White Paper sulla sicurezza di Fiery

Fiery FS200 Pro /FS200 Server

Data di pubblicazione: Maggio 2018

Serie White Paper

White Paper sulla sicurezza di Fiery

Indice

1 Descrizione del documento

Questo documento offre una panoramica sull'architettura e sugli aspetti funzionali di Fiery® Server in relazione alla sicurezza dei server Fiery FS200/FS200 Pro. Descrive i componenti hardware, la sicurezza della rete, il controllo degli accessi, il sistema operativo e la sicurezza dei dati.

Lo scopo di questo documento è di far conoscere agli utenti finali tutti i vantaggi offerti dalle funzioni di sicurezza di Fiery Server e le eventuali vulnerabilità.

1.1 Filosofia EFI sulla sicurezza

EFI™ è consapevole che la sicurezza rappresenta una delle preoccupazioni principali delle aziende moderne di tutto il mondo. Ed è per questo motivo che ha incorporato in Fiery Server efficaci funzioni di sicurezza capaci di proteggere le risorse più preziose delle aziende. Inoltre, EFI collabora attivamente con i partner OEM internazionali e i suoi team per individuare le necessità di sicurezza attuali e future delle aziende e garantire sempre la massima sicurezza dei suoi prodotti.
Come sempre, EFI consiglia agli utenti finali di combinare le funzioni di sicurezza Fiery con altri dispositivi di protezione, come password sicure e stringenti procedure fisiche, al fine di garantire la sicurezza complessiva del sistema.

1.2 Configurare la funzione Sicurezza con Fiery Configure

Gli utenti Fiery che hanno accesso alla sicurezza di Fiery Server tramite Fiery Command WorkStation® effettuando il login come amministratore possono configurare tutte le funzioni Fiery con Fiery Configure. Fiery Configure può essere avviato da Fiery Command WorkStation o WebTools™ sotto la scheda Configure.

2 Hardware e sicurezza fisica

2.1 Memoria volatile

Fiery Server usa la RAM volatile per la memoria locale della CPU e per il sistema operativo, il software del sistema Fiery e la memoria di lavoro dei dati immagine. I dati che vengono scritti sulla RAM vengono conservati per tutto il tempo in cui il server è alimentato. Quando l'alimentazione viene a mancare, tutti i dati vengono cancellati.

2.2 Memoria non volatile e Data Storage

Fiery Server contiene diversi tipi di tecnologie di memoria non volatile che conservano i dati quando viene spenta l'alimentazione. Questi dati sono le informazioni dei programmi del sistema e i dati utente.

2.2.1 Memoria flash

La memoria flash memorizza l'autodiagnostica e il programma di avvio (BIOS), oltre ad alcuni dati di configurazione del sistema. Viene programmata in fabbrica e può anche essere riprogrammata installando patch speciali create da EFI. Se i dati sono stati danneggiati o cancellati, il sistema non si avvia.

Una parte della memoria flash viene usata anche per registrare l'uso della chiave hardware che serve per attivare le opzioni del software Fiery.

Su questo componente non sono memorizzati dati utente e l'utente non vi ha accesso.

2.2.2 CMOS

La memoria CMOS alimentata a batteria memorizza le impostazioni macchina del server. Nessuna di queste informazioni è considerata confidenziale o privata. Gli utenti possono accedere a queste impostazioni su un server con Windows 8.1 Pro da Fiery Integrated Workstation (kit FACI con monitor, tastiera e mouse locali) se installato.

2.2.3 NVRAM

Fiery Server comprende alcuni componenti NVRAM contenenti il firmware operativo, dati operativi non specifici del cliente. L'utente non ha accesso a tali dati.

2.2.4 Unità disco fisso

Durante le normali operazioni di stampa e scansione e durante la creazione delle informazioni di gestione dei lavori, i dati immagine vengono scritti su un'area casuale dell'unità disco fisso (HDD).

I dati immagine e di gestione dei lavori possono essere eliminati da un operatore o dopo un periodo di tempo predefinito, rendendoli così inaccessibili.

Per proteggere i dati immagine dall'accesso non autorizzato, EFI offre la funzione Eliminazione sicura (vedere la sezione 6.2.5). Una volta abilitata dall'amministratore del sistema, l'operazione selezionata viene eseguita nel momento indicato per eliminare in modo sicuro i dati dall'unità disco fisso.

