Version 15.0.3.0
April 2018
702P06521

Xerox® FreeFlow® VI Suite

Information Assurance Disclosure 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.

Document Version: 2.0 (April 2018).

Table of Contents

1

Preface

General Purpose

The purpose of this document is to disclose information related to Xerox® FreeFlow® VI eCompose 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 for customers who require more security-related information relative to FreeFlow VI eCompose.

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 include direct, indirect, incidental, consequential, loss of business profits, or special damage, even if Xerox Corporation has been advised of the possibility of such damages.

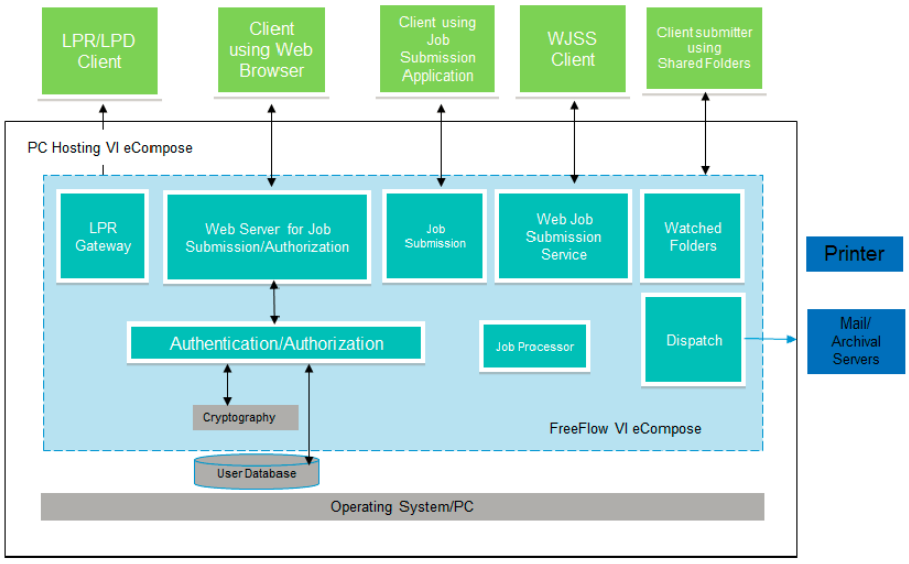
2

Product Description

VI eCompose is a client/server application that allows you to generate Adobe PDF documents from VIPP-based variable data applications and forward them 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. The PDF files, along with information from the data record that produced them, can then 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.

System Software Structure

The system software structure for the product is depicted below.



