June 2017

Xerox® FreeFlow® Print Server

Security White Paper And Configuration Guide

Solaris-based Products

Version: 1.0

Xerox® iGen®4 / iGen®150 Presses / iGen®8250 Presses
Diamond Edition® Presses
Xerox® Nuvera® 200/288/314 EA / 200/288/144/120/100 MX / 1XX EA Series
Xerox® Color 800i/1000i Presses
Xerox® Color 800/1000 Presses
Xerox® Versant® 80/2100 Presses
Xerox® DocuColor® 8080 Press
Xerox® Color C75 / J75 Presses
Xerox® Color 560 / 570 Presses
Xerox® Impika® Compact Inkjet Press
Xerox® CiPress® 325/500 Production Inkjet System
Xerox® Rialto® 900 Inkjet Press
Xerox® D95/D110/D125/D136 Copier/Printer
Xerox® DocuTech® 180/155/128 Highlight Color Systems
Xerox® DocuTech® 6180/6135/6115 Monochrome Printers
Xerox® DocuPrint® 180/155/135/115/100 MX

Table of Contents

REVISION LOG

Version	Date	Description or Purpose of Changes	Author
1.8	07/01/09	This SME has undergone a major revision (e.g., rewrite, reorganization and new sections) for the FFPS v7 SP2 software relative to the previous version for FFPS v6. There have been new sections that describe: 1. Security Scan Applications 2. Problem Escalation Expectation 3. Port Management Tool 4. Disabling or Restricting Print/Network Protocol Services 5. Standard Solaris IP Filter Setup 6. Data Overwrite 7. Removable Hard Disk Security Compliance Standards	D. Roome
2.1	05/24/10	Updates for Pre-Public version Updates for FFPS 8.0. FFPS v8 Security features: 1. IPSec configuration script is now available to protect legacy TCP/IP protocols 2. FFPS 8.0 includes Web Proxy Server for the Xerox® 800/1000 print engine. 3. SSLv2 is disabled by default; control added to Security Profile 4. SHA1 is enabled for SSL and added to Security Profile	D. Roome
2.2	09/13/10	1. Updates for FFPS 8.1 2. Added '*Security Patch Integration on FFPS*' section. 3. Added '*IT or Administrator Security Expectations*' section. 4. Added '*IP Security Data Encryption via IPSec Protocol*' section. 5. Updated Automatic Logoff section with Screen Saver information. 6. Many updates to the '*Managing Print/Network Protocol and IP Filter Services*' section and '*Print/Network Protocol <_> Port Mappings*' table. 7. Added '*FFRPS (FreeFlow Remote Print Service) Services*' section. 8. Updated '*FTP Services*' section with information for disabling FTP. 9. Updated the '*Hard Drive Removal and Purchase*' section. 10. The '*Virus Protection Software on FFPS*' section is updated.	D. Roome
2.3	05/24/11	1. Updates for FFPS 8.2 SP2 2. Customized Access Control of Job Management Features 3. Security Inventory Service Tool 4. Strong Password Enhancements and FFPS GUI Settings 5. Password Expiry Mail Notifications 6. SNMP v3 Support 7. SHA1 SSL/SSH Encryption 8. Hard Disk Purge Services 9. Updated BSM Logging Section 10. Common Criteria Certification 11. Xerox Quarterly Security Patch Clusters 12. Rapid Security Patch Delivery per Update Manager, DVD or USB	

3.0	04/09/12	1. Updates for FFPS v9 Software Release. 2. Significant DISA STIG hardening updates of existing and new STIG requirements. 3. New Windows-based software update tool 4. Systematic procedures for enabling Strong Password feature and changing FFPS user passwords. 5. New lock-user utility to lock/unlock all FFPS/Solaris System Users or individually. 6. Section reviews with additions and improvements.	D. Roome
1.0	01/01/17	Updated this document to "official" Xerox branded format, so this is a significant change from the previous document. Made several update modifications to the information, and removed outdated information. Included information related to the support of 2048-bit SSL Self-Signed Certificates.	D. Roome

1.0 FreeFlow® Print Server Security Overview

This document describes the Xerox® FreeFlow® Print Server platform Security features. It supports the latest FFPS v7, v8 and v9 software releases. This document identifies any feature that supports only specific software releases or excluded by a software release.

The Xerox® FreeFlow Print Server is an application software package tightly integrated with the Solaris OS, which has very well established highly customizable Security features. The FFPS 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 FFPS platform.

Security processes and capabilities, which exceed the scope of the FFPS software, are the responsibility of the customer. Xerox is responsible for integrating Security patches for the Solaris OS, and for supporting customer Security requirements by identifying FFPS workflows, configuration settings and alternative methods to satisfy Security requirements. If a customer has contracted with Xerox Service (e.g., ACS, XBS, etc.) to manage the security of FFPS Products, Xerox will implement and manage compliance with the customer's Security Process requirements.

Xerox will provide Security tightening recommendations and strategies, but is not responsible for auditing Xerox® printer devices. We recommend that the customer hire a CISPP professional to ensure and certify that the Xerox® printer(s) comply with the Security standards per the customer policy.

2.0 FreeFlow® Print Server Security Patches

Oracle responds to US CERT advisory council notifications of Security vulnerabilities (per reported Common Vulnerabilities and Exposures (CVE)) and develops patches that remediate the Security vulnerabilities that are applicable to Solaris® 10 and components (e.g., OpenSSH, OpenSSL, Java, etc.). Xerox has a dedicated FreeFlow® Print Server development team, which actively reviews the US CERT advisory council CVE notifications, and delivers a Security Patch Cluster to remediate the threat of these Security risks for the FreeFlow® Print Server / Solaris platform.

Xerox actively reviews US CERT advisory council CVE notifications, and delivers a Security Patch Cluster from Oracle to remediate the threat of these Security risks for the FreeFlow® Print Server / Solaris® platform. Xerox delivers a Security Patch Cluster on a quarterly (i.e., 4 times a year) basis. Xerox receives new patch updates in January, April, July and October, and will test them for supported Printer products (Xerox Nuvera®, D-Series Codier/Printer· DocuTech® and DocuPrint®) prior to delivery for customer install. This Security deliverable will include Java software updates.

The FreeFlow® Print Server / Solaris® platform is a specialized Print Service intended as a Digital Front End (DFE) to drive Xerox® high-volume printers, and some Xerox® mid-volume printers. The FreeFlow® Print Server software is tightly coupled with the Xerox Nuvera® PSIP software, which makes it important to first test Security patches delivered by Oracle® prior to customer install. Installing a Security Patch Cluster not tested and sanctioned by Xerox, could damage the integrity of the FreeFlow® Print Server software, compromise the stability of the printer, or render it completely inoperable.

Security Patch Clusters go through testing on selected FreeFlow® Print Server Patch software releases to ensure print/network connectivity and performance of the software. The Security Patch Cluster will overlay on an existing FreeFlow® Print Server installation identified as one of the tested and approved FreeFlow® Print Server Patch software releases. Customers are encouraged to work with Xerox Service Engineer (CSE) to escalate Security audit reports to the Xerox hotline that supports the specific FreeFlow® Print Server / Printer product (e.g., iGen®8250, Color C75 / J75, etc.). It is very important to provide the Common Vulnerability Exposure (CVE) number for any of the Security findings in the audit report.

2.1 Security Patch Notifications

You can find bulletin notifications for new FreeFlow® Print Server Security Patch Cluster from the **www.xerox.com** Web site under "Security® At Xerox", and offers RSS feed services for the posted bulletins. There are a couple ways to view FreeFlow® Print Server Security Cluster bulletins, and one is by going to the Web URL below:

www.xerox.com/security

In the "Select a Product Family" box, select the "Workflow software" option. In the "Select a Product' box select the "FreeFlow® Print Server" option. This will list the FreeFlow® Print Server product bulletins with the newest at the top of the list.

It is advisable that a customer concerned with the Security of their FreeFlow® Print Server / Printer device subscribe to the RSS Feed for Xerox Security Bulletins using the Web URL below:

http://rss.xerox.com/security-bulletins

Applications such as Microsoft® Outlook, Windows® Live, MSN, Yahoo, Google, Bloglines, and AOL support RSS Feed setup. Configure your application of choice for Xerox bulletin notification using the **http://rss.xerox.com/security-bulletins** Web URL. Find the details at the Web URL below:

http://www.office.xerox.com/feed/security-bulletins/enus.html

2.2 Security Patch Delivery and Install

A customer can consider a couple delivery and install methods to install the latest Security Patch Cluster on their FreeFlow® Print Server / Solaris® platform. The customer can schedule a Xerox CSE or Analyst to install the Security Patch Cluster. A FreeFlow® Print Server customer can choose to install the quarterly Security Patch Cluster, and should work with Xerox Analyst and/or Service representative to understand the expectations, as well the procedures to complete the install. The delivery and install methods are DVD/USB Media and FreeFlow® Print Server Update Manager. You can sign up for an RSS feed to FreeFlow® Print Server Security bulletins for notification of quarterly Patch Clusters ready for installation.

Note: *Make sure that you have a System Backup of the* FreeFlow® Print Server */ Windows system on a remote storage location before installing a Security Patch Cluster. You can recover the* FreeFlow® Print Server *software to the point prior to Security Patch Cluster install if the security patches had caused a software problem.*

2.2.1 DVD/USB Media Install Method

Many customers do not want the responsibility of installing the Security Patch Cluster from a remote Xerox server over the Internet, which requires access through their proxy server. Therefore, the media install method is the best option when the customer feels this is a risk.

The Security Patch Cluster deliverables are available on the Customer Field Operations (CFO) Web site once they are ready for customer delivery. The Xerox CSE/Analyst can download and prepare for the install by writing the Security Patch Cluster into a known directory on the FreeFlow® Print Server platform, or on DVD/USB media. Delivery of the Security Patch Cluster includes an ISO and ZIP archive file for convenience. Once the patch cluster has been prepared on media, run the provided install script to perform the install. The install script accepts an argument that identifies the media that contains a copy of the FreeFlow® Print Server Security Patch Cluster. (e.g., # installSecPatches.sh [disk | dvd | usb]).

If DVD/USB media is restricted from a customer location for Security reasons, such as the case with most Government agencies, transfer the Security Patch Cluster to the FreeFlow® Print Server platform using a "secure" utility such as SFTP or SCP, and install from FreeFlow® Print Server platform. The Xerox Service or Analyst representative can grant access of the Security Patch Cluster to the customers so that they can install on their own. The Xerox Service or Analyst representative can work together and arrange for the customer to install the Security Patch Cluster.

2.2.1 FreeFlow® Print Server Update Manager Install Method

This method of delivery and install provides the ability to download the Security Patch Cluster over the network and install using the FreeFlow® Print Server Update Manager. The Security Patch Cluster install using FreeFlow® Print Server Update Manager is a network delivery, and has the advantage of "ease of deliver and install". We recommend the customer use the FreeFlow® Print Server Update Manager method if they wish to perform install on their own. This empowers the customer to have the option of installing these patch updates as soon as they become available, and not need to rely on the Xerox Service team. One of the advantages to this Security Patch Cluster method is that Xerox has tested the quarterly patches with the FreeFlow® Print Server software product.

Xerox uploads the quarterly FreeFlow® Print Server Security Patch Cluster for FreeFlow® Print Server v7, v8 and v9, to an external Xerox® Server accessible over the Internet outside of the Xerox® network. The external Xerox® server does not have access to the FreeFlow® Print Server platform at a customer site. It is required that the customer proxy server information be configured on the FreeFlow® Print Server platform so that it can gain access to the Xerox® server over the Internet outside of the customer network. The FreeFlow® Print Server platform initiates the communication to download the Security Patch Cluster from behind the customer proxy server, and the communication is "secure" by SSL over port 443.

3.0 FreeFlow® Print Server Security Profiles

The FreeFlow® Print Server software provides four static system-supplied Security Profiles to allow customers flexibility in selecting the level of Security enforcement required by a customer. 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 'High' security profile, and enable/disable specific network services as mandated by the customer site requirements. You can save multiple custom profiles on the system assigned with their own custom assigned name to help the System Administrator readily differentiate between them. Although the FreeFlow® Print Server 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 procedures described throughout this document

When network security requirements are important to a customer, we recommend setting the Security Profile to 'High' or defining a "custom" profile from the system-supplied 'High' profile. All of the print/network protocol workflows supported by the FreeFlow® Print Server platform are functional with the 'High' profile setting. FreeFlow® Make Ready workflow is the only exception, which requires the FTP or IPP protocol for printing. High security disables the FTP and standard IPP services on the FreeFlow® Print Server platform, so the FreeFlow® Make Ready Administrator will need to setup that application to use "secure" ftp (SFTP), or "secure" IPP (sIPP). To ensure proper settings for Make Ready when the FreeFlow® Print Server defines a Security profile set to 'High', refer to the FreeFlow® Application Suite Security documentation.

Creating printers from the Printer Administration application for the FFMR application provides a "secure" mode option when creating the printer. You must select the "secure" option to ensure the FFMR application can access the FreeFlow® Print Server platform using SFTP or "secure" IP (sIPP) job submission workflow. You must defined an SSL certificate on the FreeFlow® Print Server platform to support sIPP job workflow. See SSL certificate setup procedure in Section 7.1.1 "*Creating/Installing SSL Certificate*"'. Alternatively, configure the FFMR application to use lpr as a job submission workflow to by-pass the "secure" mode. This does not require user authentication or data encryption over the network.

Note: *The FreeFlow® applications (e.g., FFMR) must configure the IP address of the* FreeFlow® Print Server *platform in their local hosts file, or using Domain Naming Services (DNS). This setting enables proper access to the* FreeFlow® Print Server *digital certificate when selecting the "Check Security Certificate" option is from FFMR. This will ensure retrieval of the digital certificate. You can find the hosts file in the locations below:*

Windows 7/8/10

- *c:\windows\system32\drivers\etc\hosts*

Windows XP

- *c:\windows\system32\drivers\etc\hosts*

If using DNS, then enable it on both the Windows PC and FreeFlow® Print Server *platform. You will not have access to the* FreeFlow® Print Server *digital certificate when selecting the "Check Security Certificate" option and certificate retrieval will fail.*

Note: *Custom Security profiles do not persist after a* FreeFlow® Print Server *patch software upgrade, and not backed up using the* FreeFlow® Print Server *configuration backup process. It is very important to capture the Security settings for any "custom" Security profiles to support manual creation once the software upgrade completes. You can capture the screen images of the "custom" Security profile settings for each of the tab options.*

3.1 System Supplied Security Profiles

Below is a chart, which provides a high-level overview of the "built-in" FreeFlow® Print Server Security profiles. This chart identifies the Security controls applied at each FreeFlow® Print Server Security level.

System Supplied Security Profiles Table

System Supplied Security Profile	Characteristics	Value & Marketplace
Solaris OS Only aka "None"	• Default Solaris security • All UDP/TCP ports open. • All print/network clients and services enabled. • Walkup users can print any files on the hard drive including, Saved, CD-ROM and Retain PDL jobs. • Full desktop workspace menu access • Automatic login enabled. • Access to command line via terminal window. • Supports legacy DigiPath workflow. • Supports FFMR 2.0+ workflow. • Anonymous FTP enabled in read-only mode and user permissions restricted.	• Stand-alone network confined to a controlled set of trusted users. • Print non-sensitive documents • Some print shops or physically secured University environments. • May have solid security incorporated on customer network. (e.g., firewall settings and trusted users) • Customer requires capabilities disabled by Low, Medium and High security. Optionally, create a "custom" security profile from the 'High' profile, and enable required capabilities.
Low (Default)	• Same Security as "None" (Solaris OS Only) but the system is "hardened" by FreeFlow® Print Server executing special scripts that tighten up a significant number of security configuration settings. • telnet and rsh services disabled. SSH enabled to permit secure remote login. • NFS client is enabled • AUTOFS service enabled • rusersd RPC service disabled.	• Print non-sensitive or non-"commercial-classified" documents • May have solid security incorporated on customer network. • Customer requires capabilities disabled by Low, Medium and High security. Optionally, create a "custom" security profile from the 'High' profile, and enable required capabilities.

	• Walkup users can only print Saved and CD-ROM jobs. • telnet is disabled, but the System Administrator can enable it. • SSLv2 disabled. SSLv3 enabled and required.	
Medium	• Same Security as Low and more. • AUTOFS is disabled (e.g. remote file systems such as /net/<hostname> and /home/<username> are not automatically mounted) • NFS Service is IP-filter-enabled via RPC tab, and disabled to non-authorized clients. NFS client on FreeFlow® Print Server remains enabled	• Print sensitive or "commercial-classified" documents • Additional High security features not needed and require Legacy DigiPath Workflow or Insecure FFMR workflow.
High	• Same Security as Medium and more. • Terminal (aka "command line") window is only accessible by root. All users that are not root or 'sa' can only access the system confined in the FreeFlow® Print Server GUI and their access levels as a FreeFlow® Print Server user or operator. • FTP is disabled, but there is an option to the temporarily enable this feature. Can use SFTP (secure FTP via SSH) for secure data transfer. Anonymous FTP enabled in read-only mode and user permissions are restricted. • NFS Service is disabled. NFS client on FreeFlow® Print Server remains enabled. If NFS Server re-enabled using a "custom" profile, filter remote host access to FreeFlow® Print Server via RPC tab. • DNS and NIS/NIS+ Services are disabled. • Automatic login (via GUI) is disabled (login is always required from FreeFlow® Print Server GUI) • Legacy DigiPath workflow blocked. • FFMR 2.0+ enabled with FFMR and netagent configured for in "secure" mode. • FFRPS (FreeFlow® Remote Print Service) does not have access unless the remote host granted RPC access using the RPC filter in the FreeFlow® Print Server GUI. Another option is to configure the Windows client	• Print highly-sensitive documents • Customer data privacy is required • Typical for financial and government environments. • Non-secured University environments

	(running FFRPS) and the FreeFlow® Print Server platform with an IPSec configuration. • SSLv2 is disabled. SSLv3 enabled and required. • SHA1 is required for SSH (MD5 is disabled) • SHA1 is enabled for SSL Certificate (MD5 is disabled) • Peripheral Devices (USB and CD/DVD) are disabled. • ICMP services are disabled. Job Forwarding no longer supported. It requires Echo (a.k.a., ping) service. • Router option is disabled. (Nuvera feature only).	

3.2 Security Profile Features and Services Default Settings

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

Security Profile Option Settings

		OS	Low	Medium	High
General Tab	Apply Settings After Reboot	Enabled	Enabled	Enabled	Enabled
	Automatic Logon	Enabled	Enabled	Enabled	Disabled
	Automatic Logon Username	User	User	User	User
	Automatic Logon Message	~~Disabled~~Secure	~~Disabled~~Secure	~~Enabled~~Secure	~~Enabled~~Secure
	Limit Print Service Paths	Disabled	Enabled	Enabled	Enabled
	Allowed Paths	None	Sample Jobs, Saved Jobs, CD-RW 0	CD-RW 0	None
	Minimum Password Length	6	6	6	6
	Cleanup Menus	Disabled	~~Enabled~~Disabled	Enabled	Enabled
	UNIX Terminal Authentication	Disabled	~~Enabled~~Disabled	Enabled	Enabled
System Tab	Allow_host.equiv_plus	Enabled	Disabled	Disabled	Disabled
	Anonymous FTP	Enabled	Enabled	Enabled	Enabled
	bsm	Disabled	Disabled	Enabled	Enabled
	Executable Stacks	Enabled	Disabled	Disabled	Disabled
	Hide Info Banners	Disabled	Enabled	Enabled	Enabled

	Peripheral Devices	Enabled	Enabled	Enabled	Disabled
	Remote CDE Logins	Enabled	Disabled	Disabled	Disabled
	Restrict DFS Tab	Enabled	Enabled	Enabled	Disabled
	Restrict NFS Portmon	Disabled	Enabled	Enabled	Enabled
	Router	Enabled	Enabled	Enabled	Disabled
	Secure Network Serttings	Disabled	Enabled	Enabled	Enabled
	Secure Sendmail	Disabled	Enabled	Enabled	Enabled
	Security Weaning Banners	Enabled	Disabled	Disabled	Disabled
	SNMP	Disabled	Disabled	Enabled	Disabled
	SHA1 Algorithm for SSH	Disabled	Disabled	Disabled	Enabled
	SHA1 Algorithm for SSL	Disabled	Disabled	Disabled	Enabled
	SSLv2	Enabled	Disabled	Disabled	Disabled
	TAS httpd	Enabled	Disabled	Disabled	Disabled
INIT Tab	S40LLC2	Enabled	Disabled	Disabled	Disabled
	S47ASPPP	Enabled	Disabled	Disabled	Disabled
	S70UUCP	Enabled	Disabled	Disabled	Disabled
	S72AUTOINSTALL	Enabled	Disabled	Disabled	Disabled
	S73CACHEFS.DAEMON	Enabled	Disabled	Disabled	Disabled
	S94NCALOGD	Enabled	Disabled	Disabled	Disabled
	S17HCLNFS.DAEMON	Enabled	Enabled	Disabled	Disabled
	S80MIPAGENT	Enabled	Disabled	Disabled	Disabled
	autofs	Enabled	Disabled	Disabled	Disabled
	chargen:dgram	Enabled	Disabled	Disabled	Disabled
	chargen:stream	Enabled	Disabled	Disabled	Disabled
	comsat	Enabled	Disabled	Disabled	Disabled
	daytime:dgram	Enabled	Disabled	Disabled	Disabled
	daytime:stream	Enabled	Disabled	Disabled	Disabled
	discard:dgram	Enabled	Disabled	Disabled	Disabled
	discard:stream	Enabled	Disabled	Disabled	Disabled
	echo: dgram	Enabled	Disabled	Disabled	Disabled
	echo: stream	Enabled	Disabled	Disabled	Disabled
	exec	Enabled	Disabled	Disabled	Disabled
	finger	Enabled	Disabled	Disabled	Disabled
	ftp	Enabled	Enabled	Enabled	Disabled
	gss	Enabled	Enabled	Enabled	Disabled
	ktkt_warn	Enabled	Enabled	Enabled	Disabled
	login	Enabled	Disabled	Disabled	Disabled

	name	Enabled	Disabled	Disabled	Disabled
	nfs.client	Enabled	Enabled	Disabled	Disabled
	nfs.server	Enabled	Enabled	Enabled	Disabled
	ntp	Enabled	Disabled	Disabled	Disabled
	ocfserv	Enabled	Disabled	Disabled	Disabled
	rpc.cmsd	Enabled	Disabled	Disabled	Disabled
	rpc.rusersd	Enabled	Disabled	Disabled	Disabled
	rpc.rwalld	Enabled	Disabled	Disabled	Disabled
	rpc.sprayd	Enabled	Disabled	Disabled	Disabled
	rcp.ttdbserverd	Enabled	Disabled	Disabled	Disabled
	rquotad	Enabled	Disabled	Disabled	Disabled
	rstat	Enabled	Disabled	Disabled	Disabled
	S81VOLMGT	Enabled	Enabled	Enabled	Disabled
	samba	Enabled	Enabled	Enabled	Enabled
	sendmail	Enabled	Disabled	Disabled	Disabled
	shell	Enabled	Disabled	Disabled	Disabled
	slp	Enabled	Disabled	Disabled	Disabled
	ssh	Enabled	Enabled	Enabled	Enabled
	talk	Enabled	Disabled	Disabled	Disabled
	telnet	Enabled	Disabled	Disabled	Disabled
	time:dgram	Enabled	Disabled	Disabled	Disabled
	time:stream	Enabled	Disabled	Disabled	Disabled
	uucp	Enabled	Disabled	Disabled	Disabled
	WEBEM	Enabled	Disabled	Disabled	Disabled
	Wins	Enabled	Enabled	Enabled	Enabled

3.3 Security Profile Features and Services Descriptions

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

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 Logon Username	This option is the FFPS user that is used to automatically log into the FFPS GUI at startup. Anytime that the FFPS GUI is initialized (such as a restart) it will open logged in with this FFPS user, and user credentials.
Automatic Logon Message	
Limit Print Service Paths	This feature defines the Solaris file paths accessible for job reprint. 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 reprint from any job repository or resource. The Xerox Nuvera® printer does not support this feature, and therefore reprint of jobs is not restricted.
Minimum Password Length	This setting denotes the minimum number of characters you can specify for a FreeFlow® Print Server user password when using this particular Security profile on the platform. The range allowed to define a minimum is 0 – 8 characters. The range is extended to 0 – 15 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 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. The option defines disabled by default. This will ensure the '+' is absent from the hosts.equiv file to prevent trusted user access without a password.

Anonymous FTP	You can enable/disable the anonymous FTP service on the FreeFlow® Print Server platform. The FreeFlow® Print Server platform grants anonymous FTP access even when the standard FTP service is disabled. Anonymous FTP service does not require authentication credentials. **Note:** *The Xerox Nuvera® and DT Highlight Color (HLC) printers require the Anonymous FTP service on the "private network" between* FreeFlow® Print Server *and the print engine. Do not disable the FTP service on the* FreeFlow® Print Server *platform for the Xerox Nuvera® and DT HLC printers. Anonymous user access is required between the* FreeFlow® Print Server *platform and the printer over a "private" network interface. You can disable the FTP service from the "public" network interface by closing port 21.*
bsm	Solaris Basic Security Module (BSM); This option 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 take 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
Hide Info Banners	
Peripheral Devices	This option is use to enable/disable the peripheral volume manager service so that the CD/DVD drive and USB ports are inoperable.
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.
Restrict NFS Portman	This option prevents malicious users from gaining access to files exported/shared by the NFS server by preventing custom RPC based scripts or applications used on unprivileged ports. Equivalent to setting "nfs_portmon = 1" in the /etc/system file.

