Fiery FS500 Pro/FS500 servers

Fiery Security White Paper

45234235

3 luglio 2022

Indice

Anteprima documento

Questo documento fornisce informazioni dettagliate sul modo in cui le tecnologie e le funzioni di sicurezza vengono implementate all'interno di Fiery FS500 Pro/FS500 servers, e comprende sicurezza hardware, sicurezza di rete, controllo degli accessi, sistemi operativi e sicurezza dei dati. Lo scopo del documento è di aiutare i nostri clienti a combinare la tecnologia di sicurezza della piattaforma Fiery con le proprie politiche per soddisfare i loro specifici requisiti di sicurezza.

Terminologia e convenzioni

Il presente documento utilizza la seguente terminologia per fare riferimento a Fiery FS500 Pro/FS500 servers, alle stampanti e alle applicazioni Fiery.

Termine o convenzione	**Si riferisce a**
Fiery server	Fiery FS500 Pro/FS500 servers
Stampante	Stampante, fotocopiatrice, sistema di stampa digitale, sistema di stampa o dispositivo di output
Configure	Fiery Configure
Command WorkStation	Fiery Command WorkStation
WebTools	Fiery WebTools
QuickTouch	Software Fiery QuickTouch in esecuzione sul pannello LCD del server Fiery

Filosofia EFI sulla sicurezza

EFI riconosce che la sicurezza è una delle principali preoccupazioni per le organizzazioni e le aziende in tutto il mondo. I nostri prodotti sono spesso migliorati con funzioni di sicurezza migliorate destinate a proteggere le vostre risorse aziendali. Fiery servers di EFI è progettato e fabbricato con la sicurezza come componente fondamentale per proteggere i dati di sistema in caso di inattività, nel transito e durante l'elaborazione.

Collaborando a stretto contatto con i nostri partner e fornitori globali EFI, ci impegniamo a supportare continuamente i nostri clienti con soluzioni mano a mano che si evolvono le minacce. Per ottenere la sicurezza complessiva del sistema, si consiglia agli utenti finali di combinare le funzioni di sicurezza Fiery con le politiche sulla sicurezza della propria organizzazione e le migliori prassi specifiche del settore, come le password protette e le procedure di sicurezza fisica più rigorose.

Obiettivi di sicurezza EFI

EFI ha stabilito i seguenti obiettivi quando si implementano le misure di sicurezza per Fiery server:

- **Sicurezza dei dati**: nessuna divulgazione non autorizzata dei dati durante l'elaborazione, la trasmissione (in transito) o l'archiviazione (in caso di inattività).
- **Disponibilità**: prestazioni come previsto, esenti da manipolazioni non autorizzate.
- **Controllo degli accessi**: nessuna negazione del servizio agli utenti autorizzati.
- **Manutenzione facile**: notifiche automatiche e download quando sono disponibili gli aggiornamenti di sicurezza.
- **Conformità**: supportare le normative di settore e framework di sicurezza.

Aggiornamenti della sicurezza software Fiery

La sezione fornisce una panoramica generale del processo di aggiornamento della sicurezza del software Fiery server. Le vulnerabilità di sicurezza del sistema operativo Microsoft® Windows™ non sono descritte in quanto vengono gestite direttamente da Microsoft e consegnate come aggiornamenti di Windows mano a mano che sono disponibili. Per problemi di sicurezza o vulnerabilità che potrebbero influire sui componenti hardware Fiery chiave, ad esempio scheda madre, processore, BIOS e così via, EFI collabora strettamente con i produttori per ottenere gli aggiornamenti di sicurezza necessari.

- EFI monitora il bollettino sulla cybersicurezza US-CERT settimanale emanato dalla CyberSecurity and Infrastructure Security Agency (CISA). Il bollettino fornisce un riepilogo delle nuove vulnerabilità registrate dal National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) nella scorsa settimana. Le vulnerabilità si basano sullo standard di denominazione delle vulnerabilità e delle esposizioni comuni (CVE) e sono organizzate in base alla gravità (alta, media e bassa) determinata dal Common Vulnerability Scoring System (CVSS).
- EFI fornisce patch relative alla sicurezza per ogni piattaforma Fiery server il prima possibile.
- Gli aggiornamenti per la sicurezza per il software Fiery vengono consegnati a specifici partner EFI per l'approvazione.
- Una volta approvati dai partner, gli aggiornamenti per la sicurezza per il software Fiery sono disponibili per il download.
- Fiery System Update scarica e installa gli aggiornamenti per la sicurezza se l'opzione è abilitata su Fiery server . Per impostazione predefinita, questa opzione è abilitata e si consiglia ai clienti di lasciarla abilitata.

Gli aggiornamenti software puntuali sono fondamentali per garantire il funzionamento ottimale di Fiery servers. L'installazione degli aggiornamenti per la sicurezza del software Fiery e del sistema operativo Windows è importante per garantire che Fiery servers sia protetto in ogni ambiente di stampa specificato.

Nota: Tutti gli aggiornamenti o le patch Fiery sono firmati digitalmente con SHA-2.

Configurazione delle funzioni di sicurezza di Fiery server

Configure è lo strumento principale utilizzato per configurare le funzioni di sicurezza su Fiery servers. Gli amministratori Fiery possono accedere a Configure da Command WorkStation o WebTools.

Nota: Gli utenti devono avere i privilegi di amministratore per accedere a Configure.

Per ulteriori informazioni sulla configurazione di Fiery server, vedere Linee guida per la configurazione di server Fiery protetti alla pagina 31.

Sicurezza dell'hardware

La sicurezza dell'hardware Fiery server si concentra sulla prevenzione della perdita di dati in caso di mancanza di alimentazione e accesso non autorizzato ai dati che si trovano su un dispositivo di archiviazione.

Memoria volatile

I dati scritti nella RAM volatile sono disponibili solo quando l'alimentazione è accesa. Quando l'alimentazione è spenta, tutti i dati vengono cancellati.

Per ulteriori informazioni, vedere la Sezione memoria non volatile della tabella alla pagina 24.

