Fiery FS700 Pro/FS700 servers

Security White Paper

45266125

25 November 2025

Contents

Introduction

This document provides an overview of security features in Fiery servers. It aims to inform IT administrators and security professionals about how Fiery solutions secure print environments. The document explains the principles and mechanisms used in Fiery servers to protect data, enhance network security, and maintain system integrity.

Security Principles

Fiery servers are meticulously designed to adhere to industry best practices, ensuring compliance with data protection regulations and enterprise security requirements. The fundamental principles underpinning this design are as follows:

- Data Protection: Encryption of data at-rest and data in-transit
- Network Security: Controlled access, secure communication protocols, and authentication mechanisms
- System Integrity: Firmware verification, secure boot, and security updates

In collaboration with our global partners and suppliers, we provide continuous support to our customers as threats evolve. To ensure comprehensive system security, we recommend that end users integrate Fiery security features with their own organization's security policies and adhere to industry best practices, including the implementation of secure passwords and robust physical security measures.

Authentication and Access Control

Fiery servers support multiple authentication methods, including:

- Role-Based Access Control (RBAC)
- LDAP/Active Directory Integration
- Multi-Factor Authentication (MFA) implemented using Single Sign-On (SSO)

User authentication

The authentication feature enables the Fiery server to perform the following functions:

- Authenticate a user
- Authorize actions based on the user's privileges

The Fiery server supports three user authentication methods:

- Local Authentication for users defined on the Fiery server
- Single Factor Authentication (SFA) via external network authentication servers using LDAP (e.g. Microsoft Active Directory)
- Multi-Factor Authentication (MFA) using Single Sign-on (SSO)

Regardless of the method used, the administrator accounts always require authentication. This cannot be disabled.

Group privileges

The Fiery server authorizes user actions contingent upon their group membership. Each group is associated with a specific set of privileges, such as printing in color or grayscale. The actions of group members are restricted to these privileges. The Fiery Administrator holds the authority to modify the privileges of any Fiery group, with the exception of the Administrator and Operator accounts.

In this user authentication method, the diverse privileges that can be selected for a group are as follows:

- Print in grayscale: allows group members to print jobs in grayscale. If the user does not have this privilege, the Fiery server will not print the job. If the job is a color job, it will be printed in grayscale.
- Print in color and grayscale: allows group members to print jobs with full access to the color and grayscale printing capabilities of the Fiery server. Without this or the print in grayscale privilege, the print job fails to print, and users are not able to submit a job via FTP (color devices only).
- Fiery mailbox: allows group members to have individual mailboxes. The Fiery server creates a mailbox based on the username with a mailbox privilege. Access to this mailbox is limited to users with the mailbox username and password.
- Calibration: This privilege allows group members to perform color calibration.

- Create server presets: allows group members to create server presets. Group members have access to these server presets.
- Manage workflows: This privilege allows group members to create, publish, or edit virtual printers.
- Edit jobs (Fiery XB servers only): This privilege allows group members to edit a job in the queue.

Administrators with elevated privileges can customize these features to restrict unauthorized access and enforce organizational security protocols.

Local Users

The Fiery server software interacts with unique user types, distinct from Windows users or roles. Fiery Administrators should promptly modify all default passwords after initial installation. Password access to the Fiery server must be strictly enforced.

- Maximum password length for "Administrator" and "Operator" is 64 characters when using **Configure** > **Security**.
- Maximum password length for local user accounts is 64 characters when using **Configure** > **User Accounts**.
- Administrator and Operator passwords can be changed in **Configure** > **User Accounts**.

Local Fiery user accounts and access privileges

- Administrator: Full control over Fiery server functionality, can modify Fiery group privileges except for Administrator and Operator accounts.
- Operator: Same privileges as Administrator but lacks access to server setup and job log deletion.
- Press Operator (Fiery XB servers only): Manages jobs on the press, with specific privileges added by Administrator.
- Fiery service admin (Windows servers only): A hidden Admin account for installing the trusted certificate, can't log into the Fiery server, appears on network scanning tools, and can be removed.
- Fiery_SMB_User: Default Windows printing (SMB) account that provides visibility into Fiery Server print queues through the Network Neighborhood.
- Guest (default, no password): Same privileges as Operator but can't access job logs, make edits, status changes, or preview jobs.

