



Fiery Security White Paper

Version 1.81

Date of Issue: 7/28/2006

Table of Contents

| | |
|--|-----------|
| TABLE OF CONTENTS | I |
| VERSION CONTROL | VI |
| 1 DOCUMENT OVERVIEW | 7 |
| 1.1 ELECTRONICS FOR IMAGING SECURITY PHILOSOPHY | 7 |
| 2 GENERAL SECURITY FEATURES WITH SYSTEM 5 | 7 |
| 2.1 COMPONENTS OF AN EXTERNAL NETWORK PRINT CONTROLLER | 7 |
| 2.1.1 <i>Intel based Server Hardware</i> | 7 |
| 2.1.2 <i>Proprietary EFI software</i> | 7 |
| 2.2 GENERAL AUTHENTICATION | 8 |
| 2.2.1 <i>Fiery Software Authentication</i> | 8 |
| 2.3 OPERATING SYSTEM ENVIRONMENT | 8 |
| 2.3.1 <i>Start up procedures</i> | 8 |
| 2.3.2 <i>Windows NT</i> | 8 |
| 2.3.3 <i>Local interface</i> | 9 |
| 2.4 CONNECTIVITY TO THE FIERY | 9 |
| 2.4.1 <i>Physical Ports</i> | 9 |
| 2.5 FIERY DOCUMENT FLOW | 9 |
| 2.5.1 <i>Standard Printing</i> | 9 |
| 2.5.2 <i>Group Printing</i> | 10 |
| 2.5.3 <i>Email printing</i> | 11 |
| 2.5.4 <i>Job Management</i> | 11 |
| 2.5.5 <i>Job Log</i> | 11 |
| 2.5.6 <i>Setup</i> | 12 |
| 2.5.7 <i>Scanning</i> | 12 |
| 2.6 ANTI-VIRUS SOFTWARE | 12 |
| 2.6.1 <i>Email viruses</i> | 13 |
| 3 GENERAL SECURITY FEATURES WITH SYSTEM 5.5 | 13 |
| 3.1 COMPONENTS OF AN EXTERNAL NETWORK PRINT CONTROLLER | 13 |
| 3.1.1 <i>Intel based Server Hardware</i> | 13 |
| 3.1.2 <i>Proprietary EFI software</i> | 13 |
| 3.2 GENERAL AUTHENTICATION | 13 |
| 3.2.1 <i>Fiery Software Authentication</i> | 13 |
| 3.3 OPERATING SYSTEM ENVIRONMENT | 14 |
| 3.3.1 <i>Start up procedures</i> | 14 |
| 3.3.2 <i>Windows XPe</i> | 14 |
| 3.3.3 <i>Local interface</i> | 14 |
| 3.4 CONNECTIVITY TO THE FIERY | 14 |
| 3.4.1 <i>Physical Ports</i> | 14 |
| 3.5 FIERY DOCUMENT FLOW | 15 |
| 3.5.1 <i>Standard Printing</i> | 15 |
| 3.5.2 <i>Secure Print</i> | 16 |
| 3.5.3 <i>Group Printing</i> | 17 |
| 3.5.4 <i>Email printing</i> | 17 |
| 3.5.5 <i>Job Management</i> | 17 |
| 3.5.6 <i>Job Log</i> | 17 |
| 3.5.7 <i>Setup</i> | 18 |
| 3.5.8 <i>Scanning</i> | 18 |
| 3.6 ANTI-VIRUS SOFTWARE | 18 |
| 3.6.1 <i>Email viruses</i> | 19 |
| 4 GENERAL SECURITY FEATURES WITH SYSTEM 5.1E AND 5.5E | 19 |

| | | |
|----------|--|-----------|
| 4.1 | COMPONENTS OF AN EMBEDDED NETWORK PRINT CONTROLLER | 19 |
| 4.1.1 | <i>Intel based Embedded Hardware</i> | 19 |
| 4.1.2 | <i>Proprietary EFI software</i> | 19 |
| 4.2 | GENERAL AUTHENTICATION | 19 |
| 4.3 | OPERATING SYSTEM ENVIRONMENT | 20 |
| 4.3.1 | <i>Start up procedures</i> | 20 |
| 4.3.2 | <i>Linux</i> | 20 |
| 4.3.3 | <i>Local interface</i> | 20 |
| 4.4 | CONNECTIVITY TO THE FIERY..... | 20 |
| 4.4.1 | <i>Physical Ports</i> | 20 |
| 4.4.2 | <i>Network Ports</i> | 20 |
| 4.5 | FIERY DOCUMENT FLOW | 21 |
| 4.5.1 | <i>Standard Printing</i> | 21 |
| 4.5.2 | <i>Secure Print</i> | 22 |
| 4.5.3 | <i>Group Printing</i> | 23 |
| 4.5.4 | <i>Email printing</i> | 23 |
| 4.5.5 | <i>Job Management</i> | 23 |
| 4.5.6 | <i>Job Log</i> | 24 |
| 4.5.7 | <i>Setup</i> | 24 |
| 4.5.8 | <i>Scanning</i> | 24 |
| 4.6 | ANTI-VIRUS SOFTWARE..... | 25 |
| 4.6.1 | <i>Email viruses</i> | 25 |
| 5 | GENERAL SECURITY FEATURES WITH SYSTEM 6E..... | 25 |
| 5.1 | COMPONENTS OF AN EMBEDDED NETWORK PRINT CONTROLLER | 25 |
| 5.1.1 | <i>Intel based Embedded Hardware</i> | 25 |
| 5.1.2 | <i>Proprietary EFI software</i> | 25 |
| 5.2 | GENERAL AUTHENTICATION | 25 |
| 5.3 | OPERATING SYSTEM ENVIRONMENT | 26 |
| 5.3.1 | <i>Start up procedures</i> | 26 |
| 5.3.2 | <i>Linux</i> | 26 |
| 5.3.3 | <i>Local interface</i> | 26 |
| 5.4 | CONNECTIVITY TO THE FIERY..... | 26 |
| 5.4.1 | <i>Physical Ports</i> | 26 |
| 5.4.2 | <i>Network Ports</i> | 26 |
| 5.5 | FIERY DOCUMENT FLOW | 27 |
| 5.5.1 | <i>Standard Printing</i> | 27 |
| 5.5.2 | <i>Secure Print</i> | 29 |
| 5.5.3 | <i>Group Printing</i> | 29 |
| 5.5.4 | <i>Email printing</i> | 30 |
| 5.5.5 | <i>Job Management</i> | 30 |
| 5.5.6 | <i>Job Log</i> | 30 |
| 5.5.7 | <i>Setup</i> | 31 |
| 5.5.8 | <i>Scanning</i> | 31 |
| 5.6 | ANTI-VIRUS SOFTWARE..... | 31 |
| 5.6.1 | <i>Email viruses</i> | 31 |
| 6 | GENERAL SECURITY FEATURES WITH SYSTEM 6 | 31 |
| 6.1 | COMPONENTS OF AN EXTERNAL NETWORK PRINT CONTROLLER | 31 |
| 6.1.1 | <i>Intel based Server Hardware</i> | 32 |
| 6.1.2 | <i>Proprietary EFI software</i> | 32 |
| 6.2 | GENERAL AUTHENTICATION | 32 |
| 6.2.1 | <i>Fiery Software Authentication</i> | 32 |
| 6.3 | OPERATING SYSTEM ENVIRONMENT | 32 |
| 6.3.1 | <i>Start up procedures</i> | 32 |
| 6.3.2 | <i>Windows XPe</i> | 33 |
| 6.3.3 | <i>Local interface</i> | 33 |
| 6.4 | CONNECTIVITY TO THE FIERY..... | 33 |
| 6.4.1 | <i>Physical Ports</i> | 33 |
| 6.4.2 | <i>Network Ports</i> | 34 |

| | | |
|--------------|--|-----------|
| 6.5 | FIERY DOCUMENT FLOW | 34 |
| 6.5.1 | <i>Standard Printing</i> | 34 |
| 6.5.2 | <i>Secure Print</i> | 36 |
| 6.5.3 | <i>Group Printing</i> | 37 |
| 6.5.4 | <i>Email printing</i> | 37 |
| 6.5.5 | <i>Job Management</i> | 37 |
| 6.5.6 | <i>Job Log</i> | 38 |
| 6.5.7 | <i>Setup</i> | 38 |
| 6.5.8 | <i>Scanning</i> | 38 |
| 6.6 | ANTI-VIRUS SOFTWARE..... | 39 |
| 6.6.1 | <i>Email viruses</i> | 39 |
| 7 | GENERAL SECURITY FEATURES WITH SYSTEM 7E..... | 39 |
| 7.1 | COMPONENTS OF AN EMBEDDED NETWORK PRINT CONTROLLER | 39 |
| 7.1.1 | <i>Intel based Embedded Hardware</i> | 39 |
| 7.1.2 | <i>Proprietary EFI software</i> | 39 |
| 7.2 | GENERAL AUTHENTICATION | 40 |
| 7.3 | OPERATING SYSTEM ENVIRONMENT | 40 |
| 7.3.1 | <i>Start up procedures</i> | 40 |
| 7.3.2 | <i>Linux</i> | 40 |
| 7.3.3 | <i>Local interface</i> | 40 |
| 7.4 | CONNECTIVITY TO THE FIERY..... | 40 |
| 7.4.1 | <i>Physical Ports</i> | 40 |
| 7.4.2 | <i>Network Ports</i> | 41 |
| 7.5 | FIERY DOCUMENT FLOW | 41 |
| 7.5.1 | <i>Standard Printing</i> | 41 |
| 7.5.2 | <i>Secure Print</i> | 43 |
| 7.5.3 | <i>Group Printing</i> | 43 |
| 7.5.4 | <i>Email printing</i> | 44 |
| 7.5.5 | <i>Job Management</i> | 44 |
| 7.5.6 | <i>Job Log</i> | 44 |
| 7.5.7 | <i>Setup</i> | 45 |
| 7.5.8 | <i>Scanning</i> | 45 |
| 7.6 | ANTI-VIRUS SOFTWARE..... | 45 |
| 7.6.1 | <i>Email viruses</i> | 45 |
| 8 | GENERAL SECURITY FEATURES WITH SYSTEM 7 | 46 |
| 8.1 | COMPONENTS OF AN EXTERNAL NETWORK PRINT CONTROLLER | 46 |
| 8.1.1 | <i>Intel based Server Hardware</i> | 46 |
| 8.1.2 | <i>Proprietary EFI software</i> | 46 |
| 8.2 | GENERAL AUTHENTICATION | 46 |
| 8.2.1 | <i>Fiery Software Authentication</i> | 46 |
| 8.3 | OPERATING SYSTEM ENVIRONMENT | 47 |
| 8.3.1 | <i>Start up procedures</i> | 47 |
| 8.3.2 | <i>Windows XPe</i> | 47 |
| 8.3.3 | <i>Local interface</i> | 48 |
| 8.4 | CONNECTIVITY TO THE FIERY..... | 48 |
| 8.4.1 | <i>Physical Ports</i> | 48 |
| 8.4.2 | <i>Network Ports</i> | 48 |
| 8.5 | FIERY DOCUMENT FLOW | 49 |
| 8.5.1 | <i>Standard Printing</i> | 49 |
| 8.5.2 | <i>Secure Print</i> | 51 |
| 8.5.3 | <i>Group Printing</i> | 51 |
| 8.5.4 | <i>Email printing</i> | 52 |
| 8.5.5 | <i>Job Management</i> | 52 |
| 8.5.6 | <i>Job Log</i> | 52 |
| 8.5.7 | <i>Setup</i> | 52 |
| 8.5.8 | <i>Scanning</i> | 53 |
| 8.6 | SYSTEM UPDATE..... | 53 |
| 8.7 | ANTI-VIRUS SOFTWARE..... | 53 |

| | | |
|-----------|---|-----------|
| 8.7.1 | Email viruses..... | 54 |
| 9 | GENERAL SECURITY FEATURES WITH SYSTEM 8E..... | 54 |
| 9.1 | COMPONENTS OF AN EMBEDDED NETWORK PRINT CONTROLLER..... | 54 |
| 9.1.1 | Intel based Embedded Hardware..... | 54 |
| 9.1.2 | Proprietary EFI software..... | 54 |
| 9.2 | USER AUTHENTICATION..... | 54 |
| 9.3 | OPERATING SYSTEM ENVIRONMENT..... | 55 |
| 9.3.1 | Start up procedures..... | 55 |
| 9.3.2 | Linux..... | 55 |
| 9.3.3 | Local interface..... | 55 |
| 9.4 | CONNECTIVITY TO THE FIERY..... | 55 |
| 9.4.1 | Physical Ports..... | 55 |
| 9.4.2 | Network Ports..... | 56 |
| 9.4.3 | Network Encryption..... | 56 |
| 9.5 | ENCRYPTION OF CRITICAL INFORMATION..... | 57 |
| 9.6 | FIERY DOCUMENT FLOW..... | 58 |
| 9.6.1 | Standard Printing..... | 58 |
| 9.6.2 | Secure Print..... | 60 |
| 9.6.3 | Email printing..... | 60 |
| 9.6.4 | Job Management..... | 60 |
| 9.6.5 | Job Log..... | 61 |
| 9.6.6 | Setup..... | 61 |
| 9.6.7 | Scanning..... | 61 |
| 9.7 | ANTI-VIRUS SOFTWARE..... | 61 |
| 9.7.1 | Email viruses..... | 62 |
| 9.8 | REMOVABLE HD KIT OPTION..... | 62 |
| 9.8.1 | For Embedded..... | 62 |
| 10 | GENERAL SECURITY FEATURES WITH SYSTEM 8..... | 62 |
| 10.1 | COMPONENTS OF AN EXTERNAL NETWORK PRINT CONTROLLER..... | 62 |
| 10.1.1 | Intel based Server Hardware..... | 62 |
| 10.1.2 | Proprietary EFI software..... | 62 |
| 10.2 | USER AUTHENTICATION..... | 63 |
| 10.2.1 | Fiery Software Authentication..... | 63 |
| 10.3 | OPERATING SYSTEM ENVIRONMENT..... | 63 |
| 10.3.1 | Start up procedures..... | 63 |
| 10.3.2 | Windows XPe..... | 64 |
| 10.3.3 | Local interface..... | 64 |
| 10.4 | CONNECTIVITY TO THE FIERY..... | 65 |
| 10.4.1 | Physical Ports..... | 65 |
| 10.4.2 | Network Ports..... | 65 |
| 10.4.3 | Network Encryption..... | 66 |
| 10.5 | ENCRYPTION OF CRITICAL INFORMATION..... | 67 |
| 10.6 | FIERY DOCUMENT FLOW..... | 67 |
| 10.6.1 | Standard Printing..... | 67 |
| 10.6.2 | Secure Print..... | 69 |
| 10.6.3 | Email printing..... | 70 |
| 10.6.4 | Job Management..... | 70 |
| 10.6.5 | Job Log..... | 70 |
| 10.6.6 | Setup..... | 70 |
| 10.6.7 | Scanning..... | 70 |
| 10.7 | SYSTEM UPDATE..... | 71 |
| 10.8 | ANTI-VIRUS SOFTWARE..... | 71 |
| 10.8.1 | Email viruses..... | 71 |
| 10.9 | REMOVABLE HD KIT OPTION..... | 72 |
| 10.9.1 | For Servers..... | 72 |
| 11 | PRODUCT SPECIFIC OPTIONS..... | 72 |
| 11.1 | FIERY NETWORK CONTROLLER HARDWARE MATRIX..... | 72 |

