Fiery FS600 Pro/FS600 servers

Fiery Security White Paper

45263449

6 October 2025

Contents

Document overview

This document provides details about how security technology and features are implemented within Fiery FS600 Pro/FS600 servers, and covers hardware security, network security, access control, operating systems, and data security. The intent of the document is to help our customers combine Fiery platform security technology with their own policies to meet their specific security requirements.

Terminology conventions

This document uses the following terminology to refer to the Fiery FS600 Pro/FS600 servers, printers, and Fiery applications.

Term or convention	Refers to
Fiery server	Fiery FS600 Pro/FS600 servers
Printer	Printer, copier, digital press, press, or output device
Configure	Fiery Configure
Command WorkStation	Fiery Command WorkStation
WebTools	Fiery WebTools
QuickTouch	Fiery QuickTouch software running on the Fiery server LCD panel

FIERY security philosophy

FIERY understands that security is one of the top concerns for organizations and businesses worldwide. Our products are frequently enhanced with improved security features intended to protect your company assets. Fiery servers are designed and manufactured with security as a core component to protect system data when at rest, in transit, and during processing.

Working closely with our global partners and suppliers, we are committed to continuously supporting our customers with solutions as threats evolve. To achieve overall system security, we recommend end users combine Fiery security features with their own organization's security policies and follow industry best practices, such as secure passwords and strong physical security procedures.

FIERY approach to security

FIERY security features are guided by five principles::

- **Data security**: No unauthorized disclosure of data during processing, transmission (in-transit), or storage (at rest).
- **Availability**: Performance as intended, free from unauthorized manipulation.
- **Access control**: No denial of service to authorized users.
- **IT-friendly maintenance**: Automatic notifications and downloads of security updates.
- **Compliance**: Support industry regulations and security frameworks.

Fiery software security updates

This section provides a general overview of the Fiery server software security update process. Microsoft® Windows™ OS security vulnerabilities are not described in this document since these are handled directly by Microsoft and delivered to customers as Windows updates as they become available. For security issues or vulnerabilities that could impact the core Fiery hardware components, for example, motherboard, processor, BIOS, and so on, FIERY works closely with the manufacturers to obtain the required security updates.

- FIERY monitors the weekly US-CERT Cyber Security Bulletin from the Cybersecurity and Infrastructure Security Agency (CISA). The bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. Vulnerabilities are based on the Common Vulnerabilities and Exposures (CVE) naming standard and are organized according to severity (high, medium, and low) determined by the Common Vulnerability Scoring System (CVSS).
- FIERY provides security fixes for each Fiery server platform as soon as possible.
- Fiery software security updates are delivered to FIERY partners for approval.
- When approved by the partners, Fiery software security updates are made available for download.
- Fiery System Update downloads and installs the security updates if the option is enabled on the Fiery server. By default, this option is enabled, and we recommend customers leave it enabled.

Timely software updates are critical for optimal operation of Fiery servers. Installing the software security updates for both Fiery and Windows operating system is important to keep Fiery servers secure in any given print environment.

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

Configuring the Fiery server security features

Most Fiery servers security features can be managed using Configure. Configure is found in Fiery WebTools and allows the Fiery administrator to adjust the Fiery servers security settings. Configure requires administrator rights and can be also accessed from Fiery Command WorkStation.

For more information about configuring the Fiery server, see Guidelines for secure Fiery server configuration on page 32.

Hardware security

Security on the Fiery server hardware focuses on preventing data loss in case of a power failure and unauthorized access to the data located on a storage device.

Volatile memory

Data that is written to the volatile RAM is available only while the power is on. When the power is turned off, all the data is deleted.

For more information, see Volatile memory section of the table on page 23.

Nonvolatile memory and data storage

The Fiery server contains several types of nonvolatile data storage technologies to retain data on the Fiery server when the power is turned off. This data includes system programming information and user data.

For more information, see Nonvolatile memory section of the table on page 23.

Flash memory

Flash memory stores the self-diagnostic and boot program (BIOS) and some system configuration data. Flash memory is programmed at the factory and can be reprogrammed only by installing special patches created by FIERY. If the data is corrupted or deleted, the Fiery server will not start.

CMOS

The battery-backed CMOS memory is used to store the Fiery server's machine settings. None of this information is considered confidential or private. If CMOS memory is installed, users can access these settings on a Windows 10 based server by using a monitor, keyboard, and mouse.

NVRAM

There are several small NVRAM devices in the Fiery server that contain operational firmware. These devices contain non–customer specific operational information. The user does not have access to the data contained on them.

Hard disk drive and solid state drive

During normal print and scan operations, and during creation of job management information, image data is written to a random area on the hard disk drive and solid state drive.

Image data and jobs in the queues can be manually deleted by users from Command WorkStation or any other queue operation (such as the operation from the printer LCD). Image data and objects can also be deleted automatically by using the **Clear Server** command, or when the number of printed jobs exceed the allowed parameters. Disabling the printed queue will also delete the printed jobs.

