Fiery Security White Paper

Fiery System 10, Version 2.54

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 System 10. 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 Electronics For Imaging (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 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 secuity procedures, to achieve overall system security.

1.2 Configure the Security Feature via Fiery Configure

An Administrator of a Fiery server 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 Non-Volatile Memory and Data Storage

The Fiery server contains serveral types of non-volatile 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 on 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® 7 Professional Server via the FACI (local monitor, keyboard and mouse) kit 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 job management information is created, 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, so image data becomes inaccessible.

To protect the image data from unauthorize access, EFI provides a Secure Erase feature (see section 6.2.4). Once enabled by the system adminstrator, the selected operation is carried out at the appropriate time to securely erase deleted data on 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 via the FACI kit (if enabled on a Windows 7 Professional server) or via the Fiery LCD on Fiery servers. Security access on the Fiery Server with FACI kit is controlled through 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 provides the user with the ability to lock the server drive(s) into the system for normal operation and the ability 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.

2.5 Dongles

A dongle is a small piece of hardware that connects to a laptop or desktop computer for the purpose of copy protection or authentication of software to be used on that system.

2.5.1 HASP USB Dongles

EFI HASP dongles are specifically programmed only for software protection or for feature activation.

EFI HASP dongles are encrypted. The user cannot write information to the dongles without the authorized APIs and tool kits, which come in separate packages available to vendors. Please visit http://www.safenet-inc.com/Products/Detail.aspx?id=2147483970&terms=hasp+dongle to learn more about HASP dougles.

2.5.2 EFI ES-1000 Spectrophotometer Dongle

The ES-1000 spectrophotometer is not a USB dongle. Although it is a USB device, the EEPROMS specifically have been programmed using advanced APIs and toolkits, which are available only from the manufacturer. They do not contain encryption.

They cannot be used to store, transfer information or data, or be used for any other purpose other than as a software protection mechanism for the Fiery Color Profiler Suite.

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.

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 7 Professional only)
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
6310 8010 8021-8022, 9906, 18021, 18022, 18081, 18082 21030. 22000 50006 - 50025	9906	EFI ports	Command WorkStation 4 and 5, Fiery Central, EFI SDK-based tools, Fiery Printer Driver bi-di functions, WebTools, and Fiery Direct Mobile Printing, and Native Document Conversion.
3389		RDP	Remote Desktop (Windows Fiery servers only)
9100-9103		Printing Port	Port 9100

Other TCP ports, except those specified by the OEM, are disabled. Any service depen¬dent 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 protocol used for transmitting messages over the Internet securely. The Fiery server secures http, email and LDAP communication with SSL v2/v3 and TLS.

The Fiery server uses Lightweight Directory Access Protocol (LDAP) to get user and group information from the Active Directory. Simple LDAP authenticaion is in clear text, so it is unsecure. The Adminstrator can secure the LDAP traffic by enabling SSL/TLS option on Fiery server.

The Fiery server provides the Adminstrator options to enable SSL/TLS to establish secure communication with an email server.

The Fiery server requires a certificate for LDAP communication over SSL or TLS. The Fiery server only supports importing certificates and does not support certificate generation for SSL.

3.3.3 Certificate Management

Certificates are used by the network clients to authenticate themselves in network activities that perform identity verifications. The certification method is supported by SSL/TLS that implements authentication through the exchange of certificates based on public/private keys according to the X509 standard.

In the Fiery server, certificate management allows the Fiery Administrator to do the following:

- Add, load or browse for available digital certificates created by a trusted authority and private keys.
- Create self-signed digital certificates.
- View details for available digital certificates.
- Assign or associate an available digital certificate for a particular service, such as Web Services.
- Add trusted certificates created by a trusted authority.

3.4 IEEE 802.1x

802.1x is an IEEE standard protocol for port-based network access control. This protocol provides authentication to devices attached to a LAN port and establishes a point-to-point connection only if authentication is successful.

When 802.1x is enabled, the Fiery server uses one of the two EAP methods to seek authentication from an 802.1x authentication server (such as a RADIUS server), often through an intermediate access point (an authenticator). The Fiery server seeks this authentication at start-up time or when the Ethernet cable is disconnected and reconnected. Once authenticated, the Fiery server is granted access to the network.

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 using 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 follows.

3.6.1 POP before SMTP

Some email servers still support unsecure SMTP protocol that allows anyone to send email without authentication. To prevent unauthorized access, the Fiery server supports the ability for the Administrator to enable or disable the POP authentication before SMTP. POP authentication before SMTP forces a successful login to a POP server prior to being able to send email via SMTP.

3.6.2 OP25B

Outbound Port 25 Blocking (OP25B) is an anti-spam ISP measure by which the ISP checks the IP address and the port number of all accesses through its routers and blocks access to port 25 from dynamic IP addresses on its network. The Fiery server provides the Administrator the ability to specify different port numbers besides 25 for outgoing email service.

4 Access Control

4.1 User Authentication

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

- 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 actions based on the privileges defined for a Fiery group, which the user is a member. Fiery Groups are groups of users with a predefined set of privileges. The Fiery Group assigns a set of privileges to a collection of users.

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

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. Without this or the Print in B&W privilege, 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 only with the mailbox username/password.