LDAP Authentication

The Fiery server uses LDAP version 3 (RFC 2251 compliant) to communicate with corporate servers. Through LDAPv3, it retrieves user email addresses for scanning features, as well as user and group information for authentication. This functionality is supported exclusively for LDAP connections to Active Directory servers.

The Fiery server supports the following methods of authentication using LDAP:

- Automatic
- SIMPLE
- GSSAPI

The following table describes the different LDAP authentication methods:

Authentication Method	Description	Active Directory Server
Automatic	This option selects GSSAPI or SIMPLE based on the authentication method supported by the LDAP server.	Supported
SIMPLE	Password is required. If LDAP over TLS is selected, the password is encrypted using TLS.	Supported
GSSAPI	This method uses Kerberos tickets instead of passwords, eliminating the need for TLS.	Supported

Single Sign-On (SSO)

Fiery FS700 Pro servers support the OpenID Connect protocol for cloud-based, Single Sign-On (SSO) user authentication with Microsoft Entra ID (formerly called Azure AD). Users can login to a Fiery server using their existing Entra ID credentials.

This authentication method supports Multi-Factor Authentication (MFA).

This identity management approach ensures that Fiery servers never store user passwords locally, significantly enhancing security.

Data Security Measures

To protect sensitive information, Fiery servers implement:

Encrypted Storage: Protects print jobs and configuration data

Encryption of critical customer data ensures the secure storage of passwords and related configuration information on the Fiery server. This critical information is either encrypted or hashed using cryptographic algorithms such as AES-256 and SHA-2, which adhere to the latest security standards.

Customer data stored on the disk remains inaccessible even if the disk is removed from the Fiery server. User data encryption can be enabled or disabled on Windows-based Fiery servers. For Linux-based Fiery servers, the encryption feature is always enabled.

In the event of a forgotten passphrase used for data recovery, FIERY cannot reset it, necessitating a complete software reinstall.

Windows-based servers also provide an option to encrypt the boot drive, which contains the operating system. This encryption helps prevent offline attacks on the Fiery server and ensures the boot drive cannot be used on another device.

Secure Erase: Ensures data is irrecoverable after deletion

For Linux-based FS700 Fiery servers, when a job is deleted, each job source file is overwritten three times using an algorithm based on the US DoD 5220.22-M data wipe method.

This feature is not supported on embedded Fiery servers using E600 and LX Pro hardware platforms. These platforms store document data on a Solid-State Drive (SSD), which is protected with AES-256 encryption. This encryption is always enabled and cannot be disabled.

Windows-based FS700 Pro servers support the NIST 800-88 data sanitation standard. Fiery Administrators can configure this option for 1-pass or 3-pass image overwrite methods.

Note: The secure erase feature is not supported on Fiery XB platforms or for user data stored on SSDs.

Workflows	Secure erase
Jobs stored on the Fiery server hard disk drive; Secure Erase set to **On**	Yes
Jobs stored on the Fiery server hard disk drive; Secure Erase set to **Off**	No
Jobs received by the Fiery server and deleted after Secure Erase set to **On**	Yes
Jobs received by the Fiery server and deleted before Secure Erase set to **On**	No
Copies of jobs sent to another Fiery server (load balancing)	No

Workflows	Secure erase
Jobs archived to removable media	No
Jobs archived to network drives	No
Jobs located on client devices	No
Clear server execution	Yes
Pages merged or copied into another job (for example, Fiery Impose jobs or combined PDFs)	No
Jobs received from SMB connection and saved to the Fiery server hard disk drive	No
Portions of a job written to the Fiery server hard disk drive during disk swapping or disk caching operations	No
Job Log entries	No
Job Log entries after Clear server execution	Yes
Fiery server powered off before job deletion is completed	No
Defragmenting the Fiery server hard disk drive before deleting a job	No

