Security Guide

Xerox® FreeFlow® Variable Information Suite

Printed in the United States of America.

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

BR38355

Contents

1. Introduction

Purpose

The purpose of the Security Guide is to disclose information related to Xerox® FreeFlow® VI eCompose and Xerox® FreeFlow® VI Design Express, part of the Xerox® FreeFlow® VI Suite, regarding product security. Product security, in this context, is defined as how data is stored and transmitted, how the product behaves in a networked environment, and how the product is accessed, both locally and remotely. This document describes the design, functions, and features of Xerox® FreeFlow® VI eCompose and Xerox® FreeFlow® VI Design Express relative to Information Assurance (IA), and the protection of customer-sensitive information.

This document does not provide tutorial-level information about security, connectivity, or Xerox® FreeFlow® VI eCompose and Xerox® FreeFlow® VI Design Express features and functions. This information is readily available elsewhere. It is assumed that the reader has a working knowledge of these types of topics.

> **Note**: 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 regarding FreeFlow VI eCompose or FreeFlow VI Design Express software. It is assumed that the reader is familiar with the software. Therefore, some user actions are not described in detail.

Disclaimer

To the best 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

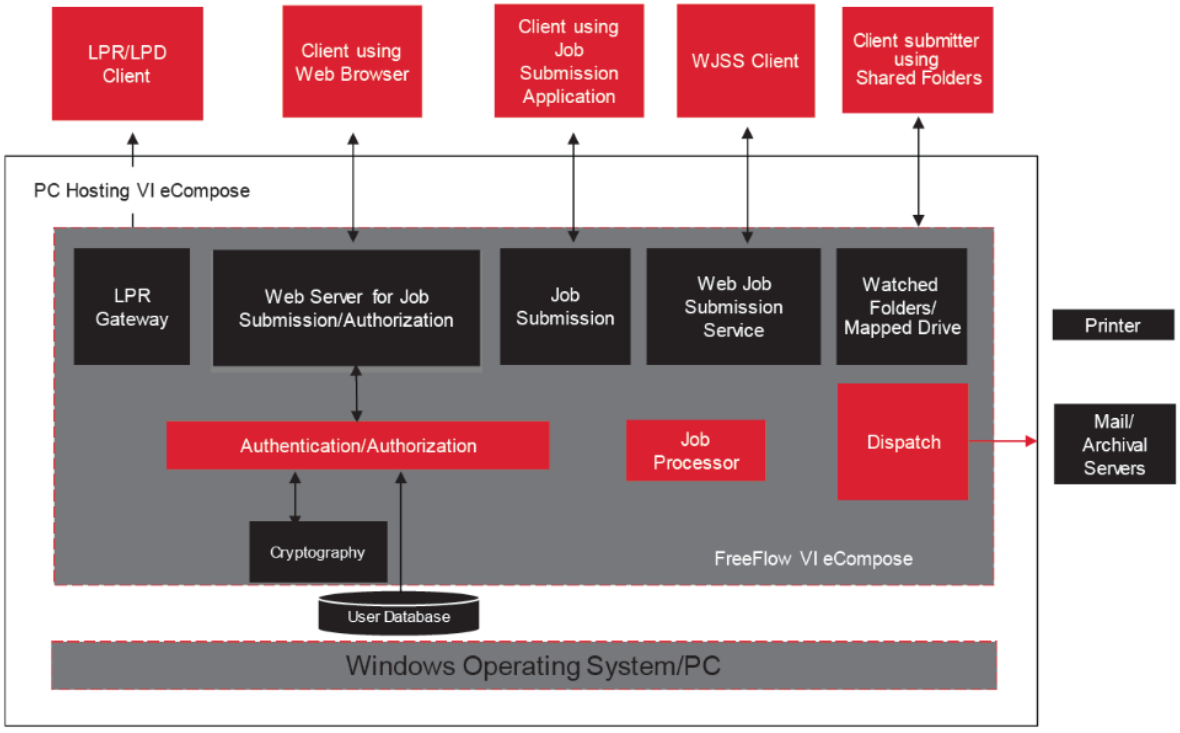
Xerox FreeFlow VI eCompose is a client-server application that allows you to generate Adobe PDF documents from VIPP® based variable data applications and forward the PDFs to other processes within the environment. VI eCompose extends the VIPP® workflow into electronic distribution and archive, by providing the ability to generate Adobe PDF files from the same data files sent to a VIPP® enabled print device. After, the PDF files, along with information from the data record that produced them, can be passed to a user-defined process using the VI eCompose Dispatch module. The files can be integrated into processes within the environment, which can include email servers or archive systems. In addition, the VI eCompose Server can forward the data submission file or the Master PDF file to an identified VIPP® enabled print device available in the Printer dialog box on the Windows server for hard copy output.

