paramètre Autoriser le déverrouillage réseau au démarrage Autoriser le démarrage sécurisé pour la validation de l'intégrité Exiger une authentification supplémentaire au démarrage EE Exiger une authentification supplémentaire au démarrage (W EN Pas autoriser les utilisateurs standard à modifier le code P Autoriser les appareils compatibles avec InstantGo ou HSTI à Autoriser les codes confidentiels améliorés au démarrage Configurer la longueur minimale du code PIN de démarrage Configurer la longueur minimale du code PIN de démarrage Configurer la longueur minimale du code PIN de démarrage Configurer l'utilisation de récupération des lecteurs du sy EConfigurer le type de chiffrement de lecteur aux lecteurs du syst Configurer le profil de validation de plateforme du module d Configurer le profil de vali	État Non configuré Non configuré					
Confidentialité de l'application							
Contenu cloud							
📋 Dossiers de travail	<	>					
< >>	Étendu Standard						
19 paramètro(c)							

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

8. Cochez « Activé », fixez le nombre minimal de caractères à 10 puis validez en cliquant sur « OK »

	🐙 Configurer la longueur minimale du code PIN de démarrage 🦳 🗌								Х
	🔚 Configurer la lor	ngueur minimale du co	de PIN de dér	marrage	Paramètre	précédent	Paramètre s	uivant	
\mathcal{C}	Non configuré Activé	Commentaire :							^
	O Désactivé	Pris en charge sur :	Au minimur	m Windows S	erver 2008 R	2 ou Windows	; 7		~
	Options :			Aide :					
(Nombre minimal de 10	caractères :		Ce pa longueur m de platefor appliqué lo démarrage Si vou exiger le no PIN de dém Si vou configurez comportan REMA Windows ta TPM 2.0 de défaut lorse Windows n valeur par o	aramètre de s ninimale pou me sécurisée rsque vous a doit compo us activez ce ombre minim narrage. us désactivez pas, les utilis t entre 6 et 2 ARQUE : si le entera de réil manière à c qu'un code f e réinitialise défaut que si	stratégie vous ur le code PIN e (TPM). Ce pa activez BitLock rter entre 4 et paramètre de hal de chiffres ce paramètre sateurs peuver code PIN com nitialiser la pér e qu'elle soit s PIN est modifi ra la période d i le TPM est ré	permet de conf de démarrage o aramètre de stra cer. Le code PIN 20 chiffres. stratégie, vous à entrer pour de e de stratégie ou nt définir un cod nporte moins de riode de verroui supérieure à la v é. Si l'opération le verrouillage d initialisé.	figurer la l'un modu tégie est de pouvez éfinir le co i ne le de PIN e 6 chiffres llage du valeur par réussit, lu TPM à l	ile ide
						ок 🔓	Annuler	Appli	quer

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

Etape 2 : Activation de Bitlocker et chiffrement du système d'exploitation.

Par défaut, Bitlocker est désactivé. Il faut l'activer afin de pouvoir lancer le chiffrement de la machine.

12. Lancez l'outil de gestion de Bitlocker

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

13. Dans la partie « Lecteur du système d'exploitation », cliquez sur « Activer Bitlocker ».

ATTENTION : l'objet de ce document est de chiffrer le lecteur du système d'exploitation. Il est possible de chiffrer un autre disque dur « interne » en utilisant la même méthode.

Concernant le chiffrement des périphériques de stockage « mobiles », un autre document décrit la marche à suivre.

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

14. Cliquez sur « Entrer un code confidentiel »

 \times

Choisir le mode de déverrouillage de votre lecteur au démarrage

Pour assurer la sécurité de vos données, vous pouvez indiquer à BitLocker d'exiger un code PIN ou un lecteur flash USB chaque fois que vous démarrez votre PC.

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

15. Saisissez le code PIN que vous souhaitez utiliser. Validez en cliquant sur « définir le code PIN »

×

Entrer un code PIN

Choisissez un code PIN constitué de 10-20 caractères.

Code PIN	
Retaper le code PIN	
	Définir le code PIN Annuler

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

16. Cliquez sur « Enregistrer » dans un fichier.

		×
<i>←</i>	R Chiffrement de lecteur BitLocker (C:)	
	Comment voulez-vous sauvegarder votre clé de récupération ?	
	i Certains paramètres sont gérés par votre administrateur système.	
	Une clé de récupération vous permet d'accéder à vos fichiers et vos dossiers, si vous rencontrez des problèmes pour déverrouiller votre PC. Il est préférable d'en avoir plusieurs et de les conserver ailleurs que sur votre PC.	
	→ Enregistrer dans un fichier	
	→ Imprimer la clé de récupération	
	Comment retrouver ma clé de récupération ultérieurement ?	
	Suivant Annule	r

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

- 17. La mise en place de la clef de recouvrement est une étape importante. Cette clef doit être stockée dans un endroit sûr et accessible uniquement aux personnes autorisées.
- 18. Bitlocker vous propose d'enregistrer cette clef au format « .txt ». Vous pouvez la stocker sur un périphérique de stockage mobile, mais il est recommandé de la stocker dans un gestionnaire de mot de passe, un logiciel type « coffre fort numérique » ou tout système de gestion de secret vous paraissant adapté à la protection de cette clef.

