May 16, 2019

Xerox® FreeFlow® Print Server v2

Information Assurance Disclosure

Version: 1.0

Xerox® Baltoro™ HF Production Inkjet Press

Table of Contents

Revision Log

Version	Date	Description or Purpose of Changes	Author
1.0	05/16/2019	Created the initial Version 1.0 of this FreeFlow® Print Server v2 / Windows® Security Information Assurance Disclosure (IAD) document for the Baltoro™ HF Production Inkjet Press.	D. Roome

Document Glossary

ACS	Affiliated Computer Services
AES	Advanced Encryption Standard
AMR	Automatic Meter Read
API	Application Programming Interface
CA	Certificate Authority
CAC	Common Access Card
CCTL	Common Criteria Testing Laboratory
CISSP	Certified Information Systems Security Professional
CBC	Cipher Block Chaining
CCC	Common Criteria Certification
CFA	Call for Assistance
CK	Crypto Key
CSE	Customer Service Engineer
DARPA	Defense Advanced Research Projects Agency
DEP	Data Execution Prevention
DES	Data Encryption Standard
DFE	Digital Front End
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DNS	Domain Naming Service
DNSSEC	DNS Security
DoD	Department of Defense
DPWS	Devices Profile for Web Services
DTLS	Datagram Transport Layer Security
DVD	Digital Versatile Disc
EAL	Evaluation Assurance Level
EDE	Encrypt-Decrypt-Encrypt
EFS	Encrypting File System
FFRPS	FreeFlow® Remote Print Service
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FSO	Field Security Operations
FTP	File Transfer Protocol

HIPPA	Health Insurance Portability and Accountability Act,
HTTP	Hyper Transfer Protocol
HTTPS	Hyper Transfer Protocol Secure
IAD	Information Assurance Document
ICMP	Internet Control Message Protocol
IIS	Internet Information Services
IOT	Image Output Terminal
IP	Internet Protocol
IPDS	Intelligent Printer Data Stream
IPP	Internet Printing Protocol
IPSec	Internet Protocol Security
IT	Information Technology
JMF	Java Media Framework
LCDS	Line Conditioned Data Stream
LPR	Line Printer
MAC	Macintosh
MAC	Message Authentication Code
MD	Message Digest
MMC	Microsoft® Management Control
MIT	Massachusetts Institute of Technology
NetBIOS	Network Basic Input/Output System
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NTP	Network Time Protocol
OS	Operating System
OSI	Open Systems Interconnection
PCI DSS	Payment Card Industry Data Security Standard
PDL	Page Description Language
PHI	Personal Health Information
PPML	Personalized Print Mark-up Language
PII	Personally Identifiable Information
PSIP	Print Station Interface Platform
RBAC	Role-Based Access Control
RC	Rivest Cipher
RDP	Remote Desktop Protocol

RFC	Request for Comment
RSA	Rivest-Shamir-Adelman
RIP	Raster Image Processing
SA	System Administrator
SAIC	Science Applications International Corporation
SCP	Secure Copy
SDLC	Secure Software Development Lifecycle
SEHOP	Structured Exception Handler Overshoot Protection
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SoV	Statement of Volatility
CMVP	Cryptographic Module Validation Program
SSH	Secure Shell
SSL	Secure Socket Layer
STIG	Security Technical Implementation Guide
TCP	Transport Control Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
TRC	Ton Reproduction Curve
TDES	Triple Data Encryption Standard
TSM	Transport Security Model
UAC	User Account Control
UDP	User Datagram Protocol
UI	User Interface
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
VIPP	Variable Data Intelligent PostScript
VPN	Virtual Private Network
Web-UI	Web User Interface
WINS	Windows® Internet Naming Service
WSD	Web Services on Devices
XEAR	Xerox Enterprise Accounting Reporter

1.0 Security Process Introduction

This document reveals Information Assurance Disclosure (IAD) for the FreeFlow® Print Server platform to provide customers with transparency to meet their Security requirements and compliances for the FreeFlow® Print Server X86 DFE platform that support the Xerox® Baltoro™ HF Production Inkjet Press. It does not provide IAD for the Baltoro™ HF printer engine. Refer to the IAD document for the Xerox® Baltoro™ HF Production Inkjet Press for the same information that pertains to the print engine. This document also identifies references to the Statement of Volatility (SoV), which describes the location, capacities and content of volatile and non-volatile memory component within the FreeFlow® Print Server X86 DFE platform that support the Xerox® Baltoro™ HF Production Inkjet Press

1.1 Purpose

The purpose of this document is to provide a high-level view of the Xerox processes that ensure the Xerox® FreeFlow® Print Server platform can satisfy customer security requirements and describe how software security is evaluated and maintained. This document also identifies security features that aid a Security Information Technology administrator to manage Security and the assurance of security of the FreeFlow® Print Server platform and Baltoro™ HF Press. It supports Windows® 10 configuration of the FreeFlow® Print Server product for the Xerox® Baltoro™ HF Production Inkjet Press.

1.2 Overview

Xerox actively delivers security features and supports the achievement of customer security requirements. Xerox allocates dedicated development and engineering team resources to support FreeFlow® Print Server security. Xerox delvers a FreeFlow® Print Server Security White Paper and Configuration Guide to assist with an understanding of the robust security features built into the FreeFlow® Print Server product, and to describe security procedures. This document is a good reference to assist the Xerox Customer Service Engineer, Analyst and/or Customer to address all security requirements.

The Windows® Operating System (OS) provides the critical security features and capabilities that enables protection of the FreeFlow® Print Server from unauthorized access and protection of sensitive data. There is empirical data shows that the Windows® OS has many fewer Security vulnerabilities compared to competitive vendors such as Apple® Macintosh® OS and Linux®. This data shows that these vendor OS products report 3 to 5 more times the Security vulnerabilities than are reported on the Microsoft® Windows® OS.

Microsoft® has built-in features and capabilities using the latest Security technologies, and this ensures the FreeFlow® Print Server product satisfies compliant requirements dictated by a customer business environment and policies to protect PII/PHI information. Windows® OS complies with Payment Card Industry data security mandates for encryption of data at rest, data in transient, and immediately responds with patches to address Security vulnerabilities notified by the US Government. Microsoft® made security enhancements in the Windows® 10 OS relative to the predecessor Windows® 7 OS.

Security processes and capabilities, which exceed the scope of the FreeFlow® Print Server software, are the responsibility of the customer. Xerox is responsible for integrating Security patches for the Windows® OS, and for supporting customer Security requirements. A customer can take responsibility to manage Security patches on the FreeFlow® Print server platform at their own risk. If a customer has contracted with Xerox Services to manage the security of FreeFlow® Print Server products, we evaluate the customer Production print workflow and identify a strategy to implement and manage compliance with the customer's security requirements.

It is the responsibility of the customer to use the information contained herein this document, and from Microsoft® knowledge databases to security tighten the FreeFlow® Print Server / Windows® platform per their requirements and policies. Some important security measures are, install of security patch updates, defining FreeFlow® Print Server users with well-defined roles, implementing password security policies, install/setup of SSL certificate, defining IP/Port filters, capturing/reviewing audit logs, etc.

Xerox can provide security tightening recommendations and solutions but is not responsible for auditing Xerox® printer devices connected to a customer network. We recommend that the customer hire a Certified Information Systems Security Professional (CISSP) specialist to ensure and certify that the Xerox® printer(s) comply with the security standards per the customer policy.

1.3 Target Audience

The target audience for this document is Xerox field personnel, FreeFlow® Print Server 3rd-party developers and customers concerned with IT security.

1.4 Disclaimer

The information in this document is accurate to the best knowledge of the authors and provided without warranty of any kind. In no event shall Xerox Corporation, or Electronics For Imaging, Inc. 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 the Xerox Corporation, or Electronics For Imaging, Inc. has been advised of the possibility of such damages.

2.0 Security Assurance and Assessment Process

The Xerox® FreeFlow® Print Server Development processes to assure security of the FreeFlow® Print Server platform is:

1. Xerox® monitors weekly-issued US-CERT (United States Computer Emergency Readiness Team) alerts at http://www.us-cert.gov, and Microsoft® Alerts that announce new security vulnerabilities and patches to remediate them.

2. Xerox® evaluates US-CERT alerts for impacts to the Windows® OS and FreeFlow® Print Server product. The development team prioritizes patches applicable to current FreeFlow® Print Server products based on severity, executes system testing, and delivers security patches for all FreeFlow® Print Server supported Xerox® printer products as a post-install package. Xerox® delivers the Microsoft® Windows® Security Patch Updates on a quarterly sequence at test and acceptance completion. The quarterly Security patch deliverable is made available to Xerox Service for electronic delivery over the internet (with Update Manager), or on DVD/USB media.

3. Xerox® delivers a FreeFlow® Print Server v2 Security White Paper and User Guide, and Security bulletins that describe a customer's options to install Microsoft® Windows® Security Patch Updates. The Security White Paper includes a strategy to manually or automatically schedule download/install of the Security Patches using the Windows® Update service, and procedures to reduce the risk of rendering the printer inoperable when installing patches not tested by Xerox®.

4. Xerox® is constantly improving existing security features and developing new features to address customer requirements. Xerox® prioritizes new value-added security features requests and make plans to deliver the feature when there is a business case for our customers. The FreeFlow® Print Server development team actively maintains Open-source software updates on the FreeFlow® Print Server / Windows® platform to keep up with Security technology.

5. Xerox® performs Security penetration-tests using Nessus (Industry-Standard Security evaluation software) against each FreeFlow® Print Server major software release and patch software releases and remediates all security findings listed in the Nessus audit reports by installing patches delivered by Microsoft®.

6. Xerox® tests each FreeFlow® Print Server software release with STIG hardening before making it available to customers that require enhanced security required by Defense Information Systems Agency (DISA). The FreeFlow® Print Server product bundles a Windows® STIG package used by the Department of Defense (DoD) and other U.S. Federal and State Government agencies/departments to satisfy DISA security requirements. This security software package contains numerous scripts that tighten the FreeFlow® Print Server platform security to meet the DISA standards.

7. Xerox® performs authentication and authorization testing on each FreeFlow® Print Server major and patch software release delivered to the field.

8. Xerox® performs testing of the Web User Interface (Web-UI) Application security controls and configuration settings on each FreeFlow® Print Server major software release delivered to the field.

9. Xerox maintains a website, https://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.

3.0 Windows® 10 Security Enhancements

Windows® 10 includes many enhanced security features that can be configured and built in security features to protect the FreeFlow® Print Server platform and Xerox® Baltoro™ HF Production Inkjet Press.

3.1 Configurable Security Enhancements

Windows® 10 offers a wide array of configurable protections for devices and users across a network enterprise (such as Windows® Defender SmartScreen, Credential Guard, Device Guard, Windows® Defender Antivirus, etc.), and memory protection options such as Data Execution Prevention, Structured Exception Handling Overwrite Protection (SEHOP), and Address Space Layout Randomization (ASLR), etc. The memory protection options mitigate against malware that attempts to manipulate memory and gain control of the FreeFlow® Print Server platform.

This section identifies some of the Windows 10 configurable enhanced security features and provides an overview of these features.

Some of the configurable enhanced security features for Windows® 10 are illustrated below:

Configurable Security Feature	Security Threat Mitigation	Description
Windows Defender SmartScreen	Phishing, Malware Websites, and unsafe downloads	Microsoft® improved SmartScreen, now called Windows® Defender SmartScreen, by integrating application reputation into the Windows® OS. This allows SmartScreen to warn a user that is about to download a high-risk file. SmartScreen will also block execution of applications known to be malicious.
Windows Defender Antivirus	Malware Attack	Capabilities of Windows Defender Antivirus are as follows: • Cloud delivered protection detect and block new malware. • Rich local context improves how to identify malware, where the malware comes from, where malware has been stored, etc. • Extensive global sensors assist with keeping Windows® Defender Antivirus updated to know about most recent malware. • Tamper proofing guards Windows® Defender Antivirus against malware attacks on itself. • Enterprise-level features offer IT professionals the tools and configuration options to make Windows® Defender Antivirus an enterprise-class antimalware solution.
Data Execution Prevention (DEP)	Malicious code in memory, Denial of Service	DEP protects memory that is otherwise prone to malicious code attacks. It marks blocks of memory as read-only, so they are not exploitable for use to execute malicious code.
Structured Exception Handling Protection (SEHOPO)	Malicious code Exception Handler exploit, Denial of Service	The Windows® OS must support appropriate exceptions for trusted applications. SEHOPO helps to prevent attackers from using malicious code to exploit the Structured Exception Handler.
Address Space Layout Randomization (ASLR)	Denial of Service	An attacker can find a vulnerability in a privileged process currently running, guess memory location of system code and data, and overwrite it. ASLR makes such an attack more difficult by making how and where data is stored in memory random. This makes it more difficult for malware to find a specific location to attack.

3.2 Built-In Security Enhancements

Microsoft® has improved Windows 10 by building in security option into the Operating System, which enable by default. You can find information pertaining to the built-in security features configured by default for Windows® 10 below:

Security Mitigation	Security Threat	Description
SYSVOL and NETLOGON SMB share hardening	man-in-the-middle attacks	Client connections to the Active Directory Domain Services default SYSVOL and NETLOGON shares on domain controllers now require SMB signing and mutual authentication (such as Kerberos).
Protected Processes	Process to process tempering	With the Protected Processes feature, Windows® 10 prevents untrusted processes from interacting or tampering with specially signed processes.
Universal Windows® apps protections	Running screen downloadable apps in an AppContainer sandbox	The OS carefully screens Universal Windows® apps before making them available, and they run in an AppContainer sandbox with limited privileges and capabilities.
Heap protections	Heap Exploitation	Windows® 10 includes protections for the heap, such as the use of internal data structures, which help protect against corruption of memory used by the heap.
Kernel pool protections	Kernel pool memory exploitation	Windows® 10 includes protections for the pool of memory used by the kernel. For example, safe unlinking protects against pool overruns. An attacker can use pool overruns combined with unlinking operations to create an attack.
Control Flow Guard	flow between code locations in memory exploits	Control Flow Guard (CFG) is a software compiled built-in mitigation and automatically enabled, so requires no configuration within the operating system. Microsoft® builds CFG into Microsoft® Edge, IE11, and other areas in Windows® 10. C or C++, or applications compiled using Visual Studio 2015 can build CFG into applications. For such an application, CFG can detect an attacker's attempt to change the intended flow of code. If this occurs, CFG terminates the application. You can request software vendors to deliver Windows® applications compiled with CFG enabled.
Microsoft® Edge Built-In Protection	Multiple browser threats	Windows® 10 includes an entirely new browser, Microsoft® Edge, designed with multiple security improvements.

4.0 FreeFlow® Print Server Device Description

The FreeFlow® Print Server product is a Digital Front End (DFE) application that supports Xerox high-volume and higher end mid-volume Xerox® printer products.

The FreeFlow® Print Server is a specialized software application that runs on the Windows® platform, which takes advantage of the robust built-in security capabilities matured over the years to prevent a breach of Personally Identifiable Information (PII)/Personal Health Information (PHI) information that can be contained in print jobs.

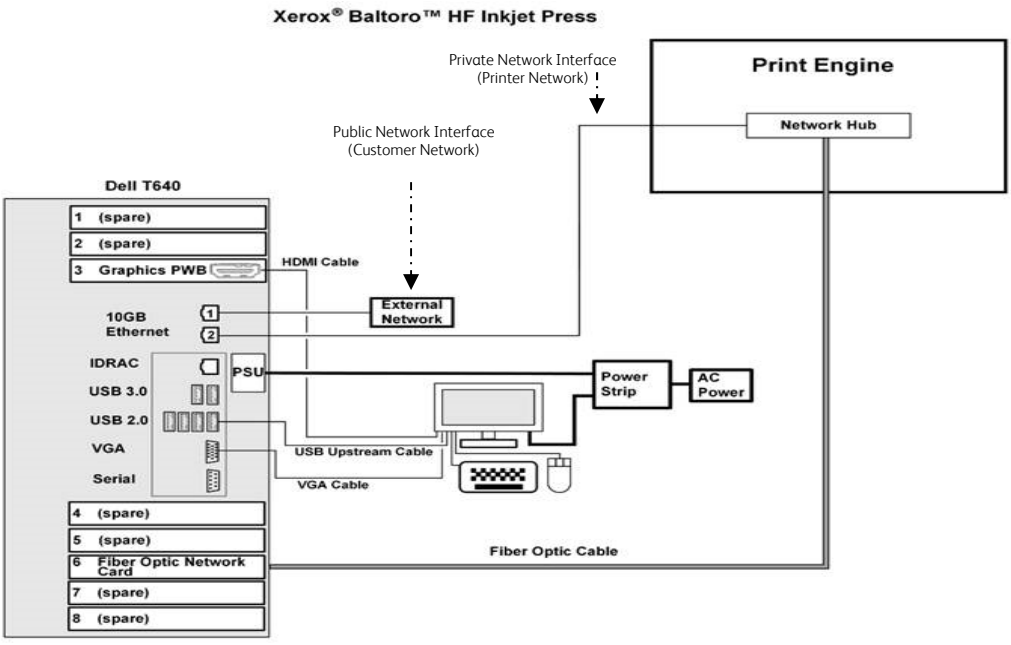
Unlike the purpose of a File Server that supports the permanent storage of data potentially containing PII/PHI, a Print Server such as the FreeFlow® Print Server holds short lived PII/PHI information with the main purpose of processing/rendering, printing, and deleting customer jobs. The FreeFlow® Print Server software deletes print jobs from the hard disk once printing completes. It is important to know the software does not delete print jobs after printing if the Retain PDL option is configured. See Section 4.2.1.5 "*Retain PDL Setting*" for more information on the Retain PDL feature.

4.1 Security-relevant Subsystems

This section identifies the location, capacities and content of volatile and non-volatile memory components within the FreeFlow® Print Server X86 DFE platform that support the Xerox® Baltoro™ HF Production Inkjet Press.

4.1.1 Physical Partitioning

See the security-relevant subsystems for the FreeFlow® Print Server Dell T640 platform below:



Customer jobs arrive over the "customer" (a.k.a., public) network interface via a print protocol service (LPR, IPP, Hot Folder, etc.). The job data stream is spooled to the hard disk,

scheduled for printing, decomposed/rendered to raster images, and delivered to the printer by the marker interface (See **Section 4.3** "*Marking <-> IOT Interface*").