Network security

Fiery servers employ the following security mechanisms to safeguard network communications:

- IP Filtering & Port Management
- Firewall Configuration
- Support for SNMP v3 for secure network monitoring and management tools

Supported Network Protocols

FS700/FS700 Pro supports a wide range of industry-standard network protocols to ensure compatibility, security, and efficient communication across diverse environments. These include:

- **Core Protocols:** TCP/IP, IPv4, IPv6
- **Web Protocols:** HTTP/1.1, HTTPS (TLS 1.2/1.3)
- **File & Print Services:** FTP, LPR, IPP 2.0, SMB v2, SMB v3, Port 9100
- **Management & Monitoring:** SNMP v1, v2c and v3
- **Remote Access:** RDP (Windows-based servers only)
- **Security & Authentication:** IPSec (IKEv2), LDAP v3, IEEE 802.1X
- **Network Services:** DHCP, DNS
- **Discovery Protocols:** WSD, Bonjour, SLP

Network ports

By default, all unused TCP/IP ports are disabled. The Fiery Administrator can enable and disable network ports. Disabling a port effectively prevents external connections that necessitate the utilization of that specific port.

Inbounds Ports

Fiery servers oversee and monitor incoming network connections, enabling only authorized traffic to access the server and safeguarding it against unauthorized access or attacks.

TCP	UDP	Port name	Dependent services
20-21		FTP	FTP
80		HTTP	WebTools, IPP

TCP	UDP	Port name	Dependent services
135		MS RPC	Microsoft® RPC Service. An additional port in the range 49152-65535 will be opened to provide SMB-related point and print service.
137-139		NETBIOS	Windows Printing. These ports are closed by default because of NetBIOS is insecure.
	161, 162	SNMP	SNMP-based tools
	427	SLP	Service Location Protocol. This is port is bloacked by default because SLP is insecure.
443		HTTPS	WebTools, IPP/s
445		SMB/IP	SMB over TCP/IP
	500	ISAKMP	IPsec
515		LPD	LPR printing
631		IPP	IPP
3389		RDP	Remote Desktop (Windows-based Fiery servers only)
3702	3702	WS-Discovery	Web Services for Devices (WSD). Enables discovery and printing to the Fiery server over WSD.
	4500	IPsec NAT traversal	IPsec
	5353	Multicase DNS (mDNS)	Bonjour
6310		DMP port	Direct Mobile Printing
8010		FIERY ports	JDF
8021-8022		FIERY ports	Fiery Harmony, Fiery HotFolders, and Fiery Command WorkStation
8090		FIERY ports	OFA
9100-9103		Printing port	Port 9100
	9906	FIERY ports	Harmony discovery
21030		FIERY ports	Fiery Image Viewer

Note: The IPSec ports (500 and 4500) are only configurable for FS700 (Linux-based Fiery servers).

Other TCP ports, except those specified by the Fiery partner, are disabled. Any service dependent on a disabled port cannot be accessed remotely.

The Fiery Administrator can also enable or disable the various dependent services provided by the Fiery server.

Outbounds Ports

Fiery servers manage and restrict outbound network traffic to ensure that only authorized communications leave the device, reducing exposure to external threats.

Outbound ports	Purpose	Default/On configuration
53	DNS	Default
67	DHCP	Default
80, 443	Fiery System updates, JDF, PrintMe and other cloud communications	Default
161, 162	SNMP	In dual IP configuration
21	Scan to FTP	On configuration
123	NTP	On configuration
389/636	LDAP services	On configuration
445	Scan to SMB/JobLog to SMB/JDF Common global path	On configuration
500/4500	IPSEC	On configuration
8080/8443	HTTP/HTTPS/FTP Proxy port	On configuration

Communication with Cloud Services

This list enumerates Fiery services and applications that require communication with external cloud-based services; for example, to download Fiery Security Updates or for License Activation. This documentation is particularly useful for customers who have disabled all external communications and are attempting to make exceptions within their corporate firewall.

