

# Security Document

for FreeFlow® Makeready, FreeFlow® Web Services, FreeFlow® Process Manager, Standalone Quick Print, FreeFlow® Scanner 665E, FreeFlow® Print Manager, and FreeFlow® Output Manager (Version 2.0) configurations

Xerox Corporation  
Global Knowledge and Language Services  
800 Phillips Road - Bldg. 845-17S  
Webster, NY 14580

Copyright © 1996-2006 Xerox Corporation. All rights reserved. XEROX®, Xerox Canada Ltd®, Xerox Limited®, FreeFlow®, The Document Company® and all identifying numbers used in connection with the Xerox products mentioned in this publication are trademarks of XEROX CORPORATION. Copyright protection claimed includes all forms and matters of copyrightable material and information now allowed by statutory or judicial law or hereinafter granted, including without limitations, material generated from the software programs which are displayed on the screen such as styles, templates, icons, screen displays looks, etc.

While every care has been taken in the preparation of this material, no liability will be accepted by Xerox Corporation arising out of any inaccuracies or omissions.

Printed in the United States of America.

Other company trademarks are acknowledged as follows:

Adaptec®, the Adaptec logo, SCSISelect®, and EZ-SCSI® are trademarks of Adaptec, Inc

Adobe PDFL - Adobe PDF Library Copyright © 1987-2005 Adobe Systems Incorporated

Adobe®, the Adobe logo, Acrobat®, the Acrobat logo, Acrobat Reader®, Distiller®, Adobe PDF JobReady™, PostScript®, and the PostScript logo are either registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Copyright 1987 - 2005 Adobe Systems Incorporated and its licensors. All rights reserved.

Autologic® is a registered trademark of Autologic Information International, Inc.

Compaq® and QVision® are registered United States Patent and Trademark Office, for Compaq Computer Corporation.

DEC, DEC RAID, and Redundant Array of Independent Disks are registered trademarks of Digital Equipment Corporation.

Dundas - This software contains material that is © 1997-2000 DUNDAS SOFTWARE LTD., all rights reserved.

Hummingbird NFS Solo® is a registered trademark of Hummingbird Communications, Ltd.

Imaging Technology provided under license by Accusoft Corporation.

ImageGear © 1996-2005 by AccuSoft Corporation. All Rights Reserved.

Intel® and Pentium® are registered trademarks of Intel Corporation.

Novell® and NetWare® are registered trademarks of Novell, Inc. in the United States and other countries.

Oracle® is a registered trademark of Oracle Corporation Redwood City, California

TMSSequoia - ScanFix® Image Optimizer Copyright © TMSSEQUOIA, Inc. 1991-2000. All rights reserved.

Sony™ and Storage by Sony™ are trademarks of Sony.

Preps™ is a registered trademark of Creo Inc. All rights reserved.

Quark® and QuarkXpress® are registered trademarks of Quark, Inc.

StorageView™ is a trademark of CMD Technology, Inc.

TextBridge® is a Registered Trademark of ScanSoft, Inc.

TIFF® is a registered trademark of Aldus Corporation.

Windows®, Windows XP®, and Internet Explorer are trademarks of Microsoft Corporation; Microsoft® and MS-DOS® are registered trademarks of Microsoft Corporation.

Portions Copyright © 2001 artofcode LLC.

This software is based in part on the work of the Independent JPEG Group.

Portions Copyright © 2001 URW++. All Rights Reserved.

This product includes software developed by the Apache Software Foundation.

Copyright © 1999-2003 The Apache Software Foundation. All rights reserved.

This software is based in part on the work of Graeme W. Gill.

© Press-sense Ltd. 2002-2005. All rights reserved

Includes Adobe® PDF Libraries and Adobe Normalizer technology

The Graphics Interchange Format® is the Copyright property of CompuServe Incorporated. GIF<sup>SM</sup> is a Service Mark of CompuServe Incorporated.

Portions contain an implementation of the LZW algorithm licensed under U.S. Patent 4,558,302

All non-Xerox brands and product names are trademarks or registered trademarks of their respective companies.

Changes are periodically made to this document. Changes, technical inaccuracies, and typographical errors will be corrected in subsequent editions.

