3.2 Network Encryption

3.2.1 IP Sec

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

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

3.2.2 LDAP Over SSL and TLS

SSL is a protocol for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. Most of today's browsers support SSL. The Fiery 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.

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.

3.2.3 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)

3.3 System Update (Windows XPe Only)

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 FACI. 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.

You can ping the server from any system on the internet to obtain the IP address.

All updates and patches will be displayed on the configuration page.

3.3.1 GRAD Server Physical Security

Physical access to the EFI hosting facility is controlled by two independent, proximity card reader systems. Fewer than 20 EFI employees may currently enter the data center unescorted. The list is subject to periodic unannounced screening to validate that the proper personnel have access to the datacenter. All visitors must pass through three controlled doors. EFI personnel and security cameras monitor the premises. Entry by non-employees is recorded in a logbook. The premises are also protected by two independent alarm systems. The external system will notify law enforcement of a breach in security.

3.3.2 GRAD Server Network Security

EFI deploys redundant pairs of firewalls to protect the servers from internal and external threats. All traffic incoming from and outgoing to the Internet is intercepted, processed and profiled on-site, and diagnostic, summary information about specific incidents is related to a security managed services firm for further analysis and attention. EFI also makes use of access control lists on routers and switches to reduce the opportunities for disruption due to worms and viruses as well as automated and human-directed attacks.

3.3.3 Internet Access High Availability

Dual Internet connections through separate ISPs, discrete paths, load balancing and SSL acceleration hardware are installed redundantly. This allows a security-compromised connection to be removed from service. Two Internet connections with different physical media and diverse transit paths connect operations to the Internet. Currently, one connection is a full DS3 (45Mbps) uplink and the other is a 60Mbps link on Ethernet. We use BGP and HSRP on duplicate routers, switches, and firewalls to ensure connectivity is not lost.

3.3.4 Site and Fault Monitoring

Over 3600 separate aspects of the application and other hosted applications are monitored by three independent stations running SiteScope and one station running Nagios. This provides an early warning should performance problems, outages or errors result from an attack. Additionally, the application itself reports errors via e-mail or pager. The types of events range from "ping and pipe" on ISP connections and servers to a user experience test on each server. SiteScope regularly logs into the web site (on each server), navigates through screens, and logs out so as to ensure timely and accurate performance.

Internal documents guide the human response to each alert, and an escalation process is in place to ensure that alerts are resolved in an efficient manner.

3.3.5 Proactive Maintenance

EFI performs monitoring, backups, patching, virus protection, account maintenance, tuning, troubleshooting, security and the like in a manner to proactively preserve the stability of the environment.

3.3.6 Anti-Virus Controls

Border firewalls, router access control lists, active virus filtering at the corporate border, anti-virus software deployed on all production, management, and pre-production systems, automatic pattern file updates, centralized virus reporting (including 24/7 alerting via e-mail and pager). Combined, these measures allow real-time situation handling on all common channels of propagation.

3.3.7 Client (Fiery) Information

3.3.7.1 Ports:

The Fiery uses port 80 to query GRAD for update information and port 443 to download updates from GRAD.

3.3.7.2 Protocols:

The Fiery uses HTTP 1.1 to query GRAD for update information and HTTPS to download updates from GRAD.

3.3.7.3 Automatic Connection Schedule:

Currently only automatic updates are available. The Fiery connects to GRAD only during the scheduled time and after the reboot when an update (using system updates or not) is installed.

3.3.7.4 System Update Utility:

System updates are downloaded by a dedicated utility and not via Internet Explorer. This allows password and proxy settings to be configured separately from the rest of the system and does not allow end users to access the GRAD connection directly.

3.3.7.5 Virus Scans:

There is no separate virus scanning done by system updates. The Fiery virus scan policy is covered in sections 5.2.1 and 5.3.5.

4 Access Control

4.1 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.

4.2 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.

5 Operating System Environment

5.1 Start up procedures

The operating system and Fiery system software are loaded from the local HDD during startup.

The BIOS resident on the Fiery motherboard is read-only and stores the information needed to boot up the operating system. Changes to the BIOS (or removal of the BIOS) prevent the Fiery 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.

5.2 Linux

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

5.2.1 Linux anti-virus software

The operating system is a dedicated operating system, 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.

5.3 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.

5.3.1 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 fully 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.

An XPe OS is essentially a de-componentized version of XP Pro operating system. As such, XPe patches that have been fully tested by EFI are really also XP Pro patches.

However, not all XP Pro patches are applicable to an XPe system since XPe is a subset of XP Pro (de-componentized). In a few instances – based on EFI internal testing, some XP Pro patches can cause XPe to crash (due to a component that is not installed on XPe). EFI has alerted Microsoft to this issue and asked that they take this into account when developing future patches and operating systems.

5.3.2 Windows XPe SP1 Discontinuance and SP2

Effective October 10, 2006 – Microsoft has officially discontinued support for Windows XP SP1 and XPe SP1. However, EFI will continue to test and release patches for XPe-based Fierys for both SP1 and SP2 systems.

All XPe-SP1 based Fierys that have all the latest security patches installed (through Fiery System Update) are equivalent to an SP2 system.

For any customer concerns regarding XPe-SP1 systems and latest SP2 patches, please contact your authorized OEM / channel technical support.

5.3.3 Security Scan Tools

Many corporate environments use network scan tools from Microsoft and other 3rd parties to search for security vulnerabilities among their deployed clients in their network. Most – if not all of these network scan tools do not support Microsoft XPe-based systems. These scan tools do not detect the latest installed patches in an XPe-based system – as such, XPe-based systems such as Fierys may be flagged for specific vulnerabilities – even if the Fiery has all the latest Microsoft security patches.

For customer concerns regarding these network security scan tools – and accurately determining if an XPe-Fiery has the latest Microsoft security patches, please contact your authorized OEM / channel technical support.

5.3.4 SMS Tools

EFI has its own dedicated system update tool for its Windows based systems. This tool handles the retrieval of all applicable MS security patches and Fiery SW updates. As such, the Fiery does not support any third party SMS tools for retrieving/pushing updates to the Fiery.

5.3.5 Windows anti-virus software

Administrators can install anti-virus software on Fierys with FACI kits. A local GUI is required for proper configuration of anti-virus software. Anti-virus software is most useful in a local GUI configuration, where users have the potential to infect the Fiery with a virus through standard Windows actions.

For Fierys without a FACI kit, it is still possible to launch anti-virus software on a remote PC and scan a shared hard drive of a Fiery, EFI supports this configuration/ workflow. However, EFI suggests the Fiery administrator work directly with the anti-virus software manufacturer for support of this operation.

EFI supports the use of antivirus solutions as used in accordance with this specification. EFI does not support or give any warranty regarding the efficacy of any anti-virus software.

5.3.5.1 Anti-Virus Software Configuration

The anti-virus software should be configured to scan for files coming into the Fiery outside of the normal print stream. 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. The administrator should only run the anti-virus software manually when the Fiery is idle and not receiving or acting upon a job

5.3.5.2 Non-FACI Systems

For non-FACI based Fiery Systems , because the system is running on Microsoft OS, EFI recognizes that the Fiery must still meet the customers company anti-virus standards. EFI has developed a patch which enables remote desktop. With this patch installed and remote desktop enabled, the administrator will be able to manage the NON-FACI system using remote desktop – and install the appropriate anti-virus software required by the company.

5.4 Email viruses

Typically, viruses transmitted via 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 Data Security

6.1 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.

6.1.1 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.

6.1.2 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).

6.2 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.