Memoria non volatile e Data Storage

Il Fiery server include diversi tipi di tecnologie di archiviazione non volatile che conservano i dati sul Fiery server quando viene spenta l'alimentazione. Questi dati sono le informazioni dei programmi del sistema e i dati utente.

Per ulteriori informazioni, vedere la Sezione memoria non volatile della tabella alla pagina 24.

Memoria flash

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

CMOS

La memoria CMOS alimentata a batteria memorizza le impostazioni macchina del Fiery server. Nessuna di queste informazioni è considerata confidenziale o privata. Se la memoria CMOS è installata, gli utenti possono accedere a queste impostazioni su un server Windows 10 IoT Enterprise 2016 o 2019 tramite il monitor, la tastiera e il mouse.

NVRAM

Sono presenti alcuni piccoli componenti NVRAM in Fiery server contenenti il firmware operativo. Tali componenti contengono dati operativi non specifici del cliente. L'utente non ha accesso a tali dati.

Hard disk drive (HDD) e unità di memoria a stato solido (SSD)

Durante le normali operazioni di stampa e scansione e durante la creazione delle informazioni per la gestione dei lavori, i dati immagine vengono scritti su un'area casuale dell'hard disk drive e dell'unità di memoria a stato solido.

I dati immagine e i lavori nelle code possono essere eliminati manualmente dagli utenti da Command WorkStation o da altre operazioni per le code (come l'operazione dal display LCD della stampante). I dati immagine e gli oggetti possono anche essere eliminati automaticamente con il comando **Ripristina server** oppure quando il numero di lavori stampati supera i parametri consentiti. La disabilitazione della coda di stampa eliminerà anche i lavori stampati.

Per proteggere i dati immagine dall'accesso non autorizzato, EFI offre la funzione Eliminazione sicura. Una volta che la funzione Eliminazione sicura viene abilitata dall'amministratore Fiery, l'operazione selezionata viene eseguita al momento indicato per eliminare in modo sicuro i dati sull'hard disk drive. La funzione Eliminazione sicura di Fiery supporta attualmente solo gli hard disk drive. Per le unità a stato solido SSD (Solid State Drives), verificare con il produttore le opzioni di sanficazione del disco prima di smaltire l'unità.

Nota: Per ulteriori informazioni sulla funzione Eliminazione sicura, vedere Eliminazione sicura alla pagina 23.

Porte fisiche

Il Fiery server può essere collegato tramite porte esterne visualizzate nella seguente tabella:

Porte Fiery	Funzione	Accesso	Controllo degli accessi
Connettore Ethernet RJ-45	Connettività Ethernet	Collegamenti di rete	Utilizza il filtraggio IP Fiery per il controllo degli accessi
Connettore di interfaccia della stampante	Stampa e scansione	Dedicato a invio/ricezione alla/dalla stampante	N/D
Porta USB	Collegamento dispositivo USB Installazione del software di sistema	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. L'archiviazione USB può anche essere disabilitata da Configure.
Connettore in fibra ottica	Connettività Ethernet 10G	Collegamenti di rete	N/D

Interfaccia locale

Su alcuni Fiery servers, l'utente può accedere alle funzioni di Fiery sul monitor di Fiery NX Station o tramite il software Fiery QuickTouch sullo schermo touchscreen, o tramite qualsiasi monitor collegato a Fiery server. L'accesso di sicurezza su Fiery server con Fiery NX Station è controllato tramite una password di amministratore di Windows. Il display touchscreen offre funzioni molto limitate che non rappresentano alcun rischio per la sicurezza.

Hard disk drive rimovibile - Opzionale

Alcuni Fiery servers sono compatibili con un kit hard disk drive 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 Fiery server.

Per server Windows autonomi

Fiery servers basato su Windows autonomo supporta un kit di opzioni con hard disk drive rimovibile. La disponibilità del kit per un prodotto Fiery specifico dipende dai termini dei contratti che EFI ha in essere con i singoli partner Fiery.

Per i server Fiery XB

Gli hard disk drive e le unità a stato solido sono rimovibili sui server Fiery XB. La maggior parte degli hard disk drive e delle unità a stato solido viene abbinata insieme in configurazione RAID. È importante rimettere le unità nella loro posizione originale per evitare la perdita di dati e una nuova installazione di software di sistema.

Abilita porte USB per l'archiviazione

Le porte USB su Fiery servers consentono il collegamento di mouse, tastiera o spettrofotometro, ma impediranno il collegamento ai dispositivi di archiviazione USB quando l'opzione Abilita archiviazione USB è disabilitata in Configure. Questa opzione è abilitata per impostazione predefinita. Se disabilitata, l'opzione disabilita le funzioni Fiery che prevedono la funzionalità di archiviazione di massa USB, ad esempio Backup e ripristino.

Sicurezza di rete

Il Fiery server comprende una serie di funzioni di sicurezza di rete progettate per controllare e gestire l'accesso alla stampante. Solo gli utenti e i gruppi autorizzati possono accedere a Fiery server e stampare sulla stampante. Il Fiery server può inoltre essere configurato per limitare o controllare le comunicazioni esterne utilizzando indirizzi IP designati e disabilitando le porte e i protocolli di rete. Fiery servers deve essere sempre usato in un ambiente di rete protetto e l'accessibilità deve essere configurata e gestita in modo corretto da un amministratore di rete qualificato e autorizzato.

Porte di rete

Per impostazione predefinita, tutte le porte TCP/IP non utilizzate dai servizi Fiery specifici sono disabilitate. L'amministratore Fiery può abilitare e disabilitare selettivamente le porte di rete. La disabilitazione di una porta di rete blocca i collegamenti che utilizzano la porta specificata. Se è abilitata una porta specifica, le connessioni esterne sono consentite tramite quella porta.