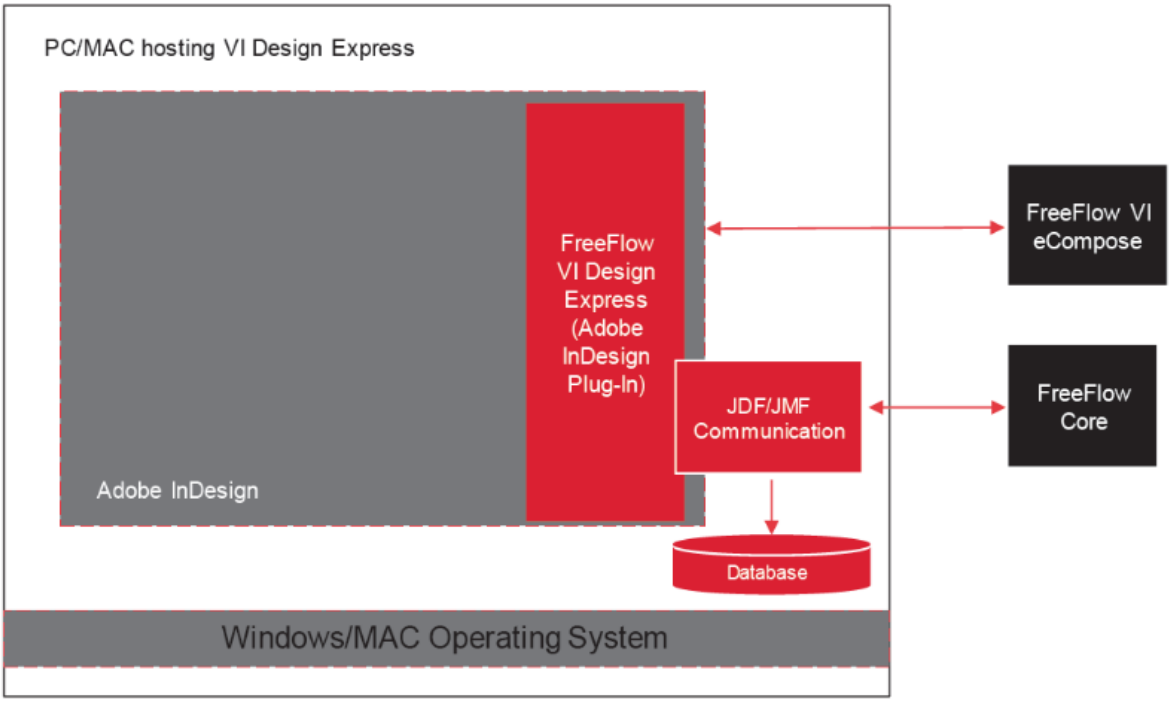
Xerox FreeFlow VI Design Express is a client application that allows you to generate Adobe PDF documents from VIPP® based variable data applications and forward the PDFs to other processes within the environment. VI Design Express is a plug-in to the Adobe InDesign application. VI Design Express generates Adobe PDF documents, which can be forwarded to an identified VIPP® enabled print device. VI Design Express can forward VIPP® files in VI Project Container format to applications such as FreeFlow Core and FreeFlow VI eCompose for further processing.

