Xerox® IJ Print Server Powered By Fiery®

Information Assurance Disclosure

January 18, 2018

4517xxxx

1 Introduction

The purpose of the Information Assurance Disclosure (IAD) is to disclose information for products with respect to device information security. Device information security means how data is stored and transmitted, how the product behaves in a networked environment, and how the product can be accessed, both locally and remotely. This document describes design, functions, and features of Xerox products relative to Information Assurance (IA).

1.1 Product Name

Company	IOT Names	Fiery Marketing Names
Xerox®	**Xerox® Trivor. Inkjet Press and Xerox® Impika® Compact, Reference, and Evolution Inkjet Presses**	**Xerox® IJ Print Server Powered by Fiery®**

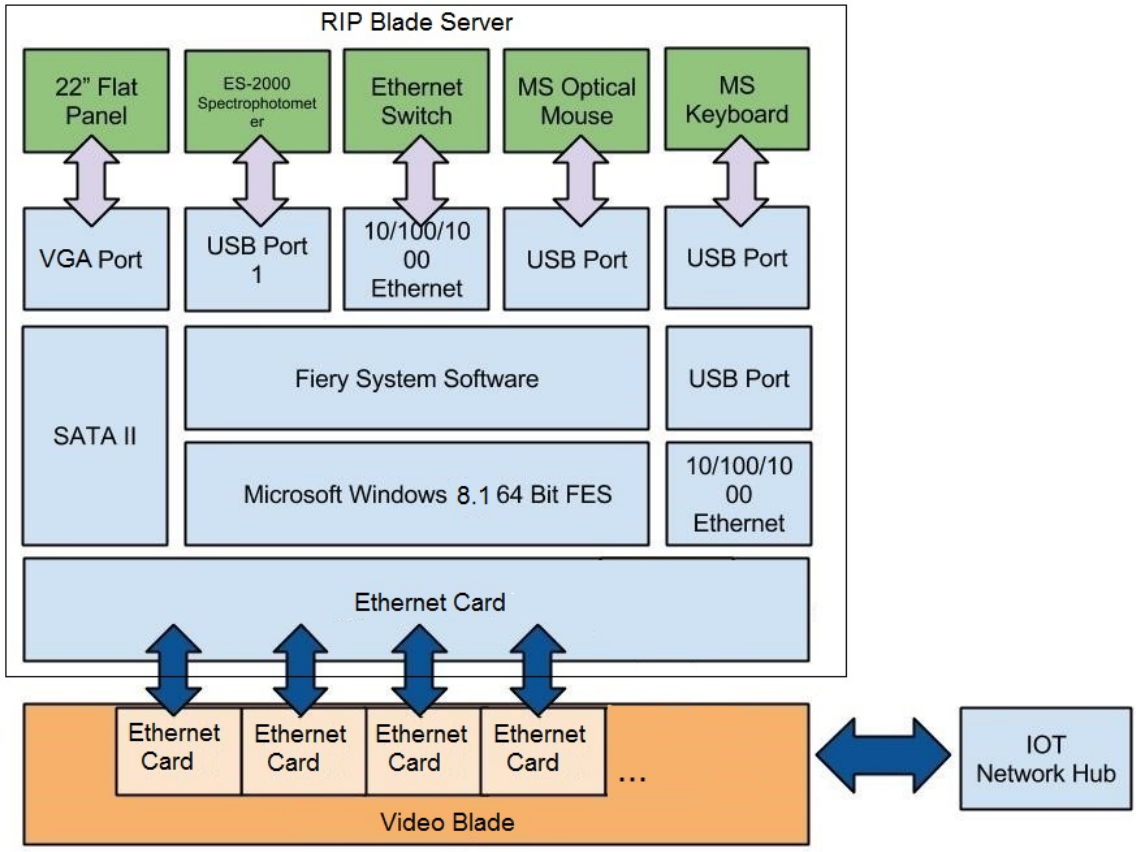
2 Digital Front End (DFE) Description

When a customer send jobs to the IJ Print Server, the motherboard of the RIP blade server processes image data. The Video blade server allows the Fiery server to communicate with the printer. The CPU controls the transfer of image data to and from the motherboard and runs the PostScript interpreter. Dual in-line memory modules (DIMMs) hold image data during printing.

The IJ Printer Server consists of 4U RIP blade, 2U RIP+Video blade, and 2U Video blade server. Depending on the system configuration, the number of the blade server differs to achieve the system throughput and scalability.