FIERY provides a secure erase feature to remove the image data from the hard disk drive. When Fiery Secure Erase is enabled by the Fiery Administrator, the selected operational mode is carried out at the appropriate time to securely erase deleted data on the hard disk drive. Fiery Secure Erase currently supports only hard disk drives. For solid state drives (SSDs), check with the manufacturer for disk sanitation options before disposing the drive.

Note: For more information about secure erase, see Secure Erase on page 22.

Physical ports

Common physical ports available on most Fiery servers:

Fiery ports	Function	Access	Access control
Ethernet RJ-45 connector	Ethernet connectivity	Network connections	Fiery IP filtering can be used to control access
Printer interface connector	Print and scan	Dedicated for sending/ receiving to/from the printer	N/A
USB Port(s)	USB device connection System software installation	Plug-and-play connector designed for use with optional removable media devices.	• For Windows-based Fiery servers, USB printing can be turned off. • Access to USB storage devices can be turned off through Windows Group Policy. • USB storage can also be disabled from Configure.
Optical fiber connector	10Gb Ethernet connectivity	Network connections	N/A

Local interface

On some Fiery servers, the user can access the Fiery functions at the Fiery NX station monitor, through the Fiery QuickTouch software on the touchscreen display, or through any monitor connected to the Fiery server. Security access on the Fiery server with Fiery NX station is controlled through a Windows Administrator password. The touchscreen display provides very limited functions that do not impose any security risk.

Trusted Platform Module (TPM)

Windows-based Fiery servers on FS600 Pro support a Trusted Platform Module (TPM). The TPM is used to enable optional paid security features. Fiery servers on FS600 Pro use the TPM to encrypt/decrypt the Fiery server boot drive (C: drive). It is also used to securely store the encryption recovery key for the boot drive. Fiery TPM modules

comply with the TPM 2.0 specification, FIPS 140-2 and Common Criteria standards. Check with your service provider for more information about Fiery Security Upgrade Kits and availability for your Fiery DFE.

Fiery Disk Drive Security Kits

Some Fiery servers support an optional disk drive security kit for increased security. This kit allows the user to lock the server drives into the system for normal operation and to remove the drives to a secure location after shutting down the Fiery server.

For Fiery XB servers

The hard disk drives and solid state drives are removable on Fiery XB servers. Most of the hard disk drives and solid state drives are paired together in RAID configuration. It is important to put the drives back to their original location to prevent data loss and a new system software installation.

Enable USB ports for storage use

USB ports on Fiery servers allow mouse, keyboard, or spectrophotometer connections. USB ports can be disabled to prevent connections with external USB storage devices such as pen drives. This option is available in Configure. When disabled, Fiery features that require writing data to an external USB drive are not available.

Network security

The Fiery server includes a variety of security features designed to control and manage network access. Only authorized users and groups can access the Fiery server and print to the printer. The Fiery server can also be configured to limit or control external communications by using designated IP addresses and by disabling network ports and protocols. Fiery servers should always be deployed in a protected network environment and accessibility should be properly configured and managed by a qualified and authorized network Administrator.

Network ports

By default, all TCP/IP ports not used by specific Fiery services are disabled. The Fiery Administrator can selectively enable and disable network ports. Disabling a network port blocks outside connections using the specified port. If a specific port is enabled, outside connections are allowed using that port.

TCP	UDP	Port name	Dependent services
20-21		FTP	FTP
80		HTTP	WebTools, IPP
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
	161, 162	SNMP	SNMP-based tools
	427	SLP	Service Location Protocol
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 Fiery servers only)
3702	3702	WS-Discovery	WSD. Discover WSD-enabled network printers, which show in Network in Windows Explorer, and can be installed by double-clicking on them.
	4500	IPsec NAT traversal	IPsec

TCP	UDP	Port name	Dependent services
	5353	Multicase DNS (mDNS)	Bonjour
6310 8010 8021-8022 8090 9906 21030 50006-50025	9906	FIERY ports	Command WorkStation, Fiery Central, Fiery SDK-based tools, Fiery Printer Driver, Fiery WebTools, Direct Mobile Printing, and Native Document Conversion
9100-9103		Printing port	Port 9100

Note: The 50006-50025 ports are enabled after Command WorkStation version 6.2 and later is installed on a standalone Fiery server.

Note: The IPSec ports (500 and 4500) are only configurable for FS600 (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 also can enable and disable the different network services provided by the Fiery server.

IP Filtering

IP filtering allows or denies connection requests to the Fiery server from defined IP addresses. The Administrator can define default policies to allow or deny incoming data packets, and can also specify filters for a maximum of 16 IP addresses or ranges to allow or deny connection requests.

Each IP filter setting specifies either an IP address or a range of IP addresses and the corresponding action. If the action is **Deny**, packets with a source address belonging to the specified addresses will be dropped, and if the action is **Accept**, the packets will be allowed.

Network authentication

SNMP v3

The Fiery server supports the latest SNMPv3 standard. SNMPv3 communication packets can be encrypted to ensure confidentiality, message integrity, and authentication.

The Fiery Administrator can select from three levels of SNMP security: Minimum, Medium, or Maximum. The Fiery Administrator also has the option to require authentication before allowing SNMP transactions as well as encrypting SNMP user names and passwords. The local Administrator can define SNMP Read and Write community names and other security settings.

