

Version 5.4.0  
Novembre 2019  
702P07033

# Xerox® FreeFlow® Core

## Security Guide

©2019 Xerox Corporation. Tous droits réservés. Xerox®, Xerox avec la marque figurative® et FreeFlow® sont des marques déposées de Xerox Corporation aux États-Unis et/ou dans d'autres pays.

Ce logiciel inclut la technologie développée par Adobe Systems Incorporated.

Adobe, le logo Adobe, le logo Adobe PDF, PDF Converter SDK, Adobe Acrobat Pro DC, Adobe Reader DC et PDF Library sont des marques de commerce ou des marques déposées de Adobe Systems Incorporated aux États-Unis et/ou dans d'autres pays.

Le navigateur Google Chrome™ est une marque déposée de Google LLC.

Microsoft®, Windows®, Edge®, Microsoft Language Pack, Microsoft Office 2013, Microsoft Office 2016, Microsoft SQL Server et Internet Explorer® sont des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.

Apple®, Macintosh®, Mac®, Mac OS® et Safari® sont des marques commerciales ou des marques déposées de Apple, Inc., aux États-Unis et dans d'autres pays.

Mozilla Firefox est une marque déposée de la Fondation Mozilla aux États-Unis et dans d'autres pays.

BR14707

# Table des matières

1 Synthèse.....	5
Objectif.....	6
Public cible.....	7
Clause d'exclusion de responsabilité.....	8
2 Description du produit.....	9
Structure du logiciel système.....	10
3 Aspects sécuritaires de certaines fonctions sélectionnées.....	11
Accès au système.....	12
Connexions réseau.....	12
Conformité FIPS.....	22
Chiffrement de données.....	23
Traitement de fichiers.....	23
Contrôle d'accès des comptes utilisateur et maintien du travail.....	24
Mots de passe du compte utilisateur.....	24
Verrouillage du compte utilisateur.....	24
Déconnexion du compte utilisateur.....	24
Activité du compte utilisateur.....	24
Maintien du travail.....	24
4 Sécurité.....	25
Protection antivirus.....	26
5 Mise à jour logicielle.....	27



# Synthèse

Ce chapitre contient :

- Objectif ..... 6
- Public cible ..... 7
- Clause d'exclusion de responsabilité ..... 8

## Objectif

Ce document a pour objectif de communiquer des informations relatives à la sécurité des produits Xerox® FreeFlow® Core et Xerox® FreeFlow® Cloud.

Les clients sont responsables de la sécurité de leur réseau et du produit FreeFlow. Ce produit FreeFlow ne sécurise aucun environnement de réseau.

## Public cible

Ce document s'adresse aux clients qui nécessitent plus d'informations relatives à la sécurité en ce qui concerne le logiciel Xerox® FreeFlow® Core.

## Clause d'exclusion de responsabilité

À notre connaissance, les informations qui figurent dans ce document sont exactes à la date de leur publication et sont fournies sans aucune garantie. En aucun cas Xerox® Corporation ne sera tenue pour responsable de tout dommage résultant de l'utilisation ou de la non-utilisation des informations fournies dans ce document, y compris tout dommage direct, indirect, accessoire ou consécutif, toute perte de profits ou tout dommage particulier, même si Xerox® Corporation a été informée de la possibilité de tels dommages.

