Version 5.4.0
November 2019
702P07033

Xerox® FreeFlow® Core Security Guide

xerox™

BR14707

Table of Contents

1

Overview

This chapter contains:

Purpose

The purpose of this document is to disclose information related to Xerox® FreeFlow® Core and Xerox® FreeFlow® Cloud product security.

Customers are responsible for the security of their network and the FreeFlow product. The FreeFlow product does not enforce security for any network environment.

Target Audience

The target audience for this document is customers who require more security-related information about Xerox® FreeFlow® Core software.

Disclaimer

The information contained in this document is accurate as of the publication date and is provided with no warranties. In no event shall Xerox® Corporation be liable for any damages resulting from the usage or disregard of the information provided in this document, including direct, indirect, incidental, consequential, loss of business profits, or special damage, even if Xerox® Corporation has been advised of the possibility of such damages.

2

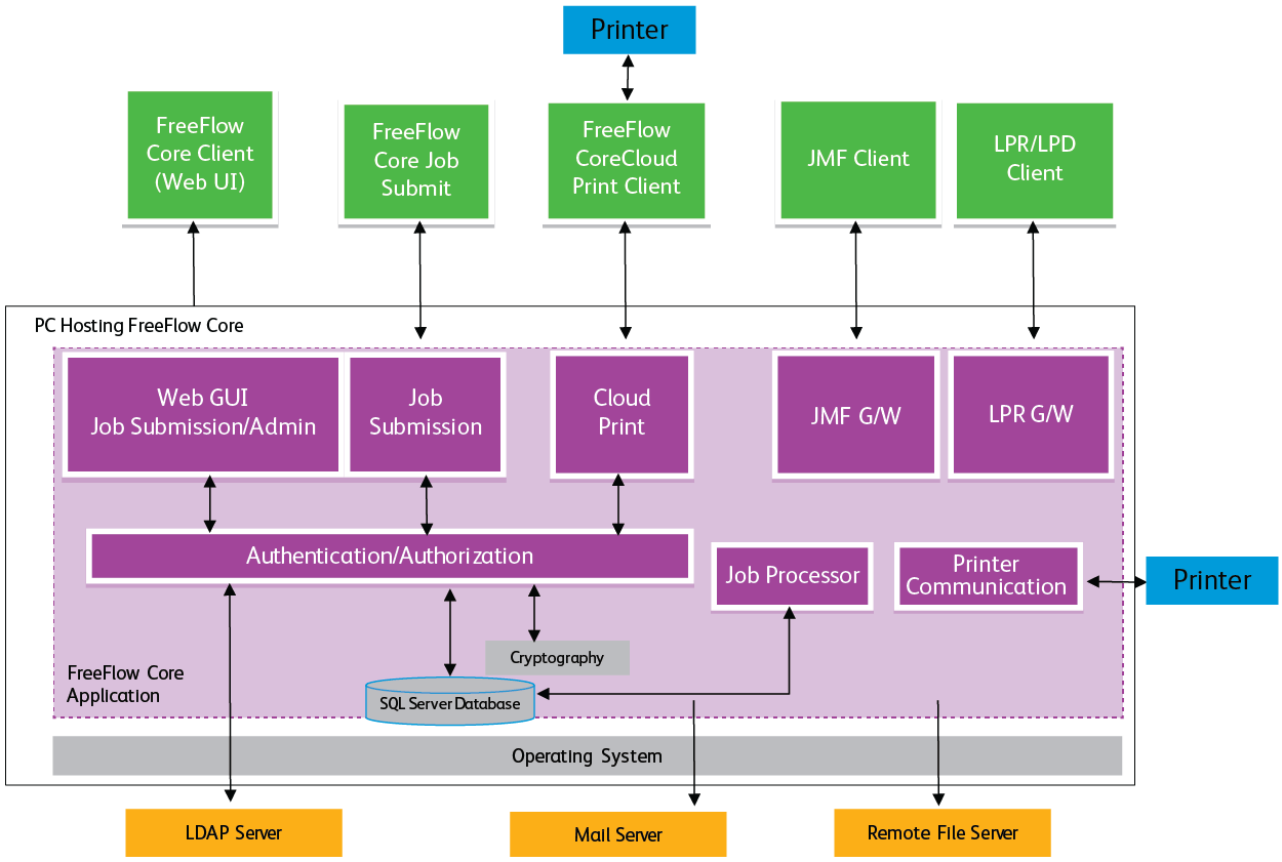
Product Description

This chapter contains:

Xerox® FreeFlow® Core is the next generation in workflow solutions from Xerox. FreeFlow Core is a browser-based solution intelligently automates and integrates the processing of print jobs, from a file preparation to a final production. FreeFlow Core gives you a hands-free workflow that operates easily, adapts effortlessly, scales quickly, and delivers consistently.

