Version 8.0
708P89670
Octobre 2009

# FreeFlow®
# Guide de sécurité

Préparé par :
Xerox Corporation
Global Knowledge and Language Services
800 Phillips Road - Bldg. 218-01A
Webster, NY 14580

Traduit par :
Xerox
GKLS European Operations
Bessemer Road
Welwyn Garden City
Hertfordshire
AL7 1BU
Royaume-Uni

# Table des matières


1 Suite d'applications FreeFlow - Sécurité ..... 1-1

Présentation ..... 1-1
Mesures de sécurité recommandées ..... 1-2
Sécurité du réseau ..... 1-2
Paramètres de pare-feu ..... 1-8
Attribution de nouveaux numéros de port ..... 1-13
Impression RDO vers le serveur d'impression FreeFlow ..... 1-14
Emplacement et accès physiques ..... 1-14
Sécurité du système / système d'exploitation ..... 1-15
Stratégie de gestion des correctifs pour FreeFlow ..... 1-15
Paramètres d'Internet Explorer ..... 1-15
Désactivation des services superflus ..... 1-16
Protection antivirus ..... 1-16
Mesures de protection antivirus ..... 1-16
Recommandations relatives à McAfee VirusScan pour FreeFlow Output Manager ..... 1-17
Recommandations relatives à McAfee VirusScan pour FreeFlow Process Manager ..... 1-18
Authentification de l'utilisateur et gestion de compte ..... 1-20

# 1 Suite d'applications FreeFlow - Sécurité

## Présentation

Ce document décrit les rôles, les responsabilités et les meilleures pratiques en matière de sécurité, ainsi que les paramètres de sécurité recommandés pour FreeFlow - Capture et mise en forme, FreeFlow Process Manager, Standalone FreeFlow Print Manager - Chemin d'impression avancé, FreeFlow Print Manager, FreeFlow JMF Service, FreeFlow Express to Print et FreeFlow Output Manager.

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 traitant à l'avance afin de limiter les risques. Xerox s'efforce de fournir le produit logiciel le plus sécurisé possible en fonction des informations et des technologies disponibles, tout en maintenant les performances, la valeur, la fonctionnalité et la productivité des produits. Les composants de FreeFlow sont soumis à des tests de conformité aux normes de sécurité, selon des outils d'analyse disponibles sur le marché. Les points faibles de l'application sont renforcés en fonction des résultats de nos analyses internes.

Après le lancement d'un produit, Xerox diffuse des bulletins mensuels recensant éventuellement les mises à jour Microsoft qu'il est nécessaire « d'exclure » du système FreeFlow. Xerox vérifie également les notes d'alertes publiées par le Cert US afin de déterminer leur pertinence pour les produits Xerox.

Bien que Xerox mette tout en œuvre pour fournir un logiciel sécurisé, il incombe au client de sécuriser son environnement en fonction de ses besoins spécifiques. En raison de la diversité de nos clients et de la richesse des flux de production qu'ils utilisent, il est impossible de fournir une solution unique qui soit à même de satisfaire le large éventail de besoins de ces clients en matière de sécurité. Certains clients, par exemple, exigent un niveau de sécurité extrêmement élevé prenant en charge un seul protocole d'impression et un seul compte opérateur système, mais ce n'est pas le cas de tous les clients. Xerox livre des produits offrant des configurations de sécurité standard et la possibilité de modifier ces configurations en fonction des besoins du client. La configuration sur site est censée être effectuée par l'administrateur système chargé de la gestion des plates-formes produit chez le client. Les activités de configuration de la sécurité doivent tenir compte de la nécessité de réduire au minimum les risques sécuritaires tout en permettant l'activation des protocoles nécessaires à la prise en charge des flux de production stratégiques du client. En fonction de ses besoins individuels, le client peut renforcer la sécurité par le biais dun pare-feu ou la mise en place un réseau privé. Il peut également renforcer le système d'exploitation afin de satisfaire à certains critères de conformité et/ou restreindre l'accès physique à son matériel informatique/réseau. Le client, également en fonction de ses besoins, peut utiliser des outils de supervision et de consignation de l'accès physique et réseau au logiciel FreeFlow, afin de déterminer si un incident de sécurité s'est produit. Le client doit également sauvegarder ses données afin de s'assurer qu'elles peuvent être récupérées en cas de suppression ou d'altération.

# Mesures de sécurité recommandées

Les systèmes les plus sûrs ne sont pas invulnérables aux attaques des personnes ayant le temps, les connaissances et l'accès nécessaires pour une opération de piratage. Parmi les menaces possibles, on compte notamment la détérioration physique du système et des réseaux ou les dommages occasionnés par des virus. Le but consiste à minimiser les risques et à établir des politiques de détection des effets négatifs d'une brèche de sécurité.

Pour obtenir un environnement sécurisé, il est recommandé d'appliquer la stratégie en 5 niveaux suivante :

- Sécurité du réseau
- Emplacement et accès physiques
- Sécurité du système / système d'exploitation
- Protection antivirus
- Authentification de l'utilisateur et gestion du mot de passe

# Sécurité du réseau

La première étape dans la mise en œuvre d'un modèle de sécurité concerne le réseau. Il s'agit en effet du point d'entrée de tout environnement avec serveur et l'emplacement où les données sensibles sont transmises d'un système à un autre. Des mécanismes de contrôle doivent absolument être mis en place pour prévenir toute intrusion et toute attaque.

Le tableau ci-après indique les paramètres de port requis pour le pare-feu du matériel ou le pare-feu Windows avec FreeFlow.

