EFI™ WHITE PAPER SERIES

Fiery® Security White Paper

Fiery FS350 Pro/FS350 Servers

DATE OF ISSUE:
JULY, 2020

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 FS350/FS350 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 Fiery 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 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 NX station using the 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 and solid state 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) and solid state drive (SSD).

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

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. The secure erase feature is not supported on the data saved on SSD.

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	Using 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 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.
Optical fiber connector	10Gb Ethernet connectivity	Network connections	N/A

2.3 Local interface

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

2.4 Removable HDD kit option

The Fiery server supports a removable HDD 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 HDD 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 Fiery partners.

2.4.2 For Fiery XB servers

The HDD/SSDs are removable on Fiery XB servers. Most of HDD/SSDs 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.

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.

By default, port filtering is enabled. Filtering a port prevents users outside the Fiery server from connecting to the Fiery server using the specified ports. If the port is unblocked, users are allowed to connect to that port.

Other TCP ports, except those specified by the Fiery partner, are disabled. Any service dependent on a disabled port cannot be accessed remotely.

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
	4500	IPsec NAT	IPsec
	5353	Multicase DNS	Bonjour
3389		RDP	Remote Desktop (Windows Fiery servers only)
3702	3702	WS-Discovery	WSD
8021, 8022, 9906	9906	EFI ports	Command WorkStation 5 and 6, Fiery Central, Fiery Printer Driver bi-di functions, WebTools.
8010, 6310			Fiery Direct Mobile Printing
21030			Fiery ImageViewer
8090			Fiery Software License
50006-50025*			Fiery XF
9100-9103	9906	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 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. The local Administrator can define SNMP read and write community names and other security settings.

3.2 IP filtering

IP filtering allows the Administrator to set a default policy to allow or deny all incoming packets. In addition, up to 16 IP addresses or ranges can be configured to override the default policy. A filter policy of "deny" will drop those packets that match any of the IP filter rules, and a default policy of "allow" will accept such packets.

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 TLS

The Fiery server requires a secure connection between clients and different server components. TLS is used to encrypt communications between the two end points. HTTPS over TLS is required when connecting to the Fiery server from WebTools and Fiery API. These communications are encrypted with TLS 1.2 and TLS 1.1. TLS 1.0 and SSL v3 has been disabled and thus all incoming connection requests using these protocols will be denied.

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 SMB

Server Message Block (SMB) is a network protocol to provide shared access to files and printers. SMB v1 is disabled on Fiery servers as it is not secure. 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.

3.5 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.

3.5 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, PEAP-MSCHAPv2 or EAP-TLS to authenticate to an 802.1x authentication server.

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

3.6 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.

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.

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

3.7 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.

3.7.1 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.

3.7.2 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.

3.8 Fiery XB network diagram

Please refer to the Addendum 1 for more information on how Fiery XB servers and high-speed inkjet printers connect to the network.

4. Access control

4.1 User authentication

The Fiery server 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 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 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 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 grayscale: This privilege allows group members to print jobs on the Fiery server. If the user does not have the "print in color and grayscale" privilege, the Fiery server forces the job to print 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 servers. 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/ 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/ group printing features.

4.2 Fiery software 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 Administrators require passwords to access the Fiery server.

Additionally, EFI recommends that the Administrator change the default password to meet the security requirements in that print environment.

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

- 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
- Press Operator (Fiery XB servers only): Has the privilege to manage jobs on the press. The Administrator can add specific privileges to this user type.
- 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. Software security updates

5.1 Security update services

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

To update Fiery software, Fiery servers periodically contact the EFI cloud service to check for the latest updates and download the necessary ones.

EFI has dedicated system tools to handle Fiery software updates such as:

- Fiery Updates in Command WorkStation: Administrators get notifications, downloads, and installation of approved and released Fiery system updates.
- Fiery Software Manager: This client application automatically checks and downloads updates to Fiery client software applications.
- System Updates: This feature provides notifications, downloads, and installation of approved and released Fiery system updates.

