January 2012
702P01427

Xerox FreeFlow® Print Server Security Guide

Document version 1.0: September 2009

Contents

1 Introduction

2 Security

1 Introduction

The Security Guide provides the information needed to perform system administration tasks for maintaining the Xerox FreeFlow® Print Server.

About this guide

This guide is intended for network and system administrators responsible for setting up and maintaining Xerox printers with Xerox FreeFlow Print Server software. System administrators should have an understanding of the Sun workstation, a familiarity with Solaris, and with basic UNIX commands. This includes the use of text editors such as vi or textedit and the ability to maneuver within the Solaris environment. To enable them to setup a customer site, system administrators are expected to have a working knowledge of Local Area Networks (LANs), communication protocols, and the applicable client platforms.

Customer support

To place a customer service call, dial the direct TTY number for assistance. The number is 1-800-735-2988.

For additional assistance, dial the following numbers:

- Service and software support: 1-800-821-2797
- Xerox documentation and software services: 1-800-327-9753

Security 2

This section describes the Xerox FreeFlow® Print Server system-supplied security profiles. It outlines the characteristics of each profile and indicates how each can be customized to create user- defined profiles. The enhanced security features in the Xerox FreeFlow Print Server protect the system against unauthorized access and modification.

This section also addresses the options available to the administrator in setting up and managing user accounts.

Finally this section offers general guidelines to security-related procedures that can be implemented to improve the security of the Xerox FreeFlow Print Server controller and the Solaris OS.

System supplied security profiles

The four system-supplied profiles are: default operating system only, low, medium, and high. The following table describes the characteristics of each security level and the configurable settings that restrict access to various devices and operating system services.

> Note Customers have the option to setup and use custom profiles. Custom profiles are copied from one of the system-supplied profiles and provides the ability to enable/disable any of the default settings. Multiple custom profiles can be saved on the system.

Table 2-1 Security Profiles

Profile	Characteristics	User	Compatibility	Comments
Default Operating System Only	All ports are open. Walkup users can reprint anything. Full workspace menu is available. Auto logon is enabled.	Physically closed environments.	Close to DocuSP 2.1 and 3.1. Similar to DocuSP 3.X “Medium”.	Anonymous FTP is read-only and restricted. The Solaris desktop is removed from all settings except none.
Low	FTP is enabled. Telnet, rsh is disabled. NFS client is enabled. AutoFS is enabled. Walkup users can reprint from “Saved Jobs” and CD-ROM. Terminal window is password protected. Auto-login is enabled.	First choice setting for most environments.	Similar to DocuSP 3.x “High”. Supports FreeFlow® workflow.	Anonymous FTP is ready-only and restricted. To enable telnet, go to [Setup], [FTP/ Remote Diagnostics].
Medium	FTP is disabled. telnet, rsh is disabled. NFS client is disabled. AutoFS is disabled, e.g.; /net/<hostname>and home/<username> are not automatically mounted). NFS server is filtered via RPC tab. Walkup user can reprint from CD_ROM. Terminal window is password protected. Auto-login is enabled.	Environments requiring high security but with a need to integrate FreeFlow/Digipath.	Supports FreeFlow workflow and legacy DigiPath workflow.	Anonymous FTP is ready-only and restricted. To enable telnet, go to [Setup], [FTP/Remote Diagnostics].

Profile	Characteristics	User	Compatibility	Comments
High	FTP is disabled. telnet, rsh is disabled. NFS client is disabled. AutoFS is disabled, e.g.; /net/<hostname>and home/<username> are not automatically mounted. NFS server is disabled on customer network. Walkup users cannot reprint anything. Terminal window is password protected. Auto login is disabled (login is always required from GUI).	For government market.	Does not support legacy DigiPath workflow. Supports FreeFlow workflow.	File FTP is disabled. File transfer can be done via Secure FTP. For CFA support, that is FTP upload of outload, go to [Setup], [FTP/Remote Diagnostics] menu, select enable FTP.
Custom	Any profile can be edited to adjust to user needs			

Note Regardless of the security profile, anonymous FTP is Read-only with restricted access to /export/home/ftphome only.

Enable and disable services

The following tables provide a list of the services that can be enabled and disabled from the Xerox FreeFlow Print Server “Setup > Security Profiles” menu options. To view the properties of a desired profile, double click on the desired profile, and a set of tabs will appear.

Note Services list may vary, depending on the product.

Table 2-2 System tab

System Service	Description
Allow_host.equiv_plus	Background: The /etc/hosts.equiv and /.rhosts files provide the remote authentication database for rlogin, rsh, rcp, and rexec. The files specify remote hosts and users that are considered to be trusted. Trusted users are allowed to access the local system without supplying a password. These files can be removed or modified to enhance security. The Xerox FreeFlow Print Server is provided with both of these files deleted entirely. The setting All_host.equiv_plus is set to disabled, then anytime that security settings are applied, the + will be removed from host.equiv. IMPORTANT NOTE: Removing the + from the hosts.equiv file will prevent the use of the Xerox command line client print from remote clients. An alternative would be to remove the + and add the name of each trusted host that requires this functionality. Leaving the + will allow a user from any remote host to access the system with the same username
Anonymous FTP	
BSM	Enable or disable the Basic Security Module (BSM) on Solaris
Executable Stacks	Some security exploits take advantage of the Solaris OE kernel executable system stack to attack the system. Some of these exploits can be avoided by making the system stack non-executable. The following lines are added to /etc/system/fP file:set noexec_user_stack=1set noexec_user_stack_log=1
Hide Info Banners	
Multicast Routing	
Remote CDE Logins	Deny all remote access (direct/broadcast) to the X server running on the Xerox FreeFlow Print Server by installing an appropriate /etc/dt/config/Xaccess file.
Restrict DFS tab	
Restrict NFS Portmon	
Router	Disable router mode by creating an empty the empty file: /etc/notrouter.
Secure File Permissions	
Secure Network Settings	
Secure Sendmail	Force sendmail to only handle outgoing mail. No incoming mail will be handled by sendmail.
Security Warning Banners	Enable security warning banners to be displayed when a user logins or telnets into the Xerox FreeFlow Print Server. The warning message explains that only authorized users should be using the system and that any others face the possibility of being monitored by law enforcement officials.