TCP	UDP	Nome porta	Servizi dipendenti
20-21		FTP	FTP
80		HTTP	WebTools, IPP
135		MS RPC	Microsoft® RPC Service (solo Windows 10). Si aprirà un'altra porta compresa tra 49152 e 65536 per fornire il servizio Point and Print SMB.
137-139		NETBIOS	Stampa Windows
	161, 162	SNMP	Fiery Central, alcuni programmi di utilità precedenti, altri strumenti basati su SNMP
	427	SLP	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 (come versioni precedenti di Command WorkStation)
631		IPP	IPP
3389		RDP	Desktop remoto (solo server Windows Fiery)

TCP	UDP	Nome porta	Servizi dipendenti
3702	3702	WS-Discovery	WSD
	4500	IPsec NAT	IPsec
	5353	Multicase DNS	Bonjour
6310 8010 8021-8022 8090 9906 21030 50006-50025	9906	Porte EFI	Command WorkStation 5 e 6, Fiery Central, strumenti SDK EFI, funzioni bidirezionali Fiery Printer Driver, WebTools, Stampa mobile diretta Fiery e conversione documenti nativi.
9100-9103		Porta di stampa	Porta 9100

Nota: Le porte 50006-50025 sono abilitate dopo che la versione 6.2 di Command WorkStation e versioni successive viene installata su un Fiery server autonomo.

Altre porte TCP, ad eccezione di quelle specificate dal Partner EFI Fiery, 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.

Filtraggio IP

Il filtraggio IP consente o nega le richieste di connessione a Fiery server da indirizzi IP predefiniti. L'amministratore può definire i criteri predefiniti per consentire o negare i pacchetti di dati in arrivo e può anche specificare i filtri per un massimo di 16 indirizzi IP o intervalli per consentire o negare le richieste di connessione.

Ogni impostazione del filtro IP specifica un indirizzo IP o un intervallo di indirizzi IP e l'azione corrispondente. Se l'azione è Nega, i pacchetti con un indirizzo di origine appartenenti agli indirizzi specificati verranno eliminati e, se l'azione è Accetta, i pacchetti saranno consentiti.

Autenticazione di rete

SNMP v3

Fiery server supporta l'ultima versione di SNMPv3. I pacchetti di comunicazione SNMPv3 possono essere crittografati per garantire la riservatezza, l'integrità e l'autenticazione dei messaggi.

L'amministratore Fiery può scegliere fra tre livelli di sicurezza SNMP: Minimo, Medio o Massimo. L'amministratore Fiery può anche richiedere l'autenticazione prima di consentire le transazioni SNMP e crittografare i nomi utente e le password SNMP. L'amministratore locale può definire i nomi delle comunità in scrittura e lettura SNMP e altre impostazioni di sicurezza.

Per ulteriori informazioni, vedere Impostazioni consigliate alla pagina 31.

IEEE 802.1 x

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

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

Il Fiery server richiede questa autenticazione all'avvio oppure quando il cavo Ethernet viene scollegato e ricollegato.

Crittografia di rete

Internet Protocol Security (IPsec)

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

Il 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 un Fiery server, tutte le comunicazioni, inclusi i lavori di stampa, vengono trasmesse sulla rete in tutta sicurezza.

HTTPS

Il Fiery server richiede un collegamento protetto tra i client e i diversi componenti server. HTTPS over TLS viene utilizzato per crittografare le comunicazioni tra i due punti finali. È necessario HTTPS quando ci si collega a Fiery server da WebTools e Fiery API. Queste comunicazioni sono crittografate con TLS 1.3 e 1.2.

Gestione certificati

Fiery servers fornisce un'interfaccia per gestire i certificati utilizzati durante le comunicazioni TLS. Fiery servers supporta il formato di certificato X.509.

Fiery servers supportare i certificati RSA con lunghezza chiave pari a 4096, 3072 e 2048 bit.

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'autorità di certificazione attendibile.

Nota: I certificati autofirmati non sono sicuri. È consigliabile che gli utenti utilizzino un certificato di un'Autorità di certificazione (CA) attendibile.

Una volta ottenuto un certificato firmato da un'Autorità di certificazione attendibile, è possibile caricarlo su Fiery server nella sezione Configure di WebTools.

Sicurezza e-mail

Il Fiery server supporta i protocolli di comunicazione e-mail POP e SMTP, quando l'e-mail è abilitata. (La funzione è disabilitata per impostazione predefinita). Per proteggere il servizio da attacchi e uso improprio, l'amministratore Fiery può abilitare altre funzioni di sicurezza.

POP prima di 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 deve abilitare l'autenticazione POP prima di SMTP.

OP25B

OP25B (Outbound Port 25 Blocking) è 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.

Per ulteriori informazioni sul flusso di lavoro di stampa via e-mail di Fiery server, vedere Stampa via e-mail alla pagina 26.

Server Message Block (SMB)

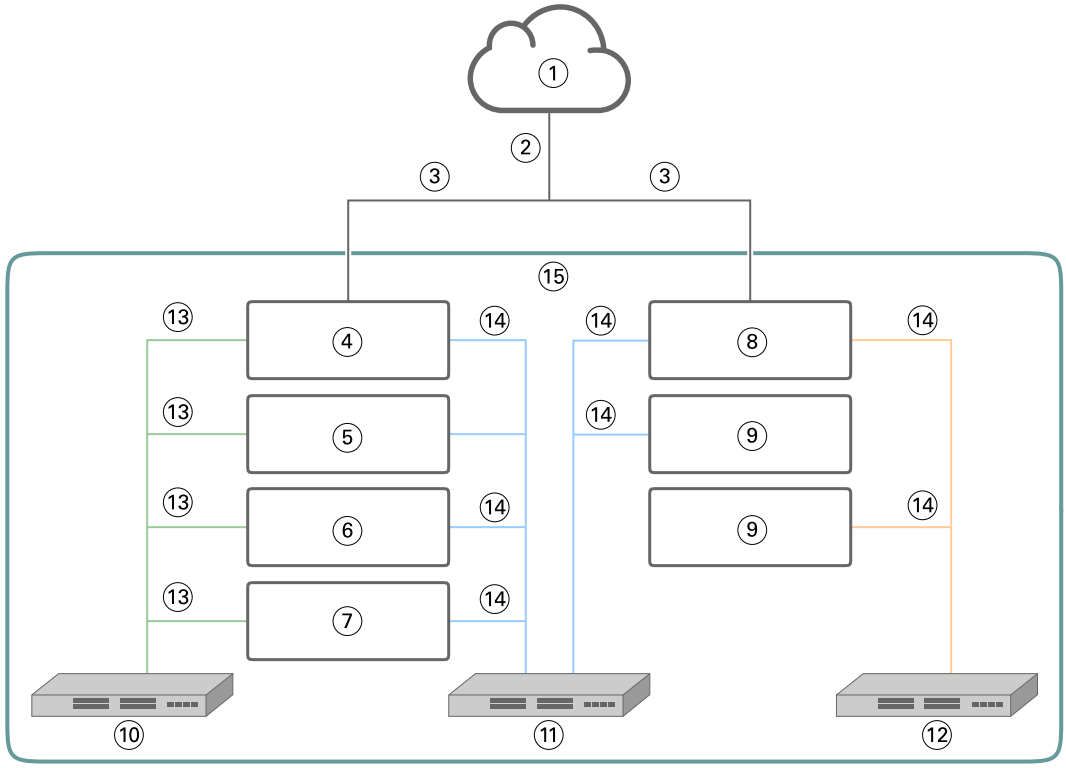
SMB è un protocollo di rete che fornisce l'accesso condiviso a file e stampanti. SMB v1 è disabilitato in Fiery servers in quanto non soddisfa gli standard di sicurezza del settore attuali. SMB v2 e v3 è ancora supportato.