---

# Table of contents

<b>Security recommendations</b> .....	<b>1-1</b>
Overview .....	1-1
Security best practices .....	1-2
1 - Network Security .....	1-3
Hardware Firewall .....	1-3
Windows Firewall .....	1-8
RDO printing to DocuSP .....	1-16
2 - Physical Location/Access .....	1-17
3 - Operating System/System Security .....	1-17
FreeFlow's patch management strategy .....	1-17
Internet Explorer settings .....	1-18
4 - Virus Protection .....	1-19
Protecting the system from virus protection .....	1-19
5 - User Authentication and Password Management .....	1-20



---

# Security recommendations

---

## Overview

---

This document describes the recommended security settings for FreeFlow Makeready, FreeFlow Web Services, FreeFlow Process Manager, FreeFlow Scanner 665E, Standalone Quick Print, FreeFlow Print Manager, and FreeFlow Output Manager (Version 2.0).

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. The components of FreeFlow are assessed for security compliance using commercially available scanning tools and manual checklists.

Application vulnerabilities are addressed based on results on the manual checklists. All unnecessary and insecure services and protocols have been disabled based on results of our internal scans, and all identified Microsoft operating system patch updates have been applied. After a product is launched, Xerox distributes monthly bulletins listing critical updates that minimally should be installed on a FreeFlow system using Microsoft Windows Update.

---

## Security best practices

---

Even the most secure systems are vulnerable to someone who has enough time, the right knowledge, and access. Threats include physical damage at the system, over networks, or damage caused by viruses. The goals are to minimize security risks, and have policies in place to detect the negative impact of a security breach.

The following 5-tier strategy is recommended for achieving a secure environment:

- Network Security
- Physical location/access security
- OS/System Security
- Virus Protection
- User Authentication and Password Management

## 1 - Network Security

---

The first step in implementing a security model is addressing the network. This is the entry point into any server environment and is where sensitive data is transmitted from system to system. There must be gatekeeper mechanisms in place that prevent entry and attack.

### Hardware Firewall

---

To secure the network, a combination of hardware and software controls is recommended, including a router, switch, and firewall. Configured correctly, these tools filter and block unsolicited traffic; and without proper configuration, they block desired inbound traffic, as well.

The following tables document the port requirements when using the various FreeFlow workflows/configurations. These ports have to be opened in the hardware firewall to allow traffic to pass from the server to the internet. By default, FreeFlow disables all unused services and protocols.

Table 1 provides the required port settings for DocuSP DFE systems.

**Table 1. Port settings for DocuSP DFE systems**

PORT	Protocol or Application	Required for DocuSP when Production Printing from FreeFlow		Required for DocuSP for Network Agent Decomp Services	
		High Security ON	High Security OFF	High Security ON	High Security OFF
21	FTP	No	Yes	No	Yes
631	IPP	No	Yes	No	Yes
22	SSH/s FTP	Yes	No	Yes	No
443	SSL/TLS	Yes	No	Yes	No
515 (or range 513 - 1023)	LPR	No	Yes	No	
111	RPC	No	No	Yes for DocuSP < 3.6	

Table 2 provides required port settings for DFE devices, not including DocuSP.

**Table 2. Port settings for DFE devices, not including DocuSP**

<b>PORT</b>	<b>Protocol or Application</b>	<b>Required for the following DFEs:</b> <ul style="list-style-type: none"> <li>• <b>EFI</b></li> <li>• <b>Creo</b></li> <li>• <b>DocuCentre</b></li> <li>• <b>WorkCentre</b></li> <li>• <b>AccXES</b></li> <li>• <b>Scanvec Amiable</b></li> </ul>	<b>Required for the following legacy DFEs</b> <ul style="list-style-type: none"> <li>• <b>GXP 4110</b></li> <li>• <b>NPS Server</b></li> <li>• <b>DT Network Server</b></li> <li>• <b>NS Plus</b></li> <li>• <b>NS + Server Series</b></li> </ul>
21	FTP	No	Yes
631	IPP	Yes only for DocuColor 6060 EFI 2.0 or greater	No
22	SSH/s FTP	No	No
443	SSL/TLS	No	No
515 (or range 513 - 1023)	LPR	Yes	Yes
111	RPC	No	No

Table 3 provides the required port settings for FreeFlow.

