VERSION 8.0.0
AUGUST 2024
702P09306

Xerox® FreeFlow® Core

Security Guide

xerox™

BR40387

Contents

Overview

This chapter contains:

Purpose

The purpose of this Security Guide is to disclose product security information related to Xerox® FreeFlow® Core. In this context, Product security is defined as how data is stored and transmitted, how the product behaves in a network environment, and how to access the product locally and remotely. This document describes the design, functions, and features of Xerox® FreeFlow® Core relative to Information Assurance (IA) and the protection of customer-sensitive information.

This document does not provide tutorial-level information about the security and connectivity of Xerox® FreeFlow® Core features and functions. For further information about these features and functions, refer to *Xerox® FreeFlow® Core Help*. It is assumed that the user has a working knowledge of these topics.

Customers are responsible for the security of their network and the FreeFlow product. The FreeFlow product does not enforce security for any network environment.

Target Audience

The target audience for this document is customers who require more security-related information about Xerox® FreeFlow® Core software.

Disclaimer

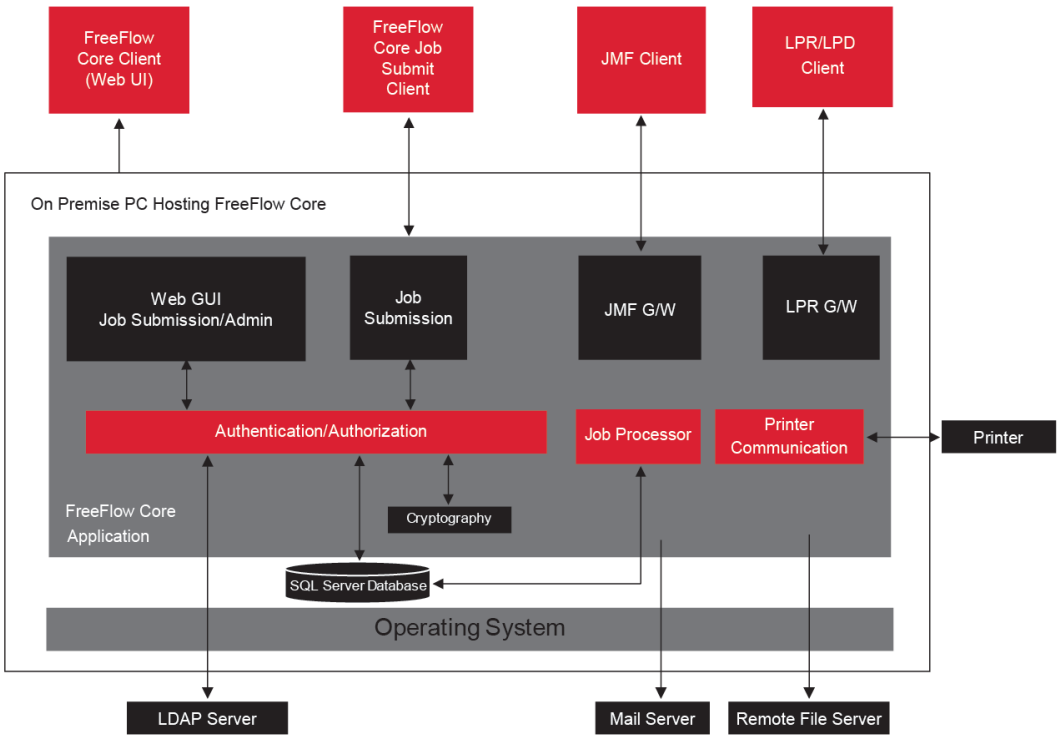
The information contained in this document is accurate as of the publication date and is provided with no warranties. In no event shall Xerox® Corporation be liable for any damages resulting from the usage or disregard of the information provided in this document, including direct, indirect, incidental, consequential, loss of business profits, or special damage, even if Xerox® Corporation has been advised of the possibility of such damages.

Product Description

This chapter contains:

Xerox® FreeFlow® Core is the next generation in workflow solutions from Xerox. FreeFlow Core is a browser-based solution intelligently automates and integrates the processing of print jobs, from a file preparation to a final production. FreeFlow Core gives you a hands-free workflow that operates easily, adapts effortlessly, scales quickly, and delivers consistently.