Xerox® FreeFlow® Core Cloud is the cloud-based configuration offerings of the solution. Running in the cloud means that Xerox installs the software on Xerox cloud servers. Xerox configures and manages the solution maintenance. You can access your dedicated and secure device from a Web browser.

System Software Structure



3

Security Aspects of Selected Features

This chapter contains:

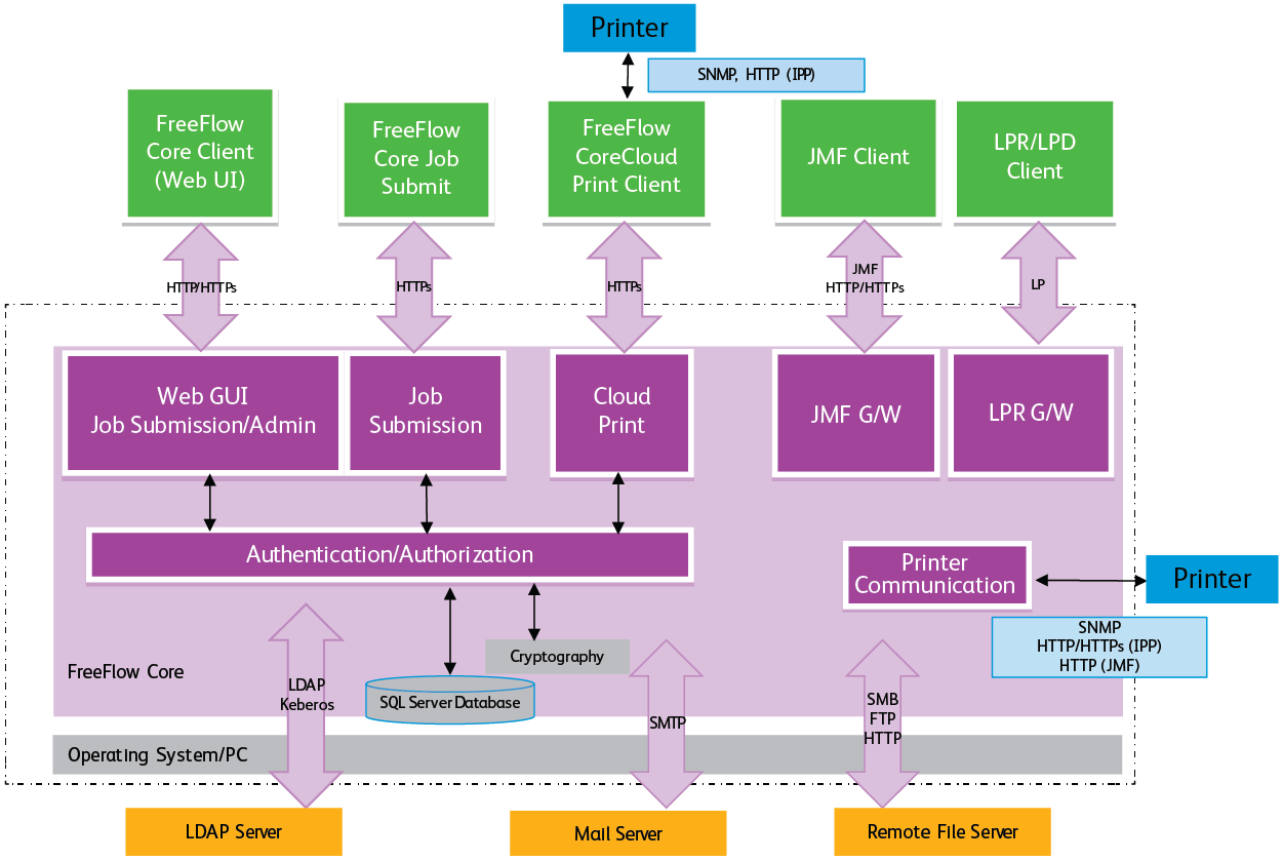
System Access

Network Connections

Xerox® FreeFlow® Core requires network connectivity for both job processing and user interactions. Refer to the security information for each network connection.

Note: To provide better security protection against vulnerability attacks, enable the Windows firewall on the server where FreeFlow Core is installed.