3

System Access

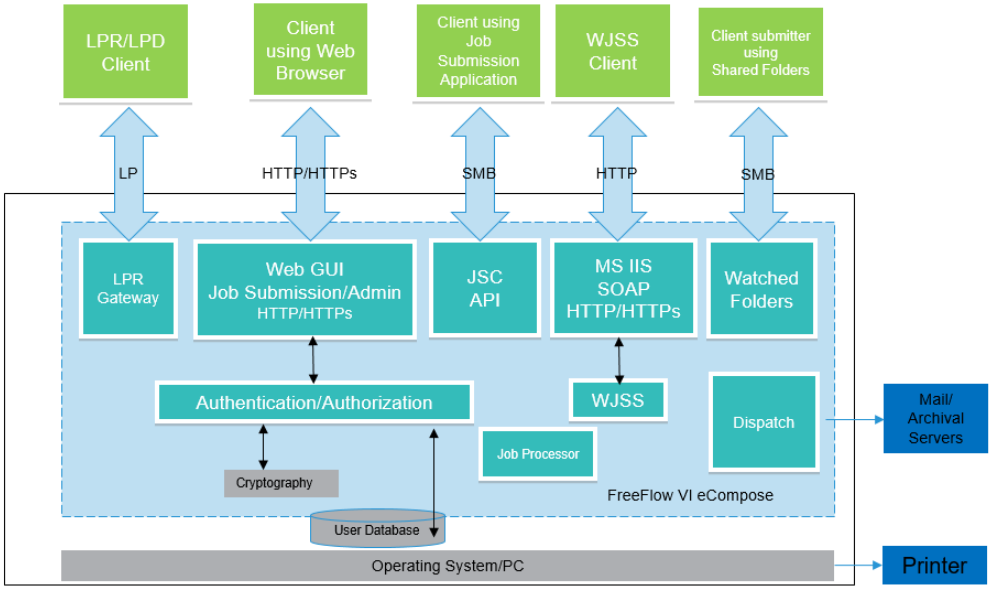
Network Connections

FreeFlow VI eCompose requires network connectivity for job submission from clients, job processing and administration using a browser. Security considerations for each network connection are documented below.

Note

To provide better security protection against vulnerability attacks, Windows Firewall is required to be enabled on the server where VI eCompose is installed unless your site has its own firewall requirements.

This diagram shows newtork protocol connections used by FreeFlow VI eCompose.



FreeFlow VI eCompose

The FreeFlow VI eCompose server allows clients using a browser to submit VIPP jobs, perform administration functions of the server. To enable a browser to access VI eCompose server, start VI eCompose Web Server or VI eCompose Secure Web Server on the server.

The VI eCompose Secure Web Server allows communication using HTTPS. Both the eCompose Web Server and Secure Web Server can be configured to use HTTP Basic Authentication. Enabling HTTPS connectivity requires a valid CA certificate installed on the system. Refer to the VI eCompose User's Guide for information on configuring the system for HTTPS via SSL with HTTP Basic Authentication

Submission of VIPP jobs can be done using LPR, watched folders, and WJSS. For allowing job submissions from LPR clients, FreeFlow VI eCompose relies on Windows TCP/IP Print Server and Print Spooler services to be enabled.

Note

The client can retrieve a VIPP job converted to PDF, which may contain customer data.

Port	Protocol or Application	Firewa ll Connection Type
80	HTTP	Inbound **Note** Port can be changed through a configuration file.
443	HTTPS	Inbound **Note** Port can be changed through a configuration file.
515	LPR	Inbound

Table 1: Firewall Configuration

User Roles

FreeFlow VI eCompose Web Server and FreeFlow VI eCompose Secure Web Server opens to a login screen if BasicAuthentication is enabled. The user must log in for access 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/Delete User, Add/Remove User from Groups (Admin, User), User Password management
  - Server Administration
  - Cluster Administration

Multiple Administrators may be logged in to FreeFlow VI eCompose Web Server at any given time.

User

The Operator has access to the following:

- Job Submission/View/Retrieval: Submit Job Dialog, Job Status.

Multiple Users may be concurrently logged in to FreeFlow Vie Compose Web Server.

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.

User passwords are transformed using a hashing algorithm (SHA-2) and stored locally on the server. The password 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 (UI) uses the FreeFlow VI eCompose connection for job submission, job view, retrieval and administration (refer to Xerox VI eCompose Client).

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

Table 2: Firewall Configuration

Watched Folders

File shares used for sharing a local watched folder and for accessing a Watched Folder in shared Windows folders may be encrypted using the Windows file system or protected using Windows user account access control.

Port	Protocol or Application	Firewall Connection Type
139, 145	SMB	Inbound - Sharing Hot Folders via Windows File Sharing Outbound - Using Hot Folders on Shared Directories

Table 3: Firewall Configuration

Web Job Submission Service (WJSS)

FreeFlow VI eCompose allows custom job submission clients to submit many VIPP data files quickly for processing. Communication to WJSS is via IIS or a Windows Service.

Note

The WJSS and VIeCompose Local Server (which includes VI eCompose Web Server and VI eCompose Secure Web Server) cannot run concurrently as they both share port 80.

Port	Protocol or Application	Firewall Connection Type
80	HTTP	Inbound

Table 4: Firewall 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 VI eCompose 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 maintains a 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 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 VI eCompose folders may be excluded from anti-virus scanning:

- X:\xvtp\bin (and subdirectories), where X is the drive where the software was installed

5

Software Update

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

Software updates for FreeFlow VI eCompose can be found at

http://www.support.xerox.com/support/variable-information-suite/software/enus.html