Table 2-3 INIT tab RC2 section

RC2 Service	Description
S40LLC2	Class II logical link control driver
S47ASPPP	Asynchronous PPP link manager. This service is re-enabled via enable-remote-diagnostics command.
S70UUCP	UUCP server
S71LDAP.CLIENT	LDAP daemon to cache server and client information for NIS lookups.
S72AUTOINSTALL	Script executed during stub JumpStart or AUTOINSTALL JumpStart
S72SLPD	Service Location Protocol daemon
S73cachefs.daemon	Starts cachefs file systems
S73NFS.CLIENT	NFS client service. Disables the statd service which is only required if your system is an NFS server or a client.
S74XNTPD	
S74AUTOFS	The automountd service is only required if your system uses NFS to automatically mount file systems. Stopping the autofs subsystem will kill the running automountd daemon and unmount any autofs file systems currently mounted.
S80SPC	SunSoft Print Client daemon
S88SENDMAIL	The sendmail daemon is used to send mail over the internet. If sendmail is not required, it can be disabled.
S89bdconfig	Solaris serial device.
S90WBEM	CIM Boot Manager. Disables WBEM clients from accessing the Xerox FreeFlow Print Server.
S93cacheos.finish	Starts cachefs file systems.
S94ncalogd	
S95ncad	Solaris network cache and accelerator.
slp	
uucp	

Table 2-4 INIT tab RC3 section

RC3 Service	Description
S15NFS.SERVER	NFS Server. Disable ability to export Xerox FreeFlow Print Server file systems. This service is enabled if legacy DigiPath/FreeFlow® and Decomposition Services (NetAgent) are enabled.
S17HCLNFS.DAEMON	

RC3 Service	Description
S25openssh.server	OpenSSH server.
S17BWNFS.DAEMON	Secure mounted file systems. There are two shared file systems that are exported by the Xerox FreeFlow Print Server. The two directories are only required for anyone with XDOD version 3.0 or below. With the release of DigiPath Version 1.0, it is not necessary to export these file systems.
S76SNMPDX	Sun Solstice Enterprise Master Agent. Solaris SNMP services are disabled. This does not prevent Xerox FreeFlow Print Server SNMP services from operating.
S77DMI	Sun Solstice Enterprise DMI Service Provider
S80MIPAGENT	Mobile IP agent
S82initsma	
S92VOLMGT	Solaris volume management daemon.

Table 2-5 INETD tab

INETD Service		Description
amiserv	RPC Smart Card Interface	Not used by the Xerox FreeFlow Print Server.
cachefs	Cached File System server	Not used by the Xerox FreeFlow Print Server.
chargen	Character Generator Protocol server	Sends revolving pattern of ASCII characters. Sometimes used in packet debugging and can be used for denial of service attacks. Not used by the Xerox FreeFlow Print Server.
comsat	Biff server	comsat is the server process which listens for reports of incoming mail and notifies users who have requested to be told when mail arrives. Not used by the Xerox FreeFlow Print Server.
daytime	Daytime Protocol server	Displays the date and time. Used primarily for testing. Not used by the Xerox FreeFlow Print Server.
discard	Discard Protocol server	Discards everything sent to it. Used primarily for testing. Not used by the Xerox FreeFlow Print Server.
dtspc	CDE sub-process Control Service	CDE sub-process Control Service (dtspcd) is a network daemon that accepts requests from clients to execute commands and launch applications remotely. Not used by the Xerox FreeFlow Print Server.
echo	Echo Protocol server	Echoes back any character sent to it. Sometimes used in packet debugging and can be used for denial of service attacks. Not used by the Xerox FreeFlow Print Server.
exec	Remote execution server	Used by rexec(1) command. Potentially dangerous—passwords and subsequent session is clear text (not encrypted). Not used by the Xerox FreeFlow Print Server.
finger	Remote user information server	Display information about local and remote users. Gives away user information. Not used by the Xerox FreeFlow Print Server.
fs	X font server	Used by CDE to dynamically render fonts. The Xerox FreeFlow Print Server uses bit-map fonts.
ktkt_warnd	Kerberos warning daemon	ktkt_warnd is a daemon on Kerberos clients that can warn users when their Kerberos tickets are about to expire. It is invoked by inetd when a ticket-granting ticket (TGT) is obtained for the first time, such as after using the kinit command.
ftp	File transfer protocol server	This can be used to enable/disable the ftp server. This does not affect using the ftp client from the Xerox FreeFlow Print Server to another host running an FTP server. Note that FreeFlow® requires this service to be enabled.