2.2.5 Porte fisiche

Fiery Server può essere collegato alle seguenti porte esterne:

Porte Fiery	Funzione	Accesso	Controllo accessi
Connettore Ethernet RJ-45	Connettività Ethernet	Collegamenti di rete (vedere collegamenti di stampa e rete più avanti)	Usare il filtraggio IP Fiery per il controllo degli accessi
Connettore interfaccia fotocopiatrice	Stampa/ Scansione	Dedicato a invio/ ricezione dal motore di stampa	N/A
Porta USB	Collegamento dispositivo USB	Connettore Plug-and-Play progettato per dispositivi rimovibili opzionali	La stampa USB è disattivabile. L'accesso ai dispositivi USB può essere disattivato con i criteri di gruppo Windows.

2.3 Interfaccia locale

L'utente può accedere alle funzioni Fiery dal kit FACI (se abilitato su un server con Windows 8.1 Pro) o dal display LCD Fiery. L'accesso a Fiery Server con il kit FACI è controllato da una password di amministratore Windows se il kit FACI è abilitato. Il display LCD Fiery offre funzioni molto limitate che non rappresentano alcun rischio per la sicurezza.

2.4 Kit HDD rimovibile opzionale

Fiery Server è compatibile con un kit disco fisso rimovibile opzionale che garantisce una maggiore sicurezza. Il kit consente di bloccare le unità disco del server durante il normale funzionamento e di rimuoverle per riporle in una postazione sicura dopo lo spegnimento del server.

2.4.1 Per server esterni

Fiery Server è compatibile con un kit disco fisso rimovibile opzionale. La disponibilità del kit per un prodotto Fiery specifico dipende dai termini dei contratti di sviluppo e distribuzione che EFI ha in essere con i singoli partner OEM.

2.4.2 Per server incorporati

I prodotti incorporati possono offrire solo HDD rimovibili come opzione coordinata OEM, perché il punto e le staffe di montaggio della stampante multifunzione (MFP) devono essere sviluppati congiuntamente con il produttore OEM. Il kit opzionale prevede l'estrazione dell'unità HDD interna dal telaio del prodotto incorporato e il montaggio in un contenitore esterno e alimentato a parte.

3 Sicurezza della rete

Le funzionalità di sicurezza standard della rete su Fiery Server possono consentire l'accesso ai sistemi di stampa solo a utenti e gruppi autorizzati, limitando la comunicazione a indirizzi IP prestabiliti, e controllando la disponibilità di porte e protocolli di rete.

Anche se Fiery Server viene fornito con diverse funzioni di sicurezza, non è un server con accesso a Internet. Deve essere installato in un ambiente protetto e l'accessibilità deve essere configurata adeguatamente dall'amministratore di rete.

3.1 Porte di rete

Fiery Server consente all'amministratore di rete di abilitare e disabilitare selettivamente le seguenti porte IP. Pertanto, è possibile bloccare le comunicazioni e gli accessi indesiderati ai sistemi da specifici protocolli di trasporto.

TCP	UDP	Porta	Servizi dipendenti
20–21		FTP	
80		HTTP	WebTools, IPP
135		MS RPC	Servizio RPC Microsoft® (solo Windows 8.1 Pro). Si aprirà un'altra porta compresa tra 49152 e 65536 per fornire il servizio Point and Print SMB.
137–139		NETBIOS	Stampa da Windows
	161, 162	SNMP	WebTools, Velocity, alcuni programmi di utilità precedenti, altri strumenti basati su SNMP
	427	SLP	
443		HTTPS	WebTools, IPP/s
445		SMB/IP	SMB su TCP/IP
	500	ISAKMP	IPSec
515		LPD	Stampa LPR, alcuni programmi di utilità precedenti (WebTools, versioni precedenti di CWS)
631		IPP	IPP
3050			Firebird
	4500	IPsec NAT	IPSec
	5353	Multicast DNS	Bonjour
3389		RDP	Remote Desktop (Windows Fiery servers only)
3702	3702	WS-Discovery	WSD
6310 8010 8021–8022 8090 9906 18021 18022 18081 18082 21030 22000 50006 - 50025*	9906	Porte EFI	Command WorkStation 4 e 5, Fiery Central, strumenti SDK EFI, funzioni bidirezionali Fiery Printer Driver, WebTools, Stampa mobile diretta Fiery e conversione documenti nativi.
9100–9103		Porta stampa	Port 9100

Altre porte TCP, ad eccezione di quelle specificate dal produttore OEM, sono disabilitate. Qualsiasi servizio dipendente da una porta disabilitata non è accessibile in remoto.

