Fiery FS500 Pro/FS500 servers

Fiery Security White Paper

45234233

27 June 2022

Contents

Document overview 5
Terminology conventions 5
EFI security philosophy 5
EFI security goals 5
Fiery software security updates 6
Configuring the Fiery server security features 6

Hardware security 8
Volatile memory 8
Nonvolatile memory and data storage 8
Flash memory 8
CMOS 8
NVRAM 8
Hard disk drive and solid state drive 9
Physical ports 9
Local interface 9
Removable hard disk drive kit option 9
For standalone Windows servers 10
For Fiery XB servers 10
Enable USB ports for storage use 10

Network security 11
Network ports 11
IP Filtering 12
Network authentication 12
Network encryption 13
Email security 13
Server Message Block (SMB) 14
Fiery XB network diagram 14

Access control 16
User authentication 16
Fiery software user authentication 16
Fiery Security Audit Log 17

Operating systems 18
Linux (FS500) 18
Accessing the system 18
Windows 10 (FS500 Pro) 18
Microsoft Windows Update 19
Windows update tools 19
Windows antivirus software 19
Email viruses 20

Data security 21
Encryption of critical information 21
Advanced Encryption Standard (AES) 21
Standard printing 21
Hold, print, and sequential print queues 22
Printed queue 22
Direct queue (direct connection) 22
Job deletion 22
Secure erase 22
System memory 23
Secure print 24
Secure print workflow 24
Email printing 25
Job management 25
Job log 25
Setup 25
Scanning 25
Distributing scanned jobs 26

Regulations and frameworks compliance 27
FIPS 140-2 compliance 28

Guidelines for secure Fiery server configuration 29

Conclusion 31

Document overview

This document provides details about how security technology and features are implemented within Fiery FS500 Pro/FS500 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 FS500 Pro/FS500 servers, printers, and Fiery applications.

Term or convention	Refers to
Fiery server	Fiery FS500 Pro/FS500 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

EFI security philosophy

EFI 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. EFI 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 EFI 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 specific industry best practices, such as secure passwords and strong physical security procedures.

EFI security goals

EFI has established the following goals when implementing security measures for the Fiery server:

- **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 when security updates are available.
- **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 since these are handled directly by Microsoft and delivered 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, EFI works closely with the manufacturers to obtain the required security updates.

- EFI 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).
- EFI provides security fixes for each Fiery server platform as soon as possible.
- Fiery software security updates are delivered to specific EFI 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: All Fiery updates or patches are digitally signed with SHA-2.

Configuring the Fiery server security features

Configure is the main tool used to configure the security features on Fiery servers. Fiery Administrators can access Configure from Command WorkStation or WebTools.

Note: Users must have Administrator privileges to access Configure.

For more information about configuring the Fiery server, see Guidelines for secure Fiery server configuration on page 29.

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 EFI. If the data is corrupted or deleted, the Fiery server does 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 IoT Enterprise 2016 or 2019 based server by using the 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.

EFI provides a secure erase feature to protect the image data from unauthorized access. When 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

The Fiery server can be connected through external ports shown in the following table:

Fiery ports	Function	Access	Access control
Ethernet RJ-45 connector	Ethernet connectivity	Network connections	Using Fiery IP filtering to control access
Printer interface connector	Print and scan	Dedicated for sending/ receiving to/from the printer	N/A
USB Port	USB device connection System software installation	Plug-and-play connector designed for use with optional removable media devices.	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.

Removable hard disk drive kit option

Some Fiery servers support a removable hard disk drive option 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 standalone Windows servers

Standalone Windows-based Fiery servers support a removable hard disk drive option kit. Whether this option kit is available or not for a specific Fiery product depends on the terms of EFI's agreements with its individual Fiery partners.

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, but will prevent connections to USB storage devices when the Enable USB Storage option is disabled in Configure. This option is enabled by default. When disabled, the option disables Fiery features requiring USB mass storage functionality, such as Backup and Restore.

Network security

The Fiery server includes a variety of network security features designed to control and manage access to the printer. 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 as well as 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 (Windows 10 only). An additional port in the range 49152-65536 will be opened to provide SMB-related point and print service.
137-139		NETBIOS	Windows Printing
	161, 162	SNMP	Fiery Central, some legacy utilities, other SNMP-based tools
	427	SLP	SLP
443		HTTPS	WebTools, IPP/s
445		SMB/IP	SMB over TCP/IP
	500	ISAKMP	IPsec
515		LPD	LPR printing, some legacy utilities (such as older versions of Command WorkStation)
631		IPP	IPP
3389		RDP	Remote Desktop (Windows Fiery servers only)
3702	3702	WS-Discovery	WSD

TCP	UDP	Port name	Dependent services
	4500	IPsec NAT	IPsec
	5353	Multicase DNS	Bonjour
6310 8010 8021-8022 8090 9906 21030 50006-50025	9906	EFI ports	Command WorkStation 5 and 6, Fiery Central, EFI SDK-based tools, Fiery Printer Driver bi-di functions, WebTools, Fiery 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.

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 29.

