

# Xerox FreeFlow<sup>®</sup> Print Server version 7 Security White Paper

## Secure Solutions For You and Your Customers

### Contents

September 2008

Author: Xerox Corporation

- 1 Executive summary
- 2 Why security matters
- 3 Xerox's commitment to security
- 4 FreeFlow Print Server security features

# Xerox FreeFlow Print Server Security White Paper

## Secure solutions for you and your customers

### Executive summary

Now more than ever, companies as well as government agencies need to keep their data safe. Drawing on our leadership in the printing industry, Xerox leads the way in providing secure document solutions. The Xerox FreeFlow Print Server provides features that offer the highest levels of security, adhere to government regulations, and enhance peace of mind. This document highlights these security capabilities and features:

**Adjust to your security needs** with the Security Management Feature

**Reuse network accounts** using Microsoft® Active Directory Services

**Manage your users and groups** with the Authentication Feature

**Know your Web users** through the Basic Access Authentication Feature

**Accept jobs from the clients you want** with the IP Filtering Feature and Port Designation

**Protect resources** so that they're tamper-free with the System Integrity Feature

**Secure http delivery** through the Transport Layer Security Feature

**Establish certain users and certain privileges** with the Access Control Feature

**Remove files permanently and completely with** Residual Information Protection

# Why security matters

Innovations in information technology have increased rapidly over the last several years, fueling the pace and productivity of business across all sectors and industries. Great strides have been made in the way information is created, stored, managed, distributed, and archived. However, this innovation has also created opportunities for those seeking to intercept or corrupt valuable information and disrupt the flow of business—privacy, property, and assets of all kinds are at stake. That makes security an issue that no one can ignore.

## Government regulations

In industries such as healthcare and financial services, new government mandates dictate that information in every form be more secure.

The Health Insurance Portability and Accountability Act (HIPAA) in healthcare, Gramm-Leach-Bliley (GLBA) in the financial sector, and the Federal Information Security Management Act of 2002 (FISMA) are just a few examples of many new security regulations being issued to oversee the way that information is printed, shared, stored, and protected.

With so many regulatory and compliance measures to respond to, Xerox has looked to federal government requirements worldwide, among others, as guidelines. By developing solutions that comply with the most stringent security standards, we can offer highly secure solutions to all of our customers in all business sectors.

## Peace of mind

In every environment, security is of critical importance.

Transactional print jobs often consist of sensitive customer data that absolutely must be protected from unauthorized viewing. And publishing jobs include product manuals, annual reports, and brochures that contain information that is often confidential until a launch date or an event.

No matter what you print, you will have greater peace of mind knowing that the printing solution assures that the data and your network will be secure.



# Xerox's commitment to security

At Xerox, security issues are front and center. As a leader in the development of digital technology, we have demonstrated a commitment to keeping digital information safe and secure by identifying potential vulnerabilities and proactively addressing them to limit risk. Our customers have responded by looking to us as a trusted provider of secure solutions with many standard and optional security features.

## Xerox security goals

We have identified five key security goals in the quest to provide secure solutions for every one of our customers:

### **Integrity**

- No unauthorized alteration of data
- System performs as intended, free from unauthorized manipulation

### **Confidentiality**

- No unauthorized disclosure of data during processing, transmission, or storage

### **Availability**

- Systems work properly
- No denial of service for authorized users
- Protection against unauthorized use of the system

### **Accountability**

- Actions of an entity can be traced directly to that entity

### **Assurance**

- Confidence that integrity, confidentiality, availability, and accountability goals have been met

# FreeFlow Print Server security features

In response to a variety of security threats, we have taken an industry-leading role by developing and implementing information security technology for nearly a decade. This commitment to security carries over to our digital on-demand production printing solutions that are powered by the FreeFlow Print Server.

## Adjust to your security needs

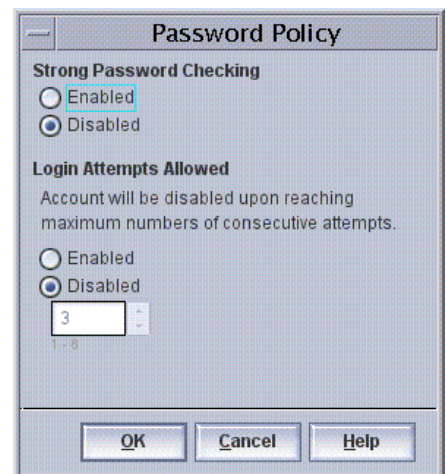
### Security Management Feature

Your security needs are yours alone. The FreeFlow Print Server allows you to adjust a range of security features to tailor security exactly to the needs of your enterprise.

