May 2018

Xerox® FreeFlow® Print Server

Information Assurance Disclosure

Version: 1.1

Xerox Nuvera® 100/120 Digital Coper/Printer
Xerox Nuvera® 100/120/144 Digital Production System
Xerox Nuvera® 100/120/144/157 EA Digital Production System
Xerox Nuvera® 200/288/314 EA Perfecting Production System
Xerox Nuvera® 100/120/144 MX Digital Production System
Xerox Nuvera® 200/288 MX Perfecting Production System

Table of Contents

Revision Log

Version	Date	Description or Purpose of Changes	Author
1.0	1/26/2018	Created the initial Version 1.0 of this FreeFlow® Print Server 7.3 / Solaris® Security Information Assurance Disclosure (IAD) document for the Nuvera® printer products.	D. Roome
1.1	05/10/2018	Updated this document with enhanced information contributing to Information Assurance Disclosure, and with information related to Security component updates made for the FreeFlow Print Server product. Added new information pertaining to system audit logging.	D. Roome

Document Glossary

ADS	Microsoft Active Directory
AES	Advanced Encryption Standard
AMD	Advanced Micro Devices
AMR	Automatic Meter Read
ATO	Authority to Operate
API	Application Programming Interface
BART	Basic Auditing and Reporting Tool
BSM	Basic Security Model
CA	Certificate Authority
CBC	Cipher Block Chaining
CCC	Common Criteria Certification
CCRA	Common Criteria Recognition Arrangement
CDE	Common Desktop Environment
CFA	Call for Assistance
CHARGEN	Character Generator
CISSP	Certified Information Systems Security Professional
CIS	Center for Internet Security
CON	Certificate of Networthiness
CPU	Central Processing Unit
CSE	Customer Service Engineer
CVE	Common Vulnerability Exposure
DARPA	Defense Advanced Research Projects Agency
DES	Data Encryption Standard
DFE	Digital Front End
DFS	Distributed File System
DHCP	Dynamic Host Configuration Protocol
DIACAP	Department of Defense Information Assurance Certificate and Accreditation Process
DISA	Defense Information Systems Agency
DNS	Domain Naming Service
DoD	Department of Defense
DOS	Disk Operating System
DTLS	Datagram Transport Layer Security

DVD	Digital Versatile Disc
EAL4	Evaluation Assurance Level 4
EDE	Encrypt-Decrypt-Encrypt
FFRPS	FreeFlow® Remote Print Service
FIPS	Federal Information Processing Standard
FSO	Field Security Operations
FTP	File Transfer Protocol
GID	Group ID
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
HIPPA	Health Insurance Portability and Accountability Act,
HTTP	Hyper Transfer Protocol
HTTPS	Hyper Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IOT	Image Output Terminal
IP	Internet Protocol
IPDS	Intelligent Printer Data Stream
IPF	Internet Protocol Filter
IPP	Internet Printing Protocol
IPSec	Internet Protocol Security
IRS	Internal Revenue Service
IT	Information Technology
JASS	Jumpstart Architecture and Security Scripts
JMF	Java Media Framework
LCDS	Line Conditioned Data Stream
LPR	Line Printer
MAC	Macintosh
MAC	Message Authentication Code
MD	Message Digest
MIT	Massachusetts Institute of Technology
NetBIOS	Network Basic Input/Output System
NFS	Network File System
NIST	National Institute of Standards & Technology
NTP	Network Time Protocol

OS	Operating System
OSI	Open Systems Interconnection
PCIDSS	Payment Card Industry Data Security Standard
PDF	Portable Document Format
PDL	Page Description Language
PHI	Personal Health Information
PII	Personally Identifiable Information
PSIP	Print Station Interface Platform
RBAC	Role-Based Access Control
RFC	Request for Comment
RIP	Raster Image Processing
RPC	Remote Procedure Call
RSA	Rivest-Shamir-Adelman
SA	System Administrator
SAR	System Activity Reporter
SCAP	Security Content Automation Protocol
SCP	Secure Copy
SCSEM	Safeguard Computer Security Evaluation Matrix
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SLP	Service Location Protocol
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SoV	Statement of Volatility
SPARC	Scalable Processor Architecture
SSH	Secure Shell
SSL	Secure Socket Layer
STIG	Security Technical Implementation Guide
SUNDR	Secure Non-Trusted Data Repository
TAS	TotalNET Advanced Server
TCP	Transport Control Protocol
TLS	Transport Layer Security
TSM	Transport Security Model
UDP	User Datagram Protocol
UI	User Interface

UID	User ID
URL	Uniform Resource Locator
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
UUCP	Unix-to-Unix Copy
VIPP	Variable Data Intelligent Postscript Printware
VPN	Virtual Private Network
WINS	Windows® Internet Naming Service
XBS	Xerox Business Services
ZFS	Zettabyte File System

1.0 Security Process Introduction

This document includes Information Assurance Disclosure for the FreeFlow® Print Server to support customers with transparency to meet their Security requirements and compliances. Refer to the Information Assurance Disclosure document for the Nuvera® printer products for the same information that pertains to the print engine. This document also provides references to the FreeFlow Print Server SoV document supporting the Nuvera® printer products, which includes location, capacities and content of volatile and non-volatile memory component within the FreeFlow® Print Server X86 embedded subsystem that support the Xerox Nuvera® printer products.

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 can satisfy customer security requirements, and how the Security of FreeFlow® Print Server software is evaluated and maintained. This document also identifies security features and capabilities, which assist a print shop System Administrator and Security IT personal to manage Security and the assurance of security on the FreeFlow® Print Server platform.

1.2 Overview

Xerox® actively supports our customer's desire to achieve a level of security to meet their business needs and goals for compliancy standards, and specific security policies. Xerox allocates dedicated development and support team resources to support FreeFlow® Print Server security. We deliver Security White Papers and Configuration Guides 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 (CSE) and/or Analyst in addressing the majority of a customer's security requirements. The intention of this document is to disclose FreeFlow® Print Server security-related information to Xerox customers.

The Xerox® FreeFlow® Print Server is an application software product tightly integrated with the Solaris® OS, which has very well established highly customizable Security features. The FreeFlow® Print Server software includes many enhancements to increase security by using time tested and robust underlying Solaris® OS features and capabilities. One of the advantages of a Unix-based system over other Operating Systems is the number of tools, and API-like utilities that assist in making Security updates highly customizable. This document describes features, tools, utilities and procedures to aid in the management and maintenance of Security for the FreeFlow® Print Server platform.

Oracle® Solaris® has built-in 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 Solaris® OS was originally designed with a focus on security capabilities such as BART (baseline files, directories and attributes for later comparison and identifying changes), BSM (DoD audit logging criteria for a "C2" level security certification), SCAP scripts (Security assessment and audit), etc.

It is the responsibility of the customer to use the information contained herein this document, and from the Oracle® knowledge database to Security tighten the FreeFlow® Print Server / Solaris® 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.

Security requirements to meet Industry Security compliancy standards (E.g., IRS SCSEM, IRS Publication 1075, DISA STIG, CIS Benchmark, NIST HIPPA, PCIDSS, etc.) that exceed the scope of the FreeFlow® Print Server software service agreement are the responsibility of the customer. Xerox® is responsible for integrating Security patches for the Solaris® OS, and provide mitigation information in response to Security findings reported by a customer. Xerox® will provide Security tightening recommendations to support customer Security strategies and policies, but is not responsible for auditing Xerox printer devices. 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 Xerox® 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 & Assessment Process

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

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

2. Xerox® evaluates US-CERT alert notification of Common Exposure Vulnerabilities (CVEs) for impacts to the Solaris® OS and FreeFlow® Print Server product. The development team prioritizes patches applicable to current FreeFlow® Print Server products based on severity, system tests patches, and makes Security patch deliverables available for all FreeFlow® Print Server software releases as a post-install package. Xerox® delivers an Oracle® Security Patch Cluster on a quarterly sequence after test and acceptance completion.

3. Xerox® delivers a FreeFlow® Print Server Solaris®-based "Security White Paper and User Guide", and Security bulletins that describe a customer's options to install Oracle® Security Patch Clusters. The Security White Paper and quarterly delivered install documents include procedures to retrieve, prepare and install a Security Patch Cluster from media (E.g., DVD, USB, hard disk) or over the Internet using the Update Manager UI on the FreeFlow® Print Server platform.

4. Xerox® and the FreeFlow® Print Server development team constantly maintains existing security features, and updates Open-Source packages (E.g., OpenSSL, OpenSSH, SMB, etc.) to keep up with Security technologies.

5. Xerox® performs Security penetration-tests using Nessus and Qualys (Industry-Standard Security evaluation software applications) against each FreeFlow® Print Server major software release and patch software releases. Xerox® performs testing of network security settings using Nessus and Qualys. Xerox® remediates all security findings listed in the Nessus and Qualys audit reports by installing patches delivered by Oracle® or disabling/removing services that are not used.

6. Xerox® tests each FreeFlow® Print Server software release with Security Technical Implementation Guide (STIG) hardening before making it available to customers that require enhanced security defined by Defense Information Systems Agency (DISA). The FreeFlow® Print Server product bundles a UNIX 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 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 Graphical User Interface (GUI) 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 FreeFlow® Print Server Product 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 Solaris® 10/11 platform, so takes advantage of the robust mature Security capabilities Oracle® has implemented and maintained over the years. The Solaris® OS was implemented with a focus on the strict Security standards demanded by Federal and State Government, and need to protect Personally Identifiable Information (PII) and classified data.

The Xerox Nuvera® printer is a specialized high-volume Production printer requiring very intensive CPU bandwidth for Raster Image Processing (RIP), real-time raster image marking and Job Manager GUI operations to manage jobs. Therefore, there is no encryption of the print data on the hard disk to ensure the FreeFlow® Print Server can exceed the rated speed of the Nuvera® printer.

Unlike the purpose of a File Server to permanently storage store information, such as Personally Identifiable Information (PII), Personal Health Information (PHI), or other private information, print data on the FreeFlow® Print Server platform hard disk is "short lived". Print jobs are submitted over the network to an input spool area on the disk, scheduled for printing, processed/rendered to and output spool area on the hard disk, printed, and deleted once printing has completed. There are Security strategies that can be applied to ensure the FreeFlow® Print Server platform functions strictly as a print service only, and can restrict login, protocol connection and file access.

The Nuvera® printer is a high-volume production printer that would typically be located in a secure physical location, and accessed by very few trusted administrators/operators. The customer print data is not stored permanently like on a File Server, and Xerox offers hard disk Security options such as Data Overwrite meeting NIST and DoD compliancy standards, and Removable Hard Drive kit.

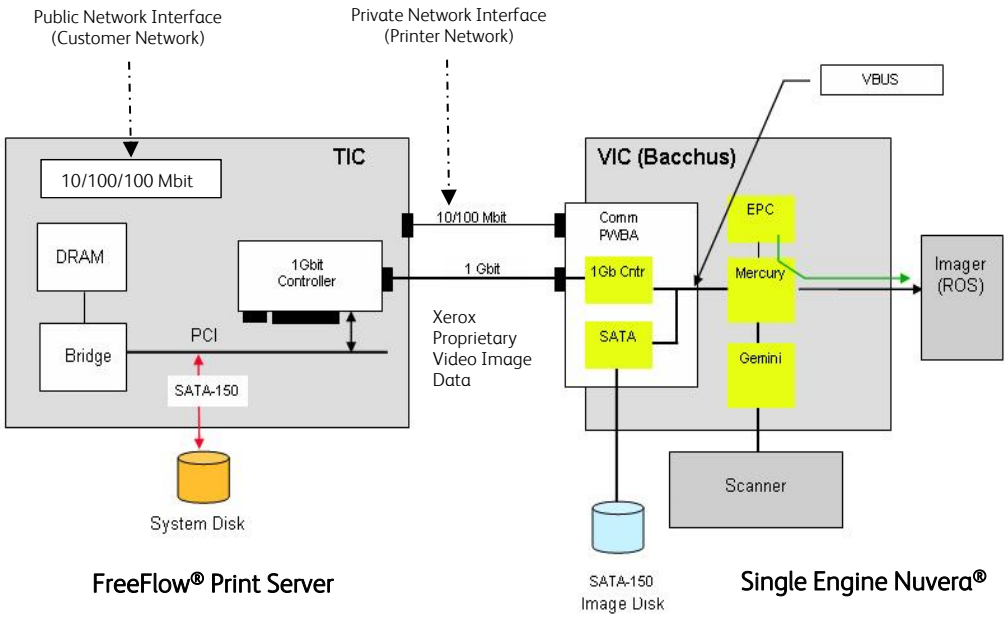
Nuvera® printer products with the FreeFlow® Print Server software is a commonly chosen product for State Government agencies (E.g., Department of Revenue, Department of Treasury, etc.) all around the US to print customer checks, and Security tightened to meet the string compliancy requirements of the IRS.

3.1 Security-relevant Subsystems

This section identifies the location, capacities and content of volatile and non-volatile memory components within the FreeFlow® Print Server X86 embedded subsystem platform that support the Xerox Nuvera® printer products.