La firma SMB viene applicata su Fiery server. La firma SMB richiede i pacchetti firmati digitalmente per consentire al destinatario di controllare l'autenticità del pacchetto per evitare attacchi "man in the middle". Se l'opzione di autenticazione SMB è abilitata, l'utente deve fornire il nome utente e la password SMB per accedere alle cartelle e ai contenuti SMB archiviati nelle cartelle SMB.

Nota: La stampa o la condivisione dei file tramite SMB possono essere limitate impostando una password in Configure.

Diagramma di rete Fiery XB

Il grafico seguente mostra come i server Fiery XB e le stampanti inkjet ad alta velocità si connettono alla rete.



1	LAN	9	Altre blade del sistema di stampa (opzionale)
2	Traffico di rete per la gestione dei lavori	10	Rete privata da 10 GbE
3	1 GbE DHCP o statico	11	Rete privata da 1 GbE
4	Blade principali Fiery	12	Rete privata da 1 GbE PLC
5	Blade Fiery RIP (facoltativo)	13	10 GbE
6	Blade Fiery #1 (facoltativo)	14	1 GbE
7	Blade Fiery #2 (facoltativo)	15	Ambiente Fiery XB chiuso
8	Blade del sistema di stampa		

Controllo degli accessi

Questo capitolo descrive come Fiery server può essere configurato per controllare l'accesso alle risorse per diversi gruppi di utenti.

Autenticazione utente

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

- Autenticare un utente
- Autorizzare azioni sulla base dei privilegi dell'utente

Il Fiery server può autenticare gli utenti che sono:

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

Il 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 bianco e nero, stampa a colori o in scala di grigi) e le azioni degli utenti appartenenti ai diversi gruppi sono limitate a tali privilegi. L'amministratore Fiery può modificare i privilegi di un qualsiasi gruppo Fiery, ad eccezione degli account Amministratore e Operatore.

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

- **Stampa in scala di grigi**: questo privilegio consente ai membri del gruppo di stampare i lavori in scala di grigi su Fiery server. Se l'utente non dispone di questo privilegio, il Fiery server non stamperà il lavoro. Se il lavoro è un lavoro a colori, verrà stampato in scala di grigi.
- **Stampa a colori e in scala di grigi**: 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 scala di grigi, 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. Il 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 modificare le stampanti virtuali.
- **Modifica dei lavori** (solo server Fiery XB): questo privilegio consente ai membri del gruppo di modificare un lavoro in coda.

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

Autenticazione utente software Fiery

Il Fiery server interagisce con diversi tipi di utenti. Sono utenti specifici del software Fiery e non hanno alcun legame con gli utenti o i ruoli definiti in Windows. Si consiglia agli amministratori Fiery di richiedere le password per accedere a Fiery server. Inoltre, EFI consiglia all'amministratore Fiery di modificare la password predefinita in modo da soddisfare i requisiti di sicurezza dell'ambiente di stampa dell'utente.

- La lunghezza massima della password sia per Amministratore sia per Operatore è di 15 caratteri quando si utilizza Configure > Security.
- La lunghezza massima della password per gli account degli utenti locali è di 64 caratteri quando si utilizza Configure > Account utente.
- Le password di amministratori e operatori possono anche essere modificate in Configure > Account utente, il numero massimo di caratteri consentiti è 64.

Di seguito sono descritti i privilegi consentiti ai diversi tipi di utente Fiery:

- **Amministratore**: ha il pieno controllo di tutte le funzionalità di Fiery server.

  L'amministratore Fiery può modificare i privilegi di un qualsiasi gruppo Fiery, ad eccezione degli account Amministratore e Operatore.
- **Operatore**: ha la maggior parte dei privilegi dell'amministratore, ma non ha accesso ad alcune funzioni del Fiery server, come la configurazione, e non può cancellare il job log.
- **Operatore del sistema di stampa** (solo server Fiery XB): è in grado di gestire i lavori sul sistema di stampa. L'amministratore può aggiungere privilegi specifici a questo tipo di utente.
- **Amministratore del servizio Fiery** (solo per Fiery servers su Windows): account admin nascosto utilizzato per installare il certificato attendibile sui server Windows. Questo account non consente agli utenti di accedere a Fiery server (locale o remoto). Questo account potrebbe apparire su alcuni strumenti di scansione di rete e può essere rimosso se necessario. È possibile utilizzare metodi standard alternativi per installare il certificato attendibile.

Log di verifica sicurezza Fiery

Per aiutare le organizzazioni a soddisfare i requisiti di conformità, gli amministratori Fiery possono raccogliere e analizzare gli eventi relativi alla sicurezza, che vengono salvati nel log di verifica sicurezza.

Il Log di verifica sicurezza è abilitato per impostazione predefinita.

Ogni evento di sicurezza è classificato come informazione, avviso o errore. Non vi sono avvisi o notifiche forniti all'amministratore, ma solo un log statico.