6.2.1 Hold and Print Queues

When a job is printed to the print or the hold queue, the job is spooled to the hard drive on the Fiery. Jobs sent to the hold queue are held on the Fiery hard drive, until the user submits the job for printing or deletes the job using a job management utility, such as the Command WorkStation, Command WorkStation ME or Clear Server.

6.2.2 Printed Queue

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

6.2.3 Direct Queue (Direct Connection)

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

- Process as soon as the current job finishes processing and 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
- The system memory may overflow to use the swap partition on the HDD as a memory buffer.

6.2.4 Job Deletion

When a job is deleted from the Fiery, 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.

6.2.5 Secure Erase

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

Secure Erase is designed to remove the content of 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 using an algorithm based on US DoD specification DoD5220.22M.

The following limitations and restrictions apply to secure erase:

- Does not apply to job files not located in systems other than the Fiery 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.

6.2.6 System Memory

Processing of some files may write some job data to the operating system memory. In some cases this memory may be cached on the HDD and is not specifically overwritten.

6.3 Secure Print

The secure print function requires the user to enter a job-specific password at the Fiery 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.

6.3.1 Workflow

The user enters a password in the Secure Print field in the Fiery Driver. When this job is sent to the Fiery's Print or Hold queue, the job is queued and held for the password.

Note: *Jobs sent with a secure print password are not viewable from Command WorkStation or Command WorkStation ME.*

From the Fiery LCD, the user enters an Secure Print window and enters a password. The user can then access the jobs sent with that password and print and/or delete the jobs.

The printed secure print job is not moved to the Printed queue. The job is deleted automatically, once it has finished printing.

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

6.4 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 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.

6.6 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 Command WorkStation. A user with administrator access can delete the job log from Command WorkStation. A user with guest access can print the job log from the Fiery LCD on certain 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.

6.7 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.

6.8 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.

Fiery Security White Paper

Version 1.81

Date of Issue: 7/28/2006

Table of Contents

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)

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 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 RIPed 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 FACI 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 FACI-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 RIPed 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 FACI 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 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.

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 RIPed 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 RIPed 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 RIPed 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 RIPed 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 RIPed 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 FACI. 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 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.

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 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.

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 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.

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 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.

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 FACI. 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 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 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

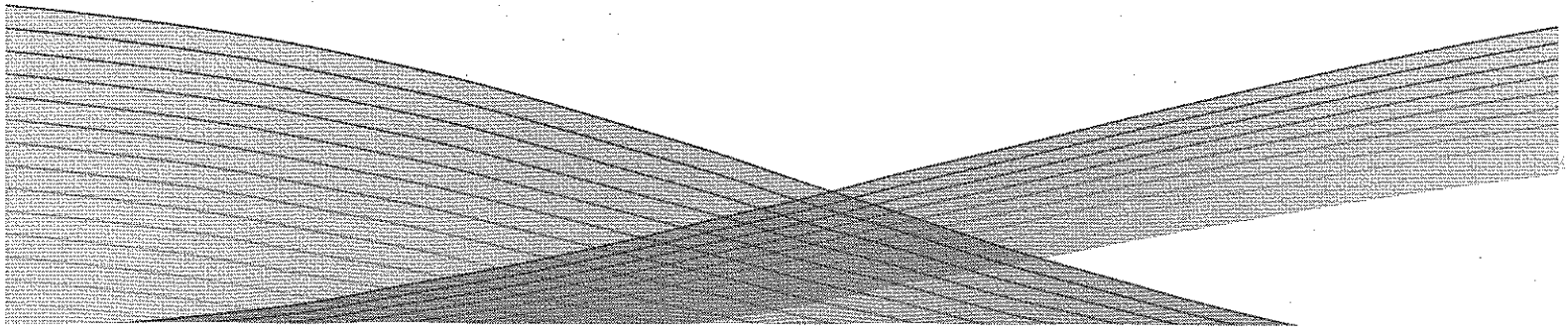
Fiery Controller	Standalone / Embedded	Operating System	Code Base	DVD-ROM	Removable Media Drive (optional)	GUI Kit
Q5500	Standalone	Windows XPe	System 7	✓	✓	✓
S600	Standalone	Windows XPe	System 7	✓	✓	✓
S400	Standalone	Windows XPe	System 7	✓	✓	✓
X7	Both	Both Windows XPe/Linux	System 7/7e	✓ (XPe only)	✓ (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	✓	✓

Xerox FreeFlow® Print Server version 7 Security White Paper Secure Solutions For You and Your Customers

Contents

September 2008

Author: Xerox Corporation



Xerox FreeFlow Print Server Security White Paper
Secure solutions for you and your customers

Executive summary

Now more than ever, companies as well as government agencies need to keep their data safe. Drawing on our leadership in the printing industry, Xerox leads the way in providing secure document solutions. The Xerox FreeFlow Print Server provides features that offer the highest levels of security, adhere to government regulations, and enhance peace of mind. This document highlights these security capabilities and features:

Adjust to your security needs with the Security Management Feature

Reuse network accounts using Microsoft® Active Directory Services

Manage your users and groups with the Authentication Feature

Know your Web users through the Basic Access Authentication Feature

Accept jobs from the clients you want with the IP Filtering Feature and Port Designation

Protect resources so that they're tamper-free with the System Integrity Feature

Secure http delivery through the Transport Layer Security Feature

Establish certain users and certain privileges with the Access Control Feature

Remove files permanently and completely with Residual Information Protection

Why security matters

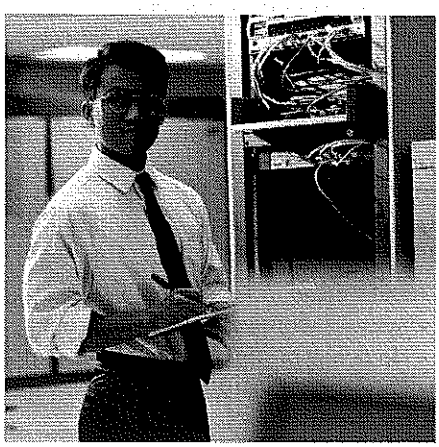
Innovations in information technology have increased rapidly over the last several years, fueling the pace and productivity of business across all sectors and industries. Great strides have been made in the way information is created, stored, managed, distributed, and archived. However, this innovation has also created opportunities for those seeking to intercept or corrupt valuable information and disrupt the flow of business—privacy, property, and assets of all kinds are at stake. That makes security an issue that no one can ignore.

Government regulations

In industries such as healthcare and financial services, new government mandates dictate that information in every form be more secure.

The Health Insurance Portability and Accountability Act (HIPAA) in healthcare, Gramm-Leach-Bliley (GLBA) in the financial sector, and the Federal Information Security Management Act of 2002 (FISMA) are just a few examples of many new security regulations being issued to oversee the way that information is printed, shared, stored, and protected.

With so many regulatory and compliance measures to respond to, Xerox has looked to federal government requirements worldwide, among others, as guidelines. By developing solutions that comply with the most stringent security standards, we can offer highly secure solutions to all of our customers in all business sectors.



Peace of mind

In every environment, security is of critical importance.

Transactional print jobs often consist of sensitive customer data that absolutely must be protected from unauthorized viewing. And publishing jobs include product manuals, annual reports, and brochures that contain information that is often confidential until a launch date or an event.

No matter what you print, you will have greater peace of mind knowing that the printing solution assures that the data and your network will be secure.

