Xerox® FreeFlow® Digital Publisher

Information Assurance Disclosure

Onsite, Cloud and ePublishing Configurations

January 2017

©2017 Xerox Corporation. All rights reserved. Xerox® and Xerox and Design® are trademarks of Xerox Corporation in the United States and/or other countries. Other company trademarks are also acknowledged.

Document Version: 2.2 (January 2017).

Preface

Purpose

The purpose of this document is to disclose information for the Xerox® FreeFlow® Digital Publisher product with respect to system security. System Security, for this paper, is defined as follows:

1) How input jobs are received, accessed, and transmitted

2) How user information is stored and transmitted

3) How the product behaves in a networked environment

4) How the product may be accessed, both locally and remotely

Please note that the customer is responsible for the security of their network. The FreeFlow Digital Publisher solution does not establish security for any network environment. The purpose of this document is to inform Xerox customers of the design, functions, and features of the Xerox FreeFlow Digital Publisher solution relative to Information Assurance (IA). This document does NOT provide tutorial level information about security, connectivity, PDLs, mobile apps, or Xerox FreeFlow Digital Publisher solution features and functions. This information is readily available elsewhere. We assume the reader has a working knowledge of these types of topics.

FreeFlow Digital Publisher normally is configured to use encrypted (recommended) data paths; however, it can be configured to use unencrypted (not recommended) data paths.

Target Audience

The target audiences for this document are customer IT and network security personnel and Xerox field personnel.

Disclaimer

The information in this document is accurate to the best knowledge of the authors, and is provided without warranty of any kind. In no event shall Xerox Corporation be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this document including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of such damages.

Table of Contents

1 System Configuration

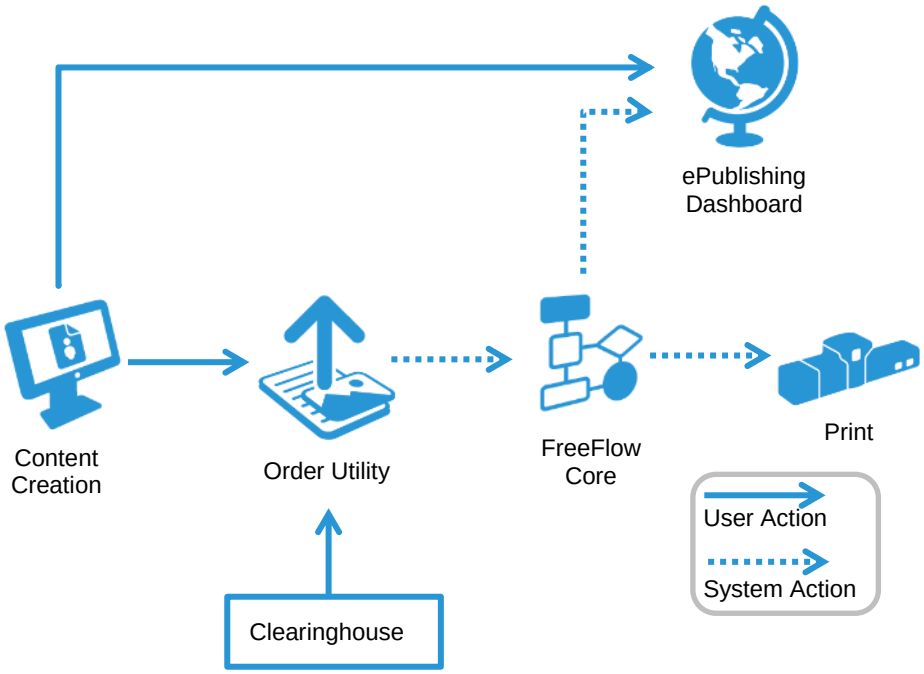
1.1 System Overview

There are three major components in FreeFlow Digital Publisher that move commands and data within the system. They are:

1. FreeFlow Digital Publisher Order Utility: Used by the print shop to submit print and ePublishing jobs into FreeFlow Core. All jobs begin with this utility. For customers using pre-paid credits, their credit balance is available from an API call to a clearinghouse system.