Fiery Service/ Application	Fully Qualified Domain Name	Port	Server Location	Usage information
System Update	https://liveupdate.fiery.com/des/hypatia.asmx	443	Fiery	Download Fiery Security Updates
OFA	https://flexlicensing.fiery.com	443	Fiery	License activation
IQ	https://iq.fiery.com/iq	443	AWS	Fiery IQ Cloud
LINQ	https://ews.fiery.com	443	Azure	Analytics

Fiery Service/ Application	Fully Qualified Domain Name	Port	Server Location	Usage information
Universal Print	Multiple domains: •portal.azure.com •print.print.microsoft.com •notification.print.microsoft.com •discovery.print.microsoft.com •graph.print.microsoft.com	80/443	Azure	IPP Proxy and Universal Print service
SSO	login.microsoft.com	80/443	Microsoft	Single Sign-On
Windows Server Update Services (WSUS)	Multiple domains: •http://windowsupdate.microsoft.com •http://.windowsupdate.microsoft.com •https://.windowsupdate.microsoft.com •http://.update.microsoft.com •https://.update.microsoft.com •http://.windowsupdate.com •http://download.windowsupdate.com •https://download.microsoft.com •http://.download.windowsupdate.com •http://wustat.windows.com •http://ntservicepack.microsoft.com •http://go.microsoft.com •http://dl.delivery.mp.microsoft.com •https://dl.delivery.mp.microsoft.com •http://.delivery.mp.microsoft.com •https://.delivery.mp.microsoft.com	80/443	Microsoft	Windows updates
Command WorkStation	Multiple domains: • https://help.fiery.com •https://learning.fiery.com •https://communities.fiery.com/s/ •https://liveupdate.fiery.com •https://iq.fiery.com	443	Fiery	

IP Filtering

IP filtering enables the Administrator to control connection requests to the Fiery server based on predefined IP addresses. By defining default policies, the Administrator can specify whether incoming data packets should be allowed or denied. Additionally, they can create filters for a maximum of 16 IP addresses or ranges, allowing or denying connection requests accordingly.

Each IP filter setting specifies either an IP address or a range of IP addresses and the corresponding action. When the action is Deny, packets with a source address belonging to the specified addresses are dropped. Conversely, when the action is Accept, packets are allowed.

Network authentication

SNMP v3

The Fiery server supports the latest SNMPv3 standard, facilitating encrypted communication packets to guarantee confidentiality, message integrity, and authentication.

The Fiery Administrator can select from three SNMP security levels: Minimum, Medium, and Maximum. At these levels, passwords are hashed using algorithms such as SHA-1 or SHA-256, and the entire SNMP message is encrypted. Additionally, the local Administrator can configure SNMP Read and Write community names along with other security settings.

IEEE 802.1x

802.1X is an IEEE standard for port-based network access control that ensures devices authenticate before accessing the local network and its resources. On Fiery servers, 802.1X can be configured to use EAP-MD5 Challenge or PEAP-MSCHAPv2 for server-based authentication, or EAP-TLS for certificate-based authentication for enhanced security. Fiery servers only support the user certificate (not the device certificate) for EAP-TLS certificate-based authentication.

The Fiery server performs authentication during startup or whenever the network connection is disconnected and reconnected.

Network encryption

Internet Protocol Security (IPsec)

IPsec enhances the security of IP-based communications by encrypting and authenticating each packet at the network layer, thereby protecting data in transit across all applications that use IP. The Fiery server employs pre-shared key authentication to establish secure connections with other systems via IPsec. Once the communication over IPsec is established between a client computer and a Fiery server, all communications, including print jobs, are securely transmitted over the network.