I log sono in un formato supportato dalle comuni soluzioni di raccolta e analisi dei log SIEM. Le informazioni sugli eventi acquisiti sono conformi alla pubblicazione speciale 800-53 dell'Istituto nazionale per gli standard e la tecnologia, *Recommended Security Controls for Federal Information Systems* (SP800-53).

L'amministratore Fiery può leggere gli eventi senza l'intervento di EFI. Gli eventi dei Fiery servers basati su Windows e Linux sono in formato JSON e possono essere elaborati da qualsiasi strumento di raccolta di log. Per i server Fiery basati su Windows, gli eventi possono essere visualizzati in Gestione eventi Windows. Gli amministratori di Fiery servers basati su Linux possono inoltrare i log a un sistema centrale di raccolta log (SysLog).

Gli eventi di sicurezza vengono mantenuti in base alla capacità di archiviazione su disco allocata. Quando la dimensione del log raggiunge il limite massimo di archiviazione (400 MB), gli eventi meno recenti vengono rimossi.

Sistemi operativi

EFI collabora strettamente con i produttori dei sistemi operativi usati in Fiery servers per ottenere gli aggiornamenti di sicurezza necessari per problemi di sicurezza o vulnerabilità che potrebbero influire sui componenti Fiery server chiave, ad esempio scheda madre, processore, BIOS e così via. Inoltre, gli aggiornamenti del software Fiery sono firmati digitalmente da EFI per evitare modifiche non autorizzate, incluso l'inserimento di malware.

Linux (FS500)

Fiery servers FS500 sono server basati su Linux progettati con un'architettura chiusa. La visibilità della rete limitata impedisce l'accesso non autorizzato.

Le caratteristiche di Fiery servers basato su Linux sono le seguenti:

- Fiery servers basato su Linux non comprende un'interfaccia locale che consente l'accesso al sistema operativo.
- SSH e Telnet non sono supportati su Fiery servers basato su Linux, che impedisce l'accesso alla shell del sistema operativo.
- Fiery servers basato su Linux non consente l'installazione di programmi non autorizzati che potrebbero rendere vulnerabile il sistema.
- Il sistema operativo Linux utilizzato su Fiery servers FS500 è un sistema operativo personalizzato solo per Fiery servers. Comprende tutti i componenti del sistema operativo richiesti da Fiery server, tranne alcuni dei componenti di uso generale e delle applicazioni per l'utente finale che si trovano nei sistemi Linux generici.

Accesso al sistema

Basato su Linux Fiery servers può essere configurato tramite la configurazione con Fiery dal pannello di controllo della stampante o tramite Configure in WebTools. WebTools è un set di pagine basate su browser che consente all'amministratore Fiery di accedere a Fiery server per la configurazione e altre attività correlate all'amministrazione del sistema. WebTools viene eseguito sull'ultimo Framework Web protetto, supportato dalla maggior parte dei browser Web più moderni.

Windows 10 (FS500 Pro)

Il sistema operativo di Fiery servers FS500 Pro è Windows 10 IoT Enterprise 2019 LTSC. Questa edizione di Windows include le più recenti funzioni di sicurezza e i miglioramenti cumulativi delle funzioni introdotti in Windows 10 versioni 1703, 1709, 1803 e 1809. Ogni build LTSC è supportata da Microsoft con gli aggiornamenti per la sicurezza per dieci anni dopo il rilascio.

Nota: Windows 10 IoT Enterprise 2019 LTSC è un equivalente binario di Windows 10 Enterprise versione 1809.

Windows 10 IoT Enterprise 2019 LTSC include le seguenti caratteristiche:

- Destinato all'utilizzo su sistemi specializzati come Fiery servers.
- Include numerosi miglioramenti a livello di sicurezza per la protezione dell'identità, delle informazioni e contro possibili minacce.
- Fornisce numerosi aggiornamenti per la sicurezza.
- Non include le applicazioni orientate al consumatore, come il calendario, il meteo, le foto e altri.

Microsoft Windows Update

Microsoft rilascia regolarmente delle patch sulla sicurezza tramite Windows Update per risolvere le potenziali minacce e vulnerabilità relative alla sicurezza del sistema operativo. L'impostazione predefinita di Windows Update su Fiery servers è di notificare agli utenti la disponibilità di patch senza però scaricarle. Se si seleziona Verifica disponibilità aggiornamenti in Windows Update nel Pannello di controllo di Windows, si attiva l'opzione aggiornamenti automatici e si avvia il processo di aggiornamento.

Strumenti di aggiornamento Windows

Il Fiery servers basato su Windows utilizza metodi standard Microsoft per aggiornare tutte le patch di sicurezza Microsoft applicabili. Il Fiery server non supporta altri strumenti di aggiornamento di terze parti per il recupero delle patch di sicurezza.

Software antivirus Windows

Fiery servers utilizza il software antivirus Microsoft e Windows 10 Defender per la protezione. In generale, un software antivirus di terze parti 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.

Occorre notare che per massimizzarne l'efficienza, il software antivirus deve essere installato, configurato ed eseguito direttamente sul Fiery server stesso. Per Fiery servers senza configurazione locale, è comunque possibile avviare un software antivirus su un PC remoto ed eseguire la scansione dell'hard disk drive condiviso di Fiery server. EFI consiglia comunque all'amministratore Fiery di tenersi in contatto diretto con il produttore del software antivirus per ogni necessità di supporto operativo.

Scansione antivirus

Una scansione antivirus di Fiery server potrebbe influire sulle prestazioni di Fiery, anche se la scansione è stata pianificata.

Antispyware

Un programma antispyware potrebbe incidere sulle prestazioni quando Fiery server riceve i file. Un esempio possono essere i lavori di stampa in arrivo, i file scaricati durante un aggiornamento di sistema Fiery server o un aggiornamento automatico di applicazioni in esecuzione su Fiery server.

Firewall incorporato

Dal momento che Fiery server ha un firewall, in genere non sono necessari firewall antivirus. EFI consiglia ai clienti di collaborare con la loro divisione IT aziendale in caso abbiano necessità di installare e di eseguire un firewall incorporato incluso nel software antivirus. Vedere Porte di rete alla pagina 11 per un elenco delle porte disponibili.