2. FreeFlow Core: an automation system for preparing jobs for printing and / or for ePublishing.

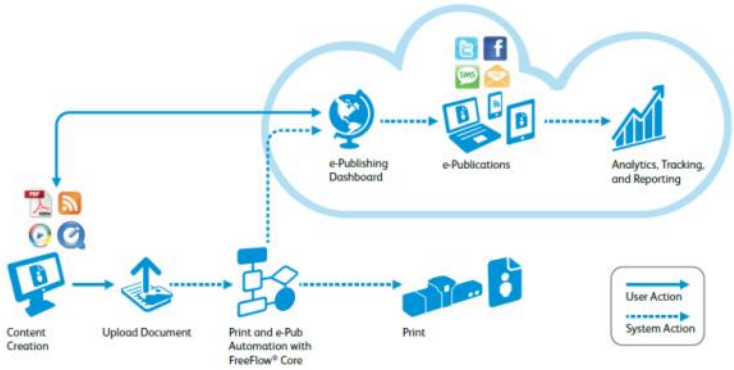
3. ePublishing Dashboard: completes the conversion of files received from Core for web and mobile-device use. Print shop personnel have access to ePublications to add videos, audio files, links, control layout, and preview as needed. When ready, the publications are approved and made available to end-users.



1.2 Configuration Diagrams

FreeFlow Digital Publisher supports three configurations: On-Premise, Cloud, and ePublishing. All three have the same data paths except that FreeFlow Core is either at the print shop site or in the cloud, and there are no printing paths with the FreeFlow Digital Publisher ePublishing configuration.

1. FreeFlow Digital Publisher On Premise.

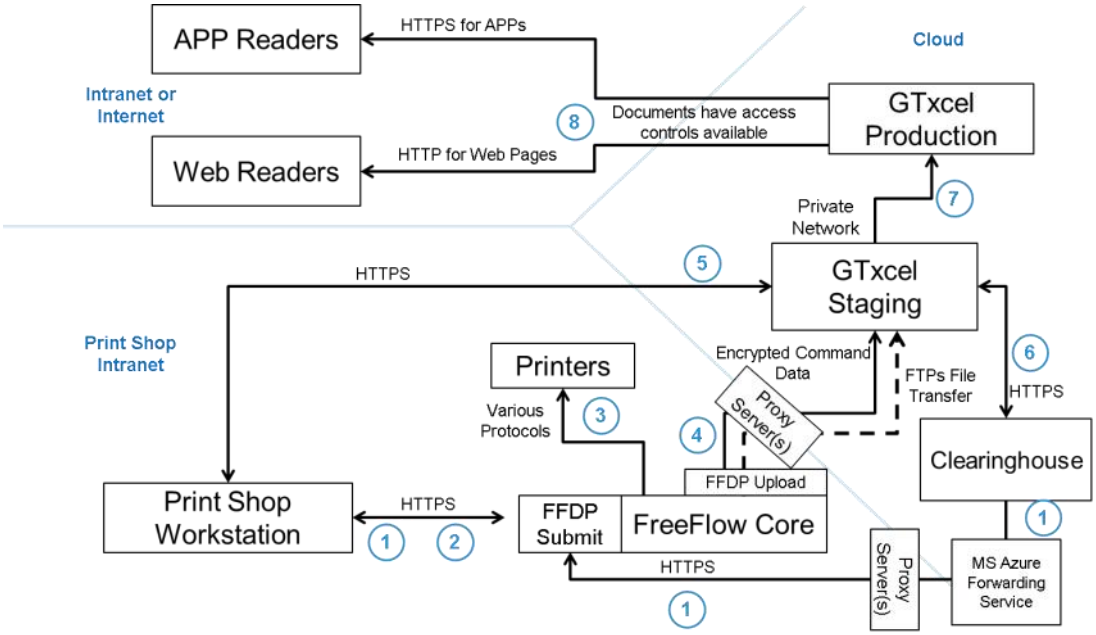


2. FreeFlow Digital Publisher Cloud

3. FreeFlow Digital Publisher ePublishing

1.3 On Premise Network Diagram

Below is a diagram of the network for the On Premise configuration. There are three sections: Print shop intranet that originate the documents and begin processing. Cloud servers that complete the processing and store the documents. And end customers that access the documents via smartdevices, PCs or MACs from an intranet or internet connection.