# Description du produit

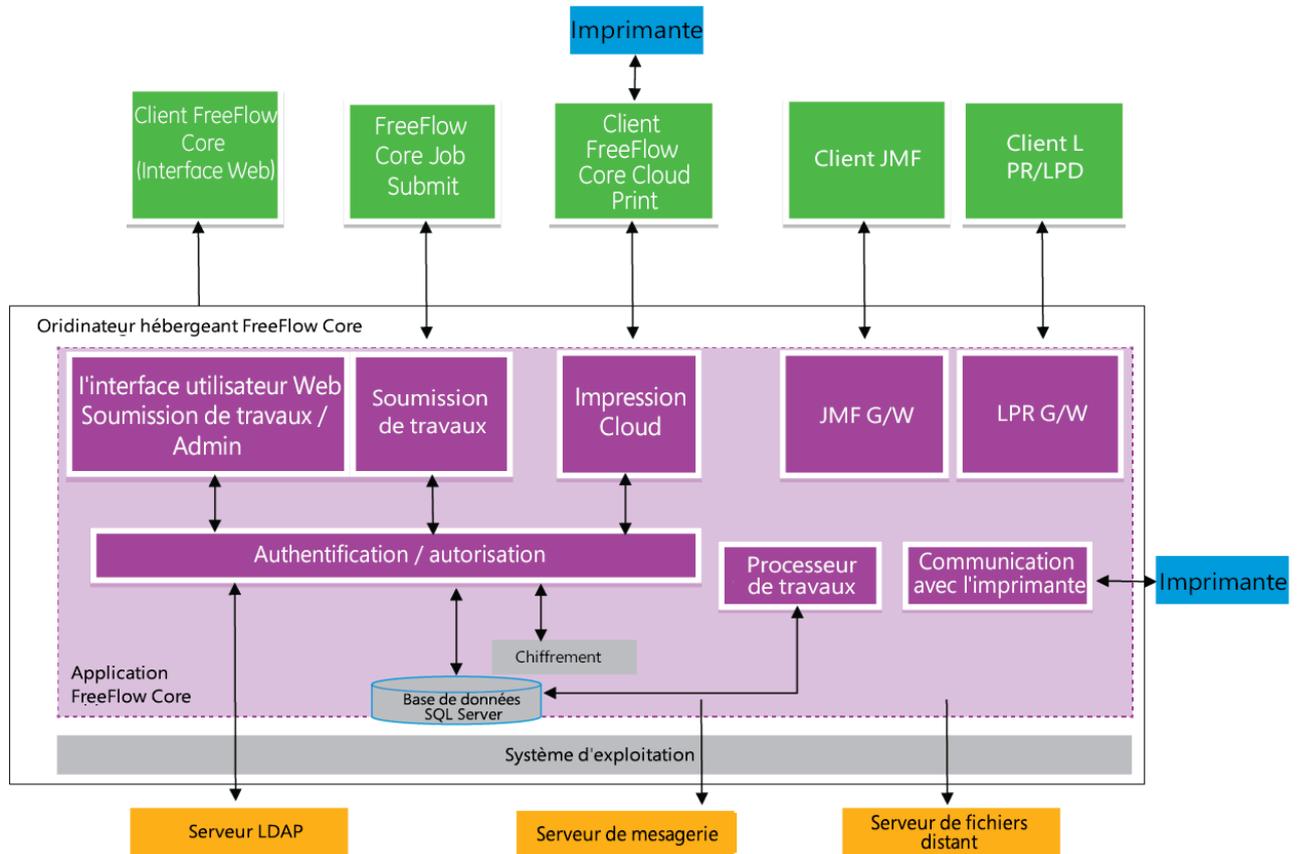
Ce chapitre contient :

- [Structure du logiciel système](#) ..... 10

Xerox® FreeFlow® Core représente la nouvelle génération des solutions de flux de travail Xerox. FreeFlow Core est une solution de type navigateur qui automatise et intègre de manière intelligente le traitement des travaux d'impression, de la préparation des fichiers à la production finale. FreeFlow Core vous offre un flux de travail sans intervention manuelle, simple d'utilisation, extrêmement souple, rapidement redimensionnable et produisant des résultats cohérents.

Xerox® FreeFlow® Core Cloud est la version cloud de la solution. Un fonctionnement dans le cloud signifie que Xerox installe le logiciel sur ses serveurs dans le cloud. Xerox configure et gère la maintenance de la solution. Vous pouvez accéder à votre appareil dédié et sécurisé depuis votre navigateur Web.

# Structure du logiciel système



# Aspects sécuritaires de certaines fonctions sélectionnées

Ce chapitre contient :

- Accès au système ..... 12
- Conformité FIPS ..... 22
- Chiffrement de données ..... 23
- Contrôle d'accès des comptes utilisateur et maintien du travail ..... 24

