June 2016
702P04294

Xerox® FreeFlow® Print Server Security Guide version 21 and higher

BR 11741

Document version 1.0: July 2015

Contents

Overview 1

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 Windows®. To enable them to set up 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

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

Xerox® FreeFlow® Print Server/Windows® Security Updates

The FreeFlow® Print Server/Windows device is a specialized Digital Front End (DFE) intended to drive selected Xerox® printers. The FreeFlow® Print Server software is tightly coupled with the Windows Embedded Standard 7 (WES7) operating system. This software may not be used for any purpose other than to drive the Xerox® printer.

Microsoft Corporation releases Windows Updates monthly; some of these updates may be applicable to the FreeFlow® Print Server/Windows device. Xerox will test the applicable updates before recommending that these updates be installed by the End User or Xerox Service.

Comprehensive Security Updates for the FreeFlow® Print Server/Windows DFE are tested and released every quarter. Updates needed to resolve critical vulnerabilities that are applicable to your product will be released in a timely manner, as driven by severity and priority.

The FreeFlow® Print Server/Windows Updates are downloadable and installed using the FreeFlow® Print Server Software Update Manager feature. If the customer cannot use this feature (e.g., their FreeFlow® Print Server systems are not permitted to connect to the Internet by the Customer's Security Management policies), they should contact Xerox Customer Service for assistance. Refer to the phone numbers in the section Customer Support on page 1-1 of this document.

Customers are encouraged to contact the Xerox Product Security Team to escalate security audit reports for review and response. It is very important that the submitter provide as much information as is available regarding the Security Vulnerability Scan Product used in generating the report. Supplying the Common Vulnerability Exposure (CVE) number associated with the security findings in the audit will help ensure a quick response.

To contact the Xerox Product Security team, use the link in the lower right corner of this web page (Contact Information):
http://www.xerox.com/information-security/enus.html

Xerox® FreeFlow® Print Server Security Profile

The Xerox® FreeFlow® Print Server software provides a static, system-supplied, FreeFlow® Print Server Security Profile as an option to define a Standard (default) or a High level of system security. Only the Windows Administrator role can change the FreeFlow® Print Server Security Profile option. A restart or shutdown of the FreeFlow® Print Server/Windows system after changing the FreeFlow® Print Server Security Profile is not required as changes are applied dynamically. The customization of system security tightening outside of the FreeFlow® Print Server Security Profile settings can be accomplished using Windows Control Panel applications.

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. A "custom" Security profile is created by copying one of the system-specified Security profiles to a new profile name. The settings for a newly created profile are initially defined by the system-specified Security profile that was copied. The configuration settings of the "custom' Security profile can be modified to meet customer site-specific requirements. Multiple custom profiles can be saved on the system assigned with their own custom assigned name to help the Windows FreeFlow® Print Server Administrator readily differentiate between them.

The table below lists the features that are controlled by each FreeFlow® Print Server system-supplied, FreeFlow® Print Server Security Profile. It includes the default settings for each FreeFlow® Print Server Security Profile. See the Profile feature options and FreeFlow® Print Server Security Profile settings below:

FreeFlow® Print Server Security Profile Feature	Standard Security	High Security
Dump File Creation	Disabled	Enabled
Enable Dead Gateway Detection	Disabled	Enabled
FTP	Enabled	Enabled
Keep Alive Time	120 Minutes	30 Minutes
No Name Released On Demand	Disabled	Enabled
Peripheral Devices	Enabled	Disabled
Perform Router Discovery	Enabled	Disabled
Strong Password	Disabled	Enabled
Synchronize Attack Protect	Disabled	Enabled
User Account Control (UAC)	Disabled	Enabled
Windows Security Patch Update	Disabled	Disabled
Protected Mode	Enabled	Enabled

FreeFlow® Print Server Security Profile Feature	Standard Security	High Security
Firewall	Enabled	Enabled
SNMP	Disabled	Disabled
Telnet	Disabled	Disabled
AutoPlay	Disabled	Disabled
DEP	Enabled	Enabled
Show Hidden Files	Enabled	Disabled
Windows System Restore	Enabled	Enabled
FIPS	Disabled	Enabled
SSLv2	Disabled	Disabled
SSLv3	Enabled	Enabled