Version Control

| Version | Date | Editor | Description of Change |
|-----------|---------|-------------|--|
| 1.1 | 8/8/03 | M Robinson | First release with descriptions of System 5.5, 5.5e, and 5.1e products |
| 1.2 | 9/2/03 | M Robinson | Added description of System 5 products |
| 1.3 | 9/12/03 | M Robinson | Added discussion of virus concerns to System 5.1e/5.5e products |
| 1.4 | 7/29/04 | M Robinson | Added description of System 6 products |
| 1.5 | 4/29/05 | M Robinson | Added description of System 6e products |
| 1.6 | 8/10/05 | A. Abrantes | Added description for System 7 and 7e products |
| 1.7 | 8/12/05 | A. Abrantes | Updated the table in section 10.0 with latest hardware information |
| 1.71-1.72 | 3/2/06 | A. Abrantes | Updated section 8.3.2.1 – Microsoft Security Patches |
| 1.8 | 3/20/06 | A. Abrantes | Added descriptions for System 8 and 8e products |
| 1.81 | 7/28/06 | A. Abrantes | Updated description for Encryption (9.5 and 10.5) |
| | | | |

Copyright © 2000-2006 Electronics For Imaging, Inc. All rights reserved.

This publication is protected by copyright, and all rights are reserved. No part of it may be copied, reproduced, distributed, disclosed or transmitted in any form or by any means for any purpose without express prior written consent from Electronics For Imaging. Information in this document is subject to change without notice and does not represent a commitment on the part of Electronics For Imaging. Electronics for Imaging, Inc. assumes no responsibility or liability for any errors or inaccuracies, makes no warranty of any kind (express, implied or statutory) with respect to this publication, and expressly disclaims any and all warranties of merchantability, fitness for particular purposes, and non-infringement of third party rights. The software described in this publication is furnished under license and may only be used or copied in accordance with the terms of such license.

1 Document Overview

This document outlines architectural and functional aspects of Fiery Network Controllers with respect to device security. The purpose of this document is to provide a general overview of the Fiery Network Controller so that end users may research security features from which they can benefit and potential vulnerabilities they may encounter. This document outlines the current System 6, 6e, 5.5, 5.5e, 5.1e, and 5 models of the Fiery Network Controller generally from the perspective of its hardware architecture, software configuration, security features, and document information flow.

1.1 Electronics For Imaging Security Philosophy

For end users, Fiery network controllers have brought tremendous value to otherwise standalone devices. EFI recommends installation of network devices such as a Fiery network controller is done in accordance with existing security paradigms. EFI's goal is to lead the printing industry in the level of security of our devices and their data. To this end, EFI has incorporated security features into its line of Fiery network controllers. To create a more secure network environment, end-users will need to combine the Fiery security features with other security safeguards.

EFI places a high priority on producing a product with strong security features. EFI has worked with all our OEM partners to determine the requirements of the digital printing community. EFI has also created a cross-functional team whose primary focus is to deal with present and future security issues. EFI hopes that the end users will be able to independently evaluate the information provided in this overview to develop their own chosen system of security. Only by choosing measures designed to enhance security such as secure password procedures and strong physical security procedures, can the end user realize a system with security features.

2 General Security Features with System 5

2.1 Components of an External Network Print Controller

A network print controller is a self-contained unit composed of:

- Intel based server with the Windows NT operating system
- Proprietary EFI software providing networking, rasterizing, color management, and job management functions

2.1.1 Intel based Server Hardware

- Intel Pentium CPU
- IDE hard disk drive
- EEPROM holding general software BIOS. The CMOS, backed up by an onboard battery, holds the BIOS setup information
- Windows NT
- Anti-Virus software support

2.1.2 Proprietary EFI software

- Command Workstation 4 providing distributed job management capabilities
- NetWise providing network software to manage communication through these external ports
- Raster Image Processor (RIP) to rasterize incoming print jobs for marking by a print engine
- Video interface to pass the rasterized print jobs to the engine for printing

When the Fiery is connected to a network, it behaves as a networked PostScript and/or PCL printer.

2.2 General Authentication

With external Fiery Advanced Controller Interface (FACI)-enabled Fiery Controllers, there are two levels of authentication: the Microsoft Windows login and Fiery login. The Microsoft Windows login authentication mechanism is determined by rules and policies determined by the operating system and the system administrator.

2.2.1 Fiery Software Authentication

The Fiery network controller 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. 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 allow access to the following functionality:

- Administrator – full control over all Fiery functionality
- Operator – same as Administrator, except no access to some server functions, such as setup, and cannot delete the job log
- Guest (default; no password) – same as Operator, except cannot access the job log, cannot make edits or status changes to print jobs.

2.3 Operating System Environment

2.3.1 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 protects Fiery functionality, such as the based software and optional "pay-for" packages. Changes to the BIOS (or removal of the BIOS) prevent the Fiery from functioning properly.

Configuration page – the Configuration page lists the values specified during setup. Some information, such as password information is not included on the configuration page.

2.3.2 Windows NT

The Fiery ships with a default Windows NT 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 includes, but is not limited to the file system, system security policy, and registry entries. In addition, this allows anyone to change the administrator password and deny access to the Fiery for other users.

If the Windows Administrator password is enabled and not entered into the system, the user is prohibited from accessing the Fiery from a FACI kit. The Fiery system software functions normally and users can access Fiery 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). Setup information such as the Fiery Administrator password or Fiery Operator password is stored in the registry as plain text.

2.3.2.1 Microsoft Security Patches

Microsoft issues security patches to address potential security holes in the Windows NT operating system. EFI carefully monitors these patches and makes recommendations to our customers about which patches are applicable to the Fiery. Not all Windows NT patches are recommended for a Fiery running System 5.

All Fierys running System 5 should use Service Pack 6a from Microsoft. A patch to update the Fiery to Service Pack 6a is available from EFI.

2.3.3 Local interface

The user can access the Fiery functions via the FACI kit (if enabled) or the Fiery LCD. The Windows Administrator password is used to control access to the Fiery if the FACI kit is enabled. The Fiery LCD only provides access to the Fiery functionality.

2.4 Connectivity to the Fiery

2.4.1 Physical Ports

The Fiery can be connected through the following external ports:

| Fiery Ports | Function | Access |
|----------------------------|---------------------------------|--|
| Interface Ports | Copier/printer connection (DDI) | |
| 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 |
| Parallel Port | Parallel connection | Bisynchronous whatever communication limited to receiving print jobs via a parallel cable. |

The Fiery administrator can also enable/disable the different network services provided by the Fiery. Enabling/disabling SNMP is available on particular Fiery with System 5 products and requires a separate patch.

2.5 Fiery Document Flow

The user can submit and manage jobs in a variety of methods to the Fiery. Some methods have some security associated with them; these are discussed below.

2.5.1 Standard Printing

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

- Hold Queue
- Print Queue
- Direct Queue (Direct connection)

The Fiery Administrator can disable the Print and Direct queues to limit automatic printing. With passwords enabled on the Fiery, this 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 will not accept new jobs.

2.5.1.1 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. 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 the Command WorkStation or Clear Server.

2.5.1.2 Printed Queue

Jobs sent to the hold or print queues are stored in the printed queue on the Fiery, if enabled. The administrator can define the number of jobs kept in the printed queue.

2.5.1.3 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 skips other waiting to process jobs
- The Fiery 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.
- Jobs 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 are 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
- On Windows systems the system memory may use the swap file on the HDD as a memory buffer.

2.5.1.4 Job Deletion

When a job is deleted from the Fiery, either automatically or using Fiery tools, the job cannot be viewed or retrieved using Fiery tools. If the job was spooled to the Fiery HDD, elements of the job may remain on the HDD and could theoretically be recovered with certain tools.

2.5.1.5 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.

2.5.2 Group Printing

Requires the user to enter a valid group name/password match for the job to start printing. The group name/password can be entered from an EFI tool with Notes functionality, such as the Fiery

Driver or the Command WorkStation. The group name is included in the Job Log when the job prints.

The purpose of this feature is to (a) require users to submit a pre-defined group name with every job for accounting purposes and (b) limit printing to individuals who have valid group name/passwords.

2.5.2.1 *Workflow*

The user enters a Group Name and Group Password in the driver, creates and prints the job. When the Fiery begins to process the job, the Fiery checks the group name/group password with the Fiery's internal printing group list. If the group name/group password is a valid match, the job will continue to process. If the group name/group password is not a valid match, the job will generate an error and move to the printed queue.

This feature can be enabled/disabled from the LCD.

2.5.2.2 *Limitations*

The group name and password strings in the job are not encrypted and can be read from the print job.

Because the system only checks for the password before ripping, it is possible to load balance a RIPped job from a similar Fiery and still print an unauthorized file. It is also possible to change the password and group strings of a RIPped job with Command Workstation and print.

The list of passwords on the Fiery is not encrypted when stored on the Fiery.

2.5.3 *Email printing*

The Fiery will receive and print jobs sent via email. The administrator can store a list on the Fiery of authorized email address; any email received from an email address not in the authorized email address list will be deleted.

2.5.4 *Job Management*

Jobs submitted to the Fiery can only be acted upon by using a Fiery job management utility with either administrator or operator access. Guest users (those 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. Setup information such as the Fiery administrator passwords, Fiery Operator passwords, and Novell passwords are sent to the Fiery in plain text.

2.5.5 *Job Log*

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

A user with operator access can view, export, or print the joblog from the following tools:

- Command WorkStation
- WebSpooler
- Fiery Spooler

A user with administrator access can delete the job log from the following tools:

- Command WorkStation

-
- WebSpooler
 - Fiery Spooler

A user with guest access can print the job log from the Fiery LCD.

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

2.5.6 Setup

Setup requires an administrator password. The Fiery can be setup up or configured from the Fiery LCD, the Fiery Setup program run from a Windows Fiery with a FOCI kit, or a remote Setup application run from the WebTools or Command WorkStation.

2.5.7 Scanning

The Fiery 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 from 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 for distribution or storage and retrieval. All scanned documents are written to disk. The administrator can configure the Fiery to delete scan jobs automatically after a predefined length of stay on the Fiery.

Scan jobs can be distributed via the following methods:

- Email – sent to a mail server where it is routed to the desired email destination. Note: if the file size is greater than the administrator-defined maximum, the job is stored on the Fiery HDD, accessible through a URL.
- Fiery Hold Queue – sent to the Fiery Hold Queue (see Printing, above) and is not kept as a scan job
- Mailbox – stored on the Fiery with a mailbox code number. The user needs to enter the correct mailbox number to access the stored scan job. Some Fiery versions also require a password. The scan job is stored in a manner to allow retrieval through a URL.

2.6 Anti-virus software

Administrators can install anti-virus software on FOCI-enabled Windows NT-based Fierys to protect against the accidental introduction of viruses on the Fiery.

Anti-virus software should only be run when the Fiery is idle and not receiving jobs. This helps prevent unforeseeable errors that may result if antivirus software acts while the Fiery attempts to process a job.

The anti-virus software should scan for files coming into the Fiery outside of the normal printstream. This includes:

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

The anti-virus software can also be configured to scan all files on the Fiery when the Fiery is not planned for use for an extended period of time.

EFI tests some System 5 Fiery products with Symantec Norton antivirus software; similar products from McAfee and TrendMicro are also compatible with the Fiery when used as described above.

2.6.1 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. The Fiery 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 and treated as such.

3 General Security Features with System 5.5

3.1 Components of an External Network Print Controller

A network print controller is a self-contained unit composed of:

- Intel based server with the Windows XPe operating system
- Proprietary EFI software providing networking, rasterizing, color management, and job management functions

3.1.1 Intel based Server Hardware

- Intel Pentium CPU
- IDE hard disk drive
- EEPROM holding general software BIOS. The CMOS, backed up by an onboard battery, holds the BIOS setup information
- Windows XPe
- Anti-Virus software support

3.1.2 Proprietary EFI software

- Command Workstation 4 providing distributed job management capabilities
- NetWise providing network software to manage communication through these external ports
- Raster Image Processor (RIP) to rasterize incoming print jobs for marking by a print engine
- Video interface to pass the rasterized print jobs to the engine for printing

When the Fiery is connected to a network, it behaves as a networked PostScript and/or PCL printer.