These Security highlights are relevant to the App Gallery system:

System Software Structure

The system software structure for the product is depicted.





3. Security Aspects of Selected Features

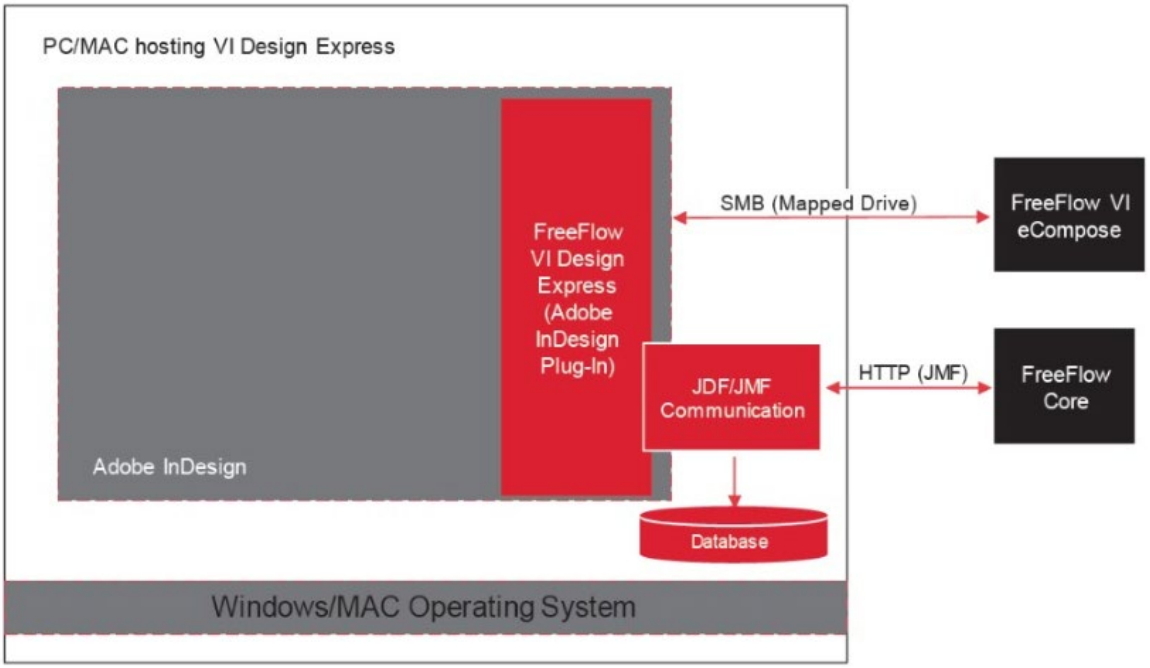
System Access

NETWORK CONNECTIONS

FreeFlow VI Design Express

FreeFlow VI Design Express software requires network connectivity for job submission to VIPP® enabled printers and other applications such FreeFlow Core. Security considerations for each network connection are documented in this guide.

This diagram shows FreeFlow VI Design Express network connections.



From FreeFlow VI Design Express, VIPP® jobs are sent to the FreeFlow Core server over HTTP using the JMF protocol.

After a job is submitted to FreeFlow Core, the status of the submitted jobs is displayed. Job status information is obtained by sending a job status request or receiving a job status signal from FreeFlow Core over HTTP using the JMF protocol. Jobs sent to FreeFlow VI eCompose are sent to a VI eCompose designated root directory path, which is a Windows shared folder. After the job is submitted, the status of the submitted job is shown at VI DesignExpress. The System administrator is responsible to set the proper security permissions on the designated root directory to be accessible by authorized users.