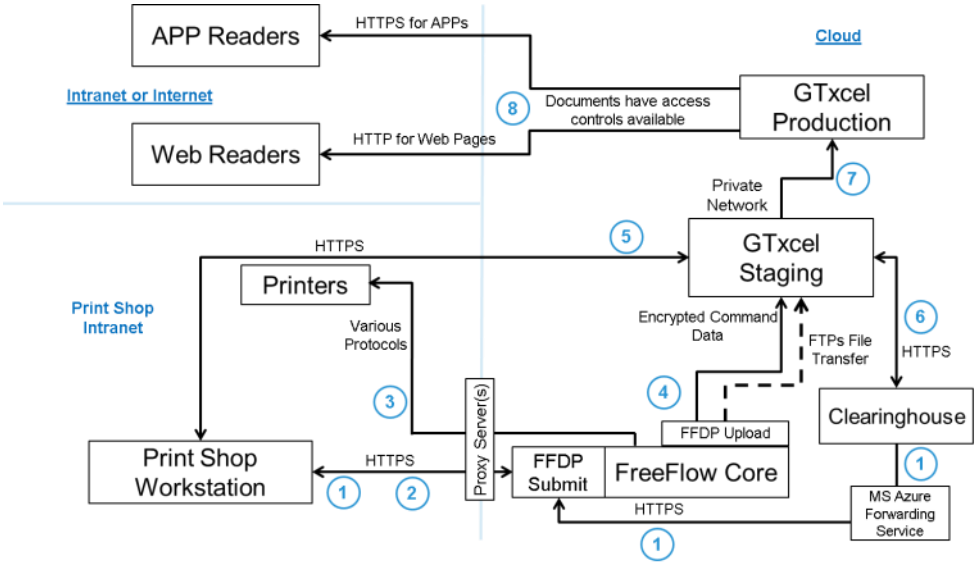


Data Flow Descriptions

1) An operator, using FFDP Submit, can view current credit balance from the Clearinghouse (for print shops using prepaid credits only). Communication is via MS Azure Forwarding Service.
2) An operator submits documents for printing and / or ePublishing
3) FreeFlow Core process documents for printing
4) FreeFlow Core process documents for ePublishing and uploads to GTxcel Staging servers.
5) An operator can preview & enhance ePublished document in preparation for publishing.
6) GTxcel staging will update credits used (for those customers using prepaid credits)
7) An operator will publish a document, which will move the document to GTxcel Production servers
8) End customers will access ePublications using the APP or Web Readers.

1.4 Cloud/ePublishing Network Diagram

Below is a diagram of the network for the Cloud or ePublishing configuration. This differs from the On Premise configuration whereby FreeFlow Core, FFDP Submit, FFDP Upload are now running on a cloud server. Otherwise the processing is the same.



Data Flow Descriptions

1) An operator, using FFDP Submit, can view current credit balance from the Clearinghouse (for print shops using prepaid credits only). Communication is via MS Azure Forwarding Service.
2) An operator submits documents for printing and / or ePublishing
3) FreeFlow Core process documents for printing
4) FreeFlow Core process documents for ePublishing and uploads to GTxcel Staging servers.
5) An operator can preview & enhance ePublished document in preparation for publishing.
6) GTxcel staging will update credits used (for those customers using prepaid credits)
7) An operator will publish a document, which will move the document to GTxcel Production servers
8) End customers will access ePublications using the APP or Web Readers.

1.5 Public URLs

There are a series of public URLs that the system must be able to access. These are listed in the applicable sections below. The current IP address of each server is provided, however, IP addresses are subject to change without notice.

In addition, the URL for each publication “Title” stored on the Production server follows a pattern based upon the publication title:

<Title>.FreeFlowDP.com/<Title>/<Unique Identifier>

Note: some print shops have arranged for a custom URL that will follow the pattern they arranged.

2 Port / Protocol Description

Xerox® FreeFlow® Digital Publisher requires network connectivity for both job processing and user interactions. Security considerations for each network connection are documented below. FreeFlow Core has its own security document located at http://www.support.xerox.com/automate in the Support and Drivers section, under Documentation. That information is not duplicated within this document.

2.1 Xerox FreeFlow Digital Publisher Order / Submission

The Xerox FreeFlow Digital Publisher Order utility is installed on the same server as FreeFlow Core. Communication is via a browser within the print shop. The IP address and URL are unique to each installation.

When a browser connects to the Xerox® FreeFlow® Digital Publisher Order webpage, an HTML 5.0 page will be downloaded to the browser. If a security certificate is installed on the server, the page is downloaded using HTTPs, else HTTP is used.