Router	Nuvera Only: This option provides the PSIP/Nuvera printer to communicate on the customer "public" network using the FFPS platform as a router. The network interface between the PSIP/Nuvera printer and FFPS platform is no longer "private" if enabled. This is used so that the PSIP/Nuver printer can use Remote Services for AMR and CFA data pushes.
Secure Network Settings	This option modifies the response/behavior of the Solaris network protocol stacks to block low-level security attacks from the network. Unpredictable impact to performance of job submission for very large job files.
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.
~~Anonymous FTP~~	~~You can enable/disable the anonymous FTP service on the FreeFlow® Print Server platform. The FreeFlow® Print Server platform grants anonymous FTP access even when the standard FTP service is disabled.~~ ~~Anonymous FTP service does not require authentication credentials.~~ ~~**Note:** *The Xerox Nuvera® and DT Highlight Color (HLC) printers require the Anonymous FTP service on the "private network" between FreeFlow® Print Server and the print engine. Do not disable the FTP service on the FreeFlow® Print Server platform for the Xerox Nuvera® and DT HLC printers. Anonymous user access is required between the FreeFlow® Print Server platform and the printer over a "private" network interface. You can disable the FTP service from the "public" network interface by closing port 21.*~~
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.
~~Restrict NFS Portman~~	~~This option prevents malicious users from gaining access to files exported/shared by the NFS server by preventing custom RPC based scripts or applications used on unprivileged ports. Equivalent to setting "nfs_portmon = 1" in the /etc/system file.~~
~~Secure Network Settings~~	~~This option modifies the response/behavior of the Solaris network protocol stacks to block low-level security attacks from the network. Unpredictable impact to performance of job submission for very large job files.~~
~~Restrict DFS Tab~~	~~This option Enables/disables the restriction of the "/local/var/spool/data" shared directory.~~

SNMP	This option pertains to an SNMP service bundled with Solaris and useful platform remote management. The FreeFlow® Print Server software does not use this built-in Solaris SNMP service, but is available if an administrator requires it for some special situation. This option is unrelated to FreeFlow® Print Server SNMP Gateway support Remote Services (Billing, CFA/Outload Transfer, etc.), CentreWare Web, Job Status information, etc.
~~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.~~
~~Peripheral Devices~~	~~This option is use to enable/disable the peripheral volume manager service so that the CD/DVD drive and USB ports are inoperable.~~
~~SSLv2 disabled~~	~~Most customers that are Security conscience require disabling the SSLv2 services. The SSLv2 have inherent Security risks, so customers favor SSLv3 services. The SSLv3 services enable when disabling SSLv2 services. Most modern Web browsers and HTTP clients support SSLv3 services.~~
SHA1 Algorithm for SSL	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 MD5, which is a legacy encryption algorithm. Hackers have compromised the legacy MD5 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 SHA1 encryption algorithm to sign created SSL certificates, and disables MD5.
SHA1 Algorithm for SSH	SSH implements a MAC (Message Authentication Code) protocol to ensure an attacker is not able to tamper with message packets. SSH v1.5 uses MD5, and SSH v2.0 supports SHA1. SHA1 is virtually unable to be cracked and thus preferred over MD5. Assigning the Security profile to 'High' will result in the FFSP software using SSH1 rather than MD5. Enabling this option will ensure usage of SHA1.
SSLv2 disabled	Most customers that are Security conscience require disabling the SSLv2 services. The SSLv2 have inherent Security risks, so customers favor SSLv3 services. The SSLv3 services enable when disabling SSLv2 services. Most modern Web browsers and HTTP clients support SSLv3 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.

INIT Services Tab

S40LLC2	This option enables a Class II logical link control driver.
S47ASPPP	Use this option to enable the Asynchronous PPP link manager: This service will enable using the enable-remote-diagnostics command.
S70UUCP	This is an UUCP server. Not used by the FreeFlow® Print Server software.
S72AUTOINSTALL	Use this option to enable a script executed during stub JumpStart or AUTOINSTALL JumpStart.
S73CACHEFS.DAEMON	Use this option to starts the cachefs file systems.
S94NCALOGD	Use this option to enable Solaris Network Cache and Accelerator services.
S17HCLNFS.DAEMON	Manages the BWNFS (B & W network file system) service; provides ability to read/write MS-DOS file system. Optionally used by FreeFlow® Print Server for DOS compatibility (For legacy Windows SMB and WINS network services compatibility, see other references for SMB/Samba).
S80MIPAGENT	Use this option to enable the Mobile IP agent. Not used by the FreeFlow® Print Server software.
~~S17HCLNFS.DAEMON~~	~~Manages the BWNFS (B & W network file system) service; provides ability to read/write MS-DOS file system. Optionally used by FreeFlow® Print Server for DOS compatibility (For legacy Windows SMB and WINS network services compatibility, see other references for SMB/Samba).~~

Services Tab

~~amiserv~~	~~Use this option to enable NFS Service to auto-mount file systems (/home and /net). RPC Smart Card Interface: Not used by FreeFlow® Print Server~~
autofs	Use this option to enable automatic file system mounting. Not used by FreeFlow® Print Server.
chargen:dgram	Use this option to enable 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 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 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 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 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 the Echo Protocol server services. This service echoes 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 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 Remote User Information Server services. This service display information about local and remote users. Reveals information about system users. Not used by FreeFlow® Print Server
ftp	Use this option to enable the FTP Server services. Client FTP services remain enabled so that files can be transferred to remote workstations from the FreeFlow® Print Server platform. **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.*
gss	Use this option to enable the RPC Authentication Program service. This service generates and validates GSS API tokens for kernel RPC. This service is required for the LDAP/ADS netJoin feature.
ktkt_warn	Use this Client-side service to communicate from the FreeFlow® Print Server platform to a Kerberos server service. This service will renew TGT (Ticket Granting Ticket) automatically up to its max renewable lifetime and warns when the Kerberos ticket is about to expire. Configure this service in the /etc/krb5/warn.conf file. Not used by FreeFlow® Print Server.
login	Use this option to enable 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 DARPA Trivial Name Server services. This service name is in.tnamed and is a server that supports the DARPA Name Server Protocol. Seldom used anymore. Not used by FreeFlow® Print Server
nfs.client	Use this option to enable 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 Server Side 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 the Network Time Protocol service. This service automatically synchronize the platform's "clock" with network time service. 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. Not used by FreeFlow® Print Server.
ocfserv	OCF Service Use this option to enable the OCF service. This is a Solaris-provided "Smart Card" service. Not used by FreeFlow® Print Server.
rpc.cmsd	Use this option to enable a data base daemon, which manages calendar data backed by files in /var/spool/calendar.
rpc.rusersd	Use this option to enable Network Username Server services. This service generates intruder information about accounts. Not used by FreeFlow® Print Server.
rpc.rwalld	Use this option to enable 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 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 the RPC-based ToolTalk Database Server services. Not used by FreeFlow® Print Server.
rquotad	Use this option to enable 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.
rstatd	Use this option to enable the Kernel Statistics server service. The rpc.rstatd process is a server, which returns performance statistics obtained from the kernel uses rpc.rstatd to collect the uptime information that it displays. This is an RPC service. Not used by FreeFlow® Print Server.
~~rquotad~~	~~Use this option to enable 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 Service Engineers (CSE).

samba	Use this option to enable Windows File Sharing (aka SMB) and WINS services. This service used by Hot Folder Gateway and other client/server file access services (e.g., Print from File, Xerox Nuvera® Scan to File, EPC Scan Back). **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	Mail Service daemon Use this option to enable Mail services. Optionally, a customer may use sendmail to deliver notification of disk space low conditions, or password expiry warnings. Not used by FreeFlow® Print Server.
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. Not used by FreeFlow® Print Server.
slp	Service Location Protocol This service advertises network services hosted by Solaris platform (e.g., LP) to remote clients. Not used by FreeFlow® Print Server, but improves interoperability with Novell clients and Mac OS clients. These clients use legacy network protocols not used today.
ssh	Use this option to enable 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 remote login access over SSH only. You can use "secure FTP" (SFTP) to transfer files that ensure user authentication and encryption of data over the network.
~~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. Not used by FreeFlow® Print Server.~~
talk	Use this option to enable 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 a legacy Time Protocol service. This service is outdated, so recommend the NTP service. 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.
uucp	Use this service 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
~~ktkt_warn~~	~~Use this Client-side service to communicate from the FreeFlow® Print Server platform to a Kerberos server service. This service will renew TGT (Ticket Granting Ticket) automatically up to its max renewable lifetime and warns when the Kerberos ticket is about to expire. Configure this service in the /etc/krb5/warn.conf file. Not used by FreeFlow® Print Server.~~
~~ocfserv~~	~~OCF Service~~ ~~Use this option to enable the OCF service. This is a Solaris-provided "Smart Card" service. Not used by FreeFlow® Print Server.~~
WEBEM	Use this option to enable the Solaris Web-based Management service. This is a Solaris-provided server to comply with Common Information Model (CIM) requirements specified by Distributed Management Task Force (DMTF). Optionally required by customer system admin. Not used by FreeFlow® Print Server.
wins	Use this option to enable 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, Xerox Nuvera® Scan to File).

RPC Tab

The RPC tab in the properties for each security profile provides connection control for RPC, NFS, traceroute and Portmap services. The IP filter options for RPC services are:

1. Enable All Connections
2. Disable All Connections
3. Enable Specified Connections
    - Define remote host(s) and users that can connect using these services.

The FreeFlow® Remote Print Server (FFRPS) application relies on RPC services to make a connection with the Xerox® printer. If all RPC connections are disabled FFRPS access is denied, so it is suggested that the 'Enable Specified Connections' option is enabled with a list of remote hosts that are used for remote FreeFlow® Print Server administration.

Note: *The FreeFlow® Print Server platform denies access to the FFRPS (FreeFlow® Remote Print Server) application when assigning the Security profile to 'High'. Select the 'Enable Specified Connections' RPC option with the remote Windows hostname or IP address running FFPRS to grant access to this application.*

3.4 Creating Custom Security Profile

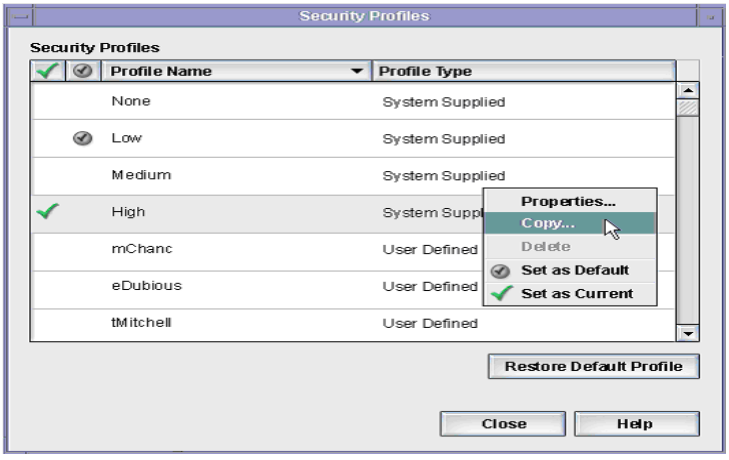
The system-supplied Security Profiles (i.e., Default Operating System Only, Low, Medium and High) are fixed, so non-modifiable. All of the options for changing Security settings or properties display as grayed out for these system-supplied profiles. A user with System Administrator privileges can create a "custom" Security Profile by copying one of the current system-supplied Security Profiles to a newly named profile.

The "custom" created Security Profile allows the option to enable/disable any of the services/features to best suit print/network protocol workflows and Security requirements. Unlike the system-supplied Profiles, you can edit custom Profile properties and/or deleted from the list of available security Profiles. We recommend you copy the 'High' security profile as a "custom" security profile, and open or close access to services as needed. Taking the approach of copying the lower system-supplied security profiles and closing access to services may result in human oversight errors, and could result in unnecessary Security vulnerabilities.

3.5 Setting the Current and Default Profiles

The System Administrator can select any Profile and set it as the 'Current' Profile, thus enabling the security settings for that Security profile. You must reboot the FreeFlow® Print Server platform after changing the 'Current' Security profile so the change will take effect. When a profile is enabled (i.e., set to 'Current') the setting will persist through FreeFlow® Print Server platform restarts and reboots.

Similarly, the administrator can specify a Security Profile as a 'Default' Profile. Specifying a Profile as default does not enable the Profile, but indicates that it will be the Profile setting, which persists across FreeFlow® Print Server software upgrades. By clicking the 'Restore Default Profile' option at the bottom of the Security profile dialog, the "Default" Profile can be selected as the 'Current' Profile. (Note that this operation will take several minutes to complete.). See the Security profile option in the Security Profiles UI screen below:



4.0 Managing User and Group Accounts

FreeFlow® Print Server users can access the system through the local GUI or remotely over the network the same as Solaris OS users. Any FreeFlow® Print Server GUI action or command line interaction is associated with a FreeFlow® Print Server user account. You create this association by the user logging into the FreeFlow® Print Server platform and is the basis for granting access (Authorization). A FreeFlow® Print Server GUI logon session (or logon session from a "local" terminal window) begins upon successful Authentication (verification) of a username and credentials (password). The logon ends by logging off which can be either user-initiated or system-initiated. Once the FreeFlow® Print Server GUI or terminal window logon session is established, the user can interact with the system, subject to the Authorization (i.e. Access Control Policies) associated with the settings of the 'Current Security' profile. 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).

You can define FreeFlow® Print Server user accounts either locally at the device or remotely from a trusted network Name Server (e.g., Microsoft Active Directory Service (ADS)). 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 to the access rights assigned to that group. You can assign multiple groups to a user, thus enabling membership in more than one group (e.g., the FreeFlow® Print Server Administrator could have a privileged Administrator account and a normal user account).

To ease transition from the legacy DocuSP user model, the FreeFlow® Print Server platform provides a set of default user accounts, one for each default User Group. See information about groups in section 4.4 "FreeFlow® Print Server *Built-In Group Accounts*". For customers that do not require authentication, you can configure the FreeFlow® Print Server platform to have the platform automatically log on using a default user account.

When you make any User and/or Group changes (such as new users) from the default settings will not persist over a FreeFlow® Print Server software upgrade or a software backup & restore. Therefore, it is very important to maintain records that illustrate the User and Group settings. This ensures the User and Group settings are recoverable on the FreeFlow® Print Server platform after a software upgrade or restore.

4.1 User Account Structure and Group Association

The FreeFlow® Print Server local user accounts are setup based on the Solaris user-operating model. A FreeFlow® Print Server user may be "locally authenticated" using the Solaris password database, or remotely authenticated using network authentication servers: NIS, NIS+, and Active Directory Services (ADS). Rules for the FreeFlow® Print Server user account are:

1. We assign each local user account to a "role", and has an associated username. The local username is typically between 2 – 8 characters in length and is case-sensitive. The Strong Password feature (described later in this document) increases the minimum password length.

2. The first character must be an alpha-character and the string must contain at least one lower case alpha-character.

3. The local username is a string of characters from the set of alpha-characters (a-z, A-Z), numeric characters (0-9), period (.), underscore (_), and hyphen (-).

4. A local FreeFlow® Print Server user account, once established, consists of the following attributes: username, password, user group, account disabled/enabled, and comments.

5. The maximum number of user accounts supported by the FreeFlow® Print Server platform is 25,000.

6. Each user account has an associated password. The password is a sequence of characters and is typically between 0-8 characters in length. The Strong Password feature (described later in this document) increases the required password length. As with all Solaris accounts, the password associated with a FreeFlow® Print Server user is case-sensitive.

7. To manage the access rights of a set of users as a collective group, you assign user accounts to a specific built-in FreeFlow® Print Server Groups. Each user account is a member of one group and is restricted to only one group.

4.2 Solaris OS-Level Built-In User Accounts

FreeFlow® Print Server software modifies the default Solaris OS installation: various Solaris services are disabled and Solaris built-in user accounts locked. The services and users modified for Security purposes are as follows:

1. nuucp account is locked
2. listen account is locked
3. adm, bin, daemon, listen, lp, noaccess, nobody, nobody4, sys, and uucp accounts are locked.

The Solaris utility services: “at, cron”, and “batch” can only be run by “system accounts”. Specifically, FreeFlow® Print Server improves system security by disabling the Solaris-default capability for a user to automate execution of “user level jobs” using these utilities. This eliminates the threat of a user installing a “Trojan Horse” or spy-ware software onto the FreeFlow® Print Server platform.

4.3 FreeFlow® Print Server Built-In User Accounts

The FreeFlow® Print Server platform is delivered with four “built-in” (aka “default”) login user accounts as follows:”

1. sa (System Administrator)
2. cse (Customer Service Engineer)
3. operator (Printer Operator)
4. user (Walk-up User)

You cannot remove the FreeFlow® Print Server 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 have accessed the system via the FreeFlow® Print Server GUI. Edit the FreeFlow® Print Server user Account Status (i.e., Enabled/Disabled) option to lock the user.

Note: *You should never disable the “sa” account to prevent all System Administrator functions so there is always an account available to manage FreeFlow® Print Server users and the FreeFlow® Print Server GUI services. It is advisable to configure more than one System Administrator for FreeFlow® Print Server GUI and User management. The System Administrator user (i.e., sa) can be unlocked and the password update with the root account.*

NOTE: *The Xerox Customer Service Engineer must have access to the "cse" password, "sa" password, and/or possibly the root password during a Service call. Alternatively, the Customer must be present to enter these passwords when required. The Xerox Service Engineers will not be able to perform their service call responsibility without appropriate access to the* FreeFlow® Print Server *platform.*

4.4 FreeFlow® Print Server Built-In Group Accounts

The FreeFlow® Print Server platform provides three default User Groups: "sa", "operator", and "user". You cannot edit, delete, disable, or remove these 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 is mapped to one of these default 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 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.

Note: *The* FreeFlow® Print Server *software grants user role and system access to a* FreeFlow® Print Server *user according to their associated* FreeFlow® Print Server *group membership.*

4.5 Managing User Accounts

The FreeFlow® Print Server GUI enables the System Administrator to manage accounts easily from the [Setup -> Users & Groups Management] UI window in the 'Users' tab. When the System Administrator selects the right mouse button in the window from the 'Users' tab, a pull-down menu appears with options to create, edit, delete, or enable/disable the account. If the assignment of an existing User to a Group needs modified, right clicking the mouse over the user ID and select the "Edit" pull-down option. Then modify the Group assignment.

When creating a new user account for the FreeFlow® Print Server platform it requires setting the User Name, Password, User Group and Account Status (i.e., Enabled/Disabled). You must assign any FreeFlow® Print Server user created from the FreeFlow® Print Server Users and Group Management UI window to one FreeFlow® Print Server group. The FreeFlow® Print Server software only allows user members of the System Administrator Group to use the FreeFlow® Print Server User and Groups Management UI window to create a new user account. The Account Status option represents locking and unlocking of the FreeFlow® Print Server user account.

Users assigned to the Users or Operators Groups will be assigned to a "restricted login shell" (rsh). The Solaris OS secures all user login sessions by limiting user access to programs and commands. Only the root account has full access to programs and the underlying file system (e.g., files and directories). Running the STIG hardening will enhance the Security tightening of user and file/directory access to meet DISA compliancy.

4.6 FreeFlow® Print Server XRXUSER Service Account

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 FreeFlow® Print Server service account only. Access to the xrxusr account via FTP, NFS, telnet, Samba, etc. is disabled. We recommend against editing of the xrxusr account settings using the SMC (Solaris Management Console) UI to unlock this account. Do not change the UID or 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, the System Administrator for the FreeFlow® Print Server platform should add/create additional user accounts via methods described in this document. Do not use the xrxusr account for any purpose, and create a new FreeFlow® Print Server user that will meet user access requirements for the FreeFlow® Print Server platform.

4.7 FreeFlow® Print Server Automatic User Account Logon

Users have direct access to the FreeFlow® Print Server platform by configuring the Automatic Logon feature in the Security Profile US window, and including via Web Print UI (HTTP) access, without having to Authenticate (i.e., type in their username and password). By default, Automatic Logion is "enabled" for the 'OS Only' Profile, and "disabled" for the 'Low', 'Medium' and 'High' Security Profiles. A member of the System Administrator group can re-configure this feature.

To disable the Automatic Logon feature without using the High Security Profile, you must create a custom profile under Security Profiles. A System Administrator disables the Automatic Logon feature by de-selecting the check box under the General tab in the new custom Security profile, and then select the 'Set to Current' option in the security profile dialog. When Automatic Logon is disabled and the Security profile is set to 'High', the FreeFlow® Print Server software will not launch completely until you select a user from the Login dialog and the password entered. This window will appear prior to display of the FreeFlow® Print Server GUI with a login dialog. A FreeFlow® Print Server user is required to enter their username and password before they can access the FreeFlow® Print Server platform through the GUI

When the System Administrator enables the Automatic Logon option, you must specify a FreeFlow® Print Server User account that will be use for the login. The standard walk-up user account is the default for automatic logon. The Administrator could configure any User account which has been set up in the 'Users & Groups Management' UI window.

Note: *When the Automatic Logon feature is enabled, users are not required to log on to gain access from the FreeFlow® Remote Print Service (FFRPS) application, the "local" GUI or the Web Internet Services UI.*

This "convenience feature" disables Logon Authentication and potentially a number of Authentication-controlled Security features; manage the Reconfiguration of Auto Logon carefully to prevent unauthorized access to the FreeFlow® Print Server *platform. The default configuration for Automatic Logon uses the standard built-in "User" account. Therefore, a "walk-up user" gains access rights of a standard User.*

However, if you define the Automatic Logon feature for a User in the System Administration Group, this action will effectively disable most Security controls enforced by the GUI and Web Internet Services UI. In this scenario, any "walk up user" and "Web Print User" gain access permissions normally reserved for the System Administrator Role. They now have nearly

unrestricted access to FreeFlow® Print Server *functions, system data files, customer data files, and can change all system security settings. Furthermore, if the Administrator "logs off" and signs back in as a "normal" user, they still have Administrator rights.*

4.8 FreeFlow® Print Server Automatic User Account Logoff

You can configure automatic log off a user on the FreeFlow® Print Server. We designed this feature to enable Automatic Logout in such a way that you can configure a timeframe from 1 to 10 minutes to represent the amount of inactive keyboard and/or mouse activity before the account logs off. You can access this feature from the [Customize ->Workspace Settings -> Home Screen] options from the main FreeFlow® Print Server GUI. When the timeout occurs, the FreeFlow® Print Server GUI access will logout the current user and switch to the built-n FreeFlow® Print Server 'user' account which has been configured for auto-logon. When a custom Security profile disables the auto-logon option, it forces a profile-defined user to log in again before displaying the FreeFlow® Print Server GUI. The procedures to enable Automatic Logoff are below:

1. [Customize -> Workspace Settings… -> Home Screen] in the FreeFlow® Print Server GUI.
2. Select the 'Enabled' radial button and enter the log-out timeframe for the user.

We disabled the XScreen saver in Solaris to give full control to the FreeFlow® Print Server GUI. Unfortunately, there is no way to currently lockout the Gnome desktop. The result is there is not linkage between the Screen Lockout and the Screen Saver features. You can setup the GNome desktop to enter a black screen mode

You can configure the 'Power Saver Setup' option so that the GNome desktop can enter a black mode. The screen will not be visible after a set timeframe when there is not keyboard/moue activity. This will also occur within 30 seconds of the print engine going into 'Power Saver' mode. These settings are persistent across restarts and reboots of the software. This acts as a screen saver that you can exit by touching the keyboard or moving the mouse. Therefore, this is not a secure option. You can access this feature as 'Monitor Off Mode' under the 'Printer' Menu -> 'Power Saver Setup' option.

The customer can secure the GNome Desktop and FreeFlow® Print Server GUI by making the settings below:

1. Enable Automatic Logout Feature
2. Setup High Security

A walk-up user to the FreeFlow® Print Server platform will only have FreeFlow® Print Server user access when you define the Security profile as 'Low'. There is no walk-up user access to the FreeFlow® Print Server software or Solaris OS once the Security profile is set to 'High'. The FreeFlow® Print Server software disables all features that would allow access (e.g., File Manager, terminal window, etc.) to the system when the Security profile is 'High', and a FreeFlow® Print Server user must enter authentication information to open the FreeFlow® Print Server GUI.

4.9 Managing User Account Lock-out

The list of locked Solaris built-in user accounts referred to above may be modified via a custom security profile (copy of the 'High' profile) under [Setup -> Security Profiles -> Custom Profile -> System] tab. There are many Solaris OS users and FreeFlow® Print Server users used internally by the software. The FreeFlow® Print Server users used by the software must not be changed or tampered with, or operation of the software could become inoperable.

You can use a FreeFlow® Print Server utility named 'lock-user' to lock all the users (e.g., 'lock-user all lock') on the Solaris / FreeFlow® Print Server platform except for root and the System

Administrator (i.e., sa). The 'lock-user' utility does not lock or unlock any FreeFlow® Print Server users added by the customer. We recommend using this utility to lock all the users, and then unlock only those users required by the customer. At a minimum, you may want to unlock the operator account (e.g., 'lock-user operator unlock'). This utility is not currently bundled with the FreeFlow® Print Server software but you can acquire it by the hotline or 3rd-level engineering.

Alternatively, you can use the Solaris password utility to lock (E.g., passwd –l <user>) and unlock (E.g., passwd –l <user>) users.

4.10 Solaris SCM User/Group Management

Although not recommended, if the System Administrator wants to permit a remote user to access the system, but does not want to make an external access user a member of a FreeFlow® Print Server Group, we recommend that the Administrator use the Solaris Management Console (SMC) application to create a new user.

