

Security Document

For FreeFlow® configurations:

FreeFlow® Makeready

FreeFlow® Web Services

FreeFlow® Process Manager

Standalone FreeFlow® Print Manager - Advanced Print Path

FreeFlow® Print Manager

FreeFlow® Print Manager JMF Service

FreeFlow® Output Manager

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

Copyright © 1996-2007 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. All instances of the name PostScript in the text are references to the PostScript language as defined by Adobe Systems Incorporated unless otherwise stated. The name PostScript also is used as a product trademark for Adobe Systems' implementation of the PostScript language interpreter, and other Adobe products.

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.

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.

PANTONE® and other Pantone Inc. trademarks are the property of Pantone Inc. All rights reserved.

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

StorageView™ is a trademark of CMD Technology, Inc.

TIFF® is a registered trademark of Aldus Corporation.

Windows®, Windows XP®, Windows Server® 2003, 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. 2002-2007. All rights reserved

Includes Adobe® PDF Libraries and Adobe Normalizer technology

The Graphics Interchange Format® is the Copyright property of CompuServe Incorporated. GIFSM is a Service Mark of CompuServe Incorporated.

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

Parts of this software Copyright © 2004-2006 Enterprise Distributed Technologies Ltd. All Rights Reserved.

Parts of this software Copyright ©1995-2003, The Cryptic Foundation Limited. All Rights Reserved.

Parts of this software are a SSLv3/TLS implementation written by Eric Rescorla by Claymore Systems, Inc. All Rights Reserved.

Parts of this software Copyright © 2002, Lee David Painter and Contributors. Contributions made by Brett Smith, Richard Pernavas, Erwin Bolwidt.

Parts of this software Copyright © 1995-2005, Jean-loup Gailly and Mark Adler.

All other product names and services mentioned in this publication are trademarks of their respective companies. They are used throughout this publication for the benefit of those companies, and are not intended to convey endorsement or other affiliation with the publication.

Companies, names, and data used in examples herein are fictitious unless otherwise noted.

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

Table of contents

1. Security recommendations	1-1
Overview	1-1
Security best practices	1-2
1 - Network Security	1-3
Hardware Firewall	1-5
Windows Firewall	1-8
Reassigning Port Numbers	1-11
Reassigning port numbers in FreeFlow Web Services	1-11
Reassigning port numbers for Repository Connector ports	1-12
Reassigning port numbers in FreeFlow Output Manager	1-13
Reassigning port numbers in the FreeFlow Accounting Module	1-14
Configuring Password Authentication for the Oracle Listener	1-15
RDO printing to FreeFlow Print Server	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
Disable nonessential services	1-19
4 - Virus Protection	1-20
Protecting the system from viruses	1-20
McAfee VirusScan configuration recommendations for FreeFlow Web Services	1-21
Disabling the script scan feature	1-21
Excluding the global.asa file	1-22
Using email in Process Manager and Web Services	1-22
5 - User Authentication and Account Management	1-23

1. Security recommendations

Overview

This document describes the recommended security settings for FreeFlow Makeready, FreeFlow Web Services, FreeFlow Process Manager, Standalone FreeFlow Print Manager - Advanced Print Path, FreeFlow Print Manager, FreeFlow Print Manager JMF Service, and FreeFlow Output Manager.

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.

Table 1-1 provides the required port settings for both Hardware Firewall or Windows Firewall with FreeFlow.



NOTE: All ports require both inbound and outbound communication unless otherwise noted.

The Windows Firewall will not prevent outbound communication, therefore, ports marked "Outbound only" do not need to be opened in the Windows Firewall.