INETD Service		Description
gssd	RPC program authentication	Generates and validates GSS-API tokens for kernel RPC.
kcms_server	KCMS library service daemon	Allows the KCMS library to access profiles on remote machines. Not used by the Xerox FreeFlow Print Server.
login	Remote login server	Used by the rlogin(1) command. Potentially dangerous— uses ~/.rhosts file for authentication; passwords and subsequent session is clear text (not encrypted).
name	DARPA trivial name server	in.tnamed is a server that supports the DARPA Name Server Protoco. Seldom used anymore. Not used by Xerox FreeFlow Print Server.
ocfserv	OCF server	The OCF server, ocfserv, is a per-host daemon that acts as the central point of communications with all smartcards connected to the host. Applications that need to use a smartcard can do so by using the APIs in libsmartcard.so or smartcard.jar. The internal implementation of these APIs communicates with ocfserv to perform the requested function. inetd(1M) automatically starts the ocfserv command when it is needed. Once started, ocfserv runs forever. If ocfserv is killed or crashes, it restarts automatically, there is not a reason to run it manually. Must have root privileges to execute this utility.
rpc.cmsd	Calendar manager service daemon	rpc.cmsd is a small database manager for appointment and resource-scheduling data. Its primary client is Calendar Manager. Not used by Xerox FreeFlow Print Server.
rpc.rusersd	network username server	Gives intruder information about accounts. Not used by Xerox FreeFlow Print Server.
rpc.rwalld	Network rwall server	Server that handles rwall(1M) command requests. Can be used for spoofing attacks. Not used by Xerox FreeFlow Print Server.
rpc.sprayd	Spray server	Records the packets sent by the spray(1M) command. Can be used in denial of service attacks. Not used by Xerox FreeFlow Print Server.
rcp.ttdbserverd	RPC-based ToolTalk database server	The RPC-based tooltalk database server is required for CDE action commands. In particular, the CDE front panel has various menu items that rely on CDE actions. Late in the CP3.1 release, the Server UI team disabled the front panel. With the panel disabled, the need for the tooltalk database server no longer exists

INETD Service		Description
rpc.rstatd	rstatd-kernel statistics server	rpc.rstatd is a server which returns performance statistics obtained from the kernel. rup(1) uses rpc.rstatd to collect the uptime information that it displays. rpc.rstatd is an RPC service.
rquotad	Remote quota server	Used by the quota (1M) command to display user quotas for remote file systems. Not used by the Xerox FreeFlow Print Server.
sadmind	Distributed system administration daemon	Used by Solstice AdminSuite applications to perform distributed system administration. Not used by the Xerox FreeFlow Print Server.
shell	Remote execution server	Used by rsh(1) and rcp(1) commands. The Xerox print command line client relies on the remote shell internet service being enabled since it uses the rcp(1) command to transfer files onto the Xerox FreeFlow Print Server. However, this service represents a security risk. Not used by the Xerox FreeFlow Print Server.
Sun-dr (DCS)	Domain configuration server	The Domain Configuration Server (DCS) is a daemon process that runs on Sun servers that support remote Dynamic Reconfiguration (DR) clients. It is started by the Service Management Facility when the first DR request is received from a client connecting to the network service sun-dr.
talk	Server for talk program	The talk utility is a two-way, screen oriented communication program. Not used by the Xerox FreeFlow Print Server.
telnet	TELNET protocol server	This can be used to enable/disable the telnet server. This does not affect using the telnet client from the Xerox FreeFlow Print Server to another host running on TELNET server.
time	Time Protocol server	Outdated time service. Seldom used anymore. Not used by the Xerox FreeFlow Print Server.
uucp	UUCP server	UNIX to UNIX system copy over networks. UUCP is not securely set up and can be exploited in many ways. Not used by the Xerox FreeFlow Print Server.

User level changes

The following user-level changes are made:

- all users for at, cron, and batch are disallowed
- nuucp account is disabled
- listen account is disabled
- password entry locked for bin, sys, adm, uucp, nobody, noaccess, nobody4, and anonymous

Solaris file permissions

Secure File Permission options can be enabled or disabled through the Xerox FreeFlow Print Server interface. Fix-modes include:

- fixmodes-xerox: fix file permissions for all packages to make them more secure. Available under the System tab under the Secure File Permissions drop-down menu.
- fixmodes-solaris: fix file permissions only for Solaris packages to make them more secure. Available under the System tab under the Secure File Permissions drop-down menu.

The fix-modes utility from the Solaris Security Toolkit adjusts group and world write permissions. It is run with the '-s' option to secure file permissions for Solaris files that were created at install time only. Customer-generated files are not affected.

> Note When this command is run, a file called /var/sadm/install/content.mods is left. Do not delete this file. It contains valuable information needed by fix modes to revert the changes to the system file permissions if the security setting is changed back to medium.

Disabling secure name service databases

The following databases are **disabled** when security is invoked:

- passwd(4)
- group(4)
- exec_attr(4)
- prof_attr(4)
- ser_attr(4)

OS and host information hidden

The ftp, telnet and sendmail banners are set to null so that users in cannot see the hostname and OS level.

> Note All of these services are prohibited with a high security setting, but if they are re-enabled manually the hostname information will remain hidden.

Sendmail daemon secured

Sendmail is forced to perform only outgoing mail. No incoming mail will be accepted.

Network parameters secured

Sun nddconfig security tool is run. For additional information, view the document, Solaris Operating Environment Network Settings for Security, at

http://www.sun.com/solutions/ blueprints/1200/network-updt1.pdf.

NFS port monitor restricted

The NFS server normally accepts requests from any port number. The NFS Server is altered to process only those requests from privileged ports. Note that with the high security setting, NFS is disabled; however if the service is re-enabled manually, the port restriction will still apply.