Note: *User accounts which are created using SMC are not "known" to the* FreeFlow® Print Server *software and thus not visible to or accessible from the* FreeFlow® Print Server *GUI. The* FreeFlow® Print Server *GUI Console Logging mechanism does not log the login information for users created by the SCM application, or 'adduser' utility. The BSM logging will write the login information and Solaris-level user access information for these created users.*

Note: *SMC requires the use of "strong passwords" when creating a new account. (See Section 5.2 "Strong Password Settings" for more information on strong passwords). Such user accounts may not be compatible with some* FreeFlow® Print Server *applications that require factory-default passwords that do not conform to SMC's specific strong password requirements.*

4.11 Customize FreeFlow® Print Server User/Group GUI Access

The FreeFlow® Print Server System Administrator has the authority to disable/enable FreeFlow® Print Server GUI Management features (i.e., Job Management, Queue Management, Printer Management, Diagnostics, etc.) represented by FreeFlow® Print Server GUI pull-down items and Icon Shortcuts. You can access for the FreeFlow® Print Server User Group and/or the Operator Group, but NOT for individual FreeFlow® Print Server Users. Any FreeFlow® Print Server User that is created will be granted access (i.e., disabled or enabled) per their associated FreeFlow® Print Server Group (Administrator, Operator, or User) for these FreeFlow® Print Server GUI features

Note: *See section 4.12 "Customize User/Group Job Management GUI Access" for detailed information about customized access control of Job Management features. The Job Management feature in* FreeFlow® Print Server *v8 SP2 and above supports a fine-grained level of control over specific features that could otherwise allow a Walk-up User or Operator to have access to a customer's sensitive data. We have back-ported this feature to the* FreeFlow® Print Server *v7.3 software release.*

FreeFlow® Print Server GUI Access Control Management Features Table

FreeFlow® Print Server GUI Feature	User Setting	Operator Setting	Administrator Setting
Queue Management (New, Delete, Properties, etc.)	Disabled	Enabled	Enabled
Reprint Management The 'Limit Print Service Paths' in the Security Profile settings is used to control user access to Job Reprint directories that contain files. The default Reprint permissions assigned to each Security Profile are: - **OS Only Security**: Full Unix File System access, Saved Jobs directory, and CD-ROM (Removable Media) - **Low Security**: Saved Jobs and CD-ROM (Removable Media) - **Medium Security**: CD-ROM (Removable Media) - **High Security**: Nothing - **Custom Security**: SA User Defined	Enabled	Enabled	Enabled
Printer Manager (Finishing, Image Quality, Tray Setup etc.)	Disabled	Disabled	Enabled
Print Resource Management (LCDS Resources, PDL Fonts, Forms, etc.)	Disabled	Enabled	Enabled
Accounting and Billing	Disabled	Enabled	Enabled
System Preferences	Disabled	Can set International, Job Processing, Stocks & Trays	Enabled
Setup 1. (System configuration, Gateways) 2. (Feature licenses, Network Configuration) 3. (Security Profile, SSL/TLS, IP Filter) 4. (Users & Groups)	Disabled	View & Print only	Enabled
Change password	Self-Only	Self-Only	Enabled
Service Diagnostics	Disabled	Disabled	Enabled
Customer Diagnostics	Enabled	Enabled	Enabled
Backup& Restore	Disabled	Enabled	Enabled

4.12 Customize User/Group Job Management GUI Access

The FreeFlow® Print Server System Administrator has the authority to disable/enable access for each of the FreeFlow® Print Server Job Management GUI features (i.e., Preview, Preflight, Print From File, Job Forwarding, Accounting Information, etc.). You can apply these access controls to the FreeFlow® Print Server Group roles, and change access for the FreeFlow® Print Server User Group and/or the FreeFlow® Print Server Operator Group, but NOT for individual FreeFlow® Print Server Users. In addition, access of the Job Management features for the System Administrator group cannot change. This feature is a very important enabler for Xerox customers that required protection of PII (Personally Identifiable Information) and/or PHI (Protected Health Information) data for compliancy of Security standards such as PCI, HIPPA, Safe Harbor, etc.

In pre- FreeFlow® Print Server v8 SP2 software releases, we defined all Job Management features for the FreeFlow® Print Server Users, Operators and System Administration groups with a default enable or disable setting. The only option for these groups was to either 'disable all' or 'enable all' Job Management operations. The FreeFlow® Print Server v8 SP2 release and above provides a disable/enable access option for each Job Management function for each FreeFlow® Print Server group (i.e., Operator, or User), and each group has its own custom access profile listing all Job Management functions. We have back-ported this feature to the FreeFlow® Print Server v7.3 software release. When the FreeFlow® Print Server software is first installed the Job Management access setting for each feature is the same default as all previous software releases.

For example, a print shop may grant their Accounting department access to the FreeFlow® Print Server accounting data (i.e., for viewing, printing, etc.) by enabling the accounting controls for the FreeFlow® Print Server User Group. Another example may be denial of access to Job Preview and Preflight from the Operator Group so they are not able to view sensitive job data.

Any FreeFlow® Print Server User that is created will be granted access (i.e., disabled or enabled) per their associated FreeFlow® Print Server Group (Operator, or User) for these custom FreeFlow® Print Server Job Manager features. The default access level for Job Management features for the User, Operator and System Administrator groups has not changed with this feature. Refer to the 'Customizable Job Management Features Table' below for the default access just after installing the FreeFlow® Print Server software. Information to help read the table and understand the availability of the Job Management features is below:

Note: *The star symbol '*' proceeding a Job Management feature in the table means it is not supported in all printer products and/or when there are licensing requirements. These features are:*

1. ***Save Form location:*** *Only available on Monochrome/HLC printers.*
2. ***Thumbnail Preview:*** *Only available when licensed.*
3. ***Job Preflight:*** *Only available on Color printers when licensed.*
4. ***Process Job:*** *Only available on Color printers.*
5. ***Capture/Transfer Jobs:*** *Only available when licensed.*
6. ***PPML Repository Location:*** *Only available when licensed.*
7. ***LCDS Resource Manager GUI:*** *Only available on Monochrome/HLC printers.*
8. ***BGF Manager GUI:*** *Only available on Monochrome/HLC printers.*

Note: *Acronyms used in the table are:*

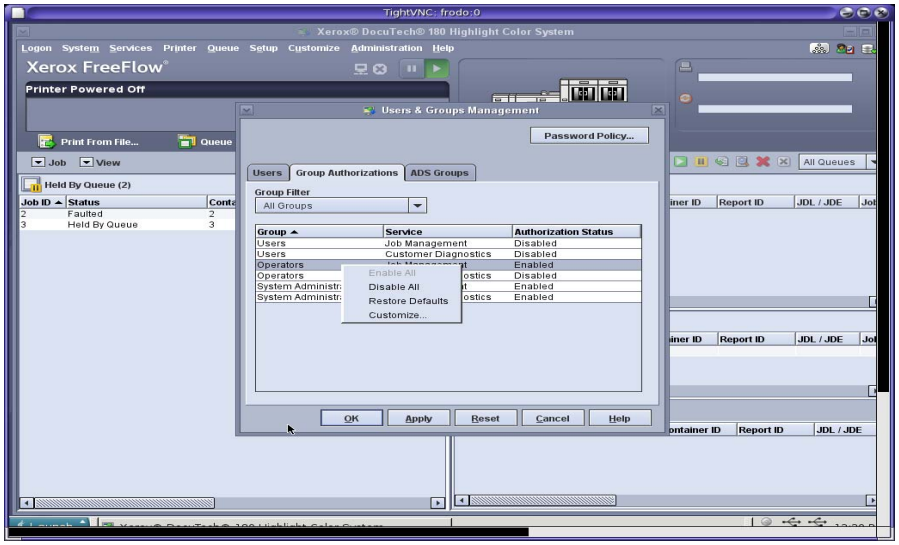
1. ***JM*** *= Job Manager*
2. ***QM*** *= Queue Manager*

3. ***SYS*** = *System Preferences*
4. ***BGF*** = *Background Form*
5. ***FFRPS*** = *FreeFlow® Remote Print Server*
6. ***ACCT*** = *Accounting*

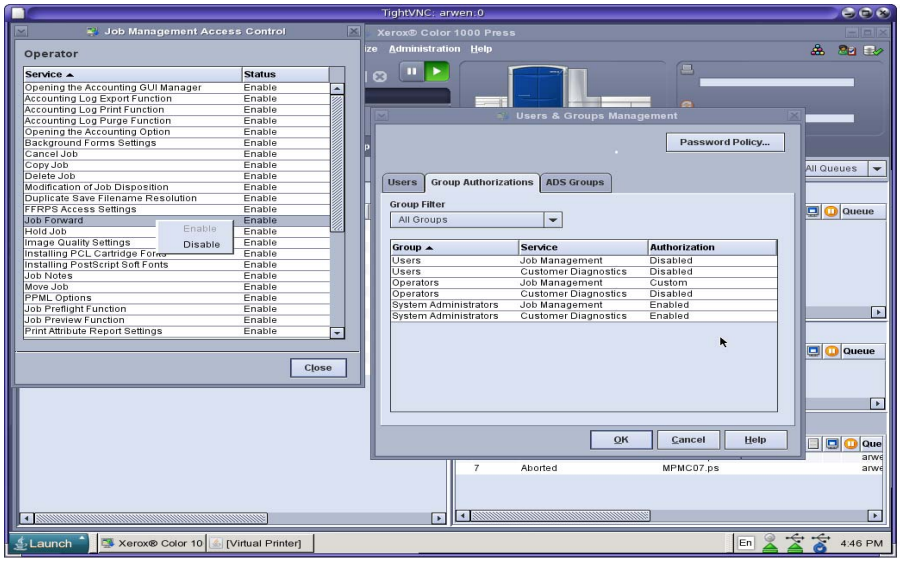
Customizable Job Management Features Table

Job Management Feature	GUI Location	Default User Setting	Default Operator Setting	Default SA Setting
Print From File	Services Menu & Shortcut Icon	Enabled	Enabled	Enabled
Modify Job Properties	**JM:** Job: Properties	Disabled	Enabled	Enabled
Disposition (Job Print/Save)	**JM:** Job: Properties: Settings: Destination	Enabled	Enabled	Enabled
Save Job Location (Job)	**JM:** Job: Properties: Settings: Destination	Enabled	Enabled	Enabled
Save Job Location (Queue)	**QM:** Properties: Destination	Enabled	Enabled	Enabled
Save Job Location (System)	**Setup:** SYS: Save tab	Enabled	Enabled	Enabled
*Save Form location (Job)	**JM:** Job: Properties: Settings: Destination	Enabled	Enabled	Enabled
*Save Form location (Queue)	**QM:** Properties: Destination	Enabled	Enabled	Enabled
*Save Form location (System)	**Setup:** SYS: Save tab	Enabled	Enabled	Enabled
Background Form (Job)	**JM:** Properties: Image Edit	Enabled	Enabled	Enabled
Background Form (Queue)	**QM:** Image Edit	Enabled	Enabled	Enabled
Background Form (System)	**Setup:** SYS: Save tab	Enabled	Enabled	Enabled
Print Banner Page	**JM:** Job: Properties: Settings: Admin Pages	Enabled	Enabled	Enabled
Print Attributes Report	**JM:** Job: Properties: Settings: Admin Pages	Enabled	Enabled	Enabled
Job Notes	**JM:** Job: Properties: Settings: Notes	Enabled	Enabled	Enabled
View Job Properties	**JM:** Job: Properties	Enabled	Enabled	Enabled
*Thumbnail Preview	**JM:** Job Options (job pull-down menu)	Disabled	Enabled	Enabled
Job Preview	**JM:** Job Options (job pull-down menu)	Disabled	Enabled	Enabled
*Job Preflight (Job)	**JM:** Job Options (job pull-down menu)	Disabled	Enabled	Enabled
*Job Preflight (Queue)	**QM:** Settings	Disabled	Enabled	Enabled
*Process Job	**JM:** Job Options (job pull-down menu)	Disabled	Enabled	Enabled
Release Jobs	**JM:** Job Options (job pull-down menu)	Disabled	Enabled	Enabled
Hold Jobs	**JM:** Job Options (job pull-down menu)	Disabled	Enabled	Enabled
Print Now	**JM:** Job Options (job pull-down menu)	Disabled	Enabled	Enabled
Proof Jobs	**JM:** Job Options (job pull-down menu)	Disabled	Enabled	Enabled
Forward Jobs	**JM:** Job Options (job pull-down menu)	Disabled	Enabled	Enabled
Move Jobs	**JM:** Job Options (job pull-down menu)	Disabled	Enabled	Enabled
Copy Jobs	**JM:** Job Options (job pull-down menu)	Disabled	Enabled	Enabled
Delete Jobs	**JM:** Job Options (job pull-down menu)	Disabled	Enabled	Enabled
Cancel Jobs	**JM:** Job Options (job pull-down menu)	Disabled	Enabled	Enabled
*Capture/Transfer Jobs	**JM:** Job Options (job pull-down menu)	Disabled	Enabled	Enabled
Duplicate Job Name Resolution	**Setup:** SYS: Save Tab	Disabled	Disabled	Enabled
*PPML Repository Location	**Setup:** SYS: PPML Tab	Disabled	Disabled	Enabled
Retain PDL Options	**Setup:** SYS: Job Processing Tab	Disabled	Enabled	Enabled
FFRPS Access	**Setup:** SYS: Remote Access Tab	Disabled	Disabled	Enabled
ACCT GUI Manager	**Administration:** Accounting	Disabled	Enabled	Enabled
ACCT Options (Logging/Purge)	**Administration:** Accounting	Disabled	Enabled	Enabled
ACCT Log Print	**Administration:** Accounting	Disabled	Enabled	Enabled
ACCT Log Purge	**Administration**: Accounting	Disabled	Enabled	Enabled
ACCT Log Export	**Administration:** Accounting	Disabled	Enabled	Enabled
*LCDS Resource Manager GUI	**Administration:** LCDS Resources	Enabled	Enabled	Enabled
*BGF Manager GUI	**Administration:** File Access	Disabled	Enabled	Enabled
Install PostScript Soft Fonts	**Administration:** PostScript/PDF/PCL Fonts	Disabled	Enabled	Enabled
Install PCL Cartridge Fonts	**Administration:** PostScript/PDF/PCL Fonts	Disabled	Enabled	Enabled
Sample Current Job	Printer	Disabled	Enabled	Enabled
Reset Job Id	System	Disabled	Disabled	Enabled

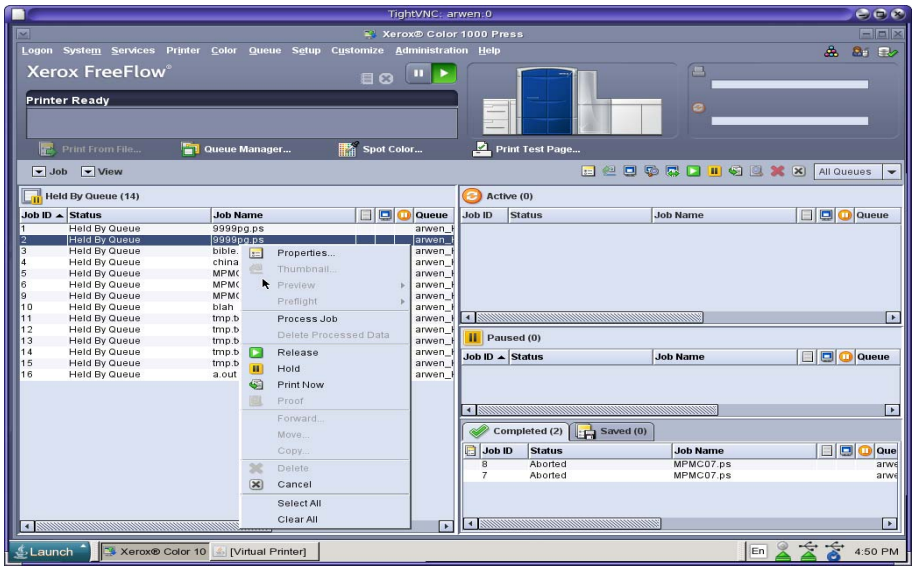
You can view and change the Job Management access control options from the [Setup -> Users & Groups … -> Group Authorization] tab illustrated below:



The screen image above illustrates the option menu when right clicking the mouse over the 'Operators' group for the 'Job Management' service. The 'Customize…' option will open the 'Job Management Access Control' UI window illustrated below:



These Job Management feature options can be individually disabled/enabled or as a group of features by highlighting many and toggling disabled/enabled. When you disable access for various Job Management functions (e.g., Thumbnails, Preview, Preflight, Forward, etc.) they gray out on the job in the FreeFlow® Print Server Job Management UI as illustrated below:



Some of the Job Management features (Save Job Location, Background Form, etc.) are available in multiple locations (Job, Queue and/or System Preferences) of the FreeFlow® Print Server GUI, and are all grayed out in all locations when the feature is disabled.

4.13 Microsoft Access Directory Services (ADS) Users and Groups

The FreeFlow® Print Server platform include ADS client services to support connection to a customer ADS domain running on Windows 2000 or higher. Once the FreeFlow® Print Server platform joins a customer ADS domain, an ADS user may log onto the FreeFlow® Print Server GUI using only their Microsoft Active Directory Services (ADS) user name and password. In this scenario, the user account should NOT be "created" on FreeFlow® Print Server platform, but must exist or be created on the customer ADS server.

ADS connectivity requires configuration of customer DNS server information on the FreeFlow® Print Server platform. You can configure the DNS information from the [Setup -> Network Configuration] pull-down option in the 'DNS' tab. In addition, the ADS user groups defined on the ADS server require mapping to their access role equivalent FreeFlow® Print Server group (i.e., System Administrator, Operator, and User groups). You can configure the ADS and FreeFlow® Print Server Group mappings from the [Setup -> Users and Groups Management] pull-down option in the 'ADS Groups' tab.. Enter the ADS Group names in the fields specified for each FreeFlow® Print Server Group. Once an ADS user logs into the FreeFlow® Print Server GUI, they will acquire the role and access permissions that are associated with their group.

4.13.1 Configure ADS Domain for FreeFlow® Print Server

The procedures for configuring an ADS Domain for the FreeFlow® Print Server platform are below:

1. Logon to FreeFlow® Print Server platform as a user who is a member of the System Administrators group.

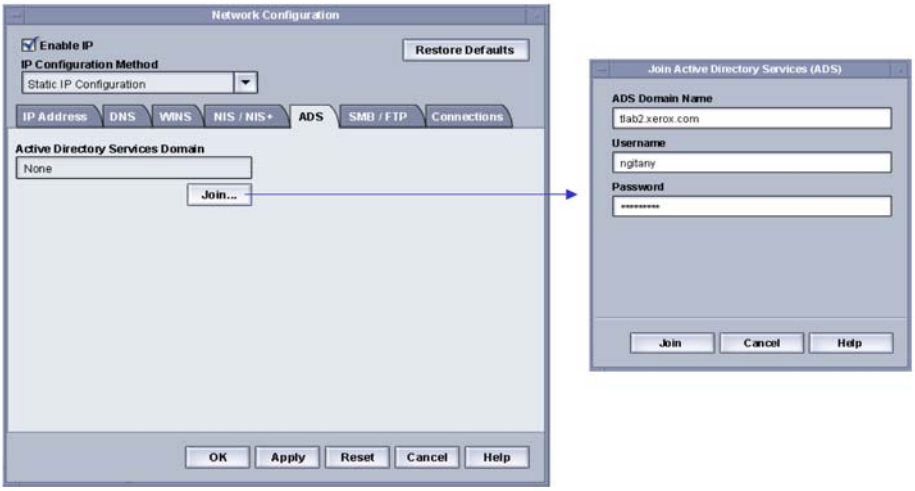
2. Select the DNS tab from [Setup -> Network Configuration] pull-down option. Make sure that you select the Enable DNS check box and that the DNS Server list is filled in with the appropriate IP addresses of up to three DNS servers to search when resolving the host names to IP addresses. (This is part of the network configuration procedure).

3. Under the ADS tab, enter in the "fully qualified domain name (FQDN)" of the ADS domain.

4. Click "Join…" button to have FreeFlow® Print Server platform join the ADS domain specified.

Note: *The Join... button will not be available if DNS is not properly configured. Verify that DNS is properly configure by attempting to ping a remote computer by its hostname.*

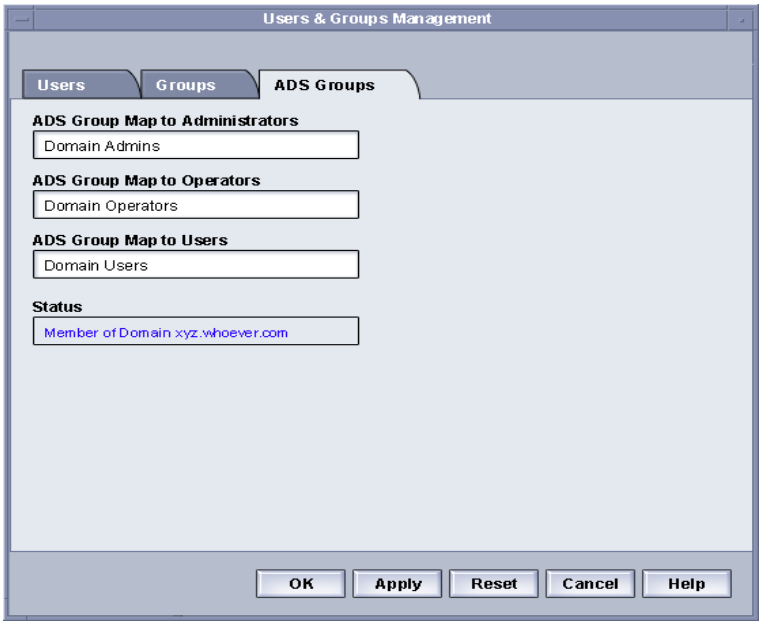
See the ADS Setup UI for ADS join below:



4.13.2 Mapping ADS and FreeFlow® Print Server Groups

Select the ADS Groups tab from the [Setup -> Setup/Users & Groups] pull-down option. Any member of the System Administrators group can specify, view and edit the mapping of ADS Groups to the three "built-in" default FreeFlow® Print Server user groups (Administrators, Operator, and Users) permitted to log on to the printer.

See the ADS Group mappings below:



4.13.3 Log into FreeFlow® Print Server GUI as ADS User

From the Logon menu, select ADS for authentication, then log on to the system with your ADS user name and password.

4.13.4 Troubleshoot ADS

A customer configures ADS services on a Windows-based server, and the FreeFlow® Print Server platform depends on these customer provided services prior to successfully joining the ADS network. The following provides a list of hints and tips to debug any FreeFlow® Print Server =reported ADS logon problem.

1. Make sure that you map valid ADS groups to corresponding FreeFlow® Print Server user groups.

2. Make sure that the user account can be logged into on a system other than FreeFlow® Print Server, via a Windows-based client configured to authenticate with ADS (to validate the user account is not disabled at the ADS server).

3. Do a simple verification to make sure that Kerberos is functional.
   - In a terminal window, as root, type: kinit <ADS username>

4. If kinit does not work, then ensure that the FreeFlow® Print Server has entries for both “forward” and “reverse” on the DNS server. Ensure you enter the DNS server setup information correctly into the FreeFlow® Print Server GUI.

5. Verify that the following files are correct:
   - /etc/defaultrouter
   - /etc/nsswitch.conf
   - /etc/resolv.conf
   - /etc/krb5.conf

6. Make sure the following link exists:
   - /etc/krb5.conf -> /etc/krbs/krb5.conf

7. If kinit works and you still cannot logon from the FreeFlow® Print Server GUI, check that the entry in /etc/gss/gsscred.conf is set to files, and not xfu.

8. Make sure that the /etc/pam.conf file contains the three FreeFlow® Print Server GUI entries. These entries are normally at the end of file and you should not comment them out.

Note: *The ADS services are not fully compatible with ADS Servers configured to support "IPv6-only". Configure the* FreeFlow® Print Server *platform and the ADS server for IPv6+IPv4 "Dual Mode".*

5.0 Managing Password Security

We ship the FreeFlow® Print Server platform by Xerox® with each FreeFlow® Print Server "built-in" user account assigned a "well known" password. The 'Change System Password' dialog window appears when the FreeFlow® Print Server software is re-installed or after running the sys-unconfig command. This prompts the person running this command to set new passwords for all built-in default User Accounts (root, system administrator, operator, user, and cse). For security reasons, it is highly recommended to change these well-known passwords from there default settings.

*sys-unconfig is a Solaris command provided to restore some settings for the Solaris OS and networking configuration back to a basic "as-manufactured" state and ready to be re-configured,

Note: *Do NOT enable the "Strong Passwords" feature in the GUI, and then perform a sys-unconfig or Software Upgrade install procedure. This can result in a lockout situation, which you can only remedy by re-installing the software. Disable "Strong Passwords" before performing the sys-unconfig or Software Upgrade.*

Note: *The Xerox Customer Service Engineer must have access to the "cse" password, "sa" password, and/or possibly the root password during a Service call. Alternatively, the Customer must be present to enter these passwords when required. The Xerox Service Engineers will not be able to perform their service call responsibility without appropriate access to the* FreeFlow® Print Server *platform. We recommend that the customer change these passwords for the CSE, and then put them back to their site-specific "secure" passwords after the CSE has completed the Service call.*

5.1 Changing User Passwords

There are two standard procedures to change password for a FreeFlow® Print Server user.

1 Users may change their own passwords from the [Logon -> Change Password] UI window in the FreeFlow® Print Server GUI.

2 A member of the "System Administrators" group can change the password of any FreeFlow® Print Server user on the system. To do so:

   a. From the [Setup -> Users & Groups -> Users] tab, double click on the user for which the password is being changed
   b. Select the 'Change Password' check box
   c. Enter the new password twice for verification
   d. Press the 'OK' button

5.2 Strong Password Settings

The FreeFlow® Print Server platform provides additional security for users required to adhere to stricter security guidelines, which require strong password policies. This feature can be enabled/disabled from the [Setup -> Users & Groups…'Password Policy …'] option in the 'Users & Groups Management' UI window. A "Strong 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{ . }.

There have been extra checks added to the Strong Password feature in the FreeFlow® Print Server v7.3 release and above. The FreeFlow® Print Server platform offers this password complexity feature with default settings to ensure compliance with the following Government STIG requirements:

1. **GEN000540:** The SA will ensure passwords are not changed more than once a day.
2. **GEN000700:** The SA will ensure passwords are changed at least every 90 days.
3. **GEN000800:** The SA will ensure passwords are not reused within the last ten changes.

The options available for configuring these extra Strong Password checks are:

1. **Maximum Age Weeks:** Use this parameter to define the number of maximum days 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 -52 weeks.

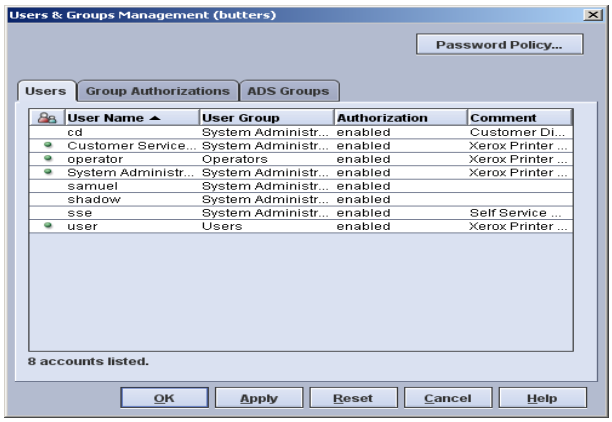
2. **Minimum Age Weeks:** Use this parameter to define the number of minimum days that a password must exist before they can change it. This parameter satisfied the Government STIG requirement GEN000540. The default value is 3 weeks, and the valid range is 0 -11 weeks. This parameter must always be less than the days defined by MAXWEEKS.