L'amministratore Fiery può inoltre abilitare e disabilitare i diversi servizi di rete forniti da Fiery Server.

L'amministratore locale può definire i nomi delle comunità in scrittura e lettura SNMP e altre impostazioni di sicurezza.

3.2 Filtraggio IP

L'amministratore può limitare i collegamenti autorizzati a Fiery Server da quegli host i cui indirizzi IP rientrano in un gruppo IP particolare. I comandi o i lavori inviati da indirizzi IP non autorizzati vengono ignorati.

3.3 Crittografia di rete

3.3.1 IPsec

Il protocollo IPsec o IP (Internet Protocol) garantisce la sicurezza di tutte le applicazioni sui protocolli IP tramite crittografia e autenticazione di ogni singolo pacchetto.

Fiery Server usa l'autenticazione con codice precondiviso per stabilire collegamenti sicuri con altri sistemi su IPsec.

Dopo aver stabilito la comunicazione sicura su IPsec tra un computer client e Fiery Server, tutte le comunicazioni, inclusi i lavori di stampa, vengono trasmesse sulla rete in tutta sicurezza.

*Queste porte sono abilitate quando Fiery Command WorkStation 6.2 o versione successiva è installato su un server Fiery esterno.

3.3.2 SSL e TLS

SSL/TLS sono protocolli a livello applicativo per la trasmissione sicura di messaggi su Internet. Fiery Server supporta i protocolli SSL v3 e TLS v1.0/v1.1/v1.2.

Varie funzioni di Fiery Server supportano SSL/TLS. Gli utenti possono accedere alla pagina iniziale di Fiery Server e alle API Web in modo sicuro su SSL/TLS. Il collegamento ai server LDAP e ai server e-mail può essere configurato per funzionare su SSL/TLS e garantire così la comunicazione sicura.

3.3.3 Gestione dei certificati

Fiery Server fornisce un'interfaccia di gestione dei certificati che gestisce i certificati usati in varie comunicazioni SSL/TLS. Supporta il formato certificato X.509.

La gestione dei certificati permette all'amministratore Fiery di fare quanto segue:

- Creare certificati digitali autofirmati.
- Aggiungere un certificato e il corrispondente codice privato per Fiery Server.
- Aggiungere, selezionare, visualizzare e rimuovere i certificati da un archivio di certificati attendibili.

3.4 IEEE 802.1x

802.1x è uno standard IEEE per il controllo degli accessi in rete basato sulle porte. Questo protocollo offre un meccanismo di autenticazione prima che il dispositivo ottenga l'accesso alla rete LAN e alle relative risorse.

Quando è abilitato, Fiery Server può essere configurato per usare EAP MD5-Challenge o PEAP-MSCHAPv2 per autenticarsi su un server di autenticazione 802.1x.

Fiery Server esegue l'autenticazione all'avvio oppure quando il cavo Ethernet viene scollegato e ricollegato.

3.5 SNMP v3

Fiery Server supporta SNMPv3, in quanto è un protocollo di rete protetto per la gestione dei dispositivi su reti IP. I pacchetti di comunicazione SNMPv3 possono essere crittografati per garantirne la riservatezza. Assicura inoltre l'integrità e l'autenticazione dei messaggi.

L'amministratore Fiery può scegliere fra tre livelli di sicurezza in SNMPv3. L'amministratore Fiery può anche richiedere l'autenticazione prima di consentire le transazioni SNMP e crittografare i nomi utente e le password SNMP.

3.6 Sicurezza e-mail

Fiery Server supporta i protocolli POP e SMTP. Per proteggere il servizio da attacchi e uso improprio, l'amministratore Fiery può abilitare altre funzioni di sicurezza come le seguenti:

3.6.1 POP before SMTP

Alcuni server e-mail supportano ancora il protocollo SMTP non protetto che consente a chiunque di inviare e-mail senza autenticazione. Per impedire l'accesso non autorizzato, alcuni server e-mail richiedono ai client e-mail di autenticarsi su POP prima di usare SMTP per inviare un'e-mail. Per tali server e-mail, l'amministratore Fiery dovrebbe abilitare l'autenticazione POP prima di SMTP.