Xerox's commitment to security

At Xerox, security issues are front and center. As a leader in the development of digital technology, we have demonstrated a commitment to keeping digital information safe and secure by identifying potential vulnerabilities and proactively addressing them to limit risk. Our customers have responded by looking to us as a trusted provider of secure solutions with many standard and optional security features.

Xerox security goals

We have identified five key security goals in the quest to provide secure solutions for every one of our customers:

Integrity
- No unauthorized alteration of data
- System performs as intended, free from unauthorized manipulation

Confidentiality
- No unauthorized disclosure of data during processing, transmission, or storage

Availability
- Systems work properly
- No denial of service for authorized users
- Protection against unauthorized use of the system

Accountability
- Actions of an entity can be traced directly to that entity

Assurance
- Confidence that integrity, confidentiality, availability, and accountability goals have been met

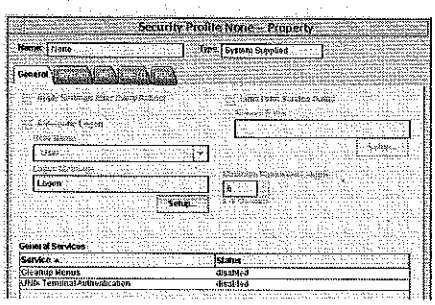
FreeFlow Print Server security features

In response to a variety of security threats, we have taken an industry-leading role by developing and implementing information security technology for nearly a decade. This commitment to security carries over to our digital on-demand production printing solutions that are powered by the FreeFlow Print Server.

Adjust to your security needs

Security Management Feature

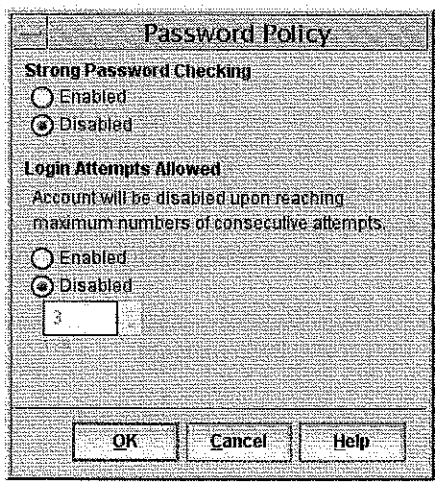
Your security needs are yours alone. The FreeFlow Print Server allows you to adjust a range of security features to tailor security exactly to the needs of your enterprise.



The Security Management feature enables authorized users to set up and control the secure operation of the printing system so that they all operate coherently and adjust to your various security needs and policies.

The security administrative functions cover the following areas:

- Configuration of automatic login for customers not interested in security—that is, a "no-security" look and feel.
- Job Management policy configuration issues, such as which users are allowed to manage jobs.
- Diagnostics policy configuration issues, such as which users are allowed to run diagnostic routines.
- Enablement of TLS/SSL security protocol and Digital Certificates management.
- Configuring the system to trust remote security databases such as W2K domains.
- Configuring the system for various security levels.
- Displaying a custom logon message.
- Preventing walk-up users from arbitrarily reprinting jobs stored on the system.
- The means for enforcing a strong password policy.
- Forcing users to re-authenticate whenever UNIX terminal access is requested.
- User accounts can be locked after a user-defined number of failed login attempts (ranging from 1 to 9).



Reuse network accounts

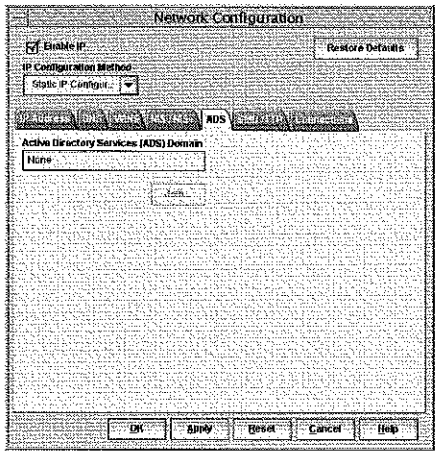
Microsoft Active Directory Services (ADS)

Our printing solutions recognize and integrate with your existing user security accounts that are defined in a remote, trusted security database and maintained by a Microsoft Windows® 2000 Domain Controller.

You can reuse these network accounts for login at the printer, instead of exclusively using the locally defined user accounts. This saves time and effort for system administrators.

With the Microsoft Active Directory Services feature, your printer can interoperate with Microsoft Active Directory Services:

- The printer can be configured to trust a Windows 2000 ADS security authority.
- Users are able to walk to the printer and authenticate using their ADS username and password. The printer will contact the trusted ADS security authority, which, in turn, will verify the user's credentials.
- ADS users and groups can be mapped to the local printer groups and, thereby, be granted a certain authorization level.



Manage your users and groups

Authentication Feature

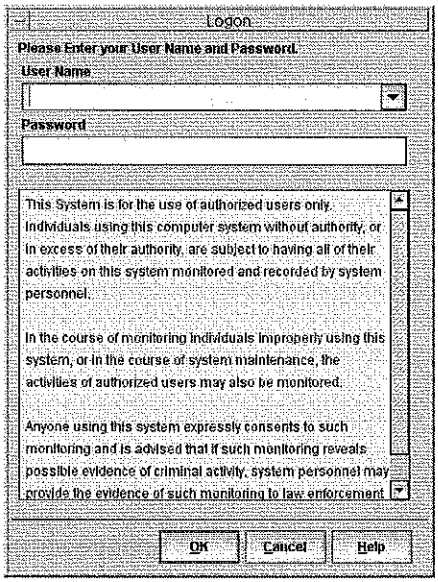
Perhaps the surest way to maintain security with any printing device is allowing only authorized users to access the system. The FreeFlow Print Server does so with its Authentication feature.

Any type of interaction between a user and a printing system through the FreeFlow Print Server is associated with a security account. This association, or logon session, is the basis for granting access to any of your users. Once the logon session is established, the user can interact with the printer, subject to restrictions based on the user's identity.

User accounts are defined either locally at the device or remotely at a trusted network location. Each user account is a member of one and only one user group. Group membership defines/authorizes the access rights of requests made by users.

A strong password feature further enhances print server security, requiring users to enter a password that contains at least one special character, one uppercase letter, and one digit. Additional parameters that keep these passwords safe include:

- Password Duration—checks on how much time has passed since passwords have changed or been updated.
- Password History—prevents users from reusing old passwords.



Know your Web users

Basic Access Authentication (BAA) Feature

Basic Authentication is an industry-standard method of authenticating a remote user of Internet Services (HTTP) or the Internet Printing Protocol (IPP).

It optionally forces users to authenticate themselves before they can access the device over HTTP. When used in conjunction with TLS/SSL, it allows for both authentication (BAA) and integrity/privacy (TLS/SSL) protection.

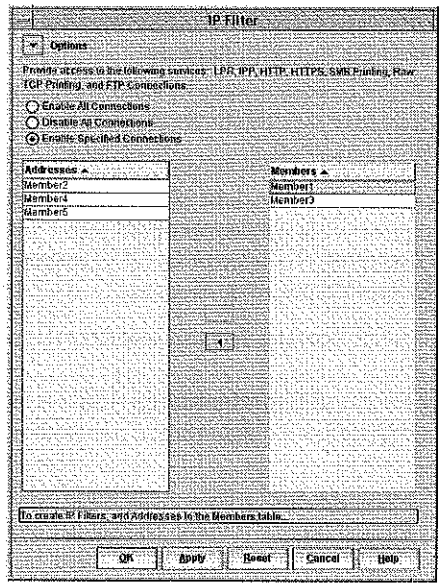
Accept jobs from only the clients you want

IP Filtering Feature

With the FreeFlow Print Server's Internet Protocol (IP) Filtering feature, you can enjoy the productivity benefits of remote job submission, while minimizing security risks.