4.1.2 FreeFlow® Print Server Purpose

The FreeFlow® Print Server is a specialized Digital Front End (DFE) representing a multiple Queue Spooler model printer architecture that provides printing services such as job processing, job management and printer management/configuration services. It incorporates a High-Speed RIP engine and Marking process (See **Section 4.3** "*Marking <-> IOT Interface*") to support performance requirements of high-speed color Xerox printers such as the Baltoro™ HF Press. It includes capabilities to manage printing resources (E.g., Fonts, Background Forms, VIPP Projects, Imposition Templates, etc.).

The FreeFlow® Print Server software application is tightly coupled with the Windows® OS software. There is a "private" network interface connection between the backend of the FreeFlow® Print Server platform to the Xerox Baltoro™ HF via a Xerox Print Station Interface Platform (PSIP). The FreeFlow® Print Server delivers job pages decomposed and rendered as Xerox proprietary raster images to the Baltoro™ HF Press over this interface. This back-end network connectivity is isolated from the front-end network interface, which is connected to the customer "public" network unless configured to route network information between these networks by defining a proxy configuration for the Baltoro™ HF Press to communicate on the customer "public" network.

There are many robust Security capabilities built-into Windows® and customized by the FreeFlow® Print Server® application. The FreeFlow® Print Server offers an on-demand Data Overwrite feature to sanitize the areas of the hard disk that hold customer data and print jobs. In addition, the software also incorporates an open-source Apache web server that exports a Web-UI User Interface for users to submit jobs and check job and machine status from remote Web clients, and to allow system administrators to remotely administer the print jobs.

Other important Security capabilities (E.g., Security Profile, STIG Package, Console Audit Logging, Password Security, etc.) are included with the FreeFlow® Print Server software, which are described herein this document. Assigning the Security profile to 'High' disables insecure network services and closes UDP/TCP ports not required for job submission workflow. See **Section 4.5.5** "*UDP/TCP Ports*", **Section 6.1** "*Security Profile*" and **Section 6.1.3** "*Security Profile UDP/TCP Port Settings*" for more information. A customer has the option to install and setup an SSL/TLS certificate on the FFPS platform to ensure secure job submission workflows, and remote Web-UI access. Optionally you can disable Web-UI access in favor of local Web-UI access to the FreeFlow® Print Server services.

Customers submit documents to the FreeFlow® Print Server over a "public" network interface, which transfer to an input spool directory on the hard disk, and schedule for processing/printing. Unlike a File Server that persistently stores user files, the life of a print job ends once the last page is printed. The FreeFlow® Print Server application deletes the customer document once a job completes printing, and proceeding jobs write over the disk sectors that held print data from deleted document files. It is important to know the software does not delete print jobs after printing if the configuration enables the Retain PDL option. See **Section 4.2.1.5** "*Retain PDL Setting*" for more information on the Retain PDL feature. The input spool directory is included as a location to sanitize this hard disk area when running the Data Overwrite application included with the FreeFlow® Print Server platform.

4.1.3 Memory Components

Refer to the official SoV document titled "*Xerox® FreeFlow® Print Server; Statement of Volatility; Supports: Baltoro™ HF Inkjet Press; Version 1.0*" dated April 2019 for external connections information. See **Section 6.11** "*Statement of Volatility (SoV)*" for information about this document.

4.1.4 External Connections

Refer to the official SoV document titled "*Xerox® FreeFlow® Print Server; Statement of Volatility; Supports: Baltoro™ HF Inkjet Press; Version 1.0*" dated April 2019 for external connections information. See **Section 6.11** "*Statement of Volatility (SoV)*" for information about this document.

4.1.5 Peripheral Devices (DVD Drive and USB Ports)

Refer to the official SoV document titled "*Xerox® FreeFlow® Print Server; Statement of Volatility; Supports: Baltoro™ HF Inkjet Press; Version 1.0*" dated April 2019 for r external connections information. See **Section 6.11** "*Statement of Volatility (SoV)*" for information about this document.

4.2 Web Graphical User Interface

This section describes the capabilities of the FreeFlow® Print Server Web-UI interface presented to the Administrator or Operator to facilitate printing-related tasks for the Baltoro™ HF Press. This section does not describe the Window Desktop or the applications available from this Windows® Desktop. The Windows® Desktop interface included a vast number of robust time-tested Security features and options widely documented and described on the Internet using a search engine.

The FreeFlow® Print Server Web-UI is a java application that runs in various Web Browsers (such as IE, Firefox, Chrome, etc.), and is accessible locally at the printer, and remotely by a Windows® or MAC® client. The main purpose of the Web-UI is to manage print jobs that are associated with a Queue (a.k.a., Virtual Printer) and listed in a Web UI Job Manager view according to the status state of the job (E.g., active, held, paused and completed). There is a very large number of options available and applicable to jobs in the held or paused state. Jobs that arrive in the Web-UI Job Manager are associated with printing requirements that you can change using the job properties option.

4.2.1 Web User UI Feature Security Considerations

There are features in the FreeFlow® Print Server Web-UI that have security implications that are worthy of understanding and consideration. This sub-section provides a customer with information to make Web-UI choices for security considerations.

4.2.1.1 Saved Jobs

The FreeFlow® Print Server application supports the decomposition and rendering of print jobs to an output file written to hard disk in a well-known location in a Xerox proprietary raster image format. The Web-UI Job Manager provides an option on a queue to write these saved jobs, and the ability to manage them. Once jobs are stored in the saved job repository for reprint (using the Print From File UI) they are available until removed by the System Administrator or Operator role. See **Section 4.2.1.3** "*Print From File*" for information about the Print From File UI submission tool.

There are security conscious customers that will not allow saved jobs as a site security policy. The Web-UI provides an option for the System Administrator to restrict this feature from the Operator role. The Saved Job directory is included as a location to sanitize this hard disk area when running the Data Overwrite application included with the FreeFlow® Print Server platform.

4.2.1.2 Background Form Manager

The FreeFlow® Print Server application supports the decomposition and rendering of print jobs that represent static text, graphics and/or images on the pages of a print job and stores them for reuse by jobs in a well-known location in a Xerox proprietary raster image format. The Web-UI provides the mechanism with the option enable writing of Background Form jobs, and the ability to manage them. A System Administrator or Operator role can submit jobs using this feature.

There are security conscious customers that will not allow Background Form jobs as a site policy. The Web-UI provides an option for the System Administrator to restrict this feature from the Operator role. The Background Form directory is included as a location to sanitize this hard disk area when running the Data Overwrite application included with the FreeFlow® Print Server platform.

4.2.1.3 Print From File

The FreeFlow® Print Server application supports a local Web-UI job submission mechanism named 'Print From File' used to select a print file from the local disk or remote storage location, define printing requirement, and submit for job scheduling/printing. A FreeFlow® Print Server System Administrator or Operator role can submit jobs using this feature if they have access to the file from the local disk or remotely connected location.

There are Security conscious customers that will not allow job submission of print jobs selected from the Web- 'Print From File' application as a site policy. The Web-UI provides an option for the System Administrator to restrict this feature from the Operator role.

4.2.1.4 Job Forwarding

The FreeFlow® Print Server application supports a Web-UI job submission mechanism referred to as a Job Forwarding application used to submit jobs from one FreeFlow® Print Server platform and Baltoro™ HF Press to another like-printer. A customer uses this feature when the Baltoro™ HF Press is inoperable because of a hardware/software issue or the printer is in maintenance mode. A customer also uses the Job Forwarding UI application to achieve load balancing when the existing printer queued with many print jobs. This job submission UI application requires ICMP (echo) and lpr (port 515) access to the receiving printer. A FreeFlow® Print Server System Administrator or Operator role can forward print jobs to a Baltoro™ HF Press that has fewer print jobs queued or is idle.

There are Security conscious customers that will not allow job submission of print jobs selected from the Web- Job Forwarding UI as a site policy. The Web-UI provides an option for the System Administrator to restrict this feature from the Operator role.

4.2.1.5 Retain PDL Setting

The Web UI includes a system setting to enable the retention of jobs after printing comes to an end state or completes printing. This is an enable/disable option in the Web UI named Retain PDL. Once print jobs enter a final status state (E.g., Successfully Completed, Aborted, etc.), the FreeFlow® Print Server removes them from the hard disk when Retain PDL is disabled. The Web UI Job Manager maintains a record of the job with job programing attributes in the "Completed Jobs" listing.

When the Retain PDL option is enabled, the FreeFlow® Print Server maintains the print job PDL (E.g., PDF, PostScript, etc.) on the hard disk to future reprinting. The FreeFlow® Print Server does not maintain jobs that process in Streaming mode with the configuration Retain PDL option enabled. Only the Spooling print data transport mode supports the Retain PDL feature. The stored PDF job files are maintained on the hard disk until a defined disk space capacity threshold is reached (E.g., 50% of the disk space) or a defined set number of hours or days.

It is a security risk to keep job data stored on the FreeFlow® Print Server platform for reprint purposes. The print data is available or persistent for some timeframe giving more opportunity to experience a breach. In addition, the Web UI operator role has the option to print a job more than once. For example, if a customer check is printed successfully, the operator could print that check additional times if Retain PDL is enabled.

There are Security conscious customers that will not allow the retention of print jobs as a site policy. The Web-UI provides an option for the System Administrator to restrict this feature from the Operator role.

4.2.1.6 Job Spooling/Streaming Option

The FreeFlow® Print Server offers options for transporting job print data from the network to the printer. The options are either Spooling or Streaming mode and defined at the queue level. By default, the transport mode is Spooling at queue creation time from the Web-UI Queue Manager. In this mode, the print job is spooled from the network to an input directory on the hard disk, scheduled for processing, and printed. Job scheduling does not begin until after a job is completely spooled to the input directory on the hard disk.

You can update the transport mode defined on a queue to Streaming. The Streaming transport mode was incorporated to handle transactional data streams such as IPDS and LCDS. In this mode, the print job is also spooled from the network to an input directory on the hard disk, scheduled for processing and printed. Streaming is different from Spooling mode in that the FreeFlow® Print Server schedules jobs for processing/printing immediately as the print data is still arriving over the network. This enables large print jobs that take a long network transfer time to begin processing and printing immediately, and not wait until the large job is completely spooled in the input directory on the hard disk.

4.2.1.7 Color Management

A FreeFlow® Print Server Web-UI authorizes the System Administrator role to calibrate and profile to color match the monitor and Baltoro™ HF Press. This will provide a controlled conversion of color representations of a monitor, scanned images, photographs. etc., to an equivalent representation of the Baltoro™ HF Press that is inside of the supported color gamut of the printer. The resultant ICC profile created during the calibration process describes the color space and gamut of the printer. The Operator role is restricted access to this capability unless the System Administrator grants them access.

4.2.1.8 Resource Management

The FreeFlow® Print Server Web-UI authorizes the System Administrator role to manage printer resources for things such as Fonts, Stocks, Spot Color Definitions, Color Profiles, User TRC's, Imposition Templates, VIPP, LCDS, etc. The Operator role is restricted access to this capability unless the System Administrator grants them access.

4.2.1.9 Job Accounting

The FreeFlow® Print Server application offers Job Accounting records to provide job accounting information (E.g., stocks used, # of each stock used, RIP/Print date/time, Job Costing information, printing attributes applied, Etc.) for completed jobs. The Web-UI provides options to manage (E.g., view, define format, print, delete) accounting records. The Operator role is restricted access to this capability unless the System Administrator grants them access.

4.2.1.10 System-Level Preferences and Options

The FreeFlow® Print Server application presents many system-level options in the Web-UI to define and customize the configuration for the onsite printing and behaviors per the customer requirements. Some of the system-level options are for Network Settings, Security Settings, Finisher Settings, Job Manager Settings, Custom Job Layout and Shortcut Settings, etc. The FreeFlow® Print Server Web-UI authorizes the System Administrator role to manage the system-level options. The Operator role is restricted access to these preferences and options unless the System Administrator grants them access.

4.2.2 Web UI Security Features and Capabilities

In addition to the robust set of Security capabilities that are build-into the underlying Windows® OS, the FreeFlow® Print Server Web-UI offers many Security related capabilities available to define locally or from a remote Windows® or MAC® client. The major security capabilities available from the Web-UI are as follows:

4.2.2.1 Security Profile

The FreeFlow® Print Server Web UI includes a Security Profile with a Standard (default) and High level to provide an easy and convenient method to define security controls in a centralized profile. Once you set the Security profile to "High", the FreeFlow® Print Server software automatically configures several built-in security options. In addition to the two static Security profile levels, a System Administrator can create a "custom" security profile that is dynamic and allows custom security settings to suit customer requirements. See **Section 6.1** "*Security Profile*" for more information.

4.2.2.2 UI Web- Feature Access Controls

Access to Web-UI features and options (E.g., Print From File, Job Manager Options, Queue Manger Options, Saved Jobs, Color Manager Options, Etc.) can be enabled/disabled by the System Administrator for users in the Operator or User groups. See **Section 5.3** "*Web-UI Feature Access Control*" for detailed information.

4.2.2.3 Secure Job Scheduling

The FreeFlow® Print Server application offers a Secure Job mode for print jobs managed in the Job Manager of the Web-UI. Jobs defined for secure printing enter the Job Manager and are not accessible without entering a secure pin number. The document (a.k.a., print job) is not available for print scheduling or modification of any kind without entering a valid pin number. Job submission applications can define a pin code for the job when they submit it for printing to the Baltoro™ HF Press. The pin code sends over the network communication in an encrypted format.

4.2.2.4 User/Group Management

The FreeFlow® Printer Server offers a User/Group management capability in the Web-UI to create and manage users that are a member of either the built-in System Administrator, Operator or User group. These built-in user accounts are accessible from the FreeFlow® Print Server Web-UI for login and are separate from the Windows® users. You use the FreeFlow® Print Server Web-UI from your browser to create new users, change the user passwords and password policies, etc. This capability supports Strong Passwords, Lock/Unlock Option, and Password Security options. Refer to **Section 5.1** "*User & Group Access & Roles*" for detailed information.

The System Administrator role can grant/deny access to features in the Web-UI for FreeFlow® Print Server users associated with either an Operator or User role. See **Section 5.3** "*Web-UI Feature Access Control*" for detailed information.

4.2.2.5 Password Security

The "built-in" FreeFlow® Print Server users define well-known passwords after the initial install of the FreeFlow® Print Server software. You should change the default password for the built-in user accounts (System Administrator, Operator and User) when initially installed. Change the passwords to the customer-required passwords to meet their Password Security requirements. The Web-UI authorizes the System Administrator role to change any user account passwords. In addition, the owners of a user account can change their own password. See **Section 6.3.1** "*FreeFlow® Print Server Password Security*" for more detailed information pertaining to Password Security settings from the FreeFlow® Print Server Web UI.

4.2.2.6 Web-UI Console Logging

The FreeFlow® Print Server platform has a Web-UI Console Logging feature that will log all tasks performed in the FreeFlow® Print Server Web-UI including user login/logout activity. See **Section 5.6.2** "*FreeFlow® Print Server Web-UI Console Logging*" for more information.

4.2.2.7 Web-UI Host Filtering

Remote hosts can be restricted from the FreeFlow® Print Server platform using the IP Filtering capability in the FreeFlow® Print Server Web-UI. This feature is a FreeFlow® Print Server interface to firewall access to the FreeFlow® Print Server Web-UI application. The Web-UI grants the System Administrator role authorization to configure Web-UI Remote Access filtering by adding one or more IP addresses of remote host(s) to be restricted. The options to define host filtering are as follows:

1 Disable All Connections
2 Enable All Connections [Default]
3 Enable Specified Connections by:
   - IP Address

- Range of IP Address'
- Subnet

When you select option #3 above, the administrator can create a list of Trusted Hosts. The hosts are simply "trusted" client platforms on the network granted permission to access the FreeFlow® Print Server Web-UI application. Only hosts in the list are grated access.

4.2.2.8 Queue Lock/Unlock

The Queue Manager feature available from the FreeFlow® Print Server Web-UI offers an option to lock and unlock access for making queue attribute modifications. Once locked only a System Administrator role can make queue property changes. The users in the Operator and User groups roles are restricted from making queue changes. This assists with configuration management control of printing requirement settings by the System Administrator.

4.2.2.9 Print Service Gateway Access Control

The FreeFlow® Print Server application offers options to disable network and Print Service Gateways that are not required for customer printing workflow. For example, gateway services for LPR, IPP, Socket (port 9100), SNMP, etc. can be disabled and enabled. Only the System Administrator role is authorized to manage Print Service Gateway settings.

The Security profile includes options to enable and disable services such as SNMP, TLS 1.0/1.2, SHA1/SHA2, etc. The Security profile disables the SSL v2/v3 cryptographic modules by default, and we recommend leaving them disabled. See **Section 6.1** "*Security Profile*" for more information.

4.3 Marking <-> IOT Interface

This section describes the FreeFlow® Print Server platform role in the Marking process with the print engine, and interfaces with the front-end of the Baltoro™ HF Press. It does not describe the Baltoro™ HF Press marking engine that marks the FreeFlow® Print Server delivered raster image pages to paper. Refer to the Information Assurance Disclosure (IAD) document for the Baltoro™ HF Press to obtain that information how the print engine marks data to the printed pages.

4.3.1 Marker Interface Purpose

The marker process running on the FreeFlow® Print Server platform communicates over a private network interface to the Baltoro™ HF Press. The main purpose of the printer network interface is for communication with the Baltoro™ HF Press to deliver raster print job pages that can be marked on the printed pages. By default, this network interface is isolated from the FreeFlow® Printer Server platform front-end network interface connected to the "public" customer network. Therefore, the Baltoro™ HF Press is not directly accessible from the customer "public" network, so does not have access to the customer "public" network. The FreeFlow® Print Server platform acts as a logical buffer for the Baltoro™ HF Press.

The main purpose of the customer network interface is for receiving documents submitted by end-users for printing. A customer can optionally define a proxy configuration on the FreeFlow® Printer Server to allow the Baltoro™ HF Press access to the customer "public" network to support Remote Services (E.g., uploading debug information (CFA data push) to Xerox server available on the Internet, support Automatic Meter Read (AMR), etc.).

