



Comprehensive Protection for Digital Documents and Devices

With the explosion of viruses and security breaches, protecting company information is important. Fiery® Security provides a complete administrator toolset to cover all aspects of document and device security. The toolset delivers the most comprehensive security measures in the print industry.

Greater Administrative Control

Fiery Security features give system administrators greater control over personal and electronic access to Fiery functions. With **3 Level Access Control**, administrators can define different user levels—each with different access privileges.

When administrators need to restrict Fiery access on the network, they can use IP Filtering. This feature restricts authorized connections to specific IP addresses or to the ones that fall within a particular IP range.

Group Printing can be employed to limit printing to specific user groups by requiring them to enter a valid group name password to start a job.

Email Printing allows administrators to restrict who can submit jobs to the Fiery via email. Administrators also can store authorized email address lists on the Fiery.

Port Blocking enables administrators to deselect any number of ports and their dependent Fiery functions in real time.

LDAP support adds an extra layer of security by enabling the Fiery to make use of email address access, email address authentication, and user password validation.

Compliant with Stringent Government and Corporate Security Standards

Fiery Security is designed to comply with the most stringent MIS/IT security standards in government and corporations. It adheres to industry standard certification policies such as IP Sec, SSL v2/v3, and X509 certificate management. IP security protocol provides security to IP protocols through an encryption and authentication mechanism.

Secure Erase¹ removes electronic data and latent file images stored on the Fiery hard drive.

User Authentication and **Disabling Network Ports and Service** keep unwanted users from accessing the system.

Anti-virus software is supported with the **Fiery Advanced Controller Interface (FACI)** Kits.

Real-time Fiery System software and Microsoft XPe updates are implemented directly through EFI WebTools to ensure the latest protection.

User Authentication and **Disabling Network Ports and Service** keep unwanted users from accessing the system.

Anti-virus software is supported with the **Fiery Advanced Controller Interface (FACI)** Kits.

Real-time Fiery System software and Microsoft XPe updates are implemented directly through EFI WebTools to ensure the latest protection.

Ensures Data Confidentiality

Fiery Security keeps digital and printed documents confidential with the following options and features:

Secure Printing requires users to enter job-specific passwords to print a job to prevent unauthorized users from printing confidential or private documents.

For maximum hard drive security, the optional **Removable Hard Drive** allows administrators with Fiery external servers to remove and lock away archived files.

Encryption of information ensures that all passwords and related configuration information are secure on the Fiery. The technology is based on the commonly accepted TwoFish method.

Keeps Track of Users on the System

Fiery Job Log Accounting lets administrators know who is using their system. It captures pertinent user data and allows only the administrator to delete single jobs or the entire job log from the system.

Ensures the latest protection

Real-time notification and download of **Fiery System software** including Fiery utilities and Microsoft critical updates ensure up-to-date software without having to call technical support or read CDs or DVDs.

¹ This is an optional Fiery embedded servers feature and comes standard on Fiery external servers.



Fiery Security

SERVER & CONTROLLER SOLUTIONS



EFI's portfolio of integrated solutions increases productivity and improves your bottom line. Find out more at www.efi.com.

Fiery Security Features

Job Management/Submission:

3 Level Access Control—Defines users types with different privileges.

Secure Job Log—Requires users to enter the administrator password when selecting print pages/job log.

Document Flow—Used when jobs submitted to the Fiery through the:

- Hold Queue
- Print Queue
- Direct Queue

Print via E-mail—Receives and prints jobs sent via email.

- Validates against an authorized email address.
- Deletes unauthorized emails received from unauthorized addresses.

Secure Print—Requires user to enter a job-specific password at the Fiery before printing job.

User Authentication—Allows administrator to define authorized users to perform functions/tasks on the Fiery.

Removable Hard Disk²—Allows moving hard drive to secure location.

Back Up and Restore—Enables back up and restoration of client settings to the same Fiery.

Scan:

Password Protected Mailboxes—Prevents unauthorized access by adding password protection.

Data Erase/Deletion:

Job Deletion—Deletes jobs from the Fiery, automatically or using Fiery tools.

Secure Erase³—Removes the job file from the Fiery HDD by overwriting it multiple times.

² Optional feature for Fiery External servers

³ Standard feature for Fiery External servers and Optional feature for Fiery Embedded servers

Network Access:

LDAP Authentication—Lightweight Directory Access Protocol (LDAP) v3, communication with corporate servers based on RFC2251.

- Fiery accesses e-mail addresses and username information.
- Fiery supports the following authentication methods using LDAP on Exchange, Novell and Domino systems:
 - Anonymous
 - SIMPLE
 - GSSAPI
 - Not available for Domino or Novell.

Port Blocking—Permits “deselect” and disable IP ports on the Fiery.

IP Filtering—Permits or denies connection requests to the Fiery from specific IP addresses or IP address range.

SNMP v3—Enables Fiery administrator to choose from three security levels.

SNTP—Allows Fiery to retrieve accurate standard time.

IP Sec support—Provides IP protocols security through encryption and authentication.

SSL/TLS support—SSL is protocol for transmitting private documents over the Web. TLS is a protocol that ensures privacy between communication applications and their Web users.

Certificate Management—Is way in which network clients authenticate network activities that perform identity verifications.

Encryption of critical information—Ensures that all passwords and related configuration information is secure.

MAC Filtering—Permits or denies connection requests to the Fiery over Ethernet based on the Media Access Control (MAC) address of the sender of the connection.

802.1x Authentication— Allows Fiery to get authenticated access to the LAN when based on the 802.1x port based access control.

Fiery System 8 Release 2

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

ColorWise, Command WorkStation, DocBuilder Pro, DocStream, EDOX, EFI, Fiery, the Fiery logo, Fiery Driven, the Fiery Driven logo, OneFlow, PrinterSite, PrintFlow, PrintMe, PrintSmith, PrintSmith Site, Prograph, Proteus and RIP-While-Print are registered trademarks of Electronics For Imaging, Inc. in the U.S. Patent and Trademark Office and/or certain other foreign jurisdictions. Bestcolor is a registered trademark of Electronics For Imaging GmbH in the U.S. Patent and Trademark Office. ADS, AutoCal, Auto-Count, Balance, Build, ColorCal, Digital StoreFront, Estimate, Fiery Link, Fiery Prints, Fiery Spark, FreeForm, Hagen, Intelligent Device Management, Logic, MicroPress, Printcafe, PSI, PSI Flexo, RIPChips, Scan, SendMe, Splash, Spot-On, VisualCal, WebTools, the EFI logo, the Fiery Prints logo, and Essential to Print are trademarks of Electronics for Imaging, Inc. Best, the Best logo, Colorproof, PhotoXposure, Remoteproof, and Screenproof are trademarks of Electronics For Imaging GmbH.

All other terms and product names may be trademarks or registered trademarks of their respective owners, and are hereby acknowledged.
©2006 Electronics For Imaging

SYS8/8e-DS-US-1006-45055921