Prérequis système pour GuardTek Post

29 juin 2018

S'applique à la version 3.5

Compatibilité matérielle/logicielle

GuardTek Post est une application web fonctionnant au sein d'un navigateur internet sur n'importe quel ordinateur capable d'exécuter l'un des navigateurs recommandés ci-dessous et supportant au moins TLS1.1 (**1.2 devraient être privilégié**).

Logiciel	
Système d'exploitation	• Microsoft Windows 10, Windows 8.1, or Windows 7 • Apple Mac OS X 10+ • Google Chrome OS • Linux Ubuntu
Navigateur Internet	Trackforce recommande la dernière version des navigateurs suivants: • Google Chrome • Microsoft Internet Explorer 11 ou Edge L'application peut fonctionner également sur les navigateurs suivants, bien que non recommandés et non testés : • Mozilla Firefox • Apple Safari

Matériel	
Processeur	CPU 32 ou 64 bit
RAM	4 Go de RAM ou plus
Ecran	1 écran avec une résolution minimale de 1280x1024 (full HD, 1920x1080, recommandé)

Réseaux et communications

Les serveurs de GuardTek Post sont situés dans un datacenter dédié et il faut que les firewalls d'entreprises soient configures pour autoriser les connexions sortantes vers ce datacenter avec les paramètres suivants :

Réseau	
Plages d'IP	212.180.59.1 à 212.180.59.31 (ou 212.180.59.0/27) 213.251.58.1 à 213.251.58.15 (ou 213.251.58.0/28) 195.21.138.97 à 195.21.138.111 (ou 195.21.138.96/28)
Ports utilisés	80 (HTTP), 443 (HTTPS), 7200 et 7203 (pour les applications mobiles m-Post et Patrol).
Bande passante	Une connexion internet à 2 Mbps minimum
Protocoles de sécurité	Toutes les communications entre les navigateurs et GuardTek Post sont établies au travers du protocole sécurisé HTTPS. Les navigateurs doivent supporter au minimum TLS1.1 et 1.2 sont recommandés.

Emails

GuardTek Post envoie des emails d'alertes et de rapports à des listes d'utilisateurs prédéterminés. Vous devez vous assurer que tous les serveurs par lesquels transitent ces emails autorisent les emails provenant de nos plages d'IP publiques. Trackforce s'assure que toutes les entrées DNS et SPF liées aux emails sont toujours à jours et correspondent à la réalité.

Videos

GuardTek Post permet l'envoi de vidéos pour certaines fonctions de l'application (les instructions, les rondes & incidents de rondes, les évènements & incidents). Ces vidéos sont envoyées et stockées sur les serveurs S3 d'Amazon pour ne pas encombrer les ressources réseau et disque des serveurs de GuardTek. Pour pouvoir envoyer ces vidéos, les clients doivent s'assurer que leur pare-feu autorisent les urls d'Amazon. A la date d'écriture de ce document, voici les urls à autoriser :

https://s3.amazonaws.com/
https://guardtek-videostore-instructions.s3.us-east-1.amazonaws.com/

Restriction d'accès

L’accès à GuardTek Post peut être restreint par les mécanismes suivants :

Autorisation	
Login/mot de passe	C’est le mécanisme par défaut et ne peut être désactivé. Chaque utilisateur doit avoir un login et un mot de passe valides pour se connecter.
Planning	Les utilisateurs peuvent être restreints à certaines plages horaires de connexion (correspondant à leur planning de travail journalier). Ceci est optionnel.
Client Digital Certificate	Un certificat client (voir Client Certificate) peut être installé sur les ordinateurs à autoriser et les utilisateurs peuvent se voir empêcher la connexion sans certificat. Dans ce cas, chaque utilisateur devra sélectionner le certificat du site sur lequel il travaille parmi ceux installés avant de se connecter. Ceci permet d’empêcher les connexions depuis des endroits non autorisé. Cette mesure est optionnelle et n’est généralement activée que pour les agents.
Affectation à un site	Chaque utilisateur est affecté à un ou plusieurs sites dans votre organisation. GuardTek Post ne permet l’accès qu’aux données des sites auxquels l’utilisateur est affecté. Ceci est obligatoire et ne peut être désactivé.