4.3.2 Marking Data Security

The Adobe® APPE decomposer renders and rasterizes job pages input as supported PDL documents that are located in an input spool directory and writes the raster image pages in Xerox proprietary format to an output back-end directory. The input and output directory locations are accessible only to the Windows® Administrator. The life of the raster image pages is represented by the timeframe to render/rasterize and deliver the pages to the Baltoro™ HF Press and raster image pages from proceeding jobs overwrite them in the output back-end directory. In addition, the raster image pages in Xerox propriety format are not readable by industry standard image applications. The output back-end directory is included as a location to sanitize this had disk area when running the Data Overwrite application included with the FreeFlow® Print Server platform.

4.4 Software Structure & Technologies

This section defines the applications, operating system and network technologies available on the FreeFlow® Print Server platform.

4.4.1 Open-Source Components

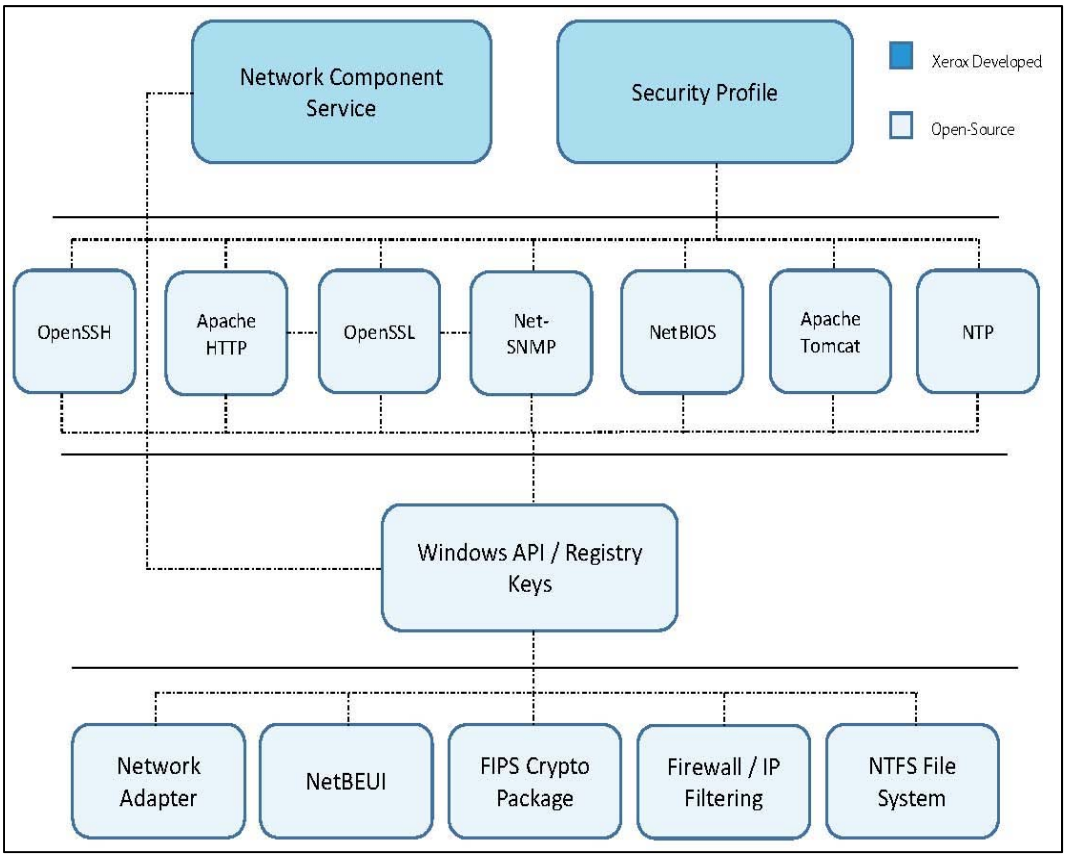
Open-Source components in the connectivity network layer implement high-level protocol services. The security-relevant network connectivity layer components for the FreeFlow® Print Server platform is:

1. Apache HTTP 2.4.38
2. OpenSSH 7.3p1
3. OpenSSL 1.1.0j
4. Net-SNMP 5.7.3 (SNMPv3)
5. Apache Tomcat 6.0.45
6. NTP 4.2.8p10

These Open-source components are updated in FreeFlow® Print Server software releases when necessary to maintain updated technology, security improvements, etc., and the version number is updated.

4.4.2 Operating System Layers

The OS layers include the operating system, network, and physical I/O drivers. The FreeFlow® Print Server application run on the Windows® OS.

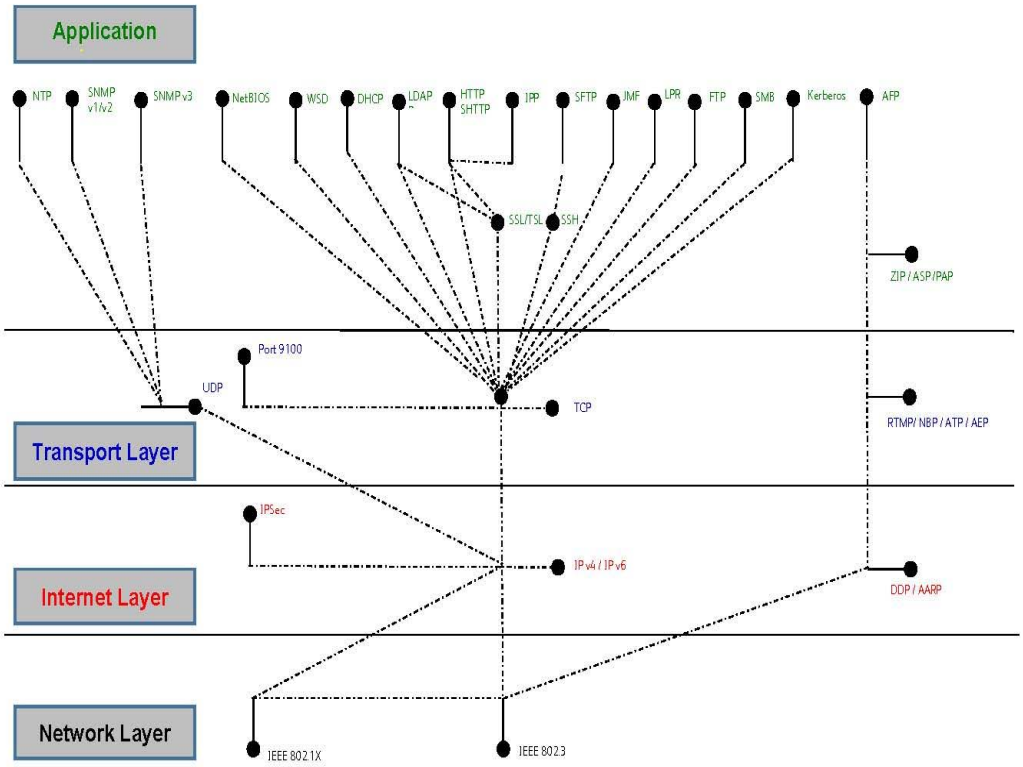


FreeFlow® Print Server Operating System Layers

Note: *The above illustration if the Operating System Layers on the FreeFlow® Print Server platform only. The Print Station Interface Platform (PSIP) component of the* Baltoro™ HF *Press defines its own Operating System Layers.*

4.4.3 Network Protocol Layers

Refer to the diagram below that illustrates the IPv4/IPv6 protocol stacks supported by the FreeFlow® Print Server platform and annotated per the DARPA model.



DARPA Network Protocol Model (a.k.a., OSI Layers)

Note: The above illustration is the OSI Layers on the FreeFlow® Print Server platform only and represents the front-end customer network interface. The Print Station Interface Platform (PSIP) component of the Baltoro™ HF Press defines its own OSI Layers.

4.5 Logical Network Access & Interface Security

This section describes the modules and methods on the FreeFlow® Print Server platform that supports secure connectivity and communications for job submission and job/printer status workflows.

4.5.1 TLS/SSL Cryptographic Module

The FreeFlow® Print Server software supports Transport Layer Security (TLS) v1.0/v1.2 cryptographic protocols to provide authentication, data integrity and encryption security for all FreeFlow® Print Server workflows that support these protocols. You can configure a self-signed SSL certificate, have it Certificate Authority (CA) signed, and install it on the FreeFlow® Print Server platform to secure and authenticate the transfer of user information and data over a network connection. After installing the SSL certificate, any remote connection request by applications supporting the TSL protocol is verified using an authentication and exchanged certificate before granting access. It is recommended that all other insecure print workflow services be disabled, and UDP/TCP ports closed to ensure only secure access to a Xerox printer. The FreeFlow® Print Server platform supports install of self-signed 1024-bit and/or 2048-bit SSL certificates.

You can use the certificate management facilities built into the Windows® platform to create, setup and install Triple DES-EDE-CBC and AES (supported by TLS v1.2 protocol) encryption, with the latter being the most secure and stronger encryption algorithm, to facilitate the secure exchange of print data between the job submission client and the FreeFlow® Print Server platform. The TLS v1.2 cryptographic module supports the SHA2 hash encryption algorithm, which is the strongest today. The Internet Print Protocol (IPP), Internet Services Web client and clients using SNMPv3 can take advantage of TLS v1.0/v1.2 protocols when submitting jobs to the printer or obtaining job or printer information. By default, the FreeFlow® Print Server platform supports TLS v1.0 and setting the Security profile to 'High' updates to TLS v1.2. See **Section 6.1** "*Security Profile*" for more information.

It is required that an SSL digital certificate be installed on the FreeFlow® Print Server / Windows® DFE platform to enable job submission workflow with SSL/TLS authentication and encryption protocols. With the certificate installed a Windows® client can retrieve it and start using it to communicate and submit "secure" data over the network to the printer. Many customers that required protection of highly sensitive, private and/or top-secret information require FIPS 140 compliant cryptographic algorithms. See **Section 4.5.2** "*FIPS 140-2 Encryption*" and **Section 6.10.2** "*Federal Information Processing Standard (FIPS 140-2)*" for more detailed information.

Customer print workflows that make use of secure SSL/TLS authentication are File Transfer Protocol (FTP), Internet Print Protocol (IPP) and Internet Services Web Client. The FreeFlow® Print Service Update Manage UI uses SSL/TLS authenticate with the Xerox Download Manager service to download and install FreeFlow® Print Server software patches and Windows® security patches. The SNMPv3 services use SSL/TLSL services to authenticate remote SNMPv3 client requests.

4.5.2 FIPS 140-2 Encryption

You can enable a group policy setting on the FreeFlow® Print Server platform to ensure that the encryption algorithm and strength is FIPS 140-2 compliant. The option that must be enabled is "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing", and it is up to the service or process handling data to apply the FIPS 140-2 compliant cryptography methods and modules built-into the Windows® OS. See **Section 6.10.2** "*Federal Information Processing Standard (FIPS 140-2)*" for more information.

FreeFlow® Print Server workflows that will support FIPS 140-2 compliant encryption and CA-signed certificates are LDAP (using SSL/TLS), sIPP (using sHTTP and SSH), FreeFlow® MakeReady (using sHTTP and SSL/TLS), SNMPv3 (using SSL/TLS), SMB, IPSec (using Kerberos), Xerox CentreWare (using SNMPv3), and Web Client Services (using sHTTP and SSL/TLS). The minimum certificate key length configured for FIPS 140-2 compliancy is at least 1024-bit, and the FreeFlow® Print Server supports 1024 and 2048-bit certificates. Once the FreeFlow® Print Server Security profile is set to 'High', services will use FIPS 140-2 compliant authentication and encryption. See **Section 6.1** "*Security Profile*" for more information.

With FIPS 140-2 algorithms configured, there are Microsoft® components that will use the FIPS group policy, and therefore ensure usage of these higher strength/complex algorithms. When the FIPS Local/Group Security Policy is set, the following components will enforce the validated module Security Policy.

1. Schannel Security Package
2. Remote Desktop Protocol (RDP) Client
3. Encrypting File System (EFS)
4. Some Microsoft® .NET Framework Applications (.NET also provides cryptographic algorithm implementations that have not been FIPS 140 validated.)

5. BitLocker® Drive Full-volume Encryption
6. IPsec Settings of Windows® Firewall
7. Effects of Setting FIPS Local/Group Security Policy Flag

The Windows® components enforcing this setting will only use those algorithms approved or allowed in FIPS mode. The specific changes are:

1. Schannel Security Package forced to negotiate sessions using TLS1.0. The following supported Cipher Suites are disabled:

    a. TLS_RSA_WITH_RC4_128_SHA
    b. TLS_RSA_WITH_RC4_128_MD5
    c. SSL_CK_RC4_128_WITH_MD5
    d. SSL_CK_DES_192_EDE3_CBC_WITH_MD5
    e. TLS_RSA_WITH_NULL_MD5
    f. TLS_RSA_WITH_NULL_SHA

2. The set of cryptographic algorithms that a Remote Desktop Protocol (RDP) server will use is scoped to:

    a. CALG_RSA_KEYX - RSA public key exchange algorithm
    b. CALG_3DES - Triple DES encryption algorithm
    c. CALG_AES_128 – 128-bit AES
    d. CALG_AES_256 – 256-bit AES
    e. CALG_SHA1 - SHA hashing algorithm
    f. CALG_SHA_256 – 256-bit SHA hashing algorithm
    g. CALG_SHA_384 – 384-bit SHA hashing algorithm
    h. CALG_SHA_512 – 512-bit SHA hashing algorithm

4.5.3 SSH Cryptographic Module

The FreeFlow® Print Server software supports SSH which uses public-key cryptography to authenticate a remote client workstation, such as Windows®, and to authenticate the user requesting desktop access. The Secure Shell protocol supports a secure FTP or Secure File Transfer Protocol (SFTP) connection for the purpose of "secure" file transfer to the FreeFlow Print Server platform.

The Windows® platform does not natively support "secure" FTP, so an implementation over SSL and SSH was delivered with the FreeFlow Print Server product. There are some limitations with the FTP over SSH, so the recommendation is to incorporate FTP over SSL method. We offer procedures to incorporate FTP over SSH if a customer prefers the "secure" transfer of data without the need to create and install an SSL certificate.

The set of Ciphers and MACs supported are as follows:

SSH Ciphers/MACs Table

Ciphers Supported	MACs Supported
3des-cbc,blowfish-cbc	ecdh-sha2-nistp256
cast128-cbc,arcfour	ecdh-sha2-nistp384
arcfour128	ecdh-sha2-nistp521
arcfour256	diffie-hellman-group-exchange-sha256
aes128-cbc	diffie-hellman-group-exchange-sha1
aes192-cbc	diffie-hellman-group14-sha1
aes256-cbc	diffie-hellman-group1-sha1
rijndael-cbc@lysator.liu.se	
aes128-ctr	
aes192-ctr	

aes256-ctr	
aes128-gcm@openssh.com	
aes256-gcm@openssh.com	
chacha20-poly1305@openssh.com	

The SSH services on the FreeFlow® Print Server platform supports a secure remote login and file transfer using a secure FTP connection. You can achieve Hot Folder workflow securely by using FTP over SSH to transfer print jobs into a FreeFlow® Print Server Hot Folder directly. Once the jobs securely transfer to a directory location associated with a queue, the Hot Folder service imports the jobs into the FreeFlow® Print Service Job Manager for print scheduling, processing and printing.

4.5.4 IPSec Protocol Security

The FreeFlow® Print Server software supports the Internet Protocol Security (IPSec) protocol, which authenticates, delivers data integrity, and encrypts each exchanged IP packet with a job submission client. The Windows® Firewall with Advanced Security service incorporates IPSec to assist with making connection security rules to define authentication of the connection and/or encryption of the data. A connection security rule forces two-peer computers to authenticate before they can establish a connection and to secure information transmitted between the two computers. Windows® Firewall with Advanced Security uses IPsec to enforce these rules. An IPSec policy must be setup by both the requester and service endpoints to ensure synchronization and compatibility.

The FreeFlow® Print Server platform supports AES block cipher encryption algorithm, which facilitates the secure exchange of print data between a remote client such as Windows®, and the FreeFlow® Print Server platform. The FreeFlow® Print Server platform supports SHA2 hash encryption algorithm, which facilitates the secure exchange of encrypted authentication data between the job submission client and the FreeFlow® Print Server platform. The Xerox® printer grants access when a shared key matches between the remote Windows® client and the FreeFlow® Print Server platform.

IPSec services enable secure network communication for remote user login and file/print protocol workflows. Network protocols that are inherently not secure, and even those that do have data encryption can benefit from IPSec services. Once you establish IPSec connectivity between the FreeFlow® Print Server platform and remote Windows® clients, insecure print, file and job management workflows can benefit from secure network communication. Some of the unsecure FreeFlow® Print Server workflows that benefit from IPSec are:

1. LPR Job Submissions
2. Port 9100 Job Submission
3. Job Forwarding Workflow
4. SMB (Windows® Folder Sharing, Print from SMB, Scan to SMB, Hot Folder, etc.)
5. XEAR Accounting Services

4.5.5 UDP/TCP Ports

There are Network/Print protocol services that are enabled and accessible on the FreeFlow® Print Server / Windows® platform to ensure support of printing workflows (e.g., FreeFlow® Make Ready, LPR, IPP, JMF/JDF, etc.). The Windows® Firewall with Advanced Security provides the ability to define rules that can close ports associated with Network / Print protocol services when not required by the customer print work flow(s).