For more information, see Recommended settings on page 32.

IEEE 802.1x

802.1x is an IEEE standard protocol for port-based network access control. This protocol provides an authentication mechanism before the Fiery server gets access to the LAN and its resources.

When enabled, the Fiery server can be configured to use EAP MD5-Challenge, PEAP-MSCHAPv2, or EAP-TLS to authenticate to an 802.1x authentication server.

The Fiery server authenticates when it is started or when the ethernet cable is disconnected and reconnected.

Network encryption

Internet Protocol Security (IPsec)

IPsec provides security to all applications over IP protocols through encryption and authentication of every packet.

The Fiery server uses pre-shared key authentication to establish secure connections with other systems over IPsec.

After a secure communication is established over IPsec between a client computer and a Fiery server, all communications—including print jobs—are securely transmitted over the network.

HTTPS

The Fiery server requires a secure connection between clients and different server components. HTTPS over TLS is used to encrypt communications between the two end points. HTTPS is required when connecting to the Fiery server from WebTools and Fiery API. These communications are encrypted with TLS 1.3 and 1.2.

Certificate management

Fiery servers provide an interface to manage the certificates used during TLS communications. Fiery servers support the X.509 certificate format.

Fiery servers support RSA Certificates with 4096, 3072, and 2048-bit key length.

Certificate management allows the Fiery Administrator to do the following:

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

Note: Self-signed certificates are not secure. We strongly recommend users to use a certificate from a trusted Certificate Authority (CA).

Once you obtain a certificate signed by a trusted Certificate Authority, you can upload the certificate to the Fiery server in the Configure section of WebTools.

Email security

The Fiery server supports POP and SMTP email communication protocols, when email is enabled. (The feature is disabled by default.) To protect the service against attack and improper use, the Fiery Administrator can enable additional security features.

POP before SMTP

Some email servers still support unsecured SMTP protocol that allows anyone to send email without authentication. To prevent unauthorized access, some email servers require email clients to authenticate over POP before using SMTP to send an email. For such email servers, the Fiery Administrator would need to enable POP authentication before SMTP.

OP25B

Outbound port 25 blocking (OP25B) is an antispam measure whereby ISPs may block packets going to port 25 through their routers. The email configuration interface allows the Fiery Administrator to specify a different port.

For more information about the Fiery server email printing workflow, see Email printing on page 25.

Server Message Block (SMB)

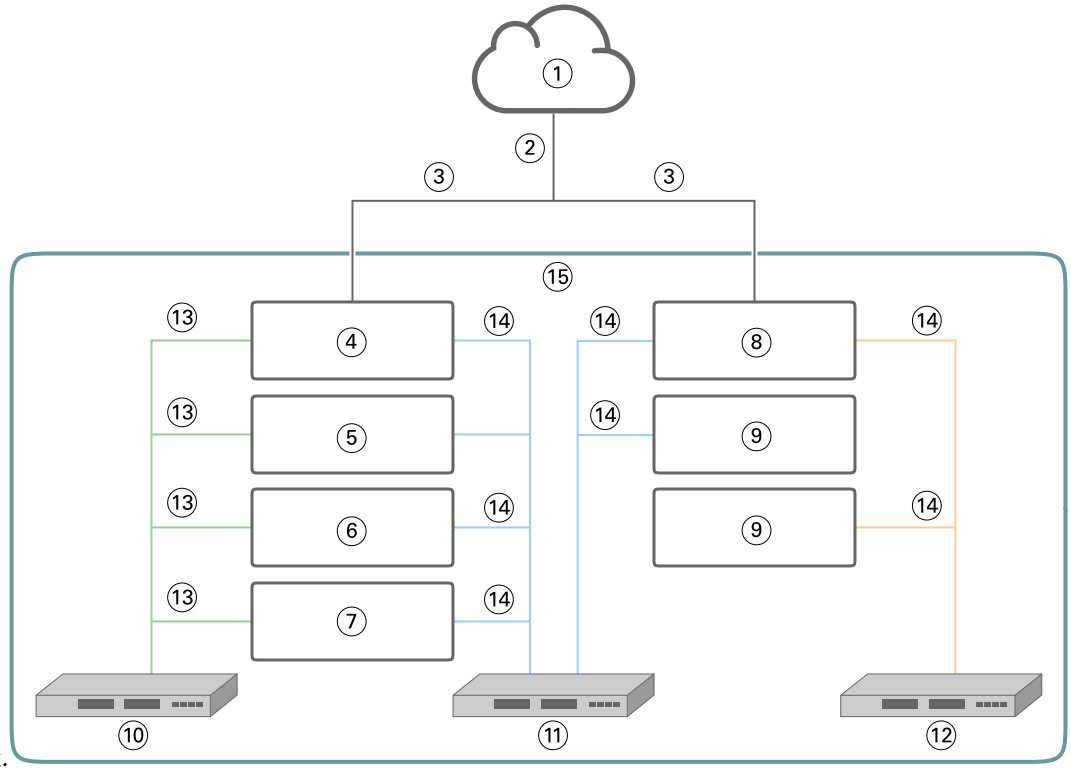
SMB is a network protocol that provides shared access to files and printers. SMB v1 is disabled on Fiery servers as it does not meet current industry security standards. SMB v2 and v3 are still supported.