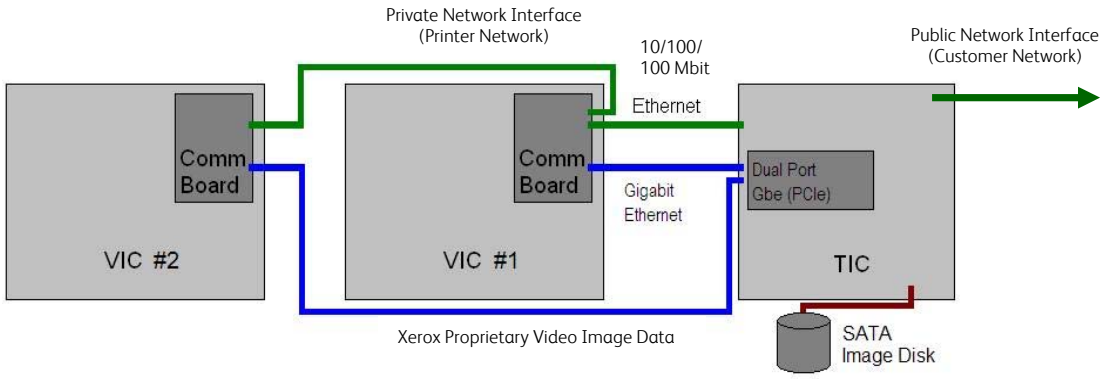
3.1.1 Physical Partitioning

See the security-relevant subsystems for the FreeFlow® Print Server / Single Engine Nuvera® illustrated below:



FreeFlow® Print Server **Single Engine Nuvera®**

See the security-relevant subsystems for the FreeFlow® Print Server / Dual Engine Nuvera® illustrated below:



Dual Engine Nuvera® **FreeFlow® Print Server**

Customer jobs arrive over the "public" network interface (a.k.a, External Network) via a network and/or print protocol services. The job data stream is spooled to the hard disk (or stream directly to the RIP via system memory buffers, scheduled for printing, decomposed/rendered to raster images, and delivered to the printer by the marker interface (See **Section 3.3** "*Marking <-> IOT Interface*").

3.1.2 FreeFlow® Print Server Purpose

The FreeFlow® Print Server platform is a specialized Digital Front End (DFE) representing a multiple Queue Spooler model printer architecture that provides printing services such as job management, job processing, transferring rasterized page images to the printer, and printer management/configuration services. It incorporates a High-Speed RIP engine and Marking process (See **Section 3.3** "*Marking <-> IOT Interface*") to support performance requirements of high-speed Xerox printers such as Nuvera®. It includes capabilities to manage printing resources (E.g., Paper Stocks, Fonts, Background Forms, VIPP Projects, Imposition Templates, etc.).

We have tightly coupled the FreeFlow® Print Server software application and the Solaris® v10/11 OS release. There is a "private" network interface connection between the back-end of the FreeFlow® Print Server subsystem to the Xerox Nuvera® printer via the Print Station Interface Platform (PSIP). The FreeFlow® Print Server delivers job pages decomposed and rendered as Xerox proprietary raster images to the Xerox Nuvera ® printer over this interface. This back-end network connectivity is isolated from the front-end network interface connected to the customer "public" network unless configured to route network information between these networks by defining a proxy configuration for the Nuvera® printer to communicate on the customer "public" network.

There are many robust Security capabilities built-into Solaris®, and customized by the FreeFlow® Print Server® application for easy configuration setup. Some features include a Security Profile, IP/RPC filter, User/Group Management, Password Security, GUI Console Audit Logging, Job Management Feature Access Control, etc. These controls in the FreeFlow® Print Server GUI use the security features of the underlying Solaris® v10/11 OS mechanisms, and configured from the GUI to make setting easy to use. The FreeFlow® Print Server offers an on-demand Data Overwrite feature to sanitize the areas of the hard disk that hold customer print jobs that may contain sensitive PII and/or private data.

There are other important Security capabilities included with the FreeFlow® Print Server / Solaris® v10/11 OS platform, which are described herein this document. Some of those capabilities are: Security Profile, STIG Hardening Package, Basic Security Model (BSM) Audit Logging, syslog Audit Logging, Password Security, Job Management User Interface (UI) Access Control, Transport Layer Security (TLS) 1.2, Cryptographic Module Secure Socket Layer (SSL) Certificate, Secure Hash Algorithm (SHA2) and Advanced Encryption Standard (AES) 256-bit Stream Encryption, etc.

Assigning the Security profile to 'High' disables insecure network services and closes User Datagram Protocol (UDP)/Transport Control Protocol (TCP) ports not required for job submission workflow. See **Section 5.1** "*Security Profile*" for more information. The FreeFlow® Print Server application also bundles a Port Management tool to manage UDP/TCP ports. A customer has the option to install and setup an SSL/TLS certificate on the FreeFlow® Print Server platform to ensure secure job submission workflows and remote management.

Customers submit documents to the FreeFlow® Print Server over a "public" network interface, which transfer to an input spool directory on the hard disk (or stream directly to the RIP via system memory buffers), 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 hold print data from deleted document files. The input spool directory is included on a hard disk location configured to be sanitized when running the Data Overwrite application included with the FreeFlow® Print Server platform.

3.1.3 Memory Components

Refer to the official SoV document titled "Xerox® FreeFlow® Print Server; Statement of Volatility; Supports Nuvera® EA/MX 100/120/144/157 and 200/288/314 IPM; Production Systems Engine" dated January 2018 for external connections information.

3.1.4 External Connections

Refer to the official SoV document titled "Xerox® FreeFlow® Print Server; Statement of Volatility; Supports Nuvera® EA/MX 100/120/144/157 and 200/288/314 IPM; Production Systems Engine" dated January 2018 for external connections information.

3.1.5 Peripheral Devices (DVD Drive and USB Ports)

Refer to the official SoV document titled "Xerox® FreeFlow® Print Server; Statement of Volatility; Supports Nuvera® EA/MX 100/120/144/157 and 200/288/314 IPM; Production Systems Engine" dated January 2018 for external connections information.

3.2 Graphical User Interface

This section describes the capabilities of the FreeFlow® Print Server GUI presented to the Administrator or Operator to facilitate printing-related tasks for the Nuvera® printer. This section does not describe the GNome Desktop or the applications available from the GNome interface. Setting the Security profile to "High" will remove all security risky application and options from the GNome Desktop GUI.

3.2.1 Graphical User Interface Purpose

The FreeFlow® Print Server GUI is a java application that runs as a local GNome Desktop application on the Solaris® v10/11 OS. This GUI is also accessible remotely from a Windows® or MAC® client using the FreeFlow® Remote Print Server application, which uses a Remote Procedure Call (RPC) based remote connection.

The main purpose of the FreeFlow® Print Server GUI is to manage print jobs that are associated with a Queue (a.k.a., Virtual Printer) and listed in a UI view (Job Manager) 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 Job Manager UI are associated with printing requirements that you can change using the job properties option from the Job Manager UI.

3.2.2 GUI Security Features & Considerations

The FreeFlow® Print Server GUI offers many Security related capabilities available to define locally or from a remote Windows® or MAC® client using the FreeFlow® Remote Print Server. The GUI Security capabilities rely on the robust set of Security capabilities that are build-into the underlying Solaris® OS. There are Security considerations related to many of the FreeFlow® Print Server GUI features.

3.2.2.1 Saved Jobs

The FreeFlow® Print Server application supports the decomposition and rendering of print jobs to an output job file written to hard disk in a well-known location in a Xerox proprietary raster image format. The FreeFlow® Print Server GUI provides an option to RIP and write saved jobs that are stored for reprint, and the ability to manage them.

The System Administrator or Operator can submit jobs using this feature. There are Security conscious customers that will not allow saved jobs as a site policy. The GUI provides an option for the System Administrator to disable the Save Job option so that Operator is restricted access from the Job Manager UI. See **Section 4.7** "*Job Manager UI Feature Access Control*" for more information. In addition, the Security Profile provides an option named "Limit Print Service Paths" to disable access to the Save Job location. See **Section 5.1** "*Security Profile*" for more information.

3.2.2.2 Background Forms Manager

The FreeFlow® Print Server application supports the decomposition and rendering of print jobs, representing static text, graphics and/or images on the pages of a print job, and storing them for reuse by jobs from a well-known directory location in a Xerox proprietary raster image format. The FreeFlow® Print Server GUI provides an option to RIP and write jobs as static Background Forms, and the ability to manage them.

The System Administrator or Operator can submit variable data jobs that can use the static saved forms. There are Security conscious customers that will not allow Background Form jobs as a site policy. The GUI provides an option for the System Administrator to disable the Background Form option so that Operator is restricted access from the Job Manager UI. See **Section 4.7** "*Job Manager UI Feature Access Control*" for more information.

3.2.2.3 Print from File

The FreeFlow® Print Server application supports a FreeFlow® Print Server GUI job submission mechanism named 'Print from File' that can be used to select a print file from the local disk or remote storage location, define printing requirement, and submit for job scheduling/printing. You can access the "Print from File" job submission mechanism remotely using the FreeFlow® Remote Print Server application from a Windows® or Macintosh® (MAC) client platform.

The Administrator or Operator can submit jobs using this feature. There are Security conscious customers that will not allow job submission of print jobs selected from the GUI as a site policy. The GUI provides an option for the System Administrator to disable this option or restrict it from the Operator. See **Section 4.7** "*Job Manager UI Feature Access Control*" for more information.

3.2.2.4 Job Forwarding

The FreeFlow® Print Server application supports a UI job submission mechanism referred to as Job Forwarding used to submit jobs from one FreeFlow® Print Server platform and Nuvera® printer to a like Nuvera® printer. A customer uses this feature when the Nuvera® printer is inoperable because of a hardware/software issue or the printer is in maintenance mode. A customer also uses Job Forwarding to achieve load balancing when the local printer is queued with multiple jobs, so can forward jobs to other remote idle printers with a minimal print job load or in an idle state.

The Job Forwarding submission UI application requires Internet Control Message Protocol (ICMP) and Line Printer (LPR) access to the receiving printer using port 515. Access to ICMP services are required on the remote printer for the Echo (a.k.a., ping) request and response service. The System Administrator or Operator can forward print jobs to a Nuvera® printer that has fewer print jobs queued or is idle. The GUI provides an option for the System Administrator to restrict this feature from the Operator. See **Section 4.7** "*Job Manager UI Feature Access Control*" for more information.

3.2.2.5 Resource Management

The FreeFlow® Print Server GUI authorizes the System Administrator to manage printer resources for things such as Fonts, Paper Stocks, Imposition Templates, Variable Data Intelligent PostScript (VIPP), Line Conditioned Data Stream (LCDS), etc. The System Administrator can grant access for resource management to the Operators.

An option is available to the System Administrator from the FreeFlow Print Server GUI to perform a Configuration Backup to a hard disk location or media (E.g., DVD or USB). This backup includes configuration settings customized by a customer, and printing resources that have been installed. The Configuration Backup can be used to restore if the software is re-installed.

3.2.2.6 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 FreeFlow® Print Server GUI provides options to manage (E.g., view, define format, print, delete) accounting records. The GUI authorizes the System Administrator to manage Job Accounting options. The Operator is restricted access to this capability unless the System Administrator grants access.

3.2.2.7 System-Level Preferences and Options

The FreeFlow® Print Server application presents many system-level options in the GUI to define and customize the configuration for onsite printing settings that meet 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 GUI authorizes the System Administrator to manage the system-level options. The Operator is restricted access to these preferences and options unless the System Administrator grants access.

3.2.2.8 User/Group Management

The FreeFlow® Printer Server offers a User/Group management capability in the GUI 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 GUI for login, and are registered Solaris® users. You use the FreeFlow® Print Server GUI to change the User passwords and some password policies. A user's group association (SA, Operator or User) defines their access (granted or restricted) to FreeFlow® Print Server® GUI features.. See **Section 4.2** "*User & Group Management*" for more detailed information.

The Users & Groups UI provides an option to enable the Strong Password option, and make Password Security option settings. The System Administrator has access to create users, manage users/groups, and make Password Security settings

3.2.2.9 Job Manager UI Feature Access Controls

The System Administrator has the authority to disable/enable access for each of the Job Management UI features (i.e., Preview, Preflight, Print from File, Job Forwarding, Accounting Information, etc.) from the FreeFlow® Print Server GUI. The System Administrator on the FreeFlow® Print Server platform manages the Operator and User group roles. The System Administrate can enable/disable Job Manager UI features for the Operator and User Group. See **Section 4.7** "*Job Manager UI Feature Access Control*" for detailed information.

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 PCIDSS, 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 the Security policies of a customer.

3.2.2.10 Password Security

The FreeFlow® Print Server platform provides a subset of the Password Security options available on the Solaris® OS platform from the Users & Groups UI in the FreeFlow® Print Server GUI. The Password Security options available are Strong Password, Minimum Password Attempt Lockout, Minimum Password Length, Password Expiry Weeks, Minimum Change Password Weeks, and Minimum Unique Sequential Passwords. There are many more Password Security options available by the Solaris® OS not included in the Users & Groups UI. The System Administrator has access to set the Security Password options. See **Section 4.5** "*Password Security*" for more detailed information.

3.2.2.11 GUI Console Logging

The FreeFlow® Print Server platform has a GUI Console Logging feature that will log all tasks performed in the FreeFlow® Print Server Web-UI including user login/logout activity. See **Section 5.3.4** "*FreeFlow® Print Server GUI Console Log*" for more information.

3.2.2.12 GUI Host Filtering

Remote hosts can be restricted from the FreeFlow® Print Server platform using the Internet Protocol (IP) Filtering capability in the FreeFlow® Print Server GUI, and filtering on "IP-based" protocols to grant/restrict remote host access for protocols such as RPC, LPR, IPP, HTTP, SMB, FTP, etc.. A System Administrator has the ability to:

1. Disable All Connections
2. Enable All Connections [Default]
3. Enable Specified Connections by:
   a) IP Address
   b) Range of IP Address'
   c) Subnet

When you select option #3, 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 platform. The FreeFlow® Print Server platform denies TCP/IP-based services/protocols from hosts not configured in the list of "trusted hosts".