The FreeFlow® Print Server platform supports many Network/Print protocol services to facilitate file access and printing workflows for Xerox® printer products. See this list below:

Print/Network Services and Ports Table

Print / Network *Protocol*	Port	Job Workflow Facilitation and Considerations
Echo	7	Echo is a service that listens on port 7 for a connection request, receives data from the remote end-point, and returns it back. The ping utility is a commonly used utility to determine if another computer is available on the network. Echo is a service of the ICMP protocol, and intruders can use this protocol to identify information about a remote computer device. The Echo port must be open to support Web UI Job forwarding job submissions between printers.
FTP	21	The File Transfer Protocol (FTP) client/server runs over port 21 and is an insecure protocol. It is recommended to close port 21 in favor of using port 22 for a "secure" connection for file transfer. FreeFlow® Make Ready has a workflow to use FTP and does have the ability to submit using "secure" FTP. Another common workflow that uses FTP is Hot Folder.
SSH	22	The Secure Shell protocol is a highly secure network service used to protect TCP/IP based protocols with data encryption and an SSL certificate. There are several "secure" utility services (e.g., SSH or putty, SFTP, SCP, etc.) that access the FreeFlow® Print Server / Windows® platform over port 22.
NTP	23	The Network Time Protocol (NTP) service runs over port 23 from a server used to synchronize the time for all of the network servers. It is not recommended to use the FreeFlow® Print Server platform as an NTP server. Setup and configuration are required to enable the FreeFlow® Print Server platform as an NTP client for the purpose of synchronizing with an NTP server on the network.
SMTP	25	The Simple Mail Transfer Protocol (SMTP) service runs over port 25 to a mail server. This is typically useful for printers that also have a scanner to mailing scanned output. This port should not be open on the FreeFlow® Print Server platform.
DNS	53	The Domain Naming Service (DNS) runs over port 53 to a DNS server to resolve domain names for the FreeFlow® Print Server platform. This port should not be open on the FreeFlow® Print Server platform.
DHCP	68	The Dynamic Host Configuration (DHCP) runs over port 68 to a DHCP server to assign a dynamic IP Address. Assign the FreeFlow® Print Server / Windows® platform a static IP address given it is a specialized server, and not a client platform. This port should not be open on the FreeFlow® Print Server platform.
HTTP	80	This service is required to connect to the FreeFlow® Print Server / Windows® platform from an HTTP client, such as the Web Print client, Internet Print Protocol (IPP) service, JMF/JDF service, FreeFlow® Print Server Core, FreeFlow® MakeReady, Remote Services, etc. The HTTP protocol is insecure, so it is recommended to close port 80 in favor of using port 443 for a "secure" HTTP connection.
Kerberos	88	The Kerberos Authentication services are an MIT technology built-into the Window OS running the FreeFlow® Print Server application. It is the default authentication technology. Protocols such as IPSec can make use of Kerberos for host/user authentication.
RPC	111	This port is used as a well-defined means for determining the ports upon which other services in the system are running. It is referred to as a "portmapper" because it provides a directory, or "mapping" between available services and their ports. Many internal FreeFlow® Print Server application processes and Windows operating system procedures depend on the RPC service.

SMB (Legacy)	135 136	The service for these SMB ports supports older legacy versions of SMB no longer used unless a Windows® environment have old Windows® versions. Close these ports unless there are older Windows® client platforms on the network that required SMB services.
WINS NetBIOS	137	This service is required for applications that require WINS running over NetBIOS to resolve domain names and used by the FreeFlow® Print Server platform to do Network Discovery. Setting the Security profile to 'High' closes this port. See **Section 6.1** "*Security Profile*" for more information.
SMB NetBIOS (UDP)	138	This is an implementation of SMB over NetBIOS using UDP/IP Datagram Service (Data Transfer) and used by the FreeFlow® Print Server platform to do Network Discovery. Setting the Security profile to 'High' closes this port. See **Section 6.1** "*Security Profile*" for more information. The FreeFlow® Print Server platform supports SMB directly over TCP, and therefore recommend closing port 138. By default, the FreeFlow® Print Server platform enables SMB v2 and disables SMB v1.
SMB NetBIOS (TCP)	139	This is an implementation of SMB over NetBIOS using TCP/IP Session Service (Session Management) and used by the FreeFlow® Print Server platform to do Network Discovery. Setting the Security profile to 'High' closes this port. See **Section 6.1** "*Security Profile*" for more information. The FreeFlow® Print Server platform supports SMB directly over TCP, and therefore recommend closing port 139. By default, the FreeFlow® Print Server platform enables SMB v2 and disables SMB v1.
Net-SNMP v3	161	This service is required for exchanging SNMP v3 messages. The SNMP v1/v2 version services are insecure, so the recommendation is to use SNMP v3 for a "secure" SNMP connection.
SNMP-Trap	162	This service is required for SNMP Traps. The SNMP v1/v2 version services are insecure, so the recommendation is to use SNMP v3 for a "secure" SNMP connection.
AppleTalk Ports	201 202 203 204 205 206 207 208	The AppleTalk Gateway is a legacy service that supports AppleTalk network for MAC® workstations. The recommendation is to close these ports The port services are 1. AppleTalk Routing Maintenance (201), 2. AppleTalk Name Binding (202), 3. Unused #1 (203), 4. AppleTalk Echo (204), 5. Unused #2 (205), 6. Zone Information (206), 7. Unused #3 (207), 7. Unused #4 (208).
HTTPS	443	Transport Layer Security (TLS) is a network security protocol that encrypts and transmits data via HTTP over the TCP/IP network. TLS is an encryption protocol layers placed between a reliable connection-oriented network layer protocol and the application protocol layer. This port is required by client submission applications such as HTTPS and "secure" IPP. Job submission applications that can take advantage of this "secure" connection protocol is the Internet Web Services, IPP clients, FreeFlow® Print Server Core, Remote Services, and/or the FreeFlow® Make Ready (v2.0 or newer) submission clients. The specific Windows® service associated with this port is 'World Wide Web Services (HTTPS Traffic-In)'.
SMB (TCP)	445	The SMB (a.k.a., Samba) service provides Windows® Folder Sharing capabilities. Print from SMB, Scan to SMB, Hot Folder, etc. require this SMB service. Enable digitally sign communications to prevent man-in-the-middle attacks against the SMB services. By default, SMB v2 services and digital signing are disabled on the FreeFlow® Print Server platform. Define the Security Profile to "High" to enable SMB v2/v3 and digital signing.
LPR	515	The LPR Gateway supports print job submissions from widely available LPR client clients. The LPR print job submission method is the most

		widely used print protocol. It is an insecure protocol in that it does not support authentication or data encryption. However, there is no known way to exploit the FreeFlow® Print Server platform over port 515. Enable IPSec services to make LPR job submissions "secured".
IPP	631	IPP client applications have been implemented by Xerox (FreeFlow® Application Suite Software such as FreeFlow® Make Ready and FreeFlow® Core), and 3rd-party partners. The IPP Gateway on the FreeFlow® Print Server platform services these IPP clients over port 631 and establishes a connection over port 80 to transfer print data. This is an insecure network connection with data transferring over the network in clear text. By default, the IPP services utilize port 80 to retrieve print data from the remote client requesting an IPP job submission. It is recommended to update the network connection to HTTPS (port 443) over TLS to ensure "secure" using user authentication and data encryption algorithms.
Web Discovery Services	3702	This is a Windows® multicast discover protocol to locate services on a local network using SOAP / UDP web services. Windows® Web Discovery automatically discover WSD-enabled network printers. The FreeFlow® Print Server platforms are eligible for discovery, as they are WSD-enabled. The FreeFlow® Print Server platform has a printer discovery capability to allow discovery and listing of all remote FreeFlow® Print Server / Printers on the network.
Windows® Remote Desktop	3389	This is Windows® graphical interface to connect to another computer running the Remote Desktop server over a network connection and view the remote Windows® Desktop on the local computer.
IPDS	5001	The IPDS print workflow has a unique protocol service that uses port 5100 for connecting to the FreeFlow® Print Server / Windows® platform to transfer print data.
JMF	7781	3rd-Party partners (e.g., XMPie and GMC PrintNet), and FreeFlow® Print Server customers have implemented JMF/JDF client applications. This is the Adobe® recommended print protocol to submit PDF jobs. It is a bi-directional protocol to submit and obtain job information for print jobs from the FreeFlow® Print Server platform on behalf of a Xerox printer.
Tomcat Web Services	8005	This service is used for the FreeFlow® Print Server Web Print client (aka, Internet Services Gateway), IPP Gateway, JMF/JDF Gateway, FreeFlow® Core, Remote Services, etc. to execute Java applets for Apaches Web services.
HTTP/TCP Symon Communications Event and Query Engine	8011	This is a port required internally by Print Protocol Gateways as a communication domain interface layer between process daemons implemented with dissimilar programming languages. This port can be closed on the "customer" network interface without impact to job submission workflows or production printing. The current FreeFlow® Print Server implementation does not close port 8011 when the Security profile is set to "High". However, a future patch software release will ensure this port is closed for the "High" profile. See the "*Protocol Service/Port State Table*" table in **Section 5.1.3** "*Security Profile UDP/TCP Port Settings*" for the impact of the Security Profile setting on TCP/TCP ports.
Proxy	8080	This proxy service transfers CFA data pushes (debug information for problem investigation) outside of a customer network to a Xerox® server, and supports the Automatic Meter Read (AMR) service. This port is required for the Baltoro™ HF Press push a CFA data push. Therefore, the FreeFlow® Print Server platform acts as a surrogate for the Baltoro™ HF Press to transfer the CFA data to a Xerox communication server on the Internet and respond to AMR requests. This port is not required inbound on the "public" network interface of the FreeFlow® Print Server platform.

SignalR	8090	The Web-UI service on the FreeFlow® Print Server platform initiates a SignalR broadcast to all Web-UI clients when the state of the Web-UI changes (e.g., job list updates, job status change, job deleted, setting change, etc.), and the change is visible to all Web-UI clients once they receive the SignalR request. This is a port required for the remote FreeFlow® Print Server Web-UI.
Web Management Service	8172	The Web Management Service handles remote requests to manage the Web Server on the FreeFlow® Print Server platform by using IIS Manager. IIS Manager supports management functions for configuring the Web Server, FTP, SNMP, NTP, SSL Certificates, etc. The type of capabilities configured are security, performance and reliability features. You can start/stop services, pause Web services backup/restore server configurations, etc.
JMF (Hot Folder)	8181	This service handles JMF requests from a remote JMF client that transfers JDF and PDL files to a Hot Folder location for print scheduling.
Socket (Raw TCP/IP)	9100 9400	The Socket Gateway supports job submissions submitted over TCP/IP to a raw port service. The Xerox® Universal Print Driver submits jobs over this connection. It is also common for mainframes to submit IPDS to the FreeFlow® Print Server Socket Gateway via these ports.
SNMP v1/v2	16611	This service is required for exchanging SNMP v1/v2 messages. The SNMP v1/v2 version services are insecure, so the recommendation is to use SNMP v3 for a "secure" SNMP connection, and close port 16611. Defining the Security profile to 'High' will disabled the SMNP v1/v2 services and enable SNMP v3.
SNMP v3	161	SNMP v3 adds much stronger security features than SNMP v1/v2, such as client authentication, encryption of credentials, and encryption of data over the network. SNMP v3 ensures "secure" remote monitoring of Xerox® printers for IPv4 and IPv6 network addressing. Defining the Security Profile to 'High" will enable SNMP v3 services and disabled SNMP v1/v2 services from the customer "public" network.
WSD Transfer	53202	This service provides the ability to specify an alternate communication port number used for metadata exchange with WSD clients. WSD-Transfer defines how to invoke a simple set of familiar verbs, such as Get, Post, Put, and Delete, using SOAP.
WSD Print	53203	This service provides the ability to simplify programming a connection to web service-enabled devices such as the FreeFlow® Print Server Printer platform. It conforms to the Devices Profile for Web Services (DPWS). It is an extensible service that replaces older Windows® networking functions and a common framework for allowing access to new device (e.g., FreeFlow® Print Server / Printer) API's.

Defining the FreeFlow® Print Server security profile to 'High' will close UDP/TCP ports that are high risk or not needed for print workflows. See **Section 4.5.5** "*UDP/TCP Ports*" and **Section 6.1.3** "*Security Profile UDP/TCP Port Settings*" for more information.

5.0 FreeFlow® Print Server System Access

This section focuses on remote host and remote/local user access to the FreeFlow® Print Server platform. You can access the FreeFlow® Print Server Web-UI, Windows® Desktop, and Windows® OS locally or remotely as a registered known user when properly authenticated.

5.1 User & Group Access and Roles

The FreeFlow® Print Server / Windows® platform has two separate mechanisms to manage Users and Groups. There is the Windows® OS management for User and Group accounts, which is a standard capability for managing Windows® users to access the Windows platform. The mechanism in Windows®, referred to as User Account Control (UAC), is a Security component allowing the Windows® Administrator management of credentials for non-administrator users to perform tasks.

The FreeFlow® Print Server application also includes its own Web-UI User and Group account management capabilities and System Administrator account to assign roles for managing FreeFlow® Print Server application capabilities such as Security, configuration elements, managing print jobs, printing-related operations, printing resources etc.

5.1.1 System Administrator Access

The FreeFlow® Print Server / Windows® platform has two separate mechanisms and Administrator accounts to manage Users and Groups. There is a built-in Administrator for the Windows® Embedded Standard 10 OS to manage User and Group accounts, which is a standard capability for managing Windows® users. These are roles granted access to Windows® OS capabilities.

The built-in Windows® Administrator has full read/write access to the Windows® system (e.g., applications, utilities, command window, files/directories, etc.). The Administrator user is a member of the Administrator group. The role of this Administrator account is to make Windows® system-level application and configuration changes (e.g., manage Windows® Users/Groups, manage Windows® Network/Security settings (E.g., Security Profile, SSL/TLS certificate install and setup), Install Windows® / FreeFlow® Print Server applications and patches, FreeFlow® Print Server / Windows® Backup & Restore, Diagnostics, etc.). The Windows Administrator role also is granted access to manage FreeFlow® Print Server system-level applications (E.g., Security Profile, FreeFlow® Print Server Backup-& Restore, etc.)

The FreeFlow® Print Server application has a built in System Administrator account with full access to the Web-UI to manage tasks such as configuration settings, features and print resources, define security settings, manage FreeFlow® Print Server application users, etc. The FreeFlow® Print Server System Administrator can grant/deny access to Web-UI features. See **Section 5.3** "*Web-UI Feature Access Control*".

5.1.2 Windows® User & Group Accounts

The Windows® OS release includes built-in Windows® users, and there are users created in Windows® by the FreeFlow® Print Server software install. The built-in Windows® account is Administrator. The Windows® Desktop users created by the FreeFlow® Print Server software is 'cse', 'xrxusr' and 'ftpuser'.

There are two user groups available on the Windows® platform, which are "Standard' and 'Administrator". By default, newly added users in Windows® will become a member of the 'Standard' group. The number of users added in the Administrator group should be very limited (e.g., Windows® Administrator, CSE and Backup/Recovery Administrator users).

The 'Administrator' user built-into Windows® is a well-defined role to perform System Administration tasks by Microsoft®. See a description of the Windows® users below:

FreeFlow® Print Server Windows® Users / Roles Table

FFPS Windows® User	User Role / Description
Administrator	1. A built-in Windows® user with full read/write access to Windows® system (e.g., applications, utilities, command window, files/directories, etc.). 2. The role of this Administrator account is to make Windows® and configuration changes (e.g., manage Windows® Users/Groups, manage Windows® Network/Security settings, install Windows® / FreeFlow® Print Server applications and patches, FreeFlow® Print Server / Windows® Backup & Restore, etc.). 3. FreeFlow® Print Server system-level application management for features such as the Security Profile, FreeFlow® Print Server Backup & Restore, Diagnostics, etc. are also granted to the Windows® Administrator. 4. The Administrator user is a member of the Administrator group. 5. It is highly recommended to create another Windows® user with Administrator privileges for recovery purposes in case the built-in Administrator account is locked out.
cse	1. This FreeFlow® Print Server install creates the 'cse' user using Windows® User management with full read/write access to Windows® system (e.g., applications, utilities, command window, files/directories, etc.). 2. The role of this 'cse' account is for the Xerox Service or Customer Service Engineer (CSE) to diagnose and report any FreeFlow® Print Server / Windows® hardware, printer or software problems. The CSE must have access to the system diagnostic and service utilities. 3. The 'cse' user is a member of the Administrator group. 4. The Xerox Customer Service Engineer (CSE) must have access to the "cse" password, Windows Administrator and FreeFlow Print Server "sa" password during a Service call to perform their service responsibilities. The customer IT group can define their own password for the Windows Administrator, FreeFlow Print Server 'sa' and 'cse' accounts but must provide them to the CSE when they service the Xerox printer. Alternatively, the Customer must be present to enter these passwords when required.
xrxusr	1. This FreeFlow® Print Server install creates the 'xrxusr' using Windows® User management with limited access to the system and for the purpose of running FreeFlow® Print Server processes. 2. The FreeFlow® Print Server defined "xrxusr' account is used for the purpose of running most of the FreeFlow® Print Server software services, so represents the FreeFlow® Print Server software like 'System Administrator' does for the Windows® OS as a "system account". 3. Access to the 'xrxusr' account is restricted to only the FreeFlow® Print Server software application. 4. The 'xrxusr' is a member of the Standard Windows® group.
ftpuser	1. This FreeFlow® Print Server install creates an 'ftpuser' user account using Windows® User management with limited access to its own home directory location. 2. The role of this 'ftpuser' user is for remote access by remote client applications such as FreeFlow® Make Ready and XEAR. 3. The 'ftpuser' is a member of the Standard group.

5.1.3 FreeFlow® Print Server User & Group Accounts

The FreeFlow® Print Server implements its own User and Group mechanism used to log into and grant access to the Web UI application and feature capabilities in the FreeFlow® Print Server Web UI.

5.1.3.1 Built-in User Accounts

The FreeFlow® Print Server application includes three "built-in" (a.k.a., default) login user accounts. These FreeFlow® Print Server users and their associated groups are independent of the Windows® OS users and groups. The 'built-in' FreeFlow® Print Server users are:

1. sa (System Administrator)
2. operator (Printer Operator)
3. user (Walk-up User)

You cannot remove the FreeFlow® Print Server built-in user accounts from the FreeFlow® Print Server application. However, any built-in user account may be "locked" by the SA as a means to ensure that unique customer-created accounts are used in place of these "built-in" accounts. Using unique user accounts is important to customers who require audit logs that identify who accesses the FreeFlow® Print Server application and the date/time accessed. Refer to **Section 6.6.2** "*FreeFlow® Print Server Web-UI Console Logging*".

Users can access the FreeFlow® Print Server application through a local/remote Web-based UI application or remotely over the network with Windows® "Remote Desktop Connection" to manage jobs and the printer. All FreeFlow® Print Server Web=UI application actions or command window actions are associated with a FreeFlow® Print Server user account. A user logging into the FreeFlow® Print Server / Windows® platform defines their role and is the basis for granting access to authorized services.