System Software Structure



Security Aspects of Selected Features

This chapter contains:

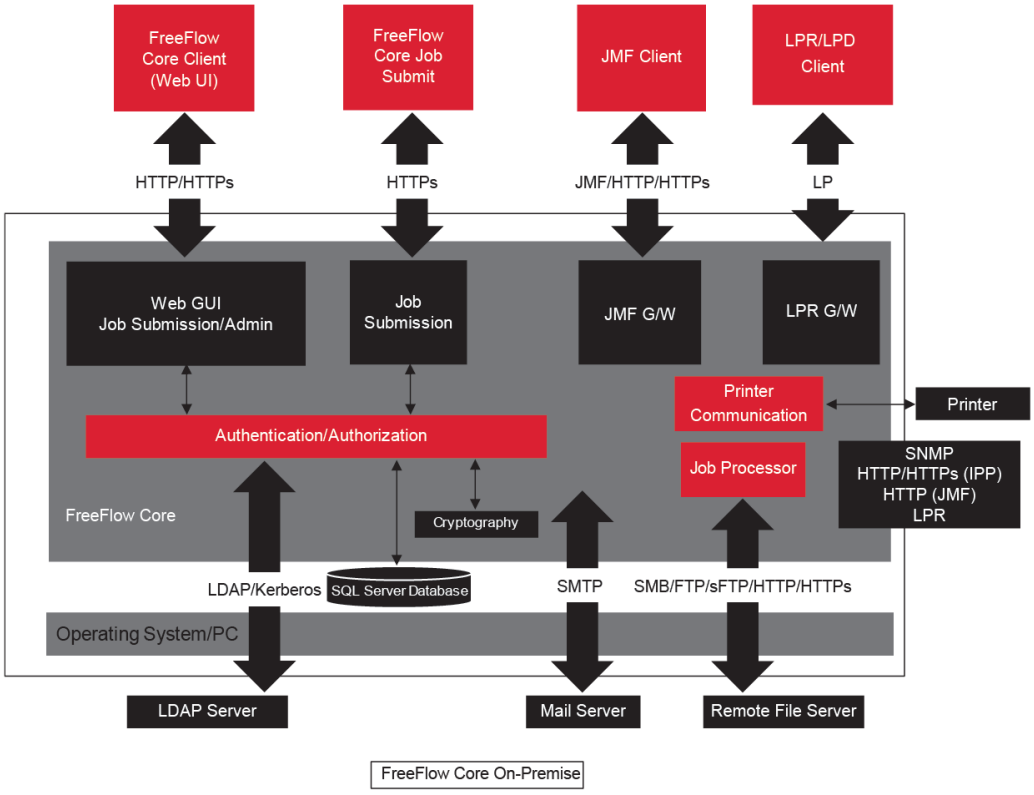
System Access

NETWORK CONNECTIONS

Xerox® FreeFlow® Core requires network connectivity for both job processing and user interactions. Refer to the security information for each network connection.

Note: To provide better security protection against vulnerability attacks, enable the Windows firewall on the server where FreeFlow Core is installed.

FreeFlow Core uses the following network protocol connections.



Xerox® FreeFlow® Core Client

A Web browser that is compatible with HTML5 and CSS3 is required to connect to FreeFlow Core. HTTPS connections are required to provide a secure download of the Xerox® FreeFlow® Core client, and secure communication between the client and Xerox® FreeFlow® Core.

- To enable HTTPS connections, add a Server Certificate to the Internet Information Services (IIS). Follow the instructions in the Windows documentation.
- If HTTPS connections are enabled, it is required to set the Require SSL setting on Microsoft Internet Information Service (IIS). From the Windows command prompt, run the batch file RequireSSL, which can be found in the directory named Support within the FreeFlow Core installation directory or at `C:\Program Files\Xerox\FreeFlow Core`.
- FreeFlow Core supports cryptographic protocols TLS.

Note: FreeFlow Core uses the operating system settings that support the TLS protocol. To ensure that the current versions of the cryptographic protocols are used, it is recommended that the operating system runs the latest updates.