FreeFlow Core uses the following network protocol connections.



Xerox® FreeFlow® Core Client

A Web browser that is compatible with HTML5 and CSS3 is required to connect to FreeFlow Core. HTTPS connections are required to provide a secure download of the Xerox® FreeFlow® Core client, and secure communication between the client and Xerox® FreeFlow® Core.

- To enable HTTPS connections, add a TLS/SSL certificate to the Internet Information Services (IIS). Follow the instructions in the Windows documentation.
- To enable HTTPS connections, add a CA certificate to the Internet Information Services (IIS) manager. Refer to the Windows documentation.
- FreeFlow Core supports cryptographic protocols TLS 1.1 and 1.2. TLS 1.0. All versions of SSL are disabled.

- No customer data is exchanged between the client and the Xerox® FreeFlow® Core server, unless users download job files.

Note: The client retrieves job properties that contain customer data.

Table 3.1 Firewall Configuration

Port	Protocol or Application	Firewall Connection Type
80	HTTP	Inbound **Note:** The port number depends on the IIS server configuration.
443	HTTPS	Inbound **Note:** The port number depends on the IIS server configuration.

User Roles

Xerox® FreeFlow® Core opens to a login screen.

- Users log in for access to the FreeFlow Core device.
- After 30 minutes of inactivity, logged-in users are logged off automatically.
- If authentication fails with the FreeFlow Core software, users are not locked out of the application.

To assign users to User Roles, refer to the FreeFlow Core help, in the *User Access Setup* topic.

Administrator Role

Administrators have access to the entire system:

- Job Management and Status tab functions: Submit Job Dialog and Job Status tabs.
- Printer Management and Status tabs
- Workflow Setup
- Administration tab functions:
  - Hot Folder Setup
  - Notifications Setup
  - User Access Setup
- Core Server Utilities available on the server desktop:
  - Xerox® FreeFlow® Core Exchange
  - Xerox® FreeFlow® Core Reports
  - Xerox® FreeFlow® Core Cloud Print Server
  - Xerox® FreeFlow® Core Certificates
  - Xerox® FreeFlow® Core License
  - Xerox® Core Configure

- Core Client Utilities:
  - Xerox® FreeFlow® Core Submit
  - Xerox® FreeFlow® Core Cloud Print Client

Note: Only one administrator at a time can be logged in to Xerox® FreeFlow® Core.

Operator Role

Operators have access to the following:

- Job Management and Status tab functions: Submit Job Dialog and Job Status tabs
- Printer Management and Status tabs
- Core Client Utilities:
  - Xerox® FreeFlow® Core Submit
  - Xerox® FreeFlow® Core Cloud Print Client

Note: Multiple operators can be logged in at the same time to Xerox® FreeFlow® Core.

Job Status Monitor Role

The Job Status Monitor role has read-only access to the Job Status tab window.

Note: Multiple users who are assigned to the Job Status Monitor role can be logged in at the same time to Xerox® FreeFlow® Core.

User Authentication

Credentials entered into the Xerox® FreeFlow® Core browser client are encrypted using AES encryption AES128. Credentials are encrypted before they are sent to the Xerox® FreeFlow® Core server.

- If authenticating users with Xerox® FreeFlow® Core, user information is encrypted using AES encryption AES128. Credentials are stored locally.
- If authenticating users with Active Directory, credentials are unencrypted before they are submitted to Active Directory. When authenticated with Active Directory, credentials are not stored locally.

The Xerox® FreeFlow® Core configuration connection to Active Directory is encrypted for the operating system configuration.

Table 3.2 Firewall Configuration

Port	Protocol or Application	Firewall Connection Type
80	HTTP	Inbound **Note:** The port number depends on the IIS server configuration.
88	Kerberos	Outbound: User Authentication **Note:** Port numbers and services depend on the server AD configuration.
• 389 • 636 • 3268 • 3269	• LDAP • LDAP SSL • LDAP GC • LDAP GC SSL	Outbound: Validates AD Groups during the AD authentication configuration **Note:** Port numbers and services depend on the server AD configuration.

SQL Server Connection

Xerox® FreeFlow® Core communicates with the SQL server using the Microsoft® Entity Framework. Encrypted communication between Xerox® FreeFlow® Core and the SQL server is enabled when the SQL server is configured to use encrypted connections.

Encrypted SQL server credentials are stored locally within the Xerox® FreeFlow® Core server.