3.2 General Authentication

With external Fiery Advanced Controller Interface (FACI)-enabled Fiery Controllers, there are two levels of authentication: the Microsoft Windows login and Fiery login. The Microsoft Windows login authentication mechanism is determined by rules and policies determined by the operating system and the system administrator.

3.2.1 Fiery Software Authentication

The Fiery network controller 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. 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 allow access to the following functionality:

- Administrator – full control over all Fiery functionality

-
- Operator – same as Administrator, except no access to some server functions, such as setup, and cannot delete the job log
 - Guest (default; no password) – same as Operator, except cannot access the job log, cannot make edits or status changes to print jobs.

3.3 Operating System Environment

3.3.1 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 protects Fiery functionality, such as the based software and optional “pay-for” packages. Changes to the BIOS (or removal of the BIOS) prevent the Fiery from functioning properly.

Configuration page – the Configuration page lists the values specified during setup. Some information, such as FTP proxy information, password information, and SNMP Community Names are not included on the configuration page.

3.3.2 Windows XPe

The Fiery ships with a default Windows XPe 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 includes, but is not limited to the file system, system security policy, and registry entries. In addition, this allows anyone to change the administrator password and deny access to the Fiery for other users.

If the Windows Administrator password is enabled and not entered into the system, the user is prohibited from accessing the Fiery from a FACI kit. The Fiery system software functions normally and users can access Fiery 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). Setup information such as the Fiery Administrator password or Fiery Operator password is stored in the registry as plain text.

3.3.2.1 Microsoft Security Patches

Microsoft regularly issues security patches to address potential security holes in the Windows XP operating system. EFI carefully monitors these patches and makes recommendations to our customers about which patches are applicable to the Fiery. Not all Windows XP patches are applicable to the Windows XPe operating system.

3.3.3 Local interface

The user can access the Fiery functions via the FACI kit (if enabled) or the Fiery LCD. The Windows Administrator password is used to control access to the Fiery if the FACI kit is enabled. The Fiery LCD only provides access to the Fiery functionality.

3.4 Connectivity to the Fiery

3.4.1 Physical Ports

The Fiery can be connected through the following external ports:

| Fiery Ports | Function | Access |
|----------------------------|---------------------------------|--|
| Interface Ports | Copier/printer connection (DDI) | |
| 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 |
| Parallel Port | Parallel connection | Bisynchronous whatever communication limited to receiving print jobs via a parallel cable. |
| USB Port | USB device connection | Plug and play connector designed for use with optional removable media devices |

The Fiery administrator can also enable/disable the different network services provided by the Fiery.

The local administrator can define SNMP read/write community names.

3.5 Fiery Document Flow

The user can submit and manage jobs in a variety of methods to the Fiery. Some methods have some security associated with them; these are discussed below.

3.5.1 Standard Printing

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

- Hold Queue
- Print Queue
- Direct Queue (Direct connection)

The Fiery Administrator can disable the Print and Direct queues to limit automatic printing. With passwords enabled on the Fiery, this 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 will not accept new jobs.

3.5.1.1 *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. 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 LE or Clear Server.

3.5.1.2 *Printed Queue*

Jobs sent to the hold or print queues are stored in the printed queue on the Fiery, if enabled. The administrator can define the number of jobs kept in the printed queue.

3.5.1.3 *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 skips other waiting to process jobs
 - The Fiery 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.
 - Jobs are not written to the printed queue. However, they appear in the job log.

Note: *only one client can print 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 are 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
- On Windows systems the system memory may use the swap file on the HDD as a memory buffer.

3.5.1.4 Job Deletion

When a job is deleted from the Fiery, either automatically or using Fiery tools, the job cannot be viewed or retrieved using Fiery tools. If the job was spooled to the Fiery HDD, elements of the job may remain on the HDD and could theoretically be recovered with certain tools.

3.5.1.5 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.

3.5.2 Secure Print

The secure print function requires the user to enter a job-specific password at the Fiery to allow the job to print. This feature requires an LCD interface local to the Fiery.

The purpose of this feature 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.

3.5.2.1 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 LE.*

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 extracted from the print job.

3.5.3 Group Printing

Requires the user to enter a valid group name/password match for the job to start printing. The group name/password can be entered from an EFI tool with Notes functionality, such as the Fiery Driver or the Command WorkStation. The group name is included in the Job Log when the job prints.

The purpose of this feature is to (a) require users to submit a pre-defined group name with every job for accounting purposes and (b) limit printing to individuals who have valid group name/passwords.

3.5.3.1 Workflow

The user enters a Group Name and Group Password in the driver, creates and prints the job. When the Fiery begins to process the job, the Fiery checks the group name/group password with the Fiery's internal printing group list. If the group name/group password is a valid match, the job will continue to process. If the group name/group password is not a valid match, the job will generate an error and move to the printed queue.

This feature can be enabled/disabled from the LCD.

3.5.3.2 Limitations

The group name and password strings in the job are not encrypted and can be read from the print job.

Because the system only checks for the password before ripping, it is possible to load balance a RIPPed job from a similar Fiery and still print an unauthorized file. It is also possible to change the password and group strings of a RIPPed job with Command Workstation and print.

The list of passwords on the Fiery is not encrypted when stored on the Fiery.

3.5.4 Email printing

The Fiery will receive and print jobs sent via email. The administrator can store a list on the Fiery of authorized email address; any email received with an email address not in the authorized email address list will be deleted.

3.5.5 Job Management

Jobs submitted to the Fiery can only be acted upon by using a Fiery job management utility with either administrator or operator access. Guest users (those 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. Setup information such as the Fiery administrator passwords, Fiery Operator passwords, and Novell passwords are sent to the Fiery in plain text.

3.5.6 Job Log

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

A user with operator access can view, export, or print the joblog from the following tools:

- Command WorkStation
- Command WorkStation LE
- WebSpooler
- Fiery Spooler

A user with administrator access can delete the job log from the following tools:

- Command WorkStation
- Command WorkStation LE
- WebSpooler
- Fiery Spooler

A user with guest access can print the job log from the Fiery LCD on certain Fierys. Other Fierys 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.

3.5.7 Setup

Setup requires an administrator password. The Fiery can be setup up or configured from the Fiery LCD, the Fiery Setup program run from a Windows Fiery with a FACL kit, or a remote Setup application run from the WebTools or Command WorkStation.

3.5.8 Scanning

The Fiery 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 from 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 for distribution or storage and retrieval. All scanned documents are written to disk. The administrator can configure the Fiery to delete scan jobs automatically after a predefined length of stay on the Fiery.

Scan jobs can be distributed via the following methods:

- Email – sent to a mail server where it is routed to the desired email destination. Note: if the file size is greater than the administrator-defined maximum, the job is stored on the Fiery HDD, accessible through a URL.
- FTP – sent to an FTP destination. A record of the transfer, including the destination, is kept in the FTP log (accessible from the LCD Print Pages command). An FTP Proxy Server can be defined to send the job through a firewall.
- Fiery Hold Queue – sent to the Fiery Hold Queue (see Printing, above) and is not kept as a scan job
- Internet Fax – sent to a mail server where it is routed to the desired internet fax destination.
- Mailbox – stored on the Fiery with a mailbox code number. The user needs to enter the correct mailbox number to access the stored scan job. Some Fiery versions also require a password. The scan job is stored in a manner to allow retrieval through a URL.

3.6 Anti-virus software

Administrators can install anti-virus software on FACL-enabled Windows XPe-based Fierys to protect against the accidental introduction of viruses on the Fiery.

Anti-virus software should only be run when the Fiery is idle and not receiving jobs. This helps prevent unforeseeable errors that may result if antivirus software acts while the Fiery attempts to process a job.

The anti-virus software should scan for files coming into the Fiery outside of the normal printstream. This includes:

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

The anti-virus software can also be configured to scan all files on the Fiery when the Fiery is not planned for use for an extended period of time.

EFI tests System 5.5 Fiery products with McAfee VirusScan software; similar products from Symantec and TrendMicro are also compatible with the Fiery when used as described above.

3.6.1 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. The Fiery 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 and treated as such.

4 General Security Features with System 5.1e and 5.5e

4.1 Components of an Embedded Network Print Controller

A network print controller is a self-contained unit composed of:

- Intel based processor with a Linux operating system
- Proprietary EFI software providing networking, rasterizing, color management, and job management functions

4.1.1 Intel based Embedded Hardware

- Intel mobile Pentium CPU
- IDE Hard Drive
- EEPROM holding general software BIOS. The CMOS, backed up by an onboard battery, holds the BIOS setup information
- Linux operating system

4.1.2 Proprietary EFI software

- Command Workstation 4 providing distributed job management capabilities
- Netwise providing network software to manage communication through these external ports
- Raster Image Processor (RIP) to rasterize incoming print jobs for marking by a print engine
- Video interface to pass the rasterized print jobs to the engine for printing

4.2 General Authentication

The Fiery network controller defines Administrator, Operator, and Guest users with different privileges. It is recommended that administrators require passwords to access the Fiery..

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

- Administrator – full control over all Fiery functionality
- Operator – same as Administrator, except no access to some server functions, such as setup, and cannot delete the job log
- Guest (default; no password) – same as Operator, except cannot access the job log, cannot make edits or status changes to print jobs.

4.3 Operating System Environment

4.3.1 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 from functioning properly.

Configuration page – the Configuration page lists the values specified during setup. Some information, such as FTP proxy information, password information, and SNMP Community Names are not included on the configuration page.

4.3.2 Linux

Linux systems do not include a local interface that allows access to the operating system.

4.3.3 Local interface

The Fiery LCD only provides access to the Fiery functionality.

4.4 Connectivity to the Fiery

4.4.1 Physical Ports

The Fiery can be connected through the following external ports:

| Fiery Ports | Function | Access |
|----------------------------|---------------------------------|--|
| Interface Ports | Copier/printer connection (DDI) | |
| Serial port | Diablo interface | |
| 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 |
| Parallel Port | Parallel connection | Bisynchronous whatever communication limited to receiving print jobs via a parallel cable. |

4.4.2 Network Ports

The Fiery allows the user to selectively enable/disable the following IP ports:

| TCP | UPD | Port Name | Dependent Service(s) |
|-----|-----|-----------|----------------------|
| 80 | | HTTP | WebTools, IPP |

| | | | |
|-----------|-------|---------------|---|
| 137-139 | | NETBIOS | Windows Printing |
| | 161-2 | SNMP | WebTools, Velocity, some legacy utilities, other SNMP-based tools |
| 515 | | LPD | LPR printing, WebTools, some legacy utilities |
| 631 | | IPP | IPP |
| 8021-8022 | | Harmony | CWS4, Velocity, EFI SDK-based tools, Fiery Driver bi-di functions |
| 9100-9103 | | Printing Port | Port 9100 |

Other TCP ports, except those specified by the OEM, are disabled. Any service dependent on a disabled port is automatically disabled.

The Fiery administrator can also enable/disable the different network services provided by the Fiery.

The local administrator can define SNMP read/write community names.

4.4.2.1 IP Filtering

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

4.5 Fiery Document Flow

The user can submit and manage jobs in a variety of methods to the Fiery. Some methods have some security associated with them; these are discussed below.

4.5.1 Standard Printing

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

- Hold Queue
- Print Queue
- Direct Queue (Direct Connection)

The Fiery Administrator can disable the Print and Direct queues to limit automatic printing. With passwords enabled on the Fiery, this 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 will not accept new jobs.

4.5.1.1 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. 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 LE or Clear Server.

4.5.1.2 Printed Queue

Jobs sent to the hold or print queues are stored in the printed queue on the Fiery, if enabled. The administrator can define the number of jobs kept in the printed queue.

4.5.1.3 *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 skips other waiting to process jobs
- The Fiery 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.
- Jobs 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
- On Linux systems the system memory may overflow to use the swap partition on the HDD as a memory buffer.

4.5.1.4 *Job Deletion*

When a job is deleted from the Fiery, either automatically or using Fiery tools, the job cannot be viewed or retrieved using Fiery tools. If the job was spooled to the Fiery HDD, elements of the job may remain on the HDD and could theoretically be recovered with certain tools.

4.5.1.5 *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.

4.5.2 *Secure Print*

The secure print function requires the user to enter a job-specific password at the Fiery to allow the job to print. This feature requires an LCD interface local to the Fiery.

The purpose of this feature 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.

4.5.2.1 *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 LE.*

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.*

4.5.3 Group Printing

Requires the user to enter a valid group name/password match for the job to start printing. The group name/password can be entered from an EFI tool with Notes functionality, such as the Fiery Driver or the Command WorkStation. The group name is included in the Job Log when the job prints.

The purpose of this feature is to (a) require users to submit a pre-defined group name with every job for accounting purposes and (b) limit printing to individuals who have valid group name/passwords.

4.5.3.1 Workflow

The user enters a Group Name and Group Password in the driver, creates and prints the job. When the Fiery begins to process the job, the Fiery checks the group name/group password with the Fiery's internal printing group list. If the group name/group password is a valid match, the job will continue to process. If the group name/group password is not a valid match, the job will generate an error and move to the printed queue.

This feature can be enabled/disabled from the LCD.

4.5.3.2 Limitations

The group name and password strings in the job are not encrypted and can be read from the print job.

Because the system only checks for the password before ripping, it is possible to load balance a RIPPed job from a similar Fiery and still print an unauthorized file. It is also possible to change the password and group strings of a RIPPed job with Command Workstation and print.

The list of passwords on the Fiery is not encrypted when stored on the Fiery.

4.5.4 Email printing

The Fiery will receive and print jobs sent via email. The administrator can store a list on the Fiery of authorized email address; any email received with an email address not in the authorized email address list will be deleted.

4.5.5 Job Management

Jobs submitted to the Fiery can only be acted upon by using a Fiery job management utility with either administrator or operator access. Guest users (those 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. Setup information such as the Fiery administrator passwords, Fiery Operator passwords, and Novell passwords are sent to the Fiery in plain text.