Table 1. Firewall Configuration for FreeFlow VI Design Express

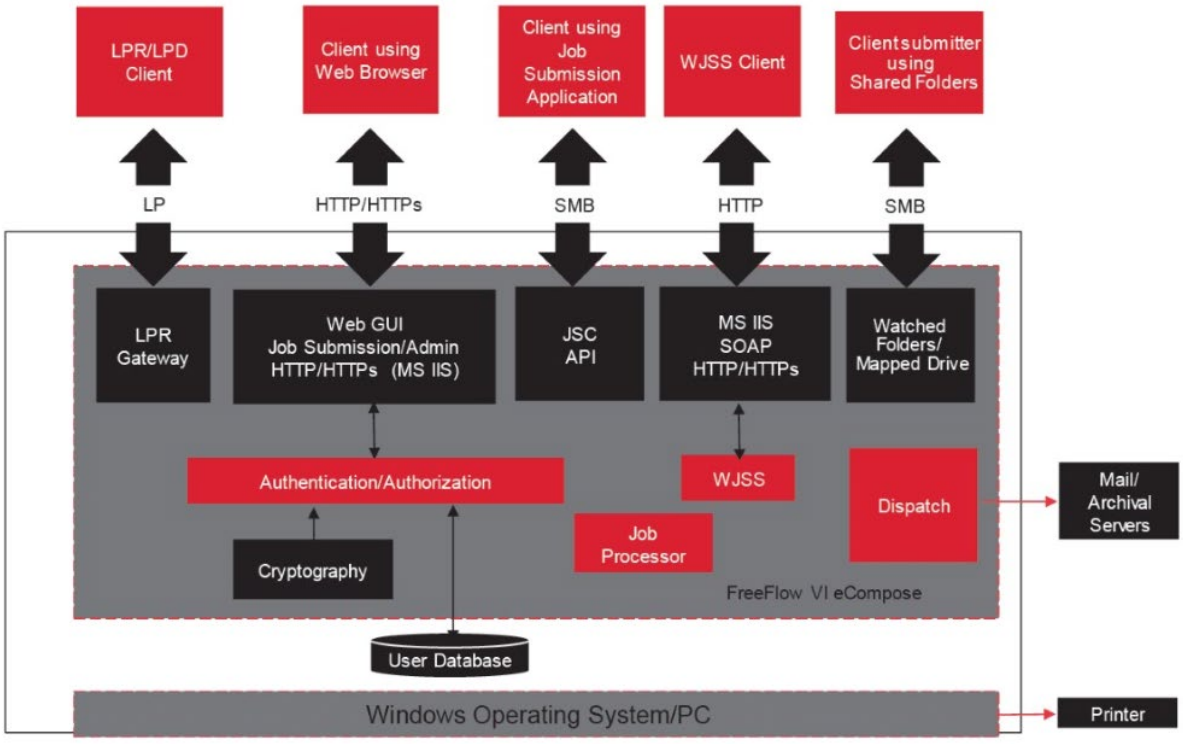
Port	Protocol or Application	Firewall Connecion Type
7751	HTTP	Outbound: Submit VIPP® jobs to Xerox FreeFlow Core and obtain job status from FreeFlow Core
8080	HTTP	Inbound: Receive job status information from FreeFlow Core **Note**: To change the port number, update the file C:\Program Files (x86)\Xerox\VIPP\VDE\jmfconnector \config\jmfClient.properties.
139.145	SMB	Inbound: Shared Root Directory using Windows file sharing Outbound: Shared Root Directory using shared directories

FreeFlow VI eCompose

FreeFlow VI eCompose software requires network connectivity for job submission from clients, and requires a Web browser for job processing and administration. Security considerations for each network connection are documented in this guide.

> **Note:** To provide better security protection against vulnerability attacks, Windows Firewall is required. Enable Windows Firewall on the server where VI eCompose is installed, unless your site has its own firewall requirements.

The diagram shows FreeFlow VI eCompose network connections.



FreeFlow VI eCompose

The FreeFlow VI eCompose server allows clients using a Web browser to submit VIPP® jobs and perform administration functions on the server. The Web Server is provided by Microsoft Internet Information Services (IIS) and can be enabled optionally during installation of the FreeFlow VI eCompose software.