- No customer data is exchanged between the client and the Xerox® FreeFlow® Core server unless users download job files.

Note: The client retrieves job properties that contain customer data.

Table 3.1 Firewall Configuration

PORT	PROTOCOL OR APPLICATION	FIREWALL CONNECTION TYPE
80	HTTP	Inbound Note: The port number depends on the IIS server configuration.
443	HTTPS	Inbound Note: The port number depends on the IIS server configuration.

User Roles

Xerox® FreeFlow® Core opens to a login screen.

- Users log in for access to the FreeFlow Core system.
- After 30 minutes of inactivity, logged-in users are logged off automatically.
- If authentication fails with the FreeFlow Core software, users are locked out of the application after three failed login attempts.

Note: For additional user account settings, refer to User Account Access and Job Retention. The FreeFlow Core Administrator configures the settings.

To assign users to User Roles, refer to the *Xerox® FreeFlow® Core Help*, *User Access Setup*.

Administrator Role

Administrators have access to the entire system:

- Job Management and Status tab functions: Submit Job Dialog and Job Status tabs.
- Printer Management and Status tabs

- Workflow Setup
- Administration tab functions:
  - Hot Folder
  - Notifications
  - User Access
  - Region
  - Security
  - Core Reports
  - Core Exchange
  - Queue Options
  - Core License
- Core Server Utilities available on the server desktop:
  - FreeFlow® Core Exchange
  - FreeFlow® Core Configure
  - FreeFlow® Core Reports for command line utility

Note: Only one administrator at a time can be logged in to Xerox® FreeFlow® Core.

Operator Role

Operators have access to the following:

- Job Management and Status tab functions: Submit Job Dialog and Job Status tabs
- Printer Management and Status tabs

Note: Multiple operators can be logged in at the same time to Xerox® FreeFlow® Core.

Job Status Monitor Role

The Job Status Monitor role has read-only access to the Job Status tab window.

Note: Multiple users who are assigned to the Job Status Monitor role can be logged in at the same time to Xerox® FreeFlow® Core.

User Authentication

Credentials entered into the Xerox® FreeFlow® Core browser client are not encrypted when using HTTP. For secure transmission, enable HTTPS and Require SSL at IIS for secure web browser access to Xerox® FreeFlow® Core.

- If authenticating users with Xerox® FreeFlow® Core, user information is unencrypted. Credentials are stored locally and encrypted.
- If authenticating users with Active Directory, credentials are unencrypted before they are submitted to Active Directory. When authenticated with Active Directory, credentials are not stored locally.

- You can configure Xerox® FreeFlow® Core authentication to use an existing Windows Active Directory. This configuration uses the current user desktop credentials as the login credentials for the Xerox® FreeFlow® Core client.

The Xerox® FreeFlow® Core configuration connection to Active Directory is encrypted for the operating system configuration.

Table 3.2 Firewall Configuration

PORT	PROTOCOL OR APPLICATION	FIREWALL CONNECTION TYPE
80	HTTP	Inbound Note: The port number depends on the IIS server configuration.
88	Kerberos	Outbound: User Authentication Note: Port numbers and services depend on the server AD configuration.
389636 3268 3269	LDAPLDAP TLS LDAP GC LDAP GC TLS	Outbound: Validates AD Groups during the AD authentication configuration Note: Port numbers and services depend on the server AD configuration.

SQL Server Connection

Xerox® FreeFlow® Core communicates with the SQL server using the Microsoft® Entity Framework. Encrypted communication between Xerox® FreeFlow® Core and the SQL server is enabled when the SQL server is configured to use encrypted connections.

Encrypted SQL server credentials are stored locally within the Xerox® FreeFlow® Core server.

To install software on a remote SQL server without SQLS Administrative privileges, create two empty databases in the SQLS Instance:

- `OapMasterDatabase`
- `OapPlatformDatabase`

PORT	PROTOCOL OR APPLICATION	FIREWALL CONNECTION TYPE
1433	SQLS	Inbound: Receives connections from Xerox® FreeFlow® Core Outbound: Communicates with the SQL server database print engine Note: The port number depends on the SQLS server configuration.
1434	SQLS Browser Service	Inbound: Receives connections from Xerox® FreeFlow® Core Outbound: Communicates with the SQL server database print engine Note: The server provides the client with the port number for connection.