Table 1-1. Required port settings for both Hardware Firewall or Windows Firewall

PORT	Protocol or Application	Required for FreeFlow Makeready	Required for Standalone FreeFlow Print Manager - Advanced Print Path	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	Required for FreeFlow Print Manager JMF Service
21	FTP	No	No	Yes	Yes	No	No	Yes, outbound only to FreeFlow Print Server for Accounting Module	No
631	IPP	Yes, outbound only to FreeFlow Print Server w/ High Security disabled	Yes, outbound only to FreeFlow Print Server w/ High Security disabled	No	Yes, outbound only to FreeFlow Print Server w/ High Security disabled	No	Yes, outbound only to FreeFlow Print Server w/ High Security disabled	Yes	Yes
443	SSL/TLS	Yes, outbound only to FreeFlow Print Server w/ High Security enabled	Yes, outbound only to FreeFlow Print Server w/ High Security enabled	No	Yes, outbound only to FreeFlow Print Server w/ High Security enabled	No	Yes, outbound only to FreeFlow Print Server w/ High Security enabled	Yes, outbound only to FreeFlow Print Server with High Security enabled	Yes, outbound only to FreeFlow Print Server with High Security enabled

Table 1-1. Required port settings for both Hardware Firewall or Windows Firewall

PORT	Protocol or Application	Required for FreeFlow Makeready	Required for Standalone FreeFlow Print Manager - Advanced Print Path	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	Required for FreeFlow Print Manager JMF Service
22	SSH/sFTP	Yes, outbound only to FreeFlow Print Server w/ High Security enabled	Yes, outbound only to FreeFlow Print Server w/ High Security enabled	Yes	Yes	No	No	Yes, outbound only to FreeFlow Print Server for Accounting Module	No
515 (or range 513 - 1023)	LPR	Yes, outbound only	Yes, outbound only	No	Yes, outbound only	No	Yes, outbound only	Yes	Yes
135	RPC End Point Mapper	No	No	No	Yes	No	No	No	No
1521	Oracle Listener	No	No	No	Yes	No	No	No	No
80	HTTP or reassigned port #	No	No	Yes	No	No	Yes	Yes on Creo	Yes on Creo
8080	HTTP	No	No	No	No	No	No	Yes, inbound only	No
8443	HTTPs	No	No	No	No	No	No	Yes, inbound only	No
5000 - 5024	Workflow Submission Clients	No	No	No	Yes	Yes	No	No	No
5025 - 5049	Workflow Job Manager	No	No	No	Yes	Yes	No	No	No
5050	Workflow Builder	No	No	No	Yes	No	No	No	No
6789	Workflow Database Server	No	No	No	Yes	No	No	No	No
7890	Workflow TaskMgr	No	No	No	Yes	No	No	No	No
8053	Workflow Folder Monitor	No	No	No	Yes	No	No	No	No
7779	JMF Listening Port	No	No	No	Yes	No	No	No	No
7781	JMF Listening Port	No	No	No	No	No	No	Yes	Yes

Table 1-1. Required port settings for both Hardware Firewall or Windows Firewall

PORT	Protocol or Application	Required for FreeFlow Makeready	Required for Standalone FreeFlow Print Manager - Advanced Print Path	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	Required for FreeFlow Print Manager JMF Service
8090	Repository Connector	Yes, w/ Repository connector	No	Yes, w/ Repository connector	Yes, w/ Repository connector	No	No	No	No
8091	Repository Connector w/SSL	Yes, w/ Repository connector	No	Yes, w/ Repository connector	Yes, w/ Repository connector	No	No	No	No
25	SMTP	No	No	Yes, outbound only	Yes, outbound only	No	No	No	No
3200	Print Provider Queues for FreeFlow Web Services	No	No	Yes	No	No	No	No	No
7117	Common Printer Admin Service	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
9090	HTTP for FreeFlow Accounting Module	No	No	No	No	No	No	Yes, inbound only	No
9443	HTTP for FreeFlow Accounting Service w/ SSL	No	No	No	No	No	No	Yes, inbound only	No
4004	Authorization Service Port	Yes, w/ CMS	No	No	Yes	Yes, Outbound only	No	Yes	Yes
5640	User Metadata Service	No	No	No	Yes	Yes, Outbound only	No	No	No

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. If the tools are configured incorrectly, they may block desired inbound traffic.