Renregistrer la clé de récupération BitLocker sous X							
\leftarrow \rightarrow \checkmark \uparrow	📙 > Ka	ateK (D:) > bitlocker		U	Rechercher dans : b	itlocker	٩
Organiser 🔻	Nouveau	dossier				∎ = ▼	?
🔚 Images	* ^	Nom		Modifié le	Туре	Taille	
🚺 Musique 頂 Vidéos			Aucun élément ne c	correspond à votre re	cherche.		
la OneDrive							
🇢 Ce PC							
🥿 KateK (D:)							
📣 Réseau	~	<					>
Nom du fichie	er: Clé d	le récupération BitLocker 7416	EDA1-C01D-41C3-A5	10-BB9F173F8734			\sim
Тур	e : Fichie	ers texte (*.txt)					\sim
▲ Masquer les do:	ssiers			<	Enregistrer	Annuler	

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

19. Cochez « chiffrer tout le lecteur » puis cliquez sur suivant

 \times

Representation of the sector of

Choisir dans quelle proportion chiffrer le lecteur

Si vous configurez BitLocker sur un nouveau lecteur ou un nouveau PC, il vous suffit de chiffrer la partie du lecteur en cours d'utilisation. BitLocker chiffre automatiquement les nouvelles données que vous ajoutez.

Si vous activez BitLocker sur un PC ou un lecteur en cours d'utilisation, chiffrez l'intégralité du lecteur. Le chiffrement de l'intégralité du lecteur garantit la protection de la totalité des données, même des données supprimées qui peuvent contenir des informations récupérables.

O Ne chiffrer que l'espace disque utilisé (plus rapide et plus efficace pour les nouveaux PC et lecteurs)

Ochiffrer tout le lecteur (opération plus lente recommandée pour les PC et les lecteurs en service)

Suivant

Annuler

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

20. Cochez « nouveau mode de chiffrement » puis cliquez sur suivant

 \times

A the second seco

Choisir le mode de chiffrement à utiliser

La mise à jour Windows 10 (Version 1511) présente un nouveau mode de chiffrement de disque (XTS-AES). Ce mode fournit une prise en charge supplémentaire de l'intégrité, mais il n'est pas compatible avec les versions antérieures de Windows.

S'il s'agit d'un lecteur amovible que vous allez utiliser sur une version antérieure de Windows, vous devez choisir le mode Compatible.

S'il s'agit d'un lecteur fixe ou si ce lecteur ne va être utilisé que sur des appareils exécutant au moins Windows 10 (Version 1511) ou version ultérieure, vous devez choisir le nouveau mode de chiffrement

Nouveau mode de chiffrement (recommandé pour les lecteurs fixes sur ce périphérique)

O Mode Compatible (recommandé pour les lecteurs pouvant être déplacés à partir de ce périphérique)

Suivant

Annuler

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

21. Cochez « Exécuter la vérification du système », puis cliquez sur « continuer »

 \times

Registration of the second seco

Êtes-vous prêt à chiffrer ce lecteur ?

Le chiffrement peut prendre un moment, selon la taille du lecteur.

Vous pouvez continuer à travailler pendant le chiffrement du lecteur, bien que les performances de votre ordinateur puissent être affectées.

Exécuter la vérification du système BitLocker

La vérification du système permet de s'assurer que BitLocker peut lire correctement les clés de récupération et de chiffrement avant de chiffrer le lecteur.

BitLocker redémarrera votre ordinateur avant d'effectuer le chiffrement.

Remarque : cette vérification peut être longue, mais elle est recommandée pour vous assurer que la méthode de déverrouillage sélectionnée fonctionne sans devoir entrer la clé de récupération.

	Continuer Annuler
22. Redémarrez l'ordinateur	
Reference in the lecteur BitLocker	
4 L'ordinateur doit être redémarré	
Redémarrer maintenant Redémarrer ultérieurement	
<u>Gérer BitLocker</u>	

23. Au démarrage de la machine vous serez invité à saisir le code PIN que vous avez défini plus haut. Attention : à la saisie du code PIN, le clavier sera en QWERTY.

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

24. Pour connaitre l'état d'avancement de la procédure de chiffrement du disque, cliquez sur l'icone cachée à droite de la barre des tâches.

