Xerox FreeFlow Core 5.0 (5.0.0.0)
July 2016
702P04448

Xerox® FreeFlow® Core
Security Guide

Printed in the United States of America.

Changes are periodically made to this document. Changes, technical inaccuracies, and typographical errors will be corrected in subsequent editions.

BR14707

Document Version: 1.0 (July 2016).

Table of Contents

1

Preface

General Purpose

The purpose of this document is to disclose information related to Xerox® FreeFlow® Core and FreeFlow Core Cloud with respect to product security. Please note that the customer is 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 relative to FreeFlow Core.

Disclaimer

To the best knowledge of our knowledge, 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

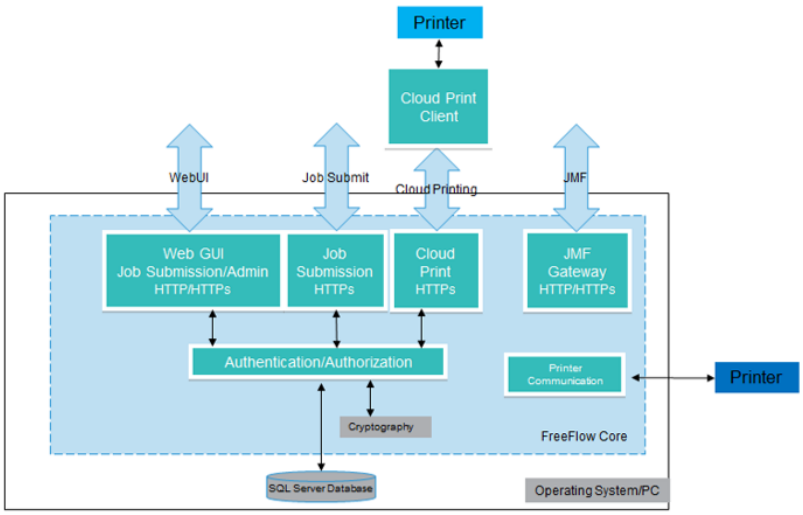
Product Description

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

FreeFlow® Core Cloud is the cloud-based configuration offering of the solution. Running in the cloud means Xerox will install the software on our cloud servers. We will configure and manage the solution maintenance. You simply access your dedicated and secure system from a web browser.

Security-related Connectivity

The security-related connectivity for the product is depicted below.



3

System Access

Network Connections

FreeFlow Core requires network connectivity for both job processing and user interactions. Security considerations for each network connection are documented below.

FreeFlow Core Client

When a browser connects to the FreeFlow Core webpage, a Silverlight client is downloaded to the browser. Secure download of the FreeFlow Core client and secure communication between the client and FreeFlow Core requires the use of HTTPS connections. To enable HTTPS connections, a TLS/SSL certificate must be added to Internet Information Services (IIS) per the Windows documentation.

Unless the user downloads job files, no customer data is exchanged between the client and the FreeFlow Core server.

Note

The client retrieves job properties, which may contain customer data.

Table 1: Firewall Configuration

Port	Protocol or Application	Firewall Connection Type
80	HTTP	Inbound **Note** Port number depends on IIS server configuration

Port	Protocol or Application	Firewall Connection Type
443	HTTPS	Inbound **Note** Port number depends on IIS server configuration

User Roles

By default, FreeFlow Core opens to a login screen. The user must log in for access to the system. Logged in users are automatically logged off after 30 minutes of inactivity.

Administrator

The administrator has access to the entire system:

- Job Management and Status tab functions: Submit Job Dialog and Job Status Tab.
- Printer Management and Status Tab
- Workflow Setup
- Administration tab functions: Hot Folder Setup, Notifications Setup, User Access Setup
- Core Server Utilities (available on 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.

One Administrator may be logged in to FreeFlow Core at any given time.

Operator

The Operator has access to the following:

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

Multiple operators may be concurrently logged in to FreeFlow Core.

Job Status Monitor

The Job Status Monitor has read-only access to the Job Status Tab window. Multiple job status monitors may be concurrently logged in to FreeFlow Core.

Multiple job status monitors may be concurrently logged on to Xerox® FreeFlow® Core.

User Authentication

Credentials entered into the FreeFlow Core Silverlight client are encrypted before they are sent to the FreeFlow Core server.

If authenticating using FreeFlow Core users, encrypted credentials are stored locally.