An RPC filter exists for FreeFlow® Remote Print Service (FFRPS) clients, which run on remote workstations such as Windows® platforms. A FFRPS client or list of clients can be granted access to the FreeFlow® Print Server platform by adding the IP address in the RPC filter list. Once you have added one or more trusted hosts to the RPC access control list, only those hosts in the list will have FreeFlow® Print Server platform access from the FreeFlow® Remote

Print Service. When the Security profile is set to 'High", this Remote Access filter must be enabled to allow FreeFlow® Remote Print Service application access to connect and manage Xerox® printers.

3.2.2.13 Queue Lock/Unlock

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

3.2.2.14 Network/Print Protocol Access Control

The FreeFlow® Print Server application offers options to disable network and print services 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. The management of these resources can be restricted from the FreeFlow® Print Server by the System Administrator. 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 SSLv2/v3 cryptographic modules and MD5 encryption by default, and we recommend leaving them disabled. See **Section 5.1** "*Security Profile*" for more information.

3.2.2.15 Retain PDL Setting

The FreeFlow® Print Server application offers and option to retain PDL files (PDF, PostScript, IPDS, etc.) on the hard disk for the purpose of reprint after the job has already been printed. This option is disabled by default, so must be enabled if retaining of jobs is a desired feature for a customer. It is recommended to disable this option to prevent printer Operators from reprinting jobs with highly sensitive information such as information about customers, or checks. The System Administrator has access to enable or disable the Retain PDL option.

3.3 Marking <-> IOT Interface

This section describes the Marking process that runs on the FreeFlow® Print Server platform, and interfaces with the front-end of the Nuvera® printer. It does not describe the Nuvera® marking engine that marks the FreeFlow® Print Server delivered raster image pages to paper. Refer to the Information Assurance Disclosure document for the Nuvera® printer to obtain information related to marking image data to the pages.

3.3.1 Marker Interface Purpose

The marker process running on the FreeFlow® Print Server platform communicates over a private network interface to the Nuvera® printer. The main purpose of the printer network interface is for communication with the Nuvera® printer 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 Nuvera® printer is not directly accessible from the customer "public" network, and the Nuvera® printer does not have access to the customer "public" network.

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 Nuvera® printer 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.).

3.3.2 Marking Data Security

The APPE decomposer renders and rasterizes job pages input as supported PDL documents from an input spool directory that receives pint jobs from the "pubic" customer network, and write raster image pages in Xerox proprietary encoded format to an output back-end directory location. The input and output directory locations are accessible only to the Solaris® root account and FreeFlow® Print Server® System Administrator.

The life of the raster image pages are represented by the timeframe to render/rasterize and deliver the pages to the Nuvera® printer. Raster image pages from proceeding jobs overwrite hard disk sectors in the output back-end directory that hold raster images from previously printed jobs that have been deleted. In addition, the raster image pages in Xerox propriety encoded format are not readable by industry standard image applications or tools, which would make reverse engineering extremely difficult. The output back-end directory is included as a location on the hard disk that is sanitized when running the Data Overwrite application included with the FreeFlow® Print Server platform.

3.4 Software Structure & Technologies

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

3.4.1 Open-Source Components

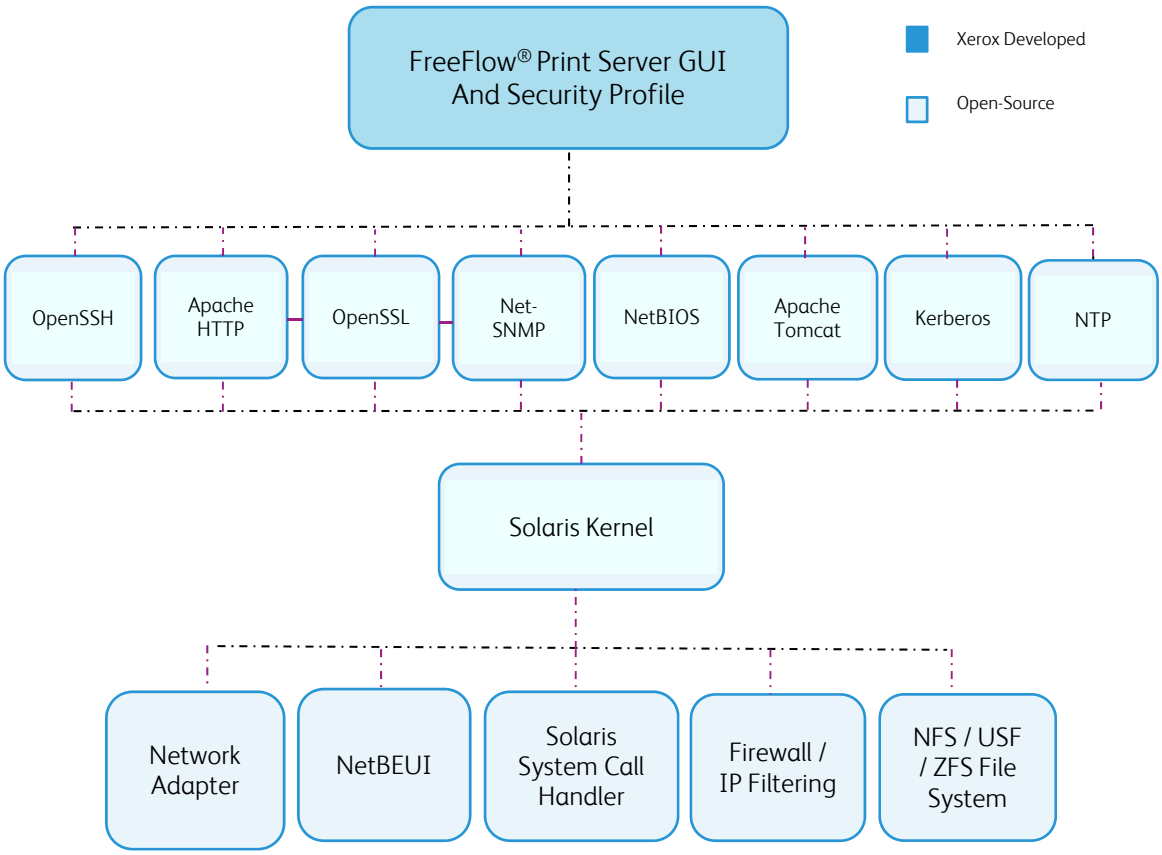
Open-source components in the connectivity layer implement high-level protocol services. The security-relevant connectivity layer components for the FreeFlow® Print Server platform supporting the Nuvera® printer are:

Open Source Package	Solaris 10	Solaris 11
Apache HTTP	2.4.33	2.4.33
Apache Tomcat	6.0.44	6.0.44
OpenSSL	1.0.2n	1.0.1t
OpenSSH	1.1.9	2.4
Samba	4.4.16	3.6.25
Net-SNMP	5.4.2.1	5.4.2.1
Kerberos	K5 Rel. 1.4.0	K5 Rel. 1.8.3
Firefox Mozilla	45.5.1	38.4.0

These Open-source components are updated in FreeFlow® Print Server software releases when necessary (E.g., maintain updated technology, Security improvements, etc.), and the version number is updated. A customer can receive Open-Source component updates in a new FreeFlow® Print Server scrape (a.k.a., clean) software install, Security Patch Cluster, or FreeFlow® Print Server software patch upgrade that is installed over-top of an existing software release. You can find bulletin notifications for new FreeFlow® Print Server Security Patch Updates from the www.xerox.com URL under "Security At Xerox®", and sign up for RSS feed services to receive posted bulletins.

3.4.2 Operating System Layers

The OS layers include the operating system, network, and physical I/O drivers. The FreeFlow® Print Server application run on the Solaris® operating system is illustrated below:

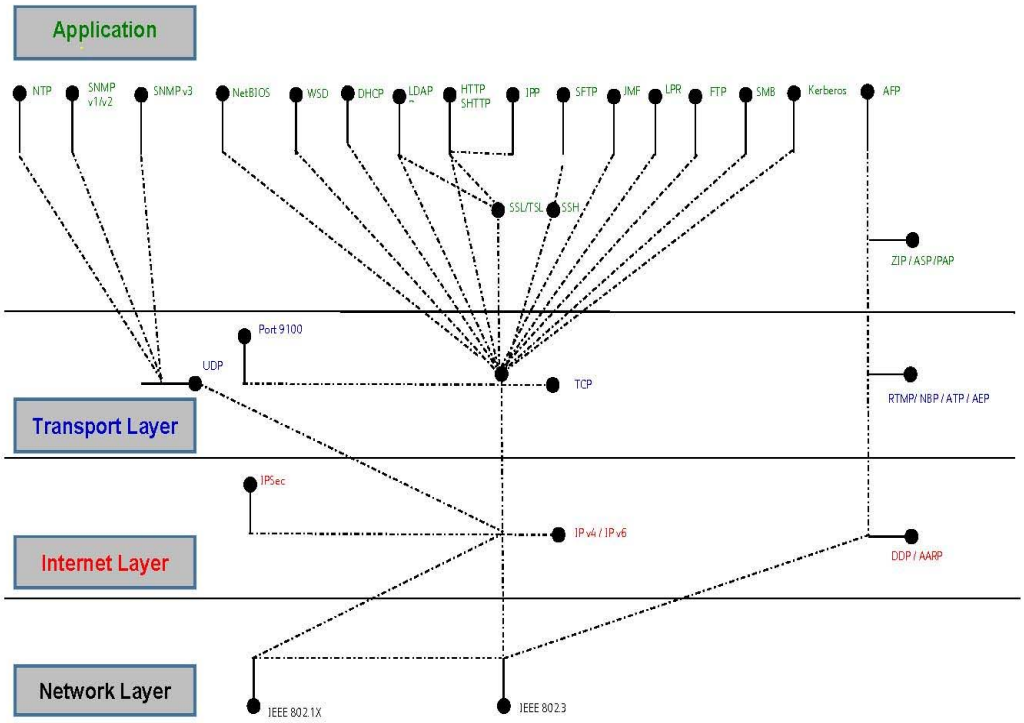


FreeFlow® Print Server Operating System Layers

Note: The above illustration of the Operating System Layers on the FreeFlow® Print Server platform only. The Print Station Interface Platform (PSIP) component of the Nuvera® printer defines its own Operating System Layers.

3.4.3 Network Protocol Layers

Refer to the diagram below that illustrates the IPv4/IPv6 protocol stacks supported by the FreeFlow® Print Server / Solaris® OS 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 Nuvera® printer defines its own OSI Layers.

3.5 Logical Network Access & Interface Security

This section describes the modules and methods on the FreeFlow® Print Server platform that supports secure connectivity and communication for job submission and job/printer status workflows. The cryptographic modules incorporated on the FreeFlow® Print Server platform are not FIPS 140-2 compliant, but do support the most current digital certificate technology, and the strongest hash and stream encryption algorithms today. The Nuvera® printer is a specialized high-volume Production printer that can operate in a secure physical location by trusted operators. The customer print data is not stored permanently like on a File Server, and Xerox offers hard disk Security options such as Data Overwrite meeting NIST and DoD compliancy standards, and Removable Hard Drive kit. See **Section 5.4** "*Hard Drive Security*" for more details.

3.5.1 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 job submission and printing 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 a remote host, the transfer of

user information and print data over a network connection. After installing the SSL certificate, any connection request from a remote client host to the FreeFlow® Print Server platform verifies the authentication and exchanged certificate information before granting access. 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 FreeFlow® Print Server / Solaris® platform to create, setup and install Triple DES-EDE-CBC and AES (supported by TLS v1.2) stream 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, 3rd-party developed Web-based job submission applications, 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 5.1** "*Security Profile*" for more information.

It is required that an SSL digital certificate be installed on the FreeFlow® Print Server / Solaris® DFE platform to enable job submission workflow with 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.

The FreeFlow® Print Service Update Manager UI uses TLS authenticate with the Xerox Download Manager service to download and install FreeFlow® Print Server software patches and Oracle® Solaris® security patches. The FreeFlow® Print Server platform initiates a "secure" communication session with the Xerox patch server using HTTP over the TSL 1.0 protocol (HTTPS on port 443) using an RSA 2018-bit certificate authentication, SHA2 hash encryption and AES 256-bit stream encryption.

The SNMPv3 services use Secure Socket Layer (SSL) services to authenticate remote SNMPv3 client requests, and securely encrypt the user passwords and job/printer information. Once the Security profile is set to "High", the SSLv3 cryptographic module is enabled to support 1024-bit/2048-bit digital certificate authentication, SHA1 hash encryption, and AES 256-bit stream encryption.

3.5.2 SSH Cryptographic Module

The FreeFlow® Print Server software supports the Secure Schell (SSH) protocol, which uses public-key cryptography to authenticate with a remote client workstation SSH request, such as Windows®, and to authenticate a user login session. The Secure Shell protocol supports Secure File Transfer Protocol (SFTP) for "secure" transfer of files between the FreeFlow® Print Server platform and a remote client workstation. A secret key is created using a key exchange algorithm between a remote client making an SSH or putty request, and the FreeFlow® Print Server platform.

The SSH service on the Solaris® OS supports configuration options that allow a customer to customize the behavior and security for remote connection sessions to the FreeFlow® Print Server platform. Restrictions can be applied, and supported Ciphers/MACs can be defined for remote connections.

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 (port 22) to transfer print jobs into a FreeFlow® Print Server Hot Folder directly. Once the job(s) securely transfer to a Hot Folder directory location associated with a queue, the Hot Folder service imports the jobs into the FreeFlow® Print Service Job Manager UI for scheduling, processing and printing.

3.5.3 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.

A customer may use an IPSec tunnel to ensure secure communications at the IP protocol layer with Xerox® printer devices. The IPSec protocol uses secure cryptography to authenticate the customer's client workstation and to create a secure encrypted tunnel to transfer data safely through un-trusted networks. In essence, it creates a Virtual Private Network (VPN) connection that protects all IP-based applications.