HTTPS

Fiery servers enforce secure communications between clients and server components using HTTPS over TLS. This ensures that all data transmitted—such as print jobs, job status updates, and administrative commands—is encrypted in transit, protecting it from interception or tampering. Fiery servers support TLS 1.3 and TLS 1.2, providing strong cryptographic protection and modern security features. HTTPS is mandatory for connections to WebTools and Fiery APIs, ensuring that administrative and operational traffic is transmitted securely.

Certificate management

Fiery servers offer an interface for managing certificates utilized during TLS communications. Fiery servers support X.509 certificates in PEM format, encoded in Base64, using RSA keys with lengths of 4096, 3072, or 2048 bits.

Certificate management enables the Fiery Administrator to perform the following actions:

- Generate self-signed digital certificates.
- Add a certificate and its associated private key for the Fiery server.
- Add, browse, view, and remove certificates from a trusted certificate authority.

Self-signed digital certificates provide encryption but do not offer automatic trust validation. For secure deployments, we recommend using certificates issued by a trusted Certificate Authority (CA) to ensure proper identity verification.

Once a certificate has been signed by a trusted CA, it can be uploaded to the Fiery server in the Configure section of WebTools.

Server Message Block (SMB)

SMBv1, the legacy protocol for file and printer sharing, is disabled on Fiery servers due to known security vulnerabilities. Fiery servers support SMBv2 and SMBv3 instead. SMB Signing is enforced, ensuring all packets are digitally signed to prevent man-in-the-middle attacks. When SMB authentication is enabled, users must provide a valid username and password to access shared folders and content. Printing or file sharing via SMB for a guest account can also be restricted by setting a password in Fiery Configure.

Hardware Security

Fiery servers are designed with enterprise-grade hardware security in mind. Protecting sensitive information is not limited to software controls; hardware components play a critical role in maintaining system integrity and data confidentiality. The key hardware elements and their security measures are outlined below.

Volatile Memory (RAM)

Fiery servers utilize volatile memory (RAM) to temporarily store data during active operations. To mitigate the risk of data exposure:

- Sensitive information in RAM is cleared immediately after use or upon system shutdown.
- Memory scrubbing techniques are applied to prevent residual data from persisting.
- Access to RAM is restricted through processor and operating system-enforced privilege separation.

Non-Volatile Memory and Data Storage

Non-volatile memory, including hard drives, solid-state drives (SSDs), and other persistent storage, retains data even when the system is powered off. Security measures include:

- User Data Encryption (UDE) to protect stored data.
- Secure deletion methods for rendering sensitive information irrecoverable when files are removed.

Flash memory

Flash memory is used for storing firmware, configuration files, and system settings. To maintain its security:

- Firmware is digitally signed to prevent tampering.
- Firmware updates are verified via cryptographic checksums before installation.
- Write-protection mechanisms prevent unauthorized modifications during runtime.

CMOS and NVRAM

Critical system parameters, such as hardware configurations and boot settings, are stored in CMOS and Non-Volatile RAM (NVRAM). To secure this data:

- Access is restricted to authorized administrative processes.
- Secure boot mechanisms ensure only trusted firmware reads and writes to these areas.
- Critical NVRAM variables are backed up and integrity-checked to prevent corruption or malicious alteration.

Storage Drives

Fiery servers use storage drives to store the operating system and system files. These drives are also used for job spooling, logs, and temporary files.

The following security features are provided to safeguard customer data:

- Drive-level encryption.
- Access control lists (ACLs) to restrict unauthorized read/write operations.
- Disk Drive Security Kits (optional for external Fiery servers) that enhance system security by allowing users to securely lock server drives during normal operation.

Physical Ports

Physical ports, such as USB, network interfaces, and service connectors, are potential vectors for unauthorized access. Fiery hardware security addresses this risk by:

- Disabling unused ports at the hardware or firmware level.
- Requiring administrative authorization for connecting external devices.
- Monitoring and logging all interactions with critical physical interfaces.