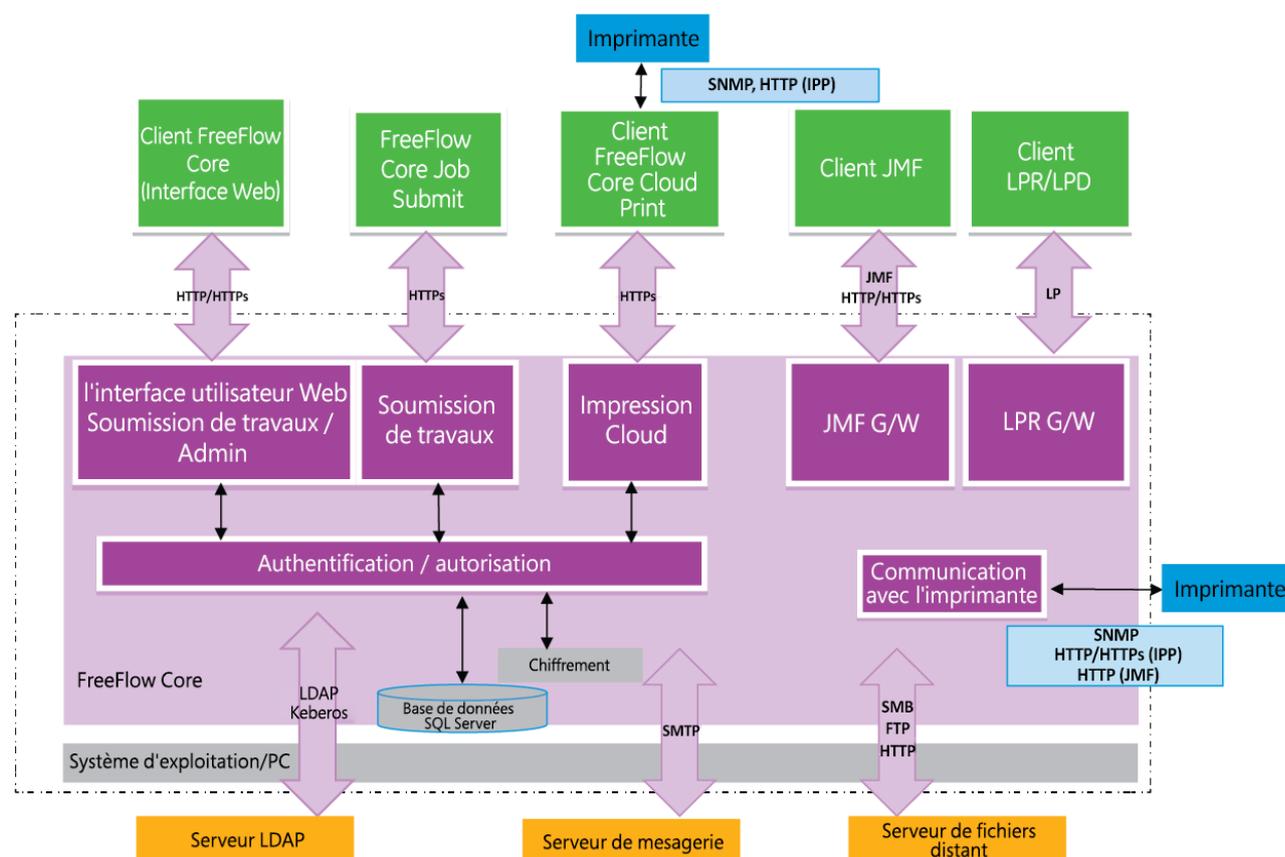
## Accès au système

### Connexions réseau

Xerox® FreeFlow® Core requiert une connexion réseau pour le traitement des travaux et les interactions des utilisateurs. Pour chaque connexion réseau, veuillez consulter les informations de sécurité.

 **Remarque :** Pour optimiser la protection contre les attaques de vulnérabilité, activez le pare-feu Windows du serveur sur lequel est installé FreeFlow Core.

FreeFlow Core utilise les connexions réseau suivantes.



### Client Xerox® FreeFlow® Core

Un navigateur Web compatible avec HTML5 et CSS3 est nécessaire pour établir la connexion avec FreeFlow Core. Le téléchargement sécurisé du client Xerox® FreeFlow® Core et la communication sécurisée entre le client et Xerox® FreeFlow® Core nécessitent l'utilisation de connexions HTTPS.

- Pour activer des connexions HTTPS, ajoutez le certificat TLS/SSL à l'IIS (Internet Information Services). Suivez les instructions contenues dans la documentation Windows.
- Pour activer des connexions HTTPS, ajoutez un certificat CA au gestionnaire IIS (Internet Information Services). Veuillez consulter la documentation Windows.
- FreeFlow Core prend en charge les protocoles cryptographiques TLS 1.1 et 1.2. TLS 1.0. Toutes les versions de SSL sont désactivées.
- À moins que l'utilisateur ne télécharge des fichiers de travaux, aucune donnée client n'est échangée entre le client et le serveur Xerox® FreeFlow® Core.

 **Remarque :** Le client récupère les propriétés des travaux contenant des données client.

**Table 3.1 Configuration du pare-feu**

Port	Protocole ou Application	Type de connexion du pare-feu
80	HTTP	Trafic entrant  <b>Remarque :</b> Le numéro de port dépend de la configuration du serveur IIS.
443	HTTPS	Trafic entrant  <b>Remarque :</b> Le numéro de port dépend de la configuration du serveur IIS.

## Rôles utilisateurs

Xerox® FreeFlow® Core s'ouvre sur un écran de connexion.

- Les utilisateurs se connectent pour accéder au périphérique FreeFlow Core.
- Après 30 minutes d'inactivité, les utilisateurs connectés sont automatiquement déconnectés.
- Avec le logiciel FreeFlow Core, les utilisateurs ne sont pas interdits d'accès à l'application si l'authentification échoue.