> Remarque
>
> Tous les ports requièrent des communications entrantes et sortantes, sauf indication contraire. Le pare-feu Windows n'interdit pas les communications sortantes ; il n'est donc pas nécessaire d'y ouvrir les ports marqués pour les communications sortantes uniquement.

Remarque

La conversion automatique des fichiers Adobe Illustrator et InDesign sur un Workflow Submission Client éloigné exige la désactivation du pare-feu Windows.

**Tableau 1-1. Paramètres de port requis pour le pare-feu du matériel ou le pare-feu Windows**

| PORT | Protocole ou Application | Requis pour FreeFlow Capture et mise en forme | Requis pour FreeFlow Print Manager Chemin d'impression avancée (version autonome) | Requis pour FreeFlow Express to Print | Requis pour les serveurs FreeFlow Process Manager | Requis pour les clients FreeFlow Process Manager | Requis pour FreeFlow Print Manager | Requis pour FreeFlow Output Manager | Requis pour FreeFlow Service JMF |
|---|---|---|---|---|---|---|---|---|---|
| 21 | FTP | Non | Non | Non | Oui | Non | Non | Oui, communications sortantes vers FreeFlow Printer Server pour le Module de comptabilité ; communications entrantes à partir de périphériques multifonctions si la fonction Envoyer à la production est activée. | Non |

**Tableau 1-1. Paramètres de port requis pour le pare-feu du matériel ou le pare-feu Windows**

| PORT | Protocole ou Application | Requis pour FreeFlow Capture et mise en forme | Requis pour FreeFlow Print Manager Chemin d'impression avancée (version autonome) | Requis pour FreeFlow Express to Print | Requis pour les serveurs FreeFlow Process Manager | Requis pour les clients FreeFlow Process Manager | Requis pour FreeFlow Print Manager | Requis pour FreeFlow Output Manager | Requis pour FreeFlow Service JMF |
|---|---|---|---|---|---|---|---|---|---|
| 22 | SSH/sFTP | Oui, communications sortantes uniquement vers le serveur d'impression FreeFlow, Sécurité élevée activée | Oui, communications sortantes uniquement vers le serveur d'impression FreeFlow, Sécurité élevée activée | Oui, communications sortantes uniquement vers le serveur d'impression FreeFlow, Sécurité élevée activée | Oui | Non | Oui, communications sortantes uniquement vers le serveur d'impression FreeFlow, Sécurité élevée activée | Oui, communications sortantes uniquement vers le serveur d'impression FreeFlow pour le Module de comptabilité | Non |
| 25 | SMTP | Non | Non | Non | Oui, communications sortantes uniquement | Non | Non | Non | Non |
| 80 | HTTP ou numéro de port réaffecté | Non | Non | Non | Non | Non | Non | Oui sur Creo | Oui sur Creo |
| 135 | RPC End Point Mapper | Non | Non | Non | Oui | Non | Non | Non | Non |
| 443 | SSL/TLS<br><br>HTTPs (pour WS) | Oui, communications sortantes uniquement vers le serveur d'impression FreeFlow, Sécurité élevée activée | Oui, communications sortantes uniquement vers le serveur d'impression FreeFlow, Sécurité élevée activée | Oui, communications sortantes uniquement vers le serveur d'impression FreeFlow, Sécurité élevée activée | Oui, communications sortantes uniquement vers le serveur d'impression FreeFlow, Sécurité élevée activée | Non | Oui, communications sortantes uniquement vers le serveur d'impression FreeFlow, Sécurité élevée activée | Oui, communications sortantes uniquement vers le serveur d'impression FreeFlow, Sécurité élevée activée | Oui, communications sortantes uniquement vers le serveur d'impression FreeFlow, Sécurité élevée activée |

**Tableau 1-1. Paramètres de port requis pour le pare-feu du matériel ou le pare-feu Windows**

| PORT | Protocole ou Application | Requis pour FreeFlow Capture et mise en forme | Requis pour FreeFlow Print Manager Chemin d'impression avancée (version autonome) | Requis pour FreeFlow Express to Print | Requis pour les serveurs FreeFlow Process Manager | Requis pour les clients FreeFlow Process Manager | Requis pour FreeFlow Print Manager | Requis pour FreeFlow Output Manager | Requis pour FreeFlow Service JMF |
|---|---|---|---|---|---|---|---|---|---|
| 631 | IPP | Oui, communications sortantes uniquement vers le serveur d'impression FreeFlow, Sécurité élevée désactivée | Oui, communications sortantes uniquement vers le serveur d'impression FreeFlow, Sécurité élevée désactivée | Oui, communications sortantes uniquement vers le serveur d'impression FreeFlow, Sécurité élevée activée | Oui, communications sortantes uniquement vers le serveur d'impression FreeFlow, Sécurité élevée désactivée | Non | Oui, communications sortantes uniquement vers le serveur d'impression FreeFlow, Sécurité élevée désactivée | Oui | Oui |
| 515 (ou plage 513 - 1023) | LPR | Oui, communications sortantes uniquement | Oui, communications sortantes uniquement | Oui, communications sortantes uniquement | Oui, communications sortantes uniquement | Non | Oui, communications sortantes uniquement | Oui | Oui |
| 1521 | Oracle Listener | Non | Non | Non | Oui | Non | Non | Non | Non |
| 8080 | HTTP | Non | Non | Non | Non | Non | Non | Oui, communications entrantes uniquement | Non |
| 8443 | HTTPs | Non | Non | Non | Non | Non | Non | Oui, communications entrantes uniquement | Non |
| 5000 - 5024 | Clients de soumission de flux de travail | Non | Non | Non | Oui | Oui | Non | Non | Non |

