Fiery Security White Paper

Fiery FS150 Pro /FS150 Servers running on Microsoft® Windows® 10 IoT Enterprise 2016 LTSB

Date of Issue: May 2018

White Paper Series

Fiery Security White Paper

Table of Contents

1 Document Overview

This document gives end users an overview of the Fiery® server's architecture and functional aspects as they relate to device security in the Fiery FS150/FS150 Pro servers. It covers hardware, network security, access control, operating system and data security.

The document's intent is to help end users understand all the Fiery server's security features that they can benefit from and to understand its potential vulnerabilities.

1.1 EFI Security Philosophy

EFI™ understands that security is one of the top concerns for business worldwide today, so we've built strong security features into the Fiery servers to protect companies' most valuable assets. We also proactively work with our global OEM partners and our cross-functional teams to determine companies' current and future security requirements so that security doesn't become an issue with our products. As always, we still recommend that end users combine Fiery security features with other safeguards, such as secure password and strong physical security procedures, to achieve overall system security.

1.2 Configure the Security Feature via Fiery Configure

Fiery users who access security the Fiery server via Fiery Command WorkStation® using the Administrator login can configure all Fiery features via Fiery Configure. Fiery Configure can be launched from Fiery Command WorkStation or WebTools™ under the Configure tab.

2 Hardware and Physical Security

2.1 Volatile Memory

The Fiery server uses volatile RAM for the CPU's local memory and for the operating system, Fiery system software and image data's working memory. Data that is written to RAM is held while the power is on. When the power is turned off, all data is deleted.

2.2 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.

2.2.1 Flash Memory

Flash memory stores the self-diagnosis and boot program (BIOS) and some system configuration data. This device 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 system does not start.

A portion of the flash memory also is used to record the use of dongle to activate Fiery software options.

No user data is stored on this device, and the user does not have data access to it.

2.2.2 CMOS

The battery-backed CMOS memory is used to store the server's machine settings. None of this information is considered confidential or private. Users may access these settings on a Windows 10 IoT Enterprise 2016 LTSB (Windows 10) server via the Fiery Integrated Workstation (FACI kit including local monitor, keyboard and mouse) if installed.

2.2.3 NVRAM

There are a number of 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.

2.2.4 Hard Disk Drive

During normal print and scan operations as well as during creation of job management information, image data is written to a random area on the hard disk drive (HDD).

Image data and job management information can be deleted by an Operator or at the end of a pre-set time period, making image data inaccessible.

To protect the image data from unauthorized access, EFI provides a Secure Erase feature (see section 6.2.5). Once enabled by the system administrator, the selected operation is carried out at the appropriate time to securely erase deleted data on the HDD.

2.2.5 Physical Ports

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

Fiery Ports	Function	Access	Access Control
Ethernet RJ-45 connector	Ethernet connectivity	Network connections (see printing and network connections below)	Use Fiery IP filtering to control access
Copier interface connector	Print/Scan	Dedicated for sending/ receiving to/from the print engine	N/A
USB Port	USB device connection	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.

2.3 Local Interface

The user can access the Fiery functions at the FACI kit (if enabled on a Windows 10 server) or at the Fiery LCD on Fiery servers. Security access on the Fiery Server with FACI kit is controlled through a Windows administrator password if the FACI kit is enabled. The Fiery LCD provides very limited functions that do not impose any security risk.

2.4 Removable HDD Kit Option

The Fiery server supports a Removable Hard Disk Drive option kit for increased security. This kit allows the user to lock the server drive(s) into the system for normal operation and to remove the drives to a secure location after powering down the server.

2.4.1 For External Servers

Fiery servers support a Removable Hard Disk Drive option kit. Whether this option kit is available for a specific Fiery product depends on the terms of EFI's development and distribution agreements with its individual OEM partners.

2.4.2 For Embedded Servers

Embedded products can only offer removable HDD as an OEM coordinated option because the mounting location and brackets for the multifunction printer (MFP) must be developed jointly with the OEM. The option kit is to take the internal HDD out from embedded chassis and mount to an external and separately powered enclosure.

3 Network Security

Standard network security features on the Fiery server include the ability to permit only authorized users and groups to access and print to the output device, limiting device communications to designated IP addresses and controlling the availability of individual network protocols and ports as desired.

Even though Fiery servers come with various security features, it is not an internet facing server. It should be deployed in a protected environment and its accessibility should be properly configured by the network administrator.

3.1 Network Ports

The Fiery server allows the network administrator the ability to selectively enable and disable the following IP ports. As a result, unwanted device communication and system access via specific transport protocols can be effectively blocked.