The Security Management feature enables authorized users to set up and control the secure operation of the printing system so that they all operate coherently and adjust to your various security needs and policies.

The security administrative functions cover the following areas:

- Configuration of automatic login for customers not interested in security—that is, a “no-security” look and feel.
- Job Management policy configuration issues, such as which users are allowed to manage jobs.
- Diagnostics policy configuration issues, such as which users are allowed to run diagnostic routines.
- Enablement of TLS/SSL security protocol and Digital Certificates management.
- Configuring the system to trust remote security databases such as W2K domains.
- Configuring the system for various security levels.
- Displaying a custom logon message.
- Preventing walk-up users from arbitrarily reprinting jobs stored on the system.
- The means for enforcing a strong password policy.
- Forcing users to re-authenticate whenever UNIX terminal access is requested.
- User accounts can be locked after a user-defined number of failed login attempts (ranging from 1 to 9).



## Reuse network accounts

### Microsoft Active Directory Services (ADS)

Our printing solutions recognize and integrate with your existing user security accounts that are defined in a remote, trusted security database and maintained by a Microsoft Windows® 2000 Domain Controller.

You can reuse these network accounts for login at the printer, instead of exclusively using the locally defined user accounts. This saves time and effort for system administrators.

With the Microsoft Active Directory Services feature, your printer can interoperate with Microsoft Active Directory Services:

- The printer can be configured to trust a Windows 2000 ADS security authority.
- Users are able to walk to the printer and authenticate using their ADS username and password. The printer will contact the trusted ADS security authority, which, in turn, will verify the user's credentials.
- ADS users and groups can be mapped to the local printer groups and, thereby, be granted a certain authorization level.

## Manage your users and groups

### Authentication Feature

Perhaps the surest way to maintain security with any printing device is allowing only authorized users to access the system. The FreeFlow Print Server does so with its Authentication feature.

Any type of interaction between a user and a printing system through the FreeFlow Print Server is associated with a security account. This association, or logon session, is the basis for granting access to any of your users. Once the logon session is established, the user can interact with the printer, subject to restrictions based on the user's identity.

User accounts are defined either locally at the device or remotely at a trusted network location. Each user account is a member of one and only one user group. Group membership defines/authorizes the access rights of requests made by users.

A strong password feature further enhances print server security, requiring users to enter a password that contains at least one special character, one uppercase letter, and one digit. Additional parameters that keep these passwords safe include:

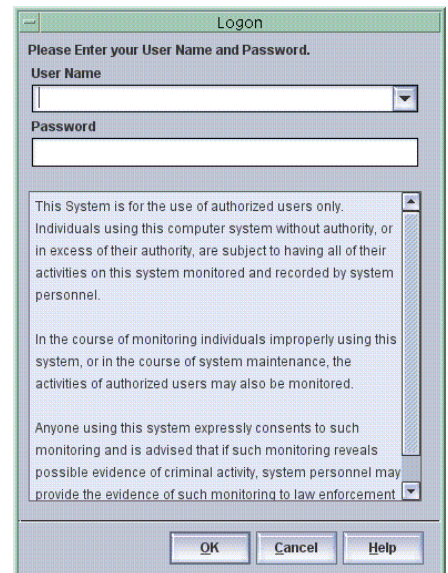
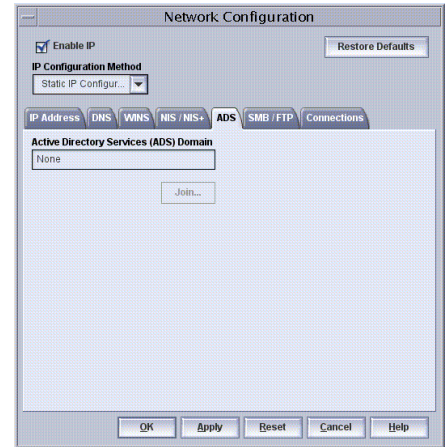
- Password Duration—checks on how much time has passed since passwords have changed or been updated.
- Password History—prevents users from reusing old passwords.

