

**GFI**

# Le standard PCI DSS et GFI EventsManager 7

Conditions PCI DSS	Vérification rétroactive	Surveillance & Rapports	Alertes	Exécution	Remarque
<b>Condition 1: Installer et maintenir une configuration de pare-feu pour protéger les données de propriétaires de carte</b>					
1.3 Etablir une configuration de pare-feu pour limiter l'accès aux données de propriétaires de cartes					
1.3.1 Limiter le trafic internet entrant aux adresses IP se trouvant dans la zone démilitarisée		●	●		Créer de nouvelles règles
1.3.6 Sécuriser et synchroniser les fichier de configuration de routeur		✓	✓		Personnaliser les règles & rapports par défaut **
1.3.7 Interdire tout autre trafic entrant ou sortant qui n'est pas spécifiquement autorisé		●	●		Créer de nouvelles règles
<b>Condition 2: Ne pas utiliser de mots de passe par défaut créés par les fournisseurs</b>					
2.2 Etablir des normes de configuration pour tous les composants du système					
2.2.2 Désactiver tous les services et protocoles non sécurisés		●	●		Condition non supportée par défaut *
<b>Condition 3: Protéger les données stockées des propriétaires de cartes</b>					
3.5 Protéger les clés utilisées pour le chiffage des données de propriétaires de carte contre la fuite et l'abus:					
3.5.1 Limiter l'accès aux clés à un nombre minimum possible de personnes		✓	✓		Personnaliser les règles & rapports par défaut **
3.6 Classer et mettre en application systématiquement tous les processus et procédures de gestion des clés utilisées pour le chiffage des données de propriétaires de cartes					
3.6.3 Sécuriser le stockage des clés		✓	✓		Personnaliser les règles & rapports par défaut **
<b>Condition 7: Limiter l'accès aux données de propriétaires de cartes au le personnel approprié de l'entreprise</b>					
7.1 Limiter l'accès aux ressources informatiques et aux détails des propriétaires de cartes aux seuls individus dont le travail nécessite un tel accès		✓	✓		Personnaliser les règles & rapports par défaut **
7.2 Etablir un mécanisme pour les systèmes avec les utilisateurs multiples qui limite l'accès selon le besoin d'utilisateur et empêche tout accès qui n'est pas spécifiquement autorisé		✓	✓		Personnaliser les règles & rapports par défaut **
<b>Condition 8: Assigner une identification unique à chaque personne ayant l'accès par ordinateur</b>					
8.5 Assurer l'authentification et la gestion appropriées d'utilisateur et de mots de passe pour les utilisateurs et les administrateurs sans contact avec les consommateurs					
8.5.1 Contrôler l'ajout, la suppression ou la modification d'identification d'utilisateur, de privilèges et d'autres paramètres d'identification		✓	✓		Règles et rapports par défaut
8.5.2 Vérifier l'identité d'utilisateur avant d'effectuer l'initialisation des mots de passe		✓	✓		Règles et rapports par défaut
8.5.3 Assigner aux utilisateurs un mot de passe unique d'accès qui est modifié après le premier usage		✓			Rapports par défaut
8.5.4 Retirer immédiatement le droit d'accès à tous les utilisateurs révoqués		✓	✓		Règles et rapports par défaut
8.5.5 Supprimer les comptes d'utilisateur inactifs, au moins tous les 90 jours		✓			Rapports par défaut
8.5.6 Activer seulement au besoin, les comptes utilisés par les distributeurs pour l'entretien à distance		✓	✓		Règles et rapports par défaut