Port	Protocol or Application	Firewall Connection Type
80	HTTP	Unencrypted (if no security certificate installed)
443	HTTPs	TLS/SSL Encrypted upon installation of SSL certificate **Note** Actual Port numbers used depend upon IIS settings.

2.1.1 User Authentication

Credentials entered into the Xerox® FreeFlow® Digital Publisher Order HTML client login are encrypted before they are sent to the Xerox® FreeFlow® Digital Publisher server using an unencrypted connection.

If authenticating with Xerox® FreeFlow® Digital Publisher users, encrypted credentials are stored locally. If authenticating with Active Directory, then credentials are unencrypted before they are submitted to Active Directory. The connection to Active Directory is encrypted per the operating system's configuration. If authenticating via Active Directory, credentials are not stored locally.

The Configuration Tool's connection to Active Directory (AD) is encrypted per the operating system's configuration.

Port	Protocol or Application	Firewall Connection Type
80	HTTP	Unencrypted (if no security certificate installed)
443	HTTPs	TLS/SSL Encrypted upon installation of SSL certificate **Note** Actual port numbers used depend upon IIS settings.
88	Kerberos	Outbound - User Authentication **Note** Actual port number 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** Actual port numbers and services used depend on server's AD configuration.

2.1.2 SQL Server Connection

The Xerox® FreeFlow® Digital Publisher Submission component communicates with SQL Server using Microsoft's Entity Framework. Encrypted communication between Xerox® FreeFlow® Digital Publisher and SQL Server is enabled when SQL Server is configured to use encrypted connections.

Encrypted SQL Server (SQLS) credentials are stored locally within the Xerox® FreeFlow® Digital Publisher server.

When using SQL Server Express, the software is installed on the same server as FreeFlow Digital Publisher Submission and FreeFlow Core. A separate SQL Server is also installed. The IP address and URL is customer specific.

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

2.1.3 Job Submit

This action moves input files to the server.

If a security certificate is installed on the server, the Submit Job UI uses an encrypted connection between the Printshop workstation connected to the Xerox® FreeFlow® Digital Publisher client and the server.

Port	Protocol or Application	Firewall Connection Type
80	HTTP	Inbound Unencrypted (if no security certificate installed)
443	HTTPs	TLS/SSL Encrypted upon installation of SSL certificate **Note** Actual Port numbers used depend upon IIS settings.

2.1.4 Hot Folders

Windows automatically encrypts the file sharing connections used for sharing local hot folders and for accessing Hot Folders in shared windows folders.

2.1.5 GTxcel Publisher Staging Service

Xerox® FreeFlow® Digital Publisher communicates to GTxcel Publisher Rest Service to fetch the Titles and Publisher for the given user using an encrypted HTTPS line.

Port	Protocol or Application	Firewall Connection Type
443	HTTPS	Inbound **Note** Actual Port number used depends upon IIS settings.
The URL for the dashboard is: https://dashboard.freeflowdp.com/rest/services **Current IP address is: 107.154.146.128**		

2.1.6 Security Certificate

GTxcel Publisher Rest Service uses a security certificate issued by GlobalSign, an identity services company. The security certificate name is Globalsign CloudSSL CA - SHA256 - G3 for HTTPS communication between the client and the server.

Note:
The security certificate must be installed on the server running Xerox® FreeFlow® Digital Publisher. In addition, the host network where Xerox® FreeFlow® Digital Publisher is installed must add this certificate to their trusted certificate group in case the certificate issuer is not recognized from their network.

2.1.6 Xerox® FreeFlow® Digital Publisher Upload Tool

Xerox® FreeFlow® Digital Publisher upload tool communicates with the GTxcel server for file transfer and commands. The Xerox® FreeFlow® Digital Publisher upload tool uses FTP for uploading files to the GTxcel server and uses HTTPS for sending commands.

Port	Protocol or Application	Firewall Connection Type
443	HTTPS	Inbound **Note** Actual Port number used depends upon IIS settings.
20	FTP	Outbound (Data Line)
21	Passive FTPs / FTP	Inbound/Outbound (Command Line) **Note** FTPs is implemented using Explicit mode to support Non-FTPs aware clients
51000-51030	FTPs	Outbound (Data Line) **Note** FTPs dynamic port
The URL for FTP and FTPs is: **ftp://uploads.freeflowdp.com** **Current IP address is 69.147.179.203**		

The GTxcel FTPs Server is implemented using Explicit FTPs Passive mode protocol, and Xerox® FreeFlow® Digital Publisher Upload tool uses this protocol to communicate with the GTxcel FTPs server.