3.6.2 OP25B

OP25B (Outbound Port 25 Blocking) e una misura antispam in base alla quale i fornitori di servizi Internet (ISP) possono bloccare i pacchetti che arrivano alla porta 25 attraverso i loro router. L'interfaccia di configurazione e-mail consente all'amministratore Fiery di specificare una porta diversa.

4 Controllo degli accessi

4.1 Autenticazione utente

La funzione Autenticazione utente di Fiery Server consente di effettuare le seguenti operazioni:

- Autenticare i nomi utente.
- Autorizzare azioni sulla base dei privilegi dell'utente.

Fiery Server può autenticare quegli utenti che sono:

- Su un dominio: utenti definiti su un server aziendale accessibile da LDAP.
- Su Fiery: utenti definiti su Fiery Server.

Fiery Server autorizza le azioni di un utente sulla base dell'appartenenza a un gruppo. A ciascun gruppo è associata una serie di privilegi (ad esempio, Stampa in B/N, Stampa a colori o B/N) e le azioni degli utenti appartenenti ai diversi gruppi sono limitate a tali privilegi.

I gruppi Fiery sono gruppi di utenti con una serie predefinita di privilegi. Il gruppo Fiery assegna una serie di privilegi a una tipologia di utenti.

L'amministratore Fiery può modificare i privilegi di un qualsiasi gruppo Fiery, ad eccezione degli utenti Amministratore, Operatore e Guest.

Per questa versione di Autenticazione utente, i diversi livelli di privilegi che possono essere modificati o selezionati per un gruppo sono i seguenti:

- Stampa in B/N — questo privilegio consente ai membri del gruppo di stampare lavori su Fiery Server. Se l'utente non ha il privilegio "Stampa a colori e in B/N", Fiery Server forza il lavoro stampandolo in bianco e nero (B/N).
- Stampa a colori e in B/N — questo privilegio consente ai membri del gruppo di stampare lavori su Fiery Server con accesso totale alle funzionalità di stampa a colori e in scala di grigi di Fiery Server. Senza questo privilegio o quello di Stampa in B/N, il lavoro non verrà stampato e gli utenti non potranno inoltrarlo tramite FTP (solo sistemi a colori).
- Fiery Mailbox — questo privilegio consente ai membri del gruppo di avere mailbox individuali. Fiery Server crea una mailbox basata sul nome utente con privilegio mailbox. L'accesso a questa mailbox è limitato agli utenti con nomeutente/password mailbox.
- Calibrazione — questo privilegio consente ai membri del gruppo di eseguire la calibrazione del colore.
- Crea preimpostazioni server — questo privilegio consente ai membri del gruppo di creare preimpostazioni server per permettere ad altri utenti Fiery di accedere alle preimpostazioni lavoro di uso comune.
- Gestione flussi di lavoro — questo privilegio consente ai membri del gruppo di creare, pubblicare o cambiare le stampanti virtuali.

Nota: Autenticazione utente sostituisce le funzioni Stampa membri/Stampa gruppi.

4.2 Autenticazione del software Fiery

Fiery Server definisce gli utenti Amministratore, Operatore e Guest con diversi privilegi. Sono utenti specifici del software Fiery e non hanno alcun legame con gli utenti o i ruoli definiti in Windows. Si consiglia agli amministratori di richiedere le password per accedere a Fiery Server. Inoltre, EFI consiglia all'amministratore di cambiare la password predefinita con una diversa definita in base ai requisiti di sicurezza dell'utente finale.

I tre livelli di password su Fiery Server consentono l'accesso ai seguenti privilegi:

- Amministratore — ha il controllo totale su tutte le funzionalità di Fiery Server.
- Operatore — ha la maggior parte degli stessi privilegi dell'amministratore, ma non ha accesso ad alcune funzioni del server, come la configurazione, e non può cancellare il job log.
- Guest (predefinito; nessuna password) — ha la maggior parte degli stessi privilegi dell'operatore, ma non può accedere al job log, non può apportare modifiche e non può cambiare lo stato dei lavori di stampa, né visualizzare in anteprima i lavori.

5 Ambiente del sistema operativo

5.1 Procedure di avvio

Il sistema operativo e il software di sistema Fiery vengono caricati dall'unità disco fisso (HDD) in fase di avvio.

Il BIOS residente sulla scheda madre Fiery è a sola lettura e memorizza le informazioni necessarie per avviare il sistema operativo. I cambiamenti al BIOS (o la rimozione del BIOS) impediscono a Fiery Server di funzionare correttamente.