Conditions PCI DSS	Vérification rétroactive	Surveillance & Rapports	Alertes	Exécution	Remarque
<b>8.5.13</b> Limiter à six, les tentatives d'accès répétées, par le blocage d'un utilisateur		✓			Rapports par défaut
<b>8.5.16</b> Authentifier tous les accès à toute base de données contenant des données de propriétaires de carte		✓	✓		Règles et rapports par défaut
<b>Condition 10: Traquer et surveiller tous les accès aux ressources de réseau et aux données de propriétaires de carte</b>					
<b>10.1</b> Enregistrer l'accès des utilisateurs et des administrateurs en particulier aux composants du système	✓	✓			Personnaliser les règles & rapports par défaut **
<b>10.2</b> Activer la vérification rétrospective automatique de tout le système pour reconstituer ces événements :					
<b>10.2.1</b> Tous les accès individuels aux données de propriétaires de carte	✓	✓		✓	Personnaliser les règles & rapports par défaut **
<b>10.2.2</b> Toutes les mesures prises par un individu ayant des droits d'accès 'root' ou d'administrateur	✓	✓		✓	Règles par défaut
<b>10.2.3</b> Accès à tous les éléments de vérification rétrospective	✓	✓		✓	Règles et rapports par défaut
<b>10.2.4</b> Tentatives d'accès invalides	✓	✓		✓	Règles et rapports par défaut
<b>10.2.5</b> Utilisation de mécanismes d'identification et d'authentification	✓	✓		✓	Règles et rapports par défaut
<b>10.2.6</b> Initialisation des enregistrements des vérification	✓	✓		✓	Règles et rapports par défaut
<b>10.2.7</b> Création et suppression d'éléments au niveau du système	✓	✓		✓	Règles et rapports par défaut
<b>10.3</b> Enregistrer les détails d'apurement de tous les événements liés aux composants du système	✓			✓	
<b>10.4</b> Synchroniser toutes les principales horloges et l'heure du système		✓	✓		Règles par défaut
<b>10.5</b> Sécuriser les dossiers d'apurement afin qu'ils ne puissent pas être modifiés					
<b>10.5.1</b> Limiter l'accès et l'affichage dossiers de vérification à ceux dont la tâche l'exige		✓	✓		Règles et rapports par défaut
<b>10.5.2</b> Protéger les fichiers de vérification contre les modifications non autorisées		✓	✓		Règles et rapports par défaut
<b>10.5.5</b> Utiliser un logiciel de contrôle de l'intégrité et de détection de changements pour assurer que les données existantes ne peuvent pas être modifiées sans générer d'alertes		✓	✓	✓	Règles et rapports par défaut
<b>10.6</b> Passer en revue, au moins chaque jour, les enregistrements de tous les composants de système		✓		✓	Programmer les rapports par défaut
<b>Condition 11: Tester régulièrement la sécurité des systèmes et des processus</b>					
<b>11.1</b> Tester chaque année les fonctions de sécurité, les restrictions, les connexions au réseau pour assurer la capacité d'identifier adéquatement et d'arrêter toutes tentatives d'accès non autorisé		●	●		
<b>11.4</b> Utiliser des systèmes de détection et de prévention d'intrusion au sein de tout le réseau et sur les machines hôtes pour surveiller le trafic et alerter les responsables en cas de menaces		●	●	●	Créer de nouvelles règles
<b>11.5</b> Déployer un logiciel de contrôle de l'intégrité des fichiers pour alerter le responsable en cas de modifications non autorisées du système central ou du contenu des fichiers			✓	✓	Règles et rapports par défaut

\* Nécessité la création d'une nouvelle règle de traitement d'événement qui ne peut pas exécuter directement cette condition mais supporte les administrateurs grâce aux fonctionnalités de surveillance, rapportage et d'alertes.

\*\* Nécessite la modification des paramètres de configuration des règles et des rapports par défaut en spécifiant les paramètres correspondant à votre environnement de réseau.

#### Légende

✓ Condition entièrement supportée

● Condition supportée partiellement grâce au rapports ou à une adaptation du produit. Certaines conditions pourraient s'appliquer.

**REMARQUE :** Les conditions applicables incluent mais ne sont pas limitées à :

- Windows Security Settings, tels que 'Password Policy' et 'Audit Policy'
- Paramétrages de compte utilisateur
- Installation et configuration appropriée d'autres logiciels et dispositifs, tels que des pare-feu