The IPSec protocol authenticates and encrypts each exchanged IP packet with a job submission client. The FreeFlow® Print Server platform supports 3DES block cipher encryption algorithm, which facilitates the secure exchange of print data between the remote client such as Windows®, and the FreeFlow® Print Server platform. The FreeFlow® Print Server platform supports SHA1 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.

The set of Ciphers and MACs supported are as follows:

IPSec Ciphers/MACs Table

Ciphers Supported	MACs Supported
aes	sha
aes-cbc	sha1
des	md5
des-cbc	hmac-md5
3des	hmac-sha
3des-cbc	hmac-sha1
blowfish	hmac-sha256
blowfish-cbc	hmac-sha384

IPSec services enable secure network communication for remote user login and file/print protocol workflows. Network protocols that are inherently insecure, 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 insecure FreeFlow® Print Server workflows that can benefit from IPSec are:

1. LPR
2. SMB
3. Port 9100 Printing
4. FFRPS (FreeFlow® Remote Print Service)
5. Job Forwarding
6. NFS (Network File System)
7. SMB (Windows® Folder Sharing, Print from SMB, Scan to SMB, Hot Folder, etc.)
8. NTP (Network Time Protocol)
9. DNS (Domain Naming Service)

3.5.4 UDP/TCP Port Management

Once you identify a customer production print workflow(s), you can close all UDP/TCP ports not required to support their workflows. One of the most common concerns of IT/Security managers is the existence of "open" UDP/TCP ports that are a frequent target of remote malicious attackers. Customers often use "Security scan" tools that attempt to survey, and subsequently access open UDP/TCP "ports" on the FreeFlow® Print Server platform, and will report ports as potential vulnerabilities, or for use in assessing management of ports.

Customers may request specific ports "closed" or "blocked", or for the associated services to be disabled or removed from the FreeFlow® Print Server platform. If the customer workflow does not require the use of open ports, and these are ports of concern to the customer, you can close or disable ports using a Port Management tool that is bundled with the FreeFlow® Print Server software.

There are Network/Print protocol services that are enabled and accessible on the FreeFlow® Print Server / Solaris® platform to ensure support of printing workflows (e.g., FreeFlow® Make Ready, LPR, Hot Folder, IPP, JMF/JDF, etc.). The FreeFlow® Print Server includes a Port Management tool 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 to Xerox® printer products.

See the network/print protocol services with associated port numbers, and a description below:

Print/Network Services and Ports Table

Print / Network *Protocol*	Port	Job Workflow Facilitation and Considerations
FTP	21	The File Transfer Protocol (FTP) services runs over port 21 and is an insecure protocol. The recommendation is 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 submit using "secure" FTP (SFTP). Another common workflow that uses FTP is Hot Folder. Defining the Security profile to "High" will close port 21 or you can use Port Management tool to close port 21 if the FTP transfer protocol is not used **Note:** *Some print engines (e.g., Xerox Nuvera® and DT 61xx HLC) require anonymous FTP service on the "private network" between* FreeFlow® Print Server *and the print engine. The standard FTP service includes anonymous FTP so they are one in the same, so you must not disable this service. The standard FTP service can be blocked (block port 21 using the Port Management tool) from the customer network to address Security requirements, and still allow Anonymous FTP access on the printer network interface.*
SSH	22	The Secure Shell protocol is a secure network service used to protect remote login and file transfer 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 platform over port 22. Hot Folder workflow is recommended using SFTP to ensure "secure" communication and to meet strict security requirements.
HTTP	80	This service is required to connect to the FreeFlow® Print Server / Solaris® platform from an HTTP client, such as the Internet Services Web client, Internet Print Protocol (IPP) service, JMF/JDF service, FreeFlow® Print Server Core, FF Make-ready, Remote Services, etc. The HTTP protocol an insecure protocol, so the recommendation is to close port 80 in favor of using port 443 for a "secure" HTTP (HTTPS) connection. Use the Port Management tool to close port 80 if the standard HTTP print workflow is not used.
RPC	111	The FreeFlow® Remote Print Service (FFRPS) application and Solaris®-based network services such as NIS+ also uses RPC services. Use this port to allow clients to establish a connection to the FreeFlow® Print Server platform (using OS level port management (RPC Port Mapper). The FreeFlow® Print Server responds to the RPC request with another open RPC port (randomly selected from a port number range) that it can open to access and application. RPC is an insecure network protocol that can be made secure using IPSec and/or defining an RPC filter list. Setting the Security profile to 'High' will close the Port Mapper service. There are RPC services required by some Xerox® printer product when communicating with the

		FreeFlow® Print Server platform over a "private" network interface.
SMB (Legacy)	135 136	The service for these SMB ports are older legacy versions of SMB no longer used unless a Windows® environment have old Windows® PC platforms that support these older versions. Close these ports unless there are older Windows® client platforms on the network that required SMB services. Setting the Security profile to 'High' will close these legacy SMB ports.
WINS NetBIOS	137	This service is required for Windows® Folder Browsing and resolving Windows® server name. For Example, it enables the FreeFlow® Print Server to be visible by "hostname" over a Windows® Network (i.e., NetBIOS over T CP/IP) to enable folder sharing and legacy Windows® printing. Setting the Security profile to 'High' closes this port. You can disable/disable the WINS service in the Options tab from Network Configuration UI in the FreeFlow® Print Server GUI.
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. The FreeFlow® Print Server platform supports SMB directly over TCP, and therefore recommend closing port 138.
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. The FreeFlow® Print Server platform supports SMB directly over TCP, and therefore recommend closing port 139.
Net-SNMP v3	161	This service is required for exchanging SNMP v3 messages and bi-directional communication for receiving job and printer status. The SNMP v1/v2 version services are insecure, so the recommendation is to use SNMP v3 for a "secure" SNMP connection. You can disable/enable the SNMP Gateway service in the SNMP tab Gateway Configuration UI in the FreeFlow® Print Server GUI. Use SNMP v3 for secure exchange of information.
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 Apple® MAC workstations. We recommend closing these ports unless they are required to download PostScript fonts from a MAC client to the PostScript Raster Image Processor (RIP) on the FreeFlow® Print Server platform. 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).
SVRLOC	7000	The Service Location Protocol (SLP) protocol is for browsing remote file systems and is required when using NFS and Samba services. It is recommended to closer this port using the Port Management tool.
SSL	443	The Secure Sockets Layer service provides encrypted and highly secure login authentication and file transfer services. This service can be used by client submission applications that support SSL/TLS such as SSH, "secure" HTTP, "secure" IPP Internet Services Web client, Remote Services, FreeFlow® Print Server Core, FreeFlow® Make Ready (v2.0 or newer) submission clients, etc. 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 SMB (port 445) service. The Samba services are available when the Security profile is set to "High". Samba services are insecure and susceptible to exploitation, so we recommend these services be disabled. If a customer is using Hot Folder workflow it is recommended to use SFTP to transfer jobs into the Hot Folder directory locations. Use the Port Management tool to close port 445 if the SMB print workflow is not used.
LPR	515	The lpr Gateway supports print job submissions from widely available lpr client workstations and implementations. The lpr print job submission method is the most widely used print protocol. The lpr protocol is insecure in that it does not support authentication or data encryption. However, there is no known way to exploit lpr over port 515. It is a well-defined print protocol that is not bi-directional so a one-way communication for the sole purpose of transferring print data to the printer. You can enable IPSec services to make lpr job submissions "secured". You can disable lpr from the LPD tab in the Gateways UI of the FreeFlow® Print Server GUI. Use the Port Management tool to close port 515 if the lpr print workflow is not used.
IPP	631	3rd-Party partners and Xerox® (FreeFlow® Application Suite Software such as FreeFlow® Make Ready and FreeFlow® Core) and FreeFlow® Print Server customers have implemented IPP client applications. You can disable/enable the IPP Gateway service in the IPP tab from the Gateways UI in the FreeFlow® Print Server GUI. The IPP Gateway on the FreeFlow® Print Server platform services 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. It is recommended to update the network connection over SSL (using a digital certificate) and HTTPS (port 443) to ensure a "secure" connection with user authentication and data encryption algorithms supported by TLS 1.2. Use the Port Management tool to close port 631 if the IPP print workflow is not used.
SUNDR	665	This is a service used to secure Network File System (NFS) on the FreeFlow® Print Server platform. It will secure an untrusted Data Repository (SUNDR). Setting the Security profile to 'High' disables NFS and closes this port. The NFS services are not disabled on the FreeFlow® Print Server for some Xerox printer products that required access to resource on the FreeFlow® Print Server hard disk. This access is over a "private" network between the FreeFlow® Print Server and the printer. The NFS services are disabled from the "public" customer network interface for these printer products when the Security profile is set to "High".
NFS	2049	Use this folder-sharing service when clients need to access NFS shares or access NFS mounted directories on the FreeFlow® Print Server platform. This service (nfsd) is shutdown when FreeFlow® Print Server Security defines a setting of "High". The FreeFlow® Print Server / Solaris® platform supports NFS v4, which is a "secure" connection over the network.

		The NFS services are not disabled on the FreeFlow® Print Server for some Xerox printer products that required access to resource on the FreeFlow® Print Server hard disk. This access is over a "private" network between the FreeFlow® Print Server and the printer. The NFS services are disabled from the "public" customer network interface for these printer products when the Security profile is set to "High".
NFS Lock Service	4045	When NFS is used, this service protects files from corruption. Setting the Security profile to 'High' disabled NFS services and closes this port. The NFS services are not disabled on the FreeFlow® Print Server for some Xerox printer products that required access to resource on the FreeFlow® Print Server hard disk. This access is over a "private" network between the FreeFlow® Print Server and the printer. The NFS services are disabled from the "public" customer network interface for these printer products when the Security profile is set to "High".
IPDS	5001	The IPDS workflow is a unique protocol service that uses port 5100 connecting to the FreeFlow® Print Server / Solaris® platform and transferring print data. This service and port are not disabled when the Security profile is set to "High". Use the Port Management tool to close port 6001 if the IPDS print workflow is not used.
Xsun	6000	The FreeFlow® Print Server Diagnostics service uses this port "internally" by the FreeFlow® Print Server Diagnostics software. Therefore, there is no risk of exploitation of port 6000 over the "public" customer network. Setting the Security profile to "High" closes this port.
MemXfer	7000	This is a service used by the DT HLC and HLC Publisher printers to access needed services on the FreeFlow® Print server platform over the private network interface. Therefore, there is no risk of exploitation of port 6000 over the "public" customer network. Setting the Security profile to "High" closes this port.
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. Only the FreeFlow® Print Server v9.3 software release supports JMF Gateway services natively. Port 7781 is left open when the Security profile is set to "High". Use the Port Management tool to close port 8181 if the JMF/JDF print workflow is not used.
Tomcat Web Services	8009	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. Port 8009 is left open when the Security profile is set to "High". Use the Port Management tool to close port 8009 if these print workflows are not used.
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. Port 8181 is left open when the Security profile is set to "High". Use the Port Management tool to close port 8181 if the JMF/JDF print workflow is not used.
Socket (Raw TCP/IP)	9100 9400	The Socket Gateway supports job submissions submitted over TCP/IP to a raw port service. The Xerox® Global 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. Use the Port Management tool to close these ports if the raw Socket print workflow is not used.
SNMP v1/v2	16611	This service is required for exchanging SNMP v1/v2 messages. The SNMP v1/v2 version services are insecure, so we recommend using SNMP v3 for a "secure" SNMP connection, and close port 16611. The SNMP v1/v2 protocol services are disabled when the Security profile is set to "High".

NFS related Services:	32771 -> 32779	"sometimes-rpc": NFS uses ports in this range for a variety of related remote file service capabilities. **Note:** *Some network scan tools not "Solaris® aware" may tag these ports with false identifiers, e.g., "filenet-rmi".* The NFS services are not disabled on the FreeFlow® Print Server for some Xerox printer products that required access to resource on the FreeFlow® Print Server hard disk. This access is over a "private" network between the FreeFlow® Print Server and the printer. The NFS services are disabled from the "public" customer network interface for these printer products when the Security profile is set to "High".

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 5.1.2** "*Security Profile UDP/TCP Port Settings*" for more information.

3.5.5 Network Protocol Filters

A network protocol filter is a mechanism that can be used to restrict access from remote computer hots and application network services. This section identifies filters that are available on the FreeFlow® Print Server platform

3.5.5.1 Internet Protocol (IP) Filter

Solaris® includes a Firewall capability called "IP filter" (IPF). The FreeFlow® Print Server makes use of this IPF mechanism to deliver a simple GUI-based IP Filter configuration setting, and provides a basic capability to block remote clients IP addresses not included in a filter list. A customer can configure the IPF service to only allow FreeFlow® Print Server access to remote "trusted hosts" for another level of security.

3.5.5.2 Remote Procedure Call (RPC) Filter

The Remote Procedure Call (RPC) services on the FreeFlow® Print Server platform can be restricted using an IP filter list. You can define a list of IP addresses as "trusted hosts" that can access RPC services, and this will restrict all other hosts assigned a IP address in not in the list from accessing RPC. This RPC filter mechanism is available from the RPC tab on the Security Profile in the FreeFlow® Print Server GUI.

The FreeFlow® Remote Print Server application accessed Xerox printers from a Windows® or MAC client platform using RPC services. You can define IP addresses for "trusted hosts" running FFRPS as a filter list to allow access to the FreeFlow® Print Server and Xerox printer. This is the same underlying RPC mechanism that use by the filter list from the RPC tab on the Security profile.

3.5.5.3 File Transfer Protocol (FTP) Filter

The FTP services include with the Solaris® OS include an FTP users filter. When you add FreeFlow® Print Server and Solaris® users to the filter list it restricts these users from accessing the platform using FTP. It is recommended that the FTP services are disabled and port 21 be blocked on the FreeFlow® Print Server / Solaris® platform in favor of SFTP to transfer files using port 22.