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 1-2 provides the required port settings for FreeFlow Print Server DFE systems.

Table 1-2. Port settings for FreeFlow Print Server DFE systems

PORT	Protocol or Application	Required for FreeFlow Print Server when Production Printing from FreeFlow or when communicating with Output Manager		Required for FreeFlow Print Server 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 FreeFlow Print Server < 3.6	

Table 1-3 provides required port settings for DFE devices, not including FreeFlow Print Server.

Table 1-3. Port settings for DFE devices, not including FreeFlow Print Server

PORT	Protocol or Application	Required for the following DFEs: <ul style="list-style-type: none"> • EFI • Creo • DocuCentre • WorkCentre • AccXES • Scanvec Amiable 	Required for the following legacy DFEs <ul style="list-style-type: none"> • GXP 4110 • NPS Server • DT Network Server • NS Plus • NS + Server Series
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
80	HTTP	Yes (Creo only)	No
161	SNMP	Yes (DocuCentre, WorkCentre only)	Yes (GXP 4110 only)

Windows Firewall

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

1 3...
2

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.

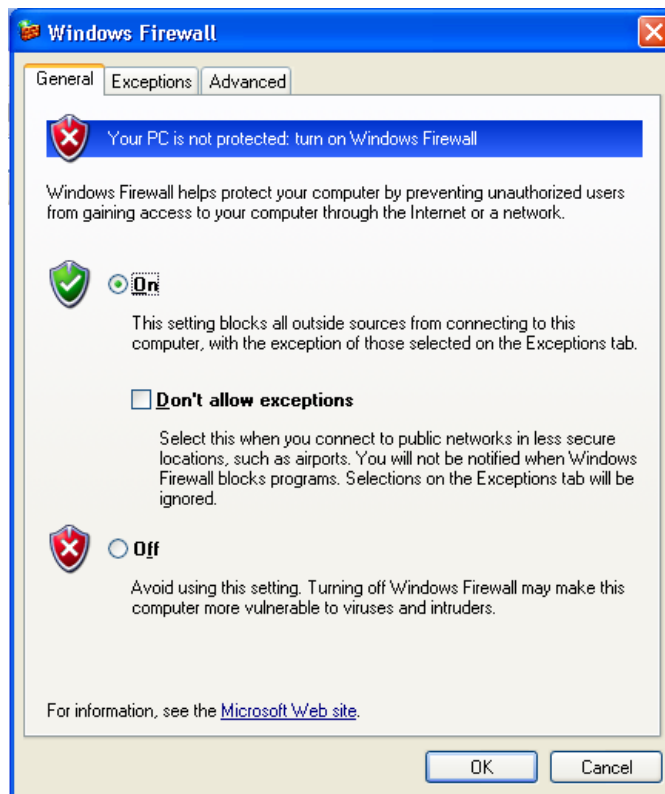


Figure 1-1. Windows Firewall dialog

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:
 - a. Select [**Add Port**] to add the applicable ports per configuration. Enter the applicable name (user defined) and port number. Refer to Table 1-3 on page 1-7 for a listing of required ports per configuration.



NOTE: The Windows Firewall will not prevent outbound communications, therefore, ports marked as "Outbound only" do not need to be added in the Windows Firewall.

- b. Select [**Add Programs**] to add the applicable exceptions per configuration. Refer to Table 1-4 on page 1-10 for a listing of required programs per configuration.

If using the Windows Firewall, Table 1-4 provides the required Windows Firewall Exceptions per configuration.



NOTE: All ports require both inbound and outbound communication unless otherwise noted.