4.5.6 Job Log

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

A user with operator access can view, export, or print the job log from the following tools:

- Command WorkStation
- Command WorkStation LE
- WebSpooler
- Fiery Spooler

A user with administrator access can delete the job log from the following tools:

- Command WorkStation
- Command WorkStation LE
- WebSpooler
- Fiery Spooler

A user with guest access can print the job log from the Fiery LCD on certain Fierys. Other Fierys 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.

4.5.7 Setup

Setup requires an administrator password. The Fiery can be setup up or configured from the Fiery LCD or a remote Setup application run from the WebTools or Command WorkStation.

4.5.8 Scanning

The Fiery 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 from 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 for distribution or storage and retrieval. All scanned documents are written to disk. The administrator can configure the Fiery to delete scan jobs automatically after a predefined length of stay on the Fiery.

Scan jobs can be distributed via the following methods:

- Email – sent to a mail server where it is routed to the desired email destination. Note: if the file size is greater than the administrator-defined maximum, the job is stored on the Fiery HDD, accessible through a URL.
- FTP – sent to an FTP destination. A record of the transfer, including the destination, is kept in the FTP log (accessible from the LCD Print Pages command). An FTP Proxy Server can be defined to send the job through a firewall.
- Fiery Hold Queue – sent to the Fiery Hold Queue (see Printing, above) and is not kept as a scan job
- Internet Fax – sent to a mail server where it is routed to the desired internet fax destination.
- Mailbox – stored on the Fiery with a mailbox code number. The user needs to enter the correct mailbox number to access the stored scan job. Some Fiery versions also require a password. The scan job is stored in a manner to allow retrieval through a URL.

4.6 Anti-virus software

The operating system is a dedicated operating system, and therefore does not have all the functionality of a complete operating system. The Fiery Controller was not designed to accept applications such as virus protection software as part of its operational model. This was done intentionally to help prevent the loading of potentially malicious software on the units, as well as to control the impact adding such applications would have on a system's operation and performance.

4.6.1 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. The Fiery 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 and treated as such.

5 General Security Features with System 6e

5.1 Components of an Embedded Network Print Controller

A network print controller is a self-contained unit composed of:

- Intel based processor with a Linux operating system
- Proprietary EFI software providing networking, rasterizing, color management, and job management functions

5.1.1 Intel based Embedded Hardware

- Intel mobile Pentium CPU
- IDE Hard Drive
- EEPROM holding general software BIOS. The CMOS, backed up by an onboard battery, holds the BIOS setup information
- Linux operating system

5.1.2 Proprietary EFI software

- Command Workstation 4 providing distributed job management capabilities
- Netwise providing network software to manage communication through these external ports
- Raster Image Processor (RIP) to rasterize incoming print jobs for marking by a print engine
- Video interface to pass the rasterized print jobs to the engine for printing

5.2 General Authentication

The Fiery network controller defines Administrator, Operator, and Guest users with different privileges. It is recommended that administrators require passwords to access the Fiery..

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

- Administrator – full control over all Fiery functionality
- Operator – same as Administrator, except no access to some server functions, such as setup, and cannot delete the job log
- Guest (default; no password) – same as Operator, except cannot access the job log, cannot make edits or status changes to print jobs.

5.3 Operating System Environment

5.3.1 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 from functioning properly.

Configuration page – the Configuration page lists the values specified during setup. Some information, such as FTP proxy information, password information, and SNMP Community Names are not included on the configuration page.

5.3.2 Linux

Linux systems do not include a local interface that allows access to the operating system.

5.3.3 Local interface

The Fiery LCD only provides access to the Fiery functionality.

5.4 Connectivity to the Fiery

5.4.1 Physical Ports

The Fiery can be connected through the following external ports:

| Fiery Ports | Function | Access |
|----------------------------|---------------------------------|--|
| Interface Ports | Copier/printer connection (DDI) | |
| Serial port | Diablo interface | |
| 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 |
| Parallel Port | Parallel connection | Bisynchronous whatever communication limited to receiving print jobs via a parallel cable. |

5.4.2 Network Ports

The Fiery allows the user to selectively enable/disable the following IP ports:

| TCP | UPD | Port Name | Dependent Service(s) |
|---------|-------|-----------|---|
| 80 | | HTTP | WebTools, IPP |
| 137-139 | | NETBIOS | Windows Printing |
| | 161-2 | SNMP | WebTools, Velocity, some legacy utilities, other SNMP-based tools |
| 515 | | LPD | LPR printing, WebTools, some legacy utilities |

| | | | |
|-----------|--|---------------|---|
| 631 | | IPP | IPP |
| 8021-8022 | | Harmony | CWS4, Velocity, EFI SDK-based tools, Fiery Driver bi-di functions |
| 9100-9103 | | Printing Port | Port 9100 |

Other TCP ports, except those specified by the OEM, are disabled. Any service dependent on a disabled port is automatically disabled.

The Fiery administrator can also enable/disable the different network services provided by the Fiery.

The local administrator can define SNMP read/write community names.

5.4.2.1 IP Filtering

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

5.5 Fiery Document Flow

The user can submit and manage jobs in a variety of methods to the Fiery. Some methods have some security associated with them; these are discussed below.

5.5.1 Standard Printing

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

- Hold Queue
- Print Queue
- Direct Queue (Direct Connection)

The Fiery Administrator can disable the Print and Direct queues to limit automatic printing. With passwords enabled on the Fiery, this 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 will not accept new jobs.

5.5.1.1 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. 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 LE or Clear Server.

5.5.1.2 Printed Queue

Jobs sent to the hold or print queues are stored in the printed queue on the Fiery, if enabled. The administrator can define the number of jobs kept in the printed queue.

5.5.1.3 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 skips other waiting to process jobs

-
- The Fiery 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.
 - Jobs 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
- On Linux systems the system memory may overflow to use the swap partition on the HDD as a memory buffer.

5.5.1.4 Job Deletion

When a job is deleted from the Fiery, either automatically or using Fiery tools, the job cannot be viewed or retrieved using Fiery tools. If the job was spooled to the Fiery HDD, elements of the job may remain on the HDD and could theoretically be recovered with certain tools.

5.5.1.5 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 the 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 (3) times.

The following limitations and restrictions apply to secure erase:

The following limitations and restrictions apply to secure erase:

- Does not apply to job files not located in systems other than the Fiery such as
 -
 - Copies of the job that are load balanced to another Fiery
 - Copies of the job that are archived to media or network drives
 - Copies of the job that are located on client workstations.
 - Pages of a job that are 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, it is not guaranteed that the job will be fully deleted.
- Jobs submitted through the following methods-
 - Submitted through FTP server.
 - Submitted through a Novell pserver.
- When printing via SMB, the print job goes through the spooler on the Fiery which saves the job to disk. The Fiery System SW has no control over this, hence the system cannot securely erase the job.
- Does not delete any job data that may have been written to disk due to disk swapping and disk caching.

Note: Disk swapping occurs when memory needs to be swapped to disk to create more virtual memory than there is physical memory. This is handled in the OS layer and the Fiery has no control of this. However, disk swap space is regularly re-written during OS operation as various segments of memory are moved between memory and disk. This can lead to some segments of the job being stored to disk temporarily.

Note: Disk caching is set to ON for servers thus the job file is overwritten 3x in the cache and may only be overwritten 1x on the drive itself depending on the cache flushing algorithm.

5.5.1.6 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.

5.5.2 Secure Print

The secure print function requires the user to enter a job-specific password at the Fiery to allow the job to print. This feature requires an LCD interface local to the Fiery.

The purpose of this feature 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.

5.5.2.1 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 LE.

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.

5.5.3 Group Printing

Requires the user to enter a valid group name/password match for the job to start printing. The group name/password can be entered from an EFI tool with Notes functionality, such as the Fiery Driver or the Command WorkStation. The group name is included in the Job Log when the job prints.

The purpose of this feature is to (a) require users to submit a pre-defined group name with every job for accounting purposes and (b) limit printing to individuals who have valid group name/passwords.

5.5.3.1 Workflow

The user enters a Group Name and Group Password in the driver, creates and prints the job. When the Fiery begins to process the job, the Fiery checks the group name/group password with the Fiery's internal printing group list. If the group name/group password

is a valid match, the job will continue to process. If the group name/group password is not a valid match, the job will generate an error and move to the printed queue.

This feature can be enabled/disabled from the LCD.

5.5.3.2 Limitations

The group name and password strings in the job are not encrypted and can be read from the print job.

Because the system only checks for the password before ripping, it is possible to load balance a RIPPed job from a similar Fiery and still print an unauthorized file. It is also possible to change the password and group strings of a RIPPed job with Command Workstation and print.

The list of passwords on the Fiery is not encrypted when stored on the Fiery.

5.5.4 Email printing

The Fiery will receive and print jobs sent via email. The administrator can store a list on the Fiery of authorized email address; any email received with an email address not in the authorized email address list will be deleted.

5.5.5 Job Management

Jobs submitted to the Fiery can only be acted upon by using a Fiery job management utility with either administrator or operator access. Guest users (those 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. Setup information such as the Fiery administrator passwords, Fiery Operator passwords, and Novell passwords are sent to the Fiery in plain text.

5.5.6 Job Log

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

A user with operator access can view, export, or print the job log from the following tools:

- Command WorkStation
- Command WorkStation LE
- WebSpooler
- Fiery Spooler

A user with administrator access can delete the job log from the following tools:

- Command WorkStation
- Command WorkStation LE
- WebSpooler
- Fiery Spooler

A user with guest access can print the job log from the Fiery LCD on certain Fierys. Other Fierys 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.

5.5.7 Setup

Setup requires an administrator password. The Fiery can be setup up or configured from the Fiery LCD or a remote Setup application run from the WebTools or Command WorkStation.

5.5.8 Scanning

The Fiery 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 from 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 for distribution or storage and retrieval. All scanned documents are written to disk. The administrator can configure the Fiery to delete scan jobs automatically after a predefined length of stay on the Fiery.

Scan jobs can be distributed via the following methods:

- Email – sent to a mail server where it is routed to the desired email destination. Note: if the file size is greater than the administrator-defined maximum, the job is stored on the Fiery HDD, accessible through a URL.
- FTP – sent to an FTP destination. A record of the transfer, including the destination, is kept in the FTP log (accessible from the LCD Print Pages command). An FTP Proxy Server can be defined to send the job through a firewall.
- Fiery Hold Queue – sent to the Fiery Hold Queue (see Printing, above) and is not kept as a scan job
- Internet Fax – sent to a mail server where it is routed to the desired internet fax destination.
- Mailbox – stored on the Fiery with a mailbox code number. The user needs to enter the correct mailbox number to access the stored scan job. Some Fiery versions also require a password. The scan job is stored in a manner to allow retrieval through a URL.

5.6 Anti-virus software

The operating system is a dedicated operating system, and therefore does not have all the functionality of a complete operating system. The Fiery Controller was not designed to accept applications such as virus protection software as part of its operational model. This was done intentionally to help prevent the loading of potentially malicious software on the units, as well as to control the impact adding such applications would have on a system's operation and performance.

5.6.1 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. The Fiery 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 and treated as such.

6 General Security Features with System 6

6.1 Components of an External Network Print Controller

A network print controller is a self-contained unit composed of:

-
- Intel based server with the Windows XPe operating system
 - Proprietary EFI software providing networking, rasterizing, color management, and job management functions

6.1.1 Intel based Server Hardware

- Intel Pentium CPU
- IDE hard disk drive
- EEPROM holding general software BIOS. The CMOS, backed up by an onboard battery, holds the BIOS setup information
- Windows XPe
- Anti-Virus software support

6.1.2 Proprietary EFI software

- Command Workstation 4 providing distributed job management capabilities
- NetWise providing network software to manage communication through these external ports
- Raster Image Processor (RIP) to rasterize incoming print jobs for marking by a print engine
- Video interface to pass the rasterized print jobs to the engine for printing

When the Fiery is connected to a network, it behaves as a networked PostScript and/or PCL printer.

6.2 General Authentication

With external Fiery Advanced Controller Interface (FACI)-enabled Fiery Controllers, there are two levels of authentication: the Microsoft Windows login and Fiery login. The Microsoft Windows login authentication mechanism is determined by rules and policies determined by the operating system and the system administrator.

6.2.1 Fiery Software Authentication

The Fiery network controller 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. 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 allow access to the following functionality:

- Administrator – full control over all Fiery functionality
- Operator – same as Administrator, except no access to some server functions, such as setup, and cannot delete the job log
- Guest (default; no password) – same as Operator, except cannot access the job log, cannot make edits or status changes to print jobs.

6.3 Operating System Environment

6.3.1 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 protects Fiery functionality, such as the based software and optional "pay-for" packages. Changes to the BIOS (or removal of the BIOS) prevent the Fiery from functioning properly.

Configuration page – the Configuration page lists the values specified during setup. Some information, such as FTP proxy information, password information, and SNMP Community Names are not included on the configuration page.

6.3.2 Windows XPe

The Fiery ships with a default Windows XPe 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 includes, but is not limited to the file system, system security policy, and registry entries. In addition, this allows anyone to change the administrator password and deny access to the Fiery for other users.

If the Windows Administrator password is enabled and not entered into the system, the user is prohibited from accessing the Fiery from a FACI kit. The Fiery system software functions normally and users can access Fiery 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). Setup information such as the Fiery Administrator password or Fiery Operator password is stored in the registry as plain text.

6.3.2.1 Microsoft Security Patches

Microsoft regularly issues security patches to address potential security holes in the Windows XP operating system. EFI carefully monitors these patches and makes recommendations to our customers about which patches are applicable to the Fiery. Not all Windows XP patches are applicable to the Windows XPe operating system.

6.3.3 Local interface

The user can access the Fiery functions via the FACI kit (if enabled) or the Fiery LCD. The Windows Administrator password is used to control access to the Fiery if the FACI kit is enabled. The Fiery LCD only provides access to the Fiery functionality.