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)

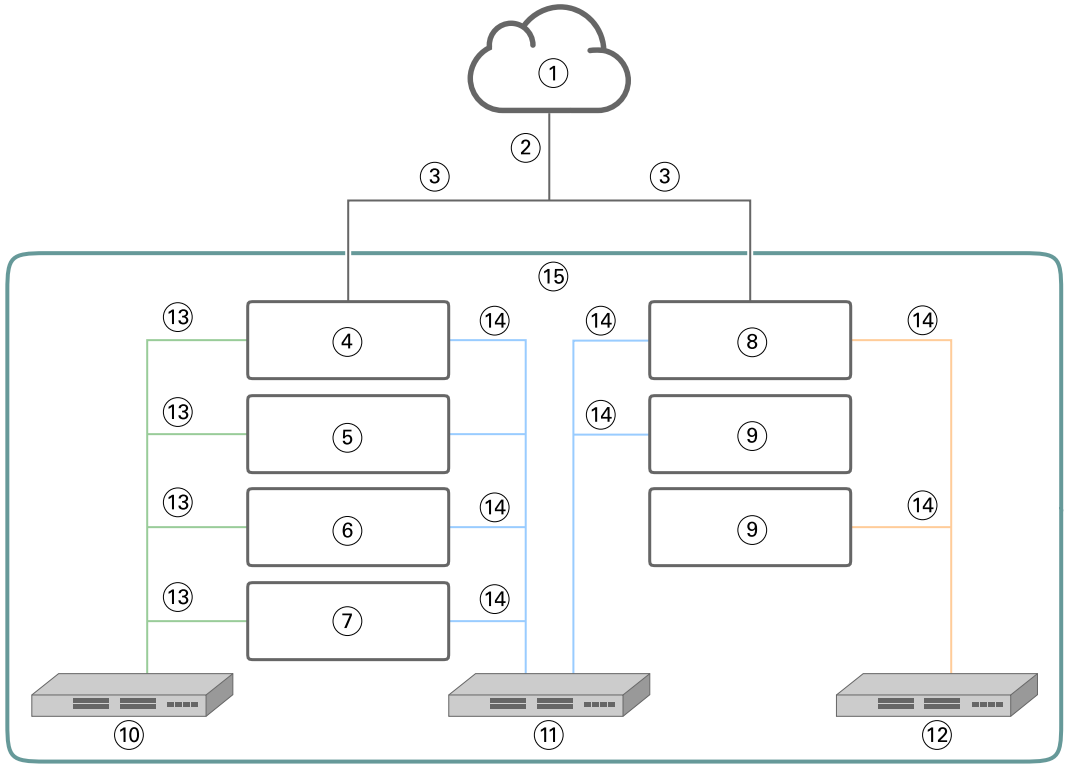
SMB is a network protocol that provides shared access to files and printers. SMB v1 is disabled on Fiery servers as it does not meet current industry security standards. SMB v2 and v3 are still supported.

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 the resources for 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 can authenticate users who are:

- Domain-based: users defined on a corporate server and accessed through LDAP
- Fiery-based: users defined on the Fiery server

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**: This privilege allows group members to print jobs in grayscale on the Fiery server. 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**: This privilege allows group members to print jobs on the Fiery server 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 the job via FTP (color devices only).
- **Fiery mailbox**: This privilege 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**: This privilege allows group members to create server presets in order to allow other Fiery users access to commonly used job 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 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 require passwords to access the Fiery server. Additionally, EFI recommends that the Fiery Administrator change the default password to meet the security requirements of user's print environment.

- Maximum allowed password for both "Administrator" and "Operator" is up to 15 characters when using Configure > Security.
- Maximum allowed password for local users accounts is up to 64 characters when using Configure > User Accounts.
- Administrator and Operator passwords can also be changed in Configure > User Accounts where the maximum allowed characters is 64.

The following describes the privileges allowed for the different Fiery user types:

- **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 most of the 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 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 EFI 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

EFI works closely with the manufacturers of the operating systems used in Fiery servers to obtain the required security updates for security issues or vulnerabilities that could impact the core Fiery server components such as motherboard, processor, BIOS, and so on. In addition, Fiery software updates are digitally signed by EFI to prevent unauthorized modification, including insertion of malware.

Linux (FS500)

FS500 Fiery servers are Linux-based servers designed with a closed architecture. Limited network visibility prevents unauthorized access.

The characteristics of Linux-based Fiery servers are as follows:

- Linux-based Fiery servers do not include a local interface that could allow access to the operating system.
- SSH and Telnet are not supported on Linux-based Fiery servers, which prevents access to the operating system shell.
- Linux-based Fiery servers do not allow installation of unauthorized programs that could potentially expose the system to vulnerabilities.
- The Linux operating system used on FS500 Fiery servers is a customized operating system for Fiery servers only. It has all the operating system components needed by a Fiery server, but not some of the general purpose components and end user applications found in common Linux systems.

Accessing the system

Linux-based Fiery servers can be configured through Fiery setup at the printer control panel or through Configure in WebTools. WebTools is a set of browser-based pages that allows the Fiery Administrator to access the Fiery server for configuration and other system administration related activities. WebTools runs on the latest secure web framework, which is supported by most modern web browsers.