**Tableau 1-1. Paramètres de port requis pour le pare-feu du matériel ou le pare-feu Windows**

| PORT | Protocole ou Application | Requis pour FreeFlow Capture et mise en forme | Requis pour FreeFlow Print Manager Chemin d'impression avancée (version autonome) | Requis pour FreeFlow Express to Print | Requis pour les serveurs FreeFlow Process Manager | Requis pour les clients FreeFlow Process Manager | Requis pour FreeFlow Print Manager | Requis pour FreeFlow Output Manager | Requis pour FreeFlow Service JMF |
|---|---|---|---|---|---|---|---|---|---|
| 5025 - 5049 | Gestionnaire de travaux | Non | Non | Non | Oui | Oui | Non | Non | Non |
| 5050 | Workflow Builder | Non | Non | Non | Oui | Non | Non | Non | Non |
| 6789 | Serveur de base de données de flux de travail | Non | Non | Non | Oui | Non | Non | Non | Non |
| 7890 | Gestionnaire de tâches de flux de travail | Non | Non | Non | Oui | Non | Non | Non | Non |
| 8053 | Workflow Folder Monitor | Non | Non | Non | Oui | Non | Non | Non | Non |
| 7779 | Port d'écoute JMF | Non | Non | Non | Oui | Non | Non | Non | Non |
| 7781 | Port d'écoute JMF | Non | Non | Non | Non | Non | Non | Oui | Oui |
| 8090 | Connecteur de référentiel | Oui, avec connecteur de référentiel | Non | Non | Oui, avec connecteur de référentiel | Non | Non | Oui, avec connecteur de référentiel | Non |
| 8091 | Connecteur de référentiel avec SSL | Oui, avec connecteur de référentiel | Non | Non | Oui, avec connecteur de référentiel | Non | Non | Oui, avec connecteur de référentiel | Non |

**Tableau 1-1. Paramètres de port requis pour le pare-feu du matériel ou le pare-feu Windows**

| PORT | Protocole ou Application | Requis pour FreeFlow Capture et mise en forme | Requis pour FreeFlow Print Manager Chemin d'impression avancée (version autonome) | Requis pour FreeFlow Express to Print | Requis pour les serveurs FreeFlow Process Manager | Requis pour les clients FreeFlow Process Manager | Requis pour FreeFlow Print Manager | Requis pour FreeFlow Output Manager | Requis pour FreeFlow Service JMF |
|---|---|---|---|---|---|---|---|---|---|
| 7117 | Common Printer Admin Service (Service d'administration des imprimantes communes) | Oui | Oui | Oui | Oui | Non | Oui | Oui | Oui |
| 9090 | HTTP pour le Module de comptabilité de FreeFLow | Non | Non | Non | Non | Non | Non | Oui, communications entrantes uniquement | Non |
| 9443 | HTTP pour le service de comptabilité de FreeFlow avec SSL | Non | Non | Non | Non | Non | Non | Oui, communications entrantes uniquement | Non |
| 4004 | Port du service d'autorisation | Oui, avec CMS | Non | Non | Oui | Oui, communications sortantes uniquement | Non | Oui | Oui |
| 5640 | Service de métadonnées utilisateur | Non | Non | Non | Oui | Oui, communications sortantes uniquement | Non | Non | Non |
| 57891 | FreeFlow Template Manager | Non | Non | Oui | Non | Non | Non | Non | Non |
| 55682 | FreeFlow Express to Print | Non | Non | Oui | Non | Non | Non | Non | Non |

# Paramètres de pare-feu

## Pare-feu matériel

Pour protéger le réseau, un ensemble de contrôles matériels et logiciels est recommandé, qui comprend un routeur, un commutateur et un pare-feu. Lorsqu'ils sont configurés correctement, ces outils filtrent et bloquent le trafic non sollicité. Dans le cas contraire, ils risquent de bloquer le trafic entrant souhaité.

Les tableaux suivants fournissent des informations sur la configuration requise pour les ports lors de l'utilisation des flux de travaux/applications FreeFlow. Ces ports doivent être ouverts dans le pare-feu matériel pour que le trafic puisse passer du serveur au réseau Internet. Par défaut, FreeFlow désactive tous les services et protocoles inutilisés.

Le tableau ci-après présente les paramètres de port requis pour les systèmes DFE équipés d'un serveur d'impression FreeFlow.

**Tableau 1-2. Paramètres de port pour les systèmes DFE équipés d'un serveur d'impression FreeFlow**

| PORT | Protocole ou Application | Requis pour le serveur d'impression FreeFlow lors de l'impression éloignée à partir de FreeFlow ou de la communication avec Output Manager | | Requis pour le serveur d'impression FreeFlow pour les services de décomposition de l'agent réseau | |
|---|---|---|---|---|---|
| | | Sécurité élevée activée | Sécurité élevée désactivée | Sécurité élevée activée | Sécurité élevée désactivée |
| 21 | FTP | Non | Oui | Non | Oui |
| 631 | IPP | Non | Oui | Non | Oui |
| 22 | SSH/s FTP | Oui | Non | Oui | Non |
| 443 | SSL/TLS | Oui | Non | Oui | Non |
| 515 (ou plage 513 - 1023) | LPR | Non | Oui | Non | |
| 111 | RPC | Non | Non | Oui pour le serveur d'impression FreeFlow < 3.6 | |

Le tableau ci-après présente les paramètres de port requis pour les différents serveurs, à l'exclusion du serveur d'impression FreeFlow.