Pour affecter des utilisateurs aux rôles d'utilisateur consultez le document d'aide de FreeFlow Core, sous *Configuration de l'accès utilisateur*.

## Rôle administrateur

L'administrateur a accès à l'intégralité du système :

- Fonctions de l'onglet Gestion et état des travaux : Boîtes de dialogue Soumission du travail et onglets États des travaux.
- Onglets Gestion et État des imprimantes
- Configuration du flux de travail
- Fonctions de l'onglet Administration :
  - Configuration du dossier actif
  - Configuration des notifications
  - Configuration de l'accès utilisateur
- Utilitaires du serveur Core disponibles sur le bureau du serveur :
  - Xerox® FreeFlow® Core Exchange
  - Rapports Xerox® FreeFlow® Core
  - Serveur Xerox® FreeFlow® Core Cloud Print
  - Certificats Xerox® FreeFlow® Core
  - Licence Xerox® FreeFlow® Core
  - Configurer Xerox® Core
- Utilitaires du client Core :

## Aspects sécuritaires de certaines fonctions sélectionnées

- Soumission de travaux Xerox®FreeFlow® Core
- Client Xerox® FreeFlow® Core Cloud Print

 **Remarque :** Un seul administrateur peut être connecté à la fois à Xerox® FreeFlow® Core.

## Rôle opérateur

Les opérateurs ont accès aux éléments suivants :

- Fonctions de l'onglet Gestion et état des travaux : Boîtes de dialogue Soumission du travail et onglets États des travaux
- Onglets Gestion et État des imprimantes
- Utilitaires du client Core :
  - Soumission de travaux Xerox®FreeFlow® Core
  - Client Xerox® FreeFlow® Core Cloud Print

 **Remarque :** Plusieurs opérateurs peuvent être connectés en même temps à Xerox® FreeFlow® Core.

## Rôle superviseur de l'état des travaux

Le rôle superviseur de l'état des travaux a accès en lecture seule à la fenêtre de l'onglet État des travaux.

 **Remarque :** Plusieurs utilisateurs jouant le rôle de superviseurs de l'état des travaux peuvent être connectés en même temps à Xerox® FreeFlow® Core.

## Authentification des utilisateurs

Les références de connexion saisies sur le client du navigateur Xerox® FreeFlow® Core sont chiffrées à l'aide du chiffrement (AES) AES 128. Les références sont chiffrées avant d'être envoyées au serveur Xerox® FreeFlow® Core.

- Si vous authentifiez des utilisateurs avec Xerox® FreeFlow® Core, les informations utilisateur sont cryptées à l'aide du cryptage (AES) AES 128. Les références de connexion sont stockées localement.
- En cas d'authentification à l'aide d'Active Directory, les références de connexion ne sont pas chiffrées avant d'être envoyées à Active Directory. En cas d'authentification à l'aide d'Active Directory, les références de connexion ne sont pas stockées localement.

La connexion de Configuration Xerox® FreeFlow® Core à Active Directory est chiffrée selon la configuration du système d'exploitation.

Table 3.2 Configuration du pare-feu

Port	Protocole ou Application	Type de connexion du pare-feu
80	HTTP	Trafic entrant  <b>Remarque :</b> Le numéro de port dépend de la configuration du serveur IIS.
88	Kerberos	Trafic sortant : Authentification des utilisateurs  <b>Remarque :</b> Les numéros de port et les services dépendent de la configuration Active Directory du serveur.
<ul style="list-style-type: none"> <li>• 389</li> <li>• 636</li> <li>• 3268</li> <li>• 3269</li> </ul>	<ul style="list-style-type: none"> <li>• LDAP</li> <li>• LDAP SSL</li> <li>• LDAP GC</li> <li>• LDAP GC SSL</li> </ul>	Trafic sortant : valide les groupes Active Directory lors de la configuration de l'authentification Active Directory.  <b>Remarque :</b> Les numéros de port et les services dépendent de la configuration Active Directory du serveur.

## Connexion à SQL Server

Xerox® FreeFlow® Core communique avec le serveur SQL à l'aide de Microsoft® Entity Framework. Une communication chiffrée entre Xerox® FreeFlow® Core et le serveur SQL est activée lorsque le serveur SQL est configuré pour utiliser des connexions chiffrées.

Les références de connexion serveur SQL chiffrées sont stockées localement sur le serveur Xerox® FreeFlow® Core.