Windows 10 (FS500 Pro)

FS500 Pro standalone Fiery servers use Windows 10 IoT Enterprise 2019 LTSC as their operating system. This Windows edition contains the latest security protections and includes the cumulative features enhancements provided in Windows 10 versions 1703, 1709, 1803, and 1809. Each LTSC build is supported by Microsoft with security updates for ten years after release.

Note: Windows 10 IoT Enterprise 2019 LTSC is a binary equivalent to Windows 10 Enterprise version 1809.

Windows 10 IoT Enterprise 2019 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 numerous security updates.
- 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 antivirus software and Windows 10 Defender 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. However, EFI suggests that the Fiery Administrator 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. EFI recommends that customers 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 11 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 spam filtering mechanism be used. Fiery servers can also be configured to print documents from specified email addresses. The anti-spam component is not required because running a separate email client (such as Outlook) on the Fiery server is not a supported operation.

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 is in use. When tuned properly, HIPS and application control are excellent security measures and 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." The solution is to 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. EFI strongly recommends that the customer configure these functionalities so that Fiery 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 or 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 the security controls for data in transit.

Encryption of critical information

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

User information 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 that is entered to recover data is forgotten, there is no way to reset it, and EFI cannot recover it. Software would have to be reinstalled.

Note: With data encryption, the disk is partitioned and only the user data partition is encrypted. Operating system partitions cannot be encrypted.

Advanced Encryption Standard (AES)

The Fiery server protects data at rest from unauthorized access. It encrypts jobs, images, and customer data using 256-bit AES algorithm.

AES is a small, fast, and hard-to-crack encryption standard suitable for a wide range of devices and applications. It provides an extra level of protection against data theft while complying with corporate security policies.

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.

EFI does not recommend printing to the direct queue. The Fiery server deletes all jobs sent by the direct connection after printing. However, EFI does not 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. 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.

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

Workflows	Secure erase
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
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 Fiery servers with 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.
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*. Third party and Fiery partner sanitation tools can be used to complete wipe 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. *Solid state drives cannot be completely sanitized by Secure Erase multi-pass overwriting methods due to the memory wear mapping that occurs. Additionally, attempts to do so would also greatly erode the operational lifetime of the solid state drive. This feature is not supported on Fiery XB platforms.			

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.

Setup

Setup requires an Administrator password. The Fiery server can be set up from the Configure tool in WebTools or 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 22.

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.

Regulations and frameworks compliance

The table below provides regulations and frameworks compliance for Fiery servers running FS500 Pro/FS500 system software.

Regulations / frameworks	Scope	NX Series (FS500 Pro)	A/E Series (FS500)
FIPS 140-2	• US Government (Federal & State) • Security Requirements for Cryptographic Modules	In compliance Windows 10 2019 LTSC FIPS certificates: • #3197 • #3196 • #3092	Not in compliance
CIS Benchmarks	• Global • Government / Private Sector • Configuration baselines and best practices for securely configuring a system	In compliance Microsoft Windows 10 Enterprise (Release 1809) Benchmark	N/A*
Security Technical Implementation Guide (STIG)	• US Government (Federal & State) Configuration standard consisting of cybersecurity requirements for a specific product	Partial compliance Windows 10 STIG version 2, R3 Exceptions: CCI-000366: Trusted Platform Module (TPM) not available	N/A*
ISO/IEC-15408	• Global • Common Criteria • Information technology security techniques evaluation criteria for IT security	Partial compliance • LDAP/AD authentication required for access control • TPM and Secure Boot not supported	Not in compliance

Regulations / frameworks	Scope	NX Series (FS500 Pro)	A/E Series (FS500)
IEEE 2600.2-2009	• Global • Government / Private Sector • Common criteria profile for hardcopy devices Environment B	Partial compliance • TPM and Secure Boot not supported • Resistance and detection requirements need optional Fiery disk drive security kit	Not in compliance
Safeguard Computer Security Evaluation Matrix (SCSEM)	• US Government (Federal & State) • Tax Information Security Guidelines For Federal, State and Local Agencies	Partial compliance • TPM and Secure Boot not supported • Resistance and detection requirements need optional Fiery disk drive security kit	Not in compliance
DoD 522.22-M	Data sanitization standard. 3-pass	In compliance	In compliance
NIST 800-88	Data sanitization standard. 1-pass	Not in compliance	Not in compliance
Army RMF certification	• US Government • Risk Management Framework for Army Information Technology	Partial compliance • TPM and Secure Boot not supported	Partial compliance • TPM and Secure Boot not supported

*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 FS500 Pro on Windows 10 2019 LTSC 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 the user to follow an advanced configuration process for hardening the server.

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 User Accounts.

The Administrator password gives a user 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 configured 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

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

Conclusion

EFI offers a robust set of standard and optional security features on the Fiery server to provide our customers with comprehensive and customizable security solutions for any environment. EFI is committed to ensuring that the Fiery server is effectively protected against vulnerability to either malicious or unintentional use so that our customers can operate their companies at maximum efficiency.