**Tableau 1-3. Paramètres de port requis pour les différents serveurs, serveur d'impression FreeFlow non inclus**

| PORT | Protocole ou Application | Requis pour les DFE suivants :<br>EFI<br>Creo<br>DocuCentre<br>WorkCentre<br>AccXES<br>Scanvec Amiable | Requis pour les DFE suivants<br>GXP 4110<br>NPS Server<br>DT Network Server<br>NS Plus<br>NS + Server Series |
|---|---|---|---|
| 21 | FTP | Non | Oui |
| 631 | IPP | Oui, pour toutes les imprimantes EFI IPP | Non |
| 22 | SSH/s FTP | Non | Non |
| 443 | SSL/TLS | Non | Non |
| 515<br>(ou plage 513 - 1023) | LPR | Oui | Oui |
| 135 | RPC | Oui, EFI uniquement | Non |
| 80 | HTTP | Oui (Creo uniquement) | Non |
| 161 | SNMP | Oui (DocuCentre, WorkCentre uniquement) | Oui (GXP 4110 uniquement) |
| 162 | SNMP | Oui (EFI uniquement) | |

## Pare-feu Windows

Sur le système FreeFlow, le pare-feu Windows est DÉSACTIVÉ par défaut pour la version de base Windows Server 2008 et Windows Vista et pour Windows 7 ; il est ACTIVÉ par défaut pour les systèmes d'exploitation Windows Server 2008 et Windows Vista.

Pour configurer le pare-feu Windows sur un système FreeFlow :

1. Ouvrez le Panneau de configuration
2. Sélectionnez [**Pare-feu Windows**].

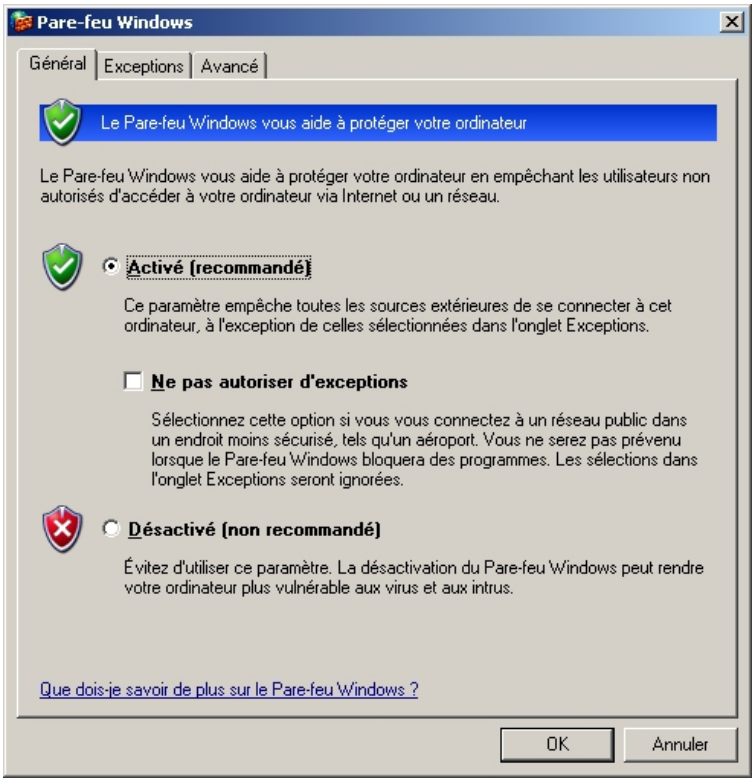


**Figure 1-1 : Boîte de dialogue Pare-feu Windows**

3. Pour activer le pare-feu Windows, sélectionnez la case d'option [**Activé**].
4. Pour désactiver le pare-feu Windows, sélectionnez la case d'option [**Désactivé**].
5. Sélectionnez l'onglet **Exceptions**.
6. Ajoutez les programmes et ports relatifs au pare-feu Windows suivants pour chaque configuration appropriée :
   a. Sélectionnez [**Ajouter un port**] pour ajouter les ports applicables. Entrez le nom approprié (défini par l'utilisateur) et le numéro de port. Pour la liste des ports requis pour chaque configuration, reportez-vous au tableau, 1-1 Paramètres de port requis pour le pare-feu du matériel ou le pare-feu Windows.

      Remarque

      Le pare-feu Windows n'interdit pas les communications sortantes ; il n'est donc pas nécessaire d'y ajouter les ports marqués pour les communications sortantes uniquement.

   b. Sélectionnez [**Ajouter des programmes**] pour ajouter les exceptions applicables à chaque configuration. Reportez-vous au tableau 1-4 Exceptions du pare-feu Windows requises à la page 11 pour la liste des programmes requis pour chaque configuration.

Si vous utilisez le pare-feu Windows, le tableau ci-après présente les exceptions du pare-feu Windows requises pour chaque configuration.

Remarque

Tous les ports requièrent des communications entrantes et sortantes, sauf indication contraire.

Remarque

Lors de l'utilisation du nœud Conversion dans Process Manager, la communication « partage de fichiers et d'imprimantes » doit être autorisée. Ceci peut être ajouté sous forme d'exception de pare-feu Windows. Pour un pare-feu matériel, les ports TCP/139 et TCP/445 doivent être ouverts.