SMB Signing is enforced on the Fiery server. SMB Signing requires packets signed digitally to allow the recipient to check the authenticity of the packet to prevent “man in the middle” attacks. If SMB authentication is enabled, the user must provide the SMB username and password to access the SMB folders and content that are stored in the SMB folders.

Note: Printing or file sharing through SMB can be restricted by setting a password in Configure.

Fiery XB network diagram

The following chart shows how Fiery XB servers and high-speed inkjet printers connect to the network.



1	LAN	9	Other press blades (optional)
2	Job management network traffic	10	10 GbE Private Network
3	1 GbE DHCP or Static	11	1 GbE Private Network
4	Fiery main blade	12	1 GbE PLC Private Network
5	Fiery RIP blade (optional)	13	10 GbE
6	Fiery blade #1 (optional)	14	1 GbE
7	Fiery blade #2 (optional)	15	Closed Fiery XB environment
8	Press blade		

Access control

This chapter describes how the Fiery server can be configured to control access to resources for the different user groups.

User authentication

The user authentication feature allows the Fiery server to do the following:

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

The Fiery server supports three user authentication methods:

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

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

The Fiery server authorizes users' actions based on their group membership. Each group is associated with a set of privileges (for example, print in grayscale, print in color or grayscale), and the actions of group members are limited to those privileges. The Fiery Administrator can modify the privileges of any Fiery group except for the Administrator and Operator accounts.

For this version of user authentication, the different 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.

Note: User authentication replaces member printing and group printing features.

Fiery software user authentication

The Fiery server software interacts with different types of users. These users are specific to the Fiery software and are not related to Windows-defined users or roles.

It is recommended that Fiery Administrators change all default passwords immediately after first time installation. Use of passwords to access the Fiery server should be enforced.

- Maximum allowed password for both "Administrator" and "Operator" is up to 15 characters when using **Configure** > **Security**.
- For local user accounts the maximum allowed password is up to 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**: Has full control over all the functionality of the Fiery server. The Fiery Administrator can modify the privileges of any Fiery group except for the Administrator and Operator accounts.
- **Operator**: Has same privileges as the Administrator, but has no access to some Fiery server functions, such as setup, and cannot delete the job log.
- **Press Operator** (Fiery XB servers only): Can manage jobs on the press. The Administrator can add specific privileges to this user type.
- **Fiery service admin** (Fiery servers on Windows only): A hidden Admin account used to install the trusted certificate on Windows servers. This account doesn't allow users to log into the Fiery server (local or remote). This account could appear on some network scanning tools and can be removed if needed. Alternative standard methods can be used to install the trusted certificate.
- **Fiery_SMB_User**: This is the default user account for Windows Printing (SMB). Allows Windows SMB users to "see" the Fiery Server in "Network Neighborhood".
- **Guest** (default; no password): has same privileges as the Operator but cannot access the job log, cannot make edits, cannot make status changes to print jobs or preview jobs.

Single Sign-on (SSO)

Fiery FS600 Pro servers support the OpenID Connect protocol for cloud-based, SSO user authentication with Microsoft Entra ID (Azure Active Directory). Users can login to a Fiery server using their existing AAD credentials.

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

The added benefit of this identity management approach is that Fiery servers do not store any user passwords locally, which helps improve security.

Fiery Security Audit Log

To help organizations with compliance requirements, Fiery Administrators can collect and analyze security-related events, which are saved to the Security Audit Log.

The Security Audit Log is enabled by default.

Each security event is classified as Information, Warning, or Error. There are no alerts or notifications provided to the administrator, only a static log.

Logs are in a format supported by common SIEM log collection and analysis solutions. Information about captured events are in accordance with NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (SP800-53).

The Fiery Administrator can read events without FIERY intervention. Events from both Windows and Linux-based Fiery servers are in JSON format and can be processed by any log collection tool. For Windows-based Fiery servers, the events can be viewed in Windows Event Manager. Administrators of Linux-based Fiery servers can forward logs to a central log collection system (SysLog).

Security events are retained based on allocated disk storage capacity. When the log size reaches the maximum storage limit (400MB), older events are removed.

Operating systems

FIERY works closely with the manufacturers of the operating systems used in Fiery servers to obtain the required security updates that could impact the core Fiery server components.

Linux (FS600)

FS600 Linux-based servers are closed systems. Limited network visibility prevents unauthorized access.

About Linux-based Fiery servers:

- Do not include a local interface that could allow access to the operating system.
- SSH and Telnet are not supported, which prevents access to the operating system shell.
- Do not allow installation of unauthorized programs that could potentially expose the system to vulnerabilities.
- The Linux operating system used on FS600 Fiery servers is a customized operating system for Fiery servers only. It has all the operating system components needed by a Fiery server, and do not include general purpose components and end user applications found in common Linux systems.
- Can be configured through Fiery setup at the printer control panel or through Configure in Fiery WebTools. Fiery WebTools is an internal browser-based application used by Fiery Administrators to access the Fiery server for configuration and other system administration activities. Fiery WebTools runs on the latest secure web framework, which is supported by most modern web browsers.