Submit Job User Interface

The Submit Job User Interface (UI) uses the Xerox® FreeFlow® Core Client connection for job submission. For information, refer to Xerox® FreeFlow® Core Client.

Table 3.3 Firewall Configuration

PORT	PROTOCOL OR APPLICATION	FIREWALL CONNECTION TYPE
80	HTTP	Inbound Note: The port number depends on the IIS server configuration.
443	HTTPS	Inbound Note: The port number depends on the IIS server configuration.

Hot Folders

Use file shares for sharing a local hot folder and for accessing a hot folder in shared Windows folders. To encrypt Windows folders, use the Windows file system. To protect Windows folders, use the Windows user account access control.

Note: When you use the user account access control, use the same service account that you used in the *Optional Installation Procedures* configuration. For more information, refer to *Xerox® FreeFlow® Core Installation Guide*.

Table 3.4 Firewall Configuration

PORT	PROTOCOL OR APPLICATION	FIREWALL CONNECTION TYPE
139, 445	SMB	Inbound: Shares hot folders using Windows file sharing Outbound: Uses hot folders on shared directories
20, 21	FTP	Inbound: Shares hot folders using FTP

Manifest Processing

During the manifest submission, Xerox® FreeFlow® Core retrieves the files listed in the manifest. You can reference the files using mapped drives, UNC file paths, HTTP, HTTPS, FTP, or sFTP URIs.

Note: HTTP and FTP URIs do not support encryption.

Use file shares for sharing a local hot folder and for accessing a hot folder in shared Windows folders. To encrypt Windows folders, use the Windows file system. To protect Windows folders, use the Windows user account access control.

Note: When you use the user account access control, use the same service account that you used for the Optional Installation Procedures configuration. For the latest office conversion enablement instructions, refer to the *Xerox® FreeFlow® Core Release Notes*. To obtain the document, access the FreeFlow® Core webpage at https://xerox.com/automate. At the top of the page, click **Owner Resources**, then click **Release Notes** which includes full system requirements.

Table 3.5 Firewall Configuration

PORT	PROTOCOL OR APPLICATION	FIREWALL CONNECTION TYPE
139, 145	SMB	Outbound: Retrieves files listed in the manifest from Shared Directories
20, 21	FTP	Outbound: Retrieves files listed in the manifest
80	HTTP	Outbound: Retrieves files listed in the manifest
443	HTTPS	Outbound: Retrieves files using the HTTPS URL listed in the manifest
22	sFTP	Outbound: Retrieves files using the secure FTP listed in the manifest

Line Printer Daemon (LPD)

Note: Line Printer (LP) commands do not support secure connections.

Table 3.6 Firewall Configuration

PORT	PROTOCOL OR APPLICATION	FIREWALL CONNECTION TYPE
515	LP	Inbound: Receives Line Printer Remote (LPR) requests and LP commands
721 to 731	LPR	Outbound: Sends LPR requests to a printer that supports LPD.

JMF Commands and Printer Status Signals

Job Messaging Format (JMF) commands and signals to a JMF client support secure connections. JMF file retrieval supports HTTPS connections.

Note: For secure JMF submissions, submit a MIME package with the JMF, JDF, and PDF files.

To enable HTTPS communication for JMF commands:

1. To add a certificate to the Java keystore, in the Xerox® FreeFlow® Core installation directory, use the `installJMFCertificate.bat` utility.
2. Restart the Xerox® FreeFlow® Core JMF Server service.
3. To test the installation, access `http://<hostname>:7759/FreeFlowCore`. If secure JMF is configured correctly, the browser displays an `HTTP Status 404` error page.

Table 3.7 Firewall Configuration

PORT	PROTOCOL OR APPLICATION	FIREWALL CONNECTION TYPE
7751	JMF	Inbound: Receives JMF commands
Varies	JMF	Outbound: Returns JMF printer status signals Note: The client that requests the JMF printer status signals or the Return JMF signal defines the required port number.
7759	sJMF	Inbound: Receives secure JMF commands

Workflow Nodes

Workflow components that retrieve or save job files can use mapped drives, UNC file paths, HTTP, HTTPS, or FTP URIs. sFTP URI supports the job file retrieval such as MAX, JMF.