To install software on a remote SQL server without SQLS Administrative privileges, create two empty databases in the SQLS Instance:

- `OapMasterDatabase`
- `OapPlatformDatabase`

Port	Protocol or Application	Firewall Connection Type
1433	SQLS	Inbound: Receives connections from Xerox® FreeFlow® Core Outbound: Communicates with the SQL server database print engine **Note:** The port number depends on the SQLS server configuration.
1434	SQLS Browser Service	Inbound: Receives connections from Xerox® FreeFlow® Core Outbound: Communicates with the SQL server database print engine **Note:** The server provides the client with the port number for connection.

Submit Job User Interface

The Submit Job User Interface (UI) uses the Xerox® FreeFlow® Core Client connection for job submission. For information, refer to Xerox® FreeFlow® Core Client.

Table 3.3 Firewall Configuration

Port	Protocol or Application	Firewall Connection Type
80	HTTP	Inbound **Note:** The port number depends on the IIS server configuration.
443	HTTPS	Inbound **Note:** The port number depends on the IIS server configuration.

Hot Folders

Use file shares for sharing a local hot folder and for accessing a hot folder in shared Windows folders. To encrypt Windows folders, use the Windows file system. To protect Windows folders, use the Windows user account access control.

Note: When you use the user account access control, use the same service account that you used in the *Optional Installation Procedures* configuration. For more information, refer to *FreeFlow Core Installation Guide*.

Table 3.4 Firewall Configuration

Port	Protocol or Application	Firewall Connection Type
139, 445	SMB	Inbound: Shares hot folders using Windows file sharing Outbound: Uses hot folders on shared directories
20, 21	FTP	Inbound: Shares hot folders using FTP

Manifest Processing

During the manifest submission, Xerox® FreeFlow® Core retrieves the files listed in the manifest. You can reference the files using mapped drives, UNC file paths, HTTP, or FTP URIs.

Note: HTTP and FTP URIs do not support encryption.

Use file shares for sharing a local hot folder and for accessing a hot folder in shared Windows folders. To encrypt Windows folders, use the Windows file system. To protect Windows folders, use the Windows user account access control.

Note: When you use the user account access control, use the same service account that you used for the Optional Installation Procedures configuration. For more information, refer to the *FreeFlow Core Installation Guide*, in the section titled *Optional Installation Procedures*.

Table 3.5 Firewall Configuration

Port	Protocol or Application	Firewall Connection Type
139, 145	SMB	Outbound: Retrieves files listed in the Manifest from Shared Directories
20, 21	FTP	Outbound: Retrieves files listed in the manifest
80	HTTP	Outbound: Retrieves files listed in the manifest

Line Printer Daemon (LPD)

Note: Line Printer (LP) commands do not support secure connections.

Table 3.6 Firewall Configuration

Port	Protocol or Application	Firewall Connection Type
515	LP	Inbound: Receives Line Printer Remote (LPR) requests and LP commands

JMF Commands and Printer Status Signals

Job Messaging Format (JMF) commands support secure connections. JMF file retrieval uses unencrypted connections.

Note: For secure JMF submissions, submit a MIME package with the JMF, JDF, and PDF files.

JMF printer status signals use an unencrypted connection. For secure JMF printer status, use the JMF StatusQuery command over a secure connection.

To enable, HTTPS communication for JMF commands:

1. To add a certificate to the Java keystore, in the Xerox® FreeFlow® Core installation directory, use the **installJMFCertificate.bat** utility.
2. Restart the Xerox® FreeFlow® Core JMF Server service.
3. To test the installation, access `http://<hostname>:7759`. If secure JMF is configured correctly, the browser displays an `HTTP Status 404` error page.

Table 3.7 Firewall Configuration

Port	Protocol or Application	Firewall Connection Type
7751	JMF	Inbound: Receives JMF commands
Var-ies	JMF	Outbound: Returns JMF printer status signals **Note:** The client that requests the JMF printer status signals or the Return JMF signal defines the required port number.
7759	sJMF	Inbound: Receives secure JMF commands

Xerox® FreeFlow® Core Submit

The connection between the Xerox® FreeFlow® Core Submit and Xerox® FreeFlow® Core is encrypted and requires installation of a CA certificate.

- To install the certificate on the server, add the certificate using the Internet Information Services (IIS) manager.
- TLS 1.2 is used between the Xerox FreeFlow Core Submit and Xerox FreeFlow Core software.
- The Xerox® FreeFlow® Core Submit application and the Microsoft Office Add-Ins software use the same secure connection to Xerox® FreeFlow® Core.
- Encrypted credentials are stored locally.