Pour installer le logiciel sur un serveur distant SQL sans privilèges administratifs SQLS, créez deux bases de données vides dans l'instance SQLS :

- OapMasterDatabase
- OapPlatformDatabase

Port	Protocole ou Application	Type de connexion du pare-feu
1433	SQLS	Trafic entrant : reçoit des connexions de Xerox® FreeFlow® Core Trafic sortant : communique avec le moteur de base de données du serveur SQL  <b>Remarque :</b> le numéro de port dépend de la configuration du serveur SQLS.
1434	Service de navigateur SQLS	Trafic entrant : reçoit des connexions de Xerox® FreeFlow® Core Trafic sortant : communique avec le moteur de base de données du serveur SQL  <b>Remarque :</b> Le serveur fournit au client un numéro de port pour la connexion.

## Interface utilisateur de Soumission des travaux

L'interface utilisateur de Soumission des travaux utilise la connexion du client Xerox® FreeFlow® Core pour soumettre les travaux. Pour plus d'informations, reportez-vous à [Client Xerox® FreeFlow® Core](#).

**Table 3.3 Configuration du pare-feu**

Port	Protocole ou Application	Type de connexion du pare-feu
80	HTTP	Trafic entrant  <b>Remarque :</b> Le numéro de port dépend de la configuration du serveur IIS.
443	HTTPS	Trafic entrant  <b>Remarque :</b> Le numéro de port dépend de la configuration du serveur IIS.

## Dossiers actifs

Utilisez les partages de fichiers pour partager un dossier actif local et pour accéder à un dossier actif dans les dossiers Windows partagés. Pour chiffrer les dossiers Windows, utilisez le système de fichiers Windows. Pour protéger les partages de dossiers Windows, utilisez le contrôle d'accès des comptes utilisateur Windows.

 **Remarque :** Lorsque vous utilisez le contrôle d'accès des comptes utilisateur, utilisez le compte de service configuré durant l'exécution des *Procédures d'installation optionnelles*. Pour plus d'informations, reportez-vous au *Guide d'installation Xerox FreeFlow Core*.

**Table 3.4 Configuration du pare-feu**

Port	Protocole ou Application	Type de connexion du pare-feu
139, 445	SMB	Trafic entrant : partage les dossiers actifs grâce au partage de fichiers Windows  Trafic sortant : utilise les dossiers actifs sur des répertoires partagés
20, 21	FTP	Trafic entrant : partage les dossiers actifs grâce au FTP

## Traitement du manifeste

Lors de la soumission du manifeste, Xerox® FreeFlow® Core récupère les fichiers répertoriés dans le manifeste. Vous pouvez référencer les fichiers à l'aide des lecteurs mappés, des chemins d'accès à des fichiers UNC, HTTP ou des URI FTP.

 **Remarque :** HTTP et les URI FTP ne prennent pas en charge le chiffrement.

Utilisez les partages de fichiers pour partager un dossier actif local et pour accéder à un dossier actif dans les dossiers Windows partagés. Pour chiffrer les dossiers Windows, utilisez le système de fichiers Windows. Pour protéger les partages de dossiers Windows, utilisez le contrôle d'accès des comptes utilisateur Windows.

 **Remarque :** Lorsque vous utilisez le contrôle d'accès des comptes utilisateur, utilisez le compte de service configuré durant l'exécution des *Procédures d'installation optionnelles*. Pour plus d'informations, reportez-vous à la section *Procédures d'installation optionnelles* du *Guide d'installation de FreeFlow Core*.

Table 3.5 Configuration du pare-feu

Port	Protocole ou Application	Type de connexion du pare-feu
139, 145	SMB	Trafic sortant : récupère les fichiers répertoriés dans le manifeste depuis des répertoires partagés
20, 21	FTP	Trafic sortant : récupère les fichiers répertoriés dans le manifeste
80	HTTP	Trafic sortant : récupère les fichiers répertoriés dans le manifeste

## Line Printer Daemon (LPD)

 **Remarque :** Les commandes Line Printer ( LP) ne prennent pas en charge les connexions sécurisées.

Table 3.6 Configuration du pare-feu

Port	Protocole ou Application	Type de connexion du pare-feu
515	LP	Trafic entrant : reçoit des requêtes LPR (Line Printer Remote) et des commandes LP

## Commandes et signaux d'état d'imprimante JMF

Les commandes JMF (Job Messaging Format) prennent en charge des connexions sécurisés. La récupération des fichiers JMF utilise des connexions non chiffrées.

 **Remarque :** Afin de garantir la sécurité des soumissions JMF, soumettez un package MIME avec les fichiers JMF, JDF et PDF.

Les signaux d'état de l'imprimante JMF utilisent une connexion non chiffrée. Pour obtenir des signaux d'état JMF sécurisés, utilisez la commande JMF StatusQuery avec une connexion sécurisée.