La pagina di configurazione riporta i valori specificati durante la configurazione. Alcune informazioni, come i dati proxy FTP, le password e i nomi delle comunità SNMP, non appaiono nella pagina di configurazione.

5.2 Linux

I sistemi Linux non comprendono un'interfaccia locale che consente l'accesso al sistema operativo.

5.2.1 Software antivirus Linux

Il sistema operativo Linux utilizzato su Fiery Server è un sistema operativo dedicato. Comprende tutti i componenti OS richiesti da Fiery Server, tranne alcuni utilizzati sui sistemi Linux generici, come Ubuntu. Oltre ad avere prestazioni migliori, questo OS dedicato non è vulnerabile ai virus come nel caso dei sistemi Linux generici e dei sistemi operativi Microsoft. Il software antivirus progettato per i sistemi operativi Linux generici potrebbe non funzionare su Fiery Server.

5.3 Windows 8.1 Pro

Fiery Server viene fornito con una password di amministratore predefinita per Windows 8.1. È consigliabile che l'amministratore provveda a cambiare la password al momento dell'installazione.
Inoltre, si consiglia fortemente di cambiare la password regolarmente, in conformità con la politica IT dell'organizzazione. La password dell'amministratore offre accesso totale a Fiery Server in locale e/o da una stazione di lavoro remota.
Consente inoltre l'accesso al file system, alla politica di sicurezza del sistema, alle voci di registro e altro. Inoltre, l'utente può cambiare la password dell'amministratore, negando a chiunque altro l'accesso a Fiery Server.

5.3.1 Patch di sicurezza Microsoft

Microsoft rilascia regolarmente patch per risolvere eventuali falle nella sicurezza del sistema operativo Windows 8.1. L'impostazione predefinita di Windows Update è di notificare agli utenti la disponibilità di patch senza però scaricarle. L'amministratore Fiery può modificare tale impostazione predefinita in Windows Update oppure installare manualmente le patch di sicurezza.

5.3.2 Strumenti SMS

EFI ha un proprio strumento di aggiornamento dedicato ai suoi sistemi basati su Windows. Questo strumento gestisce il recupero di tutte le patch di sicurezza Microsoft e degli aggiornamenti software Fiery. Fiery Server non supporta gli strumenti SMS di terzi per il recupero e l'applicazione di aggiornamenti a Fiery Server.

5.3.3 Software antivirus Windows

In genere, il software antivirus può essere usato con Fiery Server. Il software antivirus è disponibile in diverse varietà e può contenere molti componenti e funzioni specifici per una minaccia particolare. Riportiamo alcune direttive per aiutare i clienti a scegliere il software antivirus più adatto alle specifiche esigenze. Si noti che il software antivirus è particolarmente utile in una configurazione locale con kit FACI, in cui gli utenti possono inconsapevolmente trasferire un virus a Fiery Server con il normale utilizzo di Windows. Per Fiery Server senza kit FACI, è sempre possibile avviare un software antivirus su un PC remoto ed eseguire la scansione dell'unità disco fisso di un server Fiery condiviso. EFI consiglia comunque all'amministratore Fiery di tenersi in contatto diretto con il produttore del software antivirus per ogni necessità di supporto operativo. Seguono le direttive EFI per ciascuno dei componenti del software antivirus Windows:

Motore antivirus — quando un motore antivirus esegue la scansione di Fiery Server, programmata o meno, l'attività può incidere sulle prestazioni di Fiery.

Antispyware — un programma antispyware potrebbe incidere sulle prestazioni di Fiery nel caso di file in arrivo su Fiery Server. Ad esempio: lavori di stampa in arrivo, file scaricati durante un aggiornamento di sistema Fiery o un aggiornamento automatico di applicazioni in esecuzione su Fiery Server.

Firewall incorporato — poiché Fiery Server ha un firewall, in genere i firewall antivirus non sono necessari. EFI consiglia ai clienti di collaborare con la loro divisione IT aziendale e di fare riferimento alla sezione 3.1 di questo documento in caso abbiano necessità di installare ed eseguire un firewall incorporato incluso nel software antivirus.

Antispam — Fiery supporta le funzioni di stampa via e-mail e scansione via e-mail. Si consiglia di usare un meccanismo di filtraggio spam sul server. Fiery Server può anche essere configurato per stampare i documenti da indirizzi e-mail specifici. Il componente antispam non è necessario, perché non è consentito utilizzare un client e-mail separato (come Outlook) su Fiery Server.