Xerox FreeFlow Print Server router capabilities disabled

The Xerox FreeFlow Print Server router capabilities is disabled (etc/notrouter file created).

Security warning banners

Security warning banners are displayed when a user logs in or telnets into the Xerox FreeFlow Print Server. This message explains that only authorized users should be using the system and that any others face the possibility of being monitored by law enforcement officials.

enable-ftp and disable-ftp

These options allow for temporary enabling and disabling FTP alone and do not persist through reboots. You must have FTP enabled when using a Continuous Feed system, or FreeFlow® Production Print and NetAgent.

FTP is also required for the Call for Assistance (CFA) feature. The Call for Assistance uses FTP to push printer logs and a Xerox FreeFlow Print Server outload to the Print Server controller.

> Note Temporarily enable FTP through the Xerox FreeFlow Print Server Setup > FTP/Remote Diagnostics menu option.

Creating user-defined profiles

To create a customized profile, the administrator can copy and edit any security profile according to the needs of the customer environment. This new user profile can be selected, edited, set as current, set as default, or deleted.

Setting the current and default profiles

The administrator can select any profile and set it as the Current Profile. This Current Profile persists throughout Xerox FreeFlow Print Server restarts and system reboot until it is changed by the administrator. 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 across Xerox FreeFlow Print Server upgrades. By clicking the Restore Default Profile, the Default profile can be selected as the Current profile. Switching profiles may take several minutes to complete.

Account management

Any interaction between a user and the Xerox FreeFlow Print Server is associated with a user account and is done via a logon session, which is the basis for granting access.

Xerox FreeFlow Print Server user accounts are defined either locally at the device or remotely at a trusted network location like ADS. The local user account is composed of a logon user name and an assigned user group. A user account can be a member of only one user group. It is the user group that is associated with a security profile that defines the privileges of the group.

Default user accounts are provided to allow easy transition from legacy Xerox FreeFlow Print Server versions. For customers that do not require authentication, the Xerox FreeFlow Print Server can be configured to have the system automatically log on using a default user account.

Local users and groups

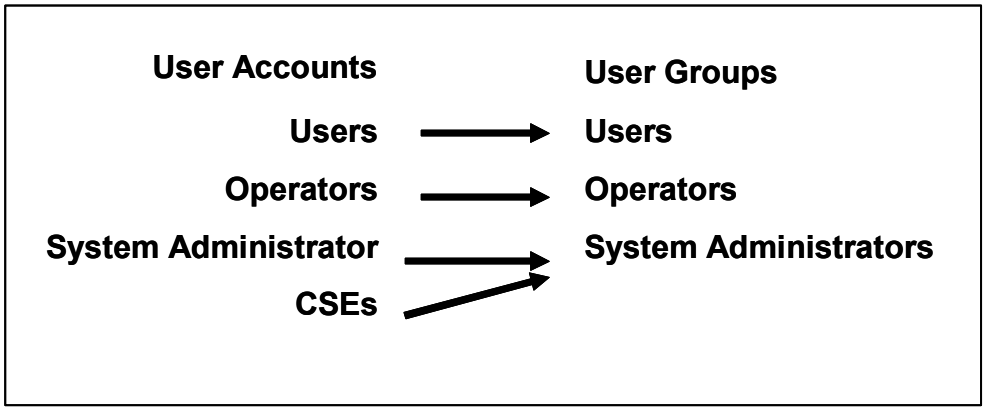
Local user accounts are constructed based on the Solaris operating system model, with its limitations and restrictions, using the [Users & Groups] selection on the Xerox FreeFlow Print Server interface.

- Each local user account has an associated user name between 2-8 characters in length and is case sensitive.
- The user name is a string of characters from the set of alphabetic characters (a-z, A-Z), numeric characters (0-9), period (.), underscore (_), and hyphen (-); the first character must be alphabetic and the string must contain at least one lower case alphabetic character.
- Each account has the following attributes: user name, password, user group, account disabled/enabled, and comments.
- The maximum number of user accounts is 25,000.
- Each local user account has an associated user password that is a sequence of characters that is case sensitive and between 0 - 8 characters in length.
- User accounts are organized into groups. Each user account is a member of only one group.

Default user groups and user accounts

The Xerox FreeFlow Print Server provides three default **user groups**: Users, Operators, and System Administrators. It also supplies four default **user accounts**: User, Operator, SA and CSE. User and Operator accounts correspond to User and Operator User Groups while SA and CSE both correspond to the System Administrators group.

Figure 1: Assignment to Groups



The User, Operator and System Administrator user accounts cannot be edited, deleted, disabled, or removed from the assigned group. The CSE account can be removed from the System Administrator group and assigned to another group or disabled.

Note It is the group that a user is associated with that defines the privileges of the user, not the current security profile.

Creating user accounts

The Xerox FreeFlow Print Server user interface enables the Administrator to manage accounts easily by selecting [Setup], [Users & Groups], and the [Users] tab.

When the administrator selects the Users tab, a pop-up window appears that enables the administrator to create, edit, or delete an account and indicate whether the account should be enabled or disabled.

Group authorization

Job Management and Customer Diagnostics are two functions of the Xerox FreeFlow Print Server that the administrator may choose to restrict. From the Setup > Users & Groups menu option, select the "Group Authorizations" tab in the interface. The administrator can choose to enable or disable the service for a particular user group.

Note The following table describes the functions allowed for the three built-in groups. The column labeled as Changeable via Graphical User Interface (GUI) implies that the function/service can be enabled/disabled from the Users & Groups / Group Authorization tab.