By integrating these hardware security measures with software and network protections, Fiery servers provide a comprehensive defense-in-depth strategy, ensuring the confidentiality, integrity, and availability of sensitive data in print environments.

System Integrity and Secure Updates

Maintaining system integrity is paramount to ensuring security. Fiery servers provide the following support:

- Security Audit Logs
- Secure Boot: Ensures that only trusted software is loaded.
- Digitally Signed Updates: Prevents tampering with software updates.
- Automated Security Updates Management: Simplifies the process of applying security updates.

Security Audit Log

Administrators with elevated privileges can access and scrutinize security events recorded in the Security Audit Log. This log is enabled by default.

Each security event is categorized as Information, Warning, or Error. The administrator receives no alerts or notifications; instead, they are presented with a static log.

The logs are formatted for compatibility with Security Information and Event Management (SIEM) tools commonly used for log collection and analysis. All captured event data complies with the standards outlined in NIST SP 800-53.

The Fiery Administrator can access the security audit log without the need for FIERY intervention. Logs for Linux-based servers are provided in Syslog Format (RFC 5424 or RFC 3164). For Windows-based servers, logs are saved in the standard Windows EVTX format and can be read from Windows Event Log Manager and many available commercial solutions that use the Windows Event Log API. Linux-based Fiery servers offer the option to forward logs to a centralized collection system such as Syslog.

Security logs are retained based on the allocated local storage capacity. When the log size exceeds the predefined storage limit (400MB), older events are automatically removed.

Secure Boot

This feature ensures the integrity of operating system files during startup by allowing only digitally signed and trusted components to load. On Fiery servers, it blocks unauthorized or malicious code from running during boot, enhancing security and reducing the risk of compromise. By default, Secure Boot is disabled.

Digitally Signed Updates

Fiery servers use digitally signed updates to ensure the integrity and authenticity of all software and firmware installations. Each update is cryptographically signed by Fiery or its authorized partners, allowing the server to verify that the content has not been altered or tampered with. This process protects against the introduction of malicious code and guarantees that only trusted updates are applied, maintaining system security and reliability.

Automated Security Updates Management

Timely software updates are critical for optimal operation of Fiery servers. Installing all security updates is important to keep Fiery servers secure in any given print environment.

Fiery System Update downloads and installs security updates if the option is enabled on the Fiery server. By default, this option is enabled, and we recommend customers leave it enabled.

Microsoft® Windows™ OS security vulnerabilities are not detailed in this document, as they are managed directly by Microsoft and distributed to customers via **Windows updates** as they become available.

To address security concerns and vulnerabilities that could impact the core Fiery hardware components, including the motherboard, processor, and firmware, FIERY collaborates closely with manufacturers to obtain the requisite security updates. These security updates are subsequently provided to customers as necessary.

Note: Fiery software updates are digitally signed using Secure Hash Algorithm (SHA-2) to prevent unauthorized modification, including insertion of malware.

Fiery Server Software Security Updates

Timely software updates are vital for optimal Fiery server operation. By applying the latest Fiery Server software security updates, system integrity is ensured, vulnerabilities are mitigated, and compliance with industry security standards is maintained.

The Fiery server security team diligently monitors and tracks security vulnerabilities through a comprehensive network of trusted and reliable sources, such as:

- US Cybersecurity and Infrastructure Security Agency (CISA) Alerts & Advisories
- US National Institute for Standards and Technology (NIST) National Vulnerability Database
- Common Vulnerabilities and Exposures (CVE) records
- CERT Coordination Center (CERT/CC) reports and advisories on software and hardware vulnerabilities
- Regional Government and Regulatory Agencies
- Software and hardware vendors' security advisories

Fiery prioritizes security fixes based on severity (Critical, High, Medium, and Low) as determined by the Common Vulnerability Scoring System (CVSS). These fixes are released after obtaining the corresponding approval from the Original Equipment Manufacturer (OEM) partner. Upon approval, Fiery software security updates are made available for download. All Fiery software updates are digitally signed using the Secure Hash Algorithm (SHA-2) to prevent unauthorized modification, including the insertion of malware.