3. **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 -30 days.

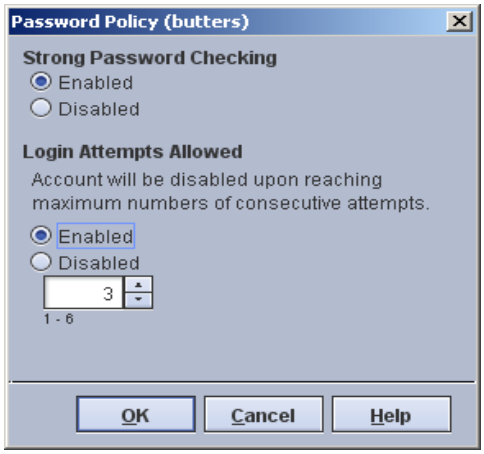
4. **Threshold:** Use this parameter to define the number of weeks prior to password expiry that a user is notified to change their password. The user login prompts to change the password once the password security reaches threshold. The default value is 14 weeks, and the valid range is 1 – 14 weeks. The parameter WARNWEEKS is the actual name that represents the threshold setting. This parameter is only meaningful when defined with the MAXWEEKS parameter, and must always be less than the weeks defined by MAXWEEKS. The 'Threshold' or 'WARNWEEKS' value starts when the FreeFlow® Print Server user password is changed, and represents the number of weeks after that password change.

5. **Minimum Password Length** Use this parameter to define the minimum number of characters a user must define for a strong 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.

The extra parameters that are defined by STIG requirements can only be defined when the "Strong Password' feature is enabled. Select the 'Users & Groups…' option from the 'Setup' pull-down menu in the FreeFlow® Print Server GUI to open the UI below:



Select the 'Password Policy…' option to display the 'Strong Password Checking' option as illustrated in the UI below:



In the FreeFlow® Print Server v7 and earlier releases, you can define the extra Strong Password parameters and/or change settings using a command line script as illustrated below:

1. cd /opt/XRXnps/ bin
2. chmod 744 config-strong-passwd-params.rb
3. ./config-strong-passwd-params.rb

A command line menu will appear as follows:

```
----------------------------------------------------------------------
The current setting for history is:                10
The current setting for minimum age weeks is:      3
The current setting for maximum age weeks is:      12
The current setting for minimum password length is:  8
The current setting for threshold is:              14
----------------------------------------------------------------------

Following are options for configuring strong password:
1 - Change history setting
2 - Change minimum age weeks
```

3 - Change maximum age weeks
4 - Change Minimum Password Length
5 - Change threshold value
6 - Reset to factory default values
7 - Exit
Please enter one of the option numbers above:

If there have already been rules defined for these parameters when they are changed, the new rules will be applied to all of the FreeFlow® Print Server users. For example, let us assume you enabled the 'Strong Password' feature on May 16 with maximum age weeks as 12. You changed the maximum age weeks to 6 weeks on June 16, so now the passwords for all FreeFlow® Print Server users will expire 6 weeks from June 16.

The recommended procedures to enable the Strong Password feature are as follows:

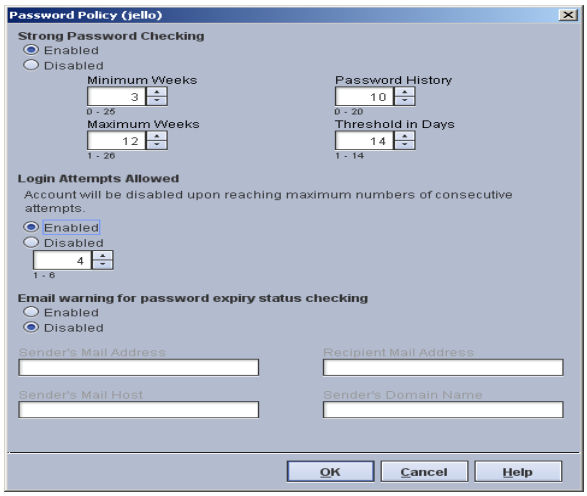
Note *This example defines a minimum length password of 14 characters.*

1. From FreeFlow® Print Server main GUI, logon as 'sa'
2. From FreeFlow® Print Server main GUI, go to 'Setup' -> 'Users & Group Management' -> 'Password Policy' option-
3. Select enabled for the 'Strong Password Policy' feature.
4. Open a terminal window on the FreeFlow® Print Server platform as root.
5. cd /opt/XRXnps/XRXsec/bin
6. chmod 744 config-strong-passwd-params.rb
7. ./config-strong-poasswd-params.rb
8. Select Option '2' and input "0".
9. Select option '4' and input "14".
10. Select option '6' to EXIT.
11. Run '/opt/XRXnps/XRXsec/bin/change_password_encrypt' script
12. Input '2a' to change the password encryption algorithm.
13. Change the FreeFlow® Print Server user password from the [Setup -> Users & Groups -> Users] tab. Double click the FreeFlow® Print Server user listed and change to a Strong Password.
14. Select the 'Change Password' check box
15. Enter a new 14 – 15 character password and retype for verification.

- e.g., Xxxxxx@1234567

16. Press the 'OK' button
17. Close the 'Users & Groups' UI window.
18. Open a terminal window on the FreeFlow® Print Server platform as root.
19. cd /opt/XRXnps/XRXsec/bin
20. chmod 744 config-strong-passwd-params.rb
21. ./config-strong-passwd-params.rb
22. Select Option '2' and input "2"
23. Select option '6' to EXIT.
24. Shutdown by typing 'init 5'
25. Power the FreeFlow® Print Server / Printer back on, and login with the new Strong Password.

In the FreeFlow® Print Server v8 SP2 and later releases, the 'Password Policy' UI has the additional Strong Password options and a new Password Expiry Mail Notification options. For more information, see section 5.7 "*Password Expire Mail Notification Feature*"'. See the illustration below:



For the FreeFlow® Print Server v8 and above releases, use the same FreeFlow® Print Server v7 procedures to enable Strong Password (and parameter changes) but use the 'Password Policy' UI window.

Notice that the maximum for Password History is a value of 20, which may not meet customer requirements if their policy expects a higher value. You can use a ruby script available on the FreeFlow® Print Server platform to set a Password History up to a maximum of 30. You can do this using the procedures below:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. cd /opt/XRXnps/XRXsec/bin
3. chmod 755 config-strong-passwd-params.rb
4. ./config-strong-passwd-params.rb

```
---------------------------------------------------------------
The current setting for history is:                10
The current setting for minimum age weeks is:      2
The current setting for maximum age weeks is:      12
The current setting for minimum password length is:  8
The current setting for threshold is:              14
---------------------------------------------------------------

Following are options for configuring strong password:
1 - Change history setting
2 - Change minimum age weeks
3 - Change maximum age weeks
4 - Change Minimum Password Length
5 - Change threshold value
6 - Reset to factory default values
7 - Exit
Please enter one of the option number above: 1
Executing Option 1...

---------------------------------------------------------------
The current setting for history is 10
Please enter a new value for history between 0 and 30: 24
```

```
---------------------------------------------------------------
The current setting for history is:                24
The current setting for minimum age weeks is:      2
The current setting for maximum age weeks is:      12
The current setting for minimum password length is:  8
The current setting for threshold is:              14
---------------------------------------------------------------

Following are options for configuring strong password:
1 - Change history setting
2 - Change minimum age weeks
3 - Change maximum age weeks
4 - Change Minimum Password Length
5 - Change threshold value
6 - Reset to factory default values
7 - Exit
Please enter one of the option number above: 7
```

Note: *You can also manage the settings for minimum and maximum password via the Security Profile (as originally designed) and modified by the "15-character password" update.*

Notes: *See the tips and hints below:*

1. *A* FreeFlow® Print Server *software restart is required when the Strong Password feature is changed.*

2. *The* FreeFlow® Print Server *Strong Password feature is independent of the OS-level strong password mechanism offered in the Solaris OS. Do not change the Strong Password feature parameters in Solaris to prevent password management problems. If you change the password, expiration parameters with Solaris utilities, the* FreeFlow® Print Server *users could locked-out without the* FreeFlow® Print Server *GUI knowledge of the settings.*

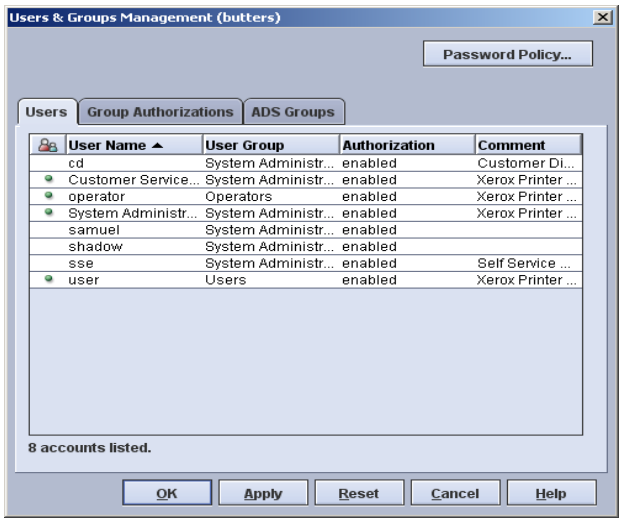
3. *A strong password cannot be set via the* FreeFlow® Print Server *GUI for root (su) account or any other Solaris user accounts not created by in the* FreeFlow® Print Server *GUI. The Solaris OS intentionally waives the Strong Password rules for the root account.*

4. *If you configure the NIS+ authentication service for the* FreeFlow® Print Server *platform, the NIS+ server enforces strong passwords setting from a centralized user database. Likewise, you can use an Active Directory server to manage Password Security options such as Strong Passwords. Once you join the ADS server to the* FreeFlow® Print Server *platform, all ADS user logins must adhere to the ADS server password policies.*

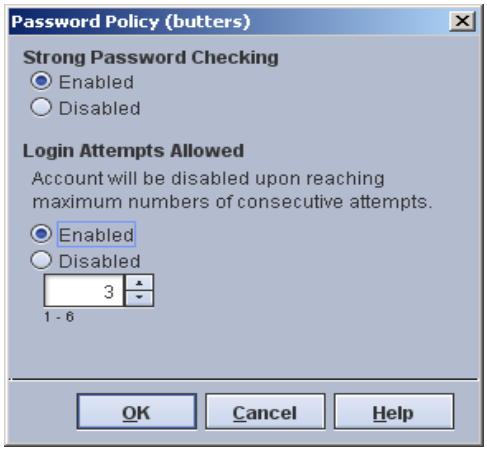
5.3 User Login Attempts Allowed

The FreeFlow® Print Server platform provides a setting to enable/disable the number of unsuccessful login attempts by the user before the account locks. You can access this feature from [Setup -> Users & Groups] pull-down option by selecting the 'Password Policy …' button in the 'Users & Groups Management' window. You can select a range of 1 to 6 for the number of logon attempts before locking out the account. The FreeFlow® Print Server platform default value is 3 for this feature.

Select the 'Password Policy…' option in the 'Users & Groups Management' UI illustrated below:



The UI dialog that is displayed for settig the 'Strong Password' and 'Login Attempts Allowed' features on FreeFlow® Print Server v7 and earlier releases is illustrated below:



Note: *The 'Password Policy' UI on* FreeFlow® Print Server *v8 SP2 and later releases will look like the screen image in the previous section 5.2 'Strong Password Settings". It has additional 'Strong Password' options and Password Expiry Mail Notification feature options.*

Notes: *See the hints and tips below:*

1. *The "lock out" policy applies to all system administrator group accounts as well as standard user accounts. In this scenario, only another System Administrator user, or the "root user", can re-enable the locked-out System Administrator account. The other recovery option is to "scrape re-install" the* FreeFlow® Print Server *software. See section 5.6 "*FreeFlow® Print Server *Administrator Lockout Prevention and Recovery" for a strategy to prevent the System Administrator lockout.*

2. *This function will only apply to failed logon attempts via the* FreeFlow® Print Server *UI and does not apply to the "root" user account.*

3. *If the customer is running NIS+ name service, this policy can be set by using the -a <# of allowed attempts> argument with rpc.nispasswdd. For example, to limit users to no more than four attempts (the default is 3), you would type 'rpc.nispasswd -a 4'. Only the root*

account on the local FreeFlow® Print Server *platform or defined on an NIS+ master server can make these changes.*

5.4 User Password Expiration

Although the FreeFlow® Print Server GUI does not provide the ability to set password expiration parameters on individual user accounts, there are a number of other ways to perform this task as follows:

1. Set via the passwd utility at the command line (i.e., see man pages)
2. Set via SMC (Solaris 10) console.
3. Assign some number of weeks for password expiration to the MINWEEKS and/or MAXWEEKS entries from the passwd file in the /etc/default directory. These values are set to null by default

Since the FreeFlow® Print Server UI does not handle password expiration; a detailed error message will not appear in a pop-up window prompting the user to enter a new password if his/her password has expired. Instead, the FreeFlow® Print Server software posts a generic message "Error: Password Verification has failed". Clicking "ok" should bring up a new window, which will allow you to continue by confirming the old password and typing in a new password. It is up to the customer to determine that the password has expired. To do so, a System Administrator can open a terminal window and attempt to login as the user in question. If the password has expired, the system will prompt the user to enter a new password.

The password expiration policies configured in the /etc/default/passwd file will apply equally to all FreeFlow® Print Server GUI-defined User Accounts. This policy implies that the System Administrator accounts will "expire" the same time the User accounts will "expire". System Administrators must plan accordingly and should not wait until the last minute to change their passwords. See section 5.6 "FreeFlow® Print Server *Administrator Lockout Prevention and Recovery*" for a strategy to prevent the System Administrator lockout.

5.5 User Password Lock/Unlock

Only a FreeFlow® Print Server user with System Administrator has privileges to unlock a locked out FreeFlow® Print Server user account. The System Administrator can lock or unlock an FreeFlow® Print Server user account either locally on the GUI, by a local command window (e.g., Start Menu -> Terminal), or by logging in remotely as the 'sa' user.

Note: *A local command window is not available in High Security Profile except for the root account. Optionally the SA can log in remotely with SSH to unlock a user account.*

You can unlock a FreeFlow® Print Server user account as the 'sa' or root account using the procedures below:

1. Use an "SSH client" software application from a networked client host.
2. Log into the FreeFlow® Print Server platform by typing 'ssh < FreeFlow® Print Server _hostname> -l sa'
3. Unlock the account by typing 'passwd –u <operator_account_name>'

If the System Administrator needs to lock any user account on the FreeFlow® Print Server platform, they can type 'passwd –l <user_account>' where 'l' is a lower case L.

An unlock utility named 'lock-user' can be used to lock all the users (e.g., 'lock-user all lock') on the Solaris / FreeFlow® Print Server platform except for root and the System Administrator (i.e., sa). The FreeFlow® Print Server software provides this tool as a convenience to facilitate locking and/or unlocking multiple user accounts at one time. This utility is not currently bundled with the FreeFlow® Print Server software but is available from the hotline or 3rd-level engineering.

If a System Administrator or Customer Service Engineer (CSE) account locks out on the FreeFlow® Print Server platform, it is possible to reset the passwords back to the default factory values from the terminal command window. You must know the root password in order to run a special command located in the /opt/XRXnps/bin directory. The command is:

/opt/XRXnps/bin/initialize-security-accounts

This command will change the passwords back to their factory default values. Reboot the FFPS platform into Single User Mode to accomplish this password reset.

Another way to accomplish this is to run the sys-unconfig command provided by Solaris; however; this action will require an understanding of system configuration options, and will reset more parameters than the default passwords.

The FreeFlow® Print Server software does NOT set a password retry lockout for the root account. The justification for this is the extreme measures required to access the FreeFlow® Print Server platform with a root lock out. The most likely recovery for such an event is a FreeFlow® Print Server software scrape install. If the customer is willing to accept that the FreeFlow® Print Server / Solaris software be scrape installed in the chance that the password is locked dues to exceeding a retry lock-out, then an update can be made for a password retry lock-out of the root account. Once you configure the FreeFlow® Print Server / Solaris system with a Security profile of 'High', additional IP filtering, and UDP/TCP port blocking, it is extremely difficult for anyone without the root password to access the Solaris OS and/or hard disk. All non-root accounts can only access the GNome desktop and FreeFlow® Print Server GUI when the system is Security tightened. The FreeFlow® Print Server System Administrator account can "secure" shell into the FreeFlow® Print Server / Solaris system using the SSH service, but even that can be disabled. Therefore, we have not had any customers requesting lockout of the root account after a log in retry count.

You can configure lockout after log in retry for the root as follows:

1. Edit the lock_after_retries in the /etc/user_attr to a value of 'yes'.
2. Edit the RETRIES parameter in the /etc/default/login file by removing the leading pound sign '#' comment.

The default retry attempts for root lockout is 5, and you can update this setting to meet the customer requirements. If the root account locks out after exceeding the number of logins per the retry setting, the FreeFlow® Print Server / Solaris software will require a fresh scrape installation. By default, the root account does not have access to log into the FreeFlow® Print Server platform remotely. We recommend the customer leave this default setting, and not allow any remote root logins.

5.6 Administrator Lockout Prevention and Recovery

It is important to identify a strategy to prevent the 'sa' account from locking without any way to unlock or reset the account.

5.6.1 Logout Situations

You can lock the SA account password under two possible conditions as follows:

1. A lock out situation can occur to the SA account when an attempt to log into FreeFlow® Print Server GUI fails the number of times allowed for the 'Login Attempts Allowed' option. The default number of retries for a successful login to the FreeFlow® Print Server GUI is 3 times. Anyone without knowledge of the actual "sa" password that attempts login could lock out the account. Someone could inadvertently lockout the System Administrator account if a CSE/Analyst (or anyone other than the actual System Administrator) exceeds the number of allowable login attempts because of not knowing the password.

   The FreeFlow® Print Server GUI will display a warning message indicating there is only 'n' number of login attempts allowed before the account is disabled. The message displayed is as follows:

   - "Invalid User Name or Password"

     "For security reasons, you now have one more login attempt allowed before your account is disabled."

     When this message is displayed do not attempt to login to the "sa" account unless you know the password. Type the password very carefully. Alternatively, the root users can reset a new password from a terminal window.

   When the last attempt to log into the SA account is an invalid password, the FreeFlow® Print Server GUI will display the following:

   - "You have exceeded the maximum number of allowed login attempts."

     "For security reasons, your account has been disabled. Contact your System Administrator for help."

2. Another way to experience SA account lockout is if you do not change the user password before the number of weeks defined by Maximum Age Weeks expires. This is a Password Security feature, which forces you to change your passwords prior to expiration. By default, FreeFlow® Print Server user accounts have 90 days before their password will expire. Allowing 90 days to pass without changing the SA password will result in an account lockout.

   It is highly recommended that the SA use a self-generated calendar or the '2.3.7 Password Expiry Mail Notification' feature as reminder to change passwords before they will expire. If the GUI displays a warning to notify the password will expire, the SA should do so as soon as possible.

If the "sa" changes their password in time, there is no lockout risk of any other FreeFlow® Print Server user since the SA account can unlock any of the other FreeFlow® Print Server user accounts.

5.6.2 Avoiding User Account Lock-out

Some of the measures to lessen the risk of the "sa" account locking out are:

1. The Xerox Customer Service Engineer (CSE) - uses the "cse" login account when performing service at the customer site. The CSE should never log into the FreeFlow® Print Server platform as "sa" without first obtaining approval and the correct password from the customer.

2. Increase the 'login attempts allowed' to 6 (max) before FreeFlow® Print Server accounts are locked out, or disable this feature. [Setup -> Users & Groups… -> Password Policy… -> Login Attempts Allowed] option.

3. Create a System Administrator equivalent user that can reset the original "sa" account if locked out. Select the [Setup -> Users & Groups…] pull-down option. Right click in the 'Users & Groups Management' UI Window and select the 'New…' option. Add the account lockout user name (e.g., reset_sa), password, and select the 'System Administrators' option for the 'User Group' pull-down menu. Close the Users and Groups Management UI windows.

4. Create an "sa" equivalent user some number of days after the Strong Password feature is enabled to ensure this account password is offset from the "main" "sa" account. The password expiration for the original built-in "sa" account will expire some number of days after enabling the Strong Password feature. Creating a System Administrator equivalent 7 or more days after enabling the Strong Password feature will prevent lockout of these two SA account roles at the same time. If the password for one of these System Administrator accounts is expired, the other account can perform the password reset to enable the account. This would also be a very useful strategy if one of the "sa" accounts is locked-out as a result of exceeding the configured 'Login Attempts Allowed' option.

5. You can accomplish another method to offset password expiration between "sa" accounts by changing an entry for the user in the /etc/shadow file. For example, you can create a FreeFlow® Print Server user named 'samuel' in the System Administrator group with an offset password expire date setting from the main "sa" account. Their /etc/shadow file entry is as follows.

   samuel:On6g/8LZ2CsDA:15111:21:84::::

   You can change the third field (15111) to move the password expiry date farther out than the main "sa" and other FreeFlow® Print Server users. To move the password expiry out 16 days add 15111 + 16 which is 15127. Update the third field of the /etc/shadow entry for samuel to 15127 and the password for this account will expire 16 days after the main "sa" account. Also, note that you can offset the password expiry data by creating a user some days after enabling the Strong Password feature. Their password will expire after the number of days set for the maximum age weeks starting on the account creation date.

6. Always change the SA password when logging in and the 'Warning' message appears indicating the password will expire, and to change the password.

7. Setup rules on the FreeFlow® Print Server platform that will send mail message notifications to the network or security administrator that warn the account password is about to expire and needs to be changed. To accomplish this see section 5.7 "*Password Expiry Mail Notification Feature*" below.

5.7 Password Expiry Mail Notification Feature

The FreeFlow® Print Server v7 and later software incorporates a feature to manage mail notifications for FreeFlow® Print Server user account expirations. This feature will allow IT/Security Administrators to setup FreeFlow® Print Server users so that they receives an email notification that the user account password is about to expire. These notifications will facilitate the need for changing the user password to prevent user account lockout.

The FreeFlow® Print Server v7 and later software incorporates a feature to manage mail notifications for FreeFlow® Print Server user account expirations. This feature will allow IT/Security Administrators to setup FreeFlow® Print Server users so that they receives an email notification that the user account password is about to expire. These notifications will facilitate the need for changing the user password to prevent user account lockout.

This feature is available to provide Network and/or Security Administrators methods for managing passwords of FreeFlow® Print Server users, and prevent "sa" account lockout on the FreeFlow® Print Server platform. It is important that that IT/Security Administrators prevent lock-out of the FreeFlow® Print Server "sa" account if the FreeFlow® Print Server platform is configured with maximum Security controls (e.g., High Security Profile, Terminal Window Access Disabled, etc.). A lock-out of the FreeFlow® Print Server "sa" account could result in the need to schedule a Xerox® Service call to manually recover the system or reinstall the software. For more information, refer to the section 5.6 "FreeFlow® Print Server *Administrator Lockout Prevention and Recovery*".

This feature does NOT enable receipt of inbound email messages by the FreeFlow® Print Server platform. There are inherent Security vulnerabilities and viruses with Mail Services, so inbound mail is discouraged to prevent Security risks. Mail messages are only outward-bound from the FreeFlow® Print Server platform to a pre-defined mail recipient that is interested in receiving password expiration notifications for of FreeFlow® Print Server user accounts.

The following section describes how the "sa" may configure the FreeFlow® Print Server Password Expiry Mail Alert options to setup mail notification warnings for FreeFlow® Print Server user account expiration. The options that are configurable for mail notification using the command line menu are as follows:

1. Sender Mail Account
   - This is the mail account used to send an expiry mail notification for a FreeFlow® Print Server user.
   - E.g., mailsa@xerox.com

2. Recipient Mail Account
   - This is the mail account on the customer network that will receive mail notifications that identify how long before FreeFlow® Print Server user accounts will expire.
   - This would typically be a Security or System Administrator IT team member.

3. Mailhost Server IP Address
   - IP Address of the network Mail Server.

4. Default Domain
   - This is the default customer DNS domain.
   - E.g., development.tc.company.com

5. Default Threshold
   - This is the default number of days prior to a FreeFlow® Print Server user account password expiring before sending a mail notification to the 'Recipient Email Address'.

6. Mail Alert Time
   - This is the time of day the mail notification to send the 'Recipient Email Address' to notify about password expiry.

7. Notification FreeFlow® Print Server User Accounts
   - Use this option for the FreeFlow® Print Server account(s) monitored for password expiry. A mail notification will be delivered to the 'Recipient Email Address' once the notification threshold is encountered.
   - E.g., "sa" Threshold = 10 days: 10 days before the "sa" password is expired the 'Sender Mail Account' will deliver a mail notification to the 'Recipient Mail Account' identifying how long before FreeFlow® Print Server users configured for mail notifications will expire.

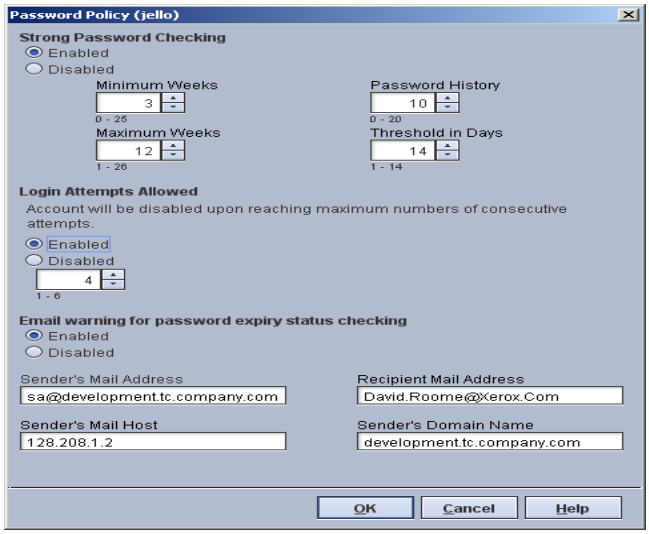
The following describes changes to the FreeFlow® Print Server user account settings that the "sa" must configure to support the Password Expire Mail Notification feature:

1. Enable the Strong Password feature. See the 5.2 '*User Strong Passwords*' section of this document for more details.

2. Set the minimum weeks (number of days a password must exist) and maximum days (number of days password can exist before expiring).

