Version 9.0 SP17
December 2015
702P04116

Xerox® FreeFlow® Application Suite
Security Guide

BR#11635

Contents

1 FreeFlow Application Suite Security

Overview

This document describes security roles and responsibilities, security best practices, and recommended security settings for Xerox® FreeFlow Makeready®, Xerox® FreeFlow Process Manager®, Standalone Xerox® FreeFlow® Print Manager - Advanced Print Path, Xerox® FreeFlow® JMF Service, Xerox® FreeFlow® Express to Print Software, and Xerox® 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. Xerox strives to provide the most secure software product possible based on the information and technologies available while maintaining the products performance, value, functionality, and productivity. The components of FreeFlow are assessed for security compliance using commercially available vulnerability and penetration scanning tools. Application vulnerabilities are addressed based on results of our internal scans.

After a product is launched, Xerox distributes bulletins when required, listing Microsoft updates that should be “excluded” on the FreeFlow system. Xerox also reviews publicly distributed US-Cert vulnerabilities for applicability to Xerox® products.

Although Xerox will strive to provide software that is secure, the customer is ultimately responsible for securing their environment to meet their specific security needs. Because of the diversity of our customers and the richness of their workflows, it is not possible to deliver a one-size-fits-all solution that will satisfy the broad range of security requirements needed by customers. For example, not every customer needs, nor wants, a very high degree of security which supports only one print protocol, and one system operator account. Xerox delivers products with standard security configurations along with the ability to modify security configurations to meet customer needs. On-site configuration is intended to be performed by the customer system administrator assigned to manage the product platforms. The security configuration activity must take into consideration and balance the need to minimize the security risks with the need to enable those protocols required to satisfy critical customer workflows.Depending on their individual needs, customers can increase security by installing a firewall, implementing a private network, hardening the Operating System to satisfy compliance requirements, and/or physically securing their computing/network hardware to a limited access area. Again, depending on their needs, customers can use tools to monitor and log physical and network access to the FreeFlow hardware and software to determine if and when a security incident has occurred. Customers also should back-up their data to ensure that it can be recovered in case of deletion or corruption.

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
- System Security
- Virus Protection
- User Authentication and Password Management

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.

The table below 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.

PORT	Protocol or Application	Required for FreeFlow Makeready	Required for Stand-alone FreeFlow Print Manager - Advanced Print Path	Required for FreeFlow Express to Print	Required for FreeFlow Process Manager servers	Required for FreeFlow Process Manager clients	Required for FreeFlow Output Manager	Required for FreeFlow JMF Service
21	FTP	No	No	No	Yes	No	Yes, outbound to FreeFlow Printer Server for Accounting Module; inbound from MFDs if Send-to-Production feature is enabled.	No

PORT	Protocol or Application	Required for FreeFlow Makeready	Required for Stand-alone FreeFlow Print Manager - Advanced Print Path	Required for FreeFlow Express to Print	Required for FreeFlow Process Manager servers	Required for FreeFlow Process Manager clients	Required for FreeFlow Output Manager	Required for FreeFlow 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, outbound only to FreeFlow Print Server w/ High Security enabled	Yes	No	Yes, outbound only to FreeFlow Print Server for Accounting Module	No
25	SMTP	No	No	No	Yes, outbound only	No	No	No
80	HTTP or reassigned port #	Yes w/ Copyright Manage-ment Service	No	No	No	No	Yes on Creo	Yes on Creo
80	WSD	Yes, outbound only to communicate with Xerox printer without high security	No	No	No	No	No	No
135	RPC End Point Mapper	No	No	No	Yes	No	No	No
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	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 with High Security enabled	Yes, outbound only to FreeFlow Print Server with High Security enabled
631	IPP	Yes, outbound only to FreeFlow Print Server w/ High Security disabled	Yes, outbound only to FreeFlow Print Server w/ High Security disabled	Yes, outbound only to FreeFlow Print Server w/ High Security enabled	Yes, outbound only to FreeFlow Print Server w/ High Security disabled	No	Yes	Yes
515 (or range 513 - 1023)	LPR	Yes, outbound only	Yes, outbound only	Yes, outbound only	Yes, outbound only	No	Yes	Yes
1521	Oracle Listener	No	No	No	Yes	No	No	No
8080	HTTP	No	No	No	No	No	Yes, inbound only	No
8443	HTTPs	No	No	No	No	No	Yes, inbound only	No
5000 - 5024	Workflow Submission Clients	No	No	No	Yes	Yes	No	No