If authenticating using Active Directory, the credentials are unencrypted before they are submitted to Active Directory. When authenticating via Active Directory, credentials are not stored locally.

FreeFlow Core's configuration's connection to Active Directory is encrypted per the operating system's configuration.

Table 2: Firewall Configuration

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

SQL Server Connection

FreeFlow Core communicates with SQL Server using Microsoft's Entity Framework. Encrypted communication between FreeFlow Core and SQL Server is enabled when SQL Server is configured to use encrypted connections.

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

To install on a remote SQL Server without SQLS Administrative privileges:

- Create two empty databases in the SQLS Instance
  - OapMasterDatabase
  - OapPlatformDatabase
- Assign ownership of the databases to a service account
- When installing FreeFlow Core, use the same service account for the SQL System Administrator
- If enabling the use of Windows Shared Directories or Microsoft Office conversion, use the same service account when performing the Optional Installation Procedures

Table 3: Firewall Configuration

Port	Protocol or Application	Firewall Connection Type
1433	SQLS	Inbound – Receiving connections from FreeFlow Core Outbound - Communicating with SQL Server Database Engine **Note** Port number depends on SQLS server configuration.
1434	SQLS Browser Service	Inbound – Receiving connections from FreeFlow Core Outbound - Communicating with SQL Server Database Engine **Note** Server will provide client with port number for connection.

Submit Job User Interface

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

Table 4: Firewall Configuration

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

Hot Folders

File shares used for sharing a local hot folder and for accessing a Hot Folder in shared Windows folders may be encrypted using the Windows file system or protected using Windows user account access control. When using user account access control use the same service account configured when performing the Optional Installation Procedures.

Table 5: Firewall Configuration

Port	Protocol or Application	Firewall Connection Type
139, 445	SMB	Inbound - Sharing Hot Folders via Windows File Sharing Outbound - Using Hot Folders on Shared Directories
20, 21	FTP	Inbound - Sharing Hot Folders via FTP

Manifest Processing

During Manifest submission, FreeFlow Core retrieves the files listed in the manifest. These files may be referenced using mapped drives or UNC file paths, HTTP, or FTP URIs.

Note

HTTP and FTP URIs do not support encryption.

File shares used for sharing local folders and for accessing shared Windows folders may be encrypted using the Windows file system or protected using Windows user account access control. When using user account access control use the same service account configured when performing the Optional Installation Procedures.

Table 6: Firewall Configuration

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

JMF Commands and Status Signals

JMF commands support secure connections. However, JMF file retrieval uses unencrypted connections. Secure JMF submission requires the submission of a MIME package with the JMF, JDF, and PDF files.

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

To enable, HTTPS communication, for JMF commands:

- Use the installJMFCertificate.bat utility in the FreeFlow Core installation directory to add a certificate to the Java keystore.
- Restart the FreeFlow Core JMF Server service.
- Test installation by going to **http://<hostname>:7759**. If secure JMF is properly configured, the browser will display an HTTP Status 404 error page.

Table 7: Firewall Configuration

Port	Protocol or Application	Firewall Connection Type
7751	JMF	Inbound - Receiving JMF commands
Varies	JMF	Outbound - Return JMF status signals **Note** Required port number is defined by the client requesting the JMF status signals or the Return JMF signal.
7759	sJMF	Inbound - Receiving secure JMF commands

FreeFlow Core Submit

The connection between the FreeFlow Core Submit and FreeFlow Core is always encrypted and requires installation of a TLS/SSL certificate. To install the certificate on the server, the TLS/SSL certificate should be added to Internet Information Services (IIS) per the Windows documentation.

The FreeFlow Core Submit application and Microsoft Office Add-Ins use the same secure connection to FreeFlow Core.

Encrypted credentials are stored locally.

Table 8: Firewall Configuration

Port	Protocol or Application	Firewall Connection Type
443	HTTPS	Inbound (in the server) – Accepting connections from the FreeFlow Core Submit client. Outbound (in the client) – Submitting jobs to FreeFlow Core Cloud

Workflow Nodes

Workflow components that retrieve or save job files may use mapped drives, UNC file paths, HTTP, or FTP URIs. HTTP and FTP URIs do not support encryption.