Anti-spam
Il Fiery server supporta le funzioni di stampa tramite e-mail e di scansione via e-mail. Si consiglia di utilizzare un meccanismo di filtraggio antispam basato sul server. Fiery servers può anche essere configurato per stampare i documenti da indirizzi e-mail specificati. Il componente antispam non è necessario, perché non è supportato il funzionamento di un client e-mail separato (come Outlook) su Fiery server.

HIPS e controllo applicativo
Data la natura complessa dei parametri Host Intrusion Protection System (HIPS) 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, HIPS e controllo applicativo sono eccellenti misure di sicurezza e coesistono con Fiery server. Tuttavia, è molto facile che insorgano problemi su Fiery server con impostazioni non corrette del parametro HIPS ed esclusioni file errate, spesso per "accettazione dei valori predefiniti". Si consiglia pertanto di rivedere le opzioni selezionate nelle impostazioni HIPS 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.

Safelist e blocklist
Le funzionalità di safelist e blocklist non presentano in linea di massima controindicazioni per Fiery server. EFI consiglia fortemente al cliente di configurare questa funzionalità in modo che i moduli Fiery non siano bloccati.

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. Il Fiery server ignora anche messaggi e-mail in RTF o HTML ed eventuali componenti JavaScript 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.

Nota: Per ulteriori informazioni sul flusso di lavoro di stampa via e-mail di Fiery server, vedere Stampa via e-mail alla pagina 26.

Sicurezza dei dati

Questa sezione descrive i controlli di sicurezza progettati per proteggere i dati utente all'interno di Fiery server e i controlli di sicurezza per i dati in transito.

Crittografia di informazioni critiche

La crittografia di informazioni critiche su Fiery server garantisce la protezione di tutte le password e le relative informazioni di configurazione memorizzate su Fiery server. Le informazioni critiche sono crittografate o protette da hash. Gli algoritmi crittografici utilizzati sono AES256, Diffie-Hellman e SHA-2 per garantire la conformità con gli standard di sicurezza più recenti.

Anche se il disco viene rimosso dal Fiery server, è impossibile leggere le informazioni dell'utente memorizzate sul disco. La crittografia dei dati utente può essere abilitata o disabilitata Fiery servers con Windows attraverso Configure . Nel caso di Fiery servers con Linux, la funzione è sempre abilitata.

Se la passphrase immessa per il recupero dei dati viene dimenticata, non è possibile ripristinarla e EFI non può recuperarla. Il software deve essere reinstallato.

Nota: Con la crittografia dei dati, il disco viene partizionato e solo la partizione dei dati utente è crittografata. Le partizioni del sistema operativo non possono essere crittografate.

AES (Advanced Encryption Standard)

Il Fiery server protegge i dati inattivi da accessi non autorizzati. Crittografa i lavori, le immagini e i dati dei clienti con l'algoritmo AES a 256 bit.

L'AES è uno standard di cifratura di piccole dimensioni, rapido e difficile da decifrare, adatto per una vasta gamma di dispositivi e applicazioni. Offre un ulteriore livello di protezione contro il furto dei dati nel rispetto delle politiche di sicurezza aziendali.

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.

Code di attesa, stampa e stampa sequenziale

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

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.

Coda di stampa

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

Coda diretta (collegamento diretto)

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

EFI sconsiglia di stampare sulla coda diretta. Il Fiery server 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 (Variable Data Printing), 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.

Eliminazione dei lavori

Un lavoro non può essere visualizzato o recuperato quando viene eliminato automaticamente da Fiery server o cancellato con gli strumenti Fiery. Se il lavoro è stato inviato in spool sull'hard disk drive di Fiery server, gli elementi del lavoro potrebbero rimanere sull'hard disk drive ed essere in teoria recuperati con alcuni strumenti, come quelli di analisi del disco.

Eliminazione sicura

Eliminazione sicura è progettata per consentire di rimuovere i contenuti di un lavoro inoltrato dall'hard disk drive di Fiery server non appena una funzione Fiery viene eliminata. Quando si seleziona un lavoro, ogni file di origine del lavoro viene sovrascritto tre volte utilizzando un algoritmo basato sul metodo di bonifica dei dati 5220.22-M US DoD.

Flussi di lavoro	Eliminazione sicura
I lavori memorizzati sull'unità di disco fisso Fiery server; Eliminazione sicura impostata su On	Sì

Flussi di lavoro	Eliminazione sicura
I lavori memorizzati sull'unità di disco fisso Fiery server; Eliminazione sicura impostata su Off	No
Lavori ricevuti da Fiery server ed eliminati dopo Eliminazione sicura impostata su On	Sì
Lavori ricevuti da Fiery server ed eliminati prima di Eliminazione sicura impostata su On	No
Copie di lavori inviati a un altro Fiery server (“bilanciamento del carico”)	No
Lavori archiviati su un supporto rimovibile	No
Lavori archiviati su unità di rete	No
Lavori che si trovano su dispositivi client	No
Esecuzione di Ripristino server	Sì
Pagine unite o copiate in un altro lavoro (ad esempio, lavori Fiery Impose o PDF combinati)	No
Lavori ricevuti dal collegamento SMB e salvati sull'hard disk drive di Fiery server	No
Porzioni di un lavoro scritte sull'hard disk drive di Fiery server durante la sostituzione del disco o le operazioni di memorizzazione nella cache sul disco	No
Voci del job log	No
Voci del job log dopo l'esecuzione di Ripristina server	Sì
Fiery server spento prima che venga completata l'eliminazione del lavoro	No
Deframmentazione dell'hard disk drive di Fiery server prima di eliminare un lavoro	No

Nota: La funzione Eliminazione sicura non è supportata sulle piattaforme Fiery XB o su Fiery servers con SSD.

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'hard disk drive e non essere quindi specificatamente sovrascritta.