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

4.2 Fiery Software Authentication

The Fiery server defines Administrator, Operator, and Guest users with different privileges. 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 a different password as defined by the end user's security requirements.

The three levels of passwords on the Fiery server allow access to the following functionality:

- Administrator – Gets full control over all the Fiery server's functionality.
- Operator – Has the same privileges as the Administrator, except he/she has no access to some server functions, such as set-up, and cannot delete the job log.
- Guest (default; no password) – Has the same privileges as Operator, except he/she cannot access the job log, cannot make edits or 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 set-up. 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 Anti-Virus Software

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

5.3 Windows 7 Professional

The Fiery server ships with a default Windows 7 Administrator password. It is recommended for the administrator to change the password upon installation. It is also highly recommended to change the password regularly to comply with the organization's IT policy. 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 and to deny 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 7 operating system. The default setting of Windows Updates is to notify users of patches and not to automatically download updates. The Fiery Administrator can change the default setting in Windows Update or manually install the security patches. Microsoft tools such as SCCM, SMS and WSUS can also be used to push Microsoft Security Patches to the Windows based Fiery systems.

5.3.2 Windows Anti-Virus Software

Administrators can install anti-virus software on Fiery servers with FACI kits. A local GUI is required for proper configuration of anti-virus software. Anti-virus software is most useful in a local GUI 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 anti-virus software on a remote PC and scan a shared Fiery hard drive. However, EFI suggests that the Fiery administrator work directly with the anti-virus software manufacturer for operational support.

EFI tests Fiery products with McAfee VirusScan software. Similar products from Symantec and TrendMicro also are compatible with the Fiery server when used as described above.

EFI supports the use of anti-virus solutions as long as they are used in accordance with this specification. EFI does not support or give any warranty regarding the efficacy of any anti-virus software.

5.3.2.1 Anti-Virus Software Configuration

The anti-virus software should be configured to scan for files coming into the Fiery server outside of the normal print stream. This includes:

- Removable media.
- Files copied to the Fiery server from a shared network directory.

The anti-virus software also can be configured to scan all Fiery files when the Fiery server is not planned for use for an extended period of time. The administrator should only run the anti-virus software manually when the Fiery server is idle and not receiving or acting upon a job.

5.3.2.2 Non-FACI Systems

For non-FACI based Fiery servers , the system is running on Microsoft operating system. EFI recognizes that the Fiery server still must meet the companies' anti-virus standards. The administrator can enable the remote desktop in Fiery WebTools configure. The administrator is able to manage the non-FACI system using remote desktop and install the appropriate anti-virus software required by the company.

5.4 Email Viruses

Typically, viruses transmitted via e-mail 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 e-mail in RTF or HTML or any included JavaScript. Aside from an e-mail response to a specific user based on a received command, all files received via e-mail are treated as PDL jobs. Please see the details on Fiery e-mail 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. 256-bit AES (Advanced Encryption Stanard) algorithm is used.

6.2 Standard Printing

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

- Hold Queue.
- Print Queue.
- Direct Queue (Direct Connection).
- Virtual Printers (custom queues defined by the Fiery Administrator).

The Fiery Administrator can disable the Print and Direct queues to limit automatic printing. With passwords enabled on the Fiery server, this feature limits printing to Fiery Operators and Administrators.

6.2.1 Hold and Print Queues

When a job is printed to the Print 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.

6.2.2 Printed Queue

Jobs sent to the print queues 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.

6.2.3 Direct Queue (Direct Connection)

Direct Queue provides the user with additional data security as jobs sent to the Direct Queue cannot be opened, viewed, edited or reprinted by other users. Only one person can be printing to the direct queue at a time. A job sent to the Direct Queue is processed as soon as the current job finishes processing and skips other jobs waiting to be processed.

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.

Jobs sent via the Direct queue are not normally stored on disk with the following exceptions:

- The job is instructed to use reverse order printing, and it exceeds the available printer memory.
- The system memory may overflow to use the swap partition on the HDD as a memory buffer.

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 not located in systems other than the Fiery server, such as:
  - 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 finished, there is no guarantee that the job will be fully deleted.
- It does not delete any job data that may have been written to disk due to disk swapping and disk caching.
- Jobs submitted through 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 when memory needs to be swapped to disk 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 re-written 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

Processing of some files may write some job data to the operating system memory. In some cases, this memory may be cached on 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'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 an 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 E-mail Printing

The Fiery server receives and prints jobs sent via e-mail. The Administrator can store a list on the Fiery server of authorized e-mail addresses. Any e-mail received with an e-mail address that is not in the authorized e-mail address list is deleted. The Administrator can turn off the e-mail printing feature. The e-mail 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, when the job is carried out, characteristics of the job in terms of paper used, color, etc. 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 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 setup either from 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:

- E-mail – In this process, an e-mail 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. A 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 Printing 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 sever to help our customers meet the need for a comprehensive and customizable security solution for any environment. EFI is committed to ensuring our customers' businesses run at top efficiency and effectively protect the Fiery server deployed against vulnerabilites from either malicious or unintenational use. Therefore, EFI is continually developing new technologies to provide comprehensive and reliable security solutions for the Fiery server.

303 Velocity Way
Foster City, CA 94404
650-357-3500
www.efi.com

05/19/11