A FreeFlow® Print Server Web application or Windows® Remote Desktop logon session begins upon successful Authentication (verification) of a username and credentials (password). The logon ends by logging off, which can be either user-initiated or system-initiated. When the Automatic User Logoff option is configured a system-initiated log off will occur when FreeFlow® Print Server Web-UI is idle for the configured timeframe (30-minute default). Once the FreeFlow® Print Server Web application or Windows® Remote Desktop login is established, the user can interact with the FreeFlow® Print Server / Windows® platform, subject to the Authorization (i.e. Access Control Policies) associated with the settings such as the associated user group, and the Web-UI Access Control options. Refer to **Section 5.3** "*Web-UI Feature Access Control*" for more detailed information.

The management of user functions requires authorization via "Role-Specific Privileges' whereby the FreeFlow® Print Server software validates access based on permissions assigned to user roles and does so using Windows® Authorization Manager Rules for role-based access control.

5.1.3.2 Built-in Group Accounts

The FreeFlow® Print Server User Groups have one or more FreeFlow® Print Server User members, which inherits a role, and set of access policies associated with that group. The main roles for a Digital Front End (DFE) Print Service used for printing are administrator and operator. The administrator role is needed to manage the system-level settings for capabilities (e.g., such as system policy settings for Job Processing, Queues, Printing Options, Network Access Settings, Accounting/Billing Settings, etc.) used for PDL job processing and printing. The operator role does not have access to most of the system-level policy settings but is intended to manage job-level settings and operations (e.g., submitting jobs, job scheduling/releasing, queue settings such as enablement of hot folders, create/delete queues, enable/disable access to queues, etc.) and pause/resume the printer. In addition to the default Operator and System Administrator users there is a built-in user named User, which has very limited access to the Web-UI features, so is the default for walk-up users. If the built-in User account is against customer policy, then disable this account.

The FreeFlow® Print Server application provides three default User Groups as follows:

1. System Administrator (**member:** sa)
2. Operator (**member**: operator)
3. Users (**member:** user)

You cannot change or remove the built in User Groups them from the FreeFlow® Print Server application. The FreeFlow® Print Server software does not provide a way to create a new User Group. Each of the "built-in" users are mapped to one of the built-in default groups. There is a capability to grant/deny FreeFlow® Print Server Web-UI access control for capabilities such as Job Management, Queue Setting, Color Management, and other Web-UI capabilities. You can control Operator and User access for each FreeFlow® Print Server Web-UI feature (e.g., Release Jobs, Print From File, Job Preview, etc.) by selecting enable/disable for each Web-UI feature from an access control list.

The general privileges granted to a User is defined by their associated group and "role" inherited by the group. The access control option to control Web-UI features is only configurable for the FreeFlow® Print Server groups and not available to control access of each user individually. Access control can only be enabled/disabled for the FreeFlow® Print Server Operator and User Groups, and it provides access/denial customization of Web-UI features through these two groups.

Only the FreeFlow® Print Server System Administrator can enable/disable access control options for the Operator and/or User Groups. Once the System Administrator grants access of Web-UI features to the Operator group, all User members of this group can access the enabled feature while logged into the FreeFlow® Print Server Web-UI. The System Administrator user has full access to FreeFlow® Print Server Web-UI features and remains static, so not changeable.

5.2 User Authentication Methods

The FreeFlow® Pint Server platform offers server authentication protocols to verify the credentials and authenticity of communication used for various print workflows. The two peers must have at least one common authentication method or communication will fail.

5.2.1 SSL/TLS Authentication

Transport Layer Security (TLS v1.2) is a network security protocol that encrypts and transmits data via FTP, HTTP or IPP over the TCP/IP network. TLS is an encryption protocol layers placed between a reliable connection-oriented network layer protocol and the application protocol layer. Certificates are part of SSL encryption supported by the TLS protocol.

Server certificates enable users to confirm the identity of a Web server before they transmit sensitive data, such as a credit card numbers, user health information and other PII data. Server certificates also contain the server's public key information to encrypt data and send back to the requesting client application.

It is required that an SSL digital certificate be installed on the FreeFlow® Print Server / Windows® platform to enable job submission workflow with SSL/TLS authentication and encryption protocols. With the certificate installed a Windows® client can retrieve it, start using it to communicate and submit "secure" data over the network to the printer.

Customer print workflows that make use of secure SSL/TLS authentication are Hot Folder (using FTP), Internet Print Protocol (IPP) and Internet Services Web Client. The FreeFlow® Print Service Update Manage UI uses SSL/TLS authenticate with the Xerox Download

Manager service to download and install FreeFlow® Print Server software patches and Windows® security patches. The SNMPv3 services use SSL/TLS services to authenticate remote SNMPv3 client requests.

5.2.2 SSH Authentication

The SSH services use public-key cryptography to authenticate remote computers and user requesting SSH access to the FreeFlow® Print Server platform. This communication protocol uses automatically generated public-private key pairs so encrypt the network connection and use password authentication for the user log on.

Customers make use of SSH services by securely transferring print jobs over port 22 using secure FTP to the FreeFlow® Print Service Hot Folder service. Once the jobs securely transfer to a directory location associated with a queue, the Hot Folder service imports the jobs into the FreeFlow® Print Service Job Manager for print scheduling, processing and printing.

5.2.3 Kerberos Authentication

The Kerberos Authentication services are an MIT technology built-into the Window OS running the FreeFlow® Print Server application. It is the default authentication technology. It supports any client computer on the same or trusted network domain that also implements Kerberos. It uses public key certificate exchange to authenticate communication between two computers.

By default, the FreeFlow® Print Server install defines the Windows® OS as a Workgroup member, and logging into the FreeFlow® Print Server platform using Windows® Remote Desktop uses the local User Account Control (UAC) authentication. The customer can update the FreeFlow® Print Server platform to be a member of a network domain, and logging into the FreeFlow® Print Server platform using Windows® Remote Desktop uses the Kerberos authentication when part of the network domain.

5.2.4 SMB Authentication

Digital Signing is a Security feature in the SMB protocol that digitally signs packets communicated between an SMB client/server. The risk of unsigned SMB packets is the potential for a man-in-the-middle attack against the SMB server. By default, the FreeFlow® Print Server / Windows® software install enables SMB v1 services, disables SMB v2 and disables digital signing of SMB packets. Defining the Security Profile to "High" disables SMB v1 and enabled SMB v2. See **Section 6.1** "*Security Profile*" for more information.

The FreeFlow® Print Server software enables SMB Digital Signing when the Security Profile is set to "High". Digital Signing of SMB packets prevents man-in-the-middle attacks. The SMB client and server can confirm the point of origination and authenticity of SMB packets they receive when digitally signed. Once the SMB server enables digital signing, any unsigned SMB client request will result in a failed connection. SMB clients that enable digital signing can still successfully connect and communicate with an SMB server configured to support unsigned SMB packets.

Customers make use of SMB services by securely transferring print jobs using digital signed SMB packets to the FreeFlow® Print Service Hot Folder service. Once the jobs securely transfer to a directory location associated with a queue, the Hot Folder service imports the jobs into the FreeFlow® Print Service Job Manager for print scheduling, processing and printing.

5.2.5 IPSec Authentication

The IPSec authentication methods supported by the FreeFlow® Print Server platform are as follows:

Kerberos v5

You can optionally configure the FreeFlow® Print Server platform with Kerberos v5 (MIT® technology) to authenticate remote host and user access when using IPSec encryption services. See **Section 5.2.3** "*Kerberos Authentication*" for more information.

Public Key Certificate

You can optionally configure the FreeFlow® Print Server platform to use the public key certificate method to authenticate remote host and user access when using IPSec encryption services. This requires the use of a signed certificate by a trusted certificate authority (CA).

Preshared Key

You can optionally configure the FreeFlow® Print Server platform to use pre-shared key to authenticate remote host and user access when using IPSec encryption services. The pre-shared key one agreed to prior to setup for authentication. This method does not require Kerberos v5 protocol or a public key certificate, so a very simple method.

5.2.6 SNMPv3 Authentication

The SNMP v3 architecture supports a "Transport Security Model" (TSM) framework defined in RFC 5590 and 5591, which identifies a model for handling security threats, security level definitions, and coexistence with transport and security other models. RFC 6353 specifies the Transport Layer Security (TLS), and Datagram Transport Layer Security (DTLS) protocols for enhanced Security of SNMP communication. It is important to understand the TMS framework to gain understanding how TLS or DTLS fit or coexist inside this framework. TSM is a part of the SNMP v3 framework along with the DTLS specification brings SNMP users, applications, and devices under the umbrella of an X.509 public key infrastructure.

The Transport Security Model provides a foundation for the following security features:

1. Confidentiality
2. Message integrity
3. Server authentication (Optionally provides client authentication)
4. Asymmetric (public-key) cryptography

The SNMP requester and SNMP services handling requests are required to have access to either a self-signed or trusted Certificate Authority (CA) for proper and successful DTLS or TLS authentication. It is common for the SNMP peers to be equipped with root certificates that represent the list of trusted CAs that an SNMP entity can use for certificate verification. You must install the digital certificate with "trusted" public keys on the SNMPv3 server and authenticity of these keys verified before granting access to the SNMP requester.

The DTLS or TLS connection uses an X.509 compliant certificate to authenticate the SNMP client and server and negotiates the encryption algorithm using a cipher suite. You can find information regarding the implementation of a cipher suite in RFC 526 "The Transport Layer Security (TLS) Protocol Version 1.2". The TLS client and server agree on an encryption algorithm and shared secret key unique to the communication session instance. Once the SNMP client/server peers have successfully authenticated, bi-directional messages transfer encrypted using the encryption algorithm and key to ensure message privacy.

The SNMP v3 services support Xerox Remote Services to retrieve printer-billing meters via the Automatic Meter Read (AMR) services, Xerox CentreWare, FreeFlow® Core services and other 3rd-party applications make requests over SNMPv3 to the FreeFlow® Print Server to retrieve jobs and printer information.

5.3 Web-UI Feature Access Control

The System Administrator has the authority to disable/enable access for each of the FreeFlow® Print Server Web-UI capabilities (e.g., Job Options, Queue Options, Job Forwarding, Accounting Options, Color Profile Options etc.) for the FreeFlow® Print Server users with an Operator or User role. You can only define Web UI feature access for these group roles, and not to individual FreeFlow® Print Server users. The System Administrator group is exempt from Access Control modification and granted full access for all operations in the FreeFlow® Print Server Web-UI.

This feature is a very important enabler for Xerox® customers that required protection of PII (Personally Identifiable Information) and/or PHI (Protected Health Information) data for compliancy of Security standards such as PCI DSS, HIPPA, Safe Harbor, etc. You can change the Access Control options for FreeFlow® Print Server Operator and User groups to a "custom" setting to meet customer security requirements and policies.

5.3.1 Job Management Access Control

Controlling the access of job operations is extremely important for customers that must protect print data (e.g., PII, PHI, etc.). You can disable operations such as preview, thumbnails, Print From File, Save Jobs, and many other Job Management features for the Operator and User role to meet specific "custom" security requirements.

The default access level to job-related operations for the User, Operator and System Administrator (SA) groups are illustrated in the below '*Job Operation Access Control Settings*' table. The System Administrator can change these access options for the FreeFlow® Print Server Operator and User groups.

Job Operation Access Control Settings Table

Job Management Option	User	Operator	SA
Background Form	Granted	Granted	Granted
Copy Job	Denied	Granted	Granted
Duplicate Job Name	Denied	Denied	Granted
Forward Job	Denied	Granted	Granted
Job Delete	Denied	Granted	Granted
Job Hold	Denied	Granted	Granted
Job Preflight	Denied	Granted	Granted
Job Preview	Denied	Granted	Granted
Job Release	Denied	Granted	Granted
Job Reset	Denied	Granted	Granted
Job Upload	Granted	Granted	Granted
Move Jobs	Denied	Granted	Granted
Print Configuration Report	Granted	Granted	Granted
Print Next	Denied	Granted	Granted
Print Now	Denied	Granted	Granted
Print Test Page	Granted	Granted	Granted
Process Job	Denied	Granted	Granted
Proof Job	Denied	Granted	Granted
Save Form Location	Granted	Granted	Granted
Save Job Location	Granted	Granted	Granted

Save/Modify Job Properties	Denied	Granted	Granted
Thumbnail	Denied	Granted	Granted
View Job Properties	Granted	Granted	Granted

5.3.2 Queue Management Access Control

Controlling the access of queue operations can be important to assist in maintaining of configuration control and prevent printing issues from incorrect queue settings set by any user with an Operator role.

The default access level to queue-related operations for the User, Operator and System Administrator (SA) groups are illustrated in the below '*Queue Operation Access Control Settings*' table.

The System Administrator can change these access options for the FreeFlow® Print Server Operator and User groups.

Queue Operation Access Control Settings Table

Queue Management Option	User	Operator	SA
Accept Jobs	Denied	Granted	Granted
Copy Queue	Denied	Granted	Granted
Create Queue	Denied	Granted	Granted
Delete Queue	Denied	Granted	Granted
Hold Jobs	Denied	Granted	Granted
Hot Folder	Denied	Granted	Granted
Job Notes	Granted	Granted	Granted
Lock Queue	Denied	Denied	Granted
Print Attributes	Granted	Granted	Granted
Print Banner	Granted	Granted	Granted
Reject Jobs	Denied	Granted	Granted
Release Jobs	Denied	Granted	Granted
Save/Modify Queue Properties	Denied	Granted	Granted
Set Default Queue	Denied	Denied	Granted
Unlock Queue	Denied	Granted	Granted
View Properties	Granted	Granted	Granted

5.3.3 Color Management Access Control

Controlling the access of color management operations can be important to assist in the maintaining of configuration control and prevent printing issues from incorrect color settings set by a user with an Operator role.

The default access level to color-related operations for the User, Operator and System Administrator (SA) groups are illustrated in the below '*Color Operation Access Control Settings*' table. The System Administrator can change these access options for the FreeFlow® Print Server Operator and User groups.

Color Operation Access Control Settings Table

Color Management Options	User	Operator	SA
Color Profiles	Settings		
Add Profile Halftone	Denied	Granted	Granted

Add Profile	Denied	Granted	Granted
Add Profile To Destination	Denied	Granted	Granted
Apply Profile Changes	Denied	Granted	Granted
Delete Profile	Denied	Granted	Granted
Export Profile	Denied	Granted	Granted
Print Attributes	Denied	Granted	Granted
Import Profile	Denied	Granted	Granted
New Profile	Denied	Denied	Granted
Print Profile List	Denied	Granted	Granted
Replace Profile	Denied	Granted	Granted
Save Profile List	Denied	Granted	Granted
Save/Modify Profile Properties	Denied	Granted	Granted
Update Profile Halftone	Denied	Denied	Granted
View Profile Properties	Granted	Granted	Granted
User TRC	**Settings**		
Copy TRC	Denied	Granted	Granted
Delete TRC	Denied	Granted	Granted
Export TRC	Denied	Granted	Granted
Import TRC	Denied	Granted	Granted
New TRC	Denied	Granted	Granted
Save/Modify TRC Properties	Denied	Granted	Granted
View TRC Properties	Granted	Granted	Granted
Spot Color	**Settings**		
Delete Spot Color	Denied	Granted	Granted
Edit Spot Color	Denied	Granted	Granted
New Spot Color	Denied	Granted	Granted
Print Sample Spot Color	Denied	Granted	Granted
Print Spot Color Swatch Book	Denied	Granted	Granted
Revert Spot Color	Denied	Denied	Granted
Device Link Profile	**Settings**		
Add Device Link Profile	Denied	Denied	Denied
Delete Device Link Profile	Denied	Denied	Denied
Device Link Print List	Denied	Denied	Denied
Device Link Properties	Denied	Denied	Denied
Device Link Save List	Denied	Denied	Denied

Note: The Baltoro® HF Press does not support Add, Edit or Delete of Color Profiles. The FreeFlow® Printer Server prevents a list of static supported Color Profiles.

5.3.4 System Level Setting Access Control

Controlling the access of System-level setting can be important to assist in the maintaining of configuration control and prevent printing issues from incorrect system level settings set by a user with an Operator role.

The default access level to system level-related operations for the User, Operator and System Administrator (SA) groups are illustrated in the below '*System Access Control*

Settings' table. The System Administrator can change these access options for the FreeFlow® Print Server Operator and User groups.

System Operation Access Control Settings Table

System Management Options	User	Operator	SA
General System Options	**Settings**		
Download License	Denied	Denied	Granted
Font Substitution	Denied	Denied	Granted
Job Scheduling	Denied	Granted	Granted
PPML	Denied	Denied	Granted
Reset Job Id	Denied	Denied	Granted
Retain PDL	Denied	Granted	Granted
Accounting Options	**Settings**		
Delete Logs	Denied	Granted	Granted
Export Logs	Denied	Granted	Granted
Print Logs	Denied	Granted	Granted
Setup Logs	Denied	Granted	Granted
Font Library Options	**Settings**		
Delete Font	Denied	Denied	Granted
Load Font	Denied	Granted	Granted
Print Font	Denied	Granted	Granted
Remote Access Options	**Settings**		
Add Access	Denied	Denied	Granted
Delete Access	Denied	Denied	Granted
Edit Access	Denied	Denied	Granted
Finishing Options	**Settings**		
Edit Finishing	Denied	Denied	Denied
Enable/Disable Finishing	Denied	Granted	Denied
Export Finishing	Denied	Denied	Denied
Delete Finishing	Denied	Denied	Denied
Device Setup	Denied	Denied	Denied
Import Finishing	Denied	Denied	Denied
New Finishing	Denied	Denied	Denied
Online/Offline	Denied	Denied	Denied
Save/Modify Finisher Properties	Denied	Denied	Denied
Revert Spot Color	Denied	Denied	Denied
View Properties	Denied	Denied	Denied
IPDS Job Profile Options	**Settings**		
IPDS Gateway	Granted	Granted	Granted
IPDS Profile Management	Granted	Granted	Granted
IPDS Pause/Continue	Granted	Granted	Granted
IPDS Profile Management Lock	Denied	Denied	Granted

Note: The Baltoro® HF Press does not support Finishing settings from the FreeFlow® Printer Server marking system.