Table 3.8 Firewall Configuration

Port	Protocol or Application	Firewall Connection Type
443	HTTPS	Inbound in the server: Accepts connections from the Xerox® FreeFlow® Core Submit client Outbound in the client: Submits jobs to Xerox® FreeFlow® Core Cloud

Workflow Nodes

Workflow components that retrieve or save job files can use mapped drives, UNC file paths, HTTP, or FTP URIs.

Note: HTTP and FTP URIs do not support encryption.

To encrypt file shares for sharing, use the Windows file system. To protect file shares, use the Windows user account access control.

Note: When you use the user account access control, use the same service account that you used in the *Optional Installation Procedures* configuration. For more information, refer to the *FreeFlow Core Installation Guide*.

Table 3.9 Firewall Configuration

Port	Protocol or Application	Firewall Connection Type
139, 445	SMB	Inbound: Retrieves files specified in a workflow component preset Outbound: Saves files to shared directories
20, 21	FTP	Outbound: Retrieves files specified in a workflow component preset
80	HTTP	Outbound: You can encrypt files in hot folders. For shared Windows folders, you can encrypt files using the Windows file system, or you can protect the files using the Windows user account access control. Retrieves files specified in a workflow component preset.

Xerox® FreeFlow® Core Printing

Xerox® FreeFlow® Core uses SNMP and HTTP with the IPP or JMF commands to determine the Digital Front End (DFE) type, using an unencrypted connection. The SNMP public community string on the printer or the DFE requires the default setting. If the SNMP public community string on the printer or the DFE was modified from the default setting, ensure that the updated setting is registered with FreeFlow Core. Ensure that all printers registered with FreeFlow Core have the same SNMP public community string. For instructions on how to update the SNMP public community string, refer to the Xerox FreeFlow Core Release Notes.

The following operations use an unencrypted connection:

- Retrieve the list of the DFE queues.
- Retrieve the list of Virtual Printers on the EFI DFE.
- Retrieve printer capabilities.
- Job operations at the DFE.
- Retrieve job accounting information. This operation is not applicable for JMF.

When connected to a DFE that is configured to support secure IPP, the print submission is encrypted. To enable secure IPP, use the Secure Printing option in the Printer Destination setup. TLS 1.2 and SHA256 encryption is used between FreeFlow Core and the DFE.

To enable secure IPP print submission to FreeFlow Print Server, do the following:

1. Add a certificate to the FreeFlow Print Server.
2. In the Xerox® FreeFlow® Print Server Setup, select **Enable SSL/TLS**.
3. To retrieve the TLS/SSL certificate from the FreeFlow Print Server, use the Xerox® FreeFlow® Core Certificate.

> **Note:** When secure IPP is configured correctly, a `Certificate successfully installed` message appears.

FreeFlow Core does not support communication to the DFE using secure JMF.

Table 3.10 Firewall Configuration

Port	Protocol or Application	Firewall Connection Type
161, 162	SNMP v1/v2	Outbound: Identifies the DFE type during a Printer Destination setup and Certificate Retrieval
80	HTTP	Outbound: Identifies the DFE type during a Printer Destination setup and Certificate Retrieval
N/A	ICMP	Outbound: Verifies device availability before Certificate Retrieval
631	IPP v1.0/v1.1	Outbound: Submits jobs to DFEs, gets job status, and submits job commands to the DFE
8010 or printer defined JMF port	JMF v1.3/v1.4	Outbound: Identifies the DFE type during Printer Registration, and submits a job to the DFE.
443	HTTPS	Outbound: Submits jobs to the DFE

Xerox® FreeFlow® Core Cloud Print

The connection between the Xerox® FreeFlow® Core Cloud Print server and client is encrypted and requires the installation of a CA certificate. TLS 1.2 is used between the FreeFlow Core Cloud Print server and the client.

To install the certificate on the server, use the Internet Information Services (IIS) manager. For more information, refer to the Windows documentation.

To determine the Digital Front End (DFE) type, using an unencrypted connection, Xerox® FreeFlow® Core Cloud Print client uses SNMP or HTTP. The SNMP public community string on the printer or DFE is set to the default setting.

The connection between the Xerox® FreeFlow® Core Cloud Print client and the Digital Front End (DFE) does not support secure IPP.