IP Filtering provides a system administrator with a means of restricting access to the system to a specific set of IP addresses. This provides a first level of defense against unauthorized use of the system. Computers whose IP addresses are outside of the allowed set are not permitted to print.

With IP Filtering, the administrator can also configure the printer to accept print jobs only from specific print servers. This prevents end users from directly accessing the printer and enables value-added solutions implemented at the print server.



Port Designation

Xerox can provide to you, as required, a complete list of the ports utilized by the FreeFlow Print Server network functionality.

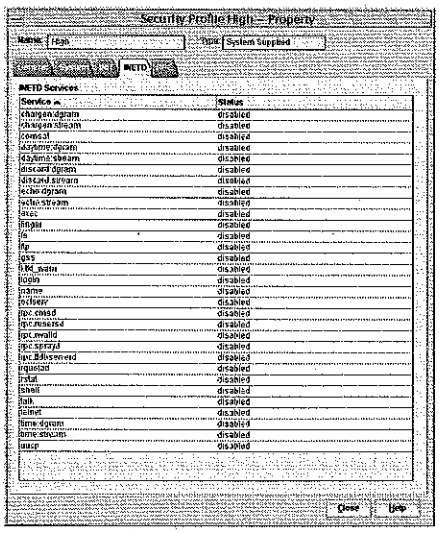
Tamper-free resources

System Integrity Feature

Even with the most stringent security restrictions in place, there are sometimes "backdoors" and vulnerabilities that can be exploited.

The System Integrity feature on the FreeFlow Print Server:

- Ensures that system resources cannot be tampered with.
- Limits access to UNIX commands through the Access Control feature in user group classification.
- Disables unneeded network applications and OS utilities.
- Provides OS security patches—working very closely with Sun, Xerox is able to provide patches in a timely fashion as they are released from Sun.
- "Hardens" the system according to security best practices—tightens the sensitive file access permissions, shuts down unneeded and/or insecure network protocol services, and restricts potentially insecure network access to trusted network hosts based on the originating IP address.



Encrypted job submission via the Web

TLS/SSL Security Feature

One of the great leaps forward in printing productivity is the ability to print from anywhere over the Internet. Unfortunately, it can be a great leap backwards in security.

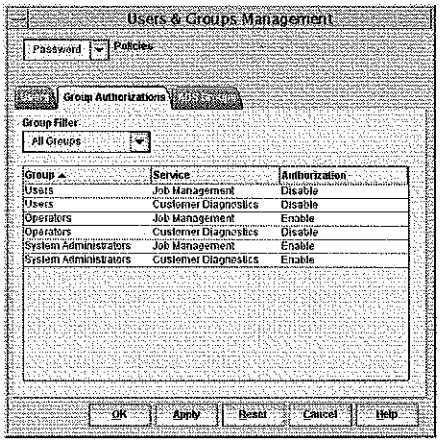
The FreeFlow Print Server's Transport Layer Security feature allows a high level of protection of the data exchanged—such as higher-level security information like user passwords or confidential print jobs—over a network. Transport Layer Security v1.0 (RFC2246) is a network security protocol widely used for applications that require secure HTTP communications.

TLS/SSL provides security protection through:

- **Message Confidentiality**—Data is encrypted through symmetric cryptography, which uses an algorithm to generate unique exchange keys for each connection.

- **Message Integrity**—A message authentication code is used to detect message tampering and forgery. The sender digitally signs the message using a session key shared with the recipient.

- **Authentication**—The identity of a peer can be authenticated using asymmetric (public key) cryptography. Servers are identified through a digital certificate issued by a certificate authority or self-signed.



Certain users, certain privileges

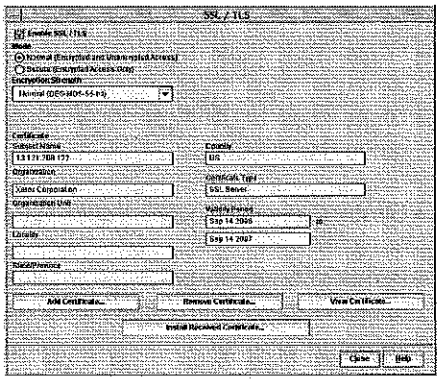
Access Control Feature

With the Access Control feature, authenticated users are assigned privileges—either as Administrators, Operators, or Users with decreasing levels of access. The higher the access level, the more features and data available. The range of available features for each access level is not configurable, with the following exceptions:

- **Job Management**—An Administrator decides the access level necessary to manage jobs. By default, any User can manage jobs, but an Administrator might decide that only Operators and/or Administrators can manage jobs. This prevents "walk-up users" from deleting print jobs submitted by other Users.

- **Diagnostics**—Diagnostic tools are restricted to Administrators by default. However, there are cases when trained Users may be entrusted with certain Diagnostic operations without necessarily granting them Administrator privileges. For these cases, it is possible to allow Operators or even regular Users access to the Diagnostic tools.

The Authorization feature, as described earlier, controls access to the Diagnostic tools as a whole. However, the Diagnostic tools are further grouped in various levels that allow for more or less functionality. The access to these levels is controlled based on a secondary authentication step, thereby providing a finer level of authorization. Once a User is authenticated in the first step and allowed access to Diagnostics as a whole, the User gains access to a certain group of tools based on a secondary password they must provide.



Permanent and complete file removal

Residual Information Protection

With the pace of business today, jobs come and jobs go quickly in your print enterprise. But proper security should prompt you to ask the question, "Do jobs ever really go?"

With the Residual Information Protection feature, the answer is yes, jobs really do go away, permanently and completely.

This feature ensures that deleted information is no longer accessible. This type of deleted information is outside of the scope of the standard security functions but it is potentially retrievable.

- **Hard drive removal**—If the hard drive isn't present, it is impossible to retrieve information from it. Many Xerox printing systems feature a hard drive that can be removed when the system is not in use. Please speak with your salesperson to see what products can be supported with a removable hard drive through Xerox Special Information Systems (XSIS).

- **Hard drive erasure**—Algorithms completely and permanently delete all files after printing.

- **Disk Overwrite Software**—Removes all data from the spool, swap, and outQ partitions of the FreeFlow Print Server hard disk so that data cannot be retrieved. Data is overwritten using a four-pass algorithm that conforms to U.S. Department of Defense Directive 5200.28-M.

For more information and additional security resources, go to:
http://www.xerox.com/security

610P727670B

The State of Nevada Purchasing Division
On behalf of the Western States Contracting Alliance (WSCA)
Request for Proposal No. 1715 for Multifunction Copiers and Related Software
Opening Date: February 4, 2009
Revised April 13, 2009

Attachment B Revised

XEROX

Please note that the following clarifications are a part of our bid proposal. These clarifications are not intended to alter the State's RFP but rather to explain our offer.

In addition, Xerox' "Terms and Conditions Attachment" which includes Xerox' lease, purchase, and maintenance terms and conditions is enclosed as required by Section 11.9 of the RFP.

In the event the State determines the terms within Xerox' "Terms and Conditions Attachment" conflict with the terms of the RFP, Contract or Participating Addendum the order of precedence within the RFP and Contract shall prevail.

5. Project Terms and Conditions

5.1.6 Equipment Inspection / Testing / Acceptance: Xerox proposes that equipment be considered accepted, upon installation of the equipment by Xerox, after the equipment successfully runs all required diagnostic routines, and the equipment is turned over to the State for use.