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 embedded 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

External Fiery servers ship with Windows 10 IoT Enterprise 2016 LTSB edition (Windows 10) operating system which contains the latest security protections.

- Windows 10 comes with SMB hardening for SYSVOL and NETLOGON shares which help mitigate man-in-middle attacks for Fiery servers joined to a domain.
- Windows 10 has better memory protections for heap and kernel pools to help prevent exploitation of memory.
- Enable Windows Defender SmartSreen feature to prevent malicious applications from being downloaded. This additional security feature may affect Fiery server performance and is not turned on by default.
- Enterprise certificate pinning helps prevent man-in-the-middle attacks.
  This is an enterprise feature. Fiery server has to join a domain to enable the feature.
- Windows Defender Antivirus which helps keep devices free of virus and other malware.
  Fiery server is configured with the feature turned on to scan c:\, but not e:\ by default to minimize performance impact. Please configure Windows Defender to scan e:\ if desired.
- Windows Data Execution Prevention (DEP) can be enabled for the Windows programs and services to help prevent malware from using memory manipulation technique.

5.3.1 Microsoft Windows Update

Microsoft regularly issues security patches to address potential security holes in the Windows 10 operating system. The default setting of Windows Update on Fiery servers is to notify users of patches without downloading them. 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.

5.3.3 Windows antivirus software

Fiery servers use Windows 10 Defender, Microsoft's antivirus software, to protect Fiery servers. 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 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 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.
- 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 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 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.

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 servers.

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 server 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.

This feature is not supported on Fiery XB platforms.

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 jobspecific password at the Fiery server to allow the job to print.

This feature requires access from the printer's control panel. 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 printer's control panel.

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.

From the printer's control panel, 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.

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.

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 QuickTouch interface.
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. Guidelines for a secure Fiery configuration

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

- Change the default Fiery Administrator password in security to conform with password policy within your organization.
- SNMP in network -> SNMP:
  (a) Choosing maximum security makes the Fiery server to support only SNMP v3.
  (b) In case SNMP manager only works with SNMP v1/v2c, please change the default read community name.
- Disable FTP printing in job submission if it's not needed.
- Disable WSD in job submission.
- Disable Windows printing in job submission if using lpr, or port9100, or IPP to print.
- Block ports (enable TCP/IP port filter in security -> TCP/IP port filtering and uncheck ports 137-139 and 445 if you don't use Windows printing, and no need to access or share file folders.

In addition to OS-level protections, the Fiery server has additional security features to help protect your data:

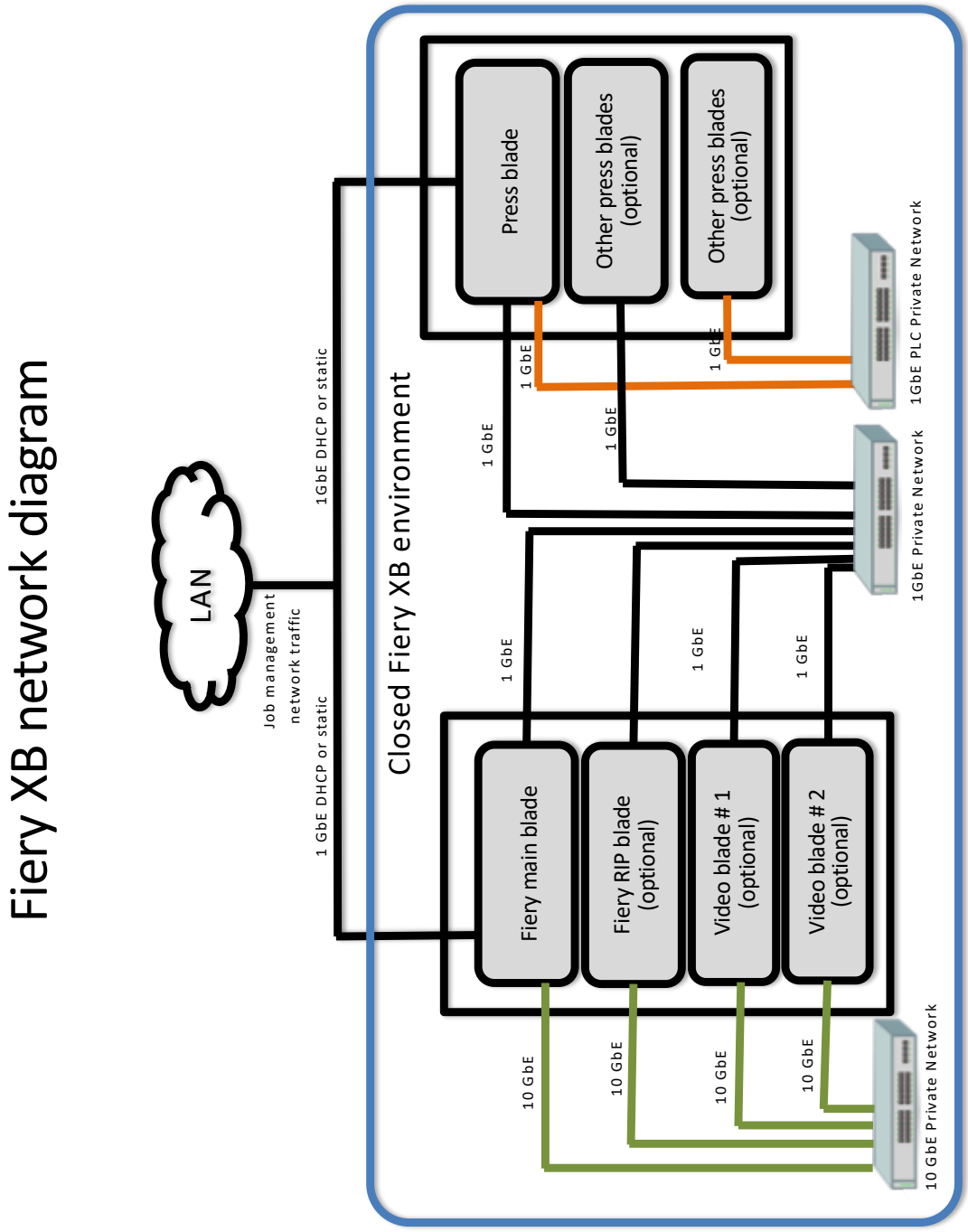
- Fiery servers come with secure print to ensure that what a user prints is picked up by that user.
- Fiery integrates with the leading job accounting solutions to include additional security through follow-me printing.

It is recommended that administrators 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 client. 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.

8. 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.

Addendum 1


Fiery XB network diagram
LAN
Job management network traffic
1GbE DHCP or static
1 GbE DHCP or static
Closed Fiery XB environment
Press blade
Other press blades (optional)
Other press blades (optional)
Fiery main blade
Fiery RIP blade (optional)
Video blade # 1 (optional)
Video blade # 2 (optional)
1 GbE
1 GbE
1 GbE
1 GbE
1 GbE
1 GbE
1 GbE
1 GbE
1GbE PLC Private Network
1GbE Private Network
10 GbE Private Network
10 GbE
10 GbE
10 GbE
10 GbE

Addendum 2

Windows 10 IoT Enterprise 2019 LTSC

Starting in 2019, some Fiery servers include Windows 10 IoT Enterprise 2019 LTSC as their operating system.

This Windows edition contains the latest security protections, and includes the cumulative feature 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. The main difference between these two versions is the licensing and distribution model.

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.

EFI fuels success.

We develop breakthrough technologies for the manufacturing of signage, packaging, textiles, ceramic tiles, and personalized documents, with a wide range of printers, inks, digital front ends, and a comprehensive business and production workflow suite that transforms and streamlines the entire production process, increasing your competitiveness and boosting productivity. Visit www.efi.com or call 650-357-3500 for more information.

FTL 061.06.20