Table 1-4. Required Windows Firewall Exceptions

PORT / Exception	FreeFlow Makeready Client	Standalone FreeFlow Print Manager - Advance Print Path	FreeFlow Web Services	FreeFlow Process Manager Server	FreeFlow Process Manager Client	FreeFlow Print Manager	FreeFlow Output Manager	FreeFlow Print Manager JMF Service
C:\Windows\System32\Dllhost.exe	No	No	No	Yes	No	No	No	No
C:\Windows\System32\msdtc.exe	No	No	No	Yes	No	No	No	No
FreeFlow Makeready (DSMR.exe)	Yes	No	No	No	No	No	No	No
ScanAndPrint.exe	Yes	No	No	No	No	No	No	No
File Manager (DPFileManager.exe)	Yes	No	Yes	Yes	No	No	No	No
Workflow Builder (WFBuilder.exe)	No	No	No	Yes	No	No	No	No
Remote Workflow Submission Client (WFSubmissionClient.exe)	No	No	No	Yes	Yes	No	No	No
Remote Workflow Job Manager Client (WFJobManager.exe)	No	No	No	Yes	Yes	No	No	No
Printer Registration (PrintRegistration.exe)	No	No	No	Yes	No	No	No	No
FreeFlow Administration Tool (E:\FreeFlow\FFAdminTool.exe)	Yes	No	Yes	Yes	No	No	No	No
Network Agent (NaAdmin.exe)	Yes	No	No	Yes	No	No	No	No
C:\Program Files\Texas Imperial\WFTPD Pro.exe	Yes	No	Yes	No	No	No	No	No
Acrobat.exe	No	No	Yes	No	No	No	No	No
Print Manager Advanced Print Path (FFPMPro.exe)	Yes	Yes	Yes	Yes	No	No	No	No

Reassigning Port Numbers

Use the following procedures when reassigning port numbers for FreeFlow Web Services, Repository Connector, and FreeFlow Output Manager.

Reassigning port numbers in FreeFlow Web Services

To reassign the HTTP and HTTPs ports in FreeFlow Web Services, change the port numbers as follows:

1 3...
2

1. Log in to the workstation as an administrator.
2. From the Windows desktop, right-click on [**My Computer**] and select [**Manage**].
3. Expand [**Services and Applications**].
4. Expand [**Internet Information Services (IIS) Manager**].
5. Expand [**Web Sites**].
6. Right-click on [**Default Web Site**] and select [**Properties**].
7. Change the [**TCP port**] and/or [**SSL port**] number(s) and select [**OK**].
8. In the same Default Web Site window, select the [**Advanced**] button.
9. In the Advanced Web Site Identification window, select [**Add**].
10. In the [**TCP port**] field, enter the new port number, and select [**OK**].
11. In the [Host Header Value] field, enter the local host address: <**127.0.0.1**>.
12. Close the Computer Management console.
13. Instruct users to include the port number in the FreeFlow Web Services URL address in order to have access.

For example: **123.456.7.0:8080/ws**

Reassigning port numbers for Repository Connector ports

To reassign the Repository Connector ports:



1. Log in to the workstation as an administrator.
2. From the Windows desktop, right-click on [**My Computer**] and select [**Manage**].
3. Expand [**Services and Applications**].
4. Expand [**Internet Information Services (IIS) Manager**].
5. Expand [**Web Sites**].
6. Right-click on [**Repository Management Service**] and select [**Properties**].
7. Change the [**TCP port**] and/or [**SSL port**] number(s) and select [**OK**].

Reassigning port numbers in FreeFlow Output Manager

To reassign the HTTP or HTTPS ports in FreeFlow Output Manager:



1. Edit the **web.xml** file using Notepad.

The file is located in **<FreeFlowOutput Manager installation directory>\jakarta-tomcat-5.5.17\webapps\WebClient\WEB-INF** directory.