The RIP blade rasterize the page description file and compresses the image pattern into memory using compression technology. The interpreter outputs the compressed raster data through the 10GB Ethernet cable to the Video Blade(s). The raster data is sent to the printer, which then renders the image on paper at maximum speed.

Figure 1: Fiery server – Print Engine System Interface Diagram



3 DFE Functions

3.1 Memory information

4U RIP Blade

Volatile Memory					
Type (SRAM, DRAM, etc)	Size	User Modifiable (Y/N)	Can hold user data (Y/N)	Function or Use	Process to Sanitize
DRAM	64 GB	Y	Y	Main System Memory	Power Off Server
SDRAM (video on motherboard)	1 GB	Y	Y	Video Memory	Power Off Server
Non-Volatile Memory					
Type (Flash, EEPROM, etc.)	Size	User Modifiable (Y/N)	Can hold user data (Y/N)	Function or Use	Process to Sanitize
Bios	8 Mb	N	N	Bios Functions	Remove from socket and destroy, but system will cease to function
Ethernet Eprom	512 MB	N	N	Ethernet Chip Firmware	Desolder and destroy, but system will cease to function
CMOS NVRAM	256 Bytes	N	N	Bios Settings Storage	Remove System Battery for 30 seconds
Media and Storage					
SSD1: Main System Drive (C:\)	240 GB	Y	Y	Windows operating system Fiery applications (possibly with user data)	Reinstall the system software.
SSD2 - 5: Data RAID Array (E:\)	1.6TB (400GB x 4)	Y	Y	Fiery System Software Print jobs, scan jobs, and other user data Backup image for factory default	Reinstall the system software.

2U RIP Blade

Volatile Memory					
Type (SRAM, DRAM, etc)	Size	User Modifiable (Y/N)	Can hold user data (Y/N)	Function or Use	Process to Sanitize
DRAM	32 or 64 GB	Y	Y	Main System Memory	Power Off Server
SDRAM (video on motherboard)	512 MB	Y	Y	Video Memory	Power Off Server
Non-Volatile Memory					
Type (Flash, EEPROM, etc.)	Size	User Modifiable (Y/N)	Can hold user data (Y/N)	Function or Use	Process to Sanitize
Bios	8 Mb	N	N	Bios Functions	Remove from socket and destroy, but system will cease to function
Ethernet Eprom	512 MB	N	N	Ethernet Chip Firmware	Desolder and destroy, but system will cease to function
CMOS NVRAM	256 Bytes	N	N	Bios Settings Storage	Remove System Battery for 30 seconds
Media and Storage					
HDD1: Main System Drive (C:\)	1TB	Y	Y	Windows operating system Fiery applications (possibly with user data)	Reinstall the system software.
HDD2-3: Data RAID Array (E:\)	2TB (1TBx2)	Y	Y	Fiery System Software Print jobs, scan jobs, and other user data Backup image for factory default	Reinstall the system software.
HDD 4-7: 2nd Data RAID Array (E:\)	4TB (1TB x 4)	Y	Y	RIP data	Reinstall the system software.

2U Video Blade

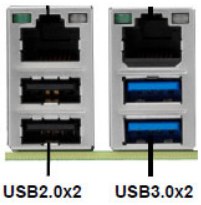
Volatile Memory					
Type (SRAM, DRAM, etc)	Size	User Modifiable (Y/N)	Can hold user data (Y/N)	Function or Use	Process to Sanitize
DRAM	64 GB	Y	Y	Main System Memory	Power Off Server
SDRAM (video on motherboard)	512 MB	Y	Y	Video Memory	Power Off Server
Non-Volatile Memory					
Type (Flash, EEPROM, etc.)	Size	User Modifiable (Y/N)	Can hold user data (Y/N)	Function or Use	Process to Sanitize
Bios	8 Mb	N	N	Bios Functions	Remove from socket and destroy, but system will cease to function
Ethernet Eprom	512 MB	N	N	Ethernet Chip Firmware	Desolder and destroy, but system will cease to function
CMOS NVRAM	256 Bytes	N	N	Bios Settings Storage	Remove System Battery for 30 seconds
Media and Storage					
HDD1: Main System Drive (C:\)	1TB	Y	Y	Windows operating system Fiery applications (possibly with user data)	Reinstall the system software.
HDD2-3: Data RAID Array (E:\)	2TB (1TBx2)	Y	Y	Fiery System Software Print jobs and other user data Backup image for factory default	Reinstall the system software.

Volatile Memory, the RAM, could contain customer data while processing customers' data. No customer data is stored in the nonvolatile memory such as BIOS, CMOS, and NVRAM.

3.2 External connections and an illustration of the connection interfaces. A table with description and usage is recommended.