The web browser communicates with FreeFlow VI eCompose server using HTTP or HTTPS. The web application for FreeFlow VI eCompose can be configured to use Basic Authentication. Enabling HTTPS connectivity requires a valid CA certificate installed on the system. For information on configuring the system for HTTPS with TLS, HTTP Basic Authentication and starting and stopping the VI eCompose Web application, refer to the *FreeFlow VI eCompose User Guide*.

You can submit VIPP® jobs using LPR, watched folders, and WJSS. To allow job submissions from LPR clients, FreeFlow VI eCompose relies on enabled services for the Windows TCP/IP print server and the print spooler.

> **Note:** The client can retrieve a VIPP® job that is converted to a PDF. The PDF can contain customer data.

Table 2. Firewall Configuration for FreeFlow VI eCompose

Port	Protocol or Application	Firewall Connecion Type
80	HTTP	Inbound **Note:** To change the port, refer to the *FreeFlow VI eCompose User Guide.*
443	HTTPS	Inbound **Note:** To change the port, refer to the *FreeFlow VI eCompose User Guide*.
515	LPR	Inbound

User Roles

If Basic Authentication is enabled, the FreeFlow VI eCompose Web Server and the FreeFlow VI eCompose Secure Web Server open to a login screen. For system access, users are required to log in to the system.

Administrator

The administrator has access to the entire system:

- Job Submission/View/Retrieval: Submit Job Dialog, Job Status.
- Change Password
- Administration:
  - User Administration: Add User, Delete User, Add User from Groups, Remove User from Groups: Admin, User, and User Password management.
  - Server Administration
  - Cluster Administration

  Note: Multiple administrators can log in to the FreeFlow VI eCompose Web server at the same time.

User

The user has access to the Job Submission/View/Retrieval where they can view the Submit Job Dialog and Job Status.

> **Note:** Multiple users can log in to the FreeFlow VI eCompose Web Server at the same time.

User Authentication

When the server is configured for HTTPS, the credentials entered into the browser are encrypted as part of HTTPS communication. If the FreeFlow VI eCompose Web Server is not using HTTPS, no credentials are encrypted. The FreeFlow VI eCompose Web Server supports cryptographic protocols TLS v1.2.

User passwords are transformed using the hashing algorithm, PBKDF2 with HMAC-SHA256. Passwords are stored locally on the server. Passwords cannot be derived from the hashed string stored on the server.

Job Submission/View/Retrieval Interface

The Job Submission/View/Retrieval, and Administration User Interface uses the FreeFlow VI eCompose connection for job submission, job view, retrieval, and administration.

For more information, refer to the Xerox VI eCompose Client.

Table 3. Firewall Configuration for Job Submission/View/Retrieval Interface

Port	Protocol or Application	Firewall Connecion Type
80	HTTP	Inbound
443	HTTPS	Inbound

Watched Folders

You can encrypt file shares for a local watched folder and for accessing a watched folder. To encrypt files, use the Windows file system or the Windows user account access control.

Table 4. Firewall Configuration for Watched Folders

Port	Protocol or Application	Firewall Connecion Type
139.145	SMB	Inbound: Shared directories using Windows file sharing. Outbound: Shared directories using Windows file sharing.

Web Job Submission Service (WJSS)

FreeFlow VI eCompose software allows custom job submission clients to submit many VIPP® data files quickly for processing. You can submit jobs to the Web Job Submission Service (WJSS) using IIS or the WJSS Proxy Server provided.

For more information, access the VI eCompose distribution, open the WJSS folder, then refer to the *FreeFlow VI eCompose Web Job Submission Service User Guide*.

> **Note**: The WJSS service is a Microsoft IIS extension. WJSS and the VI eCompose Web Server orthe VI eCompose Secure Web Server cannot run concurrently without configuration.
>
> By default, the software uses port 80 for HTTP, and port 443 for HTTPS. If you run IIS and WJSS concurrently with the VI eCompose Web Server or the VI eCompose Secure Web Server, configure the servers to use alternate ports. For more information, refer to the *FreeFlow VI eCompose User Guide*.