Windows 10 (FS600 Pro)

FS600 Pro Fiery servers run on Windows 10 IoT Enterprise 2021 LTSC. This Windows 10 version contains the latest security protections and includes the cumulative features enhancements provided up to Windows 10 version 21H2. Each LTSC build is supported by Microsoft with security updates for ten years after release.

Note: Windows 10 IoT Enterprise 2021 LTSC is binary equivalent to Windows 10 Enterprise version 21H2.

Windows 10 IoT Enterprise 2021 LTSC includes the following features:

- Intended for use on specialized systems like Fiery servers.
- Incorporates many security improvements for threat, information, and identity protection.
- Provides security updates for up to 10 years after release.
- Does not include consumer-oriented applications, such as Calendar, Weather, Photos, and others.

Microsoft Windows Update

Microsoft regularly issues security patches through **Windows Update** to address potential operating system security threats and vulnerabilities. The default setting of **Windows Update** on Fiery servers is to notify users of patches

without downloading them. Selecting **Check for updates** under **Windows Update** in the Windows **Control Panel** enables automatic updates and starts the update process.

Windows update tools

Windows-based Fiery servers use standard Microsoft methods to update all applicable Microsoft security patches. The Fiery server does not support any other third-party update tools for retrieving security patches.

Windows antivirus software

Fiery servers use Microsoft Defender antivirus software for protection. In general, third-party antivirus software can be used with a Fiery server. Antivirus software comes in many varieties and may package many components and features to address a threat.

Note that antivirus software is most useful when installed, configured, and run on the Fiery server itself. For Fiery servers without a local configuration, it is still possible to launch antivirus software on a remote client computer and scan a shared Fiery server hard drive. The Fiery Administrator must work directly with the antivirus software manufacturer for operational support.

Antivirus engine scan

An antivirus engine scan of the Fiery server may affect Fiery performance, even if the scan has been scheduled.

Antispyware

An antispyware program may affect performance when files are coming into a Fiery server. Examples are incoming print jobs, files that are downloaded during a Fiery server system update, or an automatic update of applications running on the Fiery server.

Built-in firewall

Because the Fiery server has a firewall, antivirus firewalls are not generally required. Customers should work with their own IT department, if there is a need to install and run a built-in firewall that comes as a part of antivirus software. See Network ports on page 10 for a list of available ports.

Anti-spam

The Fiery server supports print-through-email and scan-to-email features. We recommend that a server-based email spam filtering mechanism be used. Fiery servers can also be configured to print documents from specific email addresses.

Host Intrusion Protection System (HIPS) and application control

Because of the complex nature of Host Intrusion Protection System (HIPS) and application control, the antivirus configuration must be tested and carefully confirmed when either of these features are in use. When tuned properly, HIPS and application control are excellent security measures and can coexist with the Fiery server. However, it is very easy to cause Fiery server issues with the wrong HIPS parameter settings and wrong file exclusions—many times caused by "accepting the defaults." Review the selected options in HIPS or application control settings in conjunction with Fiery server settings, such as network ports, network protocols, application executables, configuration files, temp files, and so on.

Safelist and blocklist

Safelist and blocklist functionalities should not typically have adverse effects on the Fiery server. FIERY strongly recommends customers configure these functionalities so that Fiery server modules are not blocked.

Email viruses

Typically, viruses transmitted via email require some type of execution by the receiver. Attached files that are not PDL files are discarded by the Fiery server. The Fiery server also ignores email in RTF, HTML or any included JavaScript. Aside from an email response to a specific user based on a received command, all files received by email are treated as PDL jobs.

Note: For more information about Fiery server email printing workflow, see Email printing on page 25.

Data security

This section describes security controls designed to protect user data resident within the Fiery server and data in transit.

Encryption of critical information

Encryption of critical customer data ensures that all passwords and related configuration information are secured when stored in the Fiery server. Critical information is either encrypted or hashed. The cryptographic algorithms implemented are AES256, Diffie-Hellman, and SHA-2 and are used in compliance with the latest security standards.

Customer data stored on the disk cannot be read even if the disk is removed from the Fiery server. User data encryption can be enabled or disabled on Windows-based Fiery servers using Configure. For Linux-based Fiery servers, the feature is always enabled.

If the passphrase used to recover data is forgotten, there is no way to reset it, and FIERY cannot recover it. Software would have to be reinstalled.

Windows-based servers also have an option to encrypt the boot drive. The boot drive includes the Operating System and Fiery System Software. Encryption of the boot drive prevents someone from booting the Fiery server with another operating system and easily bypass the intended operating system's enforcement of file permissions.

Standard printing

Jobs submitted to the Fiery server may be sent to one of the following print queues published by the Fiery server:

- Hold queue
- Print queue
- Sequential print queue
- Direct queue direct connection
- Virtual printers (custom queues defined by the Fiery Administrator)

The Fiery Administrator can disable the print queue and direct queue to limit automatic printing.

