FreeFlow Core, Version 4.0
Août 2014
708P90732

Xerox® FreeFlow® Core
Guide de sécurité

Version du document 1.0, Août 2014

BR10173

Sommaire

Sommaire

1

Suite d'applications FreeFlow Xerox® - Sécurité

Description

Ce document contient des informations liées à la sécurité pour FreeFlow Core.

Pour Xerox, les problèmes de sécurité sont une priorité. Leader dans le développement de la technologie numérique, Xerox s'est engagé à protéger les informations numériques en identifiant les vulnérabilités potentielles et en les résolvant à l'avance afin de limiter les risques. Xerox s'efforce de fournir les produits logiciels les plus sécurisés possible en fonction des informations et des technologies disponibles, tout en maintenant les performances, la valeur, la fonctionnalité et la productivité de ses produits. La sécurité des composants de FreeFlow est évaluée à l'aide d'outils d'analyse disponibles sur le marché. Les vulnérabilités de l'application sont corrigées en fonction des résultats de nos analyses internes.

Activation et configuration du pare-feu

Il est recommandé d'activer un pare-feu sur le serveur FreeFlow Core. Les ports doivent être bloqués s'ils ne sont pas requis pour une fonction spécifique tel qu'indiqué ci-dessous :

Port	Protocole ou Application	Fonction FreeFlow Core activée
80	HTTP	Trafic entrant : démarrage de l'interface utilisateur FreeFlow Core Trafic sortant : récupération des fichiers répertoriés dans les préréglages du manifeste ou des composants

Port	Protocole ou Application	Fonction FreeFlow Core activée
161, 162	SNMP	Trafic sortant : identification du type de DFE lors de la configuration de l'imprimante
631	IPP	Trafic sortant : soumission de travaux aux DFE
25, 2525, 465, 475, 587	SMTP	Trafic sortant : envoi de notifications par courrier électronique Remarque : le numéro de port requis dépend de la configuration du serveur SMTP.
TCP, UDP : 7751	JMF	Trafic entrant : réception de requêtes JMF/JDF
Variable	JMF	Trafic sortant : renvoi de signaux d'état JMF. Le client JMF spécifie le numéro de port.
139, 445	SMB	Trafic entrant : partage de dossiers actifs via Partage de fichiers Windows Trafic sortant : utilisation de dossiers actifs sur des répertoires partagés Trafic sortant : récupération des fichiers répertoriés dans le manifeste depuis des répertoires partagés Trafic sortant : récupération des fichiers répertoriés dans les composants depuis des répertoires partagés Trafic sortant : enregistrement dans des répertoires partagés
20, 21	FTP	Trafic entrant : partage de dossiers actifs via FTP Trafic sortant : récupération des fichiers répertoriés dans les préréglages du manifeste ou des composants
443	HTTPS	Trafic entrant : partage de fichiers pour le système FreeFlow Core distant Trafic sortant : récupération de fichiers depuis le système FreeFlow Core distant

Règles du pare-feu Windows

1. Accédez à **Panneau de configuration > Système et sécurité > Pare-feu Windows > Paramètres avancés**.
2. Pour chaque règle requise, sélectionnez **Règles de trafic entrant** ou **Règles de trafic sortant** :
   a) Sous Actions, cliquez sur **Nouvelle règle**. L'Assistant Nouvelle règle de trafic entrant s'affiche.
   b) Cliquez sur **Port** pour Type de règle. Cliquez sur **Suivant**.
   c) Cliquez sur **TCP** ou **UDP** selon les informations indiquées dans le tableau ci-dessus. Entrez une valeur dans Ports locaux spécifiques en fonction du tableau ci-dessus Cliquez sur **Suivant**.
   d) Cliquez sur **Autoriser la connexion**. Cliquez sur **Suivant**.
   e) Sélectionnez toutes les cases. Cliquez sur **Suivant**.

Protection antivirus

Nous avons pris toutes les précautions nécessaires pour vous livrer un logiciel exempt de virus. Nous vous recommandons vivement de vous équiper d'un logiciel de détection de virus approuvé par le secteur informatique. Pour protéger votre système des virus, il est impératif que le logiciel de détection de virus soit constamment mis à jour.

Pour de meilleures performances, nous vous recommandons d'exclure les répertoires d'installation de FreeFlow Core et MS SQL Server des analyses antivirus.

Une autre solution consiste à exclure les dossiers FreeFlow Core suivants de l'analyse antivirus :

- <répertoire d'installation FreeFlow Core>\Platform\Spool
- <répertoire d'installation FreeFlow Core>\Logs
- <répertoire d'installation FreeFlow Core>\Platform\Logs
- <répertoire d'installation FreeFlow Core>\Web\Logs
- <répertoire d'installation FreeFlow Core>\Config
- <répertoire d'installation FreeFlow Core>\Presets

Mise à jour logicielle

Nous recommandons que tous les produits logiciels installés sur le serveur FreeFlow Core soient régulièrement mis à jour. Microsoft Update devrait être exécuté au moins une fois par mois.

Les Service Packs du système d'exploitation ne doivent pas être installés par l'intermédiaire de Microsoft Update tant que leur prise en charge n'est pas annoncée officiellement.

Xerox diffuse des bulletins mensuels recensant, lorsque c'est nécessaire, les mises à jour qu'il serait nécessaire « d'exclure » du système FreeFlow. Ces informations sont également indiquées sur le site Web www.xerox.com/security, à la section « Product Security Guidance » (Guide de sécurité produit). Les mises à jour de sécurité haute priorité sont essentielles et doivent impérativement être installées, sauf indication contraire.