3. Change the password for all FreeFlow® Print Server users (sa, cse, operator and user). The FreeFlow® Print Server software will not have any knowledge of the FreeFlow® Print Server user passwords unless they are changed. You would make this update once at the time of enabling the "Password Expiry Mail Alert" feature.

In the FreeFlow® Print Server v8 SP2 and later software releases, the mail notification for password expiry settings are in the GUI in the 'Password Policy' UI dialog accessed from the [Setup -> Users & Groups -> Password Policy…] UI dialog illustrated below:



In the FreeFlow® Print Server v7 SP3 software release the mail notification for password, expiry settings are setup with a command line utility. After enabling the "Strong Password" feature, the email notification feature can be configured using utility below:

/opt/XRXnps/XRXsec/bin/password_expiry_alert_email_config.sh

The first time running this utility, it will prompt for the site-specific password expiry configuration parameters for setting up mail notification. See the standard output and example configuration of these parameters illustrated below:

```
Config file not exist, Running first time configuration...
Creating config file

Enter Sender mail ID: sa@development.tc.company.com
Enter Recipient mail ID: David.Roome@Xerox.Com
Enter Mail Host IP Address: 128.208.1.2
Enter domain name: development.tc.company.com
Enter Password Expiry Default Threshold value: 10
Enter Email Alert Time in 24hr format (hh:mm). Press Enter for Default Value (00:01):
09:00
Do you want to enter Threshold value for individual users ? (y/n): y
Enter Username: cse
Enter Threshold (Days before expiration reminder): 16
Do you want to add one more user? (y/n): n
Configuring cron job
Done...
Completed configuration Displaying menu.
Sending test mail with your configuration.
```

Once you define the initial configuration parameters, this utility will display the main Password Expiry Mail Alert Menu options illustrated below:

```
################################################################
     Password Expiry Mail Alert Configuration Menu
################################################################

1. Create / Display Mail Notification Settings
2. Modify Mail Notification_Settings
3. Add User Threshold (Days before expiration reminder)
4. Delete User Threshold
5. Enable / Disable Mail Notification
6. Send Test Mail Notification
7. Exit
```

The definition of these options are as follows:

1. Create / Display Mail Notification Settings:

   Use this option to create and view the configuration parameters for mail notification. The first time you select this option, it will prompt to create the initial configuration.

2. Modify Mail Notification_Settings:

   Use this option to modify the configuration parameters for mail notification.

3. Add User Threshold (Days before expiration reminder):

   Use this option to define the number of days prior to a password being expired for a FreeFlow® Print Server user account to expire. **E.g.,** Set a FreeFlow® Print Server user threshold of 10 days, and the recipient mail account will received mail notification 10 days before the users password expires.

4. Delete User Threshold:

   Use this option to delete the FreeFlow® Print Server user threshold setting. This will remove a custom threshold defined for this FreeFlow® Print Server user, and go back to the default user threshold.

5. Enable / Disable Mail Notification:

   Use this option to disable or enable mail notifications for password expiry. The FreeFlow® Print Server software will not deliver Mail notifications after disabling this option.

6. Send Test Mail Notification:

   Use this option to test the mail notification capability of this feature. This will result in the sender mail account sending a test mail notification to the recipient mail account.

Selecting option 1 'Create / Display Mail Notification Settings' will show the currently configured parameters as illustrated below:

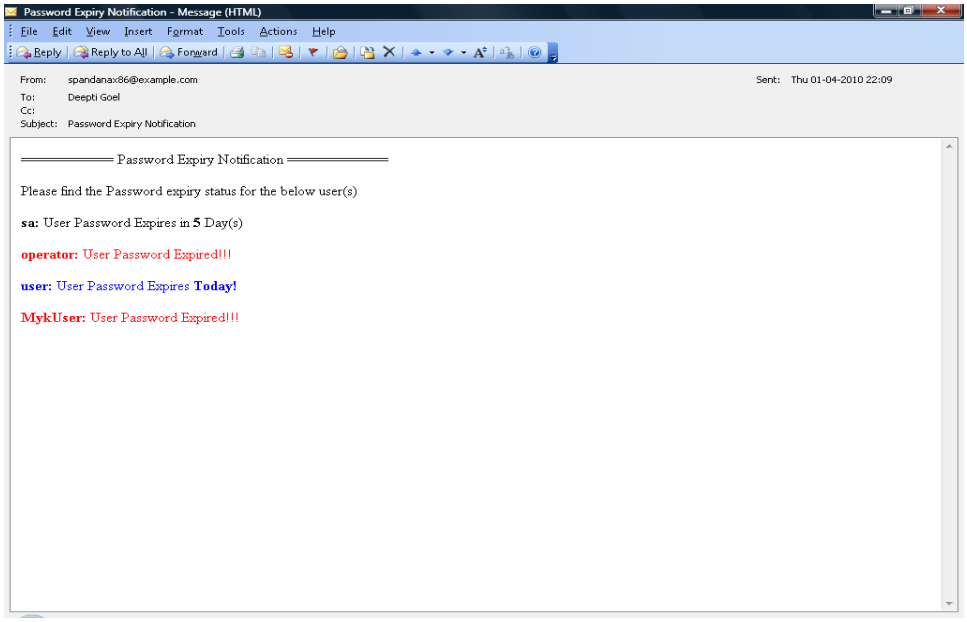
```
##############################################
Current config settings
##############################################

SENDER_EMAILID: sa@development.tc.company.com
RECIPIENT_EMAILID: David.Roome@Xerox.Com
MAILHOST: 128.208.1.2
DEFAULT_DOMAIN: development.tc.company.com
DEFAULT_THRESHOLD: 10
MAILALERT_TIME: 09:00
EMAIL_ALERT_STATUS: ENABLED
CONFIGURED_USER(S)_THRESHOLD: cse: 16

1. Display Mail Notification Settings
2. Modify Mail Notification Settings
3. Add User Threshold (Days before expiration reminder)
4. Delete User Threshold
5. Enable / Disable Mail Notification
6. Send a Test Mail Notification
7. Exit...

OPTION:
```

The FreeFlow® Print Server platform will send a mail notification to warm about an up-coming password expiry if the password age meets or exceeds the threshold limit for the FreeFlow® Print Server user. The configured sender mail account sends the mail message to the receiver mail account. See the mail notification warming about a FreeFlow® Print Server user password expiring example illustrated below:



6.0 Managing Print/Network Protocol and Filter Services

This section describes TCP/IP port designations, and methods to block, disable or enable Print/Network protocol services.

6.1 Print/Network Protocol <-> Port Mappings

See the Print/Network protocol services with associated TCP ports that the used for FreeFlow® Print Server / Xerox® printers support for workflows below:

Print/Network Services and Ports Table

Print / Network *Protocol*	Port	Job Workflow Facilitation And Considerations
FTP	21	The File Transfer Protocol (FTP) client/server 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. Another common workflow that uses FTP is Hot Folder. **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 highly secure network service used to protect TCP/IP based protocols with data encryption and an SSL certificate. There are several "secure" utility services (e.g., SSH or putty, SFTP, SCP, etc.) that access the FreeFlow® Print Server platform over port 22.
HTTP	80	This service is required to connect to the FreeFlow® Print Server / Windows® platform from an HTTP client, such as the Web Print client, Internet Print Protocol (IPP) service, JMF/JDF service, FreeFlow® Print Server Core, FF MakeReady, Remote Services, etc. The HTTP protocol is insecure, so the recommendation is to close port 80 in favor of using port 443 for a "secure" HTTP connection.
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 (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. Setting the Security profile to 'High' will close the Port Mapper service. There are RPC services are required by some 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 support older legacy versions of SMB no longer used unless a Windows® environment have old Windows® versions. Close these ports unless there are older Windows® client platforms on the network that required SMB services.

WINS NetBIOS	137	This service is required for Windows Folder Browsing and resolving Windows server names. E.G., 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. You can disable/disable the WINS service in the Options tab from [Setup/Network Configuration] 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. 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 from [Setup/Gateways] 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 MAC workstations. We recommend closing these ports The port services are 1. AppleTalk Routing Maintenance (201), 2. AppleTalk Name Binding (202), 3. Unused #1 (203), 4. AppleTalk Echo (204), 5. Unused #2 (205), 6. Zone Information (206), 7. Unused #3 (207), 7. Unused #4 (208).
SVRLOC	7000	The Service Location Protocol (SLP) protocol is for browsing remote file systems and is required when using NFS and Samba services.
SSL	443	The Secure Sockets Layer service provides encrypted and highly secure login and file transfer services. This service is required by client submission applications that support SSL/TLS (e.g., sHTTP, sIPP and SSH). This feature can be used for the Internet Web Services, IPP clients, JMF/JDF clients, FreeFlow® Print Server Core, Remote Services, and/or the FreeFlow® Make Ready (v2.0 or newer) submission clients. The specific Windows® service associated with this port is 'World Wide Web Services (HTTPS Traffic-In)'.
SMB (TCP)	445	The SMB (a.k.a., Samba) service provides Windows® Folder Sharing capabilities. Print from SMB, Scan to SMB, Hot Folder, etc. require this SMB service.
LPR	515	The lpr Gateway supports print job submissions from widely available lpr client workstations. The lpr print job submission method is the most widely used print protocol. It is an insecure protocol in that it does not support authentication or data encryption. However, there is no known way to exploit the FreeFlow® Print Server platform over port 515. Enable IPSec services to make lpr job submissions "secured".
IPP	631	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 [Setup/Gateways] in the FreeFlow® Print Server GUI. The IPP Gateway on the FreeFlow® Print Server platform services these IPP clients over port 631, and establishes a connection over port 80 to transfer

		print data. This is an insecure network connection with data transferring over the network in clear text. It is recommended to update the network connection over SSL and HTTPS (port 443) to make it "secure" for user authentication and data encryption capabilities
SUNDR	665	Use this service for a secure network file system on the FreeFlow® Print Server platform. The Secure Non-Trusted Data Repository (SUNDR)
NFS	2049	This is Sun's Network File Service. Use this folder-sharing service when clients want to export 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.
NFS Lock Service	4045	When NFS is used, this service protects files from corruption.
IPDS	5001	The IPDS workflow has a unique protocol service that uses port 5100 connecting to the FreeFlow® Print Server / Windows® platform and transferring print data.
Xsun	6000	The FreeFlow® Print Server Diagnostics service uses this port "internally" by the FreeFlow® Print Server Diagnostics software.
MemXfer	7000	This is a service used by the DT HLC and HLC Publisher printers to access needed services over the private network interface.
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.
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.
JMF (Hot Folder)	8181	This service handles JMF requests from a remote JMF client that transfers JDF and PDL files to a Hot Folder location for print scheduling.
Socket (Raw TCP/IP)	9100 9400	The Socket Gateway supports job submissions submitted over TCP/IP to a raw port service. The Xerox® 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.
SNMP v1/v2	16611	This service is required for exchanging SNMP v1/v2 messages. The SNMP v1/v2 version services are insecure, so the recommendation is to use SNMP v3 for a "secure" SNMP connection, and close port 16611.
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".*

Refer to the /etc/services file for a list of other ports used by the OS.

Note: *FreeFlow® Make Ready v2.0+ clients allow users to select whether or not the* FreeFlow® Print Server *platform they connecting to will have High Security enabled. If so, the client will use other communication paths such as sIPP (via SSL) for job submissions and SFTP for Decomposition Services (NetAgent). Alternatively, you can configure the FFMR application can be configured to use the 'lpr' utility to by-pass the "secure" encryption job submissions.*

6.2 Disable or Restrict Print/Network Protocol Services

Some print/network protocols are secure and others are insecure protocols. This is important to understand when making network Security decisions for Xerox® printer products that co-exist on a customer network. A secure print/network protocol is one that requires user credentials to access the FreeFlow® Print Server over that protocol, and requires encryption of both the credentials and the transient data transmitted over that print/network protocol. An unsecure print/network protocol is one that does not require user credentials and there is no encryption of the credentials and transient data.

There are several methods to restrict access, disable access or to remove Print/Network protocol services from the FreeFlow® Print Server platform to tighten up Security.

Restrict Client Access: The FreeFlow® Print Server GUI and Solaris provide several ways to restrict access to FreeFlow® Print Server -supplied print/network services. The FreeFlow® Print Server IP Filter feature will limit access to services such that they are only available to network Hosts and/or users specified in the IP filters configuration UI window. Although this does reduce Security risks, it is still possible for intruders to masquerade as one of the authorized Hosts and/or users in order to gain access to the FreeFlow® Print Server platform or execute a "man in the middle" attack.

Disable Services: There are Print/Network protocol services running on the FreeFlow® Print Server platform that not needed for the customer workflow, and therefore you can disable them to remove any potential Security risks. You can disable services by changing setup options on the FreeFlow® Print Server GUI, and/or using the "svcadm" command provided by the Solaris SMC tool. When services are disabled the software remains installed on the system, but they are not executed or running at system startup time. You can disable services from remote access by closing the UDP/TCP port that the service listens on when accepting remote connection requests. Use the FreeFlow® Print Server Port Management tool on the FreeFlow® Print Server platform to close UDP/TCP ports.

Remove Services: The most secure method for disabling Print/Network protocol services is to remove their packages from the FreeFlow® Print Server platform. Someone can restart a disabled Print/Network service, thus disabling is not an ideal solution for security. A careless System Administrator could restart a disabled service, and forget to disable after using the service. Worse, it is possible for an attacker who gains entry by compromising a network port to deliberately re-enable a service, and expand the security crack into a wide open door.

Warning: We recommend that an experienced Solaris System Administrator remove Print/Network protocol services not needed. Performing any step incorrectly or making a mistake during the process could damage the software and result in loss of customer data. A Xerox Service Engineer (CSE) may be need to complete software reinstall (aka "scrape install") to re-establish system operation if it had become inoperable. The removal of services is an extreme measure, which may result in unexpected system behavior or error conditions. Contact the Xerox Hotline for assistance in removing unnecessary protocol services.

6.2.1 SMB Services

The Samba services include Windows Folder sharing/browsing, Windows user-level authentication, and WINS (Windows Internet Name Service). These capabilities require the Microsoft "Server Message Block (SMB)" protocol. The installed packages for SMB services are as follows:

1. SUNWsmbac
2. SUNWsmbar
3. SUNWsmbau

The ports used by Samba for Windows Folder Sharing (i.e., also requires WINS) are:

1. 135 – used by older version of Windows (SMB)
2. 136 – used by older version of Windows (SMB)
3. 137 # NetBIOS Name Service (WINS)
4. 138 # SMB over NetBIOS using UDP/IP Datagram Service (Data Transfer)
5. 139 # SMB over NetBIOS using TCP/IP Session Service (Session Management)
6. 445 # SMB protocol over TCP/IP, without NetBios layer

To determine if these software packages are installed by do the following:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. pkginfo lgrep –i samba

To ensure existence of the latest Samba packages on the FreeFlow® Print Server platform, install the latest FreeFlow® Print Server Security Patch Cluster. You can identify the version installed as root user by typing:

/usr/sfw/sbin/smbd –V

SMB is considered a "unsecure' network protocol on the FreeFlow® Print Server platform, in that it does not support any user data encryption. The SMB service on the FreeFlow® Print Server platform does support an option to enable user authentication of user credentials. This authentication will validate user connections the same way as LanManager and Windows NT.

There FreeFlow® Print Server platform provides a utility to configure the SMB configuration to require user authentication from remote hosts. A remote Hot Folder user will be required to enter a static username and password prior to transferring files to the FreeFlow® Print Server platform. The procedures to enable this SMB authentication are as follows:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. cd /opt/XRXnps/bin
3. ./configure-samba-auth
   a. Select option 1, 'Enable authentication for Samba service and Hot Folders'
   b. Enter an SMB password when prompted.
4. Shut down the FreeFlow® Print Server platform completely and power back on.

If the customer uses SMB then this change will require use of a username and password for SMB authentication anytime SMB is used (e.g., Hot Folder job submissions).

Access to the SMB services on the FreeFlow® Print Server platform can be restricted to specific network Hosts using the IP Filter feature. Refer to section 6.4 "*FreeFlow® Print Server IP Filter*" for more information. One of the security disadvantages of the Samba services is that they emulate Windows legacy file sharing and there is no encryption technology built into the protocol. Specifically, user account passwords are sent "in the clear", and customer data is exposed to an attacker with access to the customer network.

If the customer FreeFlow® Print Server workflow does not require the SMB services, you can disable disabled to mitigate any potential Security vulnerabilities. The Hot Folder workflow can use Samba services for remote Windows users to transfer jobs into the Hot Folder directory, so disabling or removing SMB will disallow this workflow. Another method for using Hot Folder workflow is by transferring jobs from the remote Windows client into the Hot Folder directory using "secure" FTP (a.k.a., SFTP). The 'Print from File' job submission UI supports access to job files over a Samba share. The Xerox Nuvera® 'Scan to File' FreeFlow® Print Server GUI features support access to a Samba share for storing the scanned files. Removing the Samba services will constrain these features and result in error messages visible to the customer. To disable the SMB services on the FreeFlow® Print Server platform perform the following:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. svcadm disable samba
3. Shut down the FreeFlow® Print Server platform completely and power back on.

Older version of the DocuSP / FreeFlow® Print Server software ran on Solaris versions that did not support the svcadm utility. You can disable Samba on these older platforms using the procedures below:

1. Log into a terminal window on the DocuSP / FreeFlow® Print Server platform as root.
2. cd /etc/rc3.d
3. mv ./S90samba ./disable_S90samba
4. Shut down the FreeFlow® Print Server platform completely and power back on.

Another method to mitigate any potential Samba Security vulnerabilities is to remove the SMB packages using the procedures below:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. pkgrm SUNWsmbac
3. pkgrm SUNWsmbar
4. pkgrm SUNWsmbau

6.2.2 File Transfer Protocol (FTP) Services

Access to the FTP services on the FreeFlow® Print Server platform can be restricted to specific network Hosts using the IP Filter feature. For more information, refer to section 6.4 "*FreeFlow® Print Server IP Filter*". The port used by the FTP service is 21.

The FTP protocol is an "insecure' network protocol and SFTP is considered a "secure" network protocol. The SFTP uses SSH over port 22 to encrypt user credentials and data.

The Xerox Nuvera® and DT Highlight Color (HLC) printers require the FTP service on the "private network" between FreeFlow® Print Server and the print engine. Xerox Nuvera® also requires FTP services to access information on the FreeFlow® Print Server platform and for the 'Scan to File' feature from the FreeFlow® Print Server GUI. Therefore, you should not disable the FTP services for these printer products. For all other printer products, the standard FTP service on the FreeFlow® Print Server platform can be disabled which will also disable the Anonymous FTP service.

If a Xerox Nuvera® or DT HLC printer customer requires disabling of standard insecure FTP services from their public network. You can close port 21 with the Port Management Tool. You can close port 21 from the customer network interface, and the printer network interface continues to support FTP services.

When you disable standard FTP services from the Security Profile or port 21 is closed, secure FTP (SFTP) is still available to access the FreeFlow® Print Server platform for file transfers. The customer can download one of many available File Transfer programs for Windows that supports Secure FTP. The syntax for accessing Secure FTP on the FreeFlow® Print Server platform from windows is **sftp://<FreeFlow® Print Server hostname or IP Address>** with the username, password and port 22 parameters.

On product families other than Xerox Nuvera® and DT HLC printers, the FTP services on the FreeFlow® Print Server platform can be disabled/enabled from a custom Security Profile assigned as the 'Current' Profile. To disable or enable ftp open the 'Properties' window for the custom Security Profile and update this feature from the 'Services' tab. This will not affect the Anonymous ftp service on the FreeFlow® Print Server platform. To disable or enable Anonymous ftp open the 'Properties' window for the custom Security Profile and update this feature from the 'System' tab.

When you define the Security profile as 'High' the standard FTP, services are disabled. Secure FTP (SFTP) is available over top of SSH services, and can be used to transfer files securely to and from the FreeFlow® Print Server platform. With this approach, the client system must also have an "SFTP" software package (e.g., Free Flow Make Ready includes an SFTP client and "PUTTY" client for Windows).

Another method to mitigate potential FTP vulnerabilities is shutdown of the FTP services as follows:

svcadm disable svc:/network/ftp

In addition, you can remove the FTP application packages from the system permanently as follows:

1. pkgrm SUNWftpu
2. pkgrm SUNWftpr
3. pkgrm SUNWncft

6.2.3 Hot Folder Services

The Hot Folder services are available by enabling it on one or more of the FreeFlow® Print Server queues. The two methods for submitting jobs to the Hot Folder are SMB submission from a Windows client, or using the SFTP utility and transferring a job into the Hot Folder directory. It is recommended to use the SFTP utility given this job submission is "secure" by user authentication and data encryption. Use the procedures to configure SFTP Hot Folder workflow below:

Note: *Here is an example creating "secure" Hot Folder for a FreeFlow® Print Server user named Samuel.*

1. Enable hot folder for a FreeFlow® Print Server queue (samVP).
2. Create a FreeFlow® Print Server user (e.g., samuel) in the FreeFlow® Print Server GUI.
3. Change the home directory for user in /etc/passwd file for new user to /var/spool/XRXnps/hotfolders/samVP.
4. cd /var/spool/XRXnps/hotfolders
5. chown samfeng samVP
6. chmod 740 samVP
7. SFTP a job to the /var/spool/XRXnps/hotfolders/samVP directory.
    - Note: *The SFTP connection will land in the Hot Folder directory (samVP home directory).*

If there is more than one person requiring this workflow, create a new queue and user for each person. If one or more people share documents, a single queue and user can be setup for them.

If the customer insists on using SMB for Hot Folder submissions then you can enable user authentication using the procedures below:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. cd /opt/XRXnps/bin
4. ./configure-samba-auth
    a. Select option 1, 'Enable authentication for Samba service and Hot Folders'
    b. Enter an SMB password when prompted.
5. Shut down the FreeFlow® Print Server platform completely and power back on.
6. Run the security scan to validate mitigation of this vulnerability.

This change will require a standard username and password for all users submitting jobs to the Hot Folder. See section 6.2.1 "*SMB Services*" for more information.

6.2.4 Apache Services

Apache is a Web Server for the HTTP protocol. FreeFlow® Print Server software includes both Apache 2.0 and 1.3 as delivered with Solaris 10.

The FreeFlow® Print Server platform uses Apache 1.3 server as a "proxy server" for the iGen and XC 800/1000 printer families, to enable these Print Engines to connect with Xerox Diagnostics Servers.

The FreeFlow® Print Server platform uses Apache 2.0 server for the IPP job workflow over port 80. When using "secure' HTTP (SHTTP) these request are serviced by port 443 (SSL port). Port 80 is also required for Remote Services on iGen to facilitate outgoing data transfers.

The complete set of FreeFlow® Print Server Gateway services that rely on the Apache 2.0 services are:

1. IPP (Internet Print Protocol)
2. Web Internet Services
3. Scan to File (Xerox Nuvera® and EPC printers only)
4. Scan Back (EPC printers only)
5. Remote Services (iGen only)

Therefore, if the customer workflow requires one of the above listed network services, you should not remove the Apaches 2.0 server. See the packages that represent install of the Apache 1.3 and 2.0 service packages below:

1. *SUNWaclg:* # Apache Common Logging
2. *SUNWapchd* # Apache 1.3 Server Documentation
3. *SUNWapchr* # Apache 1.3 Root Components (Core Executables)
4. *SUNWapchu* # Apache 1.3 User Components
5. *SUNWapch2d* # Apache 2.0 Server Documentation
6. *SUNWapch2r* # Apache 2.0 Root Components (Core Executables)
7. *SUNWapch2u* # Apache 2.0 User Components

Get a list of the Apache software packages by doing the following:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. pkginfo lgrep –i apache

JDF Note: *If a customer requires submission of jobs to the* FreeFlow® Print Server *platform using a JDF workflow then the Apache 2.0 services are required. The FreeFlow® solution for JDF leverages the IPP Print protocol to achieve JDF workflow. Therefore, it is necessary to enable both the IPP and Apache 2.0 services on the* FreeFlow® Print Server *platform for JDT workflow.*

Apache HTTP is an "unsecure" network protocol on the FreeFlow® Print Server platform by default. However if the Apache HTTPS service is enabled for Web client access, then this is considered a "secure" network protocol with built in user authentication and data encryption capabilities. Tomcat is secure when HTTPS is used. The HTTPS service will listen on the SSL port.

If the customer FreeFlow® Print Server workflow does not require the Apaches 2.0 services, or the Apache 1.3 services for the iGen3 printer product, you can disable both Web Services to mitigate potential Security vulnerabilities. You can permanently disable the Apaches 1.3 and 2.0 services by removing them using the procedures below:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. pkgrm SUNWaclg
3. pkgrm SUNWapchd
4. pkgrm SUNWapchr
5. pkgrm SUNWapchu
6. pkgrm SUNWapch2d
7. pkgrm SUNWapch2r
8. pkgrm SUNWapch2u

The Internet Services Gateway (aka Web Print gateway) requires both the HTTP and the Apache Tomcat services, which are bundled in the Apaches 2.0 services package on the FreeFlow® Print Server platform. The HTTP protocol can be restricted to specific network Hosts using the IP Filter feature. For more information, refer to section 6.4 "*FreeFlow® Print Server IP Filter*". Other workflows that require HTTP services are JDF/JMF and Tape client.

The FreeFlow® Print Server platform incorporates the HTTP and Tomcat services represented by the XRXhttp and XRXtomcat software packages. Tomcat Web service runs over port 8009 and supplies Java Servlet runtime support and HTML responses for the FreeFlow® Print Server Web Print client (aka Internet Services Client) in support of Web Internet Services job submission and print job status.

If the customer FreeFlow® Print Server workflow does NOT require the Web Internet Services the "EPC Scan Back" feature, or IPP printing, then you can disable the HTTP and Tomcat services to mitigate or prevent any potential Security vulnerabilities. You can permanently disable the HTTP and/or Tomcat services by removing them using the procedures below:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. pkgrm XRXhttp
   - Internet Services Gateway (aka Web Print GUI)
3. pkgrm XRXtomcat
   - links to the Tomcat (Java-based) web server

The customer can remove the XRXhttp package if they wish to disable the Internet Web services only. Removing the XRXhttp package will also disable the 'EPC Scan Back' feature. This will leave the IPP services enabled.