Memoria volatile			
Tipo (SRAM, DRAM e così via)	**Modificabile dall'utente (Sì o No)**	**Funzione o utilizzo**	**Processo di sanificazione**
DRAM	Sì	Memoria di sistema principale (riceve i lavori inviati alla coda diretta)	Spento Fiery server
SDRAM (sulla scheda video)	Sì	Memoria video	Spento Fiery server

Memoria non volatile			
Tipo (SRAM, DRAM e così via)	**Modificabile dall'utente (Sì o No)**	**Funzione o utilizzo**	**Processo di sanificazione**
BIOS	No	Funzioni BIOS	Rimuovere dalla presa e distruggere, ma il sistema cesserà di funzionare.
EPROM Ethernet	No	Firmware del chip Ethernet	Dissaldare e distruggere, ma il sistema cesserà di funzionare.
NVRAM CMOS	No	Memoria impostazioni BIOS	Rimuovere la batteria di sistema per 30 secondi.
Hard disk drive (HDD) o unità di memoria a stato solido (SSD)	Sì	Sistema operativo Applicazioni Fiery (possibilmente con dati utente) Software del sistema Fiery Lavori di stampa, lavori di scansione e altri dati utente Immagine di backup per impostazioni predefinite	Reinstallare il software di sistema. La maggior parte dei lavori può essere rimossa in modo sicuro con la funzione Eliminazione sicura *. Gli strumenti di sanificazione di terze parti e partner EFI Fiery possono essere utilizzati per completare la cancellazione dei dati su questi dispositivi.
Nota: La memoria volatile e la RAM potrebbero contenere i dati del cliente durante l'elaborazione dei dati dei clienti. Nessun dato cliente viene memorizzato nella memoria non volatile come BIOS, CMOS e NVRAM. *Le unità a stato solido non possono essere completamente sanificate tramite i metodi di sovrascrittura Eliminazione sicura multi-pass a causa della mappatura della memoria che si verifica. Inoltre, i tentativi di eseguire questa operazione eroderebbero anche notevolmente la durata di vita operativa dell'unità a stato solido. Tale funzione non è supportata dalle piattaforme Fiery XB.			

Stampa protetta

La funzione Stampa protetta richiede all'utente di inserire una password specifica su Fiery server e sulla stampante per poter stampare il lavoro.

Questa funzione richiede l'accesso al pannello di controllo della stampante. Lo scopo della funzione è quello di limitare l'accesso a un documento a un utente che ha la password per il lavoro e può inserirla localmente dal pannello di controllo della stampante.

Flusso di lavoro Stampa protetta

L'utente inserisce una password nel campo Stampa sicura 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 possono essere visualizzati in Command WorkStation.

Dal pannello di controllo della stampante, l'utente accede a una finestra di stampa protetta e immette una password. L'utente può quindi localizzare i lavori inviati con quella password e stamparli e/o eliminarli.

Il lavoro protetto stampato non viene spostato nella coda di stampa e viene eliminato automaticamente dopo la stampa.

Nota: Alcune porzioni di dati potrebbero essere temporaneamente presenti nei file del sistema operativo.

Stampa via e-mail

Il 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. La funzione stampa via e-mail è disattivata per impostazione predefinita. L'amministratore può attivare e disattivare la funzione di stampa via e-mail.

Gestione dei lavori

L'esecuzione di azioni sui lavori inoltrati al Fiery server richiede il programma di utilità per la gestione dei lavori Fiery con l'accesso dell'amministratore o dell'operatore.

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, l'ora in cui è stato eseguito il lavoro 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 Command WorkStation. Un utente che accede come amministratore può eliminare il job log da Command WorkStation.

Impostazioni

Per accedere alla configurazione, è necessario immettere la password di amministratore. Il Fiery server può essere configurato dallo strumento Configure in WebTools o Command WorkStation, o dalla funzione Configurazione del pannello di controllo della stampante.

Scansione

Il Fiery server consente che un'immagine posizionata sul vetro della stampante venga acquisita dalla stazione di lavoro che ha avviato la scansione. 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.

Invio dei lavori scansionati

I lavori scansionati possono essere inviati tramite diversi metodi.

E-mail

Un messaggio e-mail con un allegato del lavoro scansionato viene inviato a un server di posta, dove viene indirizzato alla destinazione desiderata.

Nota: Se la dimensione del file del lavoro scansionato supera il limite massimo definito dall'amministratore, il lavoro viene memorizzato sull'hard disk drive di Fiery server, accessibile da un URL.

FTP

Il file viene inviato a una destinazione FTP. Nel log FTP, accessibile tramite il comando Stampa pagine del pannello di controllo della stampante, 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 server

Il file viene inviato alla coda di attesa di Fiery server e non viene conservato come lavoro scansionato.

Per ulteriori informazioni sulla coda di attesa di Fiery server, vedere Code di attesa, stampa e stampa sequenziale alla pagina 23.

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. Gli utenti devono immettere il numero di mailbox corretto per accedere al lavoro di scansione memorizzato. Gli utenti hanno la possibilità di impostare le password per proteggere il contenuto delle proprie mailbox di scansione da accessi non autorizzati. Il lavoro scansionato può essere recuperato da un URL.

Conformità alle normative e ai quadri normativi

La tabella seguente contiene la conformità alle normative e ai quadri normativi per i server Fiery che eseguono il software di sistema FS500 Pro/FS500.

Normative/Quadri normativi	**Ambito**	**Serie NX (FS500 Pro)**	**Serie A/E (FS500)**
FIPS 140-2	• Governo degli Stati Uniti (federale e statale) • Requisiti di sicurezza per i moduli di crittografia	Conforme Windows 10 2019 LTSC Certificati FIPS: • N. 3197 • N. 3196 • N. 3092	Non conforme
Benchmark AIS	• Globale • Governo/Settore privato • Linee di base di configurazione e procedure consigliate per configurare un sistema in modo sicuro	Conforme Benchmark di Microsoft Windows 10 Enterprise (versione 1809)	N/D*
Guida all'implementazione tecnica della sicurezza (STIG)	• Standard di configurazione del governo degli Stati Uniti (federale e statale) che consiste nei requisiti di sicurezza informatica per un prodotto specifico	Conformità parziale Windows 10 STIG versione 2, R3 Eccezioni: CCI-000366: modulo per una piattaforma fidata (TPM) non disponibile	N/D*

