FreeFlow Core, Version 4.0
August 2014
702P02837

Xerox® FreeFlow® Core
Security Guide

Document version 1.0, August 2014

BR10173

Table of Contents

Table of Contents

1

Xerox® FreeFlow Application Suite Security

Overview

This document contains security-related information for FreeFlow Core.

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 FreeFlow are assessed for security compliance using commercially available vulnerability and penetration scanning tools. Application vulnerabilities are addressed based on results of our internal scans.

Firewall Enablement and Configuration

It is recommended that a firewall be abled on the FreeFlow Core server. Ports should be blocked unless required to perform a specific function as detailed below:

Port	Protocol or Application	Enabled FreeFlow Core Function
80	HTTP	Inbound – Launch the FreeFlow Core UI Outbound – Retrieving files listed in Manifest or in Component presets
161,162	SNMP	Outbound – Identifying DFE type during printer setup
631	IPP	Outbound – Submitting jobs to DFEs

Port	Protocol or Application	Enabled FreeFlow Core Function
25, 2525, 465, 475, 587	SMTP	Outbound – Sending email notifications Note: Required port number depends on SMTP server configuration
TCP, UDP: 7751	JMF	Inbound – Receiving JMF/JDF Requests
varies	JMF	Outbound – Returning JMF status signals. JMF client specifies Port number.
139, 445	SMB	Inbound – Sharing Hot Folders via Windows File Sharing Outbound – Using Hot Folders on Shared Directories Outbound – Retrieving files listed in Manifest from Shared Directories Outbound – Retrieving files listed in Components from Shared Directories Outbound – Saving to Shared Directories
20,21	FTP	Inbound – Sharing Hot Folders via FTP Outbound – Retrieving files listed in Manifests or in Component presets
443	HTTPS	Inbound – Sharing files for remote FreeFlow Core system Outbound – Retrieving files from remote FreeFlow Core system

Windows Firewall Rules

1. Go to **Control Panel > System and Security > Windows Firewal > Advanced Settings**.
2. For each required rule, select **Inbound Rules** or **Outbound Rules**:
   a) Under Actions, click **New Rule**. The New Inbound Rule Wizard displays.
   b) Click **Port** for the Rule Type. Click **Next**.
   c) Click **TCP** or **UDP** per the able above. Enter a value in Specific local ports per the table above. Click **Next**.
   d) Click **Allow the Connection.** Click **Next**.
   e) Select all boxes. Click **Next**.

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 MS 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>\Platform\Spool
- <FreeFlow Core Installation directory>\Logs
- <FreeFlow Core Installation directory>\Platform\Logs
- <FreeFlow Core Installation directory>\Web\Logs
- <FreeFlow Core Installation directory>\Config
- <FreeFlow Core Installation directory>\Presets

Software Update

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

Operating system Service Packs are not to be installed through Microsoft Update until formal communication of support.

Xerox distributes monthly bulletins, when required, listing updates that should be "excluded" on the FreeFlow system. This information is also communicated on the www.xerox.com/security web site under "Product Security Guidance". High priority and security-related updates are critical and should always be installed unless they are specifically excluded.