6.4 Connectivity to the Fiery

6.4.1 Physical Ports

The Fiery can be connected through the following external ports:

| Fiery Ports | Function | Access |
|----------------------------|---------------------------------|--|
| Interface Ports | Copier/printer connection (DDI) | |
| 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 |
| Parallel Port | Parallel connection | Bisynchronous whatever communication limited to receiving print jobs via a parallel cable. |
| USB Port | USB device connection | Plug and play connector designed for use with optional removable media devices |

6.4.2 Network Ports

The Fiery allows the user to selectively enable/disable the following IP ports:

| TCP | UPD | Port Name | Dependent Service(s) |
|---------------------|-------|---------------|---|
| 80 | | HTTP | WebTools, IPP |
| | 123 | NTP | Network Time Protocol |
| 135 | | MS RPC | Microsoft RPC Service |
| 137-139 | | NETBIOS | Windows Printing |
| | 161-2 | SNMP | WebTools, Velocity, some legacy utilities, other SNMP-based tools |
| 445 | | SMB/IP | SMB over TCP/IP |
| 515 | | LPD | LPR printing, WebTools, some legacy utilities |
| 631 | | IPP | IPP |
| 8021-8022, 21030 | 9906 | Harmony | CWS4, Velocity, EFI SDK-based tools, Fiery Driver bi-di functions |
| 9100-9103 | | Printing Port | Port 9100 |

Other TCP ports, except those specified by the OEM, are disabled. Any service dependent on a disabled port is automatically disabled.

The Fiery administrator can also enable/disable the different network services provided by the Fiery.

The local administrator can define SNMP read/write community names.

6.4.2.1 IP Filtering

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

6.5 Fiery Document Flow

The user can submit and manage jobs in a variety of methods to the Fiery. Some methods have some security associated with them; these are discussed below.

6.5.1 Standard Printing

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

- Hold Queue
- Print Queue
- Direct Queue (Direct connection)

The Fiery Administrator can disable the Print and Direct queues to limit automatic printing. With passwords enabled on the Fiery, this 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 will not accept new jobs.

6.5.1.1 *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. 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 LE or Clear Server.

6.5.1.2 *Printed Queue*

Jobs sent to the hold or print queues are stored in the printed queue on the Fiery, if enabled. The administrator can define the number of jobs kept in the printed queue.

6.5.1.3 *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 skips other waiting to process jobs
- The Fiery 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.
- Jobs are not written to the printed queue. However, they appear in the job log.

Note: *only one client can print 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 are 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
- On Windows systems the system memory may use the swap file on the HDD as a memory buffer.

6.5.1.4 *Job Deletion*

When a job is deleted from the Fiery, either automatically or using Fiery tools, the job cannot be viewed or retrieved using Fiery tools. If the job was spooled to the Fiery HDD, elements of the job may remain on the HDD and could theoretically be recovered with certain tools.

6.5.1.5 *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 the 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 (3) times.

The following limitations and restrictions apply to secure erase:

The following limitations and restrictions apply to secure erase:

- Does not apply to job files not located in systems other than the Fiery such as
 -
 - Copies of the job that are load balanced to another Fiery
 - Copies of the job that are archived to media or network drives
 - Copies of the job that are located on client workstations.
 - Pages of a job that are 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, it is not guaranteed that the job will be fully deleted.
- Jobs submitted through the following methods-
 - Submitted through FTP server.
 - Submitted through a Novell pserver.
- When printing via SMB, the print job goes through the spooler on the Fiery which saves the job to disk. The Fiery System SW has no control over this, hence the system cannot securely erase the job.
- Does not delete any job data that may have been written to disk due to disk swapping and disk caching.

Note: Disk swapping occurs when memory needs to be swapped to disk to create more virtual memory than there is physical memory. This is handled in the OS layer and the Fiery has no control of this. However, disk swap space is regularly re-written during OS operation as various segments of memory are moved between memory and disk. This can lead to some segments of the job being stored to disk temporarily.

Note: Disk caching is set to ON for servers thus the job file is overwritten 3x in the cache and may only be overwritten 1x on the drive itself depending on the cache flushing algorithm.

6.5.1.6 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.

6.5.2 Secure Print

The secure print function requires the user to enter a job-specific password at the Fiery to allow the job to print. This feature requires an LCD interface local to the Fiery.

The purpose of this feature 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.

6.5.2.1 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 LE.*

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 extracted from the print job.*

6.5.3 Group Printing

Requires the user to enter a valid group name/password match for the job to start printing. The group name/password can be entered from an EFI tool with Notes functionality, such as the Fiery Driver or the Command WorkStation. The group name is included in the Job Log when the job prints.

The purpose of this feature is to (a) require users to submit a pre-defined group name with every job for accounting purposes and (b) limit printing to individuals who have valid group name/passwords.

6.5.3.1 Workflow

The user enters a Group Name and Group Password in the driver, creates and prints the job. When the Fiery begins to process the job, the Fiery checks the group name/group password with the Fiery's internal printing group list. If the group name/group password is a valid match, the job will continue to process. If the group name/group password is not a valid match, the job will generate an error and move to the printed queue.

This feature can be enabled/disabled from the LCD.

6.5.3.2 Limitations

The group name and password strings in the job are not encrypted and can be read from the print job.

Because the system only checks for the password before ripping, it is possible to load balance a RIPPed job from a similar Fiery and still print an unauthorized file. It is also possible to change the password and group strings of a RIPPed job with Command Workstation and print.

The list of passwords on the Fiery is not encrypted when stored on the Fiery.

6.5.4 Email printing

The Fiery will receive and print jobs sent via email. The administrator can store a list on the Fiery of authorized email address; any email received with an email address not in the authorized email address list will be deleted.

6.5.5 Job Management

Jobs submitted to the Fiery can only be acted upon by using a Fiery job management utility with either administrator or operator access. Guest users (those 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. Setup information such as the Fiery administrator passwords, Fiery Operator passwords, and Novell passwords are sent to the Fiery in plain text.

6.5.6 Job Log

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

A user with operator access can view, export, or print the joblog from the following tools:

- Command WorkStation
- Command WorkStation LE
- WebSpooler
- Fiery Spooler

A user with administrator access can delete the job log from the following tools:

- Command WorkStation
- Command WorkStation LE
- WebSpooler
- Fiery Spooler

A user with guest access can print the job log from the Fiery LCD on certain Fierys. Other Fierys 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.

6.5.7 Setup

Setup requires an administrator password. The Fiery can be setup up or configured from the Fiery LCD, the Fiery Setup program run from a Windows Fiery with a FACI kit, or a remote Setup application run from the WebTools or Command WorkStation.

6.5.8 Scanning

The Fiery 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 from 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 for distribution or storage and retrieval. All scanned documents are written to disk. The administrator can configure the Fiery to delete scan jobs automatically after a predefined length of stay on the Fiery.

Scan jobs can be distributed via the following methods:

- Email – sent to a mail server where it is routed to the desired email destination. Note: if the file size is greater than the administrator-defined maximum, the job is stored on the Fiery HDD, accessible through a URL.
- FTP – sent to an FTP destination. A record of the transfer, including the destination, is kept in the FTP log (accessible from the LCD Print Pages command). An FTP Proxy Server can be defined to send the job through a firewall.
- Fiery Hold Queue – sent to the Fiery Hold Queue (see Printing, above) and is not kept as a scan job
- Internet Fax – sent to a mail server where it is routed to the desired internet fax destination.
- Mailbox – stored on the Fiery with a mailbox code number. The user needs to enter the correct mailbox number to access the stored scan job. Some Fiery versions also require a password. The scan job is stored in a manner to allow retrieval through a URL.

6.6 Anti-virus software

Administrators can install anti-virus software on FACI-enabled Windows XPe-based Fierys to protect against the accidental introduction of viruses on the Fiery.

Anti-virus software should only be run when the Fiery is idle and not receiving jobs. This helps prevent unforeseeable errors that may result if antivirus software acts while the Fiery attempts to process a job.

The anti-virus software should scan for files coming into the Fiery outside of the normal printstream. This includes:

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

The anti-virus software can also be configured to scan all files on the Fiery when the Fiery is not planned for use for an extended period of time.

EFI tests System 5.5 Fiery products with McAfee VirusScan software; similar products from Symantec and TrendMicro are also compatible with the Fiery when used as described above.

6.6.1 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. The Fiery 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 and treated as such.

7 General Security Features with System 7e

7.1 Components of an Embedded Network Print Controller

A network print controller is a self-contained unit composed of:

- Intel based processor with a Linux operating system
- Proprietary EFI software providing networking, rasterizing, color management, and job management functions

7.1.1 Intel based Embedded Hardware

- Intel mobile Pentium CPU
- IDE Hard Drive
- EEPROM holding general software BIOS. The CMOS, backed up by an onboard battery, holds the BIOS setup information
- Linux operating system

7.1.2 Proprietary EFI software

- Command Workstation 4 providing distributed job management capabilities
- Netwise providing network software to manage communication through these external ports
- Raster Image Processor (RIP) to rasterize incoming print jobs for marking by a print engine
- Video interface to pass the rasterized print jobs to the engine for printing

7.2 General Authentication

The Fiery network controller defines Administrator, Operator, and Guest users with different privileges. It is recommended that administrators require passwords to access the Fiery..

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

- Administrator – full control over all Fiery functionality
- Operator – same as Administrator, except no access to some server functions, such as setup, and cannot delete the job log
- Guest (default; no password) – same as Operator, except cannot access the job log, cannot make edits or status changes to print jobs.

7.3 Operating System Environment

7.3.1 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 from functioning properly.

Configuration page – the Configuration page lists the values specified during setup. Some information, such as FTP proxy information, password information, and SNMP Community Names are not included on the configuration page.

7.3.2 Linux

Linux systems do not include a local interface that allows access to the operating system.

7.3.3 Local interface

The Fiery LCD only provides access to the Fiery functionality.

7.4 Connectivity to the Fiery

7.4.1 Physical Ports

The Fiery can be connected through the following external ports:

| Fiery Ports | Function | Access |
|----------------------------|---------------------------------|--|
| Interface Ports | Copier/printer connection (DDI) | |
| Serial port | Diablo interface | |
| 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 |
| Parallel Port | Parallel connection | Bisynchronous whatever communication limited to receiving print jobs via a parallel cable. |

7.4.2 Network Ports

The Fiery allows the user to selectively enable/disable the following IP ports:

| TCP | UPD | Port Name | Dependent Service(s) |
|-----------|-------|---------------|---|
| 80 | | HTTP | WebTools, IPP |
| 137-139 | | NETBIOS | Windows Printing |
| | 161-2 | SNMP | WebTools, Velocity, some legacy utilities, other SNMP-based tools |
| 515 | | LPD | LPR printing, WebTools, some legacy utilities |
| 631 | | IPP | IPP |
| 8021-8022 | | Harmony | CWS4, Velocity, EFI SDK-based tools, Fiery Driver bi-di functions |
| 9100-9103 | | Printing Port | Port 9100 |

Other TCP ports, except those specified by the OEM, are disabled. Any service dependent on a disabled port is automatically disabled.

The Fiery administrator can also enable/disable the different network services provided by the Fiery.

The local administrator can define SNMP read/write community names.

7.4.2.1 IP Filtering

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

7.5 Fiery Document Flow

The user can submit and manage jobs in a variety of methods to the Fiery. Some methods have some security associated with them; these are discussed below.

7.5.1 Standard Printing

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

- Hold Queue
- Print Queue
- Direct Queue (Direct Connection)

The Fiery Administrator can disable the Print and Direct queues to limit automatic printing. With passwords enabled on the Fiery, this 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 will not accept new jobs.

7.5.1.1 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. 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 LE or Clear Server.

7.5.1.2 Printed Queue

Jobs sent to the hold or print queues are stored in the printed queue on the Fiery, if enabled. The administrator can define the number of jobs kept in the printed queue.

7.5.1.3 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 skips other waiting to process jobs
- The Fiery 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.
- Jobs 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
- On Linux systems the system memory may overflow to use the swap partition on the HDD as a memory buffer.

7.5.1.4 Job Deletion

When a job is deleted from the Fiery, either automatically or using Fiery tools, the job cannot be viewed or retrieved using Fiery tools. If the job was spooled to the Fiery HDD, elements of the job may remain on the HDD and could theoretically be recovered with certain tools.

7.5.1.5 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 the 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 (3) times.

The following limitations and restrictions apply to secure erase:

- Does not apply to job files not located in systems other than the Fiery such as
 - Copies of the job that are load balanced to another Fiery
 - Copies of the job that are archived to media or network drives
 - Copies of the job that are located on client workstations.
 - Pages of a job that are 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, it is not guaranteed that the job will be fully deleted.
 - Jobs submitted through the following methods-
 - Submitted through FTP server.
 - Submitted through a Novell pserver.
 - When printing via SMB, the print job goes through the spooler on the Fiery which saves the job to disk. The Fiery System SW has no control over this, hence the system cannot securely erase the job.
 - Does not delete any job data that may have been written to disk due to disk swapping and disk caching.

Note: Disk swapping occurs when memory needs to be swapped to disk to create more virtual memory than there is physical memory. This is handled in the OS layer and the Fiery has no control of this. However, disk swap space is regularly re-written during OS operation as various segments of memory are moved between memory and disk. This can lead to some segments of the job being stored to disk temporarily.

Note: Disk caching is set to ON for servers thus the job file is overwritten 3x in the cache and may only be overwritten 1x on the drive itself depending on the cache flushing algorithm.

7.5.1.6 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.

7.5.2 Secure Print

The secure print function requires the user to enter a job-specific password at the Fiery to allow the job to print. This feature requires an LCD interface local to the Fiery.

The purpose of this feature 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.

7.5.2.1 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 LE.*

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.*

7.5.3 Group Printing

Requires the user to enter a valid group name/password match for the job to start printing. The group name/password can be entered from an EFI tool with Notes functionality, such as the Fiery

Driver or the Command WorkStation. The group name is included in the Job Log when the job prints.

The purpose of this feature is to (a) require users to submit a pre-defined group name with every job for accounting purposes and (b) limit printing to individuals who have valid group name/passwords.