**Table 3. Required port settings**

PORT	Protocol or Application	Required for FreeFlow Makeready	Required for FreeFlow Makeready with Document Library	Required for FreeFlow Web Services	Required for FreeFlow Process Manager servers	Required for FreeFlow Process Manager clients	Required for FreeFlow Print Manager	Required for FreeFlow Output Manager
21	FTP	No	No	No	Yes	No	No	No
631	IPP	No	No	No	No	No	Yes on DocuSP if High Security Disabled	Yes on FreeFlow Output Manager, WorkCentre, and NPS Server
443	SSL/TLS	No	No	No	No	No	Yes on DocuSP if High Security Enabled	Yes on DocuSP if High Security Enabled
515 (or range 513 - 1023)	LPR	No	No	No	No	No	Yes on non-DocuSP printers	Yes on non-DocuSP printers
135	RPC End Point Mapper	Yes	Yes	Yes	Yes	No	No	No
1521	Oracle Listener	No	Yes	Yes	Yes	No	No	No
51001 - 51030	DCOM	Yes	Yes	Yes	Yes	No	No	No
80	HTTP or reassigned port #	No	No	Yes	No	No	Yes	Yes on Creo
443	HTTPs or reassigned port #	No	No	Yes	No	No	No	No
8080	HTTP	No	No	No	No	No	No	Yes
8443	HTTPs	No	No	No	No	No	No	Yes
161	SNMP	No	No	No	No	No	No	Yes for SNMP devices (WorkCentre, Document Centre, 4110)
5000 - 6000	Remote Job Manager and Submission Clients	No	No	No	Yes	Yes	No	No
6620	Workflow Builder	No	No	No	Yes	No	No	No
6789	Workflow Database Server	No	No	No	Yes	No	No	No
7890	Workflow TaskMgr	No	No	No	Yes	No	No	No
8053	JDF Server	No	No	No	Yes	No	No	No
6050	Workflow Hot Folder Utility	No	No	No	Yes	Yes	No	No

**Table 3. Required port settings**

<b>PORT</b>	<b>Protocol or Application</b>	<b>Required for FreeFlow Makeready</b>	<b>Required for FreeFlow Makeready with Document Library</b>	<b>Required for FreeFlow Web Services</b>	<b>Required for FreeFlow Process Manager servers</b>	<b>Required for FreeFlow Process Manager clients</b>	<b>Required for FreeFlow Print Manager</b>	<b>Required for FreeFlow Output Manager</b>
7778	JMF Listening Port	No	No	No	Yes	No	No	No
8090	Repository Connector	Yes, w/ Repository connector	Yes, w/ Repository connector	Yes, w/ Repository connector	Yes, w/ Repository connector	No	No	No
8091	Repository Connector w/ SSL	Yes, w/ Repository connector	Yes, w/ Repository connector	Yes, w/ Repository connector	Yes, w/ Repository connector	No	No	No

## Windows Firewall

On the FreeFlow system, the Windows Firewall is DISABLED by default in the base Windows Server 2003 SP1 and manually disabled in the base Windows Professional XP SP2 operating systems.