Hold, print, and sequential print queues

When a job is printed to the print queue or the hold queue, the job is spooled to the hard drive on the Fiery server. Jobs sent to the hold queue are held on the Fiery hard disk drive until the user submits the job for printing or deletes the job using a job management utility, such as Command WorkStation.

The sequential print queue allows the Fiery server to maintain the job order on certain jobs sent from the network. The workflow will be "first in, first out" (FIFO), respecting the order in which the jobs were received over the network. Without sequential print queue enabled, print jobs submitted through the Fiery server can get out of order due to many factors, such as the Fiery server allowing smaller jobs to skip ahead while larger jobs are spooling.

Printed queue

Jobs sent to the print queue are stored in the printed queue on the Fiery server after printing, if the printed queue is enabled. The Administrator can define the number of jobs kept in the printed queue. When the printed queue is disabled, jobs are deleted automatically after being printed.

Direct queue (direct connection)

The direct queue is designed for font downloading and applications that require direct connection to the PostScript module in Fiery servers.

For environments with high-security requirements it is recommended not printing to the direct queue. The Fiery server deletes all jobs sent by the direct connection after printing. However, there is no guarantee that all temporary files relating to the job will be deleted.

Jobs of VDP (Variable Data Printing), PDF, or TIFF file types are rerouted to the print queue when sent to the direct queue. Jobs sent by the SMB network service may be routed to the print queue when sent to the direct queue.

Job deletion

A job cannot be viewed or retrieved when it is deleted automatically from the Fiery server or erased using Fiery tools. If the job was spooled to the Fiery server hard disk drive, the job elements may remain on the hard disk drive and could theoretically be recovered with certain tools, such as forensic disk analysis tools.

Secure Erase

Secure erase is designed to remove the content of a submitted job from the Fiery server hard disk drive whenever a Fiery function deletes a job. After the job is deleted, the job information cannot be recovered from the Fiery server hard drive.

For Linux-based FS600 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.

Windows-based FS600 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.

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
Jobs archived to removable media	No

Workflows	Secure erase
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

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

System memory

The processing of some files may write some job data to the operating system memory. In some cases, this memory may be swapped to the hard disk drive and is not specifically overwritten.

Volatile memory			
Type (SRAM, DRAM, and so on)	**User modifiable (Yes or No)**	**Function or use**	**Process to sanitize**
DRAM	Yes	Main System Memory (receives jobs sent to Direct queue)	Power off Fiery server
SDRAM (on video card)	Yes	Video memory	Power off Fiery server

Nonvolatile memory			
Type (SRAM, DRAM, and so on)	**User modifiable (Yes or No)**	**Function or use**	**Process to sanitize**
BIOS	No	BIOS functions	Remove from socket and destroy, but system will cease to function.
Ethernet Eprom	No	Ethernet chip firmware	Desolder and destroy, but system will cease to function.

Nonvolatile memory			
Type (SRAM, DRAM, and so on)	**User modifiable (Yes or No)**	**Function or use**	**Process to sanitize**
CMOS NVRAM	No	Bios settings storage	Remove system battery for 30 seconds.
Hard disk drive (HDD) or Solid state drive (SSD)	Yes	Operating system Fiery applications (possibly with user data) Fiery system software Print jobs, scan jobs, and other user data Backup image for factory default	Reinstall the system software. Most jobs can be securely removed with the Secure Erase feature*. OEM or third party disk sanitation tools can also be used to completely wipe the data on these devices.
Note: Volatile Memory and the RAM could contain customer data while processing customers' data. No customer data is stored in the nonvolatile memory such as BIOS, CMOS, and NVRAM. *Using multi-pass overwriting methods for jobs stored on SSDs is not recommended due to memory wear. All SSDs have a limited number of write cycles and overwriting them multiple times will greatly erode the operational lifetime of the drive. Fiery servers store job data in hard disk drives.			

Secure print

The secure print function requires the user to enter a job-specific password at the Fiery server and the printer to allow the job to print.

This feature requires access to the printer control panel. The intent of the feature is to limit access to a document to a user who has the password for the job and can enter it locally at the printer control panel.

Secure print workflow

The user enters a password in the **Secure print** field in the Fiery driver. When this job is sent to the Fiery server print or hold queue, the job is queued and held for the password.

Note: Jobs sent with a secure print password are not viewable from Command WorkStation.

From the printer control panel, the user accesses a secure print window and enters a password. The user can then locate the jobs sent with that password and print and then delete the jobs.

The printed secure job is not moved to the printed queue and is deleted automatically after printing.

Note: Some portion of the data may remain temporarily in the operating system files.

Email printing

The Fiery server receives and prints jobs sent by email. The Administrator can store a list on the Fiery server of authorized email addresses. Any email received from an email address that is not in the authorized email address list is deleted. The email printing feature is off by default. The Administrator can turn on and off the email printing feature.

Job management

Performing job actions on jobs submitted to the Fiery server requires a Fiery job management utility with either Administrator or Operator access.

