

Chiffrement DELL - Sommaire

- ➢Pré-requis
- ➢Réglage du BIOS
- ►Installation DDP
- Configuration DDP
- Sauvegarde du fichier de conf
- Ajouter des utilisateurs
- Réglage des options
- ➤Utilisation



Pré - requis

Matériel :

- ➢Portable DELL avec disque chiffrant (512e)
- Une clé USB ou autre support (CD/DVD) pour faire la sauvegarde. ATTENTION : ce support devra être conservé dans un endroit sécurisé type coffre-fort car le fichier texte copié durant la sauvegarde comporte le mot de passe en clair

Accès (droits) :

- ➢Accès complet au BIOS
- Compte administrateur local Conseil: ne pas utiliser user avec profil dans le groupe « administrateur local »



Pré - requis

Logiciel :

Site: <u>http://www.dell.com/support/home/fr/fr/rc1077983</u>

BIOS : télécharger puis installer la dernière version

Dell Data Protection : télécharger

Protection des données Dell (1)					
No	m du fichier	Importance	Date de publication	Version	Actions
De Ap	ell Data Protection	Recommandé	06/02/2013	2.2.00003.008 , A06	B Télécharger le fichier



Pré – requis



ATTENTION : sélectionner votre Système en haut



Sur certains portables, DDP peut se présenter en trois parties.

Respecter l'ordre d'installation des fichiers ainsi que les demandes de redémarrage:

- 1) Driver.exe
- 2) Middleware.exe
- 3) Software.exe



Réglage du BIOS



Security / TPM Security : cocher « TPM Security » puis valider avec « Apply » puis « exit »

TPM Security stings General P TPM Security System Information Battery Information - Boot Sequence This option lets you control whether the Trusted Platform Module (TPM) in the system is Date/Time enabled and visible to the operating system. When disabled, the BIOS will not turn on the System Configuration TPM during POST. The TPM will be non-functional and invisible to the operating system. Video When enabled, the BIOS will turn on the TPM during POST so that it can be used by the Security operating system Aurnin Password System Password NOTE Disabling this option does not change any settings you may have made to the TPM Internal HDD Password nor does it delete or change any information or keys you may have stored there. It simply Password Bypass turns off the TPM so that it cannot be used. When you re-enable this option, the TPM will Password Change function exactly as it did before it was disabled Strong Password ? When the TPM is in the enabled state you have the ability to control whether the TPM is OHOM Keybaard Access deactivated and disabled or activated and enabled. It also allows you to clear the ownership information in the TPM (if any). Physical presence is implied when you make a change to this Gammittase(H) ontion. When "Deactivate" the TPM will be deactivated and disabled, it will not execute any CPU XD Support commands that use the resources of the TPM, nor will it slow any access to stored owner Non-Admin Setup Changes information. When "Activate" the TPM will be enabled and activated. This is the normal Password Configuration operating state for the TPM when you want to use its complete array of capabilities. When Signed Firmware Update "Clear" the BIOS clears the owner information stored in the TPM. Use this setting to restore Admin Setup Lockout the TPM to its default state if you lose or forget the owner authentication data. Performance NOTE. Activation, deactivation and clear options are not affected if you load the setup Power Management program's default values. Changes to this option take effect immediately POST Behavior Virtualization Support Wireless - Maintenance + System Logs

Load Celaulta

Réglage du BIOS



P. 6

Security / TPM Security et cocher « Activate » puis valider avec « Apply ».

	TPM Security
stem Information	TPM Security
tery Information	
of Sequence	@ Deactivate
te/Time	(@ Actente
n Configuration	
	© Clear
(y)	
man Password	
stern Password	This option late you control whether the T
emai HDD Password	enabled and vasible to the operating in a long whether the Trusted Platform Module (TPM) in the system in
ssword Bypass	TPM during POST The TPM will be system. When disabled, the BIOS will not turn on the
ssword Change	When enabled the BIOS will turn on the TPM during POST or the operating system
ong Paseword	operating system
TUM Reyboard Access	
M Security	NOTE Disabling this option does not change any settings you may have made to the TF
reputrace(R)	nor does it delete or change any information or keys you may have stored there it simpl
AUXD Support	furns on the TPM so that it cannot be used When you re-enable this option, the TPM will
an-Admin Setup Changes	To entry as a did before it was disabled
assword Configuration	When the TPM is in the enabled state you have the ability to control whether the TPM is
Ingried Filmware Opdate	deactivated and disabled or activated and enabled. It also allows you to clear the
ormance	ownership information in the TPM (if any) Physical presence is implied when you make a
er Managemient	Change to this option. When "Deactivate" the TPM will be deactivated and disabled. It will
T Behavior	hat execute any commands that use the resources of the TPM, nor will it allow any acces
ustization Support	the sourced over an activity of the TEV when you want the complete man of
etens.	Capabilities when "Clear" the BIOS clears the owner information stored in the TPM Use
ntenance	this setting to restore the TPM to its default state if you lose or forget the owner
tem Logo	authentication data
and the second se	NOTE Activation deactivation and clear options are not affected if you load the setup



Réglage du BIOS

Security / Admin Password et mettre un mot de passe en le confirmant valider par OK puis Exit.





Installer DDP

- Une fois les messages d'infos et de la décompression des fichiers passés, cliquer sur Suivant.
 - Rester sur l'option Terminé et cliquer sur le bouton Suivant.