6.2.5 Jetty Web Services

Jetty is a Web Server for Remote Services. FreeFlow® Print Server software includes the Jetty 5.1.2 Web Server package, which is a 3rd-party software package. The FreeFlow® Print Server platform incorporates the Jetty Web services on the FreeFlow® Print Server platform represented by the XRXrs software package. The port used by the Jetty Web service is LocalHost 6080 and this service is required for the Remote Services.

Jetty Web is a "secure" network protocol on the FreeFlow® Print Server platform. It uses HTTPS services to achieve user credential and user data encryption.

Customer concerns with the use of Jetty could be resolved by "disabling" this web server until such time that there is a need to upload the data to Xerox.

Note: *Refer to the Remote Services Customer Disclosure Letter included in the Remote Service upload package for additional information. We provide the customer this*

information prior to the agreement to the terms and conditions statement for FreeFlow® Print Server *Remote Services. Find additional information at the URL below:*

http://www.rs.docusp.xerox.com/registration/xrs/default.aspx?HOST=&SERIAL=&LOCALE=en-US

To disable the Jetty services on the FreeFlow® Print Server platform perform the following:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. /opt/XRXnps/XRXrs/bin/RS_Status.sh disable

You can permanently disable the Jetty Web services by remove them performing the procedures below:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. pkgrm XRXrsd

6.2.6 Remote Service (Xerox Debug/Diagnostics)

The implementation and applications use for Remote Services is can vary for different Xerox® printer products. In all cases, the delivery of debug information from the printer is over a 'secure' connection, and the connection is outbound only from the Xerox® printer. The Xerox edge host server receiving the Xerox debug information does not have access to the Xerox® printer. The Remove Services only allows Xerox support personal to access a printer at the customer location if the customer accepts the connection access.

6.2.7 Lpr Gateway Services

The XRXlprpap software package includes the lp/lpr services supported by the FreeFlow® Print Server platform. The port used by the lp/lpr service is 515.

LP/LPR is an "insecure' network protocol on the FreeFlow® Print Server platform. Access to the lp/lpr services on the FreeFlow® Print Server platform can be restricted to specific network Hosts using the IP Filter feature. For more information, refer to section 6.4 "FreeFlow® Print Server *IP Filter*" for more information.

You can disable the lp/lpr services for the FreeFlow® Print Server platform from the 'LPD' tab in the Gateways window, accessed from the 'Setup' pull-down menu in the FreeFlow® Print Server GUI. Although the lp/lpr Gateway workflow is insecure, there are not inherent Security risks when using lpr for job submissions. The lpr protocol is well defined and transfers data from the lpr client to the lpr server, so is unidirectional.

6.2.8 IPP Gateway Services

The IPP Gateway providing support for the Industry-standard Internet Print Protocol. Xerox delivers support for IPP client applications with FFMR and Print Driver software. In addition, several third party integrators that deliver IPP applications that work with the FreeFlow® Print Server platform. The FreeFlow® Print Server platform incorporates the IPP (Internet Print Protocol) services represented by the XRXipp software package. The port used by the IPP service is 631. The IPP service is a protocol built on top of Apache HTTP.

The IPP service is an "unsecure" network protocol on the FreeFlow® Print Server platform by default. However, if the IPP client uses the Apache HTTPS service then it is a "secure"

network protocol with built in user authentication and data encryption capabilities. Tomcat is secure when HTTPS is used. The HTTPS service will listen on the SSL port. The IPP services on the FreeFlow® Print Server platform can be restricted to specific network Hosts using the IP Filter feature. For more information, refer to 6.4 "*FreeFlow® Print Server IP Filter*".

The JDF/JMF and Free Flow Application Suite workflow to the FreeFlow® Print Server platform relies on the 'IPP' services; and therefore do not disable IPP services if the customer uses either of these workflows. If the customer FreeFlow® Print Server workflow does not require the IPP printing it can be disabled from the IPP tabs in the Gateways window which can be accessed from the 'Setup' pull-down menu in the FreeFlow® Print Server GUI. You can permanently disable the IPP Gateway services remove them by performing the procedures below:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. pkgrm XRXipp

6.2.9 FreeFlow® Remote Print Server (FFRPS) Services

The range of ports that must be open to support RPC services for the FFRPS application is quite vast and not conducive to network and device Security.

The FFRPS application service on the FreeFlow® Print Server platform will open a random OS-assigned port (e.g., port 9000) when initializing. An FFRPS remote client running on a PC will connect to FreeFlow® Print Server on the Solaris standard port 111 (RPC Port mapper), which chooses a port for an RPC-based service to handle remote requests. The Port mapper returns the assigned RPC-base service port to the requesting client. Once the FreeFlow® Print Server platform accepts the FFRPS request for connection the Port mapper returns the port number on which the FFRPS service is currently listening (e.g., port 9000). The FFRPS client connects on that port, and FFRPS service then opens other connections on additional unspecified RPC ports. The design of the FFRPS software requires the FreeFlow® Print Server platform (via the Solaris OS) to assign RPC ports, which could be any port above 32,000.

When the FFRPS application must connect to Xerox® printers through a router or firewall server, the customer network must allow RPC ports below 10,000, and RPC ports above 32,000 to be open. You can configure the customer's firewall by opening these ports only for the Windows workstation that is running the FFRPS application. To allow FFRPS connectivity through the firewall, request that the Security IT administrator at the customer location open all network ports for the Windows-platform running the FFRPS application. The Security profile setting of 'High' closes all ports available for RPC services. You can enable RPC services for specific remote hosts by specifying their IP address in the Remote Connection tab under the System Preferences in the FreeFlow® Print Server GUI.

We do not recommend any Security profile lower than 'High" for customers that are very sensitive and concerned about protecting their print data. However, the FFRPS client connection will fail if the Security profile on the FreeFlow® Print Server platform defines a 'High' setting. The FreeFlow® Print Server software blocks RPC ports above 32,000 when the Security profile is set to 'High', and therefore denies access to the FFRPS application. To allow FFRPS access when the Security profile is 'High', the System Administrator can add the remote Windows client running the FFRPS application to the RPC filter list from the 'RPC' tab in 'Properties' window for a Security Profile. The Windows client can be added after selecting the 'Enable Specified Connections' radial button.

If the Security IT Administrator at a customer location refuses to open all the ports between the Windows client running FFRPS and the FreeFlow® Print Server platform, another option is to setup and enable IPSec using pre-shared keys between the Windows client and FreeFlow® Print Server platform. Refer to section 7.2 '*FreeFlow® Print Server IPSec Protocol Security*' for more information about IPSec for the FreeFlow® Print Server platform. You can find this document at the URL below:

http://xww.docushare-xogpsg.world.xerox.com/dsweb/View/Collection-149460

- Make sure that you log into the above URL with your s3 credentials.

A customer can remotely manage the Xerox® printers over a "secure" connection with encryption by setting up IPSec services. These services will ensure encryption of communication and remove the network firewall requirement to open all of the network ports when the Security profile is set to 'High'. The reason is that the IP network protocol layer will act as a tunnel for the RPC request/reply packets. The customer is required to configure their network firewall to enabled passing of the IPSec packets. You can find information for setting up a firewall to support IPSec = at the URL location below:

http://xww.docushare-xogpsg.world.xerox.com/dsweb/View/Collection-149460

- Make sure that you log into the above URL with your s3 credentials.

6.2.10 Job Forwarding Services

The FreeFlow® Print Server / Printer configuration will no longer support Job Forwarding once the Security profile is set to 'High'.

Create a "custom" Security profile using the built-in 'High" profile, and enable the ICMP option from the Services tab. Jobs will successfully submit to remote printers after making this configuration setting.

The /opt/XRXnps/bin/filter-ports utility has an option to enable ICMP or ECHO (a.k.a., ping) for the FreeFlow® Print Server 7.3 software. The ICMP services can be enabled in the 'Services' tab of a custom FreeFlow® Print Server Security profile.

6.2.11 SNMP Services

Version 3 of the Simple Network Management Protocol (SNMPv3) published in IETF Internet Standard 62 in the RFC specifications below:

1. **RFC 3411:** An Architecture for Describing SNMP Management Frameworks
2. **RFC 3412:** Message Processing and Dispatching for the SNMP
3. **RFC 3413:** SNMP Applications
4. **RFC 3414:** User-based Security Model (USM) for version 3 of the SNMP
5. **RFC 3415:** View-based Access Control Model (VACM) for the SNMP
6. **RFC 3416:** Version 2 of the Protocol Operations for the SNMP
7. **RFC 3417:** Transport Mappings for the SNMP
8. **RFC 3418:** Management Information Base (MIB) for the SNMP

Additional RFC specifications that support the SNMPv3 protocol services are:

1. **RFC 3410:** The SNMP – An Introduction and Applicability Statements
   - An overview of IETF standard 62 (SNMPv3) is published as an informational RFC.
2. **RFC 3584:** Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
   - Different versions of SNMP interoperate as described by the following RFC.
3. **RFC 5590:** Transport Subsystem for the Simple Network Management Protocol (SNMP)
4. **RFC 5591:** Transport Security Model for the Simple Network Management Protocol (SNMP)
5. **RFC 5953:** Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)

The initial release of SNMP v3 supported a Security architecture per [RFC 2574], which includes a MIB for Security monitoring and managing the configuration parameters. It included procedures for providing SNMP message level security. There is user-role based Security associated with SNMP access to information, and use of HMAC-MD5-96 and HMAC-SHA-96 as the authentication protocols and the use of CBC-DES as the privacy.

RFC 3414 (obsoletes RFC 2574) is an update to the User-based Security Model mechanisms for the following security features:

1. Symmetric or private-key cryptography (username/passwords).
2. Digest computation with keyed hashing algorithms (message integrity)
3. Time indicators and automatic clock synchronization
4. Data encryption

SNMP v3 adds much stronger security features than SNMP v1/v2, such as client authentication, encryption of credentials, and encryption of bidirectional SNMP traffic. SNMP v3 ensures "secure" remote monitoring of Xerox® printers for IPv4 and IPv6 network addressing. FreeFlow® Print Server supports two implementations of SNMP (Net-SNMP and Epilog Envoy) and both of these support Trap Services. The ports used by the SNMP services are port 161 (Net-SNMP v3 Services) port162 (Trap Services), and port 16611 (Epilogue v1/v2 Services).

The latest implementation is Net-SNMP to incorporate SNMP v3 and is backward compatible for SNMP v1/v2. The Epilogue Envoy implementation continues to support SNMP v1/v2, which was the original SNMP implementation on the FreeFlow® Print Server platform. By default, the FreeFlow® Print Server software is setup to use the Net-SNMP v3 services, and acts as a proxy for SNMP v1/v2 client requests.

A benefit of the Net-SNMP proxy is it will "secure" the replies for SNMP v1/v2 requests from a remote client that supports SNMP v3 security. There are configuration elements for the SNMP v3 services, which can be setup. You can enable/disabled the SNMP Gateway services from the FreeFlow® Print Server GUI. When enabled, pre-defined default configuration elements allow the SNMP v3 services to be operational. It is highly recommended to change these configuration elements to customer site-specific parameter to "Secure" SNMP from the FreeFlow® Print Server platform.

SNMP v3 protocol on the Solaris-based FreeFlow® Print Server platform incorporates authentication and encryption Security using MD5 (Message-Digest algorithm 5) for negotiation of credentials (with password encryption) and DES (Data Encryption Standard), which is based on a symmetric-key algorithm that uses a 56-bit key. The Windows-based FreeFlow® Print Server platform incorporates authentication and encryption using the AES stream algorithm and DES block algorithm. Stronger encryptions algorithms could have been chosen but have performance impacts relative to DES encryption. Any customer that is concerned about network Security should always enable the SNMP v3 services for the Xerox® printer device to satisfy Security requirements.

You can use a command line utility on the FreeFlow® Print Server platform to configure SNMP settings to customer site-specific parameters. Leaving the default parameter settings is a Security risk. The parameters that are configurable for SNMP v3 with a FreeFlow® Print Server command line utility are:

1. Read-only Username
2. Read-write Username
3. Trap Username

   These are pre-defined settings with default values. The default values are 'XRdrivers' for Read-only Username, 'Xdrivers' for Read-write Username, and 'Xtrapusr' for Trap

Username. The FreeFlow® Print Server System Administrator must change these usernames to their own site-specific user account names. The username defined by the customer must be a FreeFlow® Print Server defined user, or Active Directory network defined user.

The user assigned to the 'Read-Only Username' configuration element will have access to read the FreeFlow® Print Server and/or Printer MIB databases. There is currently no support to write information to MIB databases. Therefore, there is no support to change the 'Read-Write Username' field. This feature will be forthcoming in a future FreeFlow® Print Server software release. The user assigned to the 'Trap Username' configuration element will have access to manage SNMP trap notifications. The user managing SNMP traps is granted access for these notifications when authenticated by the 'Trap PassPhrase' and a configured secure key that matches the one generated from the characters entered for the 'Trap PassPhrase'.

The PhasePhrase parameters that are configurable for SNMP v3 with the FreeFlow® Print Server command line utility are:

1. Authentication PassPhrase
2. Privacy PassPhrase
3. Trap PassPhrase

These are pre-defined settings with default values. The default values are 'snmpv3auth' for Authentication PassPhrase, 'snmpv3priv' for Privacy PassPhrase, and 'snmpv3trapauth' for Trap PassPhrase. The SNMP client user is restricted from accessing the FreeFlow® Print Server and/or Printer MIB database information unless they have the 'Authentication PassPhrase' and configuration for the secure key generated with the 'Privacy PassPhrase'. These PassPhrase configuration elements are defined default values initially after FreeFlow® Print Server software install. We recommend changing the Passphrase parameters to site-specific values for Security reasons.

SNMP v3 supports a new "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 as 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

The 'Privacy' and 'Authentication' algorithms options defined with the FreeFlow® Print Server SNMP v3 services are common algorithm(s) used by network SNMP clients such as HP OpenView, CentreWare Web and Xerox® Device Manager. The current cryptographic modules and encryption algorithms supported for SNMP v3 are as follows:

1. FreeFlow® Print Server Solaris-based Platform
    - Uses OpenSSL from Oracle Solaris® OS.
    - DES (Stream Encryption)
    - MD5 (Block Encryption)

2. **FreeFlow® Print Server Windows-based Platform**
   - Uses OpenSSL from Net-SNMP Library
   - DES (Stream Encryption)
   - AES (Block Encryption)

FreeFlow® Print Server software delivers an SNMP agent and MIB's on both the FreeFlow® Print Server platform and the Print Engine for all new printer products. We implemented a Proxy Agent configuration to retrieve MIB information from both the FreeFlow® Print Server platform and the Print Engine. The SNMP proxy uses the Epilogue Envoy SNMP v3 agent (a.k.a., NetSNMP-based) to retrieve MIB information from the FreeFlow® Print Server platform. The legacy configuration implemented a FreeFlow® Print Server proxy agent using SNMP v1/v2 services. The FreeFlow® Print Server SNMP proxy combines the FreeFlow® Print Server and Print Engine data response, and delivers it to the Remote Services SNMP client. We configure the SNMP proxy method for all FreeFlow® Print Server supported printers that do not have a PSIP platform.

Some printer products (e.g. XC 550/560, XC C75 and XC J75) that support either a Single or a Dual IP mode. Both of these network configuration modes support the SNMP proxy and hybrid proxy configurations. The SNMP proxy and hybrid proxy configurations retrieves Remote Services requested from the print engine over a "private" network when using Single IP mode, which is the most common configuration used by Xerox® printers today. The SNMP proxy and hybrid proxy configurations retrieves Remote Services requested from the print engine over the customer "public" network when using the Dual IP mode. The Single IP mode is a more "secure" method for the Remote Services SNMP client to retrieve printing information from the FreeFlow® Print Server / Printer platform, than the Dual IP mode. The Dual IP Mode setup retrieves printer information over the customer "public" network, so needs to be concerned about the Security of this Remote Services information data.

See the SNMP Proxy configurations per each printer product below:

FreeFlow® Print Server/Printer Product SNMP Proxy Configuration Table

Printer Product	FreeFlow® Print Server <-> Printer Private Network	SNMP Proxy	Hybrid SNMP Proxy
DP 4112/4127	X	X	
DP 4590/4595/4110	X	X	
DT 61xx	X	X	
DP 1xx EPS	X	X	
DT HLC	X	X	
XC 800/1000	X	X	
XC 560/570		X	
iGen® v3/v4	X	X	
Xerox Nuvera®	X	X	
DC 5000	X	X	
DC 700 (FFPS v8)	X		X
DC 700 (Pre-FFPS v8)	X	X	
DC 24x/25x/260	X	X	
iGen®3	X	X	
iGen®4	X	X	
iGen® 150	X	X	
XV2100	X		X
XV80	X		X
XC C75		X	
XC J75		X	
XC800i_1000i	X	X	
Impika iPrint	X	X	

Note: *The XV2100, XV80 printer products support single or dual IP configurations. The proxy agent retrieves SNMP information from the print engine over the "public" network for the dual IP configuration, and over the "private" network for the single IP configuration.*

6.2.12 Socket Gateway Services

The FreeFlow® Print Server platform incorporates Socket services represented by the XRXscktgw software package. Socket service is required by TCP/IP print clients which use "raw printing" over Port 9100 or 9400, such as the Xerox® Universal Print Driver, and Microsoft Print Driver. The port used by the Socket service is 9100 and 9400.

Note: *Some LCDS print clients also use the Socket services such as the FreeFlow® Print Server Tape Client.*

Socket printing is an "unsecure" print protocol on the FreeFlow® Print Server platform. The Socket services on the FreeFlow® Print Server platform can be restricted to specific network Hosts using the IP Filter feature. For more information, refer to 6.4 "*FreeFlow® Print Server IP Filter*".

If the customer FreeFlow® Print Server workflow does not require Socket printing it can be disabled from the 'Socket' tabs in the Gateways window which can be accessed from the 'Setup' pull-down menu in the FreeFlow® Print Server GUI. You can permanently disable the Socket Gateway services or remove them by performing the procedures below:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. pkgrm XRXscktgw

6.2.13 Remote Procedure Call (RPC) Services

The FreeFlow® Remote Print Service (FFPRS) software requires RPC services to communicate with the FreeFlow® Print Server and printer. Solaris network services such as NFS and NIS+ require RPC services. The FFPRS client accesses the FreeFlow® Print Server platform over port 111, which is the Port Mapper service. The Port Mapper service dynamically defines a new unique RPC port number selected from a range of high port numbers. The RPC Port service randomly creates additional "ephemeral" ports above port number 32767 depending on the RPC service requested.

The RPC service is an "unsecure" network protocol on the FreeFlow® Print Server platform. You can restrict RPC services on the FreeFlow® Print Server platform by limiting access to only specific network hosts. You can do this by selecting the 'Enable Specified Connections' radial button from the 'RPC' tab in 'Properties' window for a Security Profile. There is also a disable option (i.e., 'Disable All Connections') or enable (i.e. 'Enable All Connections') the RPC services from the FreeFlow® Print Server platform.

In addition, some individual RPC services can be disabled/enabled from a custom Security profile assigned as the 'Current' Profile. To disable or enable RPC services open the 'Properties' window for the custom Security Profile and update these features from the 'Services' tab. The list of RPC services that can be disabled/enabled are:

1. rpc.cmsd
2. rpc.rusersd
3. rpc.rwalld
4. rpc.sprayd
5. rpc.ttdbserverd

Note: *The FreeFlow® Print Server software denies access to the FFRPS (FreeFlow® Remote Print Service) application when setting the Security profile to 'High'. Select the 'Enable Specified Connections' RPC option with the remote Windows hostname or IP address running FFPRS to grant access to this application.*

6.2.14 Network File Services (NFS)

NFS enables FreeFlow® Print Server to be both a client and server of "NFS shared directories". Access to the NFS shares can be restricted to specific network hosts and/or users when the share defines these elements as filters. The NFS server will enforce file-access control using these NFS export filters and is not dependent upon the lower-level network access controls enforced by the IP Filter. You can layer NFS Share controls on top of IP Filter controls. The port used by the NFS service is 2049.these

The NFS service is an "insecure' network protocol on the FreeFlow® Print Server platform by default. The NFS client and/or sever services on the FreeFlow® Print Server platform are disabled in 'High' Security, or can be disabled/enabled from a custom Security Profile that is assigned as the 'Current' Profile. To disable or enable nfs.client services open the 'Properties' window for the custom Security Profile and update this feature from the 'Services' tab. The nfs.server services can also be updated from the 'Services' tab. The Xerox Nuvera® 'Scan to File feature requires the NFS services if scanning a job to an NFS repository.

The FreeFlow® Print Server software includes install of the XRXxdod package to support the legacy XDOD or DigiPath printing. That package defines an NFS share in the /etc/dfs/dfstab file as follows:

/usr/sbin/share -F nfs -o ro,nosuid /local/var/spool/data

The XDOD share is a Security exposure, which will trigger an NFS-related potential vulnerability by Security scan tools. We recommend commenting out or removing this share XDOD NFS entry. If the customer is still using the legacy XDOD workflow to the FreeFlow® Print Server platform then update the entry to restrict network host access as follows:

/usr/sbin/share -F nfs -o ro=<Host1>:<Host2>,nosuid /local/var/spool/data

You can shut down the NFS service as another method to mitigate an NFS-related potential vulnerability. Use the procedures below:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. svcadm disable svc:/network/nfs/status
3. svcadm disable svc:/network/nfs/nlockmgr
4. svcadm disable svc:/network/nfs/cbd
5. svcadm disable svc:/network/nfs/mapid
6. svcadm disable svc:/network/nfs/rquota
7. svcadm disable svc:/network/nfs/client
8. svcadm disable svc:/network/nfs/server
9. shut down the FreeFlow® Print Server platform completely and power back on.

Note: *Request a utility from 3rd-level engineering to disable or enable the NFS services.*

Move the NFS start-up script on older DocuSP software releases. You can accomplish this by performing the procedures below:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. cd /etc/rc3.d
3. mv ./S17hclnfs.daemon ./disable_S17hclnfs.daemon
4. Shut down the FreeFlow® Print Server platform completely and power back on.
5. Run a security scan against the FreeFlow® Print Server platform to validate mitigation of all NFS Security vulnerabilities.

6.2.15 Telnet Services

The Telnet service enables a user to log in remotely into the FreeFlow® Print Server platform. Telnet is an "insecure protocol" and not vulnerable across potentially insecure network connections. The SSH protocol service is a secure alternative to Telnet. There are free SSH clients available for most client platforms.

The Telnet service is a "insecure' network protocol on the FreeFlow® Print Server platform. I it recommended that the SSH utility be used rather than telnet. This will ensure user credential and data encryption. The Telnet services on the FreeFlow® Print Server platform can be disabled or enabled from the current custom Security Profile configured on the FreeFlow® Print Server platform. To disable or enable telnet open the 'Properties' window for the custom Security Profile and update this feature from the 'Services' tab.

The FreeFlow® Print Server software disables the Telnet service when defining the Security profile as 'Low', 'Medium' or 'High'. The SSH utility can be used to obtain a secure login to the FreeFlow® Print Server platform.

6.2.16 AppleTalk Gateway Services

The AppleTalk Gateway supports the legacy Macintosh OS Print clients using an Apple-proprietary print protocol known as PAP. Given the AppleTalk services run over an Ethernet network, Apple customers know AppleTalk network communications as "EtherTalk". These AppleTalk services run over the Ethernet network interface, but do not use TCP/IP transport services. Therefore, there is no Internet Protocol "port" associated with this AppleTalk Gateway. The software packages that represent the AppleTalk services incorporated on the FreeFlow® Print Server platform are:

1. XRXatcor
2. XRXatlkgw

AppleTalk/EtherTalk printing is an "unsecure" print protocol on the FreeFlow® Print Server platform.

If the customer FreeFlow® Print Server workflow does not require the AppleTalk printing, disable these services from the 'AppleTalk' tab in the Gateways window. You can access this setting from the 'Setup' pull-down menu in the FreeFlow® Print Server GUI. You can permanently disable the AppleTalk Gateway services by removing them using the procedures below:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. pkgrm XRXatlkgw
3. pkgrm XRXatcor

6.2.17 Novell Netware Gateway Services

The Novell Gateway supports the legacy Novell Netware OS Print clients using Novell-proprietary protocols known as IPX/SPX. Services named PServer and QServer emulate Novell NetWare print services on the FreeFlow® Print Server platform. These Netware services run over the Ethernet network interface, but do not use TCP/IP transport services. They use their own unique transport network services. Therefore, there is no Internet Protocol "port" associated with these Netware services. The software packages that represent the Netware services incorporated on the FreeFlow® Print Server platform are:

1. XRXnwcor
2. XRXnwqsgw

Novell printing is an "unsecure" print protocol on the FreeFlow® Print Server platform.

If the customer FreeFlow® Print Server workflow does not require the Netware printing it can be disabled from the 'Netware' and 'Queue Server' tabs in the Gateways window which can be accessed from the 'Setup' pull-down menu in the FreeFlow® Print Server GUI. Disabling the Netware Gateway will also disable the IPX/SPX protocols, which may be necessary to satisfy some customers concerned about potential vulnerabilities with these legacy protocols.

You can permanently disable the Novel Netware Gateway services by removing them with the procedures below:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. pkgrm XRXnwqsgw
3. pkgrm XRXnwcor

6.2.18 TotalNet Services

The FreeFlow® Print Server software incorporates a third-party software package called TotalNet to provide network connectivity services, and this software includes its own version of Apache 1.3 HTTP server to enable remote administration of network configuration services. The FreeFlow® Print Server System Administrator has authentication access to the TotalNet service. The TotalNet HTTP service is an "unsecure" network protocol on the FreeFlow® Print Server platform given it uses HTTP. We recommend disabling this older version of Apache, or the TotalNet packages be removed to prevent Security exposures. The port used by the TotalNet HTTP service is 7777 (sometimes 7778).