Table 2-6 Enable/disable from the Group Authorizations tab

Function	Users	Operators	Administrators (sa and cse)	Changeable via GUI	Comment
Job Management (release, hold, proof, promote, move, delete, … etc)	-	Enabled	Enabled	Yes	
Queue Management (New, Delete, Properties)	-	Enabled	Enabled	No	
Queue Job Operations(Accept Jobs, Release Jobs, …etc)	-	Enabled	Enabled	No	
Reprint Management	Enabled	Enabled	Enabled	No	The Limit Print Service Paths in Security Profile controls the directories that users can reprint. The defaults are: DEFAULT- Operating System Only, Saved Jobs, and CD-ROM (Removal Media). LOW - Saved Jobs and CD-ROM (Removable Media). MED - CD-ROM (Removable Media). HIGH - Nothing. CUSTOM - User Defined.
Printer Manager(Finishing, Image Quality …etc)	-	-	Enabled	No	
Resource Management(LCDS Resources, PDL Fonts, Forms, ….etc)	-	Enabled	Enabled	No	
Accounting, Billing	-	Enabled	Enabled	No	

Function	Users	Operators	Administrators (sa and cse)	Changeable via GUI	Comment
System Preferences	-	Can set International, Job Processing, Stocks & Trays	Enabled	No	
Setup (System configuration, Gateways)	-	View & Print only	Enabled	No	
Setup (Feature licenses, Network configuration)	-	-	Enabled	No	
Setup (Security profile, SSL/TLS, IP Filter)	-	-	Enabled	No	
Setup (Users & Groups)	-	-	Enabled	No	
Change password	Self	Self	Enabled	No	
Service Diagnostics	-	-	Enabled	No	
Customer Diagnostics	Enabled	Enabled	Enabled	Yes	
Backup / Restore	-	Enabled	Enabled	No	

Auto-Logon

The Automatic Logon feature enables or disables the ability of users to directly access the Xerox FreeFlow Print Server, including Web UI (HTTP) access to the Print Server, without having to manually log on. It is enabled in the Default Operating System Only, Low, and Medium security profiles, and disabled in the High security profile. The feature can be configured by any member of the System Administrators group. To configure the Automatic Logon feature, a custom profile must be created under Security Profiles by copying one of the default security profiles. An administrator must then set the new profile as current and enable the Automatic Logon feature by selecting the checkbox under the General tab. When Automatic Logon is enabled, a user account must be specified. The default is set to automatically log on as user. When Automatic Logon is disabled, the Xerox FreeFlow Print Server will not launch completely until users log on via a logon window. This window will appear before the Xerox FreeFlow Print Server UI is displayed and will require users to manually log on before accessing the Xerox FreeFlow Print Server.

Note When the Automatic Logon feature is enabled, users are not required to log on to gain access to the system. In this case, the allowed access to the Xerox FreeFlow Print Server is established by the privileges of the user account in Automatic Logon. For example, if Automatic Logon is enabled and the user account is Administrators, then the Xerox FreeFlow Print Server will be open and all access to the Xerox FreeFlow Print Server will be granted.

Default Screen/Auto-Logoff

Under [Setup/System Preferences/Default Screen], any member of the operator or system administrators group can select which of the Xerox FreeFlow Print Server screens (Job or Print) the UI should return to after a specified amount of time (1-10 minutes) of inactivity (i.e. no movement from the keyboard or mouse). When the time-out occurs, the user will also be changed to the user account specified for auto-logon. If auto-logon is disabled, a user will be forced to log in again before the Xerox FreeFlow Print Server UI is displayed.

Password security

When the system is installed, the Change System Password dialog box appears and prompts users to establish all System Default Accounts with new passwords. For security reasons, **all system passwords must be changed.**

- **root:** has super user access to the workstation. The initial password for this account is set during installation of the operating system and should be obtained from the Xerox service personnel.

  Note For security reasons, the root account password should be changed as soon as the Xerox service personnel have completed the installation.

- The Xerox user name is the account from which the Xerox software runs. Enter the Xerox user password for this account. Contact your Customer Service Representative if this is unknown.

  Note The administrator should verify access to the Xerox application for all levels before the service installation personnel leave the site

- **ftp:** an account to permit some clients to retrieve their software from the Xerox FreeFlow Print Server controller using the TCP/IP communication protocol. This account will be set to Read-only access to the /export/home/ftp directory

  Note To maintain system security, it is recommended that any restricted access login be terminated as soon as the session has been completed.

  Note The user and group identifications, uid and gid, for the Xerox accounts that are listed above cannot be arbitrarily changed in the password and group files to new values because the software is based on the proper access to the Xerox supplied files.

  Note Please be aware that Xerox Customer Support Personnel must have access to the new root password for service and support. It is the customer's responsibility to ensure that the root and system administrator passwords are available for them.

Strong Passwords

The Xerox FreeFlow Print Server provides additional security for users required to adhere to strict security guidelines. It provides a means in which a strong password policy can be enforced.

Strong Passwords can be Enabled and Disabled (default setting) via the Password Policies window.

Strong passwords must consist of ALL of the following;

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

  Note The strong password requirements cannot be modified. A strong password cannot be set for root or any other Solaris user accounts that are not created by the Xerox FreeFlow Print Server.