PORT	Protocol or Application	Required for FreeFlow Makeready	Required for Stand-alone FreeFlow Print Manager - Advanced Print Path	Required for FreeFlow Express to Print	Required for FreeFlow Process Manager servers	Required for FreeFlow Process Manager clients	Required for FreeFlow Output Manager	Required for FreeFlow JMF Service
5025 - 5049	Workflow Job Manager	No	No	No	Yes	Yes	No	No
5050	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	Workflow Folder Monitor	No	No	No	Yes	No	No	No
7779	JMF Listening Port	No	No	No	Yes	No	No	No
7781	JMF Listening Port	No	No	No	No	No	Yes	Yes
8090	Repository Connector	Yes, w/ Repository connector and Copyright Manage-ment Service	No	No	Yes, w/ Repository connector	No	Yes, with Repository Connector	No
8091	Repository Connector w/ SSL	Yes, w/ Repository connector	No	No	Yes, w/ Repository connector	No	Yes, with Repository Connector	No
7117	Common Printer Admin Service	Yes	Yes	Yes	Yes	No	Yes	Yes
9090	HTTP for FreeFlow Accounting Module	No	No	No	No	No	Yes, inbound only	No
9443	HTTP for FreeFlow Accounting Service w/SSL	No	No	No	No	No	Yes, inbound only	No
4004	Authorization Service Port	Yes, w/ CMS	No	No	Yes	Yes, Outbound only	Yes	Yes
5640	User Metadata Service	No	No	No	Yes	Yes, Outbound only	No	No
57891	FreeFlow Template Manager	No	No	Yes	No	No	No	No
55682	FreeFlow Express to Print	No	No	Yes	No	No	No	No

Firewall Settings

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.

The table below provides the required 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	

The table below provides required port settings for DFE devices, not including FreeFlow Print Server.

PORT	Protocol or Application	Required for the following DFEs: EFI Creo DocuCentre WorkCentre AccXES Scanvec Amiable	Required for the following legacy DFEs GXP 4110 NPS Server DT Network Server NS Plus NS + Server Series
21	FTP	No	Yes
631	IPP	Yes, for all EFI IPP printers	No
22	SSH/s FTP	No	No
443	SSL/TLS	No	No
515 (or range 513 - 1023)	LPR	Yes	Yes
135	RPC	Yes, EFI only	No
80	HTTP	Yes (Creo only)	No
161	SNMP	Yes (DocuCentre, WorkCentre only)	Yes (GXP 4110 only)

PORT	Protocol or Application	Required for the following DFEs: EFI Creo DocuCentre WorkCentre AccXES Scanvec Amiable	Required for the following legacy DFEs GXP 4110 NPS Server DT Network Server NS Plus NS + Server Series
162	SNMP	Yes for EFI only	

Windows Firewall

On the FreeFlow system, the Windows Firewall is DISABLED by default in the base Windows Server 2003 operating systems and ENABLED by default in the Windows Server 2008, Windows 7, Windows 8, Windows 10, and Windows Server 2012 operating systems.

The table below provides the required Windows Firewall Exceptions per configuration.

> Note
> If using the Convert node in Process Manager, "File and Printer Sharing" communication must be allowed. This can be added as a Windows Firewall Exception. For a Hardware Firewall, ports TCP/139 and TCP/445 must be opened.

Exception	FreeFlow Makeready Client	Standalone FreeFlow Print Manager - Advance Print Path	Required for FreeFlow Express to Print	FreeFlow Process Manager Server	FreeFlow Process Manager Client	FreeFlow Print Manager	FreeFlow Output Manager	FreeFlow 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	No	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 (Print Registration.exe)	No	No	No	Yes	No	No	No	No
FreeFlow Administration Tool (E:\FreeFlow\FFAdminTool.exe)	Yes	No	No	Yes	No	No	No	No