4.0 FreeFlow® Print Server System Access

This section focuses on user access to the FreeFlow® Print Server platform from the local and remote hosts. You can access the FreeFlow® Print Server GUI, and Solaris® OS locally or remotely as a registered known user when properly authenticated.

4.1 User Based Roles (RBAC)

The Solaris® OS supports a Role-Based Access Control (RBAC) to assign users to pre-defined Roles to simplify administration of feature access policies. User access to the FreeFlow® Print Server platform is achieved using the local FreeFlow® Print Server GUI. Local terminal window, or remotely over the network, and subject to RBAC access control supported by the Solaris® OS. Any local GUI, local terminal windows, or remote login is associated with a FreeFlow® Print Server user account, which is tracked by audit services. See **Section 5.3** "*Audit Logging*" for more information

You can manage Authorization of user functions via Role Based Access Control (RBAC) whereby the OS validates access based on permissions assigned to user roles, Individual users are associated to Roles via their Group association. See **Section 4.2** "*User & Group Management*" for more information.

4.2 User & Group Management

The FreeFlow® Print Server application uses the underlying Solaris® OS user and group database and Role-Based Access Control (RBAC) to create users and assign them to pre-defined roles that achieve specific access levels in the FreeFlow® Print Server GUI and the underlying OS. The Solaris® OS installs with predefined built-in system users, which are secured by access restrictions, account locks, and an assigned login shell. You can prevent login for a user account by assigning a non-functioning shell (E.g., null shell).

The FreeFlow® Print Server GUI application built-in users are System Administrator, Operator and User. You can create users for the Operator role for the purpose of managing jobs from the Job Manager UI. Any login to the FreeFlow® Print Server GUI, is associated with a FreeFlow® Print Server user account, and audit records can be captured when GUI Console logging is enabled. A local FreeFlow® Print Server user account is composed of the username and an associated group. Each user account is a member of one group and associated with only one group. The group membership of a user account defines/authorizes the FreeFlow® Print Server user for the access rights assigned to that group.

The FreeFlow® Print Server users can access the system through the local GUI, using a local Unix terminal window, or remotely over the network using applications such as FreeFlow® Remote Print Server, SFTP, SSH, and other secure remote applications. The FreeFlow® Remote Print Server (FFRPS) application can be run on a Windows® or MAC client, and is an RPC-based connection to retrieve the FreeFlow® Print Server GUI to the client application display, and have the ability to Manage jobs and printing remotely. Login audit records are captured for terminal window and remote network login when the Security profile is set to "High". See **Section 5.3** "*Audit Logging*" for more information.

A FreeFlow® Print Server GUI logon session, login session from a "local" terminal window, or remote network login, begins upon successful authentication (a.k.a., verification) of a username and credentials (a.k.a., password). The login ends by logging off which can be either user-initiated or system-initiated. Once the FreeFlow® Print Server GUI, terminal window login, or remote network login session is established, the user can interact with the system, subject to the Authorization and Access Control Policies associated with the settings of the Current Security profile, group association, and file/directory permissions. You can manage

Authorization of user functions via Role Based Access Control (RBAC) whereby the OS validates access based on permissions assigned to user roles, (individual users are associated to Roles via their Group association).

Optionally, a customer can join a Microsoft® Active Directory (ADS) service on a customer network from the FreeFlow® Print Server for the purpose of logging into the GUI with existing ADS users. The built-in FreeFlow® Print Server groups are mapped to equivalent groups defined on the ADS network, and this will ensure the appropriate level of access for an ADS user logged into the FreeFlow® Print Server GUI. The advantage using ADS users to log into the FreeFlow® Print Server GUI is they are already existing accounts on the customer Microsoft® network, and it centralizes user and group account management. This is very useful for a customer that has a large fleet of Xerox printers, and do now wish to duplicate local FreeFlow® Print Server users for each Xerox printer.

4.3 FreeFlow® Print Server Built-In Users

The FreeFlow® Print Server platform is delivered with default built-in user account as follows:

1. sa (System Administrator)
2. cse (Customer Service Engineer)
3. operator (Printer Operator)
4. user (Walk-up User)
5. xrxusr (FreeFlow® Print Server System Account)

The FreeFlow® Print Server application has a built in System Administrator (SA) account with full access to the GUI features to manage advanced tasks such as configuration settings, patch install, print resource management, making security settings, users/groups management, backup & restore, etc. The System Administrator can grant/deny access to Job Manager UI features in the FreeFlow® Print Server GUI for Operators and Users. See **Section 4.7** "*Job Manager UI Feature Access Control*".

The Customer Service Engineer (CSE) account is used by Xerox Service while on-site doing printer maintenance or solving a FreeFlow® Print Server printing issues. This account has the same access to the system as the System Administrator. A customer can lock this account and then unlock it when needed by the CSE when on-site to perform service. The Operator is a role for those that will be managing jobs and running the printer. It is recommended to create a unique Operator account for each person that will perform this role, and then lock out the build-in Operator account. The User account is for walk-up users, and has very limited access. It is recommended that this built-in account be locked unless needed by walk-up users. Large-volume production printers are not typically used as a walk-up printer so that User account can be locked for security purposes.

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 'root' does for the Solaris® OS. The FreeFlow® Print Server platform locks the xrxusr user account by default to ensure access is restricted as an internal account only. Access to the xrxusr account via FTP, NFS, telnet, SMB, etc. is disabled. We recommend against using the xrxusr account for any purpose, and against making any account changes. Do not change the User ID (UID) or Group ID (GID) of the xrxusr account. Such actions can result in the FreeFlow® Print Server platform becoming unable to perform copying, printing and scanning functions. Instead, add/create additional user accounts with the System Administrator account if unique roles are needed to access the FreeFlow® Print Server platform for any purpose. Do not use the xrxusr account for any purpose, and create a new FreeFlow® Print Server user that will meet customer user access requirements for the FreeFlow® Print Server platform.

You cannot remove the built-in user accounts from the FreeFlow® Print Server platform. However, any of these accounts may be "locked" by the SA as a means to unsure that unique customer-created accounts are used in place of these "built-in" accounts. This capability is

important to customers who require audit logs that identify who has accessed the system via the FreeFlow® Print Server GUI and identify the time a user has had access. Edit the FreeFlow® Print Server user Account Status option (i.e., Enabled/Disabled) option to lock/unlock the built-in users.

4.4 FreeFlow® Print Server Built-In Groups

The FreeFlow® Print Server platform provides three default User Groups to define user access level in the GUI. You cannot edit, delete, disable, or remove these built-in Group accounts from the system. The FreeFlow® Print Server software does not provide a way to create a new Group. Each built-in FreeFlow® Print Server user account is mapped to one of these default built-in Groups. The three Groups are:

1. System Administrators (**members:** sa and cse)
2. Operators (**member**: operator)
3. Users (**member:** user)

The "cse" is the only built-in User account that can have its Group assignment modified. All other FreeFlow® Print Server built-in User and Group assignments are fixed. We recommended that the customer IT System Administrator lock the "cse" user account until a Xerox Service Representative requires access to the FreeFlow® Print Server platform for a Service call. Edit the FreeFlow® Print Server user Account Status (i.e., Enabled/Disabled) option to lock the "cse" user.

4.5 Password Security

The "built-in" FreeFlow® Print Server users define well-known passwords after the initial FreeFlow® Print Server software install. You should change the built-in default password for the FreeFlow® Print Server user accounts (root, system administrator, operator, user, and cse) after the initial software install. The Change System Password dialog window appears when the FreeFlow® Print Server software is first installed or after running the sys-unconfig command. This prompts the installer to set new passwords for all default User Accounts. Alternatively, the user passwords can be changed from the Users & Groups UI in the FreeFlow® Print Server GUI. For security reasons, it is highly recommended to change these well-known passwords from there default settings.

Change the passwords to the customer-required passwords to meet their Password Security requirements. The GUI authorizes the System Administrator to change any FreeFlow® Print Server user account password. In addition, the owners of a FreeFlow® Print Server user account can change their own password.

The FreeFlow® Print Server platform provides additional security for users required to adhere to stricter security guidelines per strong password policies and password security settings. The Strong Password feature can be enabled/disabled from the Users and Groups UI in the FreeFlow® Print Server GUI. A "Strong Password" (a.k.a., complex password) must satisfy all of the following requirements:

1. A minimum of 8 characters in length
2. A maximum of 15 characters in length
3. Contain at least one capital letter
4. Contain at least one number
5. Contain at least one special character {!, @, #, $, %, ^, &, *}, including open and close parentheses { ( ) }, hyphen{ - }, underscore{ _ }, and period{ . }.

The Password Security options available for configuring user password settings are:

1. **Password Complexity:** Use the Password Security parameter to enable/disable the password complexity requirements that enforce user Strong Passwords settings.

2. **Maximum Age Weeks:** Use this parameter to define the number of maximum weeks a password can exist for a user before they must change it. This parameter satisfies the Government STIG requirement GEN000700. The default value is 12 weeks, and the valid range is 0 to 52 weeks.

3. **Minimum Age Weeks:** Use this parameter to define the number of minimum weeks that a password must exist before it can be changed by the user. This parameter satisfied the Government STIG requirement GEN000540. The default value is 3 weeks, and the valid range is 0 to11 weeks. This parameter must always be less than the weeks defined by Maximum Age Weeks parameter.

4. **History:** Use this parameter to define the number of password changes you can set before reusing a previously defined password. This parameter satisfies the Government STIG requirement GEN000800. The default value is 10 days, and valid range is 0 to 30 days.

5. **Password Expiry Notification:** Use this parameter to define the number of weeks prior to password expiry that a user is notified to change their password. The user login prompts to change the password once the password security reaches this threshold. The default value is 2 weeks, and the valid range is 1 to14 weeks.

   This parameter must always be less than the weeks defined by the Maximum Age Weeks parameter. The 'Threshold' value starts when the FreeFlow® Print Server user password is changed, and represents the number of weeks after the password change.

6. **Minimum Password Length:** Use this parameter to define the minimum number of characters a user must define for a user password. This parameter satisfies the Government STIG requirement 2001-T-0018. The default value is 8 characters and the range is 8 to 15 characters.

7. **Failed Login Attempts Lockout:** This Password Security parameter defines the number of failed login attempts before locking out the user account.

Password policies can be set for the FreeFlow® defined users depending on the needs of the customer organization policies.

You can define the Strong Password, Minimum Password Length and Failed Login Attempts Lockout settings from the Users & Groups UI in the FreeFlow® Print Server GUI. There are many other Password Security settings (illustrated in the below table) supported by the underlying Solaris® OS that are not available in the FreeFlow® Print Server GUI, and they can be defined using the OS facilities.

The FreeFlow® Print Server System Administrator and root user has the role of defining and updating Password Security options. See the table illustrating the FreeFlow® Print Server User Group default access to 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
Failed Login Attempts Lockout	Denied	Denied	Granted
Password History	Denied	Denied	Granted
Minimum Password Length	Denied	Denied	Granted
Password Lock/Unlock	Denied	Denied	Granted
Maximum Age Weeks	Denied	Denied	Granted
Minimum Age Weeks	Denied	Denied	Granted
Password Expiry Notification	Denied	Denied	Granted

4.6 User Authentication Methods

The FreeFlow® Pint Server platform offers server authentication protocols to verify the credentials and authenticity of communication of remote hosts, user login and print workflows. The two peers must have at least one common authentication method or connection and communication will fail.

4.6.1 SSL/TLS Authentication

Transport Layer Security (TLS v1.2) is a network security protocol that encrypts and transmits data via HTTP and IPP over a TCP/IP network. TLS is an encryption protocol layer placed between a reliable connection-oriented network layer protocol and the application protocol layer. An SSL certificates is a protocol that authenticates a remote host to enable connection security before exchanging information between a Web-based and the FreeFlow® Print Server platform.

Server certificates enable users to confirm the identity of a Web server before transmitting 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 / Solaris® platform to enable job submission workflow with SSL/TLS authentication and encryption protocols. With the certificate installed on the FreeFlow® Print Server® platform, a Windows® client can retrieve it and start using it to connect, and submit "secure" data over the network to the printer.

Customer print workflows that make use of secure SSL/TLS authentication are Internet Print Protocol (IPP), Internet Services Web Client, Remote Services and other third-party Web-based client applications. 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 Oracle® security patches over the Internet. The customer proxy information must be configured on the FreeFlow® Print Server platform to allow access outside of a customer Intranet, and to the Xerox server available on the Internet. The SNMPv3 services use SSL/TLS services to authenticate remote SNMPv3 client requests for job and printer status.

4.6.2 SSH Authentication

The SSH services use public-key cryptography to authenticate remote computers and user requesting SSH access to the FreeFlow® Print Server platform. The communication uses automatically generated public-and private key pairs to encrypt passwords, print data in transient over the network, 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 Hot Folder service on the FreeFlow® Print Service. Platform. Once the jobs securely transfer to a directory location associated with a queue, the Hot Folder service imports the jobs into the Job Manager UI for processing and print scheduling.

4.6.3 Kerberos Authentication

The FreeFlow® Print Server platform includes Kerberos Authentication services, which are an MIT technology. It is the default authentication technology that supports secure ADS connection to Windows® 2000 and higher servers, and ADS user login to the FreeFlow® Print Server GUI. You can join a Microsoft® ADS network from the FreeFlow® Print Server GUI, which will utilize Kerberos to authenticate with ADS services on a Windows® server. Once the customer domain connection is established the customer users maintained from a ADS centralized network user database can log into the FreeFlow® Print Server GUI, and adhere to the access level of a FreeFlow® Print Server / ADS mapped group, and user Password Security defined by the ADS user database.