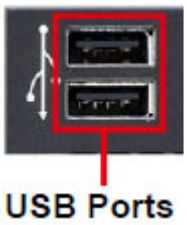
4U Video Blade

Front Bezel



Back Panel

2U RIP Blade and 2U Video Blade



Front Bezel

Back Panel

3.3 USB ports: a detailed description of the USB ports and their usage

4U RIP Blade

USB		
Printing from the USB ports can be disabled from the configuration tools.		
USB port and location	Purpose	
4 Ports on the rear I/O (2 USB 2.0, 2 USB 3.0), 2 USB 2.0 Ports on front bezel: 6 Ports Total	General-purpose, external ports are user accessible; internal ports are not. BIOS settings allow booting from the external USB backup media that was made bootable in the Fiery System Restore utility or Fiery Installer Builder utility.	

2U RIP Blade and 2U Video Blade

USB		
Printing from the USB ports can be disabled from the configuration tools.		
USB port and location	Purpose	
2 Ports on the rear I/O (2 USB 3.0), 2 USB 2.0 Ports on front bezel: 6 Ports Total	General-purpose, external ports are user accessible; internal ports are not. BIOS settings allow booting from the external USB backup media that was made bootable in the Fiery System Restore utility or Fiery Installer Builder utility.	

3.4 Wireless access methods with detailed description of usage.

There is no Wi-FI, Wi-Fi Direct, NFC, or RFID on Fiery DFEs.

3.5 Graphical user interface: a brief description of UI functionality

The administrative tasks are conducted through the DFE configuration tools, which are accessible from the DFE monitor, keyboard, and mouse. Also, they are accessible from the remote computers.

The configuration tools are password protected. DFE provides three user accounts, **admin**, **operator**, and **guest**. The level of the tasks users can perform depends on which user account is used to log in to the DFE server. The configuration tools only allow admin and operator users to access the DFE.

4 Logical access, network protocol information

4.1 IPSec, mode descriptions

IPsec or Internet Protocol security provides security to all applications over IP protocols through encryption and authentication of every packet. The Fiery server uses pre-shared key authentication to establish secure connections with other systems over IPsec. 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.

4.2 802.1x: description of interface and encryption capabilities, wired and wireless

802.1x is an IEEE standard protocol for port-based network access control. This protocol provides an authentication mechanism before the device gets access to the LAN and its resources. When enabled, the Fiery server can be configured to use EAP MD5-Challenge or PEAP-MSCHAPv2 to authenticate to an 802.1x authentication server. Fiery server authenticates at boot time or when the Ethernet cable is disconnected and reconnected.

4.3 IP Filtering description

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

4.4 Ports: full listing and purpose of TCP and UDP ports that are associated with features

TCP	UDP	Port Name
20–21		FTP
80		HTTP
135		MS RPC
137–139		NETBIOS
	161, 162	SNMP
	427	SLP
443		HTTPS
445		SMB/IP
	500	ISAKMP
515		LPD
631		IPP
3050		
	4500	IPsec NAT
	5353	Multicase DNS
3389		RDP
3702	3702	WS-Discovery
6310 8010 8021–8022 8090 9906 18081 18082 21030 22000	9906	EFI ports
9100–9103		Printing Port

LPD

Allows the Fiery server to receive print jobs via LPR.

Windows Printing

Enables SMB support in the Windows network printing environment. Allows Windows SMB users to browse the Fiery server in network neighborhood.

IPP

Enables the Fiery server to receive jobs sent via IPP (Internet Printing Protocol).

.

IPDS

Enables the Fiery server to receive the IPDS stream with the optional IPDS feature enabled.