Table 3.11 Firewall Configuration

Port	Protocol or Application	Firewall Connection Type
161, 162	SNMP (v1/v2)	Outbound: Identifies DFE type during a Printer Destination setup
631	IPP (v1.0/v1.1)	Outbound: Submits jobs to DFEs, gets job status, and submits job commands to the DFE

Port	Protocol or Application	Firewall Connection Type
443	HTTPS	Inbound in the server: Accepts connections from the Xerox® FreeFlow® Core Cloud Print client Outbound in the client: Connects to the Xerox® FreeFlow® Core Cloud Print server
8010 or printer defined JMF port	JMF v1.3/v1.4	Outbound: Identifies the DFE type during Printer Registration, and submits a job to the DFE.

Email Notification

Xerox® FreeFlow® Core is an email client that connects to a customer email server. You can encrypt email notifications, then connect to a mail server that supports encryption. SSL enables encryption of communications between the notification service and the SMTP server.

Encrypted credentials are stored locally.

Table 3.12 Firewall Configuration

Port	Protocol or Application	Firewall Connection Type
25, 2525, 465, 475, 587	SMTP	Outbound: Sends email notifications **Note:** The required port number and use of secure connection depend on the SMTP server configuration.

FIPS Compliance

Xerox® FreeFlow® Core runs on a Windows Operating System enabled for FIPS 140-2 compliance. To enable the FIPS-compliance, refer to the Microsoft documentation. By default, FreeFlow Core runs in FIPS-compliant mode.

FreeFlow Core disables support for DES/3DES ciphers.

If secure IPP Printing with Digest Authentication is required, disable the FIPS-compliant mode, then FreeFlow Core becomes non-compliant with cryptographic requirements.

Data Encryption

File Processing

FreeFlow Core does not explicitly encrypt files submitted for processing before the file is stored in the file system of the personal computer.

User Account Access and Job Retention

User Account Passwords

Reuse of passwords is allowed.

User Account Lockout

If authentication fails with FreeFlow Core, users are not locked out after failed attempts.

User Account Log Out

After 30 minutes of inactivity, logged-in users are logged off automatically. The duration of the inactivity period is not configured.

User Account Activity

The audit log of user login transactions to FreeFlow Core is not available.

Job Retention

After a job completes processing, the retention period for the jobs in FreeFlow Core is 24 hours.

The FreeFlow Core printer is configured to change the retention period before completed jobs are removed automatically. After 24 hours, the FreeFlow Core device removes completed jobs.

To remove jobs manually, use the FreeFlow Core Web GUI.

4

Security

This chapter contains:

At Xerox, security issues are front and center. As a leader in the development of digital technology, Xerox demonstrates a commitment to keep the digital information safe and secure, identify the potential vulnerabilities, and address the issues proactively to limit risks.

Xerox strives to provide the most secure software devices possible, based on the information and technologies available, while maintaining device performance, value, functionality, and productivity.

The components of Xerox® FreeFlow® Core are assessed for security compliance using commercially available vulnerability and penetration scanning tools. Application vulnerabilities are addressed based on results of Xerox scans.

Xerox distributes security bulletins when required. Security bulletin information is communicated on the Xerox Security website at https://www.xerox.com/security for Product Security Guidance. The website contains up-to-date security vulnerability printer status, white papers, Common Criteria Certification, Intel Security McAfee Information, and a portal to submit security questions to Xerox.

Virus Protection

Xerox takes special precautions to ensure that Xerox software is shipped free from computer virus contamination. The personal computer industry experts recommend Xerox to everyone looking for virus-detection software. To protect your printer from viruses, it is imperative that virus-detection software is kept up-to-date.

To improve performance, it is recommended that you exclude the Xerox® FreeFlow® Core and SQL Server installation directories from antivirus scans.

You can exclude the following files from the antivirus scans:

- `<FreeFlow Core Installation directory>\Logs`
- `<FreeFlow Core Installation directory>\Platform\Logs`
- `<FreeFlow Core Installation directory>\JobSubmit\Logs`
- `<FreeFlow Core Installation directory>\Config`
- `<FreeFlow Core Installation directory>\Platform\Config`
- `<FreeFlow Core User Data Directory>\`
- Folders outside the FreeFlow Core User Data directory that are used by FreeFlow Core

5

Software Update

It is recommended that customers keep up-to-date software for all the software devices installed on the Xerox® FreeFlow® Core server. Perform a Microsoft Windows update at least once a month.

You can find software updates for FreeFlow Core at https://www.support.xerox.com/support/core/software/enus.html. Customers can install the software update.