Note: HTTP and FTP URIs do not support encryption.

To encrypt file shares for sharing, use the Windows file system. To protect file shares, use the Windows user account access control.

Note: When you use the user account access control, use the same service account that you used in the *Optional Installation Procedures* configuration. For more information, refer to *Xerox® FreeFlow® Core Installation Guide*.

Table 3.8 Firewall Configuration

PORT	PROTOCOL OR APPLICATION	FIREWALL CONNECTION TYPE
139, 445	SMB	Inbound: Retrieves files specified in a workflow component preset Outbound: Saves files to shared directories
20, 21	FTP	Outbound: Retrieves files specified in a workflow component preset
80	HTTP	Outbound: Retrieves files specified in a workflow component preset
443	HTTPS	Outbound: Retrieves files specified in a workflow component preset

Xerox® FreeFlow® Core Printing

Xerox® FreeFlow® Core uses SNMP and HTTP with the IPP, JMF, or XBDS commands to determine the Digital Front End (DFE) type, using an unencrypted connection. The SNMP public community string on the printer or the DFE requires the default setting. If the SNMP public community string on the printer or the DFE was modified from the default setting, ensure that the updated setting is registered with FreeFlow Core. Ensure that all printers registered with FreeFlow Core have the same SNMP public community string. For instructions on how to update the SNMP public community string, refer to the Xerox FreeFlow Core Release Notes.

The following operations use an unencrypted connection:

- Retrieve the list of the DFE queues.
- Retrieve the list of Virtual Printers on the EFI DFE.
- Retrieve printer capabilities.
- Job operations at the DFE.
- Retrieve job accounting information. This operation is not applicable for JMF.
- Submission of a print job to a printer using LPR.

When connected to a DFE that is configured to support secure IPP, the print submission is encrypted. To enable secure IPP, use the Secure Printing option in the Printer Destination setup. TLS and SHA256 encryption is used between FreeFlow Core and the DFE.

Enabling a Secure IPP Print Submission to FreeFlow Print Server

To enable secure IPP print submission to FreeFlow Print Server, do the following:

1. Add a TLS certificate to the FreeFlow Print Server.
2. Select **Enable TLS** in the Xerox® FreeFlow® Print Server setup.
3. To retrieve the TLS certificate from the FreeFlow Print Server, use the Xerox® FreeFlow® Core Certificate.

Note: After successful secure IPP configuration, `Certificate installed successfully` message appears.

Enabling a Secure IPP Print Submission to Fiery

To enable secure IPP print submission to Fiery, do the following:

1. To launch Fiery UI, enter Fiery IP address in any of the web browser.
2. Select **Fiery Configure** in the left pane.
3. Login with Fiery controller credentials.
4. Select **Security**, then create self-signed certificate or fill details with certificates from CA.
5. Enable **SSL\TLS** in configure UI screen.
6. When SSL\TLS is enabled, a confirmation message appears to restart the controller.
7. Select **Yes**.
8. Launch **Core Configure Windows Utility** in Xerox® FreeFlow® Core.
9. Select **Core Certificate** tab, provide Fiery Controller IP address, and select **Retrieve Certificate**.

   `Certificate Installed Successfully` message appears.
10. Configure printer in Xerox® FreeFlow® Core with secure print option in Printer Management screen.

Xerox® FreeFlow® Core does not support communication to the DFE using secure JMF.