When enabled, Fiery System Update downloads and installs security updates automatically on the Fiery server. By default, this option is enabled, and we strongly recommend that customers maintain its active status.

Compliance and Best Practices

Robust security implementations conform to fundamental industry standards and regulatory frameworks, including:

- GDPR, EU Data Act
- ISO/IEC 27001 (FS700 Pro only)
- FIPS 140-2
- NIST 800-88. Guidelines for Media Sanitization (FS700 Pro only)
- NIST 800-52. Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
- NIST 800-171. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (FS700 Pro only)
- US DOD Cybersecurity Maturity Model Certification (CMMC). Level 2: Broad Protection of Controlled Unclassified Information (CUI) (FS700 Pro only)
- NIST 800-193. Platform Firmware Resiliency Guidelines (FS700 Pro only)
- NIST 800-53. Security and Privacy Controls for Information Systems and Organizations
- Common Criteria Protection Profile for General Purpose Operating Systems (FS700 Pro only)

To bolster security posture, IT administrators are responsible for implementing the following measures:

- Regularly applying security updates
- Enforcing robust authentication policies
- Conducting periodic security audits
- Implementing network segmentation for print environments

Guidelines for Secure Fiery Server Configuration

Fiery Administrators can follow these guidelines to strengthen security when configuring the Fiery server:

Change the Administrator password

Fiery servers are shipped from the factory with a default password for the Administrator account. This password grants complete access to the Fiery server, both locally and from a remote client. This access encompasses, but is not limited to:

- File system (Fiery servers on Windows only)
- System security settings
- Applications settings
- Registry entries

We strongly recommend changing the default Fiery Administrator password immediately after installation and at regular intervals, in accordance with your organization's security policies. The Fiery Administrator password must be modified within the Fiery platform.

Secure and Efficient Operation Best Practices

- Restrict SNMP to Version 3 for maximum security.
- Disable WSD for Job Submission to prevent its use in print workflows.
- Disable Windows Printing Protocols (LPR, port 9100, IPP) unless explicitly required.
- Enable TCP/IP Port Filtering to block unused ports and reduce risk.
- Close Ports 137–139 and 445 if not needed for Windows printing or file sharing.
- Disable HTTP on Port 80 to prevent unsecured communications.
- Enable Secure Printing so only the job owner can release print jobs.

High-Security Environments

Administrators with elevated privileges can effortlessly configure high-security settings by selecting the High-Security profile available within **WebTools** > **Configure** > **Security**.

Conclusion

Fiery servers, while equipped with robust security features, are not intended to be internet-facing. They should be deployed in a secure network environment with access carefully controlled by the network administrator. Built to meet the latest industry standards, Fiery servers provide enterprise-grade security to protect print environments against evolving cyber threats. Administrators can ensure compliance and safeguard sensitive data by fully leveraging Fiery's security capabilities.

New in FS700, FS700 Pro

- Core system modules updated to address security vulnerabilities.
- Email functionality has been deprecated to prevent email attacks and to ensure compliance with security regulations.
- All communications with the Fiery server can now be encrypted using TLS 1.3. Remote Desktop connections to Fiery servers running Windows 10 currently support TLS 1.2.
- Added TLS 1.3 support to the following Fiery applications and modules:
  - Licensing server and client components
  - IPP Proxy: required for Microsoft Universal Print
  - 802.1x network authentication protocol
  - EFI LINQ: used for Fiery Server crash reporting
  - JDF
  - System Update
  - FCC – Fiery Cloud Connector
- IPsec tools used on Linux servers were replaced with newer, more secure tools.
- Added support for Advanced Encryption Standard (AES) for SNMPv3 communications and made AES 128 the new default:
  - AES 128 (Default)
  - AES 192 (User can select from Configure)
  - AES 256 (User can select from Configure)
  - DES is still supported, although it is no longer the default option. Users can select it if necessary.