7.5.3.1 *Workflow*

The user enters a Group Name and Group Password in the driver, creates and prints the job. When the Fiery begins to process the job, the Fiery checks the group name/group password with the Fiery's internal printing group list. If the group name/group password is a valid match, the job will continue to process. If the group name/group password is not a valid match, the job will generate an error and move to the printed queue.

This feature can be enabled/disabled from the LCD.

7.5.3.2 *Limitations*

The group name and password strings in the job are not encrypted and can be read from the print job.

Because the system only checks for the password before ripping, it is possible to load balance a RIPped job from a similar Fiery and still print an unauthorized file. It is also possible to change the password and group strings of a RIPped job with Command Workstation and print.

The list of passwords on the Fiery is not encrypted when stored on the Fiery.

7.5.4 Email printing

The Fiery will receive and print jobs sent via email. The administrator can store a list on the Fiery of authorized email address; any email received with an email address not in the authorized email address list will be deleted.

7.5.5 Job Management

Jobs submitted to the Fiery can only be acted upon by using a Fiery job management utility with either administrator or operator access. Guest users (those 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. Setup information such as the Fiery administrator passwords, Fiery Operator passwords, and Novell passwords are sent to the Fiery in plain text.

7.5.6 Job Log

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

A user with operator access can view, export, or print the job log from the following tools:

- Command WorkStation
- Command WorkStation LE
- WebSpooler
- Fiery Spooler

A user with administrator access can delete the job log from the following tools:

-
- Command WorkStation
 - Command WorkStation LE
 - WebSpooler
 - Fiery Spooler

A user with guest access can print the job log from the Fiery LCD on certain Fierys. Other Fierys 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.

7.5.7 Setup

Setup requires an administrator password. The Fiery can be setup up or configured from the Fiery LCD or a remote Setup application run from the WebTools or Command WorkStation.

7.5.8 Scanning

The Fiery 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 from 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 for distribution or storage and retrieval. All scanned documents are written to disk. The administrator can configure the Fiery to delete scan jobs automatically after a predefined length of stay on the Fiery.

Scan jobs can be distributed via the following methods:

- Email – sent to a mail server where it is routed to the desired email destination. Note: if the file size is greater than the administrator-defined maximum, the job is stored on the Fiery HDD, accessible through a URL.
- FTP – sent to an FTP destination. A record of the transfer, including the destination, is kept in the FTP log (accessible from the LCD Print Pages command). An FTP Proxy Server can be defined to send the job through a firewall.
- Fiery Hold Queue – sent to the Fiery Hold Queue (see Printing, above) and is not kept as a scan job
- Internet Fax – sent to a mail server where it is routed to the desired internet fax destination.
- Mailbox – stored on the Fiery with a mailbox code number. The user needs to enter the correct mailbox number to access the stored scan job. Some Fiery versions also require a password. The scan job is stored in a manner to allow retrieval through a URL.

7.6 Anti-virus software

The operating system is a dedicated operating system, and therefore does not have all the functionality of a complete operating system. The Fiery Controller was not designed to accept applications such as virus protection software as part of its operational model. This was done intentionally to help prevent the loading of potentially malicious software on the units, as well as to control the impact adding such applications would have on a system's operation and performance.

7.6.1 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. The Fiery 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 and treated as such.

8 General Security Features with System 7

8.1 Components of an External Network Print Controller

A network print controller is a self-contained unit composed of:

- Intel based server with the Windows XPe operating system
- Proprietary EFI software providing networking, rasterizing, color management, and job management functions

8.1.1 Intel based Server Hardware

- Intel Pentium CPU
- IDE hard disk drive
- EEPROM holding general software BIOS. The CMOS, backed up by an onboard battery, holds the BIOS setup information
- Windows XPe
- Anti-Virus software support

8.1.2 Proprietary EFI software

- Command Workstation 4 providing distributed job management capabilities
- NetWise providing network software to manage communication through these external ports
- Raster Image Processor (RIP) to rasterize incoming print jobs for marking by a print engine
- Video interface to pass the rasterized print jobs to the engine for printing

When the Fiery is connected to a network, it behaves as a networked PostScript and/or PCL printer.

8.2 General Authentication

With external Fiery Advanced Controller Interface (FACI)-enabled Fiery Controllers, there are two levels of authentication: the Microsoft Windows login and Fiery login. The Microsoft Windows login authentication mechanism is determined by rules and policies determined by the operating system and the system administrator.

8.2.1 Fiery Software Authentication

The Fiery network controller 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. 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 allow access to the following functionality:

- Administrator – full control over all Fiery functionality
- Operator – same as Administrator, except no access to some server functions, such as setup, and cannot delete the job log
- Guest (default; no password) – same as Operator, except cannot access the job log, cannot make edits or status changes to print jobs.

8.3 Operating System Environment

8.3.1 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 protects Fiery functionality, such as the based software and optional "pay-for" packages. Changes to the BIOS (or removal of the BIOS) prevent the Fiery from functioning properly.

Configuration page – the Configuration page lists the values specified during setup. Some information, such as FTP proxy information, password information, and SNMP Community Names are not included on the configuration page.

8.3.2 Windows XPe

The Fiery ships with a default Windows XPe 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 includes, but is not limited to the file system, system security policy, and registry entries. In addition, this allows anyone to change the administrator password and deny access to the Fiery for other users.

If the Windows Administrator password is enabled and not entered into the system, the user is prohibited from accessing the Fiery from a FACI kit. The Fiery system software functions normally and users can access Fiery 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). Setup information such as the Fiery Administrator password or Fiery Operator password is stored in the registry as plain text.

8.3.2.1 *Microsoft Security Patches*

Microsoft regularly issues security patches to address potential security holes in the Windows XP operating system. EFI carefully monitors these patches and makes recommendations to our customers about which patches are applicable to the Fiery. Not all Windows XP patches are applicable to the Windows XPe operating system.

Process for the Microsoft security patches:

1. On the second Tuesday of every month, Microsoft provides the latest security bulletins. EFI commits to have the XPe QFE available within 5 business days (actual average has been 2 to 3 business days).
2. EFI filters which bulletins are applicable to the Fiery server within 1 business day
3. EFI tests the XPe QFE for compatibility with the Fiery server
4. EFI creates a software wrapper to update the Fiery Configuration Page
5. EFI provides the XPe QFE to OEMs for distribution and make them available to Fiery System Updates where they are immediately available for the Fiery to download.

8.3.3 Local interface

The user can access the Fiery functions via the FACI kit (if enabled) or the Fiery LCD. The Windows Administrator password is used to control access to the Fiery if the FACI kit is enabled. The Fiery LCD only provides access to the Fiery functionality.

8.4 Connectivity to the Fiery

8.4.1 Physical Ports

The Fiery can be connected through the following external ports:

| Fiery Ports | Function | Access |
|----------------------------|---------------------------------|--|
| Interface Ports | Copier/printer connection (DDI) | |
| 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 |
| Parallel Port | Parallel connection | Bisynchronous whatever communication limited to receiving print jobs via a parallel cable. |
| USB Port | USB device connection | Plug and play connector designed for use with optional removable media devices |

8.4.2 Network Ports

The Fiery allows the user to selectively enable/disable the following IP ports:

| TCP | UPD | Port Name | Dependent Service(s) |
|---------------------|-------|---------------|---|
| 80 | | HTTP | WebTools, IPP |
| | 123 | NTP | Network Time Protocol |
| 135 | | MS RPC | Microsoft RPC Service |
| 137-139 | | NETBIOS | Windows Printing |
| | 161-2 | SNMP | WebTools, Velocity, some legacy utilities, other SNMP-based tools |
| 445 | | SMB/IP | SMB over TCP/IP |
| 515 | | LPD | LPR printing, WebTools, some legacy utilities |
| 631 | | IPP | IPP |
| 8021-8022, 21030 | 9906 | Harmony | CWS4, Velocity, EFI SDK-based tools, Fiery Driver bi-di functions |
| 9100-9103 | | Printing Port | Port 9100 |

Other TCP ports, except those specified by the OEM, are disabled. Any service dependent on a disabled port is automatically disabled.

The Fiery administrator can also enable/disable the different network services provided by the Fiery.

The local administrator can define SNMP read/write community names.

8.4.2.1 IP Filtering

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

8.5 Fiery Document Flow

The user can submit and manage jobs in a variety of methods to the Fiery. Some methods have some security associated with them; these are discussed below.

8.5.1 Standard Printing

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

- Hold Queue
- Print Queue
- Direct Queue (Direct connection)

The Fiery Administrator can disable the Print and Direct queues to limit automatic printing. With passwords enabled on the Fiery, this 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 will not accept new jobs.

8.5.1.1 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. 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 LE or Clear Server.

8.5.1.2 Printed Queue

Jobs sent to the hold or print queues are stored in the printed queue on the Fiery, if enabled. The administrator can define the number of jobs kept in the printed queue.

8.5.1.3 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 skips other waiting to process jobs
- The Fiery 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.
- Jobs are not written to the printed queue. However, they appear in the job log.

Note: only one client can print 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 are 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
- On Windows systems the system memory may use the swap file on the HDD as a memory buffer.

8.5.1.4 *Job Deletion*

When a job is deleted from the Fiery, either automatically or using Fiery tools, the job cannot be viewed or retrieved using Fiery tools. If the job was spooled to the Fiery HDD, elements of the job may remain on the HDD and could theoretically be recovered with certain tools.

8.5.1.5 *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 the 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 (3) times.

The following limitations and restrictions apply to secure erase:

- Does not apply to job files not located in systems other than the Fiery such as
 -
 - Copies of the job that are load balanced to another Fiery
 - Copies of the job that are archived to media or network drives
 - Copies of the job that are located on client workstations.
 - Pages of a job that are 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, it is not guaranteed that the job will be fully deleted.
- Jobs submitted through the following methods-
 - Submitted through FTP server.
 - Submitted through a Novell pserver.
- When printing via SMB, the print job goes through the spooler on the Fiery which saves the job to disk. The Fiery System SW has no control over this, hence the system cannot securely erase the job.
- Does not delete any job data that may have been written to disk due to disk swapping and disk caching.

Note: Disk swapping occurs when memory needs to be swapped to disk to create more virtual memory than there is physical memory. This is handled in the OS layer and the Fiery has no control of this. However, disk swap space is regularly re-written during OS operation as various segments of memory are moved between memory and disk. This can lead to some segments of the job being stored to disk temporarily.

Note: Disk caching is set to ON for servers thus the job file is overwritten 3x in the cache and may only be overwritten 1x on the drive itself depending on the cache flushing algorithm.

8.5.1.6 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.

8.5.2 Secure Print

The secure print function requires the user to enter a job-specific password at the Fiery to allow the job to print. This feature requires an LCD interface local to the Fiery.

The purpose of this feature 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.

8.5.2.1 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 LE.

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 extracted from the print job.

8.5.3 Group Printing

Requires the user to enter a valid group name/password match for the job to start printing. The group name/password can be entered from an EFI tool with Notes functionality, such as the Fiery Driver or the Command WorkStation. The group name is included in the Job Log when the job prints.

The purpose of this feature is to (a) require users to submit a pre-defined group name with every job for accounting purposes and (b) limit printing to individuals who have valid group name/passwords.

8.5.3.1 Workflow

The user enters a Group Name and Group Password in the driver, creates and prints the job. When the Fiery begins to process the job, the Fiery checks the group name/group password with the Fiery's internal printing group list. If the group name/group password is a valid match, the job will continue to process. If the group name/group password is not a valid match, the job will generate an error and move to the printed queue.

This feature can be enabled/disabled from the LCD.

8.5.3.2 Limitations

The group name and password strings in the job are not encrypted and can be read from the print job.

Because the system only checks for the password before ripping, it is possible to load balance a RIPPed job from a similar Fiery and still print an unauthorized file. It is also possible to change the password and group strings of a RIPPed job with Command Workstation and print.

The list of passwords on the Fiery is not encrypted when stored on the Fiery.

8.5.4 Email printing

The Fiery will receive and print jobs sent via email. The administrator can store a list on the Fiery of authorized email address; any email received with an email address not in the authorized email address list will be deleted.

8.5.5 Job Management

Jobs submitted to the Fiery can only be acted upon by using a Fiery job management utility with either administrator or operator access. Guest users (those 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. Setup information such as the Fiery administrator passwords, Fiery Operator passwords, and Novell passwords are sent to the Fiery in plain text.

8.5.6 Job Log

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

A user with operator access can view, export, or print the joblog from the following tools:

- Command WorkStation
- Command WorkStation LE
- WebSpooler
- Fiery Spooler

A user with administrator access can delete the job log from the following tools:

- Command WorkStation
- Command WorkStation LE
- WebSpooler
- Fiery Spooler

A user with guest access can print the job log from the Fiery LCD on certain Fierys. Other Fierys 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.

8.5.7 Setup

Setup requires an administrator password. The Fiery can be setup up or configured from the Fiery LCD, the Fiery Setup program run from a Windows Fiery with a FACI kit, or a remote Setup application run from the WebTools or Command WorkStation.

8.5.8 Scanning

The Fiery 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 from 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 for distribution or storage and retrieval. All scanned documents are written to disk. The administrator can configure the Fiery to delete scan jobs automatically after a predefined length of stay on the Fiery.

Scan jobs can be distributed via the following methods:

- Email – sent to a mail server where it is routed to the desired email destination. Note: if the file size is greater than the administrator-defined maximum, the job is stored on the Fiery HDD, accessible through a URL.
- FTP – sent to an FTP destination. A record of the transfer, including the destination, is kept in the FTP log (accessible from the LCD Print Pages command). An FTP Proxy Server can be defined to send the job through a firewall.
- Fiery Hold Queue – sent to the Fiery Hold Queue (see Printing, above) and is not kept as a scan job
- Internet Fax – sent to a mail server where it is routed to the desired internet fax destination.
- Mailbox – stored on the Fiery with a mailbox code number. The user needs to enter the correct mailbox number to access the stored scan job. Some Fiery versions also require a password. The scan job is stored in a manner to allow retrieval through a URL.

