Fiery Security White Paper

System 9 R2

Version 2.2

Date of Issue: 3/30/2010

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 9 R2. It covers hardware, the network, 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 be extra safe.

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® XP Pro Server via the FACI 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

The Hard Disk Drive (HDD) can contain the following data:

- System software.
- Font data.
- User information (including password).
- Address book.
- Image data.
- Job log.

During normal print and scan operations, image data is written to a random area on the hard drive, and job management information is created.

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. However, the image data remains in its stored area until it's reused.

To protect the image data from unauthorize access, EFI provides a Secure Erase feature (see section 6.2.5). Once set, the selected operation is carried out at the appropriate time. Alternatively, the operation can be carried out as set by the system administrator.

2.3 Physical Ports

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

Fiery Ports	Function	Access
Interface Ports	Copier/printer connection (DDI)	
Serial Port	Software maintenance interface (embedded Linux system only)	
Ethernet RJ-45 connector	Ethernet connectivity	Network connections (see printing and network connections below)
Copier interface connector	Print/Scan	Dedicated for sending/receiving to/from the print engine
USB Port	USB device connection	Plug and play connector designed for use with optional removable media devices

2.4 Local Interface

The user can access the Fiery functions via the FACI kit (if enabled on a Windows XP Pro server) or via the Fiery LCD. The Windows administrator password is used to control access to the Fiery server if the FACI kit is enabled. The Fiery LCD only provides access to the Fiery functionality.

2.5 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.

2.5.1 For External Servers

Fiery servers support a generic 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.

2.5.2 For Embedded Servers

Embedded products can only offer removable HDD as an OEM coordinated option because the mounting location and brackets for the MFP must be developed jointly with the OEM. The normal internal drive can be remotely mounted externally on the MFP in a removable drive enclosure as an option.

2.6 Dongles

2.6.1 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.aladdin.com/hasp/default.aspx for more information on the dongles.

2.6.2 ES-1000 Spectrophotometer Dongle

The ES-1000 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

3.1 Network Ports

The Fiery serverallows the user to selectively enable and disable the following IP ports:

TCP	UDP	Port Name	Dependent Service(s)
20-21		FTP	
80		HTTP	WebTools™, IPP
135		MS RPC	Microsoft® RPC Service (Windows XP Pro only)
137-139		NETBIOS	Windows Printing
	161, 162	SNMP	WebTools, Velocity, some legacy utilities, other SNMP-based tools
	427	SLP	
443		HTTPS	
445		SMB/IP	SMB over TCP/IP
	500	ISAKMP	
515		LPD	LPR printing, some legacy utilities (such as WebTools, older versions of CWS)
631		IPP	IPP
	4500	IPSec NAT	
	5353	Multicase DNS	
8021-8022, 21030	9906	Harmony	CWS4, Velocity, EFI SDK-based tools, Fiery Printer Driver bi-di functions
3389		RDP	Remote Desktop
9100-9103		Printing Port	Port 9100

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.

3.1.1 MAC Address Filtering

The administrator can configure the Fiery server to allow or reject connections over ethernet based on the Media Access Control (MAC) address of the sender. The administrator can specify a list of MAC addresses on the Fiery serverand define whether or not the Fiery server should reject all ethernet connections from these MAC addresses or accept only those ethernet connections from these MAC addresses.

The following limitations apply to this feature:

- It is possible for individuals to spoof a client MAC addresses and bypass this security.

- If a router connects to the Fiery server, any client that connects to that router can bypass any MAC Address limitations since the Fiery server can decide whether or not to accept or reject communication forwarded through the router by the router's MAC Address.

3.1.2 IP Filtering

The administrator can restrict authorized connections with the Fiery serverfrom 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.

3.2 Network Encryption

3.2.1 IP Sec

IP Sec or IP Security Protocol provides security to IP protocols through encryption and authentication mechanisms. IP sec in the Fiery server allows the server to accept incoming data that supports IP sec using pre-shared key authentication method.

The pre-shared authentication keys are used strictly for establishing trust — not for application data packet protection.

3.2.2 LDAP Over SSL and TLS

SSL is a protocol for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. Most of today's browsers support SSL. The Fiery serversupports SSL v2/v3. In the Fiery, SSL creates a secure connection for transmitting data between the client and the server.

Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eaves drop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

TLS is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides connection security with some encryption method, such as the Data Encryption Standard (DES). The TLS Record Protocol also can be used without encryption. The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged.

The Lightweight Directory Access Protocol (LDAP) is used to read from and write to the Active Directory. By default, LDAP traffic is transmitted unsecured. For LDAP communication over SSL or TLS, the client would need a certificate.

Installing a valid certificate on a domain controller permits the LDAP service to listen for and automatically accept connections for LDAP and global catalog traffic. This results in communication that is confidential and secure.

Note: The Fiery server only supports importing certificates. The Fiery server does not support certificate generation for SSL.

3.2.3 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 Secure Socket Layer/Transport Layer Security (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 admininstrator 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.