Exception	FreeFlow Makeready Client	Standalone FreeFlow Print Manager - Advance Print Path	Required for FreeFlow Express to Print	FreeFlow Process Manager Server	FreeFlow Process Manager Client	FreeFlow Print Manager	FreeFlow Output Manager	FreeFlow JMF Service
Network Agent (NaAdmin.exe)	Yes	No	No	Yes	No	No	No	No
C:\Program Files\Texas Imperial\WFTPD Pro.exe	Yes	No	No	No	No	No	No	No
Acrobat.exe	No	No	No	No	No	No	No	No
Print Manager Advanced Print Path (FFPMPro.exe)	Yes	Yes	No	Yes	No	No	No	No
FreeFlow Easy to Print (FreeFlowEZ.exe)	No	No	Yes	No	No	No	No	No
File and Printer Sharing	No	No	No	Yes	No	No	No	No

Configure the Windows Firewall using the Control Panel per your specific operating system instructions.

1. Add applicable ports per your configuration as referenced in the required ports table on page 1-3.

- To add ports for the various operating systems:
  - In Windows Server 2003 and Windows Server 2008, open the Exceptions tab in the Windows Firewall user interface.
  - In Windows 7 and Windows Server 2008 R2, select Advanced Settings in the Windows Firewall user interface, then select Inbound Rules and select New Rule.
  - In Windows 8, Windows 10, and Windows Server 2012, from the Control Panel select System and Security and select the Windows Firewall. In Windows Firewall with Advanced Settings, click Inbound Rules. Under Actions, click New Rule and the New Inbound Rule Wizard displays.

  Note

  The Windows Firewall will not prevent outbound communications. Ports marked as Outbound only do not need to be added in the Windows Firewall.

2. Add the applicable program exceptions per your configuration as referenced in the Windows Firewall Exceptions table on page 1-7.

- To add program exceptions for the various operating systems:
  - In Windows Server 2003 and Windows Server 2008, open the Exceptions tab in the Windows Firewall user interface.
  - In Windows 7 and Windows Server 2008 R2, select Allow a program through Windows Firewall in the Windows Firewall user interface, then select Change Settings and select Allow another program.
  - In Windows 8, Windows 10, and Windows Server 2012, from the Control Panel, select System and Security and select the Windows Firewall. Click Turn Windows Firewall on or off. Select Turn on Windows Firewall under both the Home or work (private) network location and Public network location, or select an option that is appropriate for your location. Select OK, then click Allow a program or feature through Windows Firewall, and select Change Settings.Reassigning Port Numbers

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

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\webapps\WebClient\WEB-INF** directory.

   For example: c:\Program Files\Xerox\FreeFlow Output Manager\jakarta-tomcat\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.

To reassign the FTP port in FreeFlow Output Manager Send-to-Production feature:

1. Edit the FtpSpooler.properties file using Notepad. The file is located in <FreeFlowOutput Manager installation directory>\config directory. For example: c:\Program Files\Xerox\FreeFlow Output Manager\config\FtpSpooler.properties
2. Change the param-value for configurableFTPport to the appropriate value.
3. 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. 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.

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**].

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.

System Security

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

FreeFlow third-party patch management strategy

FreeFlow patch management strategy for Microsoft is as follows:

- It is recommended that the customer perform Microsoft Update on a monthly basis.
- Operating system Service Packs are not to be installed through Microsoft Update until formal communication of support.
- 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.

FreeFlow patch management strategy for Adobe is as follows:

- It is recommended that the customer perform Adobe Acrobat updates on a monthly basis or as the updates become available.

Internet Explorer settings

Additional settings are required for Internet Explorer as a result of a more secure Windows operating system. The default setting for Windows pop-up blocker prevents most pop-up windows. You may need to turn off the pop-up blocker.

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.

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.

To improve performance, it's recommended you exclude the following items from anti-virus scanning:

- TIF, RDO and Log file types
- C:\DSEXCHNG.DIR on Makeready systems

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 recommendations for FreeFlow Output Manager

If using McAfee VirusScan with your FreeFlow Output Manager system, it is recommended that you set up folder exclusions to avoid potential problems with Output Manager operations.

Note

If using any other virus protection other than McAfee VirusScan, it is recommended that you set up folder exclusions within that software as well.

1. Right-click on [McAfee VirusScan On-Access Scan].
2. Select [VirusScan Console].
3. Select [Tools: Unlock User Interface].