4.6.4 IPSec Authentication

A customer may use an IPSec tunnel to ensure secure communications with Xerox® printer devices. The IPSec protocol uses cryptography to authenticate the customer's client workstation and to create a secure encrypted tunnel to transfer data safely through un-trusted networks. In essence, it creates a VPN (virtual private network) connection that protects all IP-based applications. The IPSec protocol authenticates and encrypts each exchanged IP packet with a job submission client that relies on a TCP/IP network connection.

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

IKE Authentication

The FreeFlow® Print Server platform support IKE services, which are used by IPSec to setup and establish a secure authenticated communication with a remote client such as Windows®. The authentication is performed using a pre-shared key, which is a shared secret key between the two peers.

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 4.6.3** "*Kerberos Authentication*" for more information.

Pre-shared Key

You can 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 defined and 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.

4.6.5 SNMPv3 Authentication

SNMP v3 supports a Transport Security Model (TSM) defined in RFC 5591, which specifies the Transport Layer Security (TLS), and Datagram Transport Layer Security (DTLS) protocols for enhanced Security of SNMP communication. 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 RFC specification that support this TSM in the SNMP v3 architecture are RFC 5590, RFC 5591 and RFC 5593.

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

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

MIS applications and Xerox print drivers make SNMP requests to the FreeFlow® Print Server to retrieve job and printer status, and are responded to by SNMP v3 services. The SNMP v3 service ensures the remote SNMP client is authenticated to grant the connection, and encrypts the communication. The SNMP v3 services also support Xerox Remote Services request 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.

4.7 Job Manager UI Feature 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 available in the Job Manager UI such as job and thumbnail preview, Print from File, job save, and many others for the print operators 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
Disposition (Job Print/Save)	Granted	Granted	Granted
Duplicate Job Name	Denied	Denied	Granted
Forward Job	Denied	Granted	Granted
Job Cancel	Denied	Granted	Granted
Job Delete	Denied	Granted	Granted
Job Hold	Denied	Granted	Granted
Job Preflight	Denied	Granted	Granted
Job Notes	Granted	Granted	Granted
Job Preview	Denied	Granted	Granted
Job Release	Denied	Granted	Granted
Job Reset	Denied	Granted	Granted
Job Upload	Granted	Granted	Granted
Move Job	Denied	Granted	Granted
Print Configuration Report	Granted	Granted	Granted
Print Next	Denied	Granted	Granted

Print Now	Denied	Granted	Granted
Print Attributes Report	Granted	Granted	Granted
Print Banner Page	Granted	Granted	Granted
Print Test Page	Granted	Granted	Granted
Print from File	Granted	Granted	Granted
Process Job	Denied	Granted	Granted
Proof Job	Denied	Granted	Granted
Reset Job Id	Denied	Denied	Granted
Sample Current Job	Denied	Granted	Granted
Save Form Location	Granted	Granted	Granted
Save Job Location	Granted	Granted	Granted
Save/Modify Job Properties	Denied	Granted	Granted
Thumbnail Preview	Denied	Granted	Granted
View Job Properties	Granted	Granted	Granted

5.0 General Security Features / Capabilities

This section includes a description of additional general Security capabilities and compliances supported by the FreeFlow® Print Server / Solaris® platform.

5.1 Security Profile

The FreeFlow® Print Server software provides four static system-supplied Security Profiles to allow customers flexibility in selecting the level of Security enforcement that is required. The system supplied Security profiles available are: None (Operating System only), Low, Medium and High.

Customers have a broad range of security requirements and it is impossible to satisfy all with a single collection of static "security settings". If one of system-supplied Security profiles does not suit the customer requirements, there is an option to create a "custom" Security profile. You can create a "custom" Security profile by copying one of the system-specified Security profiles to a new profile name. A newly created profile defines the default settings of the build-in Security profile copied to a custom Security profile.

The configuration settings of the "custom' Security profile can be modified to meet customer site-specific requirements. For example, the System Administrator can create a custom Security profile defined with all of the Security settings of the built-in 'High' security profile, and enable/disable specific network services as mandated by the customer site requirements. You can save multiple custom profiles with their own custom assigned name to help the System Administrator readily differentiate between them. Although the Security profile does provide the ability to significantly Security tighten FreeFlow® Print Server, it does not encompass all security settings for the FreeFlow® Print Server / Solaris® OS platform. There are many additional Security hardening settings and capabilities described throughout this document.

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', the IPP workflow is inoperable. The IPP services support SSL authentication and encryption to make the connection and communication using these secure methods. You must create and install a self-signed or Certificate Authority (CA) signed SSL certificate on the FreeFlow® Print Server platform to support authentication and "secure" IPP connectivity. The client platform can then retrieve the SSL certificate for use by the IPP client to achieve successful communication with the FreeFlow® Print Server platform.

Setting the 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., Port 21 for FTP, Port 445 for SMB, etc.) using a Port Management Tool bundled with the FreeFlow® Print Server software, or open ports if required for customer print workflow.

The chart below lists the features and services managed in each FreeFlow® Print Server system-supplied security profile. It includes the default settings for the "Low" and "High" profile, and the tab they belong to in the Security profile dialog of the FreeFlow® Print Server GUI.

Profile Tab	Profile Feature	Low Setting	High Setting
General	Apply Settings After Reboot	Disabled	Enabled
	Automatic Logon	Enabled	Disabled
	Auto Logon Username	User	User
	Logon Message	Disabled	Enabled
	Limit Print Service Paths	Enabled	Enabled
	Minimum Password Length	6	6
	Cleanup Menus	Disabled	Enabled
	UNIX Terminal Authentication	Disabled	Enabled
System	allow_host.equiv_plus	Disabled	Disabled
	bsm	Disabled	Enabled
	Executable Stacks	Disabled	Disabled
	MD5 Algorithm for SSL Certificate	Disabled	Disabled
	Remote CDE Logins	Disabled	Disabled
	Restrict DFS Tab	Enabled	Disabled
	Router	Disabled	Disabled
	Secure Sendmail	Enabled	Enabled
	Security Warning Banners	Disabled	Enabled
	SHA1 Algorithm for SSH	Enabled	Disabled
	SHA1 Algorithm for SSL Certificate	Enabled	Disabled
	SHA2 Algorithm for SSH	Disabled	Enabled
	SHA2 Algorithm for SSL Certificate	Disabled	Enabled
	SNMP v1/v2c	Enabled	Disabled
	SNMP v3	Disabled	Enabled
	TAS_httpd	Disabled	Disabled
	TLSv1.0	Enabled	Disabled
	TLSv1.2	Disabled	Enabled
INIT	S40LLC2	Disabled	Disabled
	S47ASPPPD	Disabled	Disabled
	S70UUCP	Disabled	Disabled
	S72AUTOINSTALL	Disabled	Disabled

	S73CACHEFS.DAEMON	Disabled	Disabled
	S17HCLNFS.DAEMON	Enabled	Disabled
Services	autofs	Enabled	Disabled
	chargen:dgram	Disabled	Disabled
	chargen:stream	Disabled	Disabled
	comsat	Disabled	Disabled
	daytime:dgram	Disabled	Disabled
	daytime:stream	Disabled	Disabled
	discard:dgram	Disabled	Disabled
	discard:stream	Disabled	Disabled
	echo: dgram	Disabled	Disabled
	echo: stream	Disabled	Disabled
	exec	Disabled	Disabled
	finger	Disabled	Disabled
	ftp	Enabled	Disabled
	icmp	Enabled	Disabled
	login	Disabled	Disabled
	name	Disabled	Disabled
	nfs.client	Enabled	Disabled
	nfs.server	Enabled	Disabled
	ntp	Disabled	Disabled
	rpc.cmsd	Disabled	Disabled
	rpc.rusersd	Disabled	Disabled
	rpc.rwalld	Disabled	Disabled
	rpc.sprayd	Disabled	Disabled
	rcp.ttdbserverd	Disabled	Disabled
	rquotad	Disabled	Disabled
	S81VOLMGT	Enabled	Disabled
	samba	Enabled	Enabled
	sendmail	Disabled	Disabled
	shell	Disabled	Disabled
	slp	Disabled	Disabled
	ssh	Enabled	Enabled
	talk	Disabled	Disabled
	telnet	Disabled	Disabled

	time:dgram	Disabled	Disabled
	time:stream	Disabled	Disabled
	uucp	Disabled	Disabled
	WEBEM	Disabled	Disabled
	Wins	Enabled	Enabled

5.1.1 Security Profile Feature Descriptions

The tables below include a description of all the features and services available for configuration settings managed by the Security Profile. Each table section below represents a tab for each Security profile in the FreeFlow® Print Server GUI.

General Services Tab

Apply Settings After Every Reboot	If enabled, changes to a "custom" Security profile apply after a FreeFlow® Print Server reboot. Changes to a "custom" Security profile will not persist over a FreeFlow® Print Server reboot if this feature is disabled. This might be useful if a System Administrator wants to operate the FreeFlow® Print Server platform using different Security settings for the "current" Security profile, but wants the Security settings to go back to default settings after a FreeFlow® Print Server platform reboot.
Automatic Logon	If enabled, the FreeFlow® Print Server GUI will automatically login the walkup user as the User account specified in the 'User Name' field (Automatic Login Username).
Automatic Logon Username	Once the Automatic Login option is enabled a user name must be defined that will be used to log into the FreeFlow® Print Server GUI. By default, the built-in User account is configured to login, which has the least access-level to the GUI. You can change it to any FreeFlow® Print Server user.
Logon Message	This is the Banner Message that is displayed in the login UI dialog, which is used when the Security profile is set to "High". A Security conscious customer (E.g., State / Federal State Agency) can define their own Banner Message to be displayed in the login dialog UI.
Limit Print Service Paths	This feature defines the Solaris® file paths accessible for job submission or reprint from the FreeFlow® Print Server GUI. The options that are available to grant access are: 1. CD-RW 2. File System 3. Saved Job Repository. When this feature does not define any Solaris® path, the operator will not be able to submit jobs or reprint from any job repository or resource.
Minimum Password Length	This setting denotes the minimum number of characters you can specify for a FreeFlow® Print Server user password. The range allowed to define for minimum characters is 0 to 8 characters. The range is extended to 0 –to15 when the Strong Password feature is enabled.

Cleanup Menus	This feature removes access to certain Security risky menu options from the GNome Desktop. For example, this option removes "Programs…" submenu, thus preventing the user from running optional application software packages such as Terminal Window, Terminal Console, or the Desktop File Manager.
UNIX Terminal Authentication	This feature disables the ability to access a terminal window as root. The terminal window will log in as the sisuser for diagnostic access.

System Services Tab

allow_host.equiv_plus	The /etc/hosts.equiv and /.rhosts files provide the remote authentication database for rlogin, rsh, rcp, and rexec. These files specify "trusted" remote hosts and users. This grants trusted users access to the local system without supplying a password. You can remove or modify these files to enhance security. The FreeFlow® Print Server platform is delivered without the /etc/hosts.equiv and /.rhosts files. This option is defined as disabled by default. This will ensure the '+' is absent from the hosts.equiv file to prevent trusted user access without a password.
bsm	Solaris® Basic Security Module (BSM is a Solaris® OS feature for intrusion detection, which activates extensive OS-level "audit logging". Defining the Security profile to 'High' automatically enables BSM logging. This logging feature does not support log rotation by default, which results in continual log file growth.
Executable Stacks	Some security exploits allow taking advantage of the Solaris® OS kernel executable system stack to attack the system. The 'x86" platforms are much more susceptible than the SPARC platforms to this kind of attack. You can avoid these exploits by making the system stack non-executable. When this setting is enabled entries are added to /etc/system/fp file as illustrated below: set noexec_user_stack=1 set noexec_user_stack_log=1
MD Algorithm for SSL Certificate	The MD5 algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a strong cryptographic hash function, it has been found to suffer from extensive vulnerabilities. This option is disabled for both the 'Low' and 'High' security profiles. It is only available for a customer that has legacy platforms and want to assume the risk of using this legacy hash encryption algorithm. You can only defined MD5 hash encryption by creating a custom Security profile.
Remote CDE Logins	Deny all remote access (direct/broadcast) to the X server running on FreeFlow® Print Server by installing an appropriate /etc/dt/config/Xaccess file.
Restrict DFS Tab	This option enables/disables the restriction of the "/local/var/spool/data" shared directory.

Router	This option enable/disable routing of IPv4 communication between the "public" and "negative" network interfaces. Enabling routing between these two network interfaces allows remote hosts on the "public" customer network to access the printer or PSIP workstation.
Secure Sendmail	Forces sendmail service to only support outgoing e-mail, and prevent incoming e-mail. If enabled, the sendmail service will not accept any incoming e-mail. The majority of customers that care about Security do not care about e-mail, and choose to remove sendmail packages. One use case to allow outgoing e-mail is to send notifications that warn about disk space exhausted or password expiry warnings for FreeFlow® Print Server users.
Security Warning Banners	Enable this option to ensure display of a customer Security banner warning when a user logs into the FreeFlow® Print Server platform using an application (e.g., Telnet, SSH, etc.) that uses a command shell (csh, borne, bash, etc.). The default-warning message indicates that only authorized users allowed for access to the FreeFlow® Print Server platform, logins monitored, and violators turned over to law enforcement officials. The banner message can be customized for Federal and State Government agencies.
SHA1 for SSH	SSH implements a MAC (Message Authentication Code) protocol to ensure an attacker is not able to tamper with message packets. It is a cryptographic network protocol to allow remote login and other services to communicate securely. The SHA1 hash encryption is the predecessor to the latest SHA2 version of this hash encryption algorithm. SHA1 is assigned on the FreeFlow® Print Server platform for SSH when the Security profile is set to 'Low'. Assigning the Security profile to 'High' will result in the FreeFlow® Print Server platform using SSH2 rather than SHA1. Enabling this option will ensure support for SHA1 hash encryption if required by a customer.
SHA1 SSL Certificate	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 SHA1. The SHA1 hash encryption is the predecessor to the latest SHA2 hash encryption algorithm. Hackers have compromised the legacy SHA1 algorithm 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 SHA1.
SHA2 for SSH	SSH implements a MAC (Message Authentication Code) protocol to ensure an attacker is not able to tamper with message packets. SSH2 is the strongest hash encryption algorithm today. It is encryption algorithm to allow remote login and other services to authenticate and connect securely. Assigning the Security profile to 'High' will result in the FreeFlow® Print Server platform using SSH2 rather than SHA1. Enabling this option will ensure usage of SHA2.