Job log

The job log is stored on the Fiery server. Individual records of the job log cannot be deleted. The job log contains print and scan job information, such as the user who initiated the job; the time the job was carried out; and characteristics of the job in terms of paper used, color, and so on. The job log can be used to inspect the job activity of the Fiery server.

A user with Operator access can view, export, or print the job log from Command WorkStation. A user with Administrator access can delete the job log from Command WorkStation.

Remote users can see the job log on company's IQ Portal tenant if the Fiery server is connected to FIERY IQ.

Setup

Setup requires an Administrator password. The Fiery server can be set up from Configure in Fiery WebTools, Fiery Command WorkStation, or from the Setup feature on the printer control panel.

Scanning

The Fiery server allows an image placed on the printer glass to be scanned back to the workstation that initiated the scan. When a scan function is initiated from a workstation, the raw bitmap image is sent directly to the workstation.

The user can scan documents to the Fiery server for distribution, storage, and retrieval. All scanned documents are written to disk. The Administrator can configure the Fiery server to delete scan jobs automatically after a predefined timeframe.

Distributing scanned jobs

Scan jobs can be distributed by a variety of methods.

Email

An email with an attachment of the scanned job is sent to a mail server, where it is routed to the desired destination.

Note: If the file size of the scanned job is greater than the Administrator-defined maximum, the job is stored on the Fiery server hard disk drive, which is accessible through a URL.

FTP

The file is sent to an FTP destination. A record of the transfer, including the destination, is kept in the FTP log, which is accessible from the printer control panel print pages command. An FTP proxy server can be defined to send the job through a firewall.

Fiery server hold queue

The file is sent to the Fiery server hold queue and is not kept as a scan job.

For more information about the Fiery server hold queue, see Hold, print, and sequential print queues on page 21.

Internet fax

The file is sent to a mail server where it is routed to the desired internet fax destination.

Mailbox

The file is stored on the Fiery server with a mailbox code number. Users need to enter the correct mailbox number to access the stored scan job. Users have the option of setting passwords to protect the contents of their scan mailboxes against unauthorized access. The scan job is retrievable through a URL.

Fiery communications with Cloud services

Some Fiery internal services and some Fiery applications require communication with external cloud-based services; for example, to download Fiery Security Updates or for License Activation.

The information provided below is intended for IT or Network Administrators, and can be used to configure the Fiery server behind corporate firewalls.

#	Fiery Service/ Application	Remote URLs	Port	Use
1	System Update	https://liveupdate.fiery.com	443	Download Fiery patches
2	OFA	https://flexlicensing.fiery.com	443	For license activation
3	IQ	https://iq.fiery.com	443	Communication with Fiery IQ
4	LINQ	https://ews.fiery.com	443	Analytics
5	Universal Print by Microsoft	https://portal.azure.com https://print.print.microsoft.com https://notification.print.microsoft.com https://discovery.print.microsoft.com https://graph.print.microsoft.com	443	Communication with Universal Print by Microsoft
6	Single Sign-On (SSO)	https://login.microsoft.com	443	Single Sign-On (SSO)

#	Fiery Service/ Application	Remote URLs	Port	Use
7	Windows Update	https://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://*.dl.delivery.mp.microsoft.com https://*.dl.delivery.mp.microsoft.com	80 443	Windows updates
8	Command WorkStation	https://help.fiery.com https://learning.fiery.com https://communities.fiery.com/s/ https://liveupdate.fiery.com https://iq.fiery.com	443	Access Fiery services and resources
9	Fiery Driver	https://help.fiery.com	443	Access Fiery online help resources
10	Fiery Updater	https://liveupdate.fiery.com	443	Check for Fiery updates from Command WorkStation

#	Fiery Service/ Application	Remote URLs	Port	Use
11	Fiery Software Manager	https://liveupdate.fiery.com https://www.fiery.com https://solutions.fiery.com/estore/downloads https://assistance.fiery.com/ffc/whatsnew/ https://assistance.fiery.com/ffc/overview/ https://assistance.fiery.com/cws_cs/whatsnew/ https://assistance.fiery.com/cws/CRNs/ https://assistance.fiery.com/frs/CRNs/ https://assistance.fiery.com/jobflow/overview/ https://assistance.fiery.com/cps/whyupgrade/ https://assistance.fiery.com/cps/renewsmsa/ https://assistance.fiery.com/cps/spectros/ https://assistance.fiery.com/cps/CRNs/ https://assistance.fiery.com/cps/getthelatest/	443	Check for software updates
12	Fiery Software Manager	https://diumxs9ckzarso.cloudfront.net	443	Download Fiery applications
13	Fiery JobFlow	https://help.fiery.com/ https://assistance.fiery.com/jobflow/productsupport/ https://solutions.fiery.com/jobflow-cookbook	443	Access Fiery services and resources
14	Fiery Color Profiler Suite	https://help.fiery.com/cps/ https://communities.fiery.com/s/ https://www.fiery.com/products/color-imaging/fiery-color-profiler-suite/#resources https://activation.fiery.com/fulfillment/cps/?lang=en https://flexlicensing.fiery.com	443	

Regulations and frameworks compliance

The table below provides regulations and frameworks compliance for Fiery servers running FS600 Pro/FS600 system software.