File shares used for sharing local folders and for accessing shared Windows folders may be encrypted using the Windows file system or protected using Windows user account access control. When using user account access control use the same service account configured when performing the Optional Installation Procedures.

Table 9: Firewall Configuration

Port	Protocol or Application	Firewall Connection Type
139, 445	SMB	Outbound – Retrieving files specified in workflow component preset. Outbound – Saving files to shared directories.
20, 21	FTP	Outbound – Retrieving files specified in workflow component preset.

Port	Protocol or Application	Firewall Connection Type
80	HTTP	Outbound – File shares used for sharing local folders and for accessing shared Windows folders may be encrypted using the Windows file system or protected using Windows user account access control. When using user account access control use the same service account configured when performing the Optional Installation Procedures. Retrieving files specified in workflow component preset.

FreeFlow Core Printing

FreeFlow Core uses SNMP or HTTP to determine the DFE type. This is done using an unencrypted connection.

The following operations also use an unencrypted connection:

- Retrieving the list of DFE queues
- Retrieving printer capabilities
- Retrieving job status
- Submitting job operations
- Retrieving job accounting information

Print submission may be encrypted when connecting to a DFE that is configured to support secure IPP. To enable secure IPP print submission:

- Add a certificate to FreeFlow Print Server
- Select the **Enable SSL/TLS** option under FreeFlow Print Server Setup
- Use the FreeFlow Core Certificate to retrieve a TLS/SSL certificate from the FreeFlow Print Server

  Note

  A **Certificate successfully installed** message indicates secure IPP is properly configured

Once properly configured, secure IPP is enabled via the Secure Printing option in the Printer Destination setup.

Table 10: Firewall Configuration

Port	Protocol or Application	Firewall Connection Type
161, 162	SNMP	Outbound – Identifying DFE type during Printer Destination setup and Certificate Retrieval.
80	HTTP	Outbound – Identifying DFE type during Printer Destination setup and Certificate Retrieval.
N/A	ICMP	Outbound – Check device availability before Certificate Retrieval.
631	IPP	Outbound – Submitting jobs to DFEs, getting job status, and submitting job commands to the DFE.
443	HTTPS	Outbound – Submitting jobs to DFE.

FreeFlow Core Cloud Print

The connection between the FreeFlow Core Cloud Print server and client is always encrypted and requires installation of a TLS/SSL certificate.

To install the certificate on the server, the TLS/SSL certificate should be added to Internet Information Services (IIS) per the Windows documentation.

The connection between the FreeFlow Core Cloud Print client and the DFE does not support secure IPP.

Encrypted credentials are stored locally.

Table 11: Firewall Configuration

Port	Protocol or Application	Firewall Connection Type
161, 162	SNMP	Outbound - Identifying DFE type during Printer Destination setup.
631	IPP	Outbound - Submitting jobs to DFEs, getting job status, and submitting job commands to the DFE.

Port	Protocol or Application	Firewall Connection Type
443	HTTPS	Inbound (in the server) - Accepting connections from the FreeFlow Core Cloud Print client. Outbound (in the client) - Connecting to the FreeFlow Core Cloud Print server.

Email Notification

FreeFlow Core is an email client and connects to a customer's email server. Email notifications may be encrypted when connecting 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 12: Firewall Configuration

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

4

Security

At Xerox, security issues are front and center. As a leader in the development of digital technology, Xerox has demonstrated a commitment to keeping digital information safe and secure by identifying potential vulnerabilities and proactively addressing them to limit risk. Xerox strives to provide the most secure software product possible based on the information and technologies available while maintaining the products 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 our internal scans.

Xerox distributes security bulletins when required. This information is communicated on the Xerox Security website at: www.xerox.com/security under Product Security Guidance.

Virus Protection

Xerox takes special precautions to ensure its software is shipped free from computer virus contamination. It is strongly recommended that you invest in a virus detection software application that is accepted by the PC industry. To protect your system from viruses it is imperative that virus detection software is kept up to date.

To improve performance, it is recommended that you exclude the FreeFlow Core and SQL Server installation directories from anti-virus scans.

Alternatively, the following FreeFlow Core folders may be excluded from anti-virus scanning:

- <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 Sandbox>\
- Folders outside the Sandbox used by FreeFlow Core

5

Software Update

It is recommended that the customer keep all software products installed on the FreeFlow Core server up to date. Microsoft Windows Update should be performed on at least a monthly basis.