The FreeFlow® Print Server platform makes use of the Novell Netware SPX/IPX services that are included with the TotalNet software. Novell Netware clients on a customer network rely on these services for Novell connectivity to the FreeFlow® Print Server platform. Identify the existence of TotalNet service performing the procedures below:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. pkginfo lgrep –i totalnet

The listed packages for the TotalNet software are:

1. TAS
2. XRXnwcor

The TotalNet software includes its own version of HTTP services (Apache 1.3 sever). You will not need the HTTP services provided with the TotalNet software. We incorporated the TotalNet software to support AppleTalk and Netware, and bundled extra HTTP packages.

If network vulnerabilities are a customer concern, we recommended disabling these services. Any good Security scanner application will report Security vulnerabilities against the Apache HTTP services included with the TotalNet packages.

Assigning the Security profile to 'High' disables the HTTP service included with TotalNet. In addition, you can disable the TotalNet HTTP services on the FreeFlow® Print Server platform from a custom Security profile assigned as the 'Current' Profile. To disable TAS_httpd services open the 'Properties' window for the custom Security Profile and update this feature from the 'System' tab.

For legacy software releases, there are a couple of ways to disable the TotalNet services. One way is to rename the 'totalnet' directory that holds the software services by moving the TotalNet directory using the procedures below:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. cd /opt
3. mv ./totalnet ./disable_totalnet
4. Shut down the FreeFlow® Print Server platform completely and power back on.
5. Run the security scan to validate mitigation of this vulnerability.

Another method to mitigate TotalNet HTTP and Tomcat vulnerabilities is to move the start-up script. You can do this by performing the procedures below:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. cd /etc/rc3.d
3. mv ./S99TAS ./disable_S99TAS
4. Shut down the FreeFlow® Print Server platform completely and power back on.
5. Run the security scan to validate mitigation of any Apache 1.3 vulnerabilities.

Permanently disable the TotalNet services by removing the packages using the procedures below:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. pkgrm TAS
3. pkgrm XRXnwcor

6.3 FreeFlow® Print Server Port Management Tool

Solaris includes a Firewall capability called "IP filter" (IPF). FreeFlow® Print Server uses this IPF mechanism to deliver the GUI-based IP Filter functionality, which provides a basic capability to block remote clients from given IP addresses. However, some customers may require much more strict security barriers that block network services not required for their workflow. Once you identify a customer network/print workflows, you can close all UDP/TCP ports not used by network/print 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 these ports as potential vulnerabilities.

Customers may request specific ports to be "closed" or "blocked", or for the associated "services" to be "disabled" or "shutdown". If the customer workflow does not require the use of the reported open ports, and these are ports of concern to the customer, you can close or disable ports = using the FreeFlow® Print Server Port Management tool. This tool can be access

from the /opt/XRXnps/bin directory as 'filter-ports'. For example, if the customer would like port #427 closed they would use the procedures below:

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. cd /opt/XRXnps/bin
3. ./filter-ports
4. Select option #6 'Block Specific Incoming Ports'.
5. Enter 427
6. Select option #3 'udp/tcp'.
7. Exit the Port Management tool.

This tool blocks access to the ports from the "public network interface" on the FreeFlow® Print Server platform, but does not shut down the service associated with the port. For many customers, this remediation will be sufficient to meet security requirements. Blocking the UDP/TCP ports is effective to prevent network access of print protocols such as lpr, IPP, HTTP, etc. However, these services are still running internally on the FreeFlow® Print Server platform. Shutting these services down or removing their Solaris packages strengthens the Security of FreeFlow® Print Server.

Note: If the customer print workflow does not require a network service, improve the product security by taking action to disable the service. Completely removing network/print protocol Solaris packages is an even more reliable Security solution. This section provides information above in this section to perform section for specific Print/Network protocol services.

The Port Management tool is a firewall-enhancement capability that provides a very flexible way to disable/enable specific UDP/TCP ports. Once you clearly understand the customer workflow, unused ports that provide access to Print/Network protocol services in the customer workflow can be shutdown. A good approach is using option 1 to close all ports except SSH, and then open those ports required for a customer workflow.

Note: The ability to satisfy the very broad range of customer needs to block certain ports and yet leave other ports unobstructed in order to enable various print protocols and network services, requires a deeper level of technical expertise and high degree of flexibility not satisfied by the FreeFlow® Print Server *GUI today. The Port Management tool is packages on the* FreeFlow® Print Server *platform as a command line utility. Use of this tool requires knowledge of the port number to be blocked or unblocked.*

The install or presence of the Port Management tool closes various unnecessary ports by default to the public network interface:

1. 25 (SMTP email: not needed by FreeFlow® Print Server)
2. 681 (FreeFlow® Print Server internal service)
3. 1234 (FreeFlow® Print Server internal service)
4. 2020 (FreeFlow® Print Server internal service)
5. 4321 (FreeFlow® Print Server internal service)
6. 6000 (x11: used internally by FreeFlow® Print Server)
7. 7100 (font service: : used internally by FreeFlow® Print Server)
8. 9021 (FreeFlow® Print Server internal service)

By default, setting the Security profile to 'High' blocks ports greater than 32800 on the public network interface. Frequently, the RPC Port Mapper assigns ports above 32800 for RPC communication needed by FreeFlow® Print Server internal communications. Some customers are concerned that these "ephemeral RPC ports" are potentially vulnerable to attack and require closing. The FFRPS application has configuration option to dictate the RPC port(s) that it can use to make a connection to the FreeFlow® Print Server / Printer system. A strategy to limit the number of RPC ports is to define the RPC port(s) with the FFRPS application, and open those RPC ports on the FreeFlow® Print Server platform with the Port Management tool.

This would require that the Port mapper (port 111) be open, and the desired port(s) for the Xerox® printer connection.

Note: *The NFS client service, NIS+ client service, and* FreeFlow® Print Server *Remote Workflow client use "ephemeral RPC ports" in this number range. As an unavoidable side effect of disabling the amphoral RPC ports in High Security Profile, the disabling of remote access is also the effect of this setting. Ports and/or services may need enabling for customer requiring remote access such as us of the FFRPS application.*

6.4 FreeFlow® Print Server IP Filter

Remote hosts can be restricted from the FreeFlow® Print Server platform using the IP Filtering capability in the FreeFlow® Print Server GUI, and filtering on "IP-based" protocols such as LPR, IPP, HTTP, SMB, FTP, etc. This feature is a FreeFlow® Print Server interface to "SunScreen Lite" (Solaris 8 and 9) or the UNIX "IP Filter" (Solaris 10) firewall services that are part of the Solaris Operating System. Yu can access this feature = from the [Setup -> IP Filter] pull-down option in the FreeFlow® Print Server GUI. 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 to hosts not configured in the list of "Trusted hosts".

6.5 FreeFlow® Remote Print Server (FFRPS) Filter

An IP 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 from the [Setup ->System Preferences] pull-down option under the 'Remote Access' tab by adding the trusted host IP number. Once you have added one or more trusted hosts to this access control list, only those hosts in the list will have access to FFRPS service on that FreeFlow® Print Server platform. When the Security profile is set to 'High", this Remote Access filter must be enabled to allow remote FFRPS application access to connect and manager a Xerox® printer.

6.6 FreeFlow® Print Server RPC Filter

The IP Filter feature can also assist in limiting access to the FreeFlow® Print Server platform via RPC, including NFS, trace route, and Portmap. This filter can be setup for the current Security Profile in the RPC tab from the [Setup ->Security Profiles] pull-down option from the properties of that Security profile. Once you have added one or more trusted hosts to this access control list, only those hosts in the list will have access to the RPC services on that FreeFlow® Print Server platform. When the Security profile is set to 'High", this RPC filter must be enabled to allow remote RPC clients access to communicate with the FreeFlow® Print Server platform, and Xerox® printer.

6.7 Solaris OS IP Filter

You can create a custom IP filter configuration using the standard "IP Filter' (Solaris 10) firewall services that are part of the Solaris Operating system. We strongly recommend that the Port Management Tool be used to open and/or close print/network ports as a way to manage network Security on the FreeFlow® Print Server platform. This information to update the standard 'IP Filter' firewall service is a reference in case some specialized rule needs to be defined, and can't be done with the IP Filter or Port Management tool provided by the FreeFlow® Print Server software. However, the settings made in the 'IP Filter' configuration at the OS level gets over written by the FreeFlow® Print Server IP filter settings. Therefore, if a customer would like to define customized versions of the IP filter settings at the OS-level then you need to make a change to prevent the FreeFlow® Print Server software from overwriting this setup. You can define rules in the /etc/ipf/ipf.conf IP filter file to control access of Print/Network protocol services. To define a custom 'IP filter' at the OS-level for the FreeFlow® Print Server platform, perform the following:

1. cp /etc/ipf/ip.conf /etc/ipf/ip.conf_orig
2. Define the /etc/ipf/ipf.conf file with the rules to meet security requirements.

   ```
   ------------------------------------------------------
   #Always block external access to xfs
   ....
   ....

   ###Port Filter Rules###
   <<< PUT HERE >>
   ------------------------------------------------------
   ```

   Place the entries where is says 'PUT HERE' in the ip.conf file.

3. As root, type '**ipf –Fa –f /etc/ipf/ipf.conf**'
4. Edit the /opt/XRXnps/XRXscreen/bin/update-ip-filter file by adding a '#' comment character in front of the line:

   mv /tmp/ipf.$$ /etc/ipf/ipf.conf

   so that it looks like the following:

   # mv /tmp/ipf.$$ /etc/ipf/ipf.conf

5. Shutdown the DocuSP / FreeFlow® Print Server platform and then power it back up.

One other thing that needs understood is that changing the Security profile and/or any of the IP Filter settings from the FreeFlow® Print Server GUI will affect the manual edits in the ipf.conf file. For example, if you add a remote host to the IP filter list or change the Security profile from 'High' to a "custom" Security profile these changes will be removed. Therefore, make sure that all of the Security settings in made in the FreeFlow® Print Server GUI are complete (i.e., will not change) before manually updating the ipf.conf file. After you update the ipf.conf file, only make additional changes manually in the ipf.conf file.

If you make changes to one of the IP Filter mechanisms or a Security profile in the FreeFlow® Print Server GUI, it results in overwrite of any custom 'IP filter' defined at the OS-level = and no longer be applied on the system. Therefore, it is best to implement Security definitions in the FreeFlow® Print Server GUI first that meet all of the customer site Security requirements, and then make OS-level IP filter updates after. An example ipf.conf file that will shut down all Print/Network protocol services except for LPR and Port 9100 needed by the Xerox® Universal Print Driver print client is illustrated below:

```
#
# ipf.conf
#
# IP Filter rules to be loaded during startup
#
# See ipf(4) manpage for more information on
# IP Filter rules syntax.
# Following inserted by DocuSP#
# Always block external access to xfs
block in quick proto tcp from any to any port = 7100
block in quick proto udp from any to any port = 7100

### Port Filter Rules###

### Active Policy: TrustedFTPandNFSDisabled###
# rules for controlled internal interfaces
# allow everything from internal network
pass in quick on bge1 all
pass out quick on bge1 all

# Block FTP/NFS
block in quick from any to any port = 21   #ftp
block out quick from any to any port = 21  #ftp
block in quick from any to any port = 2049 #nfs

# General Security blocks
block in quick from any to any port = 22  #SSH
block in quick from any to any port = 80  #www
block in quick from any to any port = 137 #NetBIOS-SMB
block in quick from any to any port = 138 #NetBIOS-SMB
block in quick from any to any port = 139 #NetBIOS-SMB
block in quick from any to any port = 161 #NetBIOS-SMB
block in quick proto tcp from any to any port = 437   #smbprint
block in quick proto tcp from any to any port = 443   #ssl
block in quick from any to any port = 445 #NetBIOS-SMB
block in quick proto tcp from any to any port = 631   #ipp
block in quick from any to any port = 4045 #NFS
block in quick from any to any port = 4321 #rWhois
block in quick from any to any port = 6000 #Remote Sessions
block in quick from any to any port = 6001 #Remote Sessions
block in quick from any to any port = 7777 #Apache-Totalnet
block in quick from any to any port = 7778 #Apache-Totalnet
block in quick proto tcp from any to any port = 8080   #proxy
block in quick proto tcp from any to any port = 9400   #rawtcpprint

#allow TrustedDocuSP
pass in quick proto tcp from any to any port = 9400   #rawtcpprint
pass in quick proto tcp from any to any port = 9100   #rawtcpprint
pass in quick proto tcp from any to any port = 515   #printer

# allow TrustedDigiPath
pass in quick proto udp from pool/11 to any port = 111   #Portmap
pass in quick proto tcp from pool/11 to any port = 111   #Portmap

# block TrustedDigiPath from all others
```

```
block in quick proto udp from any to any port = 111   #Portmap
block in quick proto tcp from any to any port = 111   #Portmap

# Allow everything else
pass in quick all keep state
pass out quick all keep state
```

If any other print/network protocol workflow (i.e., other than lp/lpr or raw port 9100 socket job submissions) is required by the customer then the above ipf.conf file can be updated to open up the required ports.

7.0 Authentication / Encryption Protocol Security

Secure Socket Layer (SSL v.2 and SSL v.3) and Transport Layer Security (TLS) are network security protocols that encrypt and transmit data via HTTP and IPP over the TCP/IP network. SSL is an encryption protocol layer placed between a reliable connection-oriented network layer protocol and the application protocol layer. You have SSL/TLS enabled on the FreeFlow® Print Server platform once you import an SSL certificate or use the FreeFlow® Print Server built-in feature to create a "self-signed certificate" using the SSL Certificate options in the FreeFlow® Print Server GUI. The latest FreeFlow® Print Server software releases support 1024-bit SSL certificates.

Encryption can be setup in either of two modes, Normal or Secure with variable encryption strengths. When run in Normal mode, both encrypted and unencrypted transmissions are allowed using ports 80 (HTTP), 631 (IPP), and 443 (sHTTP and sIPP). In Secure mode, only encrypted transmissions are allowed using only port 443 (sHTTP and sIPP).

The certificate setup in the FreeFlow® Print Server GUI supports options for RC4 stream cipher, Data Encryption Standard (DES), and 3DES 128-bit encryption algorithms (block ciphers) to facilitate the secure exchange of print data between the job submission client and the FreeFlow® Print Server platform. The FreeFlow® Print Server platform supports Message-Digest (MD5) hash encryption algorithm, which facilitates the secure exchange of encrypted authentication data between the job submission client and FreeFlow® Print Server platform.

An optional method to update the hash encryption algorithm to Secure Hash Algorithm (SHA) and the cipher algorithm to Advanced Encryption Standard (AES) is available. The Internet Services Web client and clients using IPP can take advantage of SSLv3/TLSv1 protocols when submitting jobs to the printer.

Note: *SSL v2 was inherently flawed and its use is currently discouraged. The* FreeFlow® Print Server *software disabled the SSL v2 services by default in* FreeFlow® Print Server *8.0 software release and above. The following material about SSLv2 applies to all earlier releases. The HTTP client (a.k.a., Internet Services Web client) and the HTTP server (*FreeFlow® Print Server *Apache service) negotiate the version SSL protocol to use for data transfer and communication. For example, Internet Explorer 7 or FireFox 3 do not support SSLv2 and requires SSLv3 be used for HTTPS connections. Since the selection and use of client software is a customer responsibility, they are responsible to discontinue the use of clients, which require support for SSL v2. If a customer requires stronger enforcement measures for ensuring SSLv3 is used, refer to section 7.1 "Enabling SSL/TLS and Certificate Setup" for a procedure, that disables SSLv2 support.*

Note: *If using FreeFlow®* Make Ready *2.0+ workflow and the client is set to run with High Security mode, you need to enable the SSL/TLS option on the* FreeFlow® Print Server *platform. There is NO dependency on the* FreeFlow® Print Server *Security Profiles to establish a secure connection between the client and server. You can establish a secure connection between the FreeFlow®* Make Ready *client and* FreeFlow® Print Server *platform even if the Security profile is set to 'OS Only'.*

7.1 Enabling SSL/TLS and Certificate Setup

You can only enable SSL/TLS when there is an installed digital certificate on the FreeFlow® Print Server platform, using the [Add Certificate] button in the [Setup -> SSL/TLS…] pull-down option in the FreeFlow® Print Server GUI. Only a FreeFlow® Print Server user with System Administrator privileges have authorization to install a digital certificate on the FreeFlow® Print Server platform. The administrator selects SSL/TLS from the [Setup -> SSL/TLS…] pull-

down option and clicks on the [Add Certificate] button. This invokes the Add Certificate wizard. There are two options available when creating a digital certificate, "Self-signed certificate" or "Signed Certificate from a Certificate Authority". Use a Self-signed security certificates when the customer policy does not require the use of certificates verified by a third party Certificate Authority. You can install and use a Signed Certificate from a Certificate Authority if such a requirement exists.

For a Self-Signed Certificate, FreeFlow® Print Server creates and "signs" the certificate. The administrator needs to supply the fully qualified domain name (FQDN) or the IP address of the FreeFlow® Print Server platform, organization, and Country of the Certificate Authority. The FreeFlow® Print Server administrator can send the certificate information to a Certificate Authority (CA) if they want to install an "officially" signed SSL certificate. The Certificate Authority then returns a valid "signed "certificate that must be loaded and installed on the system.

Note: *A self-signed certificate is the most convenient way to begin using SSL/TLS and does not require the use of a server functioning as a Certificate Authority or a third party Certificate Authority. However, a self-signed certificate is not as secure as a certificate signed by a Certificate Authority. We recommend not creating an SSL certificate using the MD5 digest encryption algorithm. It is prone exploitation from an* FreeFlow® Print Server *client by means of man-in-the middle attack. Thus it is recommended that a more secure certificate be created by a reputable 3rd-party Certificate Authority.*

Note: *In* FreeFlow® Print Server *8.0, there is a Security Profile control to disable the use of MD5 when creating a self-signed certificate. In High Security mode, we replaced MD5 is replaced with the more secure SHA1 signing algorithm. You can also enable this feature by creating a Custom Profile with SHA1 enabled on the "System" tab.*

Once you install the Digital Certificate, the Enable SSL/TLS selection becomes available among the [Setup] options. At that time the administrator can select the "SSL/TLS mode of operation", Normal or Secure, from a drop-down menu. We highly recommend setting 'Secure' for the "SSL/TLS mode of operation" to force user authentication and password/data encryption from all HTTP clients accessing the FreeFlow® Print Server platform.

The FreeFlow® Print Server platform enables the SSLv2 services for use by HTTP connectivity by default when installed. However, SSLv2 protocol has potential security vulnerabilities. If an HTTP client (e.g., web browser) requests an SSLv3/TLS connection, FreeFlow® Print Server will provide one. However, many browsers define SSLv2 services for HTTP client connectivity with HTTP server services such as supported on the FreeFlow® Print Server platform. Since the negotiation of SSLv2 verses SSLv3 occurs "transparently" to the client user, the current "best practices" procedure for configuring HTTP servers recommends disabling SSLv2, and only supporting SSLv3/TLS.

In FreeFlow® Print Server 8.0, we disable SSLv2 by default in all Security Profile levels (Low, Medium and High). In releases earlier than FreeFlow® Print Server 8.0, there is a manual procedure to modify the FreeFlow® Print Server Security configuration (HTTP/SSL options) to disable SSLv2. The specific procedure will vary depending on the DocuSP/ FreeFlow® Print Server release version. See the 'Example procedure to disable SSLv2 on FreeFlow® Print Server v7' procedures section below.

Caveat: *In the past disabling SSLv2 was likely to affect customers who were running with older web browsers. Today, it is less likely (though still possible) that customers could experience such issues since the "modern Web Browsers" such as IE7 now support only SSLv3/TLS. Another potential problem defining SSLv3/TLS services is incompatibility with legacy SSL clients such as DigiPath, or some other third party SSL clients. Even if the client is capable of supporting SSLv3/TLS, this may not be the "default" configuration and thus such clients could fail to work with FreeFlow® Print Server until they are re-configured to use SSLv3/TLS.*

Example procedure to disable SSLv2 on FreeFlow® Print Server v7:

1. Login to the FreeFlow® Print Server GUI as the System Administrator. Use the FreeFlow® Print Server GUI to create/install a Self-signed certification and enable SSL.

2. Check to see if SSLv2 is enabled:

   a) Login to a command window, become an admin user, and enter:

      "/usr/sfw/bin/openssl s_client -ssl2 -connect FQDN:443 -state –debug"

      Note: *For FQDN, you can also use the current system IP address. If there is a problem with the DNS or registration of the FreeFlow® Print Server hostname with DNS, you may see "gethostbyname()" error and "connection failed" errors.)*

   b) When output from this command is not an error, it means successfully enabled the SSLv2 services.

3. To disable SSv2 on the FreeFlow® Print Server Apache 2.0 server, proceed with steps below:

   a) Edit the file "/opt/XRXnps/XRXweb/conf/ssl.conf (/etc/sfw/apache2/ssl.conf is linked to this file). Modify the line which begins with: "SSLCipherSuite", change the sub-string "+SSLv2" to "SSLv2" (or +SSL2 to !SSL2).
   b) Restart the FreeFlow® Print Server Webserver by entering the following command:
   c) /opt/XRXnps/XRXweb/bin/startWebServer restartWithSSL

4. Execute the following commands to check how SSL is now configured:

   a) /usr/sfw/bin/openssl s_client -ssl2 -connect ServerIPAddress:443 -state -debug
   b) /usr/sfw/bin/openssl s_client -ssl3 -connect ServerIPAddress:443 -state -debug

Expected Result: ssl2 connect attempt will result in error...but sslv3 should report success.

Web Browser Test:

1. Configure Internet Explorer (IE) to use only SSLv3 (by going into the Tools->Internet Options-> Advanced menu. Scroll down and put a check mark into "Use SSL 2.0" and clearing the check marks for "Use SSL 3.0" and "Use TLS 1.0".

Attempt to connect to FreeFlow® Print Server port 443 with IE. SSLv2 is enabled on the FreeFlow® Print Server platform if the connection fails, then reconfigure IE to use only SSLv3 or TLS 1.0. The connection should now succeed.

7.2 Creating/Installing SSL Certificate

The Secure Socket Layer (SSL) and Transport Layer Security (TLS) services are two protocols used to provide a reliable end-to-end secure authenticated and data-encrypted connection between two points over a network. Secure Shell (SSH) is another protocol used to provide secure authenticated and data-encrypted connections.

These protocols require the use of Digital Certificates on both client and server hosts. The FreeFlow® Print Server SSL/TLS feature allows a FreeFlow® Print Server System Administrator

to either create and use a self-signed Digital Certificate or install an existing Certificate obtained from a 3rd-party Certificate Authority (i.e. VeriSign, Thawte, etc.).

Self-Signed Certificate Setup

1. Logon to the FreeFlow® Print Server GUI as System Administrator or as a user who belongs to the System Administrator group.
2. Go to the 'SSL/TLS..' option from the [Setup] pull-down menu.
3. If not already enabled, click the 'OK' button in the "Information" pop-up box.
4. Click on the [Add Certificate] button'. This will launch the "Add Certificate Wizard".
   Step 1 - Select "Self-Signed Certificate"
   Step 2 - Select and enter either the server
   a. Domain Name
   b. IP Address
   c. Other
   Step 3 - Enter the requested information:
   a. Organization (required)
   b. Organizational Unit (optional)
   c. E-mail (optional)
   d. Locality (optional)
   e. State/Province (optional)
   f. Country (required)
   Step 4 - Enter the length of time that the certificate will be valid.
   Step 5 - Verify information entered in previous steps.
   Step 6 - A message will appear indicating that the self-signed certificate has been installed.
5. Click on the 'Enable SSL/TLS' checkbox at the top of the SSL/TLS window.
6. Select a SSL/TLS mode of operation:
   a. Normal (Encrypted and Unencrypted Access)
   b. Secure (Encrypted Access Only)
7. Select encryption strength:
   a. Normal (DES-MD5-56-bit)
   b. Normal (DES-MD5-40-bit)
   c. Normal (DES-MD5-128-bit)
   d. Normal (3DES-MD5-128-bit)
   e. High (RC4-MD5-128-bit)
   f. High (3DES-MD5-128-bit)

The meaning of "SSL/TLS mode of operation" options is as follows:

1. "**Normal**", where the FreeFlow® Print Server platform accepts connections on both ports 80 (HTTP) and 443 (HTTPS)

2. "**Secure**", where the FreeFlow® Print Server platform accepts connections only on port 443 (HTTPS).

When the "SSL/TLS mode of operation" on the FreeFlow® Print Server platform is set to "Secure", the Internet Services Web client will require a username and password to authenticate with the FreeFlow® Print Server platform. You cannot make a connection without user authentication. Only a "secure" HTTP (a.k.a.., HTTPS) can be granted access.

Note: *In FreeFlow® Print Server 8.0 and above releases, you can select SHA encryption rather than MD5 when using the above procedures.*

If the customer is not permitted to use a certificate which uses the encryption options available by the FreeFlow® Print Server SSL/TLS GUI feature, it is recommended to import a certificate created by a certified vendor of CA-signed certificates (e.g., Comodo),

Certificate Authority Signed Certificate Setup

1. If SSL/TLS is not already enabled
2. Click the [Add Certificate] button.
   Step 1 - Select "Signed Certificate from a Certificate Authority"
   Step 2 - Browse to the location of the signed certificate (.pem file).
   Step 3 - Select the file and press the 'Install' button
   Step 4 - A message will appear indicating that the certificate has been installed.
3. Click on the 'Enable SSL/TLS' checkbox at the top of the SSL/TLS window.
4. Select a SSL/TLS mode of operation:
   a. Normal (Encrypted and Unencrypted Access)
   b. Secure (Encrypted Access Only)
5. Select encryption strength:
   a. Normal (DES-MD5-56-bit)
   b. Normal (DES-MD5-40-bit)
   c. Normal (DES-MD5-128-bit)
   d. Normal (3DES-MD5-128bit)
   e. High (RC4-MD5-128-bit)
   f. High (3DES-MD5-128-bit)

7.3 FreeFlow® Print Server IPSec Protocol Security

A customer may use an IPSec tunnel to ensure secure communications with Xerox® printer devices. The IPSec protocol uses strong 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. 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.

IPSec is a "must have" for Office and Enterprise-class products purchased by Government customers. The priority of using IPSec has increased significantly it was discovered that SSL/TLS protection can be cracked with a "man in the middle attack" involving renegotiation of SSL session already established between clients and trustworthy servers.