The table below includes a description of all the features available for configuration setting changes managed by the FreeFlow® Print Server Security Profile. See the profile feature options and their descriptions below:

FreeFlow® Print Server Security Profile Feature	Feature Description
Dump File Creation	The FreeFlow® Print Server/Windows system captures crash log files when there is a critical system failure to be used as an aid for troubleshooting the root cause of the problem. It is possible for these crash logs to contain information from a customer job, so there could be some PII/PHI data. When the FreeFlow® Print Server Security Profile is set to Standard, the crash logs are captured and available on the system. When the FreeFlow® Print Server Security Profile is set to High, the dumping of crash files is disabled. This will make it more difficult for engineering to determine the cause of a crash, but will avoid the risk of capturing sensitive customer data in the Dump file.
Enabled Dead Gateway Detection	The default network gateway router in the router table could be down and unavailable which can result in failures to communicate through network routes. When the FreeFlow® Print Server Security Profile is set to High, the system detects that the default router gateway is not available, and uses another router gateway from the local IP routing table. When the FreeFlow® Print Server Security Profile is set to Standard, this failure recovery action is not performed.
FTP	The standard FTP service on the FreeFlow® Print Server system is disabled when the FreeFlow® Print Server Security Profile is set to High. All FTP functionality is available when the FreeFlow® Print Server Security Profile is set to Standard.

FreeFlow® Print Server Security Profile Feature	Feature Description
Keep Alive Time	If the keep alive request comes back with a negative response, that link is assumed to be down, and another network route can be considered to deliver the network request. This ensures that communication over the network continues even when a particular link is not available. As the feature name **keep alive** suggests, this capability is intended to ensure that the peer-to-peer communication between two internetwork host platform is "kept alive" and can achieve successful communications. The timeout is 180 minutes when the FreeFlow® Print Server Security Profile is set to Standard, and is 30 minutes when set to High. Therefore, if the FreeFlow® Print Server Security Profile is set to High, an alternative link is attempted more quickly when a link is down.
No Name Released On Demand	The option enables/disables the response of the NetBIOS name defined on the FreeFlow® Print Server system when a name release was received at the session layer of the network by a remote Windows client. An attacker can send a spoofed **Name Release** or **Name Conflict** message to a system that supports NetBIOS (such as FreeFlow® Print Server) and force it to remove its own legitimate name, leaving it unable to respond to or initiate other NetBIOS requests. This renders the FreeFlow® Print Server system unable to communicate with other NetBIOS hosts which is a denial-of-service attack. This option is enabled when the Windows Firewall Profile is set to High which prevents these attacks. This option is disabled for the Windows Firewall Profile of Standard.
Peripheral Devices	When the Windows Firewall Profile is set to Standard, peripherals such as USB/DVD and calibration devices, can be accessed. Setting the Windows Firewall Profile to High prevents access.
Perform Router Discovery	The FreeFlow® Print Server/Windows system automatically performs ICMP router discovery during start-up or software initialization when the Windows Firewall Profile is set to Standard. An attacker can listen for these router requests and spoof the requested by representing a valid network router. The automatic router discovery is disabled when the Windows Firewall Profile is set to High.
Strong Password	The password security feature forces the FreeFlow® Print Server system to adhere to stricter security guidelines by defining strong password policies. The make-up of a strong password must meet criteria with a minimum complexity criteria. (E.g., Password history which is how many unique passwords must be used before one can be reused, minimum/maximum age which is how long before a password can be changed and when it must be changed, etc.)

FreeFlow® Print Server Security Profile Feature	Feature Description
Synchronize Attack Protect	This security option is intended to prevent TCP SYN flood which is a form of denial-of-service attack where an attacker sends successions of SYN requests to a target system trying to consume system resources until that system becomes unresponsive. The protection against TCP SYN flood is minimal when the Windows Firewall Profile is set to Standard. When the Windows Firewall Profile is set to High, the TCP connection quickly times out during a TCP SYN flood which ensures protection for the integrity of the system.
User Account Control (UAC)	This feature defines notification level to the user logged into Windows when an application needs to make system changes, or Windows settings require Administrator permission. The user sees the display brightness dim, and has to approve or deny the application request to make these changes. Only the non-Administrator user receives these notifications when the Windows Firewall Profile is set to Standard. All users, even the Administrator, receive the notifications when the security is set to High.
Windows Security Patch Update	See Xerox® FreeFlow® Print Server/Windows® Security Updates on page 2-1. The automatic Updates feature for Windows updates must be disabled to ensure proper operation of the FreeFlow® Print Server. This capability is disabled when the Windows Firewall Profile is set to Standard or High.