In addition, the passwords will be forced to adhere to the following;

- A minimum password age (minimum number of days)

    - (default is one)
- A maximum password age (maximum number of days)
    - (default is 90)
- A password history (default is 10 previous passwords)

  Note The default values can be modified by editing the etc/default/passwd file to nothing, as shown below;

  MAXWEEKS=

  MINWEEKS=

  HISTORY=

How to Enable/Disable Strong Password

- From the Setup menu select [Users and Groups]
- From the Policies drop down menu select [Password]
- Enable/Disable Strong Password from the Password Policies window. The default setting is Disable.

Login Attempts Allowed

The Xerox FreeFlow Print Server has provided a means to lockout users after reaching the maximum number of consecutive attempts. Once this is done, the user will need to apply (reset) a security policy and reboot the system.

The number of failed attempts and enable/disable is configurable via the Password Policy screen. When enabled, login attempts can be set from 1-6 attempts before the user is locked out. This function will only apply to failed login attempts via the Xerox FreeFlow Print Server UI and does not apply to the root (su) user.

Note Remote Network Server: If running NIS+ name service, strong passwords would be enforced via the NIS + server. 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.

How to Enable/Disable Login Attempts

- From the Setup menu select [Users and Groups]
- From the Policies drop down menu select [Password]
- Enable/Disable Login Attempts from the Password Policies window. The default setting is Disable.

Password Expiration

The System Administrator can set a password expiration via the Solaris Management Control.

Note SMC (Solaris Management Control) has replaced AdminTool. AdminTool has been retired in Solaris 10.

1. Open a terminal window and login as root
2. Type: smc &

3. Go to: System Configuration -> Users -> User Accounts-> <select user> -> Password Options tab
4. Enter values in the drop down menus associated with each password expiration parameter.

The Xerox FreeFlow Print Server UI does not handle password expiration. Thus, the Print Server will not prompt the user to enter a new password if his/her password has expired. Instead, a message is posted indicating unknown user name or password. It is up to the customer to determine that the password has expired. To do so, the customer should open a terminal window and attempt to login as the user in question. If the password has expired, the system will prompt for the user to enter a new password.

Audit Logs

GUI Logging

Mouse clicks within the Xerox FreeFlow Print Server UI can be monitored via the Log Console. These activities are associated with the current user. This feature can only be enabled/disabled by members of the System Administrators group.

User Activity on the System

When the High security profile is enabled, the Solaris Basic Security Module (BSM) is activated.

Date/Time User Login/Logout

This information is kept in the authlog and syslog in the /var/log directory. Login/Logout to the Xerox FreeFlow Print Server is tracked as well as Network Login/Logout.

Changing individual passwords

There are two ways to change passwords: Users can change their own passwords using the selection on the Logon menu and the administrator can change the password by double clicking on the user name in the User tab of [Users and Groups Management].

Accessing the Xerox FreeFlow Print Server through ADS

If the Xerox FreeFlow Print Server has been configured to join a Windows 2000 ADS domain, users may log onto the printer using their Microsoft Active Directory Services (ADS) user names.

To provide this option, the administrator must first configure the Xerox FreeFlow Print Server appropriately for the DNS gateway (see the Gateway and Network Configuration section of this guide). Additionally, the administrator must access the [ADS Groups] tab through [Users and Groups Management] and specify or edit the mapping of the ADS groups to the Xerox FreeFlow Print Server user groups having permission to log on to the printer.

Configure Print Server to Join the ADS Domain

To enable the ADS user accounts, the Xerox FreeFlow Print Server must have DNS enabled and joined to the appropriate ADS domain.

1. Logon to the Xerox FreeFlow Print Server as a member of the System Administrators. From the Network Configuration option, select the DNS tab, make sure that the Enable DNS check box is checked. Ensure that the DNS Server list is filled in with the IP addresses of up to three DNS servers to search when resolving host names to IP addresses. This is part of the network configuration procedure.
2. Select the ADS tab, and enter in the fully qualified domain name of the ADS domain.
3. Click Join to join the Xerox FreeFlow Print Server to the ADS domain specified.

   Note If DNS is not enabled, the Join button is not available.

Map the ADS groups to the Print Server user groups

From the Setup menu, Users & Groups option, select the ADS Groups tab. A member of the System Administrators group can specify, view and edit the mapping of ADS Groups to the three Xerox FreeFlow Print Server user groups (Administrators, Operator, Users) permitted to log on to the printer.

Log on to the system with ADS user names

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

Note For this feature to work, Administrators must ensure that DNS is enabled, the Xerox FreeFlow Print Server is configured to join the ADS domain, and ADS groups are mapped to the Xerox FreeFlow Print Server user groups.

Troubleshoot ADS

Refer to the online help feature when troubleshooting ADS.

Limiting access

The Xerox FreeFlow Print Server provides options that allow the administrator to block or limit access to the system.

IP Filtering

IP Filtering allows the administrator to block IP addresses and provides access to services such as: LPR, IPP, HTTP, HTTPS, SMB Filing, Raw TCP Printing, and FTP Connections.

The administrator can limit access through the Xerox FreeFlow Print Server interface [Setup > IP Filtering menu option]. The filter allows the blocking of specific IP addresses or a range of addresses from accessing the system. Available options include: Enable All Connections, Disable All Connections, Enable Specified Connections. Additional subnet mask can also be specified.

Refer to online help for a detailed description of the IP Filtering feature. To limit access to the RPC ports, (NFS, traceroute, Portmap), use the IP Filter within the security profile under the RPC tabs.

> Note If using the Xerox FreeFlow Print Server Remote Workflow services, be sure to include the client in the members list as the application utilizes RPC.

Remote Workflow

Remote Workflow allows for a remote connection to the Xerox FreeFlow Print Server controller.