Notwithstanding acceptance, Xerox will be keep the equipment in good working order in accordance with the specifications contained in the State's solicitation or Xerox will replace the equipment with a like model at Xerox' expense.

5.4.6.10 Equipment Moves / Relocations: Prices quoted do not include the cost of any end-user requested equipment relocations. A quote will be provided to the State prior to relocation of the equipment.

5.4.8.2 Software Patches and Updates: The software maintenance agreement includes the cost of patches or fixes for the software as stated in the Solicitation. Additional features and functionality are not included in any patches or fixes and would be subject to an additional charge for the added capabilities should the end-user choose to purchase them.

8. Payment: Payment will be made in accordance with the State's Prompt Pay Act or other similar legislation.

Attachment H / Additional Clarifications (moved from Attachment B)

5. Project Terms and Conditions:

5.1.11 Termination for Non-appropriations: Xerox requests:

a) Written notice stating that your legislative body, though no action on your part, failed to appropriate funds for continuation of the obligation.

b) Certification, to the extent permitted by law, that the canceled Equipment is not being replaced by similar equipment or equipment performing similar functions.

c) You agree to make the Equipment available for pick up by Xerox. When the Equipment is picked up, the Equipment will be in good condition and free of all liens and encumbrances. You will then be released from your obligations to make any further payments to Xerox (with Xerox retaining all sums paid to date).

5.2.5 Warranty: Xerox provides warranty by way of a monthly billed maintenance agreement, which is a mandatory part of any monthly lease or rental payment. Maintenance agreements commence upon installation of the equipment. Xerox will repair or replace defective parts or equipment at Xerox' expense as long as the equipment is being maintained by Xerox under a maintenance agreement. If the maintenance agreement is cancelled or it is not renewed Xerox' obligation to repair or replace equipment ceases.

Attachment C
Master Services Agreement

17. Delivery; Acceptance of Equipment: Xerox proposes that equipment be considered accepted, upon installation of the equipment by Xerox, after the equipment successfully runs all required diagnostic routines, and the equipment is turned over to the State for use.

Notwithstanding acceptance, Xerox will be keep the equipment in good working order in accordance with the specifications contained in the State's solicitation or Xerox will replace the equipment with a like model at Xerox' expense.

30. Assignment / Delegation; Leases: Please note that Xerox automatically assigns all leases to a wholly owned subsidiary of Xerox. Such assignment shall be transparent to the State.

31. Ownership of Proprietary Information: Xerox does not anticipate the development of any customized products or programming in connection with the services provided under this Contract. Any products or programming developed while providing services under this Contract shall remain the property of Xerox, unless the State specifically contracts with and compensates Xerox to develop products or programs for the exclusive use of the State.

Xerox does agree, however, to grant the State a non-exclusive, non-transferable, perpetual right to use any programs created by Xerox under this contract strictly for the State internal business use and not for resale and/or distribution to third parties. All content and data specific to the State shall remain the property of the State.

32. Patents, Copyrights, Etc.: Xerox agrees to indemnify the State with the understanding that Xerox is promptly notified in writing and has sole control of the defense and settlement of such claims, suits, and actions, but Xerox' indemnity shall not apply to any infringement arising solely from the use or sale of equipment in combination

with any device or Equipment not provided hereunder by Xerox, or to any infringement caused by modification of the Equipment by other than Xerox.

Attachment E
RFP Terms and Conditions for Goods

3. Infringement; Indemnity: Xerox agrees to indemnify the State with the understanding that Xerox is promptly notified in writing and has sole control of the defense and settlement of such claims, suits, and actions, but Xerox' indemnity shall not apply to any infringement arising solely from the use or sale of equipment in combination with any device or Equipment not provided hereunder by Xerox, or to any infringement caused by modification of the Equipment by other than Xerox.

3. Infringement; Indemnity / Repurchase of Equipment if State is Enjoined from Using the Equipment: Xerox will repurchase and such equipment less a reasonable charge for the usage of the equipment. *Actual amount of credit, if applicable, will be determined at the time each Member-State establishes its Participating Addendum with Xerox.*

8. Delivery, Inspection, Acceptance, Risk of Loss / Acceptance: Xerox proposes that equipment be considered accepted, upon installation of the equipment by Xerox, after the equipment successfully runs all required diagnostic routines, and the equipment is turned over to the State for use.

Notwithstanding acceptance, Xerox will be keep the equipment in good working order in accordance with the specifications contained in the State's solicitation or Xerox will replace the equipment with a like model at Xerox' expense.

Xerox Corporation Terms and Conditions Attachment

The State of Nevada Purchasing Division
On behalf of the Western States Contracting Alliance (WSCA)
Request for Proposal No. 1715 for Multifunction Copiers and Related Software
Opening Date: February 4, 2009

GENERAL TERMS: The following terms apply to all transactions:

1) BASIC SERVICES. As a mandatory part of a lease, Xerox (or a designated servicer) will provide the following Basic Services under this Agreement (unless you are acquiring Equipment for which Xerox does not offer Basic Services; such Equipment to be designated as "No Svc."):
   A) REPAIRS & PARTS. Xerox will make repairs and adjustments necessary to keep Equipment in good working order (including such repairs or adjustments required during initial installation). Parts required for repair may be new, reprocessed, or recovered.
   B) HOURS & EXCLUSIONS. Unless otherwise stated, Basic Services will be provided during Xerox's standard working hours (excluding Xerox-recognized holidays) in areas within the United States, its territories, and possessions open for repair service for the Equipment at issue. You agree to give Xerox reasonable access to the Equipment. Basic Services shall cover repairs and adjustments required as a result of normal wear and tear or defects in materials or workmanship (and shall exclude repairs or adjustments Xerox determines to relate to or be affected by the use of options, accessories, or other connected products not serviced by Xerox, as well as any non-Xerox alterations, relocation, service, supplies, or consumables). You agree to use Equipment in accordance with, and to perform all operator maintenance procedures for Equipment as set forth in, the applicable manuals provided by Xerox.
   C) INSTALLATION SITE & METER READINGS. The Equipment installation site must conform to Xerox's published requirements throughout the term of this Agreement. If applicable, you agree to provide meter readings in the manner prescribed by Xerox. If you do not provide Xerox with meter readings as required, Xerox may estimate them and bill you accordingly.
   D) CARTRIDGE PRODUCTS. If Xerox is providing Basic Services for Equipment utilizing cartridges designated by Xerox as customer replaceable units, including copy/print cartridges and xerographic modules or fuser modules ("Cartridges"), you agree to use only unmodified Cartridges purchased directly from Xerox or its authorized resellers in the United States and the failure to use such Cartridges shall void any warranty applicable to such Equipment.
2) CARTRIDGES. Cartridges packed with Equipment and replacement Cartridges may be new, remanufactured or reprocessed. Remanufactured and reprocessed Cartridges meet Xerox's new Cartridge performance standards and contain new and/or reprocessed components. To enhance print quality, the Cartridge(s) for many models of Equipment have been designed to cease functioning at a predetermined point. In addition, many Equipment models are designed to function only with Cartridges that are newly manufactured original Xerox Cartridges or with Cartridges intended for use in the U.S. Equipment configuration that permits use of non-newly manufactured original Xerox Cartridges may be available from Xerox at an additional charge. Cartridges sold as Environmental Partnership ("EP") Cartridges remain the property of Xerox. You agree that you shall return all EP Cartridges and may return other Cartridges to Xerox, at Xerox's expense when using Xerox-supplied shipping labels, for remanufacturing once such Cartridges cease functioning..
3) COVENANTS. Each party agrees that it will promptly notify the other party in writing, if it relocates its principal place of business.
4) SUPPLIES INCLUDED IN BASE/PRINT CHARGES. Xerox (or a designated servicer) will provide you with black toner (excluding highlight color toner), black developer, copy Cartridges, and, if applicable, fuser ("Consumable Supplies") throughout the term of this Agreement. For full-color Equipment, Consumable Supplies shall also include, as