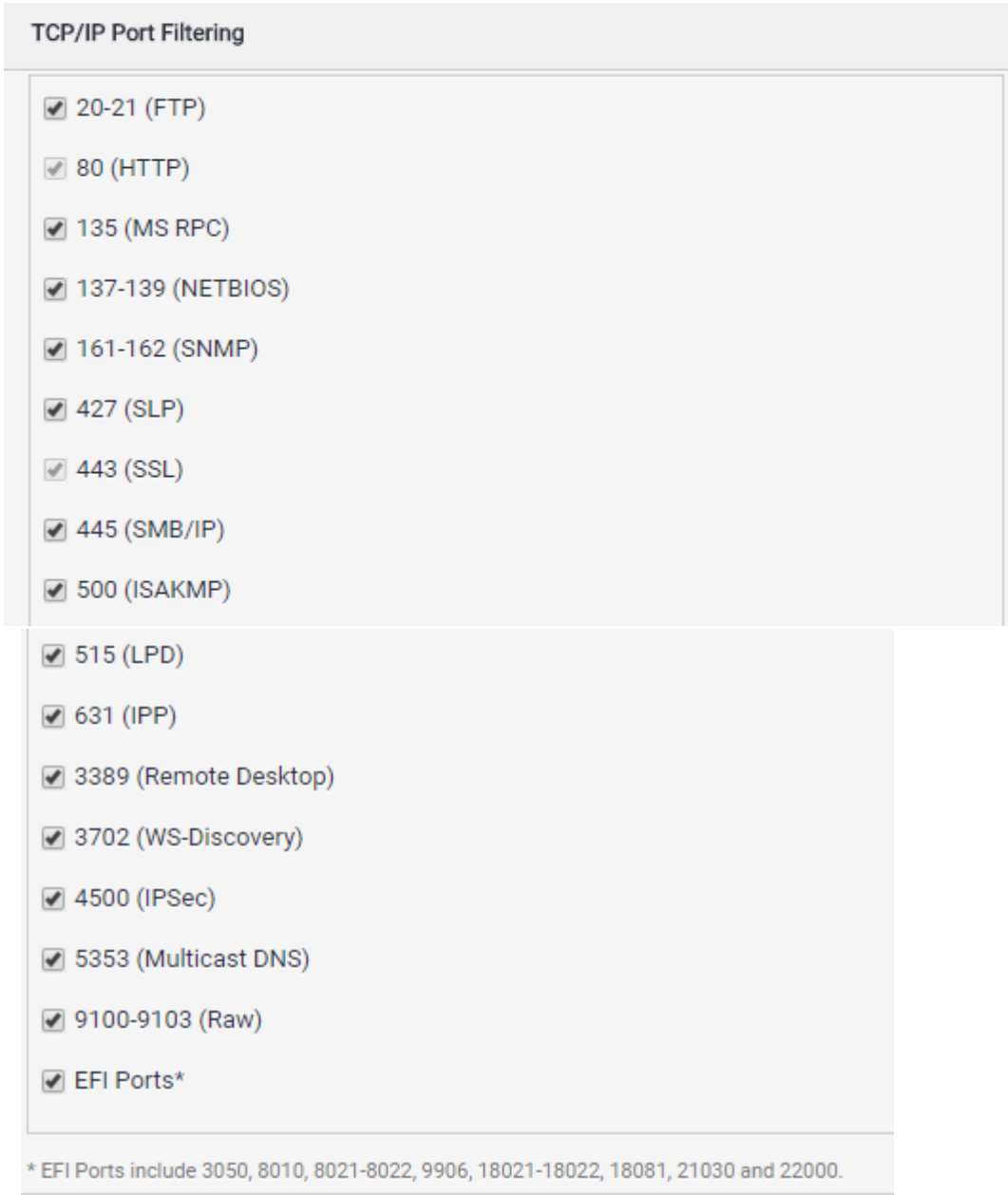
4.5 All protocols (e.g., HTTP, SNMP, TLS, SFTP, HTTPS, SSH, SMB)

HTTP, HTTPs, SMB(v3), SNMP, SLP, IPsec, SSL, and TLS(v1.1 and 1.2), LPD, IPP, RDP, WSD, Port 9100

4.6 PostScript passwords

PostScript passwords are not supported.

4.7 Detailed information on options available for disabling protocols considered no longer secure



4.8 Protection of data on the hard disk

Encryption of critical information on the Fiery server ensures that all passwords and related configuration information are secure when stored on the Fiery server. NIST 2010 compliant cryptographic algorithms, such as Twofish, are used.

5 Device software update control

5.1 Physical access methods (USB, network)

None. Patches must be digitally signed by EFI.

5.2 Logical access methods (device authentication)

None. Patches must be digitally signed by EFI.

5.3 Remote methods (remote solutions, device file distribution)

A patch file can be sent remotely to a Fiery server.

5.4 Device software upgrade file security (encryption and signature details)

All Fiery patches to update or upgrade Fiery software must be digitally signed by EFI for patches to be applied to the Fiery Server.

Only a user with Administrator privileges can access the Fiery WebTools Configure Tool.

6 Device clone file control

Fiery does not support this functionality.

7 Device configuration tools

Command Workstation Overview

Fiery Command WorkStation (Command WorkStation), the print job management interface for Fiery systems, makes centralized printing easy.