TCP	UDP	Port Name	Dependent Service(s)
20–21		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	WebTools, Fiery Central, some legacy utilities, other SNMP-based tools
	427	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 WebTools, older versions of CWS)
631		IPP	IPP
3050			Firebird
	4500	IPsec NAT	IPsec
	5353	Multicase DNS	Bonjour
3389		RDP	Remote Desktop (Windows Fiery servers only)
3702	3702	WS-Discovery	WSD
6310 8010 8021–8022 8090 9906 18021 18022 18081 18082 21030 22000 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

* These ports are enabled once Fiery Command WorkStation version 6.2 and later is installed on an external Fiery server.

Other TCP ports, except those specified by the OEM, 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.

The local administrator can define SNMP read and write community names and other security settings.

3.2 IP Filtering

The Administrator can restrict authorized connections with the Fiery server from those hosts whose IP addresses fall within a particular IP range. Commands or jobs sent from non-authorized IP addresses are ignored by the Fiery server.

3.3 Network Encryption

3.3.1 IPsec

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

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

Once 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.

3.3.2 SSL and TLS

SSL/TLS are application-level protocols used for transmitting messages over the Internet securely. Fiery servers support SSL v2/v3 and TLS v1 protocols.

Various Fiery server features support SSL/TLS. Users can access Fiery server's home page and Web APIs securely

over SSL/TLS. Connection to LDAP servers and email servers can be configured to work over SSL/TLS to ensure secure communication.

3.3.3 Certificate Management

Fiery servers provide a Certificate Management interface to manage the certificates used in various SSL/TLS communications. It supports the X.509 certificate format.

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 store.

3.4 IEEE 802.1x

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

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

Fiery server authenticates at boot time or when the Ethernet cable is disconnected and reconnected.

3.5 SNMP v3

The Fiery server supports SNMPv3 as it is a secured network protocol for managing devices on IP networks. SNMPv3 communication packets can be encrypted to ensure confidentiality. It also ensures message integrity and authentication.

The Fiery Administrator can select from three levels of security in SNMPv3. The Fiery Administrator also has the option to require authentication before allowing SNMP transactions and to encrypt SNMP user names and passwords.

3.6 Email Security

The Fiery server supports the POP and SMTP protocols. To protect the service against attack and improper use, the Fiery Administrator can enable additional security features such as the following:

3.6.1 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.

3.6.2 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.

4 Access Control

4.1 User Authentication

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

- Authenticate user names.
- 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 via LDAP.
- Fiery-based: users defined on the Fiery server.

The Fiery server authorizes a users' actions based on their group membership. Each group is associated with a set of privileges (e.g., Print in B&W, Print in color or B&W), and the actions of group members are limited to those privileges.

The Fiery Administrator can modify the privileges of any Fiery Group with the exception of the Administrator, Operator and Guest accounts.

For this version of User Authentication, the different privilege levels that can be edited or selected for a group are as follows:

- Print in B&W — This privilege allows group members to print jobs on the Fiery server. If the user does not have the "Print in Color and B&W" privilege, the Fiery server forces the job to print in black and white (B&W).
- Print in Color and B&W — 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 servers. Without this or the Print in B&W 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/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.

Note: User Authentication replaces Member Printing/Group Printing features.

4.2 Fiery Software Authentication

The Fiery server defines Administrator, Operator and Guest users. These users are specific to the Fiery software and are not related to Windows-defined users or roles. It is recommended that Administrators require passwords to access the Fiery server. Additionally, EFI recommends that the Administrator change the default password to meet the end user's security requirements.

The three users on the Fiery server allow access to the following privileges:

- Administrator — Gets full control over all of the Fiery server's functionalities.
- Operator — Has most of the same privileges as the Administrator, but has no access to some server functions, such as set-up, and cannot delete the job log.
- Guest (default; no password) — Has most of the same privileges as the Operator but cannot access the job log, cannot make edits and cannot make status changes to print jobs and preview jobs.

5 Operating System Environment

5.1 Start-up Procedures

The operating system and Fiery system software are loaded from the local HDD during startup.

The BIOS resident on the Fiery motherboard is read-only and stores the information needed to boot up the operating system. Changes to the BIOS (or removal of the BIOS) prevent the Fiery server from functioning properly.

The Configuration Page lists the values specified during setup. Some information, such as FTP proxy information, password information, and SNMP Community Names, are not included on the Configuration Page.

5.2 Linux

Linux systems do not include a local interface that allows access to the operating system.