Pour activer la communication HTTPS pour les commandes JMF :

1. Pour ajouter un certificat à la clé Java dans le répertoire installation Xerox® FreeFlow® Core, utilisez l'utilitaire **installJMFCertificate.bat**.
2. redémarrez le service Xerox® FreeFlow® Core JMF Server.
3. Pour tester l'installation, rendez-vous à l'adresse `http://<hostname>:7759`. Si le JMF sécurisé est configuré correctement, le navigateur affiche la page d'erreur HTTP Status 404.

**Table 3.7 Configuration du pare-feu**

Port	Protocole ou Application	Type de connexion du pare-feu
775-1	JMF	Trafic entrant : réception des commandes JMF
Va-ri-able	JMF	Trafic sortant : renvoie les signaux d'état de l'imprimante JMF  <b>Remarque :</b> Le client qui demande les signaux d'état de l'imprimante JMF ou le renvoi de signal JMF définit le numéro de port requis.
775-9	sJMF	Trafic entrant : reçoit les commandes JMF sécurisées

## Soumission de travaux Xerox®FreeFlow® Core

La connexion entre la Soumission de travaux Xerox® FreeFlow® Core et Xerox® FreeFlow® Core est chiffrée et requiert l'installation d'un certificat CA.

- Ajoutez le certificat à l'aide du gestionnaire Internet Information Services (IIS) pour installer le certificat sur le serveur.
- TLS 1.2 est utilisé entre la soumission de travaux Xerox FreeFlow Core et le logiciel Xerox FreeFlow Core.
- L'application Soumission de travaux Xerox® FreeFlow® Core et le logiciel complémentaire Microsoft Office utilisent la même connexion sécurisée à Xerox® FreeFlow® Core.
- Les références de connexion chiffrées sont stockées localement

**Table 3.8 Configuration du pare-feu**

Port	Protocole ou Application	Type de connexion du pare-feu
443	HTTPS	Trafic entrant sur le serveur : accepte les connexions depuis le client Soumission de travaux Xerox® Freeflow® Core Trafic sortant sur le client : soumet les travaux à Xerox® FreeFlow® Core Cloud

## Nœuds de flux de travail

Les composants de flux de travail qui récupèrent ou enregistrent des fichiers de travaux peuvent utiliser des lecteurs mappés, des chemins d'accès à des fichiers UNC, HTTP ou des URI FTP.

 **Remarque :** HTTP et les URI FTP ne prennent pas en charge le chiffrement.

Pour chiffrer les partages de fichiers, utilisez le système de fichiers Windows. Pour protéger les partages de fichiers, utilisez le contrôle d'accès des comptes utilisateur Windows.

 **Remarque :** Lorsque vous utilisez le contrôle d'accès des comptes utilisateur, utilisez le compte de service configuré durant l'exécution des *Procédures d'installation optionnelles*. Pour plus d'informations, reportez-vous au *Guide d'installation Xerox FreeFlow Core*.

Table 3.9 Configuration du pare-feu

Port	Protocole ou Application	Type de connexion du pare-feu
139, 445	SMB	Trafic entrant : récupère les fichiers spécifiés dans le pré-réglage des composants du flux de travail Trafic sortant : enregistre les fichiers dans des répertoires partagés
20, 21	FTP	Trafic sortant : récupère les fichiers spécifiés dans le pré-réglage des composants du flux de travail
80	HTTP	Trafic sortant : vous pouvez chiffrer les fichiers dans les dossier actifs. Pour les dossiers Windows partagés, vous pouvez chiffrer les fichiers à l'aide du système de fichiers Windows ou protéger les fichiers à l'aide du contrôle d'accès au compte utilisateur Windows. Récupère les fichiers spécifiés dans le pré-réglage des composants du flux de travail.

## Impression Xerox® FreeFlow® Core

Xerox® FreeFlow® Core utilise SNMP et HTTP ainsi que les commandes IPP ou JMF pour déterminer le type de DFE au moyen d'une connexion non chiffrée. La chaîne de communauté publique SNMP de l'imprimante/du DFE nécessite le réglage par défaut. Si la chaîne de communauté publique SNMP de l'imprimante ou le DFE a été modifié à partir du réglage par défaut, assurez-vous que le paramètre de mise à jour est enregistré dans FreeFlow Core. Assurez-vous que toutes les imprimantes enregistrées sur FreeFlow Core disposent d'une même chaîne de communauté publique SNMP. Pour savoir comment effectuer la mise à jour de la chaîne de communauté publique SNMP, reportez-vous aux notes de mise à jour de Xerox FreeFlow Core.