Table 3.9 Firewall Configuration

PORT	PROTOCOL OR APPLICATION	FIREWALL CONNECTION TYPE
161, 162	SNMP v1/v2	Outbound: Identifies the DFE type during a Printer Destination setup and Certificate Retrieval
80	HTTP	Inbound: JDF printer retrieves print file using HTTP. Outbound: Identifies the DFE type during a Printer Destination setup and Certificate Retrieval
N/A	ICMP	Outbound: Verifies device availability before Certificate Retrieval
631	IPP v1.0/v1.1	Outbound: Submits jobs to DFEs, gets job status, and submits job commands to the DFE
4004	JMF	Inbound: Receives the JMF `ReturnQueueEntry` message from the printer
8010 or printer defined JMF port	JMF v1.3/v1.4	Outbound: Identifies the DFE type during Printer Registration, and submits a job to the DFE.
443	HTTPS	Outbound: Printer communication to the DFE
515, 721 to 731	LPR	Outbound: Sends LPR requests to a printer that supports LPD

Email Notification

Xerox® FreeFlow® Core is an email client that connects to an accessible SMTP email server or a Google email server. You can encrypt email notifications, then connect to a mail server that supports encryption. TLS enables encryption of communications between the notification service and the SMTP server.

Encrypted credentials are stored locally.

Table 3.10 Firewall Configuration

PORT	PROTOCOL OR APPLICATION	FIREWALL CONNECTION TYPE
25, 465, 587	SMTP	Outbound: Sends email notifications Note: The required port number and use of secure connection depend on the SMTP server configuration.

FIPS and GDPR Compliance

Xerox® FreeFlow® Core runs on a Windows Operating System enabled for FIPS 140-2 compliance. To enable the FIPS-compliance, refer to the Microsoft documentation. By default, FreeFlow Core runs in FIPS-compliant mode.

FreeFlow Core disables support for DES/3DES ciphers.

If secure IPP Printing with Digest Authentication is required, disable the FIPS-compliant mode, then FreeFlow Core becomes non-compliant with cryptographic requirements.

FreeFlow Core is compliant with the EU General Data Protection Regulation (GDPR).

General Security Protection

SERVICE ACCOUNT, UTILITIES, AND COMMAND LINE INTERFACE (CLI) AUTHENTICATION

FreeFlow Core's service accounts, Utilities, and CLI now use Windows authentication. This is accomplished by adding the service account or currently logged on user account to a local Windows group named FreeFlow Core Security. For additional information, refer to the *Xerox FreeFlow Core Release Notes*.

USER DATA PROTECTION

Document and File Security

FreeFlow Core does not explicitly encrypt files submitted for processing before the file is stored in the file system of the personal computer.

Document source content contains Personally Identifiable Information (PII) or other sensitive content. Therefore, it is the responsibility of the user to handle the digital information in accordance with information protection best practices.

Personal Identifiable Information (PII)

When you register for a FreeFlow Core software license, PII information is collected. The information contains the following:

- Company Name
- Activation Key and Serial Number
- Host ID/System UUID
- User Name
- Address (Street, City, State, Zip Code, Country)
- Email address (optional)

This information is transmitted securely to the Xerox licensing host.

PII information, specifically the email address of the user that is used for password recovery, is stored on the FreeFlow Core system. The information is encrypted.

User Account Access and Job Retention

USER ACCOUNT PASSWORDS

Reuse of a password is allowed up to 10 times. The number of times a password can be reused is configurable.

USER ACCOUNT LOCKOUT

If authentication fails using Xerox FreeFlow Core Client, users are locked out after three failed login attempts for a lockout period of 30 minutes. The number of failed login attempts and the lockout period are configurable.

USER ACCOUNT LOG OUT

After 30 minutes of inactivity, users that are logged in to Xerox® FreeFlow® Core Client are logged out automatically. The duration of the inactivity period is configurable.

USER ACCOUNT ACTIVITY

The audit log of user login transactions to FreeFlow Core is located in the Windows Event Viewer, in the **Application** section of the **Windows Logs** folder.

JOB RETENTION

After a job completes processing, the retention period for the jobs in FreeFlow Core is 24 hours.

The FreeFlow Core printer is configured to change the retention period before completed jobs are removed automatically. After 24 hours, the FreeFlow Core device removes completed jobs.

To remove jobs manually, use the FreeFlow Core Web GUI.

JOB PROPERTIES

Enables restriction of downloading files found in Job Properties for a job displayed in FreeFlow Core Job Management and Status.

User Account Rights

To configure the Xerox® FreeFlow® Core service account, you can use either a local administrator account or a non-administrator account. When you use an account that is a member of the local administrator group, no special actions are required.