8.6 System Update

System Updates will keep the Fiery up-to-date by periodically contacting the update server on the internet. If a critical OS update is available, System Updates will download the update to the Fiery automatically and notify the user via LCD/ copier panel and/or FACL. System Updates allows scheduled automatic installation at preset time of the day and restarts the Fiery automatically as needed. This will keep the Fiery up-to-date without user-intervention.

Alternatively, the administrator can disable auto download and/or installation and initiate them manually. System Updates will only download and install critical Windows XPe updates issued by Microsoft as well as Fiery patches.

All updates and patches will be displayed/listed in the config page.

8.7 Anti-virus software

Administrators can install anti-virus software on FACL-enabled Windows XPe-based Fierys to protect against the accidental introduction of viruses on the Fiery.

Anti-virus software should only be run when the Fiery is idle and not receiving jobs. This helps prevent unforeseeable errors that may result if antivirus software acts while the Fiery attempts to process a job.

The anti-virus software should scan for files coming into the Fiery outside of the normal printstream. This includes:

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

The anti-virus software can also be configured to scan all files on the Fiery when the Fiery is not planned for use for an extended period of time.

EFI tests System 5.5 Fiery products with McAfee VirusScan software; similar products from Symantec and TrendMicro are also compatible with the Fiery when used as described above.

8.7.1 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. The Fiery 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 and treated as such.

9 General Security Features with System 8e

9.1 Components of an Embedded Network Print Controller

A network print controller is a self-contained unit composed of:

- Intel based processor with a Linux operating system
- Proprietary EFI software providing networking, rasterizing, color management, and job management functions

9.1.1 Intel based Embedded Hardware

- Intel mobile Pentium CPU
- IDE Hard Drive
- EEPROM holding general software BIOS. The CMOS, backed up by an onboard battery, holds the BIOS setup information
- Linux operating system

9.1.2 Proprietary EFI software

- Command Workstation 4 providing distributed job management capabilities
- Netwise providing network software to manage communication through these external ports
- Raster Image Processor (RIP) to rasterize incoming print jobs for marking by a print engine
- Video interface to pass the rasterized print jobs to the engine for printing

9.2 User Authentication

The Fiery user authentication feature allows the Fiery to:

- Authenticate user names
- Authorize actions based on the user's privileges

The Fiery can authenticate users who are:

- Domain-based: users defined on a corporate server and accessed via LDAP
- Fiery-based: users defined on the Fiery

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

The Fiery admin can modify the membership of any Fiery Group (with the exception of the admin, operator, and guest users).

For this version of User Authentication, the different privilege levels that can be edited/selected for a group are the following:

- Print in B&W - This privilege allows the members of a group to print jobs on the Fiery. If the user does not have the "Print in Color and B&W" privilege, the Fiery will force the job to print in black & white.
- Print in Color and B&W - This privilege allows the members of a group to print jobs on the Fiery with full access to the color AND grayscale printing capabilities of the Fiery. Without this or the Print in B&W privilege, the print job will fail to print. Without this or the Print in B&W privilege, user will not be able to submit the job via FTP (color devices only).
- Fiery Mailbox - This privilege allows the members of a group to have individual mailboxes. The Fiery 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.

9.3 Operating System Environment

9.3.1 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 from functioning properly.

Configuration page – the Configuration page lists the values specified during setup. Some information, such as FTP proxy information, password information, and SNMP Community Names are not included on the configuration page.

9.3.2 Linux

Linux systems do not include a local interface that allows access to the operating system.

9.3.3 Local interface

The Fiery LCD only provides access to the Fiery functionality.

9.4 Connectivity to the Fiery

9.4.1 Physical Ports

The Fiery can be connected through the following external ports:

| Fiery Ports | Function | Access |
|--------------------------|---------------------------------|--|
| Interface Ports | Copier/printer connection (DDI) | |
| Serial port | Diablo interface | |
| 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 |
| Parallel Port | Parallel connection | Bisynchronous whatever communication limited to receiving print jobs via a parallel cable. |

9.4.2 Network Ports

The Fiery allows the user to selectively enable/disable the following IP ports:

| TCP | UPD | Port Name | Dependent Service(s) |
|-----------|-------|---------------|---|
| 80 | | HTTP | WebTools, IPP |
| 137-139 | | NETBIOS | Windows Printing |
| | 161-2 | SNMP | WebTools, Velocity, some legacy utilities, other SNMP-based tools |
| 515 | | LPD | LPR printing, WebTools, some legacy utilities |
| 631 | | IPP | IPP |
| 8021-8022 | | Harmony | CWS4, Velocity, EFI SDK-based tools, Fiery Driver bi-di functions |
| 9100-9103 | | Printing Port | Port 9100 |

Other TCP ports, except those specified by the OEM, are disabled. Any service dependent on a disabled port is automatically disabled.

The Fiery administrator can also enable/disable the different network services provided by the Fiery.

The local administrator can define SNMP read/write community names.

9.4.2.1 IP Filtering

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

9.4.3 Network Encryption

9.4.3.1 IP Sec

IP Sec or IP Security Protocol provides security to IP protocols through encryption and authentication mechanisms. IP sec in the Fiery allows the Fiery to accept incoming data that supports IPsec using a specific authentication method as outlined in the following table.

The incoming data must contain the same 'authentication key' - otherwise, the incoming data will not be accepted by the Fiery.

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

9.4.3.2 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 supports 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 eavesdrop 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 can also 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 Active Directory. By default, LDAP traffic is transmitted unsecured. For LDAP communication over SSL or TLS, the client would have to have a certificate - verified by Verisign.

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

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

9.4.3.3 Certificate Management

Certificates are the way network clients authenticate themselves in network activities that perform identity verifications. The certification method is supported by SSL/TLS

(Secure Socket Layer/Transport Layer Security) that implements authentication through the exchange of certificates based on public/private keys according to the X509 standard.

In the Fiery, certificate management allows the Fiery admin to do the following:

- Add/Load/Browse for available digital certificates (created by a trusted authority) and private keys
- 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)

9.5 Encryption of Critical Information

Encryption of critical information in the Fiery ensures that all passwords and related configuration information are secure when stored in the Fiery. The encryption method used is based on the TwoFish method/algorithm of encryption. Encryption of Critical Information

Encryption of critical information in the Fiery ensures that all passwords and related configuration information are secure when stored in the Fiery. The encryption method used is based on the TwoFish method/algorithm of encryption.

9.5.1.1 *Crptographic Algorithms and Key Lengths*

For encrypting this sensitive information, EFI client applications use an implementation of the Twofish encryption algorithm. Twofish is a symmetric block cipher developed by Counterpane Labs, and was 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 Printer Controller and EFI client applications do not use proprietary encryption algorithms.

9.5.1.2 *Key Management and Algorithms*

To generate keys used for Twofish encryption, the Fiery Printer Controller 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 deterministically generate a 256-bit key for Twofish (that is, given the 32 bit shared secret key X, the generation algorithm will always produce the same 256 bit key Y).

9.6 Fiery Document Flow

The user can submit and manage jobs in a variety of methods to the Fiery. Some methods have some security associated with them; these are discussed below.

9.6.1 Standard Printing

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

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

The Fiery Administrator can disable the Print and Direct queues to limit automatic printing. With passwords enabled on the Fiery, this 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 will not accept new jobs.

9.6.1.1 *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. 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.

9.6.1.2 *Printed Queue*

Jobs sent to the hold or print queues are stored in the printed queue on the Fiery, if enabled. The administrator can define the number of jobs kept in the printed queue.

9.6.1.3 *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 skips other waiting to process jobs

-
- The Fiery 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.
 - Jobs 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
- On Linux systems the system memory may overflow to use the swap partition on the HDD as a memory buffer.

9.6.1.4 Job Deletion

When a job is deleted from the Fiery, either automatically or using Fiery tools, the job cannot be viewed or retrieved using Fiery tools. If the job was spooled to the Fiery HDD, elements of the job may remain on the HDD and could theoretically be recovered with certain tools.

9.6.1.5 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 the 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 (3) times.

The following limitations and restrictions apply to secure erase:

- Does not apply to job files not located in systems other than the Fiery such as
 -
 - Copies of the job that are load balanced to another Fiery
 - Copies of the job that are archived to media or network drives
 - Copies of the job that are located on client workstations.
 - Pages of a job that are 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, it is not guaranteed that the job will be fully deleted.
- Jobs submitted through the following methods-
 - Submitted through FTP server.
 - Submitted through a Novell pserver.
- When printing via SMB, the print job goes through the spooler on the Fiery which saves the job to disk. The Fiery System SW has no control over this, hence the system cannot securely erase the job.
- Does not delete any job data that may have been written to disk due to disk swapping and disk caching.

Note: Disk swapping occurs when memory needs to be swapped to disk to create more virtual memory than there is physical memory. This is handled in the OS layer and the Fiery has no control of this. However, disk swap space is regularly re-written during OS operation as various segments of memory are moved between memory and disk. This can lead to some segments of the job being stored to disk temporarily.

Note: Disk caching is set to ON for servers thus the job file is overwritten 3x in the cache and may only be overwritten 1x on the drive itself depending on the cache flushing algorithm.

9.6.1.6 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.

9.6.2 Secure Print

The secure print function requires the user to enter a job-specific password at the Fiery to allow the job to print. This feature requires an LCD interface local to the Fiery.

The purpose of this feature 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.

9.6.2.1 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.*

9.6.3 Email printing

The Fiery will receive and print jobs sent via email. The administrator can store a list on the Fiery of authorized email address; any email received with an email address not in the authorized email address list will be deleted.

9.6.4 Job Management

Jobs submitted to the Fiery can only be acted upon by using a Fiery job management utility with either administrator or operator access. Guest users (those 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. Setup information such as the Fiery administrator passwords, Fiery Operator passwords, and Novell passwords are sent to the Fiery in plain text.

9.6.5 Job Log

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

A user with operator access can view, export, or print the job log from the following tools:

- Command WorkStation
- Command WorkStation LE

A user with administrator access can delete the job log from the following tools:

- Command WorkStation
- Command WorkStation LE

A user with guest access can print the job log from the Fiery LCD on certain Fierys. Other Fierys 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.

9.6.6 Setup

Setup requires an administrator password. The Fiery can be setup up or configured from the Fiery LCD or a remote Setup application run from the WebTools or Command WorkStation.

9.6.7 Scanning

The Fiery 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 from 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 for distribution or storage and retrieval. All scanned documents are written to disk. The administrator can configure the Fiery to delete scan jobs automatically after a predefined length of stay on the Fiery.

Scan jobs can be distributed via the following methods:

- Email – sent to a mail server where it is routed to the desired email destination. Note: if the file size is greater than the administrator-defined maximum, the job is stored on the Fiery HDD, accessible through a URL.
- FTP – sent to an FTP destination. A record of the transfer, including the destination, is kept in the FTP log (accessible from the LCD Print Pages command). An FTP Proxy Server can be defined to send the job through a firewall.
- Fiery Hold Queue – sent to the Fiery Hold Queue (see Printing, above) and is not kept as a scan job
- Internet Fax – sent to a mail server where it is routed to the desired internet fax destination.
- Mailbox – stored on the Fiery with a mailbox code number. The user needs to enter the correct mailbox number to access the stored scan job. Some Fiery versions also require a password. The scan job is stored in a manner to allow retrieval through a URL.

9.7 Anti-virus software

The operating system is a dedicated operating system, and therefore does not have all the functionality of a complete operating system. The Fiery Controller was not designed to accept applications such as virus protection software as part of its operational model. This was done

intentionally to help prevent the loading of potentially malicious software on the units, as well as to control the impact adding such applications would have on a system's operation and performance.

9.7.1 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. The Fiery 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 and treated as such.

9.8 Removable HD Kit Option

The Fiery supports a removable hard drive option kit for increased security. This kit provide the user with the ability to both 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.

9.8.1 For Embedded

Embedded products can only offer removable HD as an OEM coordinated option, because the mounting location and bracketry 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.

10 General Security Features with System 8

10.1 Components of an External Network Print Controller

A network print controller is a self-contained unit composed of:

- Intel based server with the Windows XPe operating system
- Proprietary EFI software providing networking, rasterizing, color management, and job management functions

10.1.1 Intel based Server Hardware

- Intel Pentium CPU
- IDE hard disk drive
- EEPROM holding general software BIOS. The CMOS, backed up by an onboard battery, holds the BIOS setup information
- Windows XPe
- Anti-Virus software support

10.1.2 Proprietary EFI software

- Command Workstation 4 providing distributed job management capabilities
- NetWise providing network software to manage communication through these external ports
- Raster Image Processor (RIP) to rasterize incoming print jobs for marking by a print engine
- Video interface to pass the rasterized print jobs to the engine for printing

When the Fiery is connected to a network, it behaves as a networked PostScript and/or PCL printer.

10.2 User Authentication

The Fiery user authentication feature allows the Fiery to:

- Authenticate user names
- Authorize actions based on the user's privileges

The Fiery can authenticate users who are:

- Domain-based: users defined on a corporate server and accessed via LDAP
- Fiery-based: users defined on the Fiery

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

The Fiery admin can modify the membership of any Fiery Group (with the exception of the admin, operator, and guest users).

For this version of User Authentication, the different privilege levels that can be edited/selected for a group are the following:

- Print in B&W - This privilege allows the members of a group to print jobs on the Fiery. If the user does not have the "Print in Color and B&W" privilege, the Fiery will force the job to print in black & white.
- Print in Color and B&W - This privilege allows the members of a group to print jobs on the Fiery with full access to the color AND grayscale printing capabilities of the Fiery. Without this or the Print in B&W privilege, the print job will fail to print. Without this or the Print in B&W privilege, user will not be able to submit the job via FTP (color devices only).
- Fiery Mailbox - This privilege allows the members of a group to have individual mailboxes. The Fiery 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.