**Tableau 1-4. Exceptions du pare-feu Windows requises**

| PORT / Exception | Client FreeFlow - Capture et mise en forme | FreeFlow Print Manager - Chemin d'impression avancée (version autonome) | Requis pour FreeFlow Express to Print | FreeFlow Process Manager Serveur | Client FreeFlow Process Manager | FreeFlow Print Manager | FreeFlow Output Manager | Services JMF FreeFlow |
|---|---|---|---|---|---|---|---|---|
| C:\Windows\System32\Dllhost.exe | Non | Non | Non | Oui | Non | Non | Non | Non |
| C:\Windows\System32\msdtc.exe | Non | Non | Non | Oui | Non | Non | Non | Non |
| FreeFlow - Capture et mise en forme (DSMR.exe) | Oui | Non | Non | Non | Non | Non | Non | Non |
| ScanAndPrint.exe | Oui | Non | Non | Non | Non | Non | Non | Non |
| Gestionnaire de fichiers (DPFileManager.exe) | Oui | Non | Non | Oui | Non | Non | Non | Non |
| Workflow Builder (WFBuilder.exe) | Non | Non | Non | Oui | Non | Non | Non | Non |
| Workflow - Soumission Client distant (WFSubmissionClient.exe) | Non | Non | Non | Oui | Oui | Non | Non | Non |
| Workflow - Client de gestion des travaux distant (WFJobManager.exe) | Non | Non | Non | Oui | Oui | Non | Non | Non |
| Enregistrement des imprimantes (Print Registration.exe) | Non | Non | Non | Oui | Non | Non | Non | Non |
| Outil d'administration FreeFlow (E:\FreeFlow\FFAdminTool.exe) | Oui | Non | Non | Oui | Non | Non | Non | Non |
| Agent réseau (NaAdmin.exe) | Oui | Non | Non | Oui | Non | Non | Non | Non |

**Tableau 1-4. Exceptions du pare-feu Windows requises**

| PORT / Exception | Client FreeFlow - Capture et mise en forme | FreeFlow Print Manager - Chemin d'impression avancée (version autonome) | Requis pour FreeFlow Express to Print | FreeFlow Process Manager Serveur | Client FreeFlow Process Manager | FreeFlow Print Manager | FreeFlow Output Manager | Services JMF FreeFlow |
|---|---|---|---|---|---|---|---|---|
| C:\Program Files\Texas Imperial\WFTPD Pro.exe | Oui | Non | Non | Non | Non | Non | Non | Non |
| Acrobat.exe | Non | Non | Non | Non | Non | Non | Non | Non |
| Print Manager - Chemin d'impression avancée (FFPMPro.exe) | Oui | Oui | Non | Oui | Non | Non | Non | Non |
| FreeFlow Easy to Print (FreeFlowEZ.exe) | Non | Non | Oui | Non | Non | Non | Non | Non |
| Partage de fichiers et d'imprimantes | Non | Non | Non | Oui | Non | Non | Non | Non |

# Attribution de nouveaux numéros de port

Les procédures suivantes permettent d'attribuer de nouveaux numéros de port dans les applications FreeFlow Connecteur de référentiel et FreeFlow Output Manager.

### Attribution de nouveaux numéros aux ports du Connecteur de référentiel

Pour attribuer de nouveaux numéros aux ports du Connecteur de référentiel :

1. Connectez-vous au poste de travail en tant qu'administrateur.
2. Sur le bureau de Windows, cliquez avec le bouton droit sur [**Poste de travail**] et sélectionnez [**Gérer**].
3. Développez [**Services et applications**].
4. Développez [**Gestionnaire des services Internet (IIS)**].
5. Développez [**Sites Web**].
6. Cliquez avec le bouton droit sur [**Repository Management Service (Service de gestion des espaces d'archivage)**] et sélectionnez [**Propriétés**].
7. Modifiez le numéro du [**port TCP**] et/ou du [**port SSL**] et sélectionnez [**OK**].

### Attribution de nouveaux numéros de port dans FreeFlow Output Manager

Pour modifier les ports HTTP ou HTTPs dans FreeFlow Output Manager :

1. Ouvrez le fichier **web.xml** dans le Bloc-notes.

   Ce fichier se trouve dans le dossier **<Dossier d'installation de FreeFlowOutput Manager>\jakarta-tomcat\webapps\WebClient\WEB-INF**.

   Exemple : c:\Program Files\Xerox\FreeFlow Output Manager\jakarta-tomcat-5.0.28\webapps\WebClient\WEB-INF/web.xml
2. Dans la section **<app-web>/<servlet>** du fichier, recherchez les entrées suivantes :
   - <init-param> <param-name>**HttpPort**</param-name> <param-value>**8080** <param-value> </init-param>
   - <init-param> <param-name>**HttpsPort**</param-name> <param-value>**8443** <param-value> </init-param>
3. Remplacez la valeur des paramètres **HttpPort** et **HttpsPort** par les valeurs appropriées.
4. Enregistrez le fichier et fermez le Bloc-notes.

### Modification des numéros de port dans le Module de comptabilité de FreeFlow

Pour modifier le port FTP dans la fonction Envoyer à la production de FreeFlow Output Manager :

1. Modifiez le fichier FtpSpooler.properties à l'aide du Bloc-notes. Ce fichier se trouve dans le dossier <Dossier d'installation de FreeFlow Output Manager>\config. Exemple : c:\Program Files\Xerox\FreeFlow Output Manager\config\FtpSpooler.properties
2. Remplacez la valeur du paramètre configurableFTPport par la valeur appropriée.
3. Enregistrez le fichier et fermez le Bloc-notes.