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

1. lp/lpr
2. Port 9100 Printing
3. FFRPS (FreeFlow® Remote Print Service, aka DRW)
4. Job Forwarding
5. NFS (Network File System)
6. SMB (Windows Folder Sharing, Print from SMB, Scan to SMB, Hot Folder, etc)
7. SNMP (Simple Network Management Protocol)

8. Telnet
9. Sendmail
10. NTP (Network Time Protocol)
11. DNS (Domain Naming Service)
12. DHCP (Dynamic Host Configuration Protocol)
13. ADS (Active Directory Services)

The protocol that provide a secure connection and/or transfer mechanism (e.g., SFTP, SSH, IPP, sHTTP, etc.) also benefit from IPSec being enabled on the FreeFlow® Print Server platform. The IPSec services can enhance network security by providing an extra layer of security for currently secure log in, filing and printing protocols.

Once there are one or more remote hosts configured on the FreeFlow® Print Server platform for IPSec services, those hosts will not have any network (login, filing or printing) access until configured as an IPSec client with the shared key matching the key defined on the FreeFlow® Print Server platform. This will not affect all other remote hosts if they do not configure IPSec connectivity with the FreeFlow® Print Server platform. They can still access the FreeFlow® Print Server platform over the network. The site security and/or network administrator is responsible for incorporating secure access to the FreeFlow® Print Server platform for those remote hosts according to their site Security policies.

The customer site Security policy may be that all remote hosts on the network are required to access the Xerox® printer using secure network protocols. If this is the case, then consider an approach where the FreeFlow® Print Server platform is setup to "IP Filter" only those remote hosts that can access the printer. You can grant access to each remote "trusted" host by configuration the IPSec services and IP Filter list on the FreeFlow® Print Server Platform.

Refer to the 'FreeFlow® Print Service IPSec Client/Server Configuration' document for procedures to setup IPSec services using pre-shared keys in a Windows environment.

http://xww.docushare-xogpsg.world.xerox.com/dsweb/View/Collection-149460

- Make sure to log into this location with s3 credentials.

8.0 FreeFlow® Print Server Hard Drive Security

8.1 Hard Drive Removal and Purchase

Whenever a customer needs to dispose of or destroy the Hard Drive(s), Xerox Service provides a service to remove the hard drive and deliver this to the customer. A nominal service cost includes a flat fee which covers labor charges, and the Hard Drive replacement cost. Contact your Sales or Account representative for details.

Note: *Refer to bulletin T7591-09-28: Hard Drive Removals:*

- http://xww.thefic.xerox.com/dsweb/View/Collection-165104

Customers who need protection or assurance for the secure handling/disposal of customer data from FreeFlow® Print Server hard drives must request that Xerox Service remove the drives before removing the printer from the customer's secure facility. Xerox Service will perform the labor for a nominal fee, and hand the hard drives to the customer for further disposition. If the customer does not own the printer, they must agree to purchase the replacement HDs from Xerox Service at the current "replacement part" price.

Xerox does not currently offer a process to ensure a certified chain-of-custody and audited destruction or cleaning of the hard drives.

8.2 Hard Drive Overwrite

The following discussion about the use of the Data Overwrite "kit" or "package" applies only to FreeFlow® Print Server v7 releases and earlier. In FreeFlow® Print Server v8 and later software release, the Zetabyte File System (ZFS) is incompatible with the Data Overwrite feature. See the section 8.3 "*Hard Drive Disk Purge*" for overwrite of the ZFS drives delivered with the FreeFlow® Print Server v8 and later software releases.

In relation to the FreeFlow® Print Server platform, an optional Data Overwrite Kit can be used as a tool to assist customers meet their internal Security requirements for securely "erasing", "removing", or "shredding" print jobs which have been sent to the FreeFlow® Print Server platform. You run this process "on demand" when the FreeFlow® Print Server and printer can be taken "off line", as significant time interval may be required to overwrite all the print jobs accumulated on the hard drive(s).

Note: *With the FreeFlow® Print Server 7.0 SP3 release, the Data Overwrite software is a "bundled feature". The standard* FreeFlow® Print Server *v7 software install automatically defines the DO partition, so no longer needs selection at install time. The standard* FreeFlow® Print Server *license enablement automatically enables the Data Overwrite capability, and there is no longer any cost associated.*

The Data Overwrite feature will "scrub" directories in the "Data Overwrite partition". These directory locations typically contain:

1. Print jobs, which are stored on hard drive (s) by FreeFlow® Print Server from job submission applications.

2. Print jobs, which are stored on hard drive (s) by FreeFlow® Print Server when the submitter or operator selects the Disposition 'Save' or 'Print & Save' option.

3. Print-ready raster images sent to the printer engine.

4. Print resources, which are stored in the standard directories defined by FreeFlow® Print Server default configuration.

The print and resource data removed from the disk mostly resides under the /var/spool/XRXnps partition with the exception of outQ. The directory locations under /var/spool/XRX that backed up and overwritten are:

1. Backup
2. corefiles
3. CustomerJobs
4. debugLogs
5. downloads
6. gfm_wd
7. imp_scratch
8. inQ
9. log
10. lost+found
11. lp
12. netqreq
13. netqstatreq
14. outloads
15. outQ <---- this is partition /var/spool/XRXnps/outQ.
16. ppml2ps
17. ppr_data
18. resources
19. saved
20. storeQ
21. stream
22. swapfiles
23. tmp
24. var
25. vipp

The backed up customer print data and resources are copied back into their original location after the Data Overwrite operation is complete. This process overwrites data in three write passes using different patterns written to the entire disk or section of the disk. There is a final read pass, which verifies overwrite successfully scrubbed the hard drive data. You cannot retrieve data once it has been "scrubbed" to completion by this procedure. This four-pass algorithm conforms to NIST SP800-88 specification, and U.S. Department of Defense Directives 5200.28-M and 5220.22-M.

Note: *FreeFlow® Print Server Data Overwrite Kit has not been "certified" by any authority (e.g., NIAP or 3rd party Common Criteria Evaluation lab).*

Caveats: *See caveats below:*

1. *The Data Overwrite feature will not "scrub" directories outside of the* FreeFlow® Print Server *where jobs may have been explicitly stored by the operator. For example, a job transferred to a directory outside of* FreeFlow® Print Server *using the "Scan to File" feature will not be "scrubbed". A job that the administrator or trusted operator has saved to a directory outside the Data Overwrite partitions will not be "scrubbed".*

2. *The Data Overwrite operation does not process defective or spare blocks for SCSI and FCAL drives. It may or may not process defective/spare blocks for SATA drives. It also does not perform any special disk error recovery. Some customer data may remain on the hard drive, if the operator has loaded any customer print data to directories outside the Data Partition (e.g., using FTP or Save Job to non-standard locations).*

3. The data overwrite operation does not process defective or spare blocks for SCSI and FCAL drives. It may or may not process defective/spare blocks for SATA drives. It also does not perform any special disk error recovery.

4. *In* FreeFlow® Print Server *8.0, the Data Overwrite feature is not available in conjunction with the new Zetabyte File System (ZFS).*

.

If the system is being returned to Xerox, or for other reasons a complete Hard Drive Overwrite process is required, a Xerox Service procedure is offered using the Solaris Format command Purge utility (see 2.8 Solaris Hard Disk Purge). We strongly recommend scheduling the Hard Disk Purge procedure with Xerox Service.

Xerox also offers a "Hard Drive Removal" service, described in "2.7 Hard Drive Removal and Purchase", where the hard drive(s) can be removed and the customer may dispose of the drive securely. Please contact your local Xerox sales representative to remove hard drive(s) from the FreeFlow® Print Server platform.

Additionally, third party software with more flexibility and functions, such as UniShred Pro is available. However, total hard drive overwrite capability is not part of the Disk Overwrite software nor is it supported by the FreeFlow® Print Server. Contact the Xerox Hotline for assistance to scrub hard drive(s), or to remove hard drive(s) needing destroyed. Xerox offers a Hard Drive Disposal process, described elsewhere in this document.

8.3 Hard Drive 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 Hard Disk Overwrite procedures to remove all software and data from the hard drives. The process involves using the Solaris format command. This automated FreeFlow® Print Server services is currently only supported on DocuSP v5 and FreeFlow® Print Server v7 software releases that have UFS Disk formatted hard disks. A Service representative can manually use the 'format' command to wipe the disk clean on the FreeFlow® Print Server v8 and greater software releases that have the ZFS formatted hard disks.

For convenience, an automated Solaris hard disk purge feature is available to remove all data from multiple hard disks installed in the FreeFlow® Print Server DFE for any printer product. The advantage of this feature is it will wipe all hard disks in the FreeFlow® Print Server DFE without any need for operator intervention. We recommend the customer schedule a Xerox Service Engineer or Support Analyst to complete the hard disk purge. 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.

This feature is different from Data Overwrite 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.

The currently known advantages for using the Solaris hard disk purge procedures are as follows:

1. There is logging that will identify the status of the purge operation, and help to determine if there were problems or success. It is very important for the customer to know the disk purge was successful for all hard disks in the DFE. The ability to prove successful sanitization of printer hard disks(s) is very important to customers to satisfy their Security audits.

2. This Solaris disk purge feature writes an audit file that identifies if the operation completed successfully. If that audit identification is not present in the audit file, the operation had failed.

This Solaris disk purge feature automates the purging of multiple hard disks so that the CSE/Analyst does not need to start the operation for each disk in the DFE. The time to purge a single disk can be very long. This disk purging process will automatically purge all hard disks available in the FreeFlow® Print Server platform without interruption or operator intervention. You can start the operation prior to going home for the evening, and find all the hard disks purged in the morning. The purge process writes an audit log file to identify the final status of the purge process.

The automated hard disk purge feature from USB drive uses the Solaris 'format' command to wipe data from the disks. If the DFE has a single hard disk, the Service representative can manually use the 'format' command to wipe the disk clean. These procedures are below:

1. Reboot the system.
   Note: *You can use the shutdown option from the FreeFlow® Print Server GUI, or typing the* ***init 6*** *command from a command prompt (as root).*
2. When the system boots to the GRUB menu, select the **Solaris failsafe** option from the menu.
3. When asked to mount, type **N** and press enter.
4. At the prompt type **format**
   a. You will see a displayed list of hard drives. The data overwrite procedure must be performed on each drive individually.
   b. Select the first drive in the list.
5. At the subsequent **format>** prompt type **analyze**.
   a. You will see a displayed list of commands to analyze the disk. The recommended selection is to type **purge**
      Note: *In response to the purge command, the system will present the following message: "Ready To Purge (Will Corrupt Data). This takes a long time, but is Interruptible with CTRL-C. Continue?*
   b. As a response to the above question Type **Y**, to continue with the purge operation

   Note: See tips and hints below:
   a. Purge is a 4 pass overwrite that overwrites the available disk sectors with patterns that comply with the Department of Defense declassification regulations for data eminence.
   b. A faster option is to use the write command instead of purge. Write is a single pass overwrite.

c. *Purge can also be configured to do more than 4 passes which will be more thorough overwrite (but is a longer option). To configure purge for more passes:*
   - *Prior to typing Purge. Type setup. Hit return to accept the default values until you reach Passes. Change the Passes value to the desired number.*
   - *Note that Purge will not accept a number less than 4 and will minimally do 4 passes each time. Purge will honor higher numbers and subsequently perform a greater number of passes.]*

6. Once purge completes it will show a success message.
   - On average, it takes about 2 hours (unattended) to wipe each 160 GB drive.
7. At this point you need to **quit** analyze
8. Type **disk**, this will present a list of available hard drives; enter the number corresponding to the next drive in the list.
9. Repeat steps E until the sanitization is complete for all the drives.

You can repeat these procedures for a second hard disk if the FreeFlow® Print Server DFE is a two hard disk configuration.

8.4 Hard Drive Removal Kit

For customers who have very strong Security requirements, and need to secure/lock up the system hard drives, Xerox offers optional "Removable Hard Drive" hardware kits to enable quick and easy removal of the hard drives. For example, the US Govt. may require the customer to remove the hard drives after printing "Classified" information.

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

Availability of RHD kits may vary for different products. Contact your Sales or Account representative for details.

9.0 FreeFlow® Print Server Audit Logging

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

1. FreeFlow® Print Server Security-Generated Security Logs
2. FreeFlow® Print Server Application-Generated Logs
3. BSM-Generated Security Logs
4. Solaris-Generated Security Logs

Descriptions of these FreeFlow® Print Server Audit Logs are as follows:

1. **FreeFlow® Print Server Security-Generated Logs**:

   The FreeFlow® Print Server security configuration and "hardening" modules generate log file entries during system start-up, or after modifying security configuration settings in this file:

   /opt/XRXnps/log/xdss_log.txt

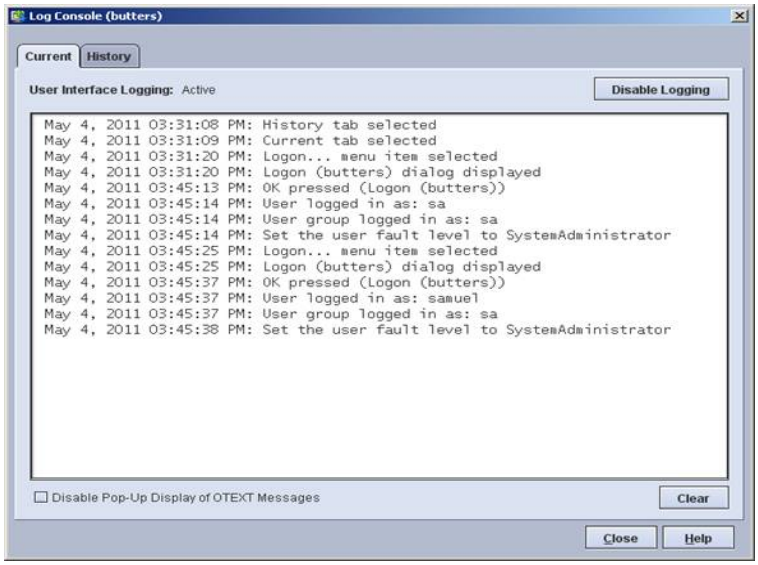
2. **FreeFlow® Print Server Application-Generated Logs:**

   a. **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 enable the "Console Logging" feature from the FreeFlow® Print Server GUI using the procedures below:

   1. Log in as System Administrator
   2. Click on "System" menu. Click on "Log Console".
   3. Log out.

   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.

b. Job Accounting Logs

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

Example Job Accounting Log:

Container ID = 205
Record status = Complete
Document Name = 30pg.pdf
Sender Name = System Administrator
Disposition = Print
Job Status = Completed
Interrupt Status = No Interruption
Print Server Name = the-hill
Virtual Printer = 32Up_Mult_Rept
Machine Type = Xerox® 4127 Copier/Printer with FreeFlow® Print Server
Job Source = None
Job Submission Date = June 11, 2009 16:19:12
Input File Size (bytes) = 42922
Job Format = PDF
Start RIP Time = June 11, 2009 16:19:15
Stop RIP Time = June 11, 2009 16:19:25
Elapsed RIP Time (seconds) = 10
Number Pages RIPped = 30
Account ID = None specified
User ID = None specified
Additional Job Data = None specified
Start Date = June 11, 2009 16:19:17
Completion Date = June 11, 2009 16:19:55
Pages To Print = 1 - End of job
Collate Mode = Yes
Copies Requested = 1
Copies Printed = 1
Total Sheets Greater than 9" Wide Printed = 31
Total Sheets Printed = 31
Total Impressions Printed = 31
Pages to Bin = 31
Number 1-Sided Sheets Printed = 31
Finishing Applied 1 = None
Medium 1) Name: Unspecified , Number Printed = 31 Plain
432 x 279 mm, White, Weight: 75.0 g/m²

c. Job Activity Logs

FreeFlow® Print Server Application modules generate log file entries (in the /opt/XRXnps/log directory) as the system performs printing, scanning, saving, copying, etc. The FreeFlow® Print Server outload does not capture the Security Profile or the Users & Group log information. Therefore, manually capturing these log and/or configuration files is important when escalating a Security problem to Xerox service. The support engineers will need to know the Security settings to enable proper evaluation of a Security problem. Some of the log file entries are useful to track the jobs processed by the FreeFlow® Print Server software.

3. **BSM-Generated Logs**

   Solaris 10 includes a feature called Basic Security Module (BSM). 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 or file delete activity. The logs produced by this feature will satisfy the Department of Defense audit logging criteria for a "C2" level security certification. The following sections provide information on how the FreeFlow® Print Server software configures the BSM services, and how to use its capabilities.

4. **Solaris-Generated Logs**

   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. You can find the most common debug information in the /var/adm and /var/log directories. For more information refer to the Solaris 10 Administration Guide or search the Web.

9.1 Solaris Basic Security Module (BSM)

When you enable the Medium or High Security profile, this automatically enables the Solaris Basic Security Module (BSM). The activities captured in logging by the FreeFlow® Print Server platform are a superset of the recommendations from Solaris Security Blueprints.

The flags track the following activity:

FLAG	Default*	LONG NAME	SHORT DESCRIPTION
no		no_class	null value for turning off event pre-selection
fr		file_read	Read of data, open for reading, etc.
fw	X	file_write	Write of data, open for writing, etc.
fa		file_attr_acc	Access object attributes: stat, pathconf, etc.
fm	X	file_attr_mod	Change object attributes: chown, flock, etc.
fc	X	file_creation	Creation of object
fd	X	file_deletion	Deletion of object
cl		file_close	close(2) system call
pc		process	Process operations: fork, exec, exit, etc.
nt		network	Network events: bind, connect, accept, etc.
ip		ipc	System V IPC operations
na	X	non_attrib	non-attributable events
ad		administrative	administrative actions: mount, exportfs, etc.
lo	X	login_logout	Login and logout events
ap	X	application	Application auditing
io		ioctl	ioctl(2) system call
ex		exec	exec(2) system call
ot		other	Everything else

all		all	All flags set
dd	X	dd.exe	Creates forensic image of NTFS drive
cs	X	cs.cert	Indicates a root compromise
cf	X	cf	Cross site scripting vulnerability.

To adjust the amount of activity captured in the audit logs, these flags can be added/removed from the audit control file located in the /etc/security directory.

9.1.1 Enabling BSM Logging

The BSM logging is disabled or enabled via a custom FreeFlow® Print Server Security Profiles. You can enable BSM logging as follows:

1. Select the [Setup -> Security Profiles…] pull-down option.
2. Set Security Profile to Medium or High
3. Right-click one of these Security profile levels and set this as 'Current'

OR

1. Create a custom security profile
2. Enable BSM in the 'System' tab from the Security profile properties from [Setup -> Security Profiles] pull-down option.
3. Shut down the FreeFlow® Print Server platform and power back on.

OR

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. cd /etc/security
3. ./bsmconv
4. Shut down the FreeFlow® Print Server platform and power back on.

Note: *BSM logs can become very large. We recommend monitoring the size of the log files; archive/rotate the log files, and transferring them to a remote storage location on a regular basis. The Solaris Console window will notify if the /var/log directory is becoming full. You can define a cron job to purge these logs based on some time duration.*

The type of logging can be defined by specifying one or more of the flags from the above table in the /etc/security/audit_control file with the 'flags:' entry. For example, 'flags:fr,fw,lo' will ensure that all login/logout, file read and file write operations are logged with the associated logged in user.

Since FreeFlow® Print Server uses its own custom PAM library, user FreeFlow® Print Server GUI login/logout/password change activities are not captured in the BSM log when the 'lo' and/or 'fr' flags are added to the /etc/security/audit_control file. However, this information is captured in the /var/log/authlog file when the current security profile is set to 'Medium', or 'High'.

To read the audit logs:

1. Open the terminal window and log in as root (su)
2. **Type:** cd /var/audit
3. **Type:** praudit <name of audit log file>

9.1.2 Disabling BSM Logging

You can disable BSM logging in one of two ways, by setting security to either Low, the "OS Only" default, or by disabling it in a 'Current' custom profile. Disable BSM logging from a custom Security profile if you wish to maintain a higher level of security.

To disable BSM logging while retaining a High or Medium Security Profile, perform the following steps:

1. Select the [Setup -> Security Profiles…] pull-down option.
2. Set Security Profile to 'OS-only' or 'Low'
3. Right-click one of these Security profile levels and set this as 'Current'

OR

1. Create a Custom Profile by copying the Medium or High security profile.
2. Select the System tab.
3. Under System Services, right-click on the 'bsm'.
4. Select disable.

OR

1. Log into a terminal window on the FreeFlow® Print Server platform as root.
2. cd /etc/security
3. ./bsmunconv
4. Shut down the FreeFlow® Print Server platform and power back on.

9.2 Solaris OS Logging

In addition to the BSM logs, auditing information can also be tracked through standard Solaris logging and extensions implemented by the FreeFlow® Print Server platform (authlog, connlog and tcpd in the /var/log directory). The authlog, connlog and tcpd logs are not standard Solaris files. You configure these settings to capture Security audit information on the FreeFlow® Print Server platform. The FreeFlow® Print Server platform modifies certain settings in the Solaris OS to capture more information in syslog. Local or remote users that login/logout of the FreeFlow® Print Server platform are tracked in this log. . In addition, if you maintain accounts on an ADS server, FreeFlow® Print Server logging captures information for each packet sent over the network in the /var/log/sso.log.

The customer can configure additional OS logs if specific audit information is required. They can do this by modifying the "syslog.conf" file.

9.3 FreeFlow® Print Server GUI Console Logging

This feature will log operations of the user logged into the FreeFlow® Print Server GUI, and some of the GUI interactions with the FreeFlow® Print Server platform. The purpose of this feature is to audit actions taken by the operator on the FreeFlow® Print Server GUI such as changing job parameters, restarting the FreeFlow® Print Server software, deleting jobs, queue settings, system settings, printer properties, job preview, and jobs printed, etc. The customer IT specialist can monitor and review this log for Security audit purposes.

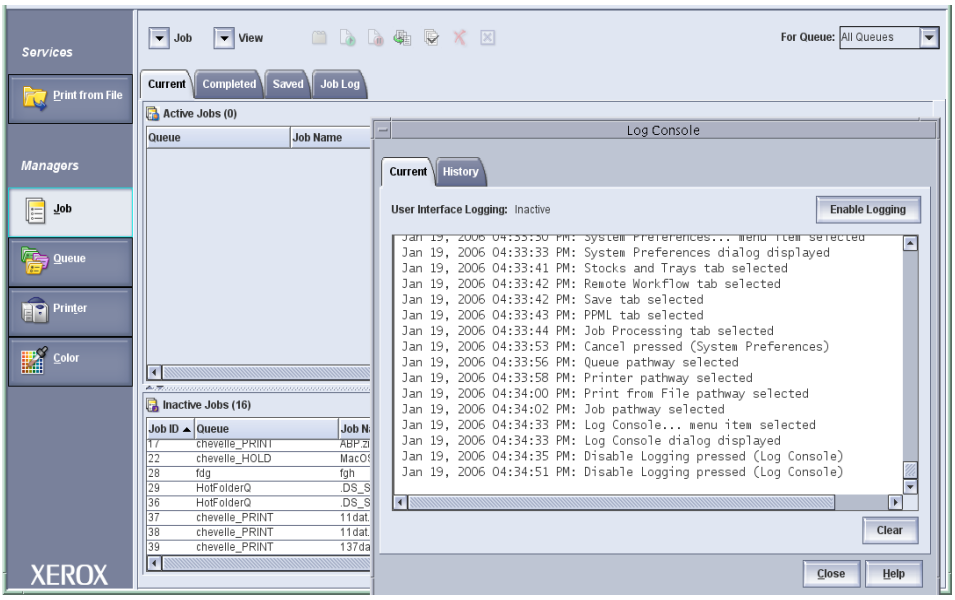
The operator or SA may access this feature from the [System -> Log Console] pull-down menu option. When you select this option, it will display a window with a view into the log and a 'Pause/Resume Logging' button to enable/disable the feature.

GUI logs are stored in the standard log location: /opt/XRXnps/logs. The actions are logged, one file per day, into a log file with a naming convention of: Console_YYYYMMDD.log.0, and are automatically purged after a 14 day time-period.

Logged Events Include:

1. The pathway navigation (Selections of Pathway buttons, Tabs, and FAB's)
2. GUI management events (Job Properties, system settings, tray settings, etc…)
3. User logon/logoff actions which help map events back to a user

See a screen shot that illustrates the Console logging below:



10.0 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 are continually enhancing and developing 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. Xerox is pro-actively planning implementation of new FreeFlow® Print Server features for customer Security requirements that meet very stringent Financial, Education and Government standards for protecting sensitive data.

10.1 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.

10.1.1 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 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. 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.

10.2 Common Criteria Certification Standard

FreeFlow® Print Server runs as an application on top of the Solaris OS. The FreeFlow® Print Server GUI mediates all user interactions and normal users do not have direct access to the operating system (the customer's SA may interact with the OS if permitted by the security configuration).

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 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. FreeFlow® Print Server version 7.3, 8.2 and 9.3 ships with this version of the Solaris OS. Oracle certifies subsequent Solaris 10 Updates and Security patches to using the Common Criteria's Assurance Continuity Process.

10.3 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 emerged from the DIACAP process.

10.4 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 ATO (Authority to Operate) 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 printer device according to Army regulations.

11.0 General FreeFlow® Print Server Security Information

11.1 FreeFlow® Print Server 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 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 required these type of applications, so removing them significantly minimize the risk of virus attacks. The default security settings (e.g., Low Profile) 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. services are disabled). Starting with DocuSP 3.8 and up, and FreeFlow® Print Server 6.0 and up, the Email Receive service is disabled by default. Therefore, software that protects against incoming mail viruses is not required.

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. 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.

Note: *We highly recommend not scheduling virus scans on the* FreeFlow® Print Server *platform while print jobs are processing and printing. Running the virus scan during production print runs may cause a noticeable reduction in overall system performance, thus reducing productivity. If a customer requires Malware scans on the* FreeFlow® Print Server *platform, we recommend scheduling a scan when the system is idle given the performance implications of running these types of services.*

11.2 Statement of Volatility (SoV)

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

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

such as a print station (PSIP) for the print engine, and workflow device such as FreeFlow® Core, etc.

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

http://www.xerox.com/information-security/enus.html

Once you navigate to the Web page for a specific printer product (E.g., C60/C70, iGen5, etc.), the respective page will have links to Security documents such as the SoV.