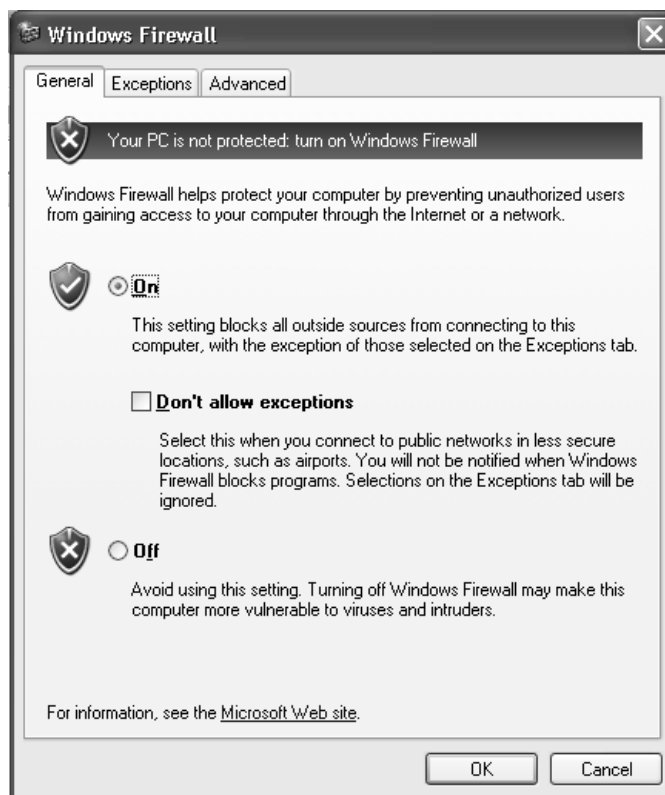


To configure the Windows Firewall on a FreeFlow system:

1. Select [**Start: Settings: Control Panel**] from the Windows desktop.
2. Select [**Windows Firewall**].
3. If prompted to start the Windows Firewall/ICS service, select [**Yes**].



*NOTE: You are prompted to start the Windows Firewall/ICS service only on Windows Server 2003 SP1 systems.*



**Figure 1. Windows Firewall dialog**

4. To enable the Windows Firewall, mark the [**On**] radio button.
5. To disable the Windows Firewall, mark the [**Off**] radio option.

6. Select the **Exceptions** tab.
7. Add the following Windows Firewall ports and programs per the appropriate configurations:



*NOTE: Refer to Table 4 for a summary of all Windows Firewall settings.*

- a. **For a FreeFlow Makeready without Document Library configuration:**
  - i. Select [**Add Port**].
  - ii. Enter the name (user defined) and port number for the following TCP ports:
    - 135 — end point mapping
  - iii. Select [**Add Programs**].
  - iv. Add the following programs:
    - FreeFlow Makeready
    - ScanAndPrint.exe (Browse to E:\FreeFlow for ScanAndPrint)
    - Document Library (DocLib.exe)
    - Quick Print (Domgr.exe)
    - File Manager (DPFileManager.exe)
    - FreeFlow Administration Tool (E:\FreeFlow\FFAdminTool.exe)

**b. For a FreeFlow Makeready with Document Library configuration:**

- i. Select [**Add Port**].
- ii. Enter the name (user defined) and port number for the following TCP ports:
  - 135 — end point mapping
- iii. Select [**Add Programs**].
- iv. Add the following programs:
  - dllhost.exe (Browse to C:\Windows\System32)
  - msdtc.exe (Browse to C:\Windows\System32)
  - FreeFlow Makeready
  - ScanAndPrint.exe (Browse to E:\FreeFlow for ScanAndPrint)
  - Document Library (DocLib.exe)
  - Quick Print (Domgr.exe)
  - File Manager (DPFileManager.exe)
  - FreeFlow Administration Tool (E:\FreeFlow\FFAdminTool.exe)



c. **For Remote FreeFlow Process Manager Clients:**

*NOTE: There are no TCP ports to add for this configuration.*

- i. Select [**Add Programs**].
- ii. Add the following programs:
  - Remote Workflow Submission Client (WFSubmissionClient.exe)
  - Remote Workflow Job manager Client (PDFJobManager.exe)

d. **For a FreeFlow Process Manager configuration:**

- i. Select [**Add Port**].
- ii. Enter the name (user defined) and port number for the following TCP ports:
  - 21 — ftp
  - 135 — end point mapping
  - 6620 — Workflow Builder
  - 6789 — Workflow Database Server
  - 7890 — Workflow Task Manager
  - 8053 — JDF Server
- iii. Select [**Add Programs**].