The administrator can limit access through the Xerox FreeFlow Print Server interface [Setup > System Preferences menu option]. Remote Workflow options include: Enable All Connections, Disable All Connections, Enable Specified Connections (by specific IP Address).

> Note The default is Enable All Connections.

Secure Socket Layer/Transport Layer Security (SSL/TLS)

The Xerox FreeFlow Print Server utilizes SSL/TLS which, when enabled, provides a secure (i.e. encrypted) path for the server to receive print jobs from clients (ex. FreeFlow MakeReady) via secure HTTP (HTTPS) or secure IPP (sIPP).

Using the SSL/TLS Security Feature

The Secure Socket Layer/Transport Layer Security (SSL/TLS) feature can be used to provide a reliable end-to-end secure and authenticated connection between two points over a network. The Xerox FreeFlow Print Server SSL/TLS user interface allows a System Administrator to do the following:

1. Create and use a self-signed SSL/TLS certificate
2. Use an existing certificate obtained from a certificate authority (i.e. VeriSign, Thawte, etc.)
3. Choose the mode in which the SSL/TLS feature will operate (normal or secure)
4. Choose an encryption strength

Creating and Using a Self-Signed Certificate

Using the Add Certificate wizard within the SSL/TLS UI, a System Administrator may create a Self-Signed Security Certificate. The wizard will request some basic information from the user. After the certificate is created, the fields within the SSL/TLS UI will be populated with the provided information, and the user will be able to select which mode and encryption strength they would like to use.

Using a Signed Certificate from a Certificate Authority

A System Administrator may also use the Add Certificate wizard to utilize a signed security certificate (.pem file) that's been obtained from a Certificate Authority (ex. VeriSign, Thawte, etc.).

Disabling SSL/TLS

The SSL/TLS feature is disabled by default. Once a certificate is added using the SSL/TLS Add Certificate wizard, the feature will be enabled. If the System Administrator wishes to disable the feature, they may do so by de-selecting the Enable SSL/TLS checkbox within the SSL/TLS UI.

Digital Certificates

SSL/TLS cannot be enabled unless a digital certificate has been installed on the system, using the Add Certificate button. Installing a digital certificate can only be done by someone with administrator privileges.

The administrator selects SSL/TLS from the [Setup] Menu and clicks on the [Add Certificate] button. This invokes the Add Certificate wizard. There are two options regarding digital certificates. One option is Self-signed certificate. This is selected when no third party Certificate Authority is being used.

Another option is Signed Certificate from a Certificate Authority. In this case, the administrator needs to supply the fully qualified domain name, IP address, organization and country of the Certificate Authority.

If the choice is to use a Certificate Authority, all Certificate information needs to be held in a file and sent to the Certificate Authority. The Authority returns a valid certificate that must be installed on the system.

> Note A self-signed certificate is not as secure as a certificate signed by a Certificate Authority. 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.

Once the Digital Certificate has been installed, the Enable SSL/TLS selection becomes available among the [Setup] options. At that time the administrator can select the mode of operation, Normal or Secure, from a drop-down menu.

Network Protocol

This section addresses Network Protocol, name service changes and the changes that occur when security is invoked.

The table below addresses the list of Network Protocols that are used by the Xerox FreeFlow Print Server software or Xerox client operations.

Table 2-7 Network Protocols

Network Protocol	Required
Samba (SMB)	Network sharing protocol required for Hot Folders and SMB filing (Nuvera only).
XSun	Required for functionality of Xerox FreeFlow Print Server diagnostics software.
HTTP	Used when connecting to the server via the HTTP gateway. Connections can also be filtered using the IP Filter feature under Setup -> IP Filter. Note When SSL is disabled (off) other web-based logins provided by the Xerox FreeFlow Print Server may not be secure. Use the HTTPs qualifier to guarantee a secure interaction.
Tomcat web server	Required for the functionality of the Xerox FreeFlow Print Server Internet Services gateway and the Xerox Remote Services application.
IPP	Required for job submissions from the FreeFlow® Print Manager and/or a Digipath (FreeFlow 2.0+) client. The IPP gateway can be enabled/disabled under Setup -> Gateways -> IPP tab. Connections can also be filtered using the IP Filter feature under Setup -> IP Filter.
Sun RPC	Used by many different clients, including DigiPath/FreeFlow and Xerox FreeFlow Print Server Remote WorkFlow (DRW), and network services such as NIS+. Typically used to establish a connection to the server, which then redirects the connection to another open port using OS level port management. This service is shutdown when Xerox FreeFlow Print Server security is set to high. Connections can also be filtered using the IP Filter feature under Setup -> Security Profiles -> <Any Profile> -> RPC tab
SNMP	Used for SNMP message exchange and traps. The SNMP gateway can be enabled/disabled under Setup -> Gateways -> SNMP.
WINS	Required when in an environment where connection to a WINS server is necessary. WINS service can be enabled/disabled under Setup -> Network Configuration -> WINS tab.
Socket (Raw TCP/IP) Printing	Required if jobs will be submitted via the socket gateway. The socket gateway can be enabled/disabled under Setup -> Gateways -> Socket. Connections can also be filtered using the IP Filter feature under Setup -> IP Filter.
LPD (LP/LPR)	Required for job submissions via the LP/LPR gateway (LP/LPR client, Xerox FreeFlow Print Server Print Service (Reprint), etc.). The port assigned to the LPD can be changed and/or the gateway can be enabled/disabled under Setup -> Gateways -> LPD.
SSH	Access the server via a secure shell (SSH, SFTP, etc.).