Pour modifier les ports HTTP ou HTTPs dans le Module de comptabilité de FreeFlow :

1. Ouvrez le fichier de propriétés **tomcat** dans le Bloc-notes.

   Ce fichier se trouve dans le dossier **c:\Program Files\Xerox\FreeFlow Accounting Module\config**.
2. Remplacez la valeur des paramètres **HttpPort** et **HttpsPort** par les valeurs appropriées.
3. Enregistrez le fichier et fermez le Bloc-notes.

**Pour modifier le numéro de port dans la fonction Envoyer à la production de FreeFlow Output Manager :**

1. Modifiez le fichier FtpSpooler.properties à l'aide du Bloc-notes. Ce fichier se trouve dans le dossier <Dossier d'installation de FreeFlow Output Manager>\config. Exemple : c:\Program Files\Xerox\FreeFlow Output Manager\config\FtpSpooler.properties
2. Remplacez la valeur du paramètre configurableFTPport par la valeur appropriée.
3. Enregistrez le fichier et fermez le Bloc-notes.

## Impression RDO vers le serveur d'impression FreeFlow

Pour permettre l'impression RDO vers le serveur d'impression FreeFlow tout en ayant activé le pare-feu Windows, désactivez le service de passerelle de la couche Application.

Pour désactiver le service de passerelle de la couche applicative :

1. Connectez-vous au poste de travail en tant qu'administrateur.
2. Sur le bureau de Windows, cliquez avec le bouton droit sur [**Poste de travail**].
3. Sélectionnez [**Gérer**].
4. Développez [**Services et applications**].
5. Sélectionnez [**Services**].
6. Cliquez deux fois sur [**Service de la passerelle de la couche Application**].
7. S'il est en cours d'exécution, interrompez le service en sélectionnant [**Arrêter**].
8. Dans la liste déroulante Type de démarrage, sélectionnez [**Désactivé**].
9. Sélectionnez [**Appliquer**].
10. Sélectionnez [**OK**].

# Emplacement et accès physiques

La seconde étape pour obtenir un système plus sécurisé consiste à restreindre l'accès physique aux systèmes et aux données. Tout accès physique aux systèmes ou aux données peut compromettre la sécurité du système.

Il est recommandé de ranger le matériel dans un endroit d'accès réservé aux personnes spécialement autorisées.

# Sécurité du système / système d'exploitation

La troisième étape pour obtenir un système plus sécurisé consiste à s'assurer que le système est mis à jour avec les correctifs correspondant aux vulnérabilités identifiées. Il est également impératif de télécharger des mises à jour très régulièrement.

## Stratégie de gestion des correctifs pour FreeFlow

La stratégie de gestion des correctifs Microsoft pour FreeFlow est la suivante :

- Il est recommandé d'exécuter le service de mise à jour Microsoft Update chaque semaine.
- Les Service Packs du système d'exploitation ne doivent pas être installés par l'intermédiaire de Microsoft Update jusqu'à communication formelle du support.
- Xerox diffuse des bulletins mensuels recensant éventuellement les mises à jour qu'il est 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 haute priorité relatives à la sécurité sont importantes et doivent impérativement être installées, sauf indication contraire.

## Paramètres d'Internet Explorer

Le renforcement de la sécurité du système d'exploitation Windows met en œuvre des paramètres supplémentaires relatifs à Internet Explorer La configuration par défaut sous Windows empêche la plupart des fenêtres contextuelles de s'afficher sur la page Web active.
Il peut toutefois s'avérer nécessaire de désactiver le bloqueur de fenêtre publicitaire intempestive.

Pour désactiver le bloqueur de fenêtre publicitaire intempestive :

1. Ouvrez Internet Explorer.
2. Sélectionnez [**Outils: Bloqueur de fenêtre publicitaire intempestive: Désactiver le bloqueur de fenêtres publicitaires intempestives**].
3. Sélectionnez [**Fichier: Fermer**] pour quitter le navigateur.

Le bloqueur ne bloque pas les fenêtres provenant des sites Web se trouvant sur votre intranet local ou sur la liste des sites autorisés. Pour accéder à un site placé à l'extérieur de votre intranet, vous devez changer les paramètres du bloqueur afin d'autoriser l'accès à l'adresse du site en question.

Pour modifier les paramètres du bloqueur :

1. Ouvrez Internet Explorer.
2. Si le bloqueur est désactivé, vous devez l'activer avant de pouvoir en modifier les paramètres. Si nécessaire, sélectionnez [**Outils: Bloqueur de fenêtre publicitaire intempestive: Activer le bloqueur de fenêtres publicitaires intempestives**].
3. Sélectionnez [**Outils: Bloqueur de fenêtre publicitaire intempestive: Paramètres du bloqueur de fenêtres publicitaires intempestives**].
4. Entrez l'adresse ou l'URL du site Web à autoriser, puis sélectionnez [**Ajouter**].
5. Sélectionnez [**Fermer**].
6. Sélectionnez [**Fichier: Fermer**] pour quitter le navigateur.

**Vérification du site Web de Microsoft**

Consultez le site www.microsoft.com pour d'autres suggestions concernant le système de sécurité.

## Désactivation des services superflus

Pour optimiser la sécurité du système, désactivez les services suivants via le Panneau de configuration :

1. Sélectionnez [**Démarrer: Paramètres: Panneau de configuration**] sur le bureau Windows.
2. Sélectionnez [**Outils d'administration: Services**].
3. Désactivez les services suivants :
   - Explorateur d'ordinateurs
   - Client de suivi de lien distribué
   - Serveur de suivi de lien distribué

   Remarque
   Applicable à un système d'exploitation serveur uniquement.

   - Accès à distance au Registre
4. Fermez le Panneau de configuration.