## iv. Add the following programs:

- dllhost.exe (Browse to C:\Windows\System32)
- msdtc.exe (Browse to C:\Windows\System32)
- Document Library (DocLib.exe)
- Quick Print (Domgr.exe)
- File Manager (DPFileManager.exe)
- Workflow Submission Client  
(E:\FreeFlow\WFSubmissionClient.exe)
- Workflow Job Manager Client  
(E:\FreeFlow\PDFJobManager.exe)
- Workflow Printer Administration  
(E:\FreeFlow\PrinterAdminApp.exe)
- FreeFlow Administration Tool  
(E:\FreeFlow\FFAdminTool.exe)
- Workflow Builder (E:\FreeFlow\WFBuilder.exe)
- C:\Windows\ADAM\dsamain.exe

**e. For a FreeFlow Web Services configuration:**

- i. Select [**Add Port**].
- ii. Enter the name (user defined) and port number for the following TCP ports:
  - 135 — end point mapping
  - 80 (or reassigned HTTP port)
  - 443 (or reassigned HTTPS port)
- iii. Select [**Add Programs**].
- iv. Add the following programs:
  - dllhost.exe (Browse to C:\Windows\System32)
  - msdtc.exe (Browse to C:\Windows\System32)
  - w3wp.exe (Browse to C:\Windows\System32\inetsrv)
  - Document Library (DocLib.exe)
  - Quick Print (Domgr.exe)
  - File Manager (DPFileManager.exe)
  - FreeFlow Administration Tool (E:\FreeFlow\FFAdminTool.exe)

If using the Windows Firewall, Table 4 provides the required Windows Firewall settings per configuration.

**Table 4. Required Windows Firewall settings**

PORT / Exception	FreeFlow Makeready Client	FreeFlow Makeready with Document Library	FreeFlow Web Services	FreeFlow Process Manager Server	FreeFlow Process Manager Client	FreeFlow Scanner 665E	Standalone Quick Print
135	Yes	Yes	Yes	Yes	No	No	No
80 or reassigned HTTP port	No	No	Yes	No	No	No	No
443 or reassigned HTTPs port	No	No	Yes	No	No	No	No
6620	No	No	No	Yes	No	No	No
6789	No	No	No	Yes	No	No	No
7890	No	No	No	Yes	No	No	No
8053	No	No	No	Yes	No	No	No
21	No	No	No	Yes	No	No	No
C:\Windows\System32\Dllhost.exe	No	Yes	Yes	Yes	No	No	No
C:\Windows\System32\msdtc.exe	No	Yes	Yes	Yes	No	No	No
C:\Windows\System32\inetrv\w3wp.exe	No	No	Yes - for FreeFlow Process Manager integration	No	No	No	No
Document Library	Yes	Yes	No	Yes	No	No	No
FreeFlow Makeready	Yes	Yes	No	No	No	No	No
E:\FreeFlow\ScanAndPrint.exe	Yes	Yes	No	No	No	No	No
Quick Print w/ FreeFlow Scanner 665E	Yes	Yes	Yes	Yes	No	Yes	Yes
File Manager	Yes	Yes	Yes	Yes	No	No	No
Remote Workflow Submission Client	No	No	No	Yes	Yes	No	No
Remote Workflow Job Manager Client	No	No	No	Yes	Yes	No	No
Workflow Printer Administration	No	No	No	Yes	No	No	No
6050 - Workflow Hot Folder Utility	No	No	No	Yes	Yes	No	No

**Table 4. Required Windows Firewall settings**

<b>PORT / Exception</b>	<b>FreeFlow Makeready Client</b>	<b>FreeFlow Makeready with Document Library</b>	<b>FreeFlow Web Services</b>	<b>FreeFlow Process Manager Server</b>	<b>FreeFlow Process Manager Client</b>	<b>FreeFlow Scanner 665E</b>	<b>Standalone Quick Print</b>
7778 - JMF Listening Port	No	No	No	Yes	Yes	No	Yes
8090 or reassigned port # - Repository Connector	Yes w/ Repository Connector	Yes w/ Repository Connector	Yes w/ Repository Connector	Yes w/ Repository Connector	No	No	No
8091 or reassigned port # - Repository Connector with SSL	Yes w/ Repository Connector	Yes w/ Repository Connector	Yes w/ Repository Connector	Yes w/ Repository Connector	No	No	No
FreeFlow Administration Tool (E:\FreeFlow\FFAdminTool.exe)	Yes	Yes	Yes	Yes	Yes	No	No
C:\Windows\ADA Mdsamain.exe (FreeFlow Directory Services)	No	No	No	No	Yes	No	No
Workflow Builder (E:\FreeFlow\WFBuilder.exe)	No	No	No	No	Yes	No	No
E:\FreeFlow\ScanAndPrint.exe	No	No	No	No	No	Yes	No
Library Administration Tool	Yes	Yes	No	Yes	No	No	No
Library Search	Yes	Yes	No	No	Yes	No	No
Batch Tool	Yes	Yes	No	Yes	Yes	No	No
E:\FreeFlow\neta gtst.exe	Yes	Yes	No	Yes	Yes	No	No
C:\Program Files\Texas Imperial\WFTPD Pro.exe	Yes	Yes	Yes	No	No	No	No