SHA2 SSL Certificate	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 SHA1, which is a legacy encryption algorithm. SHA1 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 SHA1.
SNMP v1/v2c	This option pertains to an SNMP service bundled with Solaris® used to handle request for job and printer status information, and Remote Service requests. The SNMP v1/v2 services are an insecure bi-directional protocol, so it is recommended they be disabled in favor of SNMP v3 if you care about information security. SNMP services on the FreeFlow® Print Server support workflows such as requests for job and printer information from Xerox print drivers, MIS applications and 3rd-party applications. Remote Services use the SNMP services for AMR and to retrieve other printing related information. The SNMP v1/v2 services are enabled and SNMP v3 services disabled when the security profile is set to "Low". Setting the security profile to and the "High" disables the SNMP v1/v2 services and enables 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. SNMP services on the FreeFlow® Print Server support workflows such as requests for job and printer information from Xerox print drivers, MIS applications and 3rd-party applications. Remote Services use the SNMP services for AMR and to retrieve other printing related information. The SNMP v1/v2 services are enabled and SNMP v3 services disabled when the security profile is set to "Low". Setting the security profile to and the "High" disables the SNMP v1/v2 services and enables SNMP v3 services.
TAS_httpd	A networking package named TotalNet is installed on the FreeFlow® Print Server platform to support legacy networking protocols such as NetWare and AppleTalk. It also includes an HTTP (Apache 1.3) service not needed for FreeFlow® Print Server print workflows. Always disable this option. Optionally, we recommend removing the TotalNet packages from the FreeFlow® Print Server platform.

TLSv1.0	Transport Layer Security (TLS) v1.0 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 PCIDSS, and newer higher strength encryption algorithms are supported by the latest TLS v1.2 cryptographic module. Some older browsers or applications may require the TLS v1.0 protocol, which would be otherwise inoperable if this service is disabled. The TLS v1.0 service is enabled when the Security profile is set to "Low", and TLS v1.2 when set to "High". Optionally, you can create a "custom" Security profile from the built-in "High" profile, and enable TLS v1.0 if these services are needed.
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. It is the latest version of TLS today. This cryptographic protocol offers support for SHA2 hash encryption and AES block/stream encryption. The TLS v1.2 service can be enabled by setting the Security profile to 'High'.

INIT Services Tab

S40LLC2	This option enables/disables a Class II logical link control driver used for interfacing between the Ethernet network interface and network software such as NetBIOS, SNA and OSI.
S47ASPPPD	Use this option to enable/disable the Asynchronous PPP link manager: This service will enable using the enable-remote-diagnostics command.
S70UUCP	This is an UUCP server. UUCP is an abbreviation of Unix-to-Unix Copy. The term generally refers to a suite of computer programs and protocols allowing remote execution of commands and transfer of files, email and net news between computers This service is needed or used by the FreeFlow® Print Server software.
S72AUTOINSTALL	Use this option to enable/disable a script executed during stub JumpStart or Auto-Install JumpStart.
S73CACHEFS.DAEMON	Use this option to enable/disable starting of Cache file system services.
S17HCLNFS.DAEMON	Manages the BWNFS (B & W Network File System) service; provides ability to read/write an MS-DOS file system. Optionally used by FreeFlow® Print Server for DOS compatibility. This service is for legacy Windows® SMB and WINS network services compatibility, see other references for SMB/Samba. This is an obsolete service.

Services Tab

autofs	Use this option to enable/disable automatic file system mounting. The auto-mount file system feature is not used by FreeFlow® Print Server software, and recommended that this option remain disabled.
chargen:dgram	Use this option to enable/disable Character Generator Protocol services. This service sends revolving pattern of ASCII characters. Sometimes used in packet debugging

	and can be used for denial of service attacks. Not used by FreeFlow® Print Server
chargen:stream	Use this option to enable/disable Character Generator Protocol services. This is the same service as chargen:dgram except a more robust and reliable TCP/IP connection service. Not used by FreeFlow® Print Server
comsat	Use this option to enable/disable Biff server services. comsat is the BSD legacy "talk" server process, which listens for reports of incoming mail and notifies users who have requested notification of mail arrivals. Not used by FreeFlow® Print Server
daytime:dgram	Use this option to enable/disable Daytime Protocol Server services. This service displays the date and time, by using UDP datagram packets. Used primarily for testing. Not used by FreeFlow® Print Server
daytime:stream	This is the same as the daytime:dgram service except that is uses a reliable TCP/IP connection service. Not used by FreeFlow® Print Server.
discard:dgram	Use this option to enable/disable the Discard Protocol Server services. This service discards everything received. Testing purposes are the primary use for these services. Not used by FreeFlow® Print Server
discard:stream	This is the same as the discard:dgram service except that is uses a reliable TCP/IP connection service. Not used by FreeFlow® Print Server.
echo:dgram	Use this option to enable/disable the Echo Protocol server services. This service will echo back any character sent to it. Sometimes used in packet debugging and can be used for denial of service attacks. Uses UDP/IP. Not used by FreeFlow® Print Server.
echo:stream	This is the same as the echo:dgram service except that is uses a reliable TCP/IP connection service. Not used by FreeFlow® Print Server.
exec	Use this option to enable/disable Remote Execution Server services. The rexec command uses this service. This is a Security risk service given passwords and subsequent sessions are in clear text (not encrypted). Not used by FreeFlow® Print Server.
finger	Use this option to enable/disable Remote User Information Server services. This service displays information about local and remote users. Reveals information about system users. Not used by FreeFlow® Print Server.
ftp	Use this option to enable/disable the FTP Server services. Client FTP services remain enabled so that files can be transferred to remote workstations from the FreeFlow® Print Server platform. It is recommended to disable standard FTP in favor of SFTP for "secure" file transfer. **Note:** *Do not disable FTP services for the Xerox Nuvera® or DT HLC printer products. They require anonymous FTP communication between the* FreeFlow® Print Server *platform and printer engine software over a "private" network interface for proper operation. You can disable the FTP service over the "public" network interface by closing port 21.*
icmp	Internet Control Message Protocol (ICMP) is an extension of the Internet Protocol (IP). ICMP supports packets containing error, control, and informational messages. Disable this service unless using the Job

	Forwarding capability to forward print jobs from one Xerox to another. This service is required to support the Job Forwarding feature on the FreeFlow® Print Server platform, which submits one or more jobs from one printer to another like-printer. The only service of ICMP required by Job Forwarding is echo (a.k.a., ping).
login	Use this option to enable/disable the Remote Login Server service. The rlogin command uses this service. This is a Security risk given it uses the .rhosts file for authentication, so passwords and subsequent sessions are in clear text (not encrypted).
name	Use this option to enable/disable DARPA Trivial Name Server services. This service name is in.tnamed and supports the DARPA Name Server Protocol. Seldom. Not used by FreeFlow® Print Server.
nfs.client	Use this option to enable/disable client-side NFS Server service. This service provides the ability to access remote NFS shares from the FreeFlow® Print Server platform.
nfs.server	Use this option to enable/disable server-side ide NFS Server services. This service provides the ability to share file device and hard disk resources from the FreeFlow® Print Server platform.
ntp	Use this option to enable/disable the Network Time Protocol service. This service automatically synchronizes the platform's "clock" with network time service from an NTP server. Transmits multicast packets to search for NTP servers, if not configured with the server's unicast address. Highly secure conscience customers require NTP services to ensure accurate time associate with audit log information.
rpc.rusersd	Use this option to enable/disable Network Username Server services. This service generates intruder information about accounts. Not used by FreeFlow® Print Server.
rpc.rwalld	Use this option to enable/disable Network rwall Server services. This service handles rwall command requests. You can use this service for spoofing attacks. Not used by FreeFlow® Print Server.
rpc.sprayd	Use this option to enable/disable Spray Server service. This service captures the packets sent by the spray command. You can use the service in denial of service attacks. Not used by FreeFlow® Print Server
rcp.ttdbserverd	Use this option to enable/disable the RPC-based ToolTalk Database Server services. Not used by FreeFlow® Print Server.
rquotad	Use this option to enable/disable the Remote Quota server service. The quota command uses this service to display user quotas for remote file systems. Not used by FreeFlow® Print Server
S81VOLMGT	Use this service to enable/disable peripheral devices (USB ports and CD/DVD drives). Optionally required by customer system administrators, operators, or Xerox Customer Service Engineers (CSE). You can disable the volfs service and then enable it using the svcadm command only when there is a need to access the DVD drive or USB port.

samba	Use this option to enable/disable Windows® File Sharing (aka SMB) and WINS services. **NOTE:** *Since Samba emulates a family of very old Windows® Folder Sharing and WINS protocols, and is inherently insecure. Optionally required by customer network administrators, system administrators, operators, and/or Xerox Service Engineers (CSE). Alternatively, you can use "secure" FTP for Hot Folder workflow, and disable/remove Samba.*
sendmail	Use this option to enable/disable Mail services. Optionally, a customer may use sendmail to deliver notification of disk space low conditions, or password expiry warnings.
shell	Use this option to enable Remote Execution services. The rsh and rcp commands rely on this service. The legacy DocuSP "print command line client" relies on the enablement of remote shell services, since it uses the rcp command to transfer files onto the FreeFlow® Print Server. However, this service represents a security risk, so it is recommended to disable this service.
slp	Use this option to enable/disable the Service Location Protocol services. This service advertises network services hosted by Solaris® platform (e.g., LPR) to remote clients. Not used by FreeFlow® Print Server, but improves interoperability with legacy Novell clients and Mac OS clients. These clients use legacy network protocols not used today.
ssh	Use this option to enable/disable SSH services. SSH provides user authentication and encrypted secure communications via Secure (remote) Shell, and Secure FTP (SFTP). Once the Security profile has been set to 'High', The FreeFlow® Print Server platform restricts telnet and rlogin commands, so can only remote login securely using the SHH (port 22) service. You can use "secure FTP" (SFTP) to transfer files, which ensures user authentication and encryption of data over the network.
talk	Use this option to enable/disable the "talk" legacy service. The talk utility is a two-way, screen oriented communication program. Not used by FreeFlow® Print Server.
telnet	Use this option to enable/disables the Telnet service. This does not affect using the telnet client from the FreeFlow® Print Server platform to another network host running a Telnet server. The Telnet service is an insecure communication, thus SSH is the recommended alternative to ensure secure connectivity.
time:dgram	Use this option to enable/disable a legacy Time Protocol service. This service is outdated, so recommend it be disabled. Used by FreeFlow® Print Server.
time:stream	Same as time:dgram except a more robust and reliable TCP/IP service. Not used by FreeFlow® Print Server. We recommend this service be disabled.
uucp	Use this option to disable/enable UNIX-to-UNIX copy. This service is used to perform a UNIX-to-UNIX platform copy over the networks. The UUCP service is not a secure protocol and easily exploitable. Not used by FreeFlow® Print Server.

WEBEM	This WEBEM option is use to enable/disable Solaris® Web-based Management service. This service complies with Common Information Model (CIM) requirements specified by Distributed Management Task Force (DMTF). This service is not required for the FreeFlow® Print Server product, but can optionally be used by a customer.
wins	Use this option to enable/disable the Windows® Internet Name Service. This is a Windows® NetBios Name service, which is the Windows® equivalent to DNS for domain names. Samba includes this service to facilitate access to Windows® hosts and shared folders. See comments elsewhere in this table regarding Samba security issues. Optionally required for Windows® folder sharing and FreeFlow® Print Server GUI access to Windows® folders (E.g., Print from File) on a remote host.

5.1.2 Security Profile UDP/TCP Port Settings

Setting the Security profile to 'High' closes many of the UDP / TCP ports that are not required and/or could pose a Security risk. 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
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	SSL	Opened	Opened
445	SMB (TCP)	Opened	Opened
515	LPR	Opened	Opened

631	IPP	Opened	Closed
5001	IPDS	Opened	Closed
7781	JMF	Opened	Closed
8005	Tomcat Web Services	Opened	Opened
8080	Proxy	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

5.2 Anti-Virus Software Protection

Anti-virus software is not bundled with the FreeFlow® Print Server system software. Customers may choose to acquire and install anti-virus software for "peace of mind". Traditional Worms and Viruses rarely if ever infect the FreeFlow® Print Server application and the underlying Solaris® OS. There have not been any report of viruses or malware compromises of the FreeFlow® Print Server platform to the engineering team. Compared to Microsoft® Windows®, the Solaris® OS is much less susceptible to these issues given the Solaris® OS is less widespread, used for specialized computing purposes, and therefore less commonly targeted.

The purpose of the FreeFlow® Print Server platform is a 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. The FreeFlow® Print Server platform does not require these type of applications, so removing them significantly minimize the risk of virus attacks. The security profile settings of "High" supported on the FreeFlow® Print Server system inhibits some of the most common methods for accessing the server (E.g. Services such as FTP, Telnet, Sendmail, etc.). Many services and UDP/TCP ports are disabled when the Security profile is set to "High".