## Know your Web users

### Basic Access Authentication (BAA) Feature

Basic Authentication is an industry-standard method of authenticating a remote user of Internet Services (HTTP) or the Internet Printing Protocol (IPP).

It optionally forces users to authenticate themselves before they can access the device over HTTP. When used in conjunction with TLS/SSL, it allows for both authentication (BAA) and integrity/privacy (TLS/SSL) protection.



## Accept jobs from only the clients you want

### IP Filtering Feature

With the FreeFlow Print Server's Internet Protocol (IP) Filtering feature, you can enjoy the productivity benefits of remote job submission, while minimizing security risks.

IP Filtering provides a system administrator with a means of restricting access to the system to a specific set of IP addresses. This provides a first level of defense against unauthorized use of the system. Computers whose IP addresses are outside of the allowed set are not permitted to print.

With IP Filtering, the administrator can also configure the printer to accept print jobs only from specific print servers. This prevents end users from directly accessing the printer and enables value-added solutions implemented at the print server.

### Port Designation

Xerox can provide to you, as required, a complete list of the ports utilized by the FreeFlow Print Server network functionality.

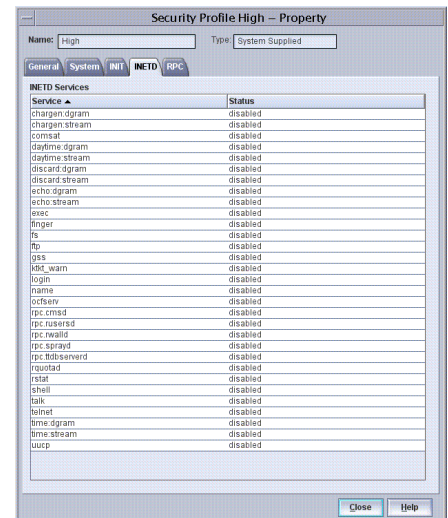
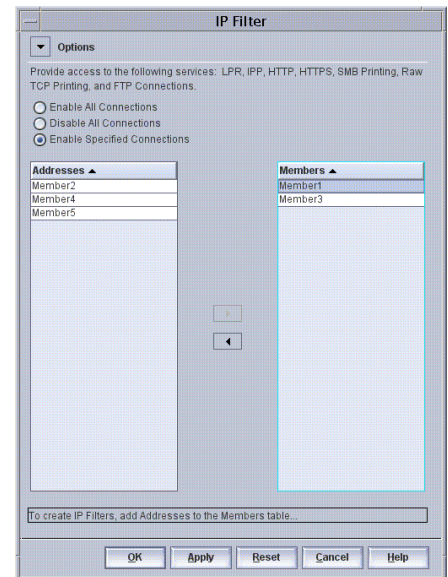
## Tamper-free resources

### System Integrity Feature

Even with the most stringent security restrictions in place, there are sometimes "backdoors" and vulnerabilities that can be exploited.

The System Integrity feature on the FreeFlow Print Server:

- Ensures that system resources cannot be tampered with.
- Limits access to UNIX commands through the Access Control feature in user group classification.
- Disables unneeded network applications and OS utilities.
- Provides OS security patches—working very closely with Sun, Xerox is able to provide patches in a timely fashion as they are released from Sun.
- "Hardens" the system according to security best practices—tightens the sensitive file access permissions, shuts down unneeded and/or insecure network protocol services, and restricts potentially insecure network access to trusted network hosts based on the originating IP address.



## Encrypted job submission via the Web

### TLS/SSL Security Feature

One of the great leaps forward in printing productivity is the ability to print from anywhere over the Internet. Unfortunately, it can be a great leap backwards in security.

The FreeFlow Print Server's Transport Layer Security feature allows a high level of protection of the data exchanged—such as higher-level security information like user passwords or confidential print jobs—over a network. Transport Layer Security v1.0 (RFC2246) is a network security protocol widely used for applications that require secure HTTP communications.