5.2.1 Linux Antivirus Software

The Linux operating system used on Fiery servers is a dedicated OS for Fiery servers only. It has all of the OS components needed by a Fiery server, but not some of the general-purpose components for Linux systems, such as Ubuntu. In addition to having better performance, this dedicated OS is not subject to the same virus vulnerability as a general-purpose Linux system and Microsoft OS. The antivirus software designed for a general-purpose Linux OS may not be able to run on Fiery servers.

5.3 Windows 10

The Fiery server ships with a default Windows 10 administrator password. It is recommended that the administrator change the password upon installation. It is also highly recommended to change the password regularly in compliance with the organization's IT policy. The administrator password gives a user full access to the Fiery server locally and/or from a remote workstation. That includes, but is not limited to, the file system, system security policy and registry entries. In addition, this user can change the administrator password, denying anyone else access to the Fiery server.

5.3.1 Microsoft Security Patches

Microsoft regularly issues security patches to address potential security holes in the Windows 10 operating system. The default setting of Windows Update to notify users of patches without downloading them is disabled. As a result, the Windows Update status is not up to date. Clicking on "Check for updates" enables the automatic updates and starts the update immediately.

5.3.2 Windows Update Tools

Windows-based Fiery servers are capable of using 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. EFI has its own dedicated system update tool to handle Fiery software patches.

5.3.3 Windows Antivirus Software

In general, 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 particular threat. Here are a few guidelines to help customers have confidence in the antivirus software they choose. Please note that antivirus software is most useful in a local FACI kit configuration, where users have the potential to infect the Fiery server with a virus through standard Windows actions. For Fiery servers without a FACI kit, it is still possible to launch antivirus software on a remote PC 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. The following are the EFI guidelines for each of the components of Windows antivirus software:

Virus engine — When an antivirus engine scans the Fiery server, regardless of whether it's a scheduled scan or not, it may affect Fiery performance.

Antispyware — An antispyware program may affect Fiery performance when files are coming into a Fiery server. Examples are incoming print jobs, files that download during a Fiery System Update or an automatic update of applications running on a Fiery server.

Built-in firewall — Since the Fiery server has a firewall, antivirus firewalls are not generally required. EFI recommends that customers work with their own IT department and refer to section 3.1 of this document if there is a need to install and run a built-in firewall that comes as part of antivirus software.

Antispam — Fiery supports print-via-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 antispam component is not required because running a separate email client (such as Outlook) on the Fiery server is not a supported operation.

Whitelist and blacklist — The whitelist and blacklist functionalities should not typically have adverse effects on the Fiery server. EFI strongly recommends that the customer configure this functionality so that it does not blacklist Fiery modules.

HID and application control — Because of the complex nature of HID and application control, the antivirus configuration must be tested and carefully confirmed when either of these features is in use. When tuned properly, HID and application control are excellent security measures and coexist with the Fiery server. However, it is very easy to cause server issues with the wrong HID parameter settings and wrong file exclusions — many times caused by "accepting the defaults." The solution is to review the selected options in HID and/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.

5.4 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 via email are treated as PDL jobs. Please see the details on Fiery email printing workflow in Section 6.4 in this document.

6 Data Security

6.1 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. NIST 2010 compliant cryptographic algorithms are used.

6.2 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. With passwords enabled on the Fiery server, this feature limits printing to Fiery Operators and Administrators.

6.2.1 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 drive until the user submits the job for printing or deletes the job using a job management utility, such as the Fiery Command WorkStation, Fiery Command WorkStation ME or Clear Server.

The Sequential Print Queue allows the Fiery 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 can get out of order due to many factors, such as the Fiery allowing smaller jobs to skip ahead while larger jobs are spooling.

6.2.2 Printed Queue

Jobs sent to the Print Queue are stored in the Printed Queue on the Fiery server, if 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.

6.2.3 Direct Queue (Direct Connection)

Direct Queue is designed for font downloading and applications that require direct connection to PostScript module in Fiery controllers.

EFI does not recommend printing to the Direct Queue. Fiery deletes all jobs sent via the direct connection after printing. However, EFI does not guarantee that all temporary files relating to the job will be deleted.

Jobs of VDP, PDF or TIFF file types are rerouted to the Print Queue when sent to the Direct Queue. Jobs sent via the SMB network service may be routed to the Print Queue when sent to the Direct Queue.

6.2.4 Job Deletion

When a job is deleted from the Fiery automatically or using Fiery tools, the job cannot be viewed or retrieved using Fiery tools. If the job was spooled to the Fiery HDD, the job's elements may remain on the HDD and could theoretically be recovered with certain tools, such as forensic disk analysis tools.