Options d'installation	TA A
Veuillez sélectionner l'une des options ci-dessous :	9
1 (* Terminé Installe ou met à niveau tous les composants de ce prog	iciel
C Limité Installe les pilotes et l'intergiciel, mais pas l'application.	
Appuyez sur « Suivant » pour continuer	2

A la fin de l'installation redémarrer le portable



Configurer DDP



Maintenance Module TPM	ta Protection Access Mots de passe	Périphériques 1 Module) 2	
Affichez le statut di Affichez les informa Self-Encryptin Affichez le statut et	Maintenance	ata Protection Access (2) – Mots de passe Périphériques Module TPM (Trusted Platform Module)	×
Accès S	Informations su	ur le périphérique ici afficher Detell Data Protection Access Maintenance Mots de passe Périphériques	? ?
	Accès	Non détenu prendre la propriété Statut de verrouillage indisponible Informations sur le périphérique	affiche
			_



Mettre un mot de passe en le confirmant puis « Suivant »





Modifier la propriété

Détell Data Protection Access Maintenance Mots de passe Périphériques récédent Module TPM (Trusted P Statut : Active désactiver Détenu modifier la propriété Si OK	Saisir Administrateur et Mot de passe puis Suivant.	
Informations sur le périphérique	Data Protection Access Security Wizard Self-Encrypting Drive Créez un mot de passe pour ce Self-Encrypting de Windows.	Contro de passe avant le démarrage Nom windows du portable
Accès Self-Encrypting Drive	Domaine : 06TESTMICK Administrateur ************************************	 Nom login de la session. Administrateur si vous avez suivis mes recommandations Mot de passe Confirmation Mot de passe
	Accès Self-Encrypting Drive	Précédent Suivant

Sauvegarde

Sauvegarde du fichier de configuration sur une clé USB. ATTENTION : à conserver dans un endroit sécurisé type coffre-fort car comporte le mot de passe en clair

Data Protection Access	? -
Security Wizard	X Subscription Mar
Self-Encrypting Drive	
Choisissez un emplacement où sauvegarder le mot lecteur. Cette sauvegarde sera requise si vous oublie lecteur.	de passe et le nom d'utilisateur de l'administrateur de ez les informations de connexion de l'administrateur de
I si vous perdez cette sauvegarde et oubliez votr	e mot de passe, vous n'aurez pas accès à vos données.
Vous ne pouvez pas réinitialiser votre mot de pa	asse.
choisir un emplacement :	
F:\Sauvegarde DDP Parc	courir 1
	4
	Précédent Suivant
Accès Self-Encrypting Drive	avance

P. 13

Définir les utilisateurs autorisés

P 14 Pour l'instant seul l'administrateur local à ce droit.
 Conseil: passer par Ajouter un utilisateur via la gestion de compte windows.

D¢LL	Data Protection Access	? _ X
Securi	ty Wizard	X Izard
Ajou	ter un utilisateur du Self-Encrypting Drive	
Fourni	ssez le domaine et le nom d'utilisateur Windows de l'utilisateur du lecteur que vous voulez aj	outer.
061	TESTMICK	
Ajout	ter un utilisateur via Gestion de compte Windows	
	ici	
	Précédent	t
Accès	Self-Encrypting Drive	avancé 🖌



Cliquer sur Emplacements ceci afin de choisir un compte local ou un compte sur un serveur Active Directory. Dans mon cas ça sera un compte local. Puis cliquer sur Avancé.

Sélectionnez un utilisateur ou un groupe	?	? _ ×	
Sélectionnez le type de cet objet :		Sunterent excent/fizard	
un utilisateur ou un groupe	Types d'objets	Sélectionnez un utilisateur ou un groupe	? ×
A partir de cet emplacement :			
USTESTMICK	Emplacements	Sélectionnez le type de cet objet :	
Entrez le nom de l'objet à sélectionner (<u>exemples</u>) :	lecteur qu	e v un utilisateur ou un groupe	Types d'objets
(E	Vérifier les noms	À partir de cet emplacement :	
		OGTESTMICK	Emplacements
Avancé	OK Annuler Précédent	Requêtes communes Nom : Commence par Description : Commence par Comptes désactivés Mot de passe sans date d'expiration Nombre de jours depuis la dernière session :	1 Colonnes Rechercher Arrêter 3
Accès Self-Encrypting Drive		Résultats de la recherche :	OK Annuler
		Nom (RDN) Dossier	
		Administrateur OfTESTMICK Whyte OfTESTMICK TEST OFTESTMICK 2	

Conseil : même mot de passe que celui d'ouverture de session du compte utilisé (à condition qu'il respecte la complexité demandée) car nous allons synchroniser le compte DDP et avec celui de Windows.

Si vous n'êtes pas le propriétaire de ce compte (mot de passe inconnu) mettre un mot de passe provisoire et cocher la case « Exigez de l'utilisateur qu'il réinitialise son mot de passe... ».





Réglage des options

Cercles verts : options "indispensables".

Cercles roses : options selon votre convenance.

Deta Protection Access	▶ ? - ×
Maintenance Mots de passe Périphériques	
précédent Self-Encrypting Drive	
Gestion du périphérique	masquer
Protection des données : Activée désactiver Verrouillage : Activée désactiver Administrateur du lecteur (O6TESTMICK\administrateur) <u>changer</u> Utilisateurs du lecteur (enregistrés) : 1 <u>ajouter/supprimer des utilisateurs</u> Synchronisation du mot de passe Windows Activée <u>désactiver</u> Mémoriser le nom du dernier utilisateur (Activée) <u>désactiver</u> Sélection du nom d'utilisateur (Désactivée) <u>activer</u> Effacement des données cryptographiques : <u>confirmer</u>	
Informations sur le nérinhérique	afficher
Accès Self-Encrypling Drive	accueil 👻

Si vous avez mis le même mot de passe utilisateur windows et DDP, je vous recommande maintenant d'avoir la Synchronisation du mot de passe windows Activée. (changement mot de passe windows → automatiquement dans DDP)

P. 17



Utilisation





Merci de votre attention.

Des questions ?