TLS/SSL provides security protection through:

- **Message Confidentiality**—Data is encrypted through symmetric cryptography, which uses an algorithm to generate unique exchange keys for each connection.
- **Message Integrity**—A message authentication code is used to detect message tampering and forgery. The sender digitally signs the message using a session key shared with the recipient.
- **Authentication**—The identity of a peer can be authenticated using asymmetric (public key) cryptography. Servers are identified through a digital certificate issued by a certificate authority or self-signed.

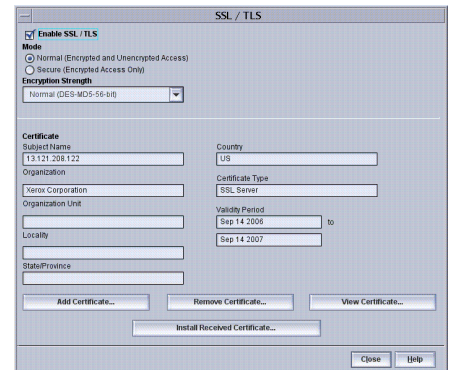
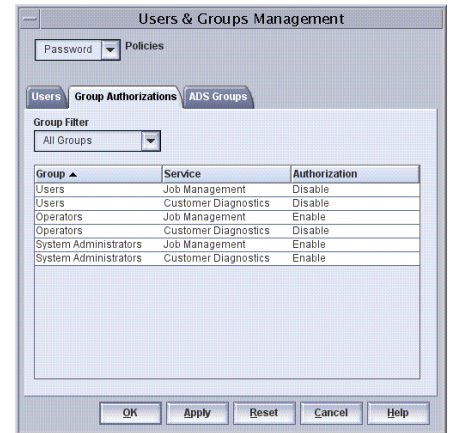
## Certain users, certain privileges

### Access Control Feature

With the Access Control feature, authenticated users are assigned privileges—either as Administrators, Operators, or Users with decreasing levels of access. The higher the access level, the more features and data available. The range of available features for each access level is not configurable, with the following exceptions:

- **Job Management**—An Administrator decides the access level necessary to manage jobs. By default, any User can manage jobs, but an Administrator might decide that only Operators and/or Administrators can manage jobs. This prevents “walk-up users” from deleting print jobs submitted by other Users.
- **Diagnostics**—Diagnostic tools are restricted to Administrators by default. However, there are cases when trained Users may be entrusted with certain Diagnostic operations without necessarily granting them Administrator privileges. For these cases, it is possible to allow Operators or even regular Users access to the Diagnostic tools.

The Authorization feature, as described earlier, controls access to the Diagnostic tools as a whole. However, the Diagnostic tools are further grouped in various levels that allow for more or less functionality. The access to these levels is controlled based on a secondary authentication step, thereby providing a finer level of authorization. Once a User is authenticated in the first step and allowed access to Diagnostics as a whole, the User gains access to a certain group of tools based on a secondary password they must provide.



## Permanent and complete file removal

### Residual Information Protection

With the pace of business today, jobs come and jobs go quickly in your print enterprise. But proper security should prompt you to ask the question, “Do jobs ever really go?”

With the Residual Information Protection feature, the answer is yes, jobs really do go away, permanently and completely.

This feature ensures that deleted information is no longer accessible. This type of deleted information is outside of the scope of the standard security functions but it is potentially retrievable.

- **Hard drive removal**—If the hard drive isn't present, it is impossible to retrieve information from it. Many Xerox printing systems feature a hard drive that can be removed when the system is not in use. Please speak with your salesperson to see what products can be supported with a removable hard drive through Xerox Special Information Systems (XSIS).
- **Hard drive erasure**—Algorithms completely and permanently delete all files after printing.
- **Disk Overwrite Software**—Removes all data from the spool, swap, and outQ partitions of the FreeFlow Print Server hard disk so that data cannot be retrieved. Data is overwritten using a four-pass algorithm that conforms to U.S. Department of Defense Directive 5200.28-M.

**For more information and additional security resources, go to:**

<http://www.xerox.com/security>



© 2008 Xerox Corporation. All rights reserved. Xerox®, the sphere of connectivity design, and FreeFlow® are trademarks of Xerox Corporation in the United States and/or other countries.

Microsoft® and Windows® are trademarks of Microsoft Corporation in the U.S. and/or other countries. Product appearance, build status, and/or specifications are subject to change without notice. 09/08