# Protection antivirus

La quatrième étape pour maintenir une sécurité supérieure des systèmes consiste à utiliser un logiciel de détection de virus.

## Mesures de 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 afin de continuer à protéger votre système contre les virus.

Remarque
C'est en effet au client que revient en définitive la responsabilité de protéger son système contre les virus.

Il est préférable d'utiliser des applications de détection et de contrôle des virus approuvées par le secteur informatique.

Afin d'améliorer les performances, il est recommandé d'exclure les éléments suivants de la vérification antivirus :

- Fichiers TIF, RDO et fichiers journaux.
- C:\DSEXCHNG.DIR sur les systèmes Capture et mise en forme

Parmi les applications de détection et de contrôle de virus les plus courantes, on compte :

- Norton Anti-Virus de Symantec
- McAfee VirusScan de Network Associates, Inc.

  Remarque

  Pour être efficaces et garantir une protection contre les nouveaux virus, ces logiciels doivent être mis à jour régulièrement.

Il est fortement conseillé de suivre les recommandations ci-après pour éviter toute contamination du système :

- Exécutez un programme de détection de virus régulièrement (au moins une fois pas semaine) sur l'ensemble des systèmes.
- Si vous détectez un virus sur un système, supprimez le fichier infecté. Récupérez ensuite le fichier à l'aide de la fonction de restauration.

  Remarque

  Cette procédure a pour but d'éviter une altération des données sur le poste de travail à la suite de l'élimination d'un virus.

Vous pouvez ensuite supprimer le virus en appliquant les procédures décrites par votre logiciel antivirus.

## Recommandations relatives à McAfee VirusScan pour FreeFlow Output Manager

Si vous utilisez McAfee VirusScan avec votre système FreeFlow Output Manager, il est recommandé de définir les dossiers à exclure afin d'éviter tout problème lors de l'utilisation d'Output Manager.

Remarque

Si vous utilisez un logiciel antivirus autre que McAfee VirusScan, il est recommandé de définir les dossiers à exclure dans ce logiciel également.

1. Cliquez avec le bouton droit sur [**McAfee VirusScan On-Access Scan**] (Analyse McAfee VirusScan lors de l'accès).
2. Sélectionnez [**VirusScan Console**] (Console VirusScan).
3. Sélectionnez [**Tools: Unlock User Interface**] (Outils: Déverrouiller l'interface utilisateur).

   Remarque

   Si l'option Déverrouiller l'interface utilisateur est estompée, sélectionnez [**Tools: Open Remote Console**] (Outils: Ouvrir la console distante) et sous Connect to Computer (Se connecter à l'ordinateur), entrez l'adresse IP du système Output Manager, puis sélectionnez [OK]. Ceci active l'option Déverrouiller l'interface utilisateur.

   Remarque

   Si un mot de passe est requis, contactez votre administrateur système.

4. Cliquez avec le bouton droit sur [**On-Access Scanner**] (Analyse lors de l'accès) et sélectionnez [**Properties**] (Propriétés).
5. Sélectionnez [**All Processes**] (Tous les processus).

6. Sélectionnez l'onglet **Detection** (Détection).
   a. Sous What not to scan (Éléments à exclure de l'analyse), sélectionnez [**Exclusions**].
   b. Sélectionnez [**Add**] (Ajouter) pour ajouter les exclusions.
   c. Sous What not to scan (Éléments à exclure de l'analyse), sélectionnez [**By name/location**] (Par nom/emplacement).
   d. Utilisez le bouton [**Browse**] (Parcourir) pour rechercher et sélectionner les dossiers suivants :
   – C:\Program Files\Xerox\FreeFlow Output Manager\persistence
   – C:\Program Files\Xerox\FreeFlow Output Manager\spool

   Remarque
   Il est possible que le dossier FreeFlow Output Manager ne se trouve pas sur le lecteur C: sur votre système FreeFlow. Si nécessaire, recherchez l'emplacement approprié et sélectionnez le dossier.

   e. Cochez la case [**Also exclude subfolders**] (Exclure aussi les sous-dossiers).
   f. Sous When to exclude (Quand exclure), cochez les cases [**On read**] (À la lecture) et [**On write**] (À l'écriture).
   g. Sélectionnez [**OK**].
7. Sélectionnez [**OK**] pour fermer Set Exclusions (Définir les exclusions).
8. Sélectionnez [**OK**] pour fermer On-Access Scan Properties (Propriétés de l'analyse lors de l'accès).
9. Sélectionnez [**Tools: Lock User Interface**] (Outils: Verrouiller l'interface utilisateur).

## Recommandations relatives à McAfee VirusScan pour FreeFlow Process Manager

Si vous utilisez McAfee VirusScan avec votre système FreeFlow Process Manager, il est recommandé de définir les dossiers à exclure afin d'éviter tout problème lors de l'utilisation de Process Manager.

Remarque
Si vous utilisez un logiciel antivirus autre que McAfee VirusScan, il est recommandé de définir les dossiers à exclure dans ce logiciel également.

1. Cliquez avec le bouton droit sur [**McAfee VirusScan On-Access Scan**] (Analyse McAfee VirusScan lors de l'accès).
2. Sélectionnez [**VirusScan Console**] (Console VirusScan).
3. Sélectionnez [**Tools: Unlock User Interface**] (Outils: Déverrouiller l'interface utilisateur).

   Remarque
   Si l'option Déverrouiller l'interface utilisateur est estompée, sélectionnez [**Tools: Open Remote Console**] (Outils: Ouvrir la console distante) et sous Connect to Computer (Se connecter à l'ordinateur), entrez l'adresse IP du système Process Manager, puis sélectionnez [**OK**]. Ceci active l'option Déverrouiller l'interface utilisateur.