## RDO printing to DocuSP

---

To allow RDO printing to DocuSP with the Windows Firewall enabled, you must disable the Application Layer Gateway Service.



To disable the Application Layer Gateway Service:

1. Log in to the workstation as an administrator.
2. From the Windows desktop, right-click on [**My Computer**].
3. Select [**Manage**].
4. Expand [**Services and Applications**].
5. Select [**Services**].
6. Double-click on [**Application Layer Gateway Services**].
7. Stop the service, if it is running, by selecting [**Stop**].
8. In the Startup Type drop-down list, select [**Disabled**].
9. Select [**Apply**].
10. Select [**OK**].

---

## 2 - Physical Location/Access

---

The second step in acquiring a more secure system is to restrict physical access to systems and data. Any physical access to systems or data allows opportunities for the system to be compromised.

It is recommended that hardware be stored in a limited access area and that only authorized personnel be allowed access to the systems.

---

## 3 - Operating System/System Security

---

The third step in acquiring a more secure system is keeping the system up to date with patches for known vulnerabilities. Performing routine downloads of updates is imperative.

### **FreeFlow's patch management strategy**

---

FreeFlow's patch management strategy for Microsoft is as follows:

- All vendor security patches available before launch are validated and included in our product, if possible.
- It is recommended that the customer perform Windows Update on a weekly basis. Customers requiring Xerox assistance in installing Microsoft updates or in configuring their system for Automatic Updates should contact the Customer Support Hotline or make arrangements with their Xerox Representative. Xerox will install approved Service Packs and non-critical updates at the next service call.
- Operating system Service Packs are not to be installed through Windows Update. Approved Service Packs will be deployed through formal communication.
- Xerox distributes monthly bulletins listing critical or important ***minimal*** updates that should be installed on the FreeFlow system through Windows Update.

## Internet Explorer settings

---

Additional settings are required for Internet Explorer as a result of more secure Windows XP SP2 and Windows Server 2003 SP1 Service Packs.

### Microsoft XP SP2 pop-up blocker

If your client has Windows XP with SP2 operating system, you may need to turn off the pop-up blocker. The default setting for the Windows XP SP2 pop-up blocker prevents most pop-up windows.



To turn off the pop-up blocker:

1. Open Internet Explorer.
2. Select [**Tools: Pop-up Blocker: Turn Off Pop-up Blocker**].
3. Select [**File: Close**] to close the browser.

The Pop-up Blocker does not block pop-ups from web sites that are on your local intranet or are listed as a Trusted Site. If you are browsing a web site outside your intranet, you must change the Pop-up Blocker settings to allow the address of the web site you wish to browse.



To change the pop-up blocker settings:

1. Open Internet Explorer.
2. If the Pop-up Blocker is turned off, you must turn on the Pop-up Blocker before changing the Pop-up Blocker settings. If necessary, turn on the Pop-up Blocker settings by selecting [**Tools: Pop-up Blocker: Turn On Pop-up Blocker**].
3. Select [**Tools: Pop-up Blocker: Pop-up Blocker Settings**].
4. Enter the address or URL of the web site you want to allow, and select [**Add**].
5. Select [**Close**].
6. Select [**File: Close**] to close the browser.

### Check Microsoft's website

Check [www.microsoft.com](http://www.microsoft.com) for additional suggestions regarding system security.