5.3.5 System Level Setting Access Control

Controlling the access of FreeFlow® Print Server Resource Management Menu settings can be important to assist in the maintaining of configuration control and prevent printing issues from incorrect resource management settings set by a user with an Operator role.

The default access level to Resource Management Menu options for the User, Operator and System Administrator (SA) groups are illustrated in the below '*Resource Management Menu Access Control Settings*' table.

The Administrator can change these access options for the FreeFlow® Print Server Operator and User groups.

Resource Menu Operation Access Control Settings Table

Resource Management Menu Options	User	Operator	SA
Resource Menus	**Settings**		
Color Profile Tab	Granted	Granted	Granted
Finisher Tab	Granted	Granted	Granted
Font Library Tab	Granted	Granted	Granted
Gateway Tab	Denied	Denied	Granted
Queue Tab	Granted	Granted	Granted
Spot Color Tab	Granted	Granted	Granted
Stock Library Tab	Granted	Granted	Granted
User TRC Tab	Granted	Granted	Granted
Admin Menus	**Settings**		
Accounting Tab	Denied	Granted	Granted
License Tab	Denied	Denied	Granted
Network Tab	Denied	Granted	Granted
System Tab	Denied	Granted	Granted
Setup Tab	Denied	Granted	Granted
User Access Tab	Denied	Denied	Granted
IPS Manager Menus	**Settings**		
Fonts Tab	Denied	Denied	Granted
Job Profile Tab	Granted	Granted	Granted
System Configuration Tab	Granted	Granted	Granted
Trace Tab	Denied	Denied	Granted

6.0 General Security Features / Capabilities

This section includes a description of additional general Security capabilities supported by the FreeFlow® Print Server / Windows® platform. These capabilities can be used by a customer to assist with meeting their security requirements, compliancy standards and policies.

6.1 Security Profile

The FreeFlow® Print Server software provides two static system-supplied Security Profiles as options to define a Standard (default) or a High level of system Security. Only the Windows® Administrator role can change the Security Profile option. The "default" Security profile after the FreeFlow® Print Server software install is 'Standard'. The Security Profile settings are dynamic meaning it's not required to perform a restart or shutdown of the FreeFlow® Print Server / Windows® platform after changing the Security Profile level.

The ability to define a "custom" Security profile is available on the FreeFlow® Print Server / Windows® platform. You can accomplish this by copying one of the built-in profiles (Default or High) and defining the new copy with a "custom' name. The benefit of a "custom" Security profile is the ability to change security settings dynamically as the System Administrator role. The recommendation is to create a "custom" Security profile from the built-in 'High' profile and change specific settings to meet site job workflow and/or security requirements. You can access and modify Security setting options using Windows® applications and utilities if they are not currently available from the FreeFlow® Print Server Security profile.

For customers interested in the security of their print data, prevention of 'Denial of Service' attacks, or other types of computer attacks, set the Security profile to 'High'. Once the FreeFlow® Print Server Security profile is set to 'High', it disables IPP workflow, but can be enabled by setting up a "secure" IPP configuration. The IPP services support SSL authentication and encryption to make the connection and communication using these secure methods. This requires creating and installing a self-signed SSL certificate on the FreeFlow® Print Server platform.

Setting the FreeFlow® Print Server Security profile to 'High' closes many of the UDP / TCP ports that are not required and/or could pose a Security risk. You can block specific ports (e.g., SMB (445), SNMP (161), etc.) from Windows® Firewall that are still open when a "custom" security profile is defined.

6.1.1 Security Profile Default Settings

The chart below lists the features managed in each FreeFlow® Print Server system-supplied security profiles. It includes the default settings (Standard), and the settings when set to 'High'. See the profile feature options and Security profile settings below:

Security Profile Option Settings Table

Security Profile Feature	Standard (default)	High
Auto Play	Disabled	Disabled
DEP	Enabled	Enabled
DES	Disabled	Disabled
Dump File Creation	Enabled	Disabled
Enable Dead Gateway Detection	Disabled	Enabled
FIPS	Disabled	Enabled

Firewall	Enabled	Enabled
FTP	Enabled	Enabled
Keep Alive Time	120 Minutes	30 Minutes
No Name Released On Demand	Disabled	Enabled
Peripheral Devices	Enabled	Disabled
Perform Router Discovery	Enabled	Disabled
Protect Mode	Enabled	Disabled
SHA1	Enabled	Disabled
SHA2	Disabled	Enabled
Show Hidden Files	Enabled	Disabled
SSLv2	Disabled	Disabled
SSLv3	Disabled	Disabled
SMB Digital Signing	Disabled	Enabled
SMBv1	Enabled	Disabled
SMBv2	Disabled	Enabled
SNMP v1/v2	Enabled	Disabled
SNMPv3	Disabled	Enabled
Strong Password	Disabled	Enabled
Synchronize Attack Protect	Disabled	Enabled
Telnet	Disabled	Disabled
TLSv1.0	Enabled	Disabled
TLSv1.2	Disabled	Enabled
User Account Control (UAC)	Disabled	Enabled
Windows® Patch Update	Disabled	Disabled
Windows® System Restore	Enabled	Enabled

6.1.2 Security Profile Feature Descriptions

The table below include a description of all the features available for configuration setting changes managed by the Security Profiles. See the profile feature options and their descriptions below:

Security Profile Options Description Table

Security Profile Feature	Feature Description
Auto Play	The Auto Play service detects and automatically launches an appropriate application to play or display the content on DVD media when inserted in a DVD drive. The "Standard" and" High" built-in Security profiles disables the Auto Play service. A customer can enable this feature using a "custom" Security profile.
DEP	Data Execution Prevention (DEP) is a security feature that can help prevent damage to your computer from viruses and other security threats. Harmful programs can try to attack Windows® by attempting to code from system memory locations reserved for Windows® and other authorized programs. These types of attacks can harm your programs and files.

	DEP can help protect your computer by monitoring your programs to make sure that they use system memory safely. If DEP notices a program on your computer using memory incorrectly, it closes the program and notifies you.
DES	SSL Certificates need to be "signed" by a "hash algorithm". By default, the FreeFlow® Print Server software creates self-signed certificates and signs them using DES, which is a legacy encryption algorithm. Define the Security profile to 'High' to use a stronger hash encryption when creating an SSL certificate. Triple DES (3DES), officially the Triple Data Encryption Algorithm (TDEA or Triple DEA), is a symmetric-key block cipher, which applies the Data encryption Standard (DES) cipher algorithm three times to each data block.
Dump File Creation	The FreeFlow® Print Server / Windows® platform will capture crash log files when there is a critical system failure to assist with troubleshooting the root cause of the problem. It is possible for these crash logs to contain information from a customer job, so there could be some PII/PHI data. When the Security profile is set to "Standard", the crash logs will be captured and available on the FreeFlow® Print Server platform. Setting the Security profile is set to "High" disables the dumping of crash files.
Enable Dead Gateway Detection	This feature allows the FreeFlow® Print Server to communicate to an endpoint device on the network through network routes when the default gateway server is down and unavailable. When the Security profile is set to "High", the FreeFlow® Print Server platform will detect that the default router gateway is not available and use another router gateway from the local IP routing table. The FreeFlow® Print Server platform will not handle this failure detection when the Security profile is set to "Standard".
FIPS	This is a US Federal Information Processing Standard (FIPS 140) security and interoperability requirement for Federal Government networked devices. When the Security profile is set to "Standard", the encryption algorithm is weak to moderate in strength. Define a Security profile of 'High' to enable FIPS 140 compliancy and force strong encryption algorithm settings.
Firewall	The Windows® Firewall apply Security blocking and filtering settings to prevent connections and/or logins to the computer from malicious sources. Both the "Standard" and "High" Security profiles enable the Windows® firewall by default.
FTP	The "High" Security profile disables the standard FTP service by default. The "Standard" Security profile enables the standard FTP service by default. You can define the Security Profile to 'High' to block standard FTP services. Files can be transferred to the FreeFlow® Print Server platform using "secure" FTP over port 22 when standard FTP services are disabled.
Keep Alive Time	A network link is down if the keep alive request comes back with a negative response. When the "Enable Dead Gateway Detection" setting is enabled, the FreeFlow® Print Server platform will consider another network route to deliver the network request when a network link is down. This ensures that communication over the network continues even when a particular link is not available. As the feature name "keep alive" suggests, this capability ensures that the peer-to-peer communication between two internetwork host platforms keeps "alive" and can achieve successful communications. The timeout when the Security profile is set to "Standard" is 180 minutes, and for "High" is 30 minutes. Therefore, the "High" Security profile reattempts the communication at a much quicker time interval.
No Name Released On Demand	This option will enable/disable the response of the NetBIOS name defined on the FreeFlow® Print Server platform when a remote Windows® client receives a name release at the Session network layer.

	An attacker can send a spoofed "Name Release" or "Name Conflict" message to a server that supports NetBIOS (such as FreeFlow® Print Server) and force it to remove its own legitimate name, and then unable to respond to or initiate other NetBIOS requests. This will render the FreeFlow® Print Server platform unable to communicate with other NetBIOS hosts, which is a denial-of-service attack. The "High" Security profile enables this option so prevents these attacks. The "Standard" Security profile disables this option.
Peripheral Devices	Peripherals (USB/DVD and Calibration devices) are accessible when the Security profile is set to "Standard". Setting the Security profile to "High" will prevent access to peripherals.
Perform Router Discovery	The FreeFlow® Print Server / Windows® platform will automatically perform ICMP router discovery during start-up or software initialization when the Security profile is set to "Standard". An attacker can listen for these router requests and spoof the requested by representing a valid network router. The automatic router discovery is disabled when the Security profile is set to "High".
Protected Mode	The purpose of the Protected Mode option is to protect Internet Explorer by making it much more difficult to install malicious software on the FreeFlow® Print Server platform and delivers warning notifications when web pages try to run software programs. Both the "Standard" and "High" Security profiles enable this capability.
Show Hidden Files	Hidden files are visible from the file system (e.g., via Windows® Explorer) when the Security profile is set to "Standard", and the hidden files are not visible when the Security profile is set to "High".
SMB Digital Signing	Digital Signing is a Security feature in the SMB protocol that digitally signs packets communicated between an SMB client/server. By default, the FreeFlow® Print Server / Windows® software install enables SMB v2 services, disables SMB v1 and disables digital signing of SMB packets. Setting the Security Profile to "High" enables SMB Digital Signing.
SMBv1	Server Message Block (SMB) is commonly used by the FreeFlow Print Server platform to share Hot Folder directories to remote Windows clients. In some cases, it is used to access remote print jobs from a remote SMB server for print jobs and/or resources. SMBv1 was targeted by the Wannacrypt ransomware. It is recommended that SMB be disabled for security reasons.
SMBv2	Server Message Block (SMB) is commonly used by the FreeFlow Print Server platform to share Hot Folder directories to remote Windows clients. In some cases, it is used to access remote print jobs from a remote SMB server for print jobs and/or resources. The SMB v2 services are both enabled when the Security Profile is set to "High". The SMB v2 protocols offers better performance and increased security over the original SMB v1 protocol.
SNMP v1/v2	SNMP v1/v2c enables remote monitoring of printers but lacks security protections other than the "community string" password control that are not encrypted. The "Standard" Security profile enables SNMP v1/v2, and the "High" Security profile enables the "secure" SNMP v3 services.
SNMP v3	SNMP v3 adds much stronger security features such as client authentication, encryption of credentials, and encryption of bidirectional SNMP traffic. SNMPv3 ensures "secure" remote monitoring of Xerox® printers for IPv4 and IPv6 network addressing. The "Standard" Security profile enables SNMP v1/v2, and the "High" Security profile enables the "secure" SNMP v3 services.
SHA2	SSL Certificates need to be "signed" by a "hash algorithm". By default, the FreeFlow® Print Server software creates self-signed certificates and signs them using DES, which is a legacy encryption algorithm.

	DES is inherently insecure so no longer considered a viable encryption algorithm. Assigning the Security profile to 'High' will result in the FreeFlow® Print Server software using the SHA2 encryption algorithm to sign created SSL certificates, and disables DES.
SSLv2	The Secure Socket Layer (SSL) v2 is available but is a legacy cryptographic module and disabled by the FreeFlow® Print Server platform by default. The industry no longer considers SSL v2/v3 secure, so we recommend leaving it disabled. We make it available if a customer must support a legacy application that supports older certificates defined with weak encryption such as 3DES. It is desirable to use the TLS cryptographic module to ensure the highest level of Security. See the description for TLS v1.0 or v1.2 protocol settings in this table. Both the "Standard" and "High" Security profiles disable SSLv2 services, and only optionally available for a customer using a legacy Web browser and/or SSL certificate.
SSLv3	The Secure Socket Layer (SSL) v3 is available but is a legacy cryptographic module and disabled by the FreeFlow® Print Server platform by default. The industry no longer considers SSL v2/v3 secure, so we recommend leaving it disabled. We make it available if a customer must support a legacy application that supports older certificates defined with weak encryption such as 3DES. It is desirable to use the TLS cryptographic module to ensure the highest level of Security. See the description for TLS v1.0 or v1.2 protocol settings in this table. Both the "Standard" and "High" Security profiles disable SSLv3 services, and only optionally available for a customer using a legacy Web browser and/or SSL certificate.
TLSv1.0	Transport Layer Security (TLS) is the successor to its predecessor Secure Socket Layer (SSL), and is a cryptographic protocol to provide communication security over a computer network. Security compliancy standards such as PCI DSS, and newer higher strength encryption algorithms do not support TLS v1.0 in favor of the updated TLS v1.2 cryptographic protocol. Some older browsers or applications may require the TLS v1.0 protocol, which would be otherwise inoperable if this service is disabled. In these environments, use the "Standard" Security profile or create a "custom" Security profile from the built-in "High" profile, and enable TLS v1.0.
TLSv1.2	TLS v1.2 is currently the latest Transport Layer Security protocol used to provide communication security over a computer network. RFC 5246 defined TLS v1.2 in August 2008 and based on the earlier TLS 1.1 specification. This cryptographic protocol offers support for SHA2 hash encryption and AES block/stream encryption. You can enable the TLS v1.2 service by setting the Security profile to "High".
Strong Password	This Password Security feature forces the FreeFlow® Print Server platform to adhere to stricter security guidelines by defining strong password policies. The enablement of the Strong Password option forces FreeFlow® Print Server users to meet minimum complexity criteria that make it more difficult for anyone other than the owner of the user account to obtain the password and use it for malicious intentions.
Synchronize Attack Protect	This Security option prevents TCP SYN flood, which is a form of denial-of-service-attack. This is when an attacker sends successions of SYN requests to a target computer platform trying to consume system resources until that computer platform becomes unresponsive. The protection against TCP SYN flood is minimal when the Security profile is set to "Standard". When the Security profile is set to "High", the TCP connection quickly times out during a TCP SYN flood, which ensures protection for the integrity of the FreeFlow® Print Server platform and Xerox printer.
Telnet	This option enables a user to remotely log into the FreeFlow® Print Server platform over a Telnet session. The Tenet service is insecure, so should be

	restricted across networks intended to be secure. Both the "Standard" and "High" Security profiles disable this capability. A customer can enable Telnet services using a "custom" Security Profile. The FreeFlow® Print Server platform supports the SSH service as an alternative "secure" login service. There are applications that build-in an SSH client to ensure they support a "secure" login session, and there are free utilities such as "putty" that can be used to login to the FreeFlow® Print Server platform over SSH.
User Account Control (UAC)	This feature defines notification level to users when an application needs to make system changes, or Windows® settings require Administrator permission. The user will see the monitor screen light dim and must approve or deny the application request to make these changes. Only the non-Administrator user will get these notifications when the Security profile is set to "Standard". All users even the Administrator will get these notifications when the Security profile is set to "High".
Windows® Patch Update	You can use the "Windows® Patch Update" service to install patches (including Security patches) on the FreeFlow® Print Server platform directly from Microsoft®, and ensuring the earliest possible Security vulnerability mitigation. See **Section 2.0** "*Security Assurance and Assessment Process*" for information pertaining to Security patches. There are a couple of options to install patches directly from Microsoft®. One method is a manual method by selecting a "Check for Updates" option, downloading patches and then installing them. An alternative method is to schedule the patch updates so that they occur automatically. This feature disables/enables the automatic patch update method only, so even when disabled you can perform the manual patch install. We recommend the manual method for installing the patches to provide an opportunity for a FreeFlow® Print Server System Backup or Windows® Restore Point prior to the patch install. The 'Standard' and 'High' Security profiles define the "Windows® Patch Update" option as disabled by default.
Windows® System Restore	A FreeFlow® Print Server System Administrator uses a System Restore capability to restore the FreeFlow® Print Server platform to a system state captured in a System Backup. The enablement of this option will prevent restore of a System Backup. Both the "Standard" and "High" Security profiles enable this capability. A customer can disable System Resource services using a "custom" Security Profile.

6.1.3 Security Profile UDP/TCP Port Settings

The table below illustrates the state of the protocol service and ports for built-in Security profile settings.