   Remarque
   Si un mot de passe est requis, contactez votre administrateur système.

4. Cliquez avec le bouton droit sur [**On-Access Scanner**] (Analyse lors de l'accès) et sélectionnez [**Properties**] (Propriétés).
5. Sélectionnez [**All Processes**] (Tous les processus).

6. Sélectionnez l'onglet **Detection** (Détection).
   a. Sous What not to scan (Éléments à exclure de l'analyse), sélectionnez [**Exclusions**].
   b. Sélectionnez [**Add**] (Ajouter) pour ajouter les exclusions.
   c. Sous What not to scan (Éléments à exclure de l'analyse), sélectionnez [**By name/ location**] (Par nom/emplacement).
   d. Utilisez le bouton [**Browse**] (Parcourir) pour rechercher et sélectionner les dossiers suivants :
   – C:\Documents and Settings\All Users\Appliccations Data\Enfocus Prefs
   – C:\Program Files\Enfocus
   – Pour tous les systèmes Process Manager qui utilisent des nœuds externes, les entrées, les sorties et les dossiers d'erreur utilisés par les nœuds externes doivent être exclus, sinon, des erreurs surviennent avec ces flux de travail.
   – E:\FFxTools

   Remarque

   Il est possible que le dossier FFxTools ne se trouve pas sur le lecteur E: sur votre système FreeFlow. Si nécessaire, recherchez l'emplacement approprié et sélectionnez le dossier.

   – E:\Pitstop_HOT_FOLDERS

   Remarque

   Il est possible que le dossier Pitstop_HOT_FOLDERS ne se trouve pas sur le lecteur E: sur votre système FreeFlow. Si nécessaire, recherchez l'emplacement approprié et sélectionnez le dossier.

   – E:\FreeFlow\ProcessManager\Spool

   Remarque

   Il est possible que le dossier FreeFlow\ProcessManager\Spool ne se trouve pas sur le lecteur E: sur votre système FreeFlow. Si nécessaire, recherchez l'emplacement approprié et sélectionnez le dossier.

   e. Cochez la case [**Also exclude subfolders**] (Exclure aussi les sous-dossiers).
   f. Sous When to exclude (Quand procéder à l'exclusion), cochez les cases [**On read**] (À la lecture) et [**On write**] (À l'écriture).
   g. Sélectionnez [**OK**].
7. Sélectionnez [**OK**] pour fermer Set Exclusions (Définir les exclusions).
8. Sélectionnez [**OK**] pour fermer On-Access Scan Properties (Propriétés de l'analyse lors de l'accès).
9. Sélectionnez [**Tools: Lock User Interface**] (Outils: Verrouiller l'interface utilisateur).
10. Il est recommandé de lancer une analyse contre les virus dans les dossiers exclus avant ou après l'exécution de Process Manager afin de s'assurer que les dossiers ne sont pas infectés.

# Authentification de l'utilisateur et gestion de compte

La cinquième étape pour obtenir un système plus sécurisé consiste à mettre en place des mesures strictes de contrôle d'accès. Cela permet d'assurer que seuls les utilisateurs autorisés peuvent accéder aux données sensibles. Le modèle de sécurité en vigueur dans FreeFlow 6.0 a été remplacé par un modèle utilisateur qui stipule que le système d'exploitation est responsable de l'authentification, prend en charge une autorisation plus spécifique et permet une intégration plus étroite avec les fonctions de gestion des utilisateurs existantes du client. Consultez la section « Gestion des comptes utilisateur » dans le guide de l'administrateur pour plus d'informations sur la gestion de vos comptes.

Reportez-vous à la section précédente, Recommandations relatives à McAfee VirusScan pour FreeFlow Process Manager, pour savoir comment procéder pour que les dossiers faisant l'objet d'accès fréquents ne soient pas affectés par l'analyse antivirus.

Vous trouverez ci-dessous des recommandations et des fonctions destinées à préserver la sécurité du système FreeFlow :

- Connexion et authentification
  - **Authentification des utilisateurs via le système d'exploitation et autorisation au niveau applicatif** — FreeFlow Process Manager, les services de gestion de copyright, FreeFlow Output Manager et Printer Registration prennent en charge l'authentification des utilisateurs via le système d'exploitation et l'autorisation au niveau applicatif via l'appartenance aux groupes du système d'exploitation.
- Mots de passe complexes
  - Il est recommandé d'activer les mots de passe complexes dans la stratégie de sécurité locale.
- Gestion des comptes utilisateur

  Exécutez les étapes suivantes pour gérer vos comptes utilisateur sur le système FreeFlow :
  - **Utilisateurs: Test Account (Compte de test)** et modifiez le nom de connexion et le mot de passe du compte de test.

  a. Supprimez les comptes utilisateur inactifs au moins tous les 90 jours.
  b. N'utilisez pas de compte / mot de passe de groupe, partagé ou générique.
  c. Changez les mots de passe d'accès au système au moins tous les 30 jours à l'aide de la sécurité locale.
  d. Les mots de passe des comptes administrateur et utilisateur FreeFlow doivent comporter au moins 7 caractères.

**ATTENTION**

La modification du mot de passe de XDL_ADMIN entraîne le redémarrage de certains services et une incompatibilité avec le mot de passe côté client. Contactez votre interlocuteur Xerox pour faire correspondre votre mot de passe côté client et le nouveau mot de passe de XDL_ADMIN.