

XEROX®

Technology | Document Management | Consulting Services

Secure solutions for you and your customers



FreeFlow™ DocuSP® 4.x

Xerox Nuvera™ Digital Copier/Printer
Xerox Nuvera™ Digital Production System
DocuTech® Production Publishers
DocuPrint® Enterprise Printing Systems



Executive Summary

Why is security more important than ever?

New government regulations have been implemented as a response to new corporate realities. And increasing competition makes complete satisfaction a critical factor in retaining customers.

Xerox has been a leader in providing secure document solutions to the printing industry for years. The FreeFlow™ DocuSP® Controller, version 4.x, and production printing solutions including the Xerox Nuvera™ Digital Copier/Printer, Xerox Nuvera™ Digital Production System, DocuTech® Production Publishers, and DocuPrint® Enterprise Printing Systems provide security features that offer the highest levels of security, adhere to government regulations, and offer customers peace of mind.

This document highlights these security capabilities and features:

Adjust to your security needs	 Security Management Feature
Reuse network accounts	 Microsoft Active Directory Services
Manage your users and groups	 Authentication Feature
Know your Web users	 Basic Access Authentication Feature
Accept jobs from the clients you want	 IP Filtering Feature
Tamper-free resources	 System Integrity Feature
Secure http delivery	 Transport Layer Security Feature
Certain users, certain privileges	 Access Control Feature
Really get rid of old information	 Residual Information Protection

1

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, 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 health care, 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, among others, as guidelines. By developing solutions that comply with the most stringent security standards, Xerox is in a position to offer highly secure solutions to all of its 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 a event.

No matter what you print for your customers, they will have greater peace of mind knowing that the printing solution assures that the data that leaves their walls for your enterprise will be as secure as if it never left.

Customers with peace of mind are more likely to be returning customers.

2 Xerox commitment to security

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

Xerox Security Goals

Xerox has 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



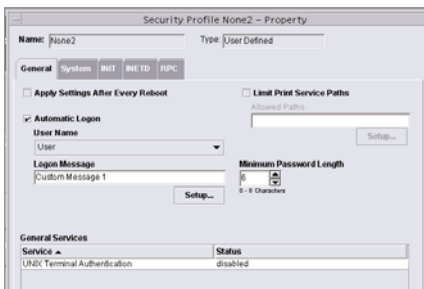
Assurance

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

3

FreeFlow™ DocuSP® Security Features

In response to a variety of security threats, Xerox has taken an industry-leading role by developing and implementing information security technology for nearly a decade. This commitment to security carries over to the Xerox's digital on demand production printing solutions that are powered by FreeFlow™ DocuSP® 4.x, including the Xerox Nuvera™ Digital Copier/Printer, the Xerox Nuvera™ Digital Production System, the DocuTech® Production Publishers, and the DocuPrint® Enterprise Printing Systems.



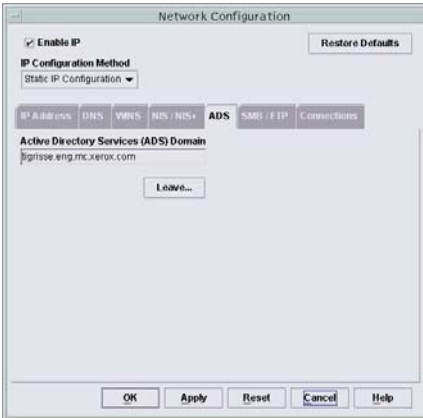
Adjust to your security needs Security Management Feature

Your security needs are yours alone. Xerox DocuSP® 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 diagnostics 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.
- Forcing users to choose passwords of a minimum length.
- Forcing users to re-authenticate whenever UNIX terminal access is requested.



Reuse network accounts

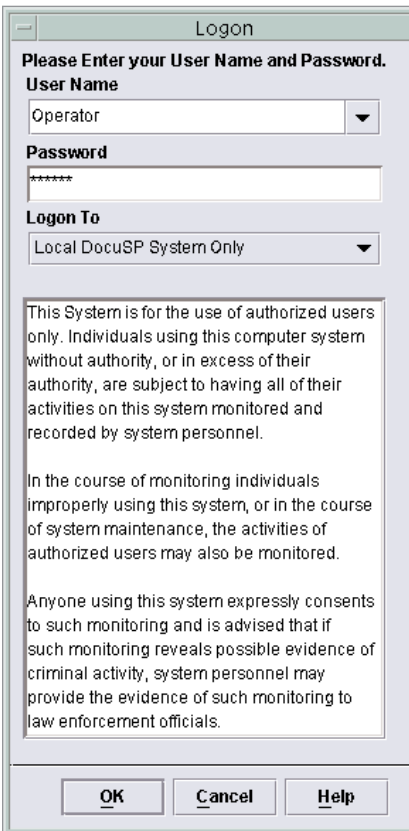
Microsoft® Active Directory Services

Customers have asked us to allow our printing solutions to recognize and integrate with their existing user security accounts that are defined in a remote, trusted security database, maintained in this case by a Microsoft Windows® 2000 Domain Controller.

Customers would like to be able to 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.

The Microsoft Active Directory Services feature answers this customer request by allowing the printer to interoperate with Microsoft Active Directory Services (ADS).

- 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. FreeFlow™ DocuSP® does so with its Authentication feature.

Any type of interaction between a user and a printing system through FreeFlow™ DocuSP® 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.

For customers that do not always require authentication, FreeFlow™ DocuSP® can automatically log in using a default user account. The default account can be assigned to any of the existing groups, allowing the customer to select the features available for anonymous usage.

Know your Web users

Basic Access Authentication 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.

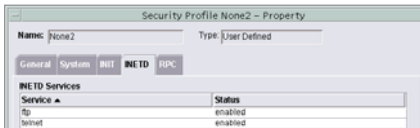
Accept jobs from only the clients you want

IP Filtering Feature

With FreeFlow™ DocuSP®'s IP Filtering feature, you can enjoy the productivity benefits of remote job submission, while minimizing security risks.

Internet Protocol (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.



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.

FreeFlow™ DocuSP's System Integrity feature:

- Ensures that system resources cannot be tampered with.
- Limits “backdoor” access using Solaris OS commands.
- Disables unneeded network applications and OS utilities.
- Provides OS security patches.
- “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.

Secure http delivery

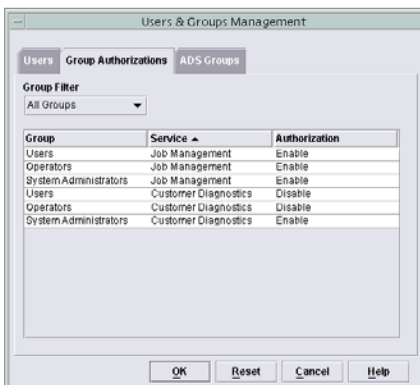
Transport Layer Security Feature

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.

FreeFlow™ DocuSP®'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**—Diagnostics tools are restricted to Administrators by default. However, there are cases when trained users may be entrusted with certain diagnostics operations without necessarily granting them Administrator privileges. For these cases, it is possible to allow Operators or even regular Users access to the Diagnostics tools.

The Authorization feature, as described earlier, controls access to the Diagnostics tools as a whole. However, the Diagnostics 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.

Really get rid of old information

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 yet 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.
- **Hard drive erasure**—Algorithms completely and permanently delete all files after printing.

For more information and additional security resources, go to:
<http://www.xerox.com/security>