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 servercan 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 admininstrator, 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 be 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 serverallow 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.

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 operating system is a dedicated operating system that does not have all the functionality of a complete operating system. The Fiery server was not designed to accept certain applications, such as virus protection software, as part of its operational model. This feature intentionally was created to prevent the loading of potentially malicious software on the units and to control the impact of these applications on the system's operation and performance.

5.3 Windows XP Pro

The Fiery server ships with a default Windows XP Pro Administrator password. It is recommended for the administrator to change the password upon installation. Without an administrator password, all users have full access to the machine locally and/or from a remote workstation. This feature includes, but is not limited to the file system, system security policy, and registry entries. In addition, this feature allows anyone to change the administrator password and to deny access to the Fiery server.

If the Windows administrator password is enabled and not entered into the system, the user is prohibited from accessing the Fiery server from a FACI kit. The Fiery system software functions normally, and users can access Fiery server features from standard Fiery tools.

Some product settings are stored in the Windows registry. None of the entries are encrypted except for the network configuration, which includes Novell passwords. Set-up information, such as the Fiery Administrator password or Fiery Operator password, is stored in the registry as plain text.

5.3.1 Microsoft Security Patches

Microsoft regularly issues security patches to address potential security holes in the Windows XP operating system. The Automatic Updates in Security Center are designed to notify users of these patches but don’t download automatically. The Fiery administrator has to manually install the secuirty patches if it is not set to automatic install.

5.3.2 SMS Tools

EFI has its own dedicated system update tool for its Windows-based systems. This tool handles the retrieval of all applicable MS security patches and Fiery software updates. The Fiery server

does not support any third-party SMS tools for retrieving and pushing updates to the Fiery server.

5.3.3 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 Fierys without a FACI kit, it is still possible to launch anti-virus software on a remote PC and scan a shared Fiery hard drive, if EFI supports this configuration or workflow. 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.

5.3.3.1 Anti-Virus Software Configuration

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

- Removable media.
- Files copied to the Fiery serverfrom 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.

5.3.3.2 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 WT 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 serverensures that all passwords and related configuration information are secure when stored in the Fiery server. The encryption method used is based on the TwoFish method/algorithm of encryption.

6.1.1 Cryptographic Algorithms and Key Lengths

For encrypting sensitive information, EFI client applications use an implementation of the Twofish encryption algorithm. Twofish is a symmetric block cipher developed by Counterpane Labs and is one of the five finalists for the NIST's Advanced Encryption Standard. EFI client applications use Twofish with a 256-bit key in Cipher Feedback (CFB) mode (Twofish: 128 bit block, 16 rounds and a 256-bit key).

Note: The Fiery server and EFI client applications do not use proprietary encryption algorithms.

6.1.2 Key Management and Algorithms

To generate keys used for Twofish encryption, the Fiery server and EFI client applications use the Diffie-Hellman key agreement protocol. Our Diffie-Hellman implementation uses a 28 bit modulus and generates a 32 bit shared secret key. This 32 bit shared secret key is then used to generate a 256-bit key for Twofish (that is, given the 32 bit shared secret key X, the generation algorithm always produces the same 256 bit key Y).

6.2 Standard Printing

Jobs submitted to the Fiery serverare 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. The product does not prevent users from filling up the hard disk by submitting an excessive quantity of print jobs. If the hard disk fills up, the Fiery server does not accept new jobs.

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 Command WorkStation®, 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)

Jobs sent to the direct queue may be written to the Fiery HDD and have the following characteristics:

- Process as soon as the current job finishes processing and skip other waiting to be process jobs.
- The Fiery server receives and processes one page of the job at a time from the client. The connection with the client remains open until all pages are processed by the Fiery.
- Are not written to the printed queue. However, they appear in the job log.

Note: Only one person can be printing to the direct queue at a time.

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.

6.2.5 Secure Erase

Secure erase is an optional feature that can be enabled by the Fiery administrator.

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:

- 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.
- 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.
- 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.

Note: Disk caching is set to ON for servers; thus, the job file is overwritten three times in the cache and may only be overwritten one time on the drive itself depending on the cache flushing algorithm.

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 Command WorkStation or 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 print job is not moved to the Printed queue. The job is deleted automatically, once it has finished printing.

Note: The secure print password string in the job is not encrypted and can be read from the print job.

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.

The Fiery client utilities do not use encryption when communicating with the Fiery server. Set-up information, such as the Fiery Administrator passwords, Fiery Operator passwords, and Novell passwords, are sent to the Fiery server in plain text.

6.6 Job Log

The job log is stored on the Fiery server. Individual records of the job log cannot be deleted.

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. A user with guest access can print the job log from the Fiery LCD on certain Fiery servers. Other Fiery servers require administrator access to print the job log from the LCD.

An individual can create a tool based on the EFI SDK to retrieve, export, print or delete the job log from the Fiery server.

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 WebTools and 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 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.