For example: c:\Program Files\Xerox\FreeFlow Output Manager\jakarta-tomcat-5.0.28\webapps\WebClient\WEB-INF\web.xml

2. Search for the following entries in the file, located in the **<web-app>/<servlet>** section:
 - `<init-param> <param-name>HttpPort</param-name>
<param-value>8080<param-value> </init-param>`
 - `<init-param> <param-name>HttpsPort</param-name>
<param-value>8443<param-value> </init-param>`
3. Change the param-value for **HttpPort** and **HttpsPort** to the appropriate values.
4. Save the changes and close the Notepad.

Reassigning port numbers in the FreeFlow Accounting Module

To reassign the HTTP or HTTPS ports in the FreeFlow Accounting Module:

1 3...
2

1. Edit the **tomcat** properties file using Notepad.

The file is located in **c:\Program Files\Xerox\FreeFlow Accounting Module\config** directory.

2. Change the param-value for **HttpPort** and **HttpsPort** to the appropriate values.
3. Save the changes and close the Notepad.

Configuring Password Authentication for the Oracle Listener



NOTE: The information in this section was obtained from the Oracle9i Net Services Administrator Guide.

It is important to provide security through a password for the listener. With a password, privileged operations, such as saving configuration changes or stopping the listener, will require a password.

Use the Listener Control utility's `CHANGE_PASSWORD` command to set or modify an encrypted password in the `PASSWORDS-listener_name` parameter in the `listener.ora` file. If the `PASSWORDS_listener_name` parameter is set to an unencrypted password, you must manually remove it from the `listener.ora` file prior to modifying it. If the unencrypted password is not removed, you will be unable to successfully set an encrypted password.



To set a new encrypted password with the `CHANGE_PASSWORD` command, issue the following commands from the Listener Control utility:

1. Select [**Start: Run**].
 - a. Enter `<LSNRCTL>`
 - b. Select [**Enter**]. The `LSNRCTL` prompt displays.
2. Enter the following commands:
 - a. At the `LSNRCTL` command prompt, enter `<CHANGE_PASSWORD>`
 - b. Enter the Old password.
 - c. Enter a New password.
 - d. Reenter the new password.
 - e. At the `LSNRCTL` command prompt, enter `<SAVE_CONFIG>`



NOTE: If you are administering the listener remotely over an insecure network and require maximum security, configure the listener with a secure protocol address that uses the TCP/IP with SSL protocol. If the listener has multiple protocol addresses, ensure that the TCP/IP with SSL protocol address is listed in the `listener.ora` file.

RDO printing to FreeFlow Print Server

To allow RDO printing to FreeFlow Print Server 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 Microsoft Update on a weekly basis. Customers requiring Xerox assistance in installing Microsoft update 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 Microsoft Update. Approved Service Packs will be deployed through formal communication.
- Xerox distributes monthly bulletins, when required, listing updates that should be "excluded" on the FreeFlow system. This information is also communicated on the www.xerox.com/security web site under "Product Security Guidance". High priority and security-related updates are critical and should always be installed unless they are specifically excluded.

Internet Explorer settings

Additional settings are required for Internet Explorer as a result of more secure Windows XP SP2 and Windows Server 2003 SP2 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 for additional suggestions regarding system security.

Disable nonessential services

To enhance the security of the system, the following services should be disabled through the Control Panel:



1. Select [**Start: Settings: Control Panel**] from the Windows desktop.
2. Select [**Administrative Tools: Services**].
3. Disable the following services:
 - Computer Browser
 - Distributed Link Tracking Client
 - Distributed Link Tracking Server



NOTE: Applicable to a server operating system only.

- Remote Registry
4. Close the Control Panel.

4 - Virus Protection

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

Protecting the system from viruses

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.



NOTE: The customer is ultimately responsible for protecting their systems against 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. 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.

McAfee VirusScan configuration recommendations for FreeFlow Web Services

If using McAfee VirusScan with your FreeFlow Web Services system, it is recommended that you disable the script scan feature and exclude the global.asa file from the Newsway folder to obtain optimum performance on your system.