10.2.1 Fiery Software Authentication

The Fiery network controller 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. 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 allow access to the following functionality:

- Administrator – full control over all Fiery functionality
- Operator – same as Administrator, except no access to some server functions, such as setup, and cannot delete the job log
- Guest (default; no password) – same as Operator, except cannot access the job log, cannot make edits or status changes to print jobs.

10.3 Operating System Environment

10.3.1 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 protects Fiery functionality, such as the based software and optional "pay-for" packages. Changes to the BIOS (or removal of the BIOS) prevent the Fiery from functioning properly.

Configuration page – the Configuration page lists the values specified during setup. Some information, such as FTP proxy information, password information, and SNMP Community Names are not included on the configuration page.

10.3.2 Windows XPe

The Fiery ships with a default Windows XPe 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 includes, but is not limited to the file system, system security policy, and registry entries. In addition, this allows anyone to change the administrator password and deny access to the Fiery for other users.

If the Windows Administrator password is enabled and not entered into the system, the user is prohibited from accessing the Fiery from a FACL kit. The Fiery system software functions normally and users can access Fiery 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). Setup information such as the Fiery Administrator password or Fiery Operator password is stored in the registry as plain text.

10.3.2.1 Microsoft Security Patches

Microsoft regularly issues security patches to address potential security holes in the Windows XP operating system. EFI carefully monitors these patches and makes recommendations to our customers about which patches are applicable to the Fiery. Not all Windows XP patches are applicable to the Windows XPe operating system.

Process for the Microsoft security patches:

1. On the second Tuesday of every month, Microsoft provides the latest security bulletins. EFI commits to have the XPe QFE available within 5 business days (actual average has been 2 to 3 business days).
2. EFI filters which bulletins are applicable to the Fiery server within 1 business day
3. EFI tests the XPe QFE for compatibility with the Fiery server
4. EFI creates a software wrapper to update the Fiery Configuration Page
5. EFI provides the XPe QFE to OEMs for distribution and make them available to Fiery System Updates where they are immediately available for the Fiery to.

10.3.3 Local interface

The user can access the Fiery functions via the FACL kit (if enabled) or the Fiery LCD. The Windows Administrator password is used to control access to the Fiery if the FACL kit is enabled. The Fiery LCD only provides access to the Fiery functionality.

10.4 Connectivity to the Fiery

10.4.1 Physical Ports

The Fiery can be connected through the following external ports:

| Fiery Ports | Function | Access |
|----------------------------|---------------------------------|--|
| Interface Ports | Copier/printer connection (DDI) | |
| 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 |
| Parallel Port | Parallel connection | Bisynchronous whatever communication limited to receiving print jobs via a parallel cable. |
| USB Port | USB device connection | Plug and play connector designed for use with optional removable media devices |

10.4.2 Network Ports

The Fiery allows the user to selectively enable/disable the following IP ports:

| TCP | UPD | Port Name | Dependent Service(s) |
|---------------------|-------|---------------|---|
| 80 | | HTTP | WebTools, IPP |
| | 123 | NTP | Network Time Protocol |
| 135 | | MS RPC | Microsoft RPC Service |
| 137-139 | | NETBIOS | Windows Printing |
| | 161-2 | SNMP | WebTools, Velocity, some legacy utilities, other SNMP-based tools |
| 445 | | SMB/IP | SMB over TCP/IP |
| 515 | | LPD | LPR printing, WebTools, some legacy utilities |
| 631 | | IPP | IPP |
| 8021-8022, 21030 | 9906 | Harmony | CWS4, Velocity, EFI SDK-based tools, Fiery Driver bi-di functions |
| 9100-9103 | | Printing Port | Port 9100 |

Other TCP ports, except those specified by the OEM, are disabled. Any service dependent on a disabled port is automatically disabled.

The Fiery administrator can also enable/disable the different network services provided by the Fiery.

The local administrator can define SNMP read/write community names.

10.4.2.1 IP Filtering

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

10.4.3 Network Encryption

10.4.3.1 IP Sec

IP Sec or IP Security Protocol provides security to IP protocols through encryption and authentication mechanisms. IP sec in the Fiery allows the Fiery to accept incoming data that supports IPsec using a specific authentication method as outlined in the following table.

The incoming data must contain the same 'authentication key' - otherwise, the incoming data will not be accepted by the Fiery.

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

10.4.3.2 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 supports 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 eavesdrop 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 can also 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 Active Directory. By default, LDAP traffic is transmitted unsecured. For LDAP communication over SSL or TLS, the client would have to have a certificate - verified by Verisign.

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

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

10.4.3.3 Certificate Management

Certificates are the way network clients authenticate themselves in network activities that perform identity verifications. The certification method is supported by SSL/TLS

(Secure Socket Layer/Transport Layer Security) that implements authentication through the exchange of certificates based on public/private keys according to the X509 standard.

In the Fiery, certificate management allows the Fiery admin to do the following:

- Add/Load/Browse for available digital certificates (created by a trusted authority) and private keys
- 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)

10.5 Encryption of Critical Information

Encryption of critical information in the Fiery ensures that all passwords and related configuration information are secure when stored in the Fiery. The encryption method used is based on the TwoFish method/algorithm of encryption.

10.5.1.1 *Cryptographic Algorithms and Key Lengths*

For encrypting this sensitive information, EFI client applications use an implementation of the Twofish encryption algorithm. Twofish is a symmetric block cipher developed by Counterpane Labs, and was 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 Printer Controller and EFI client applications do not use proprietary encryption algorithms.

10.5.1.2 *Key Management and Algorithms*

To generate keys used for Twofish encryption, the Fiery Printer Controller 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 deterministically generate a 256-bit key for Twofish (that is, given the 32 bit shared secret key X, the generation algorithm will always produce the same 256 bit key Y).

10.6 Fiery Document Flow

The user can submit and manage jobs in a variety of methods to the Fiery. Some methods have some security associated with them; these are discussed below.

10.6.1 Standard Printing

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

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

The Fiery Administrator can disable the Print and Direct queues to limit automatic printing. With passwords enabled on the Fiery, this 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 will not accept new jobs.

10.6.1.1 *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. 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.

10.6.1.2 *Printed Queue*

Jobs sent to the hold or print queues are stored in the printed queue on the Fiery, if enabled. The administrator can define the number of jobs kept in the printed queue.

10.6.1.3 *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 skips other waiting to process jobs
- The Fiery 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.
- Jobs are not written to the printed queue. However, they appear in the job log.

Note: *only one client can print 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 are 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
- On Windows systems the system memory may use the swap file on the HDD as a memory buffer.

10.6.1.4 *Job Deletion*

When a job is deleted from the Fiery, either automatically or using Fiery tools, the job cannot be viewed or retrieved using Fiery tools. If the job was spooled to the Fiery HDD, elements of the job may remain on the HDD and could theoretically be recovered with certain tools.

10.6.1.5 *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 the 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 (3) times.

The following limitations and restrictions apply to secure erase:

- Does not apply to job files not located in systems other than the Fiery such as
 -
 - Copies of the job that are load balanced to another Fiery

-
- Copies of the job that are archived to media or network drives
 - Copies of the job that are located on client workstations.
 - Pages of a job that are 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, it is not guaranteed that the job will be fully deleted.
 - Jobs submitted through the following methods-
 - Submitted through FTP server.
 - Submitted through a Novell pserver.
 - When printing via SMB, the print job goes through the spooler on the Fiery which saves the job to disk. The Fiery System SW has no control over this, hence the system cannot securely erase the job.
 - Does not delete any job data that may have been written to disk due to disk swapping and disk caching.

Note: Disk swapping occurs when memory needs to be swapped to disk to create more virtual memory than there is physical memory. This is handled in the OS layer and the Fiery has no control of this. However, disk swap space is regularly re-written during OS operation as various segments of memory are moved between memory and disk. This can lead to some segments of the job being stored to disk temporarily.

Note: Disk caching is set to ON for servers thus the job file is overwritten 3x in the cache and may only be overwritten 1x on the drive itself depending on the cache flushing algorithm.

10.6.1.6 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.

10.6.2 Secure Print

The secure print function requires the user to enter a job-specific password at the Fiery to allow the job to print. This feature requires an LCD interface local to the Fiery.

The purpose of this feature 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.

10.6.2.1 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 extracted from the print job.*

10.6.3 Email printing

The Fiery will receive and print jobs sent via email. The administrator can store a list on the Fiery of authorized email address; any email received with an email address not in the authorized email address list will be deleted.

10.6.4 Job Management

Jobs submitted to the Fiery can only be acted upon by using a Fiery job management utility with either administrator or operator access. Guest users (those 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. Setup information such as the Fiery administrator passwords, Fiery Operator passwords, and Novell passwords are sent to the Fiery in plain text.

10.6.5 Job Log

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

A user with operator access can view, export, or print the joblog from the following tools:

- Command WorkStation
- Command WorkStation ME

A user with administrator access can delete the job log from the following tools:

- Command WorkStation
- Command WorkStation ME

A user with guest access can print the job log from the Fiery LCD on certain Fierys. Other Fierys 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.

10.6.6 Setup

Setup requires an administrator password. The Fiery can be setup up or configured from the Fiery LCD, the Fiery Setup program run from a Windows Fiery with a FACI kit, or a remote Setup application run from the WebTools or Command WorkStation.

10.6.7 Scanning

The Fiery 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 from 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 for distribution or storage and retrieval. All scanned documents are written to disk. The administrator can configure the Fiery to delete scan jobs automatically after a predefined length of stay on the Fiery.

Scan jobs can be distributed via the following methods:

- Email – sent to a mail server where it is routed to the desired email destination.
Note: if the file size is greater than the administrator-defined maximum, the job is stored on the Fiery HDD, accessible through a URL.

-
- FTP – sent to an FTP destination. A record of the transfer, including the destination, is kept in the FTP log (accessible from the LCD Print Pages command). An FTP Proxy Server can be defined to send the job through a firewall.
 - Fiery Hold Queue – sent to the Fiery Hold Queue (see Printing, above) and is not kept as a scan job
 - Internet Fax – sent to a mail server where it is routed to the desired internet fax destination.
 - Mailbox – stored on the Fiery with a mailbox code number. The user needs to enter the correct mailbox number to access the stored scan job. Some Fiery versions also require a password. The scan job is stored in a manner to allow retrieval through a URL.

10.7 System Update

System Updates will keep the Fiery up-to-date by periodically contacting the update server on the internet. If a critical OS update is available, System Updates will download the update to the Fiery automatically and notify the user via LCD/ copier panel and/or FACL. System Updates allows scheduled automatic installation at preset time of the day and restarts the Fiery automatically as needed. This will keep the Fiery up-to-date without user-intervention.

Alternatively, the administrator can disable auto download and/or installation and initiate them manually. System Updates will only download and install critical Windows XPe updates issued by Microsoft as well as Fiery patches.

Note: The communication is via HTTPS on port 443 only.

You can ping the server from any system on the internet to obtain the IP address, however PING will not complete the respond due to security and network performance implementations.

All updates and patches will be displayed/listed in the config page.

10.8 Anti-virus software

Administrators can install anti-virus software on FACL-enabled Windows XPe-based Fierys to protect against the accidental introduction of viruses on the Fiery.

Anti-virus software should only be run when the Fiery is idle and not receiving jobs. This helps prevent unforeseeable errors that may result if antivirus software acts while the Fiery attempts to process a job.

The anti-virus software should scan for files coming into the Fiery outside of the normal printstream. This includes:

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

The anti-virus software can also be configured to scan all files on the Fiery when the Fiery is not planned for use for an extended period of time.

EFI tests System 5.5 and up Fiery products with McAfee VirusScan software; similar products from Symantec and TrendMicro are also compatible with the Fiery when used as described above.

10.8.1 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. The Fiery 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 and treated as such.

10.9 Removable HD Kit Option

The Fiery supports a removable hard drive option kit for increased security. This kit provide the user with the ability to both 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.

10.9.1 For Servers

Two Kits will be available, one for Q-4500 series and one for the Q-5000 series products. These kits provide the user with the ability to both 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.

11 Product Specific options

11.1 Fiery Network Controller Hardware Matrix

| Fiery Controller | Standalone / Embedded | Operating System | Code Base | DVD-ROM | Removable Media Drive (optional) | GUI Kit |
|------------------|-----------------------|------------------------|-----------------------|--------------|----------------------------------|--------------|
| Q5500 | Standalone | Windows XPe | System 7 | ✓ | ✓ | ✓ |
| S600 | Standalone | Windows XPe | System 7 | ✓ | ✓ | ✓ |
| S400 | Standalone | Windows XPe | System 7 | ✓ | ✓ | ✓ |
| X7 | Both | Both Windows XPe/Linux | System 7/7e | ✓ (XPe only) | ✓ (XPe only) | ✓ (XPe only) |
| X6 | Both | Both Windows XPe/Linux | System 6/6e | ✓ (XPe only) | ✓ (XPe only) | ✓ (XPe only) |
| Q5000 | Standalone | Windows XPe | System 6 | ✓ | ✓ | ✓ |
| S550 | Standalone | Windows XPe | System 6 | ✓ | ✓ | ✓ |
| S350 | Standalone | Windows XPe | System 6 | ✓ | ✓ | ✓ |
| Q4500 | Standalone | Windows XPe | System 5.5 | ✓ | ✓ | ✓ |
| S500 | Standalone | Windows XPe | System 5.5 | ✓ | ✓ | ✓ |
| S300 | Standalone | Windows XPe | System 5.5 | ✓ | ✓ | ✓ |
| X5 | Standalone | Windows XPe | System 5.5 | CD-ROM | ✓ | ✓ |
| X5 | Standalone | Linux | System 5.1e | CD-ROM | | |
| X3e | Embedded | Linux | System 5.1e, 5.5e, 6e | | | |
| Z5 | Standalone | Windows NT | System 5 | CD-ROM | ✓ | ✓ |
| X5 | Standalone | Windows NT | System 5 | CD-ROM | ✓ | ✓ |