Les opérations suivantes utilisent une connexion non chiffrée :

- Récupération de la liste des files du DFE.
- Récupération des imprimantes virtuelles sur le contrôleur numérique EFI.
- Récupération des fonctions de l'imprimante.
- Opérations liées aux travaux au DFE.
- Récupération des informations de comptabilisation des travaux. Cette opération n'est pas applicable pour JMF.

La soumission d'impressions est chiffrée lors d'une connexion à un DFE configuré pour prendre en charge le protocole IPP sécurisé. Utilisez l'option Impression protégée dans la configuration de la destination de l'imprimante pour activer le protocole IPP sécurisé. Les chiffrements TLS 1.2 et SHA256 sont utilisés entre FreeFlow Core et le DFE.

Procédez de la manière suivante pour activer la soumission d'impressions avec le protocole IPP sécurisé au serveur d'impression FreeFlow :

1. Ajoutez un certificat au serveur d'impression FreeFlow.
2. Dans la configuration du serveur d'impression Xerox® FreeFlow®, sélectionnez **Activer SSL/TLS**.
3. Utilisez Certificat Xerox® FreeFlow® Core pour récupérer le certificat TLS/SSL du serveur d'impression FreeFlow.



**Remarque :** Lorsque l'IPP sécurisé est correctement configuré, un message indiquant que l'installation du certificat a réussi s'affiche.

FreeFlow Core ne prend pas en charge la communication avec DFE à partir d'un JMF sécurisé.

**Table 3.10 Configuration du pare-feu**

Port	Protocole ou Application	Type de connexion du pare-feu
161, 162	SNMP v1/v2	Trafic sortant : identifie le type de DFE lors de la configuration de la destination d'une imprimante et de la récupération du certificat
80	HTTP	Trafic sortant : identifie le type de DFE lors de la configuration de la destination d'une imprimante et de la récupération du certificat
N/A	ICMP	Trafic sortant : vérifie la disponibilité du périphérique avant de récupérer le certificat
631	IPP v1.0/v1.1	Trafic sortant : soumet les travaux vers des DFE, obtient l'état des travaux et soumet les commandes de travaux vers le DFE
8010 ou port JMF de l'imprimante définie	JMF v1.3/v1.4	Trafic sortant : identifie le type de DFE pendant l'enregistrement de l'imprimante et soumet un travail au DFE.
443	HTTPS	Trafic sortant : soumet les travaux au DFE

## Xerox® FreeFlow® Core Cloud Print

La connexion entre le client et le serveur Xerox® FreeFlow® Core Cloud Print est chiffrée et requiert l'installation d'un certificat CA. TLS 1.2 est utilisé entre le client et le serveur FreeFlow Core Cloud Print.

Utilisez le gestionnaire Internet Information Services (IIS) pour installer le certificat sur le serveur. Pour plus d'informations, veuillez consulter la documentation Windows.

Grâce à une connexion sécurisée et afin de déterminer le type de DFE, le client Xerox® FreeFlow® Core Cloud Print utilise SNMP ou HTTP. Les réglages de la chaîne communauté publique SNMP de l'imprimante ou du DFE sont définis par défaut.

La connexion entre le client Xerox® FreeFlow® Core Cloud Print et le DFE ne prend pas en charge le protocole IPP sécurisé.

**Table 3.11 Configuration du pare-feu**

Port	Protocole ou Application	Type de connexion du pare-feu
161, 162	SNMP (v1/v2)	Trafic sortant : identifie le type de DFE lors de la configuration de la destination de l'imprimante
631	IPP (v1.0/v1.1)	Trafic sortant : soumet les travaux vers des DFE, obtient l'état des travaux et soumet les commandes de travaux vers le DFE

Port	Protocole ou Application	Type de connexion du pare-feu
443	HTTPS	Trafic entrant sur le serveur : accepte les connexions depuis le client Xerox® Freeflow® Core Cloud Print  Trafic sortant sur le client : Connecte au serveur Xerox® FreeFlow® Core Cloud Print
8010 ou port JMF de l'imprimante définie	JMF v1.3/v1.4	Trafic sortant : identifie le type de DFE pendant l'enregistrement de l'imprimante et soumet un travail au DFE.

## Notification par courrier électronique

Xerox® FreeFlow® Core est un client de messagerie qui se connecte au serveur de messagerie d'un client. Vous avez la possibilité de chiffrer les notifications par courrier électronique, puis connecter à un serveur de messagerie qui prend en charge le chiffrement. SSL permet le chiffrement des communications entre le service de notification et le serveur SMTP.

Les références de connexion chiffrées sont stockées localement.