Lista bianca e lista nera — le funzionalità di lista bianca e lista nera non presentano in linea di massima controindicazioni per Fiery Server. EFI consiglia fortemente di configurare questa funzionalità in modo che i moduli Fiery non siano inclusi nella lista nera.

HID e controllo applicativo — data la natura complessa dei parametri HID e controllo applicativo, la configurazione antivirus deve essere testata e verificata con attenzione quando si usa una di queste funzioni. Se messe a punto correttamente, HID e controllo applicativo sono eccellenti misure di sicurezza e coesistono con Fiery Server. Tuttavia, è molto facile che insorgano problemi sul server in caso di impostazioni non corrette del parametro HID e di esclusioni file errate, spesso per "accettazione dei valori predefiniti". Si consiglia pertanto di rivedere le opzioni selezionate nelle impostazioni HID e/o controllo applicativo insieme alle impostazioni di Fiery Server come porte di rete, protocolli di rete, eseguibili applicativi, file di configurazione, file temporanei e così via.

5.4 Virus trasmessi via e-mail

In genere, i virus trasmessi via e-mail richiedono l'esecuzione di alcune operazioni da parte di chi li riceve. Gli allegati che non sono file PDL vengono scartati da Fiery Server. Fiery Server ignora anche messaggi e-mail in RTF o HTML ed eventuali componenti Script inclusi. A parte la risposta e-mail a un utente specifico sulla base di un comando ricevuto, tutti i file ricevuti via e-mail sono considerati lavori PDL. Vedere i dettagli sul flusso di lavoro di stampa via e-mail nella sezione 6.4 di questo documento.

6 Sicurezza dei dati

6.1 Crittografia delle informazioni critiche

La crittografia di informazioni importanti su Fiery Server garantisce la protezione di tutte le password e delle relative informazioni di configurazione memorizzate su Fiery Server. Gli algoritmi crittografici usati sono conformi a NIST 2010.

6.2 Stampa standard

I lavori inoltrati a Fiery Server possono essere inviati a una delle seguenti code di stampa pubblicate da Fiery Server:

- Coda di attesa
- Coda di stampa
- Coda di stampa sequenziale
- Coda diretta (collegamento diretto)
- Stampanti virtuali (code personalizzate definite dall'amministratore Fiery).

L'amministratore Fiery può disabilitare la coda di stampa e la coda diretta per limitare la stampa automatica. Se su Fiery Server le password sono state abilitate, questa funzione consentirà la stampa solo agli operatori e amministratori Fiery.

6.2.1 Code di attesa, stampa e stampa sequenziale

Quando un lavoro viene stampato sulla coda di stampa o di attesa, viene inviato in spool sul disco fisso di Fiery Server. I lavori inviati alla coda di attesa vengono conservati sull'unità disco fisso di Fiery Server finché l'utente non inoltra il lavoro in stampa o non lo elimina con un programma di gestione dei lavori, come Fiery Command WorkStation, Fiery Command WorkStation ME o Ripristina server.

La coda di stampa sequenziale consente a Fiery Server di mantenere l'ordine di alcuni lavori inviati dalla rete. Il flusso di lavoro seguirà l'ordine di arrivo 'First In, First Out' (FIFO), rispettando l'ordine in cui i lavori vengono ricevuti sulla rete. Se la coda di stampa sequenziale non è abilitata, i lavori di stampa inoltrati a Fiery Server possono perdere l'ordine di arrivo a causa di diversi fattori, come ad esempio il fatto che Fiery Server fa passare avanti lavori più piccoli mentre è in corso lo spool di lavori più grandi.

6.2.2 Coda dei lavori stampati

I lavori inviati alla coda di stampa vengono memorizzati nella coda dei lavori stampati su Fiery Server, se abilitata. L'amministratore può definire il numero di lavori da conservare nella coda dei lavori stampati. Se la coda dei lavori stampati è disabilitata, i lavori vengono automaticamente eliminati dopo la stampa.

6.2.3 Coda diretta (collegamento diretto)

La coda diretta viene utilizzata per scaricare i font e le applicazioni che richiedono il collegamento diretto al modulo PostScript dei controller Fiery.

EFI sconsiglia di stampare sulla coda diretta. Fiery elimina tutti i lavori inviati tramite collegamento diretto dopo la stampa. Tuttavia, EFI non garantisce l'eliminazione totale di tutti i file temporanei relativi al lavoro.