Account Management

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

Xerox® FreeFlow® Print Server user accounts are defined locally at the device. 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 Windows Firewall Profile that defines the privileges of the group.

Default user accounts are provided to allow easy transition from legacy Xerox® FreeFlow® Print Server versions.

FreeFlow® Print Server/Windows Users and Groups

The Xerox® FreeFlow® Print Server/Windows system has two separate users and groups mechanisms to manage users and groups. The first is the Windows Embedded Standard 7 (WES 7) management for User and Group accounts which is a standard Windows capability. The mechanism in Windows is referred to as User Account Control (UAC) which is considered a security component allowing the Windows Administrator to manage the credentials for non-administrator users to perform tasks. The application also includes its own user and group account management capabilities to assign roles for managing the print server configuration, managing print jobs, and printing-related operations.

The FreeFlow® Print Server application is delivered with the following built-in, or default, login user accounts:

- System Administrator (sa)
- Printer Operator (operator)
- Walk-up User (user)

These user accounts cannot be removed from the system. However, any built-in account of the FreeFlow® Print Server may be “locked” by the System Administrator to ensure that unique, customer-created accounts are used in place of these built-in accounts. This capability is important to customers who require audit logs that identify who has accessed the system.

In addition to the print server application user accounts, there are also two built-in Windows accounts:

- Administrator
- Guest

There are also three FreeFlow® Print Server users that are created by the Windows Users Management application:

- cse
- ftpuser
- xrxusr

The following user groups are available on the Windows 7 system:

- Standard
- Administrator

By default, newly added users in Windows become members of the Standard group. The number of users that are added in the Administrator group should be very limited (e.g., Windows Administrator, and CSE). Important information about these accounts is outlined below:

Administrator

1. This is a built-in Windows 7 user with full read/write access to Windows system (e.g., applications, utilities, command window, files/directories, etc.).
2. The role of the Administrator account is to make system-level, application and configuration changes to the Windows and FreeFlow® Print Server such as:
   - Manage Windows Users/Groups
   - Manage Windows Network/Security settings
   - Install Windows/FreeFlow Print Server applications and updates
3. The Administrator user is a member of the Administrator group.
4. It is highly recommended that another Windows user be created with Administrator privileges for recovery of the original Administrator account, if needed.

Guest

1. This is a built-in Windows 7 user with limited access to the Windows system including:
   - Applications granted by Administrator
   - Utilities
   - Files and directories under the Guest home directory only
2. The Guest account on the FreeFlow® Print Server/Windows configuration has no role and is disabled.
3. The Guest user is a member of the Standard group.

cse

1. The FreeFlow® Print Server installation creates the **cse** user with Windows User management with full read/write access to Windows system including:
   - Applications
   - Utilities
   - Command window
   - Files and directories
2. The role of this **cse** account is for the Xerox Service or Customer Service Engineer (CSE) to diagnose and report any FreeFlow® Print Server/Windows hardware and printer problems or software problems. The CSE must have access to all of the system diagnostic and service utilities.

3. The **cse** user is a member of the Administrator group.
4. The Xerox CSE must have access to the **cse** password, **sa** password, and/or possibly the Windows Administrator account password during a service call. The customer IT group can define its own password for the **cse** account, but must provide it to the Xerox CSE when he or she needs to access the system for diagnosis. Alternatively, the customer must be present to enter the passwords when required. The Xerox CSE will not be able to perform the service call responsibility without appropriate access to the FreeFlow® Print Server system.

ftpuser

1. The FreeFlow® Print Server installation creates this **ftpuser** with Windows User management with limited access to the system such as a home directory location.
2. The role of this **ftpuser** user is for remote access by remote client applications such as XEAR.
3. The **ftpuser** is a member of the Standard group.

xrxusr

1. The FreeFlow® Print Server installation creates the **xrxusr** with Windows User management with limited access to the system.
2. The **xrxusr** is a member of the Standard group.