Protocol Service/Port State Table

UDP/TCP Incoming Port State (Opened/Closed)			
Port	Protocol Service Name	Standard Security Profile	High Security Profile
21	FTP	Opened	Closed
22	SSH	Opened	Opened
23	NTP	Opened	Closed
25	SMTP	Opened	Closed
53	DNS	Opened	Closed
68	DHCP	Opened	Closed
80	HTTP	Opened	Closed
88	Kerberos	Opened	Closed

111	RPC	Opened	Closed
135	SMB Legacy	Opened	Closed
136	SMB Legacy	Opened	Closed
137	WINS NetBIOS	Opened	Closed
138	SMB NetBIOS (UDP)	Opened	Closed
139	SMB NetBIOS (TCP)	Opened	Closed
161	Net-SNMP v3	Opened	Opened
162	SNMP-Trap	Opened	Opened
201	AppleTalk Routing Maintenance	Opened	Closed
202	AppleTalk Name Binding	Opened	Closed
203	AppleTalk Unused #1	Opened	Closed
204	AppleTalk Echo	Opened	Closed
205	AppleTalk Unused #2	Opened	Closed
206	Zone Information	Opened	Closed
207	AppleTalk Unused #3	Opened	Closed
208	AppleTalk Unused #4	Opened	Closed
443	HTTPS	Opened	Opened
445	SMB (TCP)	Opened	Opened
515	LPR	Opened	Opened
631	IPP	Opened	Closed
3702	Web Discovery Services	Opened	Closed
3389	Windows® Remote Desktop	Opened	Closed
5001	IPDS	Opened	Closed
7781	JMF	Opened	Closed
8005	Tomcat Web Services	Opened	Opened
8011	Gateway Domain Interface Bridge		
8080	Proxy	Opened	Closed
8082	CWIS	Opened	Closed
8085	CWIS Secure	Opened	Opened
8090	SignalR	Opened	Opened
8172	Web Management Service	Opened	Closed
8181	JMF (Hot Folder)	Opened	Closed
9100	Socket (Raw TCP)	Opened	Opened
9400	Socket (Raw TCP)	Opened	Opened
16611	SNMP v1/v2	Opened	Closed
53202	WSD Transfer	Opened	Closed
53203	WSD Print	Opened	Closed

6.2 User Based Roles (RBAC)

The FreeFlow® Print Server / Windows® platform has two separate mechanisms to manage Users and Groups.

There is a Windows® Embedded Standard 10 management for User and Group accounts, which is a standard capability for managing Windows® users. The mechanism in Windows® referred to as User Account Control (UAC) is a Security component allowing the Windows® Administrator management of credentials for non-administrator users to access elements of the system and perform tasks.

The FreeFlow ®Print Server application also includes its own User and Group account management capabilities to assign roles for managing the FreeFlow® Print Server Web UI, configuration, print jobs and printing related operations.

See **Section 5.1** "*User & Groups Access and Roles*" for more information.

6.3 Password Security

The "built-in" FreeFlow® Print Server users define well-known passwords after the initial FreeFlow® Print Server software installation. It is recommended to change the built–in default password for the FreeFlow® Print Server User accounts (System Administrator, CSE, Operator and User) when initially installed. Change the passwords to the customer-required passwords to meet their Password Security requirements. Only the System Administrator or account owner can change a FreeFlow® Print Server user account password. These built-in user accounts are accessible by the FreeFlow® Print Server Web-UI and are separate from the Windows® built-in users. You use the FreeFlow® Print Server Web-UI from your browser to change the User passwords and the System Administrator can change password policies.

6.3.1 FreeFlow® Print Server Password Security

See a description of the parameters available to customize Password Security settings in support of ensuring Strong Password policies and FreeFlow® Print Server User account protection illustrated below:

Web-UI Password Security Settings Table

Password Security Policy	Policy Description	Allowable Range	Default Value
Password Complexity	**FreeFlow® Print Server Web-UI:** Strong Password Use the Password Security parameter to enable/disable the password complexity requirements that enforce user Strong Passwords settings.	Enable/Disable	Disable
Password History	**FreeFlow® Print Server Web-UI:** Require a series of unique password changes before reusing a password. The Password Security parameter defines the number of unique password changes that must be consecutively set for a user account before reusing a password.	Disable 1->30 Passwords	Disable 10 Passwords
Maximum Age Weeks	**FreeFlow® Print Server Web-UI:** Set to expire after a duration. Use this Password Security parameter to define the number of maximum days a user account password must exist before allowing the password to be changed. Ignore this option by enabling the "Password Never Expires" option.	Enable/Disable 1 – 25 Days	Disable 25 Days
Minimum Age Weeks	**FreeFlow® Print Server Web-UI:** Deny password changes for a minimum duration. This Password Security parameter defines the number of minimum days that a password must exist before it is changed. This setting must always be less than the Maximum Age Weeks setting.	Enable/Disable 1 – 30 Days	Disable 2 Days

Password Expiration Notification	**FreeFlow® Print Server Web-UI:** Send password expired notivication- This is a parameter defines the number of days prior to password expiration (per Maximum Age Weeks) that the user will be notified and prompted to change their password. This ensures the user is notified a specified number of days before locking out the account. 'Account Lockout Threshold' is another known name for this option.	Enable/Disable 1 – 14 Days	Disable 4 Days
Minimum Password Length	**FreeFlow® Print Server Web-UI:** Minimum Password Length This Password Security parameter defines the minimum number of required characters for the user password to be valid.	1 – 30 Characters	6 Characters
Account Lockout Duration	**FreeFlow® Print Server Web-UI:** Reset account lockout counter This Password Security parameter defines the number of minutes that a user account remains in a locked-out state before it is automatically unlocked.	1 – 99,999 Minutes	4 Minutes
# Failed Login Attempts Lockout	**FreeFlow® Print Server Web-UI:** Suspend Account After This Password Security parameter defines the number of failed login attempts before locking out the user account.	Enable/Disable 1 – 10 Failed Logins	Disable 3
Account Lockout Counter Reset	**FreeFlow® Print Server Web-UI:** Suspend Account for a minimum duration This Password Security parameter defines the amount of time that must elapse after a user account is locked-out and will be unlocked. The counter is set back to 0 after the time is elapsed, which unlocks the account.	Enable/Disable 1 – 99,999 Minutes	Disable 5 Minutes
Reset Password Allowed Times	**FreeFlow® Print Server Web-UI:** Allowed times to Reset password This Password Security parameter defines the number of times a user can reset their password in a 24-hour period.	1 - 24	10
Automatic Logoff	**FreeFlow® Print Server Web-UI:** Automatic Logoff Automatic logoff of a FreeFlow® Print Server user is possible to protect the FreeFlow® Print Server / Windows® platform if the user walks away. You can configure the Automatic Logoff option to a timeframe from 1 to 10 minutes. The FreeFlow® Print Server Web-UI will logout if the keyboard and/or mouse is inactive for the defined timeframe setting.	Enable/Disable 1 – 30 Minutes	Disable

The FreeFlow® Print Server System Administrator has the role of defining and updating Password Security options.

See the table illustrating the FreeFlow® Print Server User Group default access to FreeFlow® Print Server Security Password options below:

Password Security Option Access Table

Security Password Option	User	Operator	Administrator
Automatic Logon/Logoff	Denied	Denied	Granted
Change Own Password	Granted	Granted	Granted
Change System-Wide User Settings	Denied	Denied	Granted
Enable/Disable Strong Password	Denied	Denied	Granted
Number Failed Login Attempts Allowed	Denied	Denied	Granted
Password Expiration	Granted	Granted	Granted
Password Expiry Notification	Granted	Granted	Granted
Password History	Denied	Denied	Granted
Password Length	Denied	Denied	Granted
Password Lock/Unlock	Denied	Denied	Granted
Password Max Age Weeks	Denied	Denied	Granted

6.3.1 Windows® Password Security

In addition to the FreeFlow® Print Server built-in User accounts, there is a Windows® built-in ® Administrator account, and FreeFlow® Print Server defined Windows® users (CSE, xrxusr and sftpuser) added for FreeFlow® Print Server / Windows® system level roles. The Windows® built-in Administrator and those installed for the Windows® environment by the FreeFlow® Print Server installation is accessible by the Windows® Remote Desktop Connection application. Changing the Windows® user default password is highly recommended, and especially the Administrator and CSE given they have privileged access to the Windows® platform. Use the Windows® Administrator user to change these passwords.

Password policies can be set for the Windows® defined users depending on the needs of the customer organization policies. For example, it is possible to specify minimum password length, no blank passwords, and maximum and minimum password age. It is also possible to prevent users from reusing passwords and ensure that they use specific characters in their password, making a password complex and more difficult to crack. You can define Windows® user account policies for Password Security and Account Lockout options from the Windows® local policy settings.

See the Password Security and Account Lockout options in the table below:

Windows® Password Security Settings Table

Password Security Policy	Policy Description	Allowable Range	Default Value
Enforce Password History	**Windows® Local Security Policy:** Require a series of unique password changes before reusing a password. This security setting determines the number of unique new passwords that have to be associated with a user account before allowing reuse of an old password. The value must be between 0 and 24 passwords. This policy enables administrators to enhance security by ensuring continual reuse is not possible for old passwords. Once a password is changed, prevent changing of the same password by enabling the security policy setting Minimum Password Age, to maintain the effectiveness of the password history. See Minimum Password Age for information about the security policy Minimum Password Age.	0 -> 24 Passwords	0
Passwords must meet complexity requirements	**Windows® Local Security Policy:** Password Complexity (a.k.a., Strong Password). This security setting determines whether passwords must meet complexity requirements. Passwords must meet strong criteria after enabling this policy. The minimum password requirements are below: a. Not contain the user's account name or parts of the user's full name that exceed two consecutive characters b. Be at least six characters in length c. Contain characters from three of the following four categories: d. English uppercase characters (A through Z) e. English lowercase characters (a through z)	Enabled/Disabled	Disabled

	f. Base 10 digits (0 through 9) g. Non-alphabetic characters (for example, !, $, #, %) h. When passwords are changed or created complexity requirements are enforced.		
Maximum Password Age	**Windows® Local Security Policy:** Set to expire after a duration. This security setting determines the period of time (in days) you can used a password before the system requires the user to change it. You can set passwords to expire after a number of days between 1 and 999, or you can specify that passwords never expire by setting the number of days to 0. If the maximum password age is between 1 and 999 days, the Minimum password age must be less than the maximum password age. If the maximum password age is set to 0, the minimum password age can be any value between 0 and 998 days. **Note:** It is a security best practice to have passwords expire every 30 to 90 days, depending on your environment. This way, an attacker has a limited amount of time in which to crack a user's password and have access to your network resources.	Enabled/Disabled 0 – 999 Days	Disabled 0 Days

Minimum Password Age	**Windows® Local Security Policy:** Deny password changes for a minimum duration. This security setting determines the period of time (in days) you can use a password before the user can change it. You can set a value between 1 and 998 days, or you can allow changes immediately by setting the number of days to 0. The minimum password age must be less than the Maximum password age, unless the maximum password age is set to 0, indicating that passwords will never expire. If the maximum password age is set to 0, the minimum password age can be set to any value between 0 and 998. Configure the minimum password age to be more than 0 if you want Enforce password history to be effective. Without a minimum password age, users can cycle through passwords repeatedly until they get to an old favorite. The default setting does not follow this recommendation, so that an administrator can specify a password for a user and then require the user to change the administrator-defined password when the user logs on. If the password history is set to 0, the user does not have to choose a new password. For this reason, Enforce password history is set to 1 by default.	Enabled/Disabled 0 – 999 Days	Disabled 0 Days
Password Expiration Notification	**Windows® Local Security Policy:** Send password expired notivications This is a parameter defines the number of days prior to password expiration (per Maximum Age Weeks) that the user will be notified and prompted to change their password. This ensures the user is notified a specified number of days before locking out the account. 'Account Lockout Threshold' is another known name for this option.	Enable/Disable 1 – 14 Days	Disable 4 Days

Minimum Password Length	**Windows® Local Security Policy:** Minimum Password Length This security setting determines the least number of characters that a password for a user account may contain. You can set a value of between 1 and 14 characters, or you can establish that no password is required by setting the number of characters to 0.	0 – 14 Characters	0 Characters
Store passwords using reversible encryption	**Windows® Local Security Policy:** Strong Encryption This security setting determines whether the operating system stores passwords using reversible encryption. This policy provides support for applications that use protocols that require knowledge of the user's password for authentication purposes. Storing passwords using reversible encryption is essentially the same as storing plaintext versions of the passwords. For this reason, you should never enable this policy unless application requirements outweigh the need to protect password information. This policy is required when using Challenge-Handshake Authentication Protocol (CHAP) authentication through remote access or Internet Authentication Services (IAS). It is also required when using Digest Authentication in Internet Information Services (IIS).	Enabled/Disabled	Disabled
Account Lockout Duration	**Windows® Local Security Policy:** Suspend Account for a minimum duration This security setting determines the number of minutes a locked-out account remains locked out before automatically unlocked. The available range is from 0 minutes through 99,999 minutes. If you set the account lockout duration to 0, the system locks out the account until an administrator explicitly unlocks it. The account lockout duration must be greater than or equal to the reset time if	0 – 99,999 Minutes	0 Minutes

	you have defined the account lockout threshold,		
Account Lockout Threshold	**Windows® Local Security Policy:** Failed login attempt threshold. This security setting determines the number of failed login attempts before lockout of a user account. The administrator must unlock a locked-out account before the account is usable or wait until the lockout duration for the account has expired. You can set a value between 0 and 999 failed logon attempts. If you set the value to 0, the system will never lock out the account. Workstations or member servers can experience a failed logon attempt when locked using either CTRL+ALT+DELETE or password-protected screen savers.	0 – 999 Minutes	0 Minutes
Reset Account Lockout Counter After	**Windows® Local Security Policy:** Lockout Counter Reset Duration Automatic logoff of a FreeFlow® Print Server user is possible to protect the FreeFlow® Print Server / Windows® platform if the user walks away. You can configure the Automatic Logout option to a timeframe from 1 to 10 minutes. The FreeFlow® Print Server Web-UI will logout if the keyboard and/or mouse is inactive for the defined timeframe setting.	0 – 99,999 Minutes	0 Minutes

6.4 Firewall & Protocol Filtering

The FreeFlow® Print Server application relies on Windows® built-in network protocol filters, applications and utilities to customize Network Security. The Windows® Firewall is a network-aware application that offers incoming and outgoing protocol filtering to "customize" access of network domains, public networks, and private networks. This firewall offers advanced Security settings per a snap-in referred to as Microsoft® Management Control (MMC). This snap-in technology integrates Internet Protocol Security (IPSec) settings to provide synergy between IPSec negotiation findings and protocol blocking decisions and allows setting of Group policies. Combining protocol filtering and IPsec reduces the possibility of having conflicts between firewall rules and IPSec connection security settings.

The Windows® Firewall offers the ability to define firewall and connection rules to represent a site Security policy that apply to these different network types per a Domain, Private and Public network profile. A site Security policy defines rules that are used to analyze network traffic and determine connection access/deny settings for network servers such as the FreeFlow® Print Server / Windows® platform. Other example filtering rules defined in a firewall policy are source/destination IP addresses, IP port number, IPSec settings, users and groups in Active directory, network interface settings, services, etc. Firewall settings defined by network

Security policies protect internal networks, computers on the networks, server/client applications and data stored on servers/clients.

For example, a firewall policy defined to allow incoming traffic for a remote management application such as Remote Desktop over a connection to a private network and might block the same application access from domain or public networks. Other network Security policies can be defined with access/deny for files and printing services, peer-to-per discovery (such as the IPP protocol), and connectivity with Windows® "Connect Now" devices. A customer may want to allow network discovery from a FreeFlow® Print Server / Windows® configuration using a firewall policy defined to allow access to only a "private" network or a handful of remote computer clients. The term "private network" when talking about Windows® Firewall is a profile defining the "customer" network that is not outside of a domain or over the public Internet.

Once the FreeFlow® Print Server platform defines a restrictive Security policy, it blocks all incoming network traffic from all unsolicited networks and/or computers. You can define "custom" rules per a firewall profile that authorizes incoming network traffic to pass through from a remote domain or public network, and for specific remote computers. All outbound ports on the FreeFlow® Print Server / Windows® platform are open by default.

6.5 Anti-Virus Software Protection

Anti-virus software is not bundled with the FreeFlow® Print Server software product. Customers may choose to acquire and install Anti-virus software for "peace of mind" protection from Malware. Xerox supports a customer installing and running Xerox tested Anti-Virus software on the FreeFlow® Print Server platform. It is the responsibility of a customer to maintain applications and plug-in updates. Xerox Service is not responsible for Anti-Virus services on the FreeFlow® Print Server platform. Installing 3rd-party software on the FreeFlow® Print Server platform not tested by Xerox can potentially cause reliability and/or performance problems, and even render the FreeFlow® Print Server software inoperable. Xerox will recommend a customer remove the Anti-Virus software if it causes FreeFlow® Print Server operational problems, and Xerox will investigate the problem. The Anti-Virus products currently tested by Xerox are as follows:

Symantec™ Endpoint Protection 12.1.5
McAfee Complete Endpoint Protection Enterprise

Note: Only enable Virus and Spyware protection on the FreeFlow® Print Server platform when using these Security applications. Applying other Firewall settings using Anti-Virus applications can close ports and/or shut down services, required for job submission workflows, required interfaces between the printer engine and FreeFlow® Print Server, and can render printing inoperable.

The FreeFlow® Print Server system is a specialized Digital Front End (DFE) that provides printing services such as job processing, job management and printer management services. The most common methods for virus attacks occur by Web browsing, receiving unsolicited Email attachments, and downloading Internet files. We do not expect these types of uses for the FreeFlow® Print Server platform, and therefore limit them to minimize the risk of virus attacks. Setting the Security profile on the FreeFlow® Print Server platform to 'High' closes many TCP/UDP ports, shuts down service (Mail Services, Peripheral devices, etc.), insecure connection protocols, etc.), so inhibits, or significantly reduces the ability to receive unsolicited files. See **Section 6.1** "*Security Profile*" for more information.

6.6 Audit Logging

There are four types of FreeFlow® Print Server Audit Logs related to Security.

1 Windows® OS Audit Logging
2 FreeFlow® Print Server Web-UI Condole Logging
3 FreeFlow® Print Server Job/Printing Logs
4 FreeFlow® Print Server Accounting Logs

6.6.1 Windows® OS Audit Logging

The Windows® OS incorporates a very robust event logging service that supports an audit trail for tracking of potential Security problems, ensure user accountability, and include evidence or forensics if the FreeFlow® Print Server platform has experienced a Security breach. The Administrator can customize the types of audit events (E.g., logon/logout events, process tracking, system events, directory service access, access to objects such as files/folders, User and Group Account Management, etc.) written into the audit log, and can specify them for successful and unsuccessful events.

6.6.2 FreeFlow® Print Server Web-UI Console Logging

The FreeFlow® Print Server platform has a 'Console Logging' feature that will log all tasks performed in the FreeFlow® Print Server Web-UI including user login/logout activity. Defining users in the FreeFlow® Print Server Web-UI that are associated with the operators that manage print job using the Job Manager ensures console audit records that identify all operations the user performed when making selections on the Web-UI. For example, if an operator prints a job with sensitive user information more than one time the Console audit log will identify the person logged in as the operator, and that the job printed more than once.