When you use a non-administrator account, additional rights are required, in addition to standard user group rights. FreeFlow® Core Configure adds additional rights automatically, as listed in the following table:

GROUP POLICY SETTING	CONSTANT NAME
Act as part of the operating system	SeTcbPrivilege
Adjust memory quotas for a process	SeIncreaseQuotaPrivilege
Allow log on locally	SeInteractiveLogonRight
Backup Files and Directories	SeBackupPrivilege
Create a token object	SeCreateTokenPrivilege
Create global objects	SeCreateGlobalPrivilege
Create permanent shared objects	SeCreatePermanentPrivilege
Debug Programs	SeDebugPrivilege
Load and unload device drivers	SeLoadDriverPrivilege
Log on as a batch job	SeBatchLogonRight
Log on as a service	SeServiceLogonRight
Manage auditing and security log	SeSecurityPrivilege
Perform volume maintenance tasks	SeManageVolumePrivilege
Profile single process	SeProfileSingleProcessPrivilege
Profile system performance	SeSystemProfilePrivilege
Replace a process level token	SeAssignPrimaryTokenPrivilege

Note: The rights listed in the table are defined at https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-rights-assignment.

Security

This chapter contains:

At Xerox, security issues are front and center. As a leader in the development of digital technology, Xerox demonstrates a commitment to keep the digital information safe and secure, identify the potential vulnerabilities, and address the issues proactively to limit risks.

Xerox strives to provide the most secure software devices possible, based on the information and technologies available, while maintaining device performance, value, functionality, and productivity.

The components of Xerox® FreeFlow® Core are assessed for security compliance using commercially available vulnerability and penetration scanning tools. Application vulnerabilities are addressed based on results of Xerox scans.

Xerox distributes security bulletins when required. Security bulletin information is communicated on the Xerox Security website at https://www.xerox.com/security for Product Security Guidance. The website contains up-to-date security vulnerability printer status, white papers, Common Criteria Certification, Intel Security McAfee Information, and a portal to submit security questions to Xerox.

Virus Protection

Xerox takes special precautions to ensure that Xerox software is shipped free from computer virus contamination. Xerox recommends that Anti-Virus Detection and EndPoint Intrusion Detection and Prevention are installed on the FreeFlow Core Server. This software and the operating system are kept up-to-date with the latest security patches as advised by the respective vendors.

To improve performance, it is recommended that you exclude the Xerox® FreeFlow® Core and SQL Server installation directories from antivirus scans.

You can exclude the following files from the antivirus scans:

- `<FreeFlow Core Installation directory>\Logs`
- `<FreeFlow Core Installation directory>\Platform\Logs`
- `<FreeFlow Core Installation directory>\JobSubmit\Logs`
- `<FreeFlow Core Installation directory>\Config`
- `<FreeFlow Core Installation directory>\Platform\Config`
- `<FreeFlow Core User Data Directory>\`
- Folders outside the FreeFlow Core User Data directory that are used by FreeFlow Core

Software Update

Xerox is not responsible for the state of the operating system that runs Xerox® FreeFlow® Core. It is the responsibility of the customer to keep the system up-to-date and ensure that it is patched and configured properly. Perform a Microsoft® Windows® update at least once a month.

When you perform the Windows updates, to apply the update, use the **Windows Update** option. It is recommended not to install optional preview updates, because they can affect the reliability of the Xerox® FreeFlow® Core server.

You can find software updates for FreeFlow Core at https://www.support.xerox.com/support/core/software/enus.html. Customers can install the software update.

Additional Information and Resources

Security @ Xerox

Xerox maintains an up-to-date public webpage that contains the latest security information that pertains to its products. Refer to www.xerox.com/security.

Responses to Known Vulnerabilities

Xerox has created a document that details the Xerox Vulnerability Management and Disclosure Policy that is used in the discovery and remediation of vulnerabilities in Xerox software and hardware. You can download this document from this page: https://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html.

Additional Resources

SECURITY RESOURCE	URL
Frequently Asked Security Questions	www.xerox.com/en-us/information-security/frequently-asked-questions
Bulletins, Advisories, and Security Updates	www.xerox.com/security
Security News Archive	security.business.xerox.com/en-us/news/
Xerox Trust Center	https://trust.corp.xerox.com/