Table 5. Firewall Configuration for the WJSS

Port	Protocol or Application	Firewall Connecion Type
80	HTTP	Inbound

DATA ENCRYPTION

File Processing

FreeFlow VI eCompose and FreeFlow VI Design Express do not fully encrypt files submitted for processing before the files are stored on the file system of the computer.

USER ACCOUNT ACCESS AND JOB RETENTION

The following functionality is enabled through a configuration file. For details, refer to the *FreeFlow VI eCompose User Guide*.

User Account Passwords

When enabled, user account passwords are required to meet the following criteria:

- A password must be at least eight characters in length.
- A password must contain letters and numbers.
- A password must contain lower and uppercase letters.
- A password must contain at least one special character, for example, #, !, $.
- A password must not contain contextual information, such as the user name or website name.

When enabled, a user password cannot be reused.

User Account Lockout

When enabled, if the user fails to log in successfully after a configurable number of attempts, theaccount is locked out for a configurable period of time.

User Account Log Out

When enabled, after 30 minutes of inactivity, logged-in users are logged out automatically. Theduration of the inactivity period is configurable.

User Account Activity

Unsuccessful login attempts are logged in the vtpweb.log file. This file is located in the X:\Program Files(x86)\Xerox\VIPP\xvtp\bin directory, where X is the partition where the VI eCompose software is installed.

Job Retention

After a job completes processing through VI eCompose, it is the responsibility for the submitter todelete the job from the system.

4. Security

At Xerox, security issues are at the forefront of activities. As a leader in the development of digital technology, Xerox has demonstrated a commitment to keeping digital information safe and secure. To limit risk, Xerox identifies potential vulnerabilities and proactively addresses them. Xerox strives to provide the most secure software products possible, based on the information and technologies available, while maintaining product performance, value, functionality, and productivity. The applications of the FreeFlow Variable Information Suite are assessed for security compliance, using commercially available vulnerability and penetration scanning tools. Application vulnerabilities are addressed based on the results of our internal scans.

Xerox maintains the website http://www.xerox.com/security/ with up-to-date security vulnerability 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 software is shipped free from computer virus contamination. Xerox recommends that Anti-Virus Detection and EndPoint Intrusion Detection and Prevention are installed on the host system. This software and the operating system are kept up-to-date with the latest security patches as advised by the respective vendors.

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

You can exclude the following FreeFlow VI eCompose directories from antivirus scanning:

X:\Program Files(x86)\Xerox\VIPP\xvtp\bin: This directory and its subdirectories, where X is the drive where the software is installed.

You can exclude the following FreeFlow VI Design Express directories from antivirus scanning:

X:\Program Files(x86)\Xerox\VIPP\VDE\bin: This directory and its subdirectories, where X is the drive where the software is installed.

5. Software Update

It is recommended that customers keep up to date all software products installed on the FreeFlow VI eCompose server and FreeFlow VI Design Express. At least once a month, perform a Microsoft Windows update.

For FreeFlow VI eCompose and FreeFlow VI Design Express software updates, click the link: http://www.support.xerox.com.

6. Additional Information & Resources

Security @ Xerox

Xerox maintains an up-to-date public webpage that contains the latest security information thatpertains to its products. Refer to http://www.xerox.com/security.

Responses to Known Vulnerabilities

Xerox has created a document which details the Xerox Vulnerability Management and Disclosure Policy used in discovery and remediation of vulnerabilities in Xerox software and hardware. It can be downloaded from this page: http://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html.

Additional Resources

Table 4. Below are additional resources.

Security Resource	URL
Frequently Asked Security Questions	https://www.xerox.com/en-us/information-security/frequently-asked-questions
Bulletins, Advisories, and Security Updates	http://www.xerox.com/security
Security News Archive	https://security.business.xerox.com/en-us/news/