6.2.5 Secure Erase

Secure Erase is designed to remove the content of a submitted job from the Fiery HDD whenever a Fiery function deletes a job. At the instance of deletion, each job source file is overwritten three times using an algorithm based on US DoD specification DoD5220.22M.

The following limitations and restrictions apply to Secure Erase:

- It does not apply to job files located in systems other than the Fiery server, such as the following:
  - Copies of the job load balanced to another Fiery server.
  - Copies of the job archived to media or network drives.
  - Copies of the job located on client workstations.
  - Pages of a job merged or copied entirely into another job.
- It does not delete any entries from the job log.
- If the system is manually powered off before a job deletion has completed, there is no guarantee that the job will be fully deleted.
- Jobs deleted before this feature is enabled are not securely erased.
- It does not delete any job data that may have been written to disk due to disk swapping.
- It disables automatic defragmentation on Windows OS. If enabled, the OS could move job data around as it defragments. In that case, portions of the job data in the original location might not be overwritten for a secure erase.
- Jobs submitted through an FTP server may be saved by the FTP client before being passed to the Fiery system software. Because the Fiery system software has no control over this process, the system cannot securely erase the jobs saved by the FTP client.
- Jobs printed via SMB go through the spooler on the Fiery, which saves the jobs to disk. Because the Fiery system software has no control over this process, the system cannot securely erase these jobs.

Note: Disk swapping occurs to create more virtual memory than there is physical memory. This process is handled in the operating system layer, and the Fiery server has

no control over it. However, disk swap space is regularly rewritten during the operating system operation as various segments of memory are moved between memory and disk. This process can lead to some job segments being stored to disk temporarily.

6.2.6 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 HDD and is not specifically overwritten.

6.3 Secure Print

The Secure Print function requires the user to enter a job-specific password at the Fiery server to allow the job to print. This feature requires an LCD interface local to the Fiery server.

The feature's purpose is to limit access to a document to a user who (a) has the password for the job and (b) can enter it locally at the Fiery server.

6.3.1 Workflow

The user enters a password in the Secure Print field in the Fiery Driver. When this job is sent to the Fiery server's 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 Fiery Command WorkStation or Fiery Command WorkStation ME.

From the Fiery LCD, the user enters a Secure Print window and enters a password. The user can then access the jobs sent with that password and print and/or delete the jobs.

The printed secure job is not moved to the Printed Queue. The job is deleted automatically, once it has finished printing.

6.4 Email Printing

The Fiery server receives and prints jobs sent via 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 Administrator can turn off the email printing feature. The email printing feature is off by default.

6.5 Job Management

Jobs submitted to the Fiery server can only be acted upon by using a Fiery job management utility with either Administrator or Operator access. Guest users (those users with no password) can view the file names and job attributes but can neither act upon nor preview these jobs.

6.6 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 Fiery Command WorkStation. A user with Administrator access can delete the job log from the Fiery Command WorkStation. A user with Guest access can print the job log from the Fiery LCD only if this access is granted by the Administrator.

6.7 Setup

Setup requires an administrator password. The Fiery server can be set up either from the Fiery Configure tool or from setup in Fiery LCD. The Fiery Configure tool can be launched from the Fiery WebTools and Fiery Command WorkStation.

6.8 Scanning

The Fiery server allows an image placed on the copier glass to be scanned back to the workstation that initiated the scan using a Fiery TWAIN plug-in. The plug-in is supported with the Adobe® Photoshop and Textbridge applications. 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.

Scan jobs can be distributed via the following methods:

- Email — In this process, an email is sent to a mail server, where it is routed to the desired destination. Note: If the file size is greater than the Administrator-defined maximum, the job is stored on the Fiery HDD, which is accessible through a URL.
- FTP — The file is sent to a FTP destination. A record of the transfer, including the destination, is kept in the FTP log, which is accessible from the LCD Print Pages command. An FTP Proxy Server can be defined to send the job through a firewall.
- Fiery Hold Queue — The file is sent to the Fiery Hold Queue (see 6.2.1 section above) and is not kept as a scan job.
- 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. The user needs to enter the correct mailbox number to access the stored scan job. Some Fiery server versions also require a password. The scan job is retrievable through a URL.

7 Conclusion

EFI offers a robust set of standard features and options on the Fiery server to help our customers meet the need for a comprehensive and customizable security solution for any environment. EFI is committed to ensuring that our customers' businesses run at top efficiency and effectively protect the Fiery server against vulnerabilities from either malicious or unintentional use. Therefore, EFI is continually developing new technologies to provide comprehensive and reliable security solutions for the Fiery server.

6750 Dumbarton Circle
Fremont, CA 94555
650-357-3500
www.efi.com

GVP.057.06.17_US