Regulations / frameworks	Scope	NX Series (FS600 Pro)	A/E Series (FS600)
FIPS 140-2	• USA, Canada • Security Requirements for Cryptographic Modules	In compliance Windows 10 2021 LTSC	Not in compliance
CIS Benchmark	• Configuration baselines and best practices for securely configuring a system	In compliance Microsoft Windows 10 Enterprise (Release 21H2) Benchmark	N/A*
Security Technical Implementation Guide (STIG)	Security configuration standard for hardware and software used by US Department of Defense (DOD) agencies.	In compliance Windows 10 STIG version 2, R4	N/A*
Common Criteria	• Information technology security techniques evaluation criteria for IT security	In compliance	Not in compliance
Safeguard Computer Security Evaluation Matrix (SCSEM)	• US Government (Federal & State) • Tax Information Security Guidelines For Federal, State and Local Agencies	In compliance Resistance and detection requirements need optional Fiery disk drive security kit	Not in compliance
DoD 522.22-M	Data sanitization standard.	N/A	In compliance 3-pass
NIST 800-88	Data sanitization standard.	In compliance 1-pass or 3-pass	Not in compliance

*Out of scope of regulation or framework. A and E-Series Linux-based servers are closed systems with no direct access to the file system. Limited network visibility prevents unauthorized access.

FIPS 140-2 compliance

When configured properly, Fiery servers running FS600 Pro on Windows 10 2021 LTSC can comply with FIPS 140-2 data encryption guidelines. A Fiery server in *FIPS 140-2 Mode*, uses only cryptographic algorithms validated and certified under the U.S. Federal Government's Cryptographic Algorithm Validation Program (CAVP) to encrypt data at rest and in-transit.

Enabling *FIPS 140-2 Mode* in Fiery requires certified Fiery professional hardening services.

Guidelines for secure Fiery server configuration

The following guidelines can help Fiery Administrators improve security when configuring the Fiery server.

Changing the Administrator password

We recommend you change the default Fiery Administrator password upon installation and at regular intervals as required by your organization's security policies. The Administrator default password should be changed in **Fiery Setup Wizard** during first-time setup. The Administrator and the Operator passwords can be changed after first-time setup in WebTools: **Configure** > **Security** > **Administrator Password** (or Operator, respectively). Password setup is also available from **Configure** > **User Accounts** > **Fiery Contact List**.

The Administrator password provides full access to the Fiery server locally or from a remote client. Full access includes, but is not limited to:

- File system
- System security policy
- Registry entries
- Administrator password, which denies anonymous users access to the Fiery server

Recommended settings

- Choose **Maximum** security level for SNMP in **Network** > **SNMP**:

  Choosing maximum security restricts support on the Fiery server to SNMP v3 only.

  If SNMP manager works only with SNMP v1/v2c, change the value of the **Read Community Name** field. The Fiery server allows you to change the values of SNMP **Read Community Name** and **Write Community Name** fields from WebTools (**Configure** > **Network** > **SNMP**) and printer control panel (**Network** > **SNMP**).
- Disable WSD in job submission.
- Disable Windows printing in job submission if using lpr, port 9100, or IPP to print.
- Block ports by enabling TCP/IP port filter in **Security** > **TCP/IP** port filtering.

  Clear ports 137-139 and 445 if you are not using Windows printing and do not have the need to access or share file folders. Disable unsecured Port 80 (HTTP) communications.

In addition to operating system level protections, the Fiery server has the following additional security features to help protect your data:

- Fiery servers come with secure print to make sure that the user picks up only his or her printing job.
- Fiery servers integrate with the leading job accounting solutions to include additional security through follow-me printing.

Fiery servers come with numerous security features but are not internet-facing servers. They should be placed in a protected environment and their accessibility should be properly managed by the network Administrator.

Selecting High security profile

The Fiery server provides pre-defined security recommendations based on different risks and threat levels (**Standard**, **High**, **Current**). This feature is called **Security Profiles** and can be accessed from the following locations:

- Fiery Software Wizard
- **WebTools** > **Configure** > **Security**

The **High** security profile allows the Fiery server to be even more secure and enables the most commonly used security features.

Option	High
TCP/IP Port Filtering	Enabled
Service Location Protocol (SLP)	Disabled
Bonjour	Disabled
Secure Erase	Enabled
Remote Desktop	Disabled
SMB Password	Enabled
USB Storage Devices	Disabled
PostScript Security	Enabled
Port 9100	Disabled
LPD	Enabled
Windows Printing	Disabled
IPP	Enabled
Web Services for Devices (WSD)	Disabled
Print via Email	Disabled
FTP Printing	Disabled
Direct Mobile Printing	Disabled

FIERY recommends using the **High** security profile for environments with maximum security requirements.

Conclusion

FIERY offers a robust set of standard and optional security features for Fiery servers. These comprehensive and customizable security features are suitable for customers of any size, including customers with strict security requirements. FIERY is committed to delivering enhanced security features that protect Fiery servers against vulnerabilities, malicious or unintentional use and to safeguard customer data without impacting efficiency.

Copyright information