To eliminate the risk of Malware contamination on the FreeFlow® Print Server platform, the customer should first perform a Malware scan on all removable media and removable storage devices before installing and reading the media from FreeFlow® Print Server platform. This precaution will greatly reduce the risk of FreeFlow® Print Server exposure to Malware and risk of exploitation as a "carrier" or repository for Malware

We do not prohibit installing of anti-virus software on the FreeFlow® Print Server platform. However, Xerox has not performed any testing of anti-virus applications, so cannot comment on their effectiveness or possible impact to the productivity and reliability of printer operation. We recommend running Anti-Virus and Malware scans when production printing is completed, and the printer is idle.

5.3 Audit Logging

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

1. BSM Security Audit Logs
2. Solaris® OS Audit Logs
3. System Activity Reporter
4. FreeFlow® Print Server GUI Console Logs
5. FreeFlow® Print Server Job Accounting
6. FreeFlow® Print Server Job/Print Activity Logs

5.3.1 BSM Security Audit Log

The Solaris® 11 OS includes a feature called Basic Security Module (BSM) used for forensic level audit logging. This produces a very detailed level of logging of all operating-system-level events, which have a security implication. For example, noting remote user logins, file delete activity, file read/write activity, etc. The logs produced by this feature will satisfy the Department of Defense audit logging criteria for a "C2" level security certification.

5.3.2 Solaris® OS Audit Log

The Solaris®-Generated logging is quite extensive and complex, so this document does not attempt to provide a comprehensive description of all this system logging The process daemon used to manage this audit logging is referred to as syslog. You can configure syslog to capture debug log information for several of the built-in Solaris® services and the level of verbosity of information to capture. In addition, the syslog service can be defined to write each log record dynamically in real-time over the network to a network server. For more information, refer to the Solaris® Administration Guide or search the Web.

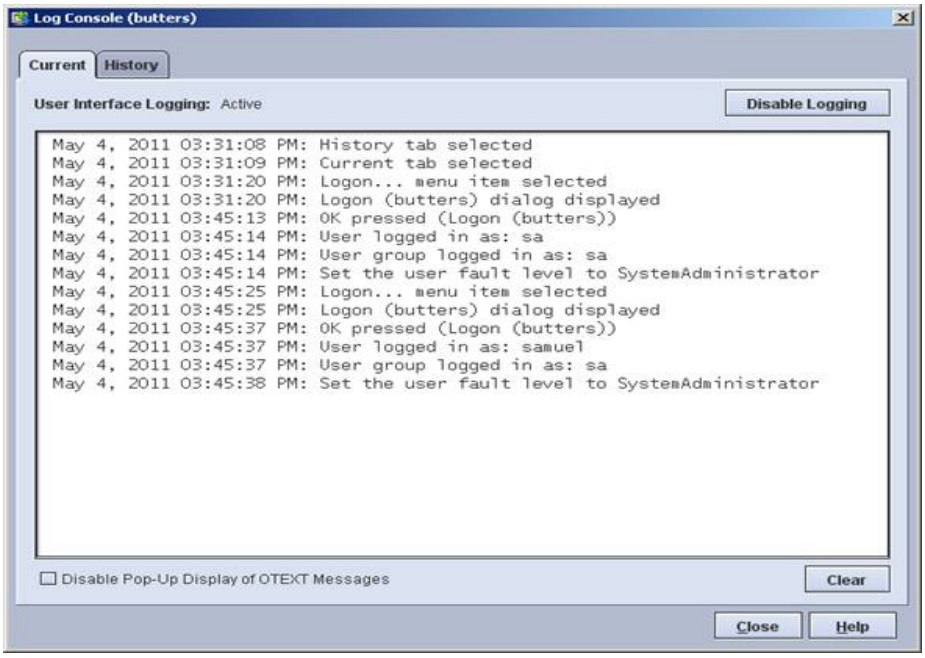
5.3.3 System Activity Reporter

The System Activity Reporter (SAR) service samples system activity and cumulative activity counters in the Solaris OS at intervals of 5 seconds or greater. It will generate automatic reports to measure and monitor system performance. This audit logging is disabled by default, and must be enabled, and setup if required by a customer.

5.3.4 FreeFlow® Print Server GUI Console Log

The FreeFlow® Print Server platform has a Console Logging feature that will log all tasks performed in the FreeFlow® Print Server GUI including user login activity. You can use the System Administrator login enable the "Console Logging" feature from the "Log Console" UI under

An example of the console log illustrating a user login is below:



The example above shows that the 'sa' account and user 'samuel' logged into the FreeFlow® Print Server GUI. Note that user 'samuel' is associated with the System Administrator group, so has SA equivalent access to the FreeFlow® Print Server GUI.

5.3.5 FreeFlow® Print Server Job Accounting

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, Copies, Impressions Printed, Plex, Account ID, etc.

5.3.6 FreeFlow® Print Server Job/Print Activity Logs

FreeFlow® Print Server application modules generate log file entries in a well-defined directory as the system performs job scheduling, rendering/rasterizing, printing, saving, etc. These logs can be analyzed by FreeFlow® Print Server support engineers to identify the security configuration settings, and any risks that may exist. There are log file entries useful to track the jobs processed and printed by the FreeFlow® Print Server software. The information in the FreeFlow® Print Server logs is extensive, and provides details that can be used to audit activity performed by the FreeFlow® Print Server / Solaris® OS users.

5.4 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:

5.4.1 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, or tightly controlling access to a user defined area. Network access to the system can be completely restricted except for access required to perform job submission workflows only. The FreeFlow® Print Server application and Windows® Desktop are not accessible until a user provides their login credentials in the FreeFlow® Print Server GUI. All non-Administrator accounts can be restricted from accessing (coping/deleting) user and print data from the FreeFlow® Print Server GUI, GNome File Manager, or command line shell. They are also restricted from deleting system files that could make the FreeFlow® Print Server / Solaris® platform inoperable.

5.4.2 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 completely 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.).

5.4.3 Hard Disk Purge

When a customer returns a Xerox® printer (E.g., termination of lease), they may wish to sanitize the hard disk(s). The customer can use the Solaris® Format Purge operation to remove all FreeFlow Print Service and Solaris® OS software and data from the hard drive(s). The process involves using the Solaris® format command.

We recommend the customer schedule a Xerox Service Engineer or Support Analyst to complete the hard disk purge operation. It is possible that the hard disk purge process fails for some known or unknown reason. If this occurs, the customer does have the option to remove and purchase the hard disk(s) for a nominal fee. They can then have the data destroyed by a specialist certified in data destruction.

Always capture a System Backup of the FreeFlow® Print Server / Solaris® OS prior to executing the Hard Disk Purge operation if you want the current configuration restored after the disk purge is completed. Even more important is backup of all user and print related data (E.g., VIPP/LCDS resources, Fonts, Print Jobs, etc.) using the Configuration Backup operation. You can use the System Backup or Configuration Backup to restore the FreeFlow® Print Server / Solaris® OS back to the customer customized configuration.

This feature is different from Data Overwrite feature (described in **Section 5.4.2** "*Data Overwrite Feature*" in that the purge operation will result in the permanent removal of all Solaris®, FreeFlow® Print Server platform and user data files. The Data Overwrite feature only purges the user data files on the hard disk(s) in pre-defined directory locations designated for user and print data. Always capture a FreeFlow® Print Server System Backup prior to executing the Hard Disk Purge process to ensure there is a System Recovery in case the disk purge causes a problem. Even more important is backup of all user and print related data (E.g., VIPP/LCDS resources, Fonts, Print Jobs, etc.). Restore user and print backed up data once the hard disk purge operation completes.

A customer can encounter several use cases that require purging the printer hard disk(s) in the FreeFlow® Print Server platform. Some of them are:

1. The customer is returning the printer back to Xerox.
2. Customer is moving the printer to another location.
3. The printer will be idle for a long timeframe.
4. The hard drive has defects and needs replaced.

5.4.4 Removable Hard Drive Kit

For customers who have very strong Security requirements, and need to secure/lock up the FreeFlow® Print Server hard drive(s), Xerox offers an optional "Removable Hard Drive" hardware kits to enable hard drive lock, quick and easy removal of the hard drives. For example, the US Government may require the customer to remove the hard drives after printing "Classified" information, and replacing it with a hard drive used to print more public information.

XSIS offers "removable hard drive kits" which greatly facilitates application-specific software setups, where you keep the hard drive locked up and swap it in when secured print jobs or resources are scheduled for production printing.

5.4.5 Hard Drive Removal and Purchase

Whenever a customer needs to dispose of or destroy the hard drive(s), Xerox Service provides an optional service to remove the hard drive and leave it with the customer for disposal. 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.

5.5 PII/PHI Security Compliancy Standards

Although we designed and developed the FreeFlow® Print Server security features with industry standard certification guidelines in mind, there is no Security authority that has officially certified the FreeFlow® Print Server platform. The FreeFlow® Print Server Security team is aware of several Security compliance standards, and we continually enhanced and developed new Security features to close compliancy gaps.

The FreeFlow® Print Server software includes a very robust set of capabilities, settings and tools that can address the vast majority of customer Security requirements. We have placed the FreeFlow® Print Server platform in several State and Federal Government locations that have the highest level of Security requirements and strict Security compliance standards. Xerox is pro-actively implements new FreeFlow® Print Server features for customer Security requirements that meet very stringent Financial, Education and Government standards for protecting sensitive data.

5.5.1 DIACAP Security Standard

The DIACAP (Department of Defense Information Assurance Certificate and Accreditation Process) standard is a Security compliance required by US Government agencies which are responsible for systems that are owned or controlled by the Department of Defense (or by commercial systems which are under contract to the Department of Defense) before any network device can be incorporated on their network. When an institution completes this Accreditation for a network device, the device qualifies as network worthy for the US Government network and receive an ATO (Authority to Operate) certificate. An institution that would like to achieve the ATO must provide a sponsor (i.e., IT or Security representative) to work through the DIACAP process under the auspices of its internal DOD-inspected Security process. Xerox requires customer sponsorship to partake and complete the DIACAP process.

Xerox is required to evaluate the FreeFlow® Print Server platform for compliance with "STIG" Security requirements as part of satisfying DIACAP compliancy. Security Gaps which are of concern to the customer's Security manager need to be remediated by the installation of security Patches and/or reconfiguration (aka "STIG hardening") of Solaris® and/or FreeFlow® Print Server software.

5.5.2 STIG Toolkit

STIG (Security Technical Implementation Guide) is a set of Security policies, requirements, checklists, and compliance assessment methodology used by Defense Information Systems Agency (DISA) Field Security Operations (FSO) to evaluate software applications prior to deployment 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 a Xerox® printer with FreeFlow® Print Server is permitted to connect to the customer's network.

The FreeFlow® Print Server platform bundles a STIG toolkit to assist government agencies to obtain DIACAP (Department of Defense Information Assurance Certification and Accreditation Process) compliancy and other State Department (E.g., IRS) required compliance standards. All STIG requirements can be categorized into 4 different groups (i.e., Cat 1, 2, 3 & 4) with Cat 1 being the highest priority and Cat 4 the lowest priority.

The FreeFlow® Print Server STIG Toolkit delivers a set of Solaris® 'JASS scripts' that can be used to satisfy specific STIG requirements to meet strict Federal and State security requirements.

5.5.3 Common Criteria Certification Standard

FreeFlow® Print Server runs as an application on top of the Solaris® OS, which meets the Common Criteria Certificate (CCC) compliant standard for the underlying OS mechanisms that it utilizes for connectivity and security. The FreeFlow® Print Server GUI mediates all user interactions and non-Administrator users do not have direct access to the operating system (the System Administrator role may interact with the OS if permitted by the security configuration).

Oracle® has received certification for the Solaris® 10 Operating System Updates 5, 7 and 9 under the Common Criteria at EAL4+ under the Controlled Access Protection Profile and Role Based Access Control Protection Profile and certified for use on SPARC and AMD/Intel based platforms.

Oracle Solaris 11 is certified under the Canadian Common Criteria Scheme at Evaluation Assurance Level 4 (EAL4) and augmented by flaw remediation (EAL4+). EAL4 is the highest level of evaluation mutually recognized by 26 countries under the Common Criteria Recognition Arrangement (CCRA). Oracle certifies subsequent Solaris® Updates and Security patches using the Common Criteria's Assurance Continuity Process.

Solaris® implements all Network Security mechanisms and interactions with the customer's network and Solaris® performs the authentication/authorization. Thus, Solaris® ensures the infrastructure for FreeFlow® Print Server application security. Oracle® certifies subsequent Solaris® OS updates and Security patches to using the Common Criteria's Assurance Continuity Process.

5.5.4 Authority to Operate (ATO) Certification

The customer's Security manager requires an ATO before considering any network device worthy for connectivity on the Army network. This is a certificate obtained by the customer after they have successfully complete the DIACAP process.

5.5.5 Certificate of Networthiness (CON) Standard

Prior to connecting a Xerox® printer to a US Army Enterprise Network, it requires completion of the Certificate of Networthiness (CON) process. A pre-requisite to achieve the CON is for the customer to acquire the Authority to Operate (ATO) by going through the DIACAP process. Once achieving the DIACAP process, an ATO represents the official certification for compliancy and ensures qualification for CON compliancy. Identification of a formally acknowledged sponsor to obtain CON compliancy is a requirement of the CON submission process, and the sponsor must be an Army officer.

A networked device can only qualify for connectivity with the Army Enterprise Network after successfully completing the CON process. The Army sponsor initiates and drives the CON process for the customer requiring Army network connectivity. The sponsor provides the information for how they plan to operate, manage, support and maintain the networked Xerox printer device according to Army regulations.

5.6 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 a device, and more specifically the locations, capacities and contents of volatile and non-volatile memory components. 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 an 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, other devices interfaces such as a Print Station Interface Platform (PSIP) for some print engines, and workflow device such as FreeFlow® Core, etc.