applicable, color toner and developer. You agree that the Consumable Supplies are Xerox's property until used by you, that you will use them only with the Equipment, that you will return all Cartridges to Xerox for remanufacturing once they have been run to their cease-function point (at Xerox's expense when using Xerox-supplied shipping labels), and that at the end of the term of this Agreement either (a) you will return any unused Consumable Supplies to Xerox (at Xerox's expense when using Xerox-supplied shipping labels)or (b) destroy them in a manner permitted by applicable law. Should your use of Consumable Supplies exceed Xerox's published yields for these items by more than 10%, you agree that Xerox shall have the right to charge you for any such excess usage. When requested by Xerox, you agree to provide meter readings and inventory of Consumable Supplies in your possession.

5) EXTENDED SERVICE HOURS. If this option has been selected, Xerox will provide Basic Services during the hours indicated, with the first number establishing the number of eight-hour shifts covered and the second establishing the days of the week (e.g., 2 x 6 would provide service from 8:00 A.M. to 11:59 P.M., Monday through Saturday). The cost of this enhanced service coverage will be billed separately and, as such, is not included in your Minimum Lease Payment or Print Charges.

6) NOTICES. Notices must be in writing and will be deemed given five (5) days after mailing, or two (2) days after sending by nationally recognized overnight courier, to the other party's business address, or to such other address designated by either party to the other by written notice given pursuant to this sentence. The term "business address" shall mean, for you, the "Bill to" address listed on the first page of this Agreement and, for Xerox, our inquiry address set forth on the most recent invoice to you.

SOFTWARE TERMS: The following additional terms apply only to transactions covering Application Software and/or Xerox-brand Equipment:

1) SOFTWARE LICENSE. The following terms apply to copyrighted software and the accompanying documentation, including, but not limited to, operating system software, provided with or within the Xerox-brand Equipment acquired hereunder ("Base Software") as well as software specifically set out as "Application Software" on the face of this Agreement. This license does not apply to any Diagnostic Software or to any software and accompanying documentation made subject to a separate license agreement.
   A) Xerox grants you a non-exclusive, non-transferable license to use the Base Software within the United States, its territories, and possessions (the "United States") only on or with the Equipment with which (or within which) it was delivered. For Application Software, Xerox grants you a non-exclusive, non-transferable license to use this software within the United States on any single unit of equipment for as long as you are current in the payment of any indicated software license fees (including any Annual Renewal Fees). You have no other rights to the Base or Application Software and, in particular, may not: (1) distribute, copy, modify, create derivatives of, decompile, or reverse engineer this software; (2) activate any software delivered with or within the Equipment in an unactivated state; or, (3) allow others to engage in same. Title to the Base and Application Software and all copyrights and other intellectual property rights in it shall at all times reside solely with Xerox and/or its licensors (who shall be considered third-party beneficiaries of this Agreement's software and limitation of liability provisions). Base and Application Software may contain, or be modified to contain, computer code capable of automatically disabling proper operation or functioning of the Equipment. Such disabling code may be activated if: (a) Xerox is denied access to the Base or Application Software to periodically reset such code; (b) you otherwise breach any term of this Agreement; or, (c) your license is terminated or expires.
   B) Xerox may terminate your license for any Base Software (1) immediately if you no longer use or possess the Equipment or are a lessor of the Equipment and your first lessee no longer uses or possesses it, or (2) upon the termination of any agreement under which you have rented or leased the Equipment.
   C) If you transfer possession of the Equipment after you obtain title to it, Xerox will offer the transferee a license to use the Base Software within the United States on or with it, subject to Xerox's then-applicable terms and license fees, if any, and provided the transfer is not in violation of Xerox's rights.
   D) Xerox warrants that the Base and Application Software will perform in material conformity with its user documentation for a ninety (90) day period from the date it is delivered or, for software installed by Xerox, the date of software installation. Neither Xerox nor its licensors warrant that the Base or Application Software will be free from errors or that its operation will be uninterrupted.

2) SOFTWARE SUPPORT. During the period that Xerox (or a designated servicer) provides Basic Services for the Equipment but in no event longer than five (5) years after Xerox stops taking orders from customers for their acquisition of the subject model of Equipment, Xerox (or a designated servicer) will also provide software support for the Base Software under the following terms. For Application Software licensed pursuant to this Agreement, Xerox will provide software support under the following terms provided you are current in the payment of all Initial License and Annual Renewal Fees (or, for programs not requiring Annual Renewal Fees, the payment of the Initial License Fee and the annual "Support Only" Fees).
   A) Xerox will assure that Base and Application Software performs in material conformity with its user documentation and will maintain a toll-free hotline during standard business hours to answer related questions.
   B) Xerox may make available new releases of the Base or Application Software that primarily incorporate coding error fixes and are designated as "Maintenance Releases". Maintenance Releases are provided at no charge and must be implemented within six (6) months after being made available to you. Each new Maintenance Release shall be

considered Base or Application Software governed by these Software Terms. New releases of the Base or Application Software that are not Maintenance Releases, if any, may be subject to additional license fees at Xerox's then-current pricing and shall be considered Base or Application Software governed by these Software Terms (unless otherwise noted). Xerox will not be in breach of its software support obligations hereunder if, in order to implement, in whole or in part, a new release of Base or Application Software provided or made available to you by Xerox, you must procure, at your expense, additional hardware and/or software from Xerox or any other entity. You agree to return or destroy all prior releases.

C) Xerox will use reasonable efforts, either directly and/or with its vendors, to resolve coding errors or provide workarounds or patches, provided you report problems as specified by Xerox.

D) Xerox shall not be obligated (1) to support any Base or Application Software that is two or more releases older than Xerox's most current release or (2) to remedy coding errors if you have modified the Base or Application Software.

E) For Application Software, Xerox may annually increase the Annual Renewal and Support-Only Fees, each such increase not to exceed 10%. (For state and local-government customers, this adjustment shall take place at the commencement of each of your annual contract cycles.)

3) DIAGNOSTIC SOFTWARE. Software used to maintain the Equipment and/or diagnose its failures or substandard performance (collectively "Diagnostic Software") is embedded in, resides on, or may be loaded onto the Equipment. The Diagnostic Software and method of entry or access to it constitute valuable trade secrets of Xerox. Title to the Diagnostic Software shall at all times remain solely with Xerox and/or Xerox's licensors. You agree that (a) your acquisition of the Equipment does not grant you a license or right to use the Diagnostic Software in any manner, and (b) that unless separately licensed by Xerox to do so, you will not use, reproduce, distribute, or disclose the Diagnostic Software for any purpose (or allow third parties to do so). You agree at all times (including subsequent to the expiration of this Agreement) to allow Xerox to access, monitor, and otherwise take steps to prevent unauthorized use or reproduction of the Diagnostic Software.