Accessing the System

Users of the FreeFlow® Print Server can access the system in any of the following ways:

- Through a Web-based FreeFlow® Print Server application
- Remotely over the network with Remote Desktop Connection (the same way as users of Windows operating system users)

Accessing the System through the Web Application

All FreeFlow® Print Server Web application actions or command window actions are associated with a FreeFlow® Print Server user account. This association is created when the user logs into the FreeFlow® Print Server/Windows system, and is the basis for granting access (authorization). A FreeFlow® Print Server Web application or Windows Remote Desktop logon session begins upon successful Authentication (verification) of a user name and credentials (password).

The logon session ends by the user logging off, or by the expiration of the logon session; the default time-out value is 30 minutes. Once the FreeFlow® Print Server Web application or Windows Remote Desktop login is established, the user can interact with the system, subject to the Authorization (i.e., Access Control Policies) associated with the settings such as the associated user group, and the Job Management Access Control options. Authorization of user functions is managed by **Role-Specific Privileges** whereby the Windows operating system validates access based on permissions assigned to user roles. Each user is associated to roles by the group they are assigned to.

Accessing the System Using Remote Desktop Connection

The Xerox® FreeFlow® Print Server version 20.0 supports the use of the Windows Remote Desktop Connection, which enables a user to connect to the print server remotely from a client PC. Connecting remotely is the recommended method for the Administrator to directly access the operating system of the FreeFlow® print server to perform system maintenance and configuration tasks. By default, the print server will permit only the Windows Administrator account to log in using this method.

Remote Desktop Client software is available from Microsoft and is included with certain versions of Windows Vista, Windows 7, and Windows 8. More information is available from Microsoft:
http://windows.microsoft.com/en-us/windows7/products/features/remote-desktop-connection

Password Security

Each of the built-in User accounts for the FreeFlow® Print Server has a “well known” password assigned when the product is shipped and installed by Xerox. The built-in, default User accounts are:

- FFPS Administrator
- FFPS Operator
- FFPS User

The passwords for these accounts should be changed once the software is installed to ensure security. Customers can change these passwords using the FFPS Administrator account. The built-in user accounts are accessible through the user interface for the FreeFlow® Print Server, and are separate from the Windows built-in users. Changing password policies for these users is done by logging into the printer using the user interface for the FreeFlow® Print Server.

There are also two built-in User accounts for Windows:

- Windows Administrator
- Windows Guest

Additionally, there are users defined for the FreeFlow® Print Server/Windows system level roles:

- CSE
- FTP User
- XRXusr

For access to both the Windows built-in users and the users installed for the Windows environment by the FreeFlow® Print Server installation, use the Windows Remote Desktop application. Changes to the password policies for these users are made by logging into the printer using the Windows Remote Desktop. The customer is also advised to set passwords on these accounts according to their password policies once the software is installed. Passwords can be changed from the Windows Administrator user.

The FreeFlow® Print Server/Windows system provides additional user security by applying more-complex passwords and customizable policies that force users into adhering to much stricter security guidelines. A **strong password** must satisfy **all** of the complexity requirements below:

- Not contain FFPS User account name nor any part of user’s full name more than two consecutive characters.
- Have a minimum of six characters
- Have characters from three of the categories below:
  - Uppercase characters (A through Z)
  - Lowercase characters (a through z)
  - Numeric digits (0 through 9)
  - Non-alphabetic characters: (E.g., !, $, #, %)

Parameters to customize password security that ensures strong password polices are described below:

Meet Password Complexity Requirements

Description:	This parameter is used to enable or disable the password complexity requirements that enforce strong password settings.
Allowable Values:	Enable/Disable
Windows 7 Default Value:	Disable
FreeFlow Print Server Web User Interface Default Value:	Disable

Password History

Description:	This parameter defines the number of unique password changes required before a password for a user account can be reused.
Windows 7 Allowable Range:	0 - 24
FreeFlow Print Server Web User Interface Default Value:	1 - 30
Default Value:	10