Una volta inviati alla coda diretta, i lavori di tipo file VDP, PDF o TIFF vengono reindirizzati alla coda di stampa. Una volta inviati alla coda diretta, i lavori inviati tramite il servizio di rete SMB possono essere reindirizzati alla coda di stampa.

6.2.4 Eliminazione dei lavori

Quando un lavoro viene eliminato da Fiery Server automaticamente o con gli strumenti Fiery, non può più essere visualizzato o recuperato con gli strumenti Fiery. Se il lavoro è stato inviato in spool sull'unità disco fisso di Fiery Server, gli elementi del lavoro potrebbero rimanere sull'unità disco fisso ed essere in teoria recuperati con alcuni strumenti, come quelli di analisi del disco.

6.2.5 Eliminazione sicura

Eliminazione sicura consente di rimuovere dall'unità disco fisso Fiery i contenuti di un lavoro inoltrato non appena viene eliminato. Al momento dell'eliminazione, il file originale del lavoro viene sovrascritto tre volte con un algoritmo basato sulle specifiche DoD5220.22M del Dipartimento della Difesa americano.

Eliminazione sicura è soggetta alle seguenti limitazioni e restrizioni:

- Non si applica ai file dei lavori residenti su sistemi diversi da Fiery Server, come i seguenti:
  – copie del lavoro distribuite su un altro Fiery Server.
  – copie del lavoro archiviate su unità di rete o supporti di memorizzazione.
  – copie del lavoro residenti su stazioni di lavoro client.
  – pagine di un lavoro combinate o copiate interamente in un altro lavoro.
- Non elimina le voci dal Job Log.
- Se il sistema viene spento manualmente prima che venga completata la cancellazione di un lavoro, questo potrebbe non essere eliminato del tutto.
- Non elimina i dati di un lavoro che potrebbero essere stati scritti sul disco dopo l'operazione di swap del disco o di copia del disco.
- I lavori inoltrati da un server FTP potrebbero essere salvati dal client FTP prima di essere trasmessi al software di sistema Fiery. Poiché il software di sistema Fiery non ha alcun controllo su questo processo, il sistema non può eliminare in modo sicuro i lavori salvati dal client FTP.
- I lavori stampati via SMB passano attraverso lo spooler su Fiery, che li salva sul disco. Poiché il software di sistema Fiery non ha alcun controllo su questo processo, il sistema non può eliminare in modo sicuro questi lavori.

Nota: Lo swap del disco viene eseguito quando si ha più necessità di memoria virtuale che di memoria fisica. Il processo viene gestito al livello del sistema operativo e Fiery Server non ha alcun controllo su di esso. Tuttavia, lo spazio di swap del disco viene regolarmente riscritto durante l'esecuzione del sistema operativo, in quanto vari segmenti di memoria vengono spostati tra la memoria e il disco. Questo processo può comportare la memorizzazione temporanea su disco di alcuni segmenti del lavoro.

6.2.6 Memoria di sistema

L'elaborazione di alcuni file potrebbe comportare la scrittura di alcuni dati nella memoria del sistema operativo. In alcuni casi, questa memoria potrebbe essere copiata sull'unità disco fisso (HDD) e non essere quindi specificatamente sovrascritta.

6.3 Stampa protetta

La funzione Stampa protetta richiede all'utente di inserire una password specifica su Fiery Server per poter stampare il lavoro. Questa funzione richiede la presenza di un'interfaccia LCD locale su Fiery Server.

Lo scopo della funzione è di limitare l'accesso a un documento da parte di un utente che (a) conosce la password del lavoro e (b) può immetterla in locale su Fiery Server.

6.3.1 Flusso di lavoro

L'utente inserisce una password nel campo Stampa protetta di Fiery Driver. Quando il lavoro viene inviato alla coda di stampa o di attesa di Fiery Server, viene messo in coda e rimane in attesa dell'inserimento della password.

Nota: I lavori inviati con una password di stampa protetta non sono visualizzabili da Fiery Command WorkStation o Fiery Command WorkStation ME.

Dal display LCD Fiery, l'utente accede alla finestra Stampa protetta e inserisce la password. L'utente può quindi accedere ai lavori inviati con quella password e stamparli e/o eliminarli.

Il lavoro stampato con la funzione Stampa protetta non viene spostato nella coda dei lavori stampati, ma viene automaticamente eliminato al termine della stampa.