Note

If the Unlock User Interface is greyed out, select [Tools: Open Remote Console] and in the Connect to Computer area input the IP Address of the Output Manager system, then select [OK]. This activates the Unlock Use Interface option.

Note

If a password is required, contact your system administrator.

4. Right-click on [On-Access Scanner] and select [Properties].
5. Select [All Processes].
6. Select the Detection tab.
   a. Under What not to scan, select [Exclusions].
   b. Select [Add] to add exclusions.
   c. In the What to Exclude section, select [By name/location].
   d. Use [Browse] to locate and select the following folders:

      C:\Program Files\Xerox\FreeFlow Output Manager\persistence

      C:\Program Files\Xerox\FreeFlow Output Manager\spool

Note

The FreeFlow Output Manager directory may not be located on the C: drive on your FreeFlow system. If necessary, search for the appropriate location and select the folders.

   a. Mark the [Also exclude subfolders] check box.
   b. In the When to exclude section, mark the [On read] and [On write] check boxes.
   c. Select [OK].
7. Select [OK] to close Set Exclusions.
8. Select [OK] to close On-Access Scan Properties.
9. Select [**Tools: Lock User Interface**].

McAfee VirusScan recommendations for FreeFlow Process Manager

If using McAfee VirusScan with your FreeFlow Process Manager system, it is recommended that you set up folder exclusions to avoid potential problems with Process Manager operations.

Note

If using any other virus protection other than McAfee VirusScan, it is recommended that you set up folder exclusions within that software as well.

1. Right-click on [**McAfee VirusScan On-Access Scan**].
2. Select [**VirusScan Console**].
3. Select [**Tools: Unlock User Interface**].

Note

If the Unlock User Interface is greyed out, select [**Tools: Open Remote Console**] and in the Connect to Computer area input the IP Address of the Process Manager system, then select [**OK**]. This activates the Unlock Use Interface option.

Note

If a password is required, contact your system administrator.

4. Right-click on [**On-Access Scanner**] and select [**Properties**].
5. Select [**All Processes**].
6. Select the **Detection** tab.
   a. Under What not to scan, select [**Exclusions**].
   b. Select [**Add**] to add exclusions.
   c. In the What to Exclude section, select [**By name/location**].
   d. Use [**Browse**] to locate and select the following folders:

      C:\Documents and Settings\All Users\Applications Data\Enfocus Prefs folder

      C:\Program Files\Enfocus software

   For any Process Manager utilizing external nodes, the input, output, and error folders utilized by the external nodes need to be excluded, otherwise, failures result with these workflows.

      E:\FFxTools

   The FFxTools directory may not be located on the E: drive on your FreeFlow system. If necessary, search for the appropriate location and select the folder.

      E:\Pitstop_HOT_FOLDERS

   Note

   The Pitstop_HOT_FOLDERS directory may not be located on the E: drive on your FreeFlow system. If necessary, search for the appropriate location and select the folder.

      E:\FreeFlow\ProcessManager\Spool

   Note

   The FreeFlow\ProcessManager\Spool directory may not be located on the E: drive on your FreeFlow system. If necessary, search for the appropriate location and select the folder.

   a. Mark the [**Also exclude subfolders**] check box.
   b. In the When to exclude section, mark the [**On read**] and [**On write**] check boxes.
   c. Select [**OK**].
7. Select [**OK**] to close Set Exclusions.
8. Select [**OK**] to close On-Access Scan Properties.
9. Select [**Tools: Lock User Interface**].
10. It is recommended to run a virus scan on the excluded folders before or after production runs with Process Manager to ensure folders are not infected.

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 applies 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 is this chapter for more information on managing your accounts.

Refer to the previous section, McAfee VirusScan recommendations for FreeFlow Process Manager, to ensure that frequently accessed folders are not impacted by the virus scan.

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

- Login and authentication

  User Authentication and application-level Authorization through the Operating System
  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.

- 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:

  Users: Test Account and change the login name and password for "test".

  a. Remove inactive user accounts at least every 90 days.
  b. Do not use group, shared, or generic accounts and passwords.
  c. Change user passwords at least every 30 days using the Local Security Policy for system access.
  d. 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.