Maximum Age Weeks:

Description:	This parameter defines the maximum number of days a user account password can be used before it must be changed. This setting is ignored for a user account if the **Password Never Expires** option is enabled.
Windows 7 Allowable Range:	0 - 999
FreeFlow Print Server Web User Interface Allowable Range:	0 - 25
Windows 7 Default Value:	30
FreeFlow Print Server Web User Interface Default Value:	30

Minimum Age Weeks

Description:	This parameter defines the minimum number of days that a password must be used before it is changed. This setting must always be less than the **Maximum Age Weeks** setting.
Windows 7 Allowable Range:	0 - 999
FreeFlow Print Server Web User Interface Allowable Range:	0 - 30
Default Value:	2

Password Expiration Notification

Description:	This parameter defines the number of days before the locking or expiring of a user account password occurs that the user is warned and prompted to change his or her password. This parameter takes effect with the **Maximum Age Weeks** parameter and resets to zero when a user changes his or her password.
Windows 7 Allowable Range:	0 - 90
FreeFlow Print Server Web User Interface Allowable Range:	0 - 14
Default Value:	5

Minimum Password Length

Description:	This parameter defines the minimum number of characters for a password.
Windows 7 Allowable Range:	0 - 30
FreeFlow Print Server Web User Interface Allowable Range:	0 - 30
Windows 7 Default Value:	8
FreeFlow Print Server Web User Interface Default Value:	4

Account Lockout Threshold

Description:	This parameter defines the number of failed user account logon attempts before the account is locked out.
Windows 7 Allowable Range:	0 - 999
FreeFlow Print Server Web User Interface Allowable Range:	0 - 10
Windows 7 Default Value:	3
FreeFlow Print Server Web User Interface Default Value:	2

Account Lockout Duration

Description:	This parameter defines the number of minutes that a user account remains locked out before it is automatically unlocked.
Allowable Range:	0 - 99,999
Windows 7 Default Value:	1440
FreeFlow Print Server Web User Interface Default Value:	3

Account Lockout Counter Reset

Description:	This parameter defines the number of minutes that must elapse after a user password is timed-out due to exceeding the **Account Lockout Threshold** setting, before setting the counter back to zero which unlocks the account.
Allowable Range:	1 - 99,999
Windows 7 Default Value:	1440
FreeFlow Print Server Web User Interface Default Value:	5

Reset Password Allowed Times

Description:	This parameter defines the number of times a user can reset his or her password in a 24-hour period.
Windows 7 Allowable Range:	0 - 24
FreeFlow Print Server Web User Interface Allowable Range:	0 - 24
Windows 7 Default Value:	5
FreeFlow Print Server Web User Interface Default Value:	10

Access Control of FreeFlow® Print Sever GUI Management

The FreeFlow® Print Sever System Administrator has the authority to disable/enable FreeFlow® Print Sever Web UI Management features (i.e., Job Management, Queue Management, Printer Management, Diagnostics, etc.) that are represented by FreeFlow® Print Sever Web UI pull-down items. Access can be changed for the FreeFlow® Print Sever User Group and/or the Operator Group, but NOT for individual FreeFlow® Print Sever Users. Any FreeFlow® Print Sever User that is created will be granted access (i.e., disabled or enabled) per their associated FreeFlow® Print Sever Group (Administrator, Operator, or User) for these FreeFlow® Print Sever GUI features. By default all the Job management features are enabled for System Administrator and it is read only. System Administration features cannot be modified.

Network Security

Windows Firewall

The FreeFlow® Print Sever software relies on Windows built-in, network protocol filters, applications, and utilities to customize network security. The Windows firewall is a network-aware application that offers incoming and outgoing protocol filtering as a way to "customize" access to network domains, public networks, and private networks. The Windows firewall offers the ability to define firewall and connection rules defining a particular security policy that applies to these different network types. These security policies define rules that are used to analyze network traffic and to determine connection access/deny for network servers such as the FreeFlow® Print Sever/Windows platform. Other example filtering rules that can be defined in firewall policy are listed below:

- Source/destination IP addresses
- IP port number
- IPSec settings
- Users and groups in Active directory
- Network interface settings
- Services