NOTE: FreeFlow Web Services also supports Norton AntiVirus. However, this section pertains only to using McAfee VirusScan with your FreeFlow Web Services system. Refer to the Norton AntiVirus documentation for procedures on disabling the script scan feature and excluding the global.asa file in Norton AntiVirus.

Disabling the script scan feature

When McAfee Antivirus scans the FreeFlow Web Services server, the performance of the FreeFlow Web Services application may become slow, eventually causing the system to lock up. Therefore, it is recommended that you disable the script scan feature by unregistering the scripproxy.dll.



NOTE: Running script scanning on a FreeFlow Web Services system can cause a memory leak in the ISS worker process, which will eventually lock up the server.



1. From the System Tray, open the VirusScan Console.



*NOTE: If the VirusScan Console is not available from the System Tray, select [**Start: Programs: Network Associates: VirusScan Console**].*

2. Highlight [**On-Access Scanner**] and select [**Properties**].
3. Select the **ScriptScan** tab.
4. Clear the [**Enable ScriptScan**] check box. and select [**Apply**].
5. Start the **Command Prompt** and do the following:
 - a. Enter <regsvr32 /u c:\Program Files\Network Associates\VirusScan\scriptproxy.dll.>
 - b. Close the Command Prompt.
6. Close the VirusScan Console.

Excluding the global.asa file

If you are using McAfee VirusScan with your FreeFlow Web Services system, it is recommended to exclude the global.asa file, located in the Newsway folder, from VirusScan.



To exclude the global.asa file on a FreeFlow Web Services system:

1. From the System Tray, right click on the **VirusScan** icon and select [**On-Demand Scan**].
2. Select the **Detection** tab.
3. Select [**Exclusions**].
4. Select [**Add**].
5. In the What to exclude area:
 - a. Select [**By name/location**].
 - b. Select [**Browse**] and locate e:\Newsway\global.asa
 - c. Select [**Ok**].
 - d. Select [**Ok**].
6. Select [**Save as default**].

Using email in Process Manager and Web Services

If using email notification in Process Manager, or email in Web Services, you will need to ensure that your anti-virus software does not block port 25.



To unblock port 25 in McAfee:

1. From the System Tray, open the VirusScan Console.



*NOTE: If the VirusScan Console is not available from the System Tray, select [**Start: Programs: Network Associates: VirusScan Console**].*

2. Highlight [**Access Protection**] and select [**Properties**].
3. Clear the [**Prevent mass mailing worms from sending mail**] check box. and select [**Apply**].

5 - User Authentication and Account 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. The security model in FreeFlow 6.0 has changed to a user model that transfers the responsibility for authentication to the operating system, supports finer-grained authorization, and allows closer integration with existing customer user-management capabilities. Review the “User account management section” later in this chapter for more information on managing your accounts.

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

- **Login and authentication**
 - **For FreeFlow Process Manager, Copyright Management Services, FreeFlow Output Manager, and Printer Registration** — Supports user authentication through the operating system and application-level authorization through membership in operating system groups.
 - **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 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 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.

- **Complex passwords**

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

- **User account management**

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

1. After FreeFlow Web Services is installed, there are two accounts created by default. The password and/or user name for these accounts must be changed so that system security is not breached.
 - **For the Print Provider default account** — Login with your Print Provider administrator account (the default administrator account is “printer”). Go to [**Settings: Site: Print Provider Accounts**] and change the login name and password for “printer”.
 - **For the Print Buyer default account** — Go to [**Customers: Users: Test Account**] and change the login name and password for “test”.
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.
5. FreeFlow administrator and user account passwords require a minimum user password length of 7 characters.



CAUTION

Changing the XDL_ADMIN password will cause some services to be re-started and will create a mismatch with the client-side password. Please contact your Xerox representative to match your client-side password with the new password for XDL_ADMIN.