LEASE TERMS: The following additional terms apply only to lease transactions:

1) NON-CANCELABLE LEASE. THIS AGREEMENT IS A LEASE AND IT CANNOT BE CANCELED OR TERMINATED EXCEPT AS EXPRESSLY PROVIDED HEREIN, AND YOUR OBLIGATION TO MAKE ALL PAYMENTS DUE OR TO BECOME DUE SHALL BE ABSOLUTE AND UNCONDITIONAL AND SHALL NOT BE SUBJECT TO ANY DELAY, REDUCTION, SET-OFF, DEFENSE, COUNTERCLAIM OR RECOUPMENT FOR ANY REASON WHATSOEVER, IRRESPECTIVE OF XEROX'S PERFORMANCE OF ITS OBLIGATIONS HEREUNDER. ANY CLAIM AGAINST XEROX MAY BE ASSERTED SOLELY AGAINST XEROX IN A SEPARATE ACTION.

2) LEASE COMMENCEMENT, PAYMENT, TAXES & CREDIT HISTORY.

   A) The lease term for this Agreement shall commence upon installation of the Equipment; provided, however, for customer-installable Equipment, the lease term for this Agreement shall commence upon delivery of the Equipment.

   B) Invoices are payable upon receipt and you agree to pay Xerox each Minimum Lease Payment, all Print Charges and all other sums due as follows: (i) if the invoice displays a due date, payment is due and must be received by Xerox on or before said due date, or (ii) if the invoice does not display a due date, payment is due and must be received by Xerox no later than thirty (30) days after the invoice date. Restrictive covenants on instruments or documents submitted for or with payments you send to Xerox will not reduce your obligations.

   C) You shall be responsible for any and all applicable Taxes, which will be included in Xerox's invoice unless you provide proof of your tax exempt status. "Taxes" shall mean any tax, assessment or charge imposed or collected by any governmental entity or any political subdivision thereof, however designated or levied, imposed on this Agreement or the amounts payable to Xerox by you for the billing of Products, Print Charges, services and maintenance of any kind; Taxes include, but are not limited to, sales and use, rental, excise, gross receipts and occupational or privilege taxes, plus any interest and/or penalty thereon, but excluding any personal property taxes and taxes on Xerox's net income. If a taxing authority determines that Xerox did not collect all applicable Taxes, you shall remain liable to Xerox for such additional Taxes.

   D) You, to the extent required by applicable law, authorize Xerox (or its agent) to obtain credit reports, make such other credit inquiries as Xerox may deem necessary at any time, furnish payment history information to credit reporting agencies, and release to prospective assignees of this Agreement or any rights hereunder credit-related information Xerox has about you and this Agreement. Even if Products have been delivered, Xerox may, within sixty (60) days following its acceptance of this Agreement, revoke the Agreement if your credit approval is denied.

3) ASSIGNMENT.

   A) If you wish to assign any rights or obligations under this Agreement, you shall provide a written notice to Xerox of such request for consent, with said notice including the name of the proposed assignee. Your request to assign this Agreement will be granted by Xerox if: (1) you are not in default under this Agreement or any other agreement with Xerox; (2) the proposed assignee agrees to the section of this Agreement titled "LEASE COMMENCEMENT, PAYMENT, TAXES & CREDIT HISTORY" as applicable to it, for the purposes of the proposed assignment; (3) the proposed assignee meets Xerox's then current credit criteria for similar transactions as determined by Xerox in its sole discretion; and, (4) you and the proposed assignee execute a writing, in a form acceptable to Xerox, confirming said assignment. Assignment by you requires the written consent of Xerox and may not be accomplished by operation of law.

   B) Xerox may assign this Agreement, in whole or in part, to a parent, subsidiary or affiliate of Xerox, or to a person or entity for the purposes of securitizing a pool of assets or as part of a third party financial transaction without prior notice to you; provided, however, any proposed assignment to a person or entity not identified previously in this sentence

shall require your prior written consent. In the event of an assignment permitted by the preceding sentence, Xerox, without notice to you, may release information it has about you related to this Agreement. Each successive assignee of Xerox shall have all of the rights but none of the obligations of Xerox hereunder. You shall continue to look to Xerox for performance of Xerox's obligations, including the provision of Basic Services, and you hereby waive and release any assignees of Xerox from any such claim relating to or arising from the performance of Xerox's obligations hereunder. You shall not assert any defense, counterclaim or setoff that you may have or claim against Xerox against any assignees of Xerox. In the event of an assignment by Xerox, you shall remit payments due in accordance with remittance instructions of the assignee.

4) MINIMUM LEASE PAYMENTS. The Minimum Lease Payments, along with any additional Print Charges, cover your cost for the use of the Equipment and its maintenance as described herein. Each Minimum Lease Payment (which may be billed on more than one invoice) shall consist of the total of (a) any Periodic Base Charge, and (b) any Periodic Minimum Number of Prints multiplied by the applicable Meter 1 Print Charge(s). For full-color Equipment, color copies are counted on Meter 1.

5) MAINTENANCE COMPONENT PRICE INCREASES. Xerox may annually increase that amount of the Minimum Lease Payment and Print Charges you are charged for maintenance of the Equipment (the "Maintenance Component"), each such increase not to exceed 10%. (For state and local government customers, this adjustment shall take place at the commencement of each of your annual contract cycles.)

6) TITLE, RISK & RELOCATION. Title to the Equipment shall remain with Xerox until you exercise your option to purchase it. Until you exercise your option to purchase the Equipment, you agree that: (a) it shall remain personal property; (b) you will not attach any of it as a fixture to any real estate; (c) you will not pledge, sub-lease or part with possession of it or file or permit to be filed any lien against it; and, (d) you will not make any permanent alterations to it. The risk of loss due to your fault or negligence, as well as theft, fire or disappearance, shall pass to you upon shipment from a Xerox controlled facility. The risk of loss due to all other causes shall remain with Xerox unless and until you exercise your option to purchase the Equipment. Until title passes to you, all Equipment relocations must be arranged (or approved in advance) by Xerox and shall be at your expense. While Equipment is being relocated, you are responsible for all payments required to Xerox under this Agreement. Equipment cannot be relocated outside of the United States, its territories or possessions until you have exercised the Purchase Option indicated in this Agreement. If you acquire title to the Equipment, you must comply with all applicable laws and regulations regarding the export of any commodity, technology and/or software. All parts/materials replaced, including as part of an upgrade, will become Xerox's property.

7) DEFAULT & REMEDIES; LATE CHARGES & COLLECTION COSTS.

A) For any payment not received by Xerox within ten (10) days of the due date as set forth herein, Xerox may charge, and you agree to pay, a late charge equal to the higher of five percent (5%) of the amount due or $25 (not to exceed the maximum amount permitted by law) as reasonable collection costs.

B) You will be in default under this Agreement if (1) Xerox does not receive any payment within fifteen (15) days after the date it is due or (2) if you breach any other obligation hereunder. If you default, Xerox, in addition to its other remedies (including the cessation of Basic Services), may require immediate payment, as liquidated damages for loss of bargain and not as a penalty, of: (a) all amounts then due, plus interest on all amounts due from the due date until paid at the rate of one and one-half percent (1.5%) per month (not to exceed the maximum amount permitted by law); (b) the remaining Minimum Lease Payments in the Agreement's term less any unearned finance, maintenance, and supply charges (as reflected on the lessor's books and records); (c) a reasonable disengagement fee calculated by Xerox that will not exceed fifteen percent (15%) of the amount in (b) above (said amount is available from Xerox upon request); and (d) all applicable Taxes. You also shall either (1) make the Equipment available for removal by Xerox when requested to do so by Xerox and, at the time of removal, the Equipment shall be in the same condition as when delivered (reasonable wear and tear excepted), together with any related software, or (2) purchase the Equipment "AS IS, WHERE IS" and WITHOUT ANY WARRANTY AS TO CONDITION OR VALUE by paying Xerox the Purchase Option and all applicable Taxes. Xerox's decision to waive or forgive a particular default shall not prevent Xerox from declaring any other default. In addition, if you default under this Agreement, you agree to pay all of the costs Xerox incurs to enforce its rights against you, including reasonable attorneys' fees and actual costs.