**Table 3.12 Configuration du pare-feu**

Port	Protocole ou Application	Type de connexion du pare-feu
25, 2525, 465, 475, 587	SMTP	Trafic sortant : envoie des notifications par courrier électronique   <b>Remarque :</b> Le numéro de port requis et l'utilisation d'une connexion sécurisée dépendent de la configuration du serveur SMTP.

## Conformité FIPS

Xerox® FreeFlow® Core fonctionne sous les systèmes d'exploitation Windows bénéficiant de la conformité FIPS 140-2. Veuillez consulter la documentation Windows pour activer la conformité FIPS. Par défaut, FreeFlow Core fonctionne en mode Conformité FIPS.

FreeFlow Core désactive la prise en charge des chiffres DES/3DES.

Si une impression IPP sécurisée avec authentification Digest est requise, désactivez le mode Conformité FIPS, FreeFlow Core devient alors non conforme aux exigences cryptographiques.

## Chiffrement de données

### Traitement de fichiers

FreeFlow Core ne procède pas explicitement au chiffrement des fichiers soumis pour traitement avant le stockage dans le système de fichiers de l'ordinateur.

## Contrôle d'accès des comptes utilisateur et maintien du travail

### Mots de passe du compte utilisateur

La réutilisation des mots de passe est autorisée.

### Verrouillage du compte utilisateur

Avec FreeFlow Core, les utilisateurs ne sont pas bloqués après l'échec des tentatives lorsque l'authentification échoue.

### Déconnexion du compte utilisateur

Après 30 minutes d'inactivité, les utilisateurs connectés sont automatiquement déconnectés. La durée de la période d'inactivité n'est pas configurable.

### Activité du compte utilisateur

Le journal d'audit des transactions de connexion utilisateur à FreeFlow Core n'est pas disponible.

### Maintien du travail

Une fois le travail terminé, la durée de conservation des travaux dans FreeFlow Core est de 24 heures.

L'imprimante FreeFlow Core est configurée pour modifier la période de conservation avant la suppression automatique des travaux terminés. Après 24 heures, le appareil FreeFlow Core supprime les travaux terminés.

Pour supprimer manuellement des travaux, utilisez l'interface utilisateur Web de FreeFlow Core.

# Sécurité

Ce chapitre contient :

- **Protection antivirus** ..... 26

Pour Xerox, les problèmes de sécurité constitue la priorité absolue. Leader dans le développement de la technologie numérique, Xerox 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 possibles en fonction des informations et des technologies disponibles, tout en maintenant les performances, la valeur, la fonctionnalité et la productivité de son produit.

La sécurité des composants de Xerox® FreeFlow® Core est évaluée à l'aide d'outils d'analyse disponibles sur le marché. Les vulnérabilités de l'application sont corrigées en fonction des résultats des analyses Xerox.

Xerox distribue des bulletins de sécurité sur demande. Pour connaître les directives relatives à la sécurité du produit consultez les informations sur les bulletins de sécurité transmises via le site Web Sécurité Xerox à l'adresse <https://www.xerox.com/security>. Le site Web contient le statut de vulnérabilité en matière de sécurité le plus récent, l'état de l'imprimante, des livres blancs, la certification de critères communs, les informations de sécurité Intel Security McAfee, ainsi qu'un portail permettant d'envoyer des questions relatives à la sécurité à Xerox.

## Protection antivirus

Xerox prend toutes les précautions nécessaires pour s'assurer que son logiciel vous soit livré sans virus. Les experts de l'industrie des ordinateurs personnels recommandent Xerox à tous ceux qui recherchent un logiciel de détection de virus. Pour protéger votre imprimante 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 Xerox® FreeFlow® Core et SQL Server des analyses antivirus.

Vous pouvez exclure les fichiers suivants des analyses antivirus :

- <répertoire d'installation FreeFlow Core>\Logs
- <répertoire d'installation FreeFlow Core>\Platform\Logs
- <répertoire d'installation FreeFlow Core>\JobSubmit\Logs
- <répertoire d'installation FreeFlow Core>\Config
- <répertoire d'installation FreeFlow Core>\Platform\Config
- <répertoire de données utilisateur FreeFlow Core>\
- Dossiers en dehors du répertoire de données utilisateur FreeFlow Core utilisés par FreeFlow Core

## Mise à jour logicielle

Nous recommandons aux clients de maintenir les logiciels à jour pour tous les périphériques logiciels installés sur le serveur Xerox® FreeFlow® Core. Effectuez une mise à jour Microsoft Windows au moins une fois par mois.

Vous trouverez des mises à jour logicielle de FreeFlow Core à l'adresse <https://www.support.xerox.com/support/core/software/enus.html>. Les clients peuvent installer la mise à jour logicielle.

Mise à jour logicielle