1. From Port 21, the Xerox® FreeFlow® Digital Publisher Upload tool initiates the FTPs communication with the GTxcel FTPs Server by explicitly asking for an SSL handshake, which is initiated upon issuing either the AUTH TLS or AUTH SSL command from the client using port 21.
2. Upon successful authentication, a random port number is specified by the GTxcel FTPs server from the dynamic port range 51000 – 51030 for the Xerox® FreeFlow® Digital Publisher Upload tool to establish a secure data channel for transferring data. The dynamic port range is allowed at the server so multiple clients can talk to the server using various ports simultaneously.
3. The Xerox® FreeFlow® Digital Publisher Upload tool establishes another TCP connection (Data line) to the random port of the server from the host network over which the files are transferred. The communication channel via port 21 for command exchange will be open until the operation completes.

See Section 3 - Appendix for additional information on FTP modes and operation.

2.1.7 Clearinghouse System

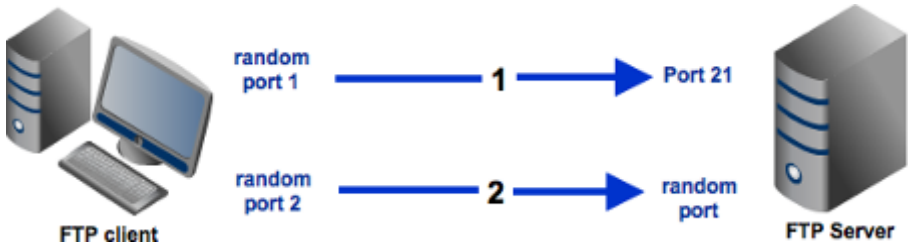
Xerox® FreeFlow® Digital Publisher communicates with a Clearinghouse System to track credits using an encrypted HTTPS line. The Clearinghouse System is using the Azure Forwarding service hosted on the Azure Cloud for fetching the credits. The Xerox® FreeFlow® Digital Publisher communicates with this service in order to access the Clearinghouse System.

Port	Protocol or Application	Firewall Connection Type
443	HTTPS	Inbound **Note** Actual Port number used depends upon IIS settings.
The Service URL is: **https://xeroxchsprod.servicebus.windows.net/OrderingService/customerCreditBalanceQuery** **Current IP address is 168.61.148.205** **The URL to access the Azure Forwarding service is: https://xeroxchsprod-sb.accesscontrol.windows.net/WRAPv0.9/** **Current IP address is 23.99.129.64**		

3 FTP Mode Description

Active and passive are the two modes in which FTP can run. FTP opens two channels between the client and the server -- the command channel and the data channel (which are actually separate TCP connections). The command channel is for commands and responses. The data channel is for actually transferring files. It's an efficient way to send commands to the server without having to wait for the current data transfer to finish.

Passive mode is generally used in situations where the FTP server is not able to establish the data channel. One of the major reasons for this is network firewalls.



Two separate methods were developed to invoke client security for use with FTP clients: Implicit and Explicit. The implicit method requires that Transport Layer Security is established from the beginning of the connection, which in turn breaks the compatibility with non-FTPS-aware clients and servers. The explicit method uses standard FTP protocol commands and replies in order to upgrade a plain text connection to an encrypted one, allowing a single control port to be used for serving both FTPS-aware and non-FTPS-aware clients.

FreeFlow Digital Publisher normally uses FTPs Passive Mode with Explicit Method. FreeFlow Digital Publisher can be configured for standard, unencrypted FTP, though this is not recommended.

3.1 Implicit

Negotiation is not supported with implicit FTPS configurations. A client is immediately expected to challenge the FTPS server with a TLS ClientHello message. If such a message is not received by the FTPS server, the server should drop the connection.

3.2 Explicit

In explicit mode (also known as FTPES), an FTPS client must "explicitly request" security from an FTPS server and then establish a mutually agreed upon encryption method. If a client does not request security, the FTPS server can either allow the client to continue in insecure mode or refuse the connection.