8) PURCHASE LEASE OPTIONS. The following options are available for Equipment subject to this Agreement.

A) PURCHASE OPTION. If not in default, you may purchase the Equipment, "AS IS, WHERE-IS" and WITHOUT ANY WARRANTY AS TO CONDITION OR VALUE: (i) at the end of the lease term for the Purchase Option indicated on the face of this Agreement (i.e. either a set dollar amount or the Fair Market Value of the Equipment at the lease term's conclusion ["FMV"]), plus all applicable Taxes, or (ii) any time during the lease term by paying: (1) all amounts then due; (2) the remaining Minimum Lease Payments in the Agreement's term less any unearned finance, maintenance, and supply charges (as reflected on the lessor's books and records); (3) a reasonable disengagement fee calculated by Xerox that will not exceed fifteen percent (15%) of the amount in (2) above (said amount is available from Xerox upon request); (4) the applicable Purchase Option; and (5) all applicable Taxes.

B) RENEWAL. Unless either party provides notice at least thirty (30) days before the end of the lease term of its intention not to renew this Agreement, it will be renewed automatically on a month-to-month basis at the same price, terms and conditions and billing frequency as the original Agreement. During this renewal period, either party may terminate this Agreement upon at least thirty (30) days notice.

C) LEASE TERMINATION. Upon termination pursuant to B. above, and if you have not purchased the Equipment, you shall make the Equipment available for removal by Xerox when requested to do so by Xerox and, at the time of removal, the Equipment shall be in the same condition as when delivered (reasonable wear and tear excepted), together with any related software.

9) PROTECTION OF XEROX'S RIGHTS. You hereby authorize Xerox or its agents to file, by any permissible means, financing statements necessary to protect Xerox's rights as the Equipment Lessor. Xerox, on your behalf and at your expense, may take any action required to be taken by you under this Agreement that you fail to take.

10) WARRANTY DISCLAIMER & WAIVERS. XEROX DISCLAIMS, AND YOU WAIVE, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE. The parties intend this Agreement to be a "finance lease" under Article 2A of the Uniform Commercial Code. Except to the extent expressly provided, herein and to the extent permitted by applicable law, you waive all rights and remedies conferred upon a lessee by said Article.

SALE TERMS:

1. PAYMENT & TAXES.

A. Payment (including applicable Taxes) is due within thirty (30) days after receipt of the invoice with all maintenance charges being billed in arrears. . Restrictive covenants on instruments or documents submitted for or with payments you send to Xerox will not reduce your obligations.

B. You shall be responsible for any and all applicable Taxes, which will be included in Xerox's invoice unless you provide proof of your tax exempt status. "Taxes" shall mean any tax, assessment or charge imposed or collected by any governmental entity or any political subdivision thereof, however designated or levied, imposed on this Agreement or the amounts payable to Xerox by you for the billing of Products, Print Charges, services and maintenance of any kind; Taxes include, but are not limited to, sales and use, rental, excise, gross receipts and occupational or privilege taxes, plus any interest and/or penalty thereon, but excluding any taxes on Xerox's net income. If a taxing authority determines that Xerox did not collect all applicable Taxes, you shall remain liable to Xerox for such additional Taxes.

2. DEFAULT & REMEDIES; LATE CHARGES & COLLECTION COSTS.

A. For any payment not received by Xerox within ten (10) days of the due date as set forth herein, Xerox may charge, and you agree to pay, a late charge equal to the higher of five percent (5%) of the amount due or $25 (not to exceed the maximum amount permitted by law) as reasonable collection costs.

3. COMMENCEMENT, TITLE, RISK, AND RELOCATION.

A. The term for this Agreement and any warranty applicable to the Equipment shall commence upon installation of the Equipment; provided, however, for customer-installable Equipment, the term for this Agreement and any express warranty period applicable to the Equipment shall commence upon equipment delivery date.

B. Title and risk of loss to Equipment will pass to you upon shipment from a Xerox controlled facility. Upon passage to you of title to the Equipment, you must comply with all applicable laws and regulations regarding the export of any commodity, technology and/or software. Until you have paid for the Equipment in full, you agree that: (1) it shall remain personal property; (2) you will not attach any of it as a fixture to any real estate; (3) you will not pledge, sub-lease or part with possession of it or file or permit to be filed any lien against it; and, (4) you will not make any permanent alterations to it.

C. Until you have paid for the Equipment in full, you must provide Xerox prior written notice of all Equipment relocations and, upon your request, Xerox may arrange to relocate the Equipment at your expense. While Equipment is being relocated, you are responsible for all payments required under this Agreement to Xerox. All parts/materials replaced, including as part of an upgrade, will become Xerox's property.

MAINTENANCE TERMS: The following additional terms apply only to maintenance transactions:

1. PAYMENT & TAXES.

A. Payment (including applicable Taxes) is due within thirty (30) days after receipt of the invoice with all maintenance charges being billed in arrears. . Restrictive covenants on instruments or documents submitted for or with payments you send to Xerox will not reduce your obligations.

B. You shall be responsible for any and all applicable Taxes, which will be included in Xerox's invoice unless you provide proof of your tax exempt status. "Taxes" shall mean any tax, assessment or charge imposed or collected by any governmental entity or any political subdivision thereof, however designated or levied, imposed on this Agreement or the amounts payable to Xerox by you for the billing of Products, Print Charges, services and maintenance of any kind; Taxes include, but are not limited to, sales and use, rental, excise, gross receipts and occupational or privilege taxes, plus any interest and/or penalty thereon, but excluding any taxes on Xerox's net income. If a taxing authority determines that Xerox did not collect all applicable Taxes, you shall remain liable to Xerox for such additional Taxes.

2. MINIMUM PERIODIC MAINTENANCE PAYMENTS. Each Minimum Maintenance Payment includes a Periodic Base Charge, and may include a Periodic Minimum Number of Prints. Minimum Periodic Base Charges are billed in advance, with additional Print Charges billed in arrears.

3. DEFAULT & REMEDIES; LATE CHARGES & COLLECTION COSTS.

A. For any payment not received by Xerox within ten (10) days of the due date as set forth herein, Xerox may charge, and you agree to pay, a late charge equal to the higher of five percent (5%) of the amount due or $25 (not to exceed the maximum amount permitted by law) as reasonable collection costs.

B. You will be in default under this Agreement if (1) Xerox does not receive any payment within fifteen (15) days after the date it is due or (2) if you breach any other obligation hereunder. If you default, Xerox, in addition to its other remedies (including the cessation of Basic Services), may require immediate payment, as liquidated damages for loss of bargain and not as a penalty, of (a) all amounts then due, plus interest on all amounts due from the due date until paid at the rate of one and one-half percent (1.5%) per month (not to exceed the maximum amount permitted by law); (b) the lesser of the remaining Minimum Periodic Base Charge in the Agreement's term or six (6) such payments for one-year agreements (and twelve (12) such payments for multi-year agreements); and, (c) all applicable Taxes. Xerox's decision to waive or forgive a particular default shall not prevent Xerox from declaring any other default. In addition, if you default under this Agreement, you agree to pay all of the costs Xerox incurs to enforce its rights against you, including reasonable attorneys' fees and actual costs.