6.4 Stampa via e-mail

Fiery Server riceve e stampa i lavori inviati tramite e-mail. L'amministratore può conservare su Fiery Server un elenco di indirizzi e-mail autorizzati. I messaggi e-mail provenienti da indirizzi e-mail che non figurano nell'elenco verranno eliminati. L'amministratore può disattivare la funzione di stampa via e-mail che è disattivata per impostazione predefinita.

6.5 Gestione dei lavori

I lavori inoltrati a Fiery Server possono essere gestiti solo con un programma di gestione dei lavori Fiery con accesso come amministratore o operatore. Gli utenti Guest (senza password) possono visualizzare i nomi file e gli attributi dei lavori, ma non possono modificarli o visualizzarli in anteprima.

6.6 Job log

Il job log è memorizzato su Fiery Server. Non è possibile eliminare le singole voci del job log. Il job log contiene le informazioni sui lavori di stampa e scansione, ad esempio, il nome dell'utente che ha avviato il lavoro, la data e le caratteristiche del lavoro come la carta utilizzata, il colore e così via. Il job log è utile per analizzare le attività di Fiery Server sui lavori.

Un utente che accede come operatore può visualizzare, esportare o stampare il job log da Fiery Command WorkStation. Un utente che accede come amministratore può eliminare il job log da Fiery Command WorkStation. Un utente che accede come Guest può stampare il job log dal display LCD Fiery solo se autorizzato dall'amministratore.

6.7 Configurazione

Per accedere alla configurazione, è necessario immettere la password di amministratore. Fiery Server può essere configurato sia da Fiery Configure che dal display LCD Fiery. Fiery Configure può essere avviato da Fiery WebTools e Fiery Command WorkStation.

6.8 Scansione

Fiery Server consente di eseguire la scansione di un'immagine posizionata sul piano di copiatura della fotocopiatrice memorizzandola sulla stazione di lavoro da cui è stata avviata usando il modulo aggiuntivo TWAIN di Fiery. Il modulo aggiuntivo è supportato dalle applicazioni Adobe® Photoshop e Textbridge. Quando viene avviata una scansione da una stazione di lavoro, l'immagine bitmap "raw" viene inviata direttamente alla stazione di lavoro.

L'utente può eseguire la scansione di documenti su Fiery Server per poterli distribuire, archiviare e recuperare. Tutti i documenti acquisiti vengono scritti sul disco. L'amministratore può configurare Fiery Server in modo che elimini i lavori di scansione automaticamente dopo un periodo di tempo predefinito.

I lavori di scansione possono essere distribuiti utilizzando i seguenti metodi:

- E-mail — con questo metodo, viene inviata un'e-mail a un server di posta, da cui viene reindirizzata alla destinazione desiderata. Nota: se la dimensione del file supera il limite massimo definito dall'amministratore, il lavoro viene memorizzato sull'unità disco fisso di Fiery, accessibile da un URL.
- FTP — il file viene inviato a una destinazione FTP. Nel log FTP, accessibile tramite il menu Stampa pagine dal display LCD, viene conservata la traccia registrata del trasferimento, inclusa la destinazione. È possibile definire un server Proxy FTP per inviare il lavoro attraverso un firewall.
- Coda di attesa di Fiery — il file viene inviato alla coda di attesa di Fiery (vedere la sezione 6.2.1 più sopra) e non viene conservato come lavoro di scansione.
- Internet Fax — il file viene inviato a un server di posta, da cui viene reindirizzato alla destinazione Internet Fax desiderata.
- Mailbox — il file viene memorizzato su Fiery Server con il numero di codice di una mailbox. Per accedere al lavoro di scansione memorizzato, l'utente deve immettere il numero di mailbox corretto. Alcune versioni di Fiery Server richiedono anche una password. Il lavoro di scansione può essere recuperato da un URL.

7 Conclusione

EFI mette a disposizione dei clienti un'ampia gamma di funzioni e opzioni su Fiery Server, offrendo soluzioni complete e personalizzabili per la sicurezza di ogni ambiente. L'impegno di EFI è di garantire alle aziende sue clienti la massima efficienza operativa e di proteggere in modo efficace Fiery Server da qualsiasi vulnerabilità causata da uso non autorizzato o involontario. Per questo motivo, EFI sviluppa costantemente nuove tecnologie al fine di offrire soluzioni complete e affidabili per la sicurezza di Fiery Server.

TL035.07.18_IT