Network Protocol	Required
FTP	Access the server via FTP and/or submit jobs from a DigiPath/FreeFlow client via the Digipath/FreeFlow Print Manager. This service (ftpd) is shutdown when Xerox FreeFlow Print Server security is set to high. In FreeFlow v2.0, the client has the ability to use secure FTP (sFTP) when Xerox FreeFlow Print Server security is set to high and FTP is not available. Connections can also be filtered using the IP Filter feature under Setup -> Security Profiles -> <Any Profile> -> RPC tab.
SSL	Required when using the TLS/SSL security feature and/or a FreeFlow 2.0+ client with Xerox FreeFlow Print Server security is set to high. Connections can also be filtered using the IP Filter feature under Setup -> IP Filter.
NFS	Necessary when using NFS mounted directories. This service is disabled when Xerox FreeFlow Print Server security is set to high. Connections can also be filtered using the IP Filter feature under Setup -> Security Profiles -> <Any Profile> -> RPC tab.

Note The IP Filtering (Setup->IP Filter) feature can also help in limiting access to the server. This is the Xerox FreeFlow Print Server's GUI interface to the SunScreen Lite firewall that is part of the Solaris 8 Operating System. This feature allows the user to limit the number of clients who are allowed to access the server via services such as LPR, IPP, HTTP, HTTPS, SMB Printing, and FTP. By default, the firewall is disabled (all ports open), but can be enabled to either only allow specified connections (by IP address, IP address range, or subnet mask) or to close all ports. For DRW clients, this mechanism exists under System Preferences -> Remote Workflow -> Enable Specified Connections.

Note FreeFlow® v2.0 and newer allows users to select whether or not the Xerox FreeFlow Print Server server 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).

Secure Print

MICR mode

The MICR mode disables all Xerox FreeFlow Print Server features that allow additional prints to be produced (such as Sample Print, Reposition Output, etc.).

Prevent Unauthorized Queue Changes

Queue Lock

- Queues can be locked and unlocked by the System Administrator.
- Properties of a locked queue cannot be changed without first unlocking the queue.
- Locked queues can only be deleted by the System Administrator.
- Locked queues can be copied by an Operator. The resulting new queue will not be locked.
- An Operator can change the Accept/Do Not Accept Jobs and Release/Do Not Release Jobs attributes on a locked queue.
- Placing the cursor on the tool tip accesses the date and time the queue was last locked.

Roles and responsibilities

Xerox will make every effort to assist the administrator in ensuring that the customer environment is secure.

Xerox responsibilities

Xerox is committed to providing a level of security which will allow the Xerox FreeFlow Print Server controller to be a good network citizen in response to current security intrusions. Additional security beyond this remains the responsibility of the customer.

Xerox is constantly evaluating the security of the Xerox FreeFlow Print Server controller and the Sun Solaris operating system. Xerox is committed to providing the latest Solaris security patches provided by Sun Microsystems in each major Xerox FreeFlow Print Server release. The Xerox FreeFlow Print Server development team will also add Solaris security patches in between major release cycles. All OS security patches for applications that are added during a Xerox FreeFlow Print Server install will be included, even if the application code is not normally used by Xerox FreeFlow Print Server users. Security patches for applications that are not loaded by a Xerox FreeFlow Print Server install will not be evaluated or included. Only the version of a patch impacting security will be included. If a security patch has a newer version that is not security related, then this patch will not be updated to the newer version. Any security patch that is determined to have a negative impact to Xerox FreeFlow Print Server operation will not be added.

Customer Responsibilities

The administrator has the primary responsibility for maintaining the security of the network within the customer site. It is important that network security is continuously monitored and maintained, and that appropriate security policies are established and followed.

The procedures outlined in this document assume a basic knowledge of UNIX, the vi editor, and general computing concepts. It is expected that the network administrator or system administrator responsible for network security understands the base commands (cd, chmod, cp, grep, kill, ln, ls, man, more, ps, etc.), and the UNIX directory path and filename structures shown in this document.

There is information within the text and in the appendix sections for reference to those who may not use UNIX often.

The Xerox FreeFlow Print Server operates on a Solaris OS. Enhancements have been made to increase security over the default OS configuration. Additional Solaris patches required by the Xerox FreeFlow Print Server are included as well. Several scripts are used to provide additional security for the Print Server. Not all scripts are public knowledge, only those that are public are defined in this document and these can be performed by the customer.

Xerox FreeFlow Print Server engineering will evaluate the latest Sun Security Alert Packs issued by Sun Microsystems and integrate these patches into the Print Server releases. Local customer support will be responsible for loading the latest Print Server software.

Xerox strongly recommends that the customer change passwords from the default settings since the ultimate security of the printing system resides with the customer.

Note Please be aware that the Xerox Customer Support Personnel must have access to the new root password for service and support. It is the customer's responsibility to ensure that the root password is available for them.

Security tips

The following recommendations will enhance security.

Virus Scan

The Xerox FreeFlow Print Server runs on the Solaris 10 Operating System (OS). This OS makes the Xerox FreeFlow Print Server less susceptible to virus and worms.

Online Help for security

A great deal of helpful security information can be found in Online Help. Security tools and blueprints may be found at:

http://www.sun.com/solutions/blueprints/

Other security information, including alerts, may be found at:

`http://sunsolve.sun.com/pub-cgi/ show.pl?target=security/sec`

http://www.cert.org/nav/ index_main.html

http://www.cve.mitre.org/

http://www.xerox.com\securi