## 4 - Virus Protection

---

The fourth step in maintaining a more secure system is to use virus detection software.

### **Protecting the system from virus protection**

---

Xerox takes special precautions to ensure its software is shipped free from computer virus contamination. It is strongly recommended that you invest in a virus detection software application to protect your system from viruses.

Computer viruses are best detected by virus detection and control application software that is accepted by the PC industry.

Some of the virus detection and control applications available to and widely-used by the PC industry include:

- Norton Anti-Virus by Symantec
- McAfee VirusScan by Network Associates, Inc.



*NOTE: To ensure maximum protection from new viruses, update or upgrade your virus detection software frequently.*

It is strongly recommended that you follow these guidelines to keep your system decontaminated:

- On a regular basis (at least weekly), run virus detection software on all systems.
- In the event you find a virus on a system, delete the infected file using Document Library. Then, recover the file via restore.



*NOTE: This is to protect your data in the event of corruption during the course of the virus removal.*

You can then remove the virus using the procedures supplied with your virus protection software.

---

## 5 - User Authentication and Password Management

---

The fifth step in acquiring a more secure system is to implement strong access control measures. This will ensure that critical data can be accessed only in an authorized manner. Our software imposes a very complex security program based on “access control lists” that control user rights and privileges to all objects in the repository. Review the “User account management section” later in this chapter for more information on managing your accounts.

The following are security recommendations for keeping the FreeFlow system secure:

- **Login and authentication**
  - **For FreeFlow Process Manager systems** — FreeFlow Process Manager supports user authentication and application level authorization through the FreeFlow Administration Tool directory service facility. The FreeFlow Administration Tool adheres to operating system defined password administration policies.
  - **For FreeFlow Web Services systems** — FreeFlow Web Services provides LDAP support which enables FreeFlow to easily integrate with any LDAP compliant system. This will insure that all user information will be available to the FreeFlow Web Services 5.0 system through a simple setup. FreeFlow Web Services also provides Single Sign-on capability through the Automatic Login feature. This feature enables the authentication of Print Buyer users through an external system. This external system receives authentication requests in the http format and responds with a standard XML reply.

The Automatic Login allows for a seamless integration between FreeFlow Web Services 5.0 to external applications, such as organization intranets. A user that has logged in to an external system will not have to re-enter his credentials (username, password) when coming over from an external application into FreeFlow Web Services 5.0

- **For legacy Document Library** — The legacy Document Library application allows you to enable or disable complex passwords, specify a password expiration date, and enable or disable the “Remember Password” option for applications that access the Document Library repository.

It is recommended that you:

Enable complex passwords for all users

Enable password expiration

Not enable “Remember Password”



*NOTE: If your Domain or Local Security Policy requires complex passwords, the setting for complexity in the Library Administration Tool must be enabled.*

- **Complex passwords**

It is recommended that you enable complex passwords in the Local Security Policy.



*NOTE: If using the legacy Document Library, the complex password setting is set by default in the Library Administration Tool. It is recommended that you keep Complexity enabled for FreeFlow. If your Domain or Local Security Policy requires complex passwords, the setting for complexity in the Library Administration Tool must be enabled.*

- **User account name requirements**

If using legacy Document Library, the Document Library user accounts cannot be renamed.

- **User account management**

The following steps are recommended for managing your user accounts on the FreeFlow system:



1. Identify all users with a unique user name before allowing them access to the FreeFlow system. This ensures that actions taken on critical data and systems are performed by known and authorized users.
2. Remove inactive user accounts at least every 90 days.
3. Do not use group, shared, or generic accounts and passwords.
4. Change user passwords at least every 30 days using the Local Security Policy for system access.



*NOTE: If using legacy Document Library, set the user password expiration in Library Administration Tool.*

5. FreeFlow administrator and user account passwords require a minimum user password length of 7 characters.
6. If using legacy Document Library, users can change their own user account passwords.



#### **CAUTION**

***DO NOT*** change the *xdl\_admin* password on FreeFlow Process Manager servers. If you change the *xdl\_admin* password on a FreeFlow Process Manager server, you must contact your Xerox Representative.