6.6.3 FreeFlow® Print Server Job/Printing Logs

FreeFlow® Print Server Application modules generate log file entries in a well-defined directory as the system performs job scheduling, processing, saving, printing, etc. The FreeFlow® Print Server support engineers will need to know the Security settings to enable proper evaluation of a Security problem. Some of the log file entries are useful to track the jobs processed and printed by the FreeFlow® Print Server software.

6.6.4 FreeFlow® Print Server Accounting Logs

The accounting logs capture statistics and characteristic of each job received, processed and printed/saved on the FreeFlow® Print Server platform. Some of the useful Security audit information is Sender Name, Job Name, Account ID, etc.

6.7 Xerox® Remote Services

Xerox® Remote Services provides services to assist with the remote management of a customer fleet of Xerox printer products. Remote Services offers services such as delivering debug log data push, billing meter read to a Xerox communication server over the Internet, and download/install of security patches and patch releases and security patches. Remote Services require connectivity with a Xerox communication server over the Internet, so you must configure customer proxy information on the FreeFlow® Print Server platform to allow communication with the Xerox server.

Xerox designed the FreeFlow® Print Server platform and Xerox® Remote Services secure connectivity for customers' print workflows while employing the latest secure technologies. The FreeFlow® Print Server utilizes a secure Transport Layer Security (TLS) 1.0 connection over the standard port 443 in order to communicate externally to the remote Xerox® Communication Servers. The customer proxy information is required to be setup on the FreeFlow® Print Server platform so it can access to the Xerox® Communication Servers over the Internet.

The Xerox® Communications Servers sit behind a secure firewall and are not accessible from the Internet. The FreeFlow® Print Server within the customer environment directly initiate all communications with the remote Xerox® Communications Servers. Standard network firewall configurations on site must be defined to enable communication. To successfully access the Xerox communication server, you must define a valid URL address from the FreeFlow® Print Server platform. The FreeFlow® Print Server provides a registration key to access the services on the Xerox® Communication Servers. Registration with these Xerox servers also requires an SSL certificate for credential authentication. The Xerox® Communication Server validates the supplied credentials and accepts the FreeFlow® Print Server request. The Remote Services on the FreeFlow® Print Server platform authenticates the remote Xerox® Communications Servers and activates the service.

To push debug information or download Security patches, the FreeFlow® Print Server platform initiates a "secure" communication session with the Xerox® communication server using HTTP over the TLS 1.0 protocol (HTTPS on port 443) using an RSA 2018-bit certificate, SHA2 hash and AES 256-bit stream encryption algorithms. This connection ensures authentication of the FreeFlow® Print Server platform for the Xerox server, and sets up encrypted communication of the data. A Xerox® Communication Server does not initiate or have access to the FreeFlow® Print Server platform behind the customer firewall. The Xerox® Communication Server and FreeFlow® Print Server platform both authenticate each other before making a connection between the two end-points, and data transfer.

6.8 Hard Drive Security

A very important Security consideration is the protection of customer data written on the hard disks available in the FreeFlow® Print Server platform. This is extremely important when printing PII/PHI data on Xerox printer devices. The features offered to protect private data on the hard disk are outlined in this section.

6.8.1 Hard Disk Access Restriction

The first line of defense to protect this private data is removal of FreeFlow® Print Server user access from the hard disk. Network access to the system can be completely restricted except for access required to perform job submission workflows and remote management only. The FreeFlow® Print Server application and Windows® Desktop are not accessible until a user provides their login credentials. You must first provide Windows® credentials to launch the Windows® OS and Desktop. All non-Administrator accounts are restricted from accessing (coping/deletion) user and print data using a command prompt or the Windows®

Explorer. They are also restricted from deleting system files that could make the FreeFlow® Print Server / Windows® platform inoperable.

A user must also provide their username and password credentials to launch the FreeFlow® Print Server applications. Find information regarding FreeFlow® Print Server user roles granted by their group association in **Section 5.1** "*User & Group Access and Roles*". The Web-UI grants users access to print data in a restricted mode that is constrained by the bounds of the UI options and does not allow full access to the user/print data contained on the underlying hard disk. The FreeFlow® Print Server System Administrator can deny Operator and Users access from Web-UI features that have access to the print data by disabling those features. See **Section 5.3** "*Web-UI Feature Access Control*" for more information.

6.8.2 Hard Disk Encryption

The Windows® 10 OS has BitLocker built-in, which supports 128-bit and 256-bit encryption for active hard disks in the FreeFlow® Print Server platform. BitLocker protects hard drives from an "offline" attack, which prevents an information breach a computer or hard drive(s) with PII/PHI data. Once you enable BitLocker encryption for a hard drive an attacker does not have the ability to beach the hard disk information. There are protections (such as password or key authentication) that prevent install of the hard drive in another computer or device to harvest the data. BitLocker also protects from and attacker booting the hard disk from an alternative Operating System.

The FreeFlow® Print Server platform includes two hard disks, one that run the Windows® OS, and the other that is used for print job data, print resources, and information associated with each print job. Enablement of the Trusted Platform Module (TPM) from the BIOS on the Dell platform running the FreeFlow® Print Server / Window® 10 OS software is required to support BitLocker hard disk encryption. You can enable BitLocker encryption for the C:\ and D:\ drives allocated for the FreeFlow® Print Server software and Solaris OS after TPM enabled.

6.8.3 Data Overwrite Feature

The FreeFlow® Print Server support a configurable one-pass to twenty one-pass Data Overwrite algorithm that conforms to the National Institute of Standards and Technology (NIST) SP800-88 specification, and U.S. Department of Defense Directive 5220.22-M. A customer would use this software to destroy user or print data potentially with PII/PHI information from the FreeFlow® Print Server hard disk. This service sanitizes the data and renders it unrecoverable, and therefore unable for a criminal to breach the information.

The hard disk location categories targeted by the Data Overwrite operation to sanitize user and print data are things such as input directory PDL files, output directory Xerox proprietary files, Hot Folder print files, internal FreeFlow® Print Server job database information, Accounting data, Fonts, System files (E.g., recycle bin, temporary file locations, etc.).

6.8.4 Hard Disk Purge

When a customer returns a Xerox® printer (e.g., termination of lease), they may wish to sanitize the hard disk(s) in the FreeFlow® Print Server platform. The Windows® format utility does not sanitize a hard disk per the NIST SP800-88 specification, and U.S. Department of Defense Directive 5220.22-M. Therefore, the best approach to purge the hard disks is with a hard disk sanitizing software tool provided by a third-party vendor, and that support the U.S. DoD 5220.22-M standard along with other international data sanitizing standards.

Alternatively, a customer can use the Data Overwrite software service provided with the FreeFlow® Print Server platform with U.S. DoD 5220.22-M hard disk sanitizing compliancy to destroy the user and print data areas of the hard disk(s), and then run the Windows® format utility to format the entire hard disk. The Data Overwrite service does not sanitize the Windows® registry information, which has network information such as the IP address and domain name. The Windows® format utility deletes the network information in the registry, but not per the U.S. DoD 5220.22-M standard.

6.8.5 Removable Hard Drive Kit

Xerox offers an optional removable hard disk kit to facilitate securing or locking the hard disk. This kit provides a quick and easy removal of the FreeFlow® Print Server platform hard drives and store them in a safe or locked cabinet when not in use. For example, the U.S. Government commonly requires the customer to remove the hard drives after printing classified information and installs a second set of hard drives when printing non-classified information.

6.8.6 Hard Drive Removal and Purchase

Whenever a customer needs to dispose of or destroy the hard drives, Xerox Service provides an optional service to remove the hard drive and securely deliver them to the customer. Xerox supports this service only for customers in the USA and Canada. The customer is responsible for protection or destruction of any data on the hard disk.

6.10 PII/PHI Security Compliancy Standards

It is the customer that is responsible to ensure that any device (such as FreeFlow® Print Server / Windows® Platform and Xerox printer) introduced onto their network environment is compliant with the Security guidelines and best-practice recommendations to protect the data that they submit to the printer, and that is processed / stored on that device. For the FreeFlow® Print Server platform and Xerox® Printer products that interact for printing purposes, the customer can choose one or more workflows to submit jobs data (i.e., PDL files), and each job submission workflow has its benefits and sometimes weaknesses relative to the Security of the data being transferred over the network connection.

The other consideration relative to the security of PII/PHI data is how the customer manages jobs once they arrive onto the FreeFlow® Print Server DFE. Jobs that are immediately scheduled and printed have a “short-life” in that they are only stored on the FreeFlow® Print Server platform hard disk for the “life of the job”. On the other hand, using a workflow where jobs are submitted to a FreeFlow® Print Server queue that does not release for scheduling means that print data is on the FreeFlow® Print Server platform hard disk for and unknown timeframe that is controlled by the printer operator when they schedule jobs for printing. The FreeFlow® Print Server / Windows® software product has Security settings to protect PII/PHI data “at rest” on the FreeFlow® Print Server platform hard disk. Security Compliance regulations/guidelines frequently cited as “Must Have" by customers include:

1. Payment Card Industry Data Security Standard (PCI DSS)
2. Health Insurance Portability and Accountability Act (HIPAA)
3. Federal Information Security Management Act (FISMA)
4. Security Technical Implementation Guidelines (STIG)
5. Federal Information Processing Standards (FIPS)
6. National Institute of Standards and Technology Special Publications (NIST)

Windows® 10 provides all the security features and capabilities needed by customers to configure and manage the FreeFlow® Print Server products appropriately to comply with these regulations, guidelines, and recommendations. Given the history, and widespread use of the Windows® OS it has become very mature and quick reacting to Security risks, new capabilities

and new technologies. The number of IT professionals that support the Microsoft® Windows® Operating System is vast when compared to other vendor OS products (i.e., Apple®, Linux®, etc.), so the comfort level managing the FreeFlow® Print Server / Windows® configuration is quite high and easy for customers.

The other advantage of Windows® OS is the vast number of Security features and technologies such as those listed below:

1. Secure Software Development Lifecycle (SDLC)
2. Data Execution Prevention
3. Address Space Layout Randomization
4. Structured Exception Handler Overshoot Protection (SEHOP)
5. User Account Control (UAC)
6. DNS Security (DNSSEC)
7. Bitlocker (Logical Volume Encryption)
8. Encrypted File System (EFS)
9. Strong Encryption Algorithms
10. FIPS 140-2 encryption standard compliance
11. Customer-managed Network Firewall with automatic updates
12. Common Access Card (CAC)
13. Advanced User Authentication features (Single Sign On, Smart Card, Fingerprint reader, centralized user accounts and password support)
14. Customer-installed Security Patches/updates with minimal delay after release
15. Customer-managed monitoring and management of security features
16. IT/Support-delivered Customization of OS "footprint" (i.e., remove packages in the field
17. Applocker (Xerox® or IT can manage what software may be installed by users/operators)
18. Approved by US DOD and NSA
19. IPsec (network-level encryption)
20. Support for Enterprise - specific Virtual Private Networks (VPNs)

Xerox® designed and developed the FreeFlow® Print Server platform with Industry Standard Security Certification guidelines. This is the case even though not officially certified by any Security authority. Xerox® is aware of Security compliance standards, and we are continually enhancing and developing new Security features to close compliancy gaps. The FreeFlow® Print Server platform implements a very robust set of capabilities, settings and tools to address customer Security requirements, and remediate Security risks. Xerox® understands the importance of Security today, and pro-actively planning implementation of new customer Security requirements that meet very stringent Financial, Education and Government standards for protecting sensitive PII/PHI, and classified data. We actively work with our customer Security requirements and concerns to address them.

6.10.1 Security Technical Implementation Guide (STIG)

STIG (Security Technical Implementation Guide) is a set of Security policies, requirements, checklists, and compliance assessment methodology used by the Defense Information Systems Agency (DISA) Field Security Operations (FSO) to evaluate software applications before deployed in a DISA-supported computing environment. Government customers who must comply with Security Policies directed by the Department of Defense (DoD) may require "STIG" compliance before FreeFlow® Print Server is permitted to connect to the customer's network.

The FreeFlow® Print Server STIG toolkit incorporated in the FreeFlow® Print Server v2 / Windows® software release and later can assist government agencies to obtain DIACAP (Department of Defense Information Assurance Certification and Accreditation Process) compliancy. All STIG requirements can be categorized into 3 different groups (i.e., Cat 1, 2, & 3) with Cat 1 being the highest priority and Cat 3 the lowest priority.

You can perform STIG hardening using a STIG hardening tool delivered with the FreeFlow® Print Server software distribution. The Windows® Administrator and CSE users have the authority to run the STIG hardening on the FreeFlow® Print Server platform. The Windows® Administrator or CSE user can apply STIG hardening for the FreeFlow® Print Server / Windows® components below:

1. Windows® 10 Operating System
2. Internet Information Services (IIS 10.0)
3. Internet Explorer 11.0
4. .Net Framework 4.5.2

6.10.2 Federal Information Processing Standard (FIPS 140-2)

The United States Federal Information Processing Standard (FIPS) defines security and interoperability requirements for computer systems used by the U.S. federal government. The FIPS 140 standard defines approved cryptographic algorithms. The FIPS 140 standard also sets forth requirements for key generation and for key management. The National Institute of Standards and Technology (NIST) uses the Cryptographic Module Validation Program (CMVP) to determine if an implementation of a cryptographic algorithm is compliant with the FIPS 140 standard. A cryptographic algorithm is FIPS 140-2 compliant only after NIST has received, validated and passed the algorithm. An encryption algorithm not sanctioned by NIST is not FIPS-compliant even if the implementation produces identical data as a validated implementation of the same algorithm. See **Section 4.5.2** "*FIPS 140-2 Encryption*" for information on FIPS 140-2 and the FreeFlow® Print Server product.

Microsoft® Windows® products incorporate cryptographic modules that comply with Federal Information Processing Standard (FIPS) 140 which is a U.S. Federal government standard. This is the Security Requirement of the US Federal government for Cryptographic Modules and the Windows® OS is certified and therefore compliant with the FIPS 140-2 standard. It is important that PII/PHI data be protected while in transient over the network to the Xerox® printer, and while "at rest" on the FreeFlow® Print Server system hard disk. The software also encrypts the user passwords to ensure the integrity of authentication in that the password remain private to the authorized owner of their own access information.

The FreeFlow® Print Server / Windows® platform does support FIPS 140-2 encryption for PII/PHI data in transient over the network, data that is "at rest' on the hard disk, and for user passwords. Once the FreeFlow® Print Server Security profile is set to 'High' services will use FIPS 140-2 compliant authentication and encryption. See **Section 6.1** "*Security Profile*" for more information.

The technologies implemented are as follows:

1. Transport Layer Security (TLS)/Secure Sockets Layer (SSL) for data in transient over the network.
2. Disk Encryption: Windows® Bit Locker feature in the Windows® OS, which is FIPS 140-2 compliant.
3. FIPS 140-2 compliant cryptographic algorithms for Passwords/User Information.

FIPS 140 compliancy for these areas is extremely important for any business requiring PCI DSS and/or HIPPA compliancy when printing credit card or health related information.

6.10.3 Common Criteria Certification

The Windows® OS has achieved Common Criteria Certification (CCC) and EAL 4 certification. Microsoft® has made the efforts to acquire this certification by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) perform the CCC evaluation and an assessment of these results by National Information Assurance Partnership (NIAP). A server platform (such as FreeFlow® Print Server) must adhere to an abundant number of Security criteria, and it involves a very stringent set of Security methodologies and tests performed by an accreditation organization such as the National Information Assurance Partnership (NIAP). They also evaluate a development organization in terms of following good Security development practices and processes and expending the costs and efforts it takes to deliver a "secure" network device.

The FreeFlow® Print Server software product is an application on top of the Windows® v10 OS, and therefore a product that can partially claim CCC and EAL 4 certification. The FreeFlow® Print Server platform ensures that all FreeFlow® Print Server user interactions are restricted and mediated from the FreeFlow® Print Server Web-UI, and they have no access to the Windows® OS. The SA may interact with the OS if permitted by the security configuration. Microsoft® has built-in Windows® OS features and capabilities using the latest Security technologies, and this ensures the FreeFlow® Print Server product satisfies critical data-protection compliant requirements dictated by a customer business environment. The built-in Windows® networking capabilities ensures interactions with the customer's network and authentication/authorization mechanisms, which are CCC and EA4+ certified.

6.11 Statement of Volatility (SoV)

The main function of the Statement of Volatility is to describe the volatile and non-volatile nature of the memory on the device, and more specifically the locations, capacities and contents of volatile and non-volatile memory devices. A customer that installs a device in their facility environment and/or on their network require knowledge of whether memory can store data when the device is powered off (non-volatile) or not (volatile).

It is common policy for customers that print highly sensitive data such as Personally Identifiable Information (PII), Personal Health Information (PHI), and Government Top Secret Classified Information, to require a SoV for the printer device installed at their facility and on their network. The SoV provides these customers with the information they need to make Security decisions about how they want to handle a printer device. The devices for a Xerox® printer include the print engine, FreeFlow® Print Server, and other devices interfaces such as a Print Station Interface Platform (PSIP) for the print engine, and workflow device such as FreeFlow® Core, etc.

You can find the SoV specification for all Xerox® printer devices on the Xerox® Public Web from the "Security @ Xerox® Site" at the URL below:

https://security.business.xerox.com/en-us/

Once you navigate to the Web page for a specific printer product (E.g., iGen5® Press, Baltoro™ HF Press, etc.), the respective page will have links to Security documents such as the SoV.

Refer to the official SoV document titled "*Xerox® FreeFlow® Print Server; Statement of Volatility; Supports:* Baltoro™ HF Press*; Version 1.0*" dated April 2018 for external connections information.

6.11 Response to Known Vulnerabilities

Xerox maintains a website, https://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.

6.12 FreeFlow® Print Server Software Upgrades

FreeFlow Print Server uses the Update Manager for periodic updates including security fixes and Maintenance Releases or Supplies Planning and Releasing (SPAR Releases). Customers can reference the Xerox® FreeFlow® Print Server Software Update Manager User *guide* for further information. If no updates are available through that method customers can work with their local service team to see if a newer release is available.