Firewall settings that are defined by Windows Firewall Profiles protect the following:

- Internal networks
- Computers on the networks
- Server/client applications
- Data stored on servers/client

For example, a firewall policy may be defined to allow incoming traffic for a remote management application such as Remote Desktop over a connection to a private network, and might block the same application access from domain or public networks. Other network security policies can be defined with access/deny for access to file and printing services. A customer may want to allow network discovery from a FreeFlow® Print Sever/Windows configuration that defines a firewall that is on a private network. Do not define firewall policies for the **private** network between the FreeFlow® Print Sever software and the print engine software. The term **private** network, when talking about the Windows firewall, is a profile defining the **customer** network that is not outside of a domain or over the public Internet. All unsolicited incoming traffic from locations other than the private network are blocked. Custom rules can be defined per a firewall profile that authorizes incoming network traffic to pass through from a remote domain or public network. All outbound ports on the FreeFlow® Print Sever/Windows platform are open by default.

There are Network/Print protocol services that are enabled and accessible on the FreeFlow® Print Sever/Windows platform to ensure support of printing workflows (e.g., FFMR, lpr, IPP, etc.). The Windows firewall with Advanced Security provides the ability to define rules that can close ports associated with these Network/Print protocol services if they are not required by the customer print workflow(s). These network/print protocol services and their associated ports are as follows:

HTTP (Port 80)

This service is required to connect to the FreeFlow® Print Sever/Windows system from the Web user interface of the FreeFlow® Print Sever; therefore, this port must not be blocked unless the system is set up for **secure** connection of the Web user interface for the FreeFlow® Print Sever. See *"SSL (443)"*.

SSL (443)

The Secure Sockets Layer service provides encrypted and highly-secure login and file transfer services. This service is only used by the Web user interface for the FreeFlow® Print Sever to access the printer when a customer wants to **secure** web access.

IPP (Port 631)

This service is necessary for job submissions from the FreeFlow® Application Suite clients (e.g., FreeFlow® Makeready®, 3rd-party IPP clients, and custom IPP clients developed by customers.

SNMP (Port 161)

This service is used for exchanging SNMP messages. Use SNMP v3 for secure exchange of information.

SNMP (Port 162)

This services is used for SNMP Traps.

LP/LPR (Port 515)

The lp/lpr Gateway supports print job submissions from lp/lpr clients which are available on all operating systems. The lp/lpr print job submission method is the most widely-used print protocol.

TCP Raw Sockets (Port 9100 and 9400)

The Socket Gateway supports job submissions that are submitted over TCP/IP to a raw port service.

FTP (Port 21)

This is the standard File Transfer Protocol used to access the FreeFlow® Print Server system to transfer files and/or submit jobs from the FreeFlow® Makeready® client applications.

RDP (Port 3389)

The is the standard Windows Remote Desktop service used for remote management of the Windows system.

WSD Printing (Port 3702, 53302, 53303)

This is the Microsoft Web Services for Devices Printing protocol gateway. Native Windows Print Drivers can send jobs to WSD Print gateway using these ports.

Web Management (Port 8172)

This service is required for remote management of the FreeFlow® Print Server Web software through the Web user interface of the FreeFlow® Print Server.

SignalR (Port 8080, 8090)

File and PrinterSharing (SMB-In) (Port 445)

CWIS (Port 8082)

Secure CWIS (Port 8085)

AppleTalk (Ports 201, 202, 203, 204, 205, 206, 207, 208)

JMF Hot Folder (Port 8181)

Tomcat server (Port 8005)

JMF gateway (Port 7781)

In addition, the following programs are added in firewall program exception:

- Snmpd
- Snmptrap
- Combined-service
- ftp
- ICMPv4/ICMPv6

Secure Network Communication Security

Transport Layer Security (TLS) Protocol, Secure Sockets Layers (SSL)

The Transport Layer Security (TLS) protocol, Secure Sockets Layer (SSL) protocol services can be used to authenticate servers and clients, and then encrypt all messages between the authenticated end-points. This is most important when data must be transferred between applications across an untrusted network such as “public” networks. Some industries such as the US Government or Medical markets require data encryption over the network always, and even when communicating internally on a “private” network. Internet Explorer® version 10 which is included with FreeFlow® Print Server/Windows Digital Front End (DFE) supports multiple versions of TLS/SSL. The versions used by Internet Explorer can be changed by the user. TLS/SSL protocols are based on the use of public key cryptography which involves the exchange of a two keys (public and private key). The FreeFlow® Print Server/Windows DFE can be configured to require TLS/SSL communication by installing a Certificate that has been signed by a Certificate Authority.