Through Command WorkStation users can:

- Display a summary of activity that is occurring either on all Fiery servers or on a selected server.
- View jobs that are being spooled, processed (RIPped), or printed, as well as general server information.
- Access and view the status of print jobs.
- Transfer jobs from one Fiery server to another on the network.
- View unlimited thumbnails across servers and full screen job previews from the Active Jobs queue, or jobs that have been RIPped or held.
- Simplify document creation with Preview tools to save, add, delete, zoom, copy, undo, and organize documents from one file to another, regardless of application or platform.
- Process jobs faster with eight short-cut action buttons: Print, Hold, Process/Hold, Delete, Archive, Preview, Impose, and Properties.
- Search and find local or archived jobs.
- Archive jobs to the Fiery server hard drive, network server, or removable media.
- Search and add Fiery servers by using the Auto Search function, or specify the Fiery server name or IP address.
- Download and import fonts, as well as PostScript, PDF, and EPS jobs.
- View job activity records – ideal for archiving, billing, and accounting purposes. The Job Log window allows for printing or exporting records into other applications, such as spreadsheets or databases.
- Select a single job or a group of jobs and easily change job properties.

In the new Job Center, the queues (for example, hold, printed, archived) have moved to the server list on the left, allowing more space for the main job list, so that more jobs can be displayed at one time.

WebTools Overview

WebTools is a set of browser-based pages for the user and administrator to access certain Fiery functionality. WebTools incorporates the Sidebar, a vertical menu on the left side of WebTools, which allows access to the w1indows of the application.

Connecting to the Fiery server using WebTools

The user can enter the Fiery server's DNS name or IP address in the Address section of the browser to connect. The server must have web services enabled to access this functionality via a browser.

If the connection to the Fiery server is lost during a browser session, the user will not detect the loss of connection until requesting updated information.

Configure

Configure allows the Fiery administrator to configure the Fiery server. After the Configure tab is selected, the Fiery server displays the login window. The user must log in with administrator rights.

Select a high-level category on the left side (Fiery Server, Job Submission, etc.), and then lower-level category (for example, Queues). The options are displayed on the right side. Select a setting and click Save.

If you open Configure from WebTools, you can still switch to using other WebTools pages at any time from the Sidebar menu.

8 System access

8.1 Authentication model, detailed description of authentication types (local, network, etc.)

Fiery servers support Admin, Operator, and Guest. Admin and Operator require password authentication both locally and from the network.

8.2 Card authentication types available, including SIPR.

Card authentication is not supported.

8.3 Authorization methods (LDAP, SMB, etc.)

Fiery local users, LDAP, and SMB are supported.

9 System accounts

By default, the Fiery server provides three system accounts: Administrator, Operator, and Guest. The Administrator user can add user accounts. Each user account belongs to a group; privileges assigned to groups control user activities.

10 Security-related features

10.1 Audit log: brief description, with table of all event types.

Windows Audit Log

10.2 User access control: brief description of any account based role feature.

Fiery client applications (Command WorkStation, Hot folder, Virtual printer), WebTools

10.3 Restricted administrator feature

Fiery Configuration

10.4 Remote user interface feature

Fiery client applications (Command WorkStation, Hot folder, Virtual printer), WebTools

10.5 Remote Services (AKA SMart eSolutions): remote services functionality, features, and options, including Xerox's ability to upgrade software, apply configuration settings or clone files, install options, etc. Content of data transmitted from the device to Xerox, including detail of optional log contents, with respect to Personal or Customer Identifiable Information (PII/CII), or any data a customer may classify as sensitive.

The Fiery forwards the needed information to the supported remove services. The Fiery passes through information.

10.6 Data encryption: content and detail of encryption security for data at rest in the system, including encryption algorithm information

3DES, AES128 for settings and some Fiery files, TwoFish 256 for some Fiery Files

10.7 Image overwrite: content and detail of overwrite security for data at rest in the system, including NIST, ISO, etc. references to algorithms used. Include number of passes and integrity checking of the feature and error handling.

The Fiery does not support secure Image overwrite.

10.8 FIPS 140-2: describe any FIPS capability of device, including list of non-FIPS compliant protocols / features

The Fiery has no FIPS capability.

10.9 E-mail signing and encryption: features and protocol (e.g. TLS) support

E-mail can be encrypted via TLS.

10.10 Software self-test: feature with failure behavior

Fiery includes a hardware diagnostics tool.

Any other security features not included above that pertain to the security of stored data or data in transit, including feature description

11 Response to known vulnerabilities

Xerox maintains a website, https://www.xerox.com/security, with up-to-date security vulnerability status, white papers, Common Criteria Certification, Intel Security McAfee information, and a portal to submit security questions to Xerox.