IPSec Services

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

The IPSec service provides encryption and authentication for all TCP/IP and UDP/IP protocols that do not offer protection via SSL/TLS or SSH. The System Administrator can activate this feature to allow one or more remote Windows clients **secure** connectivity to the FreeFlow® Print Server/Windows system. Once the remote Windows client(s) and FreeFlow® Print Server software is set up and configured for IPSec, all login, filing or folder sharing, and printing sessions over TCP/IP or UDP/IP are secured by encryption. Access to the FreeFlow® Print Server system is granted when the remote Windows client and the FreeFlow® Print Server/Windows 7 system have mutually-authenticated.

The Advanced Security feature as part of the Windows Firewall services integrates Internet Protocol Security (IPSec) settings to provide synergy between IPSec-negotiated settings and protocol blocking decisions, and it also allows setting of Group policies. Combining protocol filtering and IPsec reduces the possibility of conflicts between firewall rules and IPSec connection security settings.

The priority of using IPSec has increased significantly due to the discovery of vulnerabilities in older versions of SSL/TLS protocol. Refer to the following Web site for the latest information:

https://www.openssl.org/news/vulnerabilities.html

The version of SSL included with the FreeFlow® Print Server does not have these vulnerabilities, but use of IPsec is recommended when sensitive data is transmitted to the FreeFlow® Print Server DFE.

On Demand Data Overwrite

- The Hard disk data over write is designed to remove all customer images permanently from FreeFlow® Print Server hard disks. It is an on demand data overwrite. It removes only the deleted files.
- The Data Overwrite feature conforms to the NIST SP-800-88 specification and performs a Clear operation on the Hard Disk Drives to sanitize customer image files. The Clear pattern is a single pass write of all zeros to each addressable section of the file. The user may select to run this pass multiple times, as desired.
- It also provides an option to wipe the following customer data:
  - Accounting logs
  - Customer Jobs in the Hot folders, Job input Queue, and Job Database
  - Debug logs/outloads Customer Installed Font files
  - Print Queues
  - RIP Output Queue
  - Windows Recycle bin
  - Windows System page file, System Hibernation file and Temp files
  - FTP folders

- Customer loaded Print resources (e.g., Signatures, background forms)

- It does not provide an option to perform verification of the customer image deletion.

STIG

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 before they are deployed in a DISA-supported computing environment. Government customers who must comply with Security Policies directed by the Department of Defense (DoD) may require STIG compliance before FreeFlow® Print Server is permitted to connect to the customer's network.

The FreeFlow® Print Server STIG tool incorporated in the FreeFlow® Print Server v20.0 and above software releases can be used 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. Currently FreeFlow® Print Server 20.0 supports only cat 1 and 2.

In addition, organizations that work with confidential/sensitive data may need to comply with NIST SP800-53 and IRS Printer SCSEM security standards.

The FreeFlow® Print Server STIG tool can be used by customers to implement security controls required to achieve compliance with these standards.

Hard Drive Encryption

FreeFlow® Print Server allows the customer to encrypt its hard drive using Windows Bit Locker. This enables the customer to store the Job data in encrypted format on the hard drive.

802.1x

FreeFlow® Print Server Supports 802.1x, which is an IEEE standard protocol for port-based network access control. This protocol provides authentication to devices attached to a LAN port and establishes a point-to-point connection only if authentication is successful.

FIPS 140-2 Compliance

FreeFlow® Print Server runs as an application on top of the Microsoft Windows 7 OS. The Microsoft windows cryptographic modules comply with U.S federal government standard , Federal Information Processing Standard(FIPS) 140-2. FreeFlow® Print Server uses FIPS 140-2 compliance crypto library to store the user password.


xerox