Normative/Quadri normativi	Ambito	Serie NX (FS500 Pro)	Serie A/E (FS500)
International Standards Organization/IEC-15408	• Globale • Criteri comuni • Criteri di valutazione delle tecniche di sicurezza delle tecnologie dell'informazione per la sicurezza IT	Conformità parziale • Autenticazione LDAP/AD richiesta per il controllo degli accessi • TPM e Avvio protetto non supportati	Non conforme
IEEE 2600.2-2009	• Globale • Governo/Settore privato • Profilo dei criteri comuni per le periferiche di copia cartacea Ambiente B	Conformità parziale • TPM e Avvio protetto non supportati • I requisiti di resistenza e rilevamento richiedono un kit di sicurezza per unità disco Fiery opzionale	Non conforme
Safeguard Computer Security Evaluation Matrix (SCSEM)	• Governo degli Stati Uniti (federale e statale) • Linee guida sulla sicurezza delle informazioni fiscali per le agenzie federali, statali e locali	Conformità parziale • TPM e Avvio protetto non supportati • I requisiti di resistenza e rilevamento richiedono un kit di sicurezza per unità disco Fiery opzionale	Non conforme
DoD 522.22-M	Standard di sanificazione dei dati. 3 passate	Conforme	Conforme
NIST 800-88	Standard di sanificazione dei dati. 1 passata	Non conforme	Non conforme
Certificazione del quadro di gestione del rischio dell'esercito	• Governo degli Stati Uniti • Quadro di gestione del rischio per la tecnologia dell'informazione dell'esercito	Conformità parziale • TPM e Avvio protetto non supportati	Conformità parziale • TPM e Avvio protetto non supportati

*Non rientra nell'ambito di applicazione della normativa o del quadro normativo. I server della serie A e della serie E basati su Linux sono sistemi chiusi, senza accesso diretto al file system. La visibilità della rete limitata impedisce l'accesso non autorizzato.

Conformità FIPS 140-2

Se configurati correttamente, i server Fiery eseguono FS500 Pro su Windows 10 2019 LTSC sono conformi alle linee guida per la crittografia dei dati FIPS 140-2. Un server Fiery in *Modo FIPS 140-2* utilizza solo gli algoritmi crittografici convalidati e certificati ai sensi del Cryptographic Algorithm Validation Program (CAVP) del governo federale degli Stati Uniti per crittografare i dati a riposo e in movimento.

L'abilitazione di *Modo FIPS 140-2* in Fiery richiede il rispetto di un processo di configurazione avanzata per la protezione del server.

Linee guida per la configurazione di server Fiery protetti

Le seguenti linee guida possono aiutare gli amministratori Fiery a migliorare la sicurezza durante la configurazione di Fiery server.

Modifica della password dell'amministratore

Si consiglia di modificare la password predefinita dell'amministratore Fiery al momento dell'installazione e, a intervalli regolari, come richiesto dalle politiche sulla sicurezza dell'azienda. La password predefinita dell'amministratore deve essere modificata in Configurazione Fiery guidata durante la configurazione iniziale. Le password di Amministratore e Operatore possono essere modificate dopo la prima configurazione in WebTools: Configure > Sicurezza > Password Amministratore (oppure Operatore, rispettivamente). La configurazione della password è disponibile anche dagli Account utente.

La password dell'amministratore offre un accesso totale a Fiery server in locale e/o da un client remoto. L'accesso completo include, ma non è limitato a:

- File System
- Politica sulla sicurezza del sistema
- Voci di registro
- Password dell'amministratore, che nega agli utenti anonimi l'accesso aFiery server

Impostazioni consigliate

- Selezionare il livello di sicurezza Massimo per SNMP in Rete > SNMP:

  La scelta della sicurezza massima limita il supporto su Fiery server solo per SNMP v3.

  Se l'SNMP manager funziona solo con SNMP v1/v2c, modificare il valore del campo Lettura nome comunità. Il Fiery server consente di modificare i valori dei campi Lettura nome comunità e Scrittura nome comunità dell'SNMP da WebTools (Configure > Rete > SNMP) e dal pannello di controllo della stampante (Rete > SNMP).
- Disabilitare WSD in inoltro dei lavori.
- Disabilitare la stampa in Windows in inoltro dei lavori se si utilizza LPR, porta 9100 o IPP per la stampa.
- Bloccare le porte attivando il filtro della porta TCP/IP in Sicurezza > TCP/IP Filtraggio porta.

  Deselezionare le porte 137-139 e 445 se non si usa la stampa in Windows e non è necessario accedere alle cartelle dei file o condividerle. Disabilitare le comunicazioni porta 80 (HTTP) non protette.

Oltre alle protezioni a livello di sistema operativo, Fiery server dispone delle seguenti funzioni di sicurezza aggiuntive per proteggere i dati:

- Fiery servers dispone di una stampa protetta per assicurarsi che l'utente prelevi solo il suo lavoro di stampa.
- Fiery servers si integra con le principali soluzioni di account lavori per includere una maggiore sicurezza tramite la stampa follow-me.

Fiery servers dispone di numerose funzioni di sicurezza, ma non sono server connessi a Internet. Deve essere installato in un ambiente protetto e l'accessibilità deve essere configurata adeguatamente dall'amministratore di rete.

Selezionare un profilo di sicurezza Elevato

Il Fiery server offre consigli sulla sicurezza predefiniti basati su diversi livelli di rischi e minacce (Standard, Elevato, Corrente). Questa funzione è denominata Profili di sicurezza ed è accessibile dalle seguenti sezioni:

- Procedura guidata software Fiery
- WebTools > Configure > Sicurezza

Il profilo di sicurezza Elevato consente a Fiery server di fornire ancora più sicurezza e di abilitare le funzioni di sicurezza più comunemente usate.

Opzione	Elevato
Filtro porta TCP/IP	Abilitato
SLP (Service Location Protocol)	Disabilitato
Bonjour	Disabilitato
Eliminazione sicura	Abilitata
Desktop remoto	Disabilitato
Password SMB	Abilitata
Dispositivi di memoria USB	Disabilitato
Sicurezza PostScript	Abilitata
Porta 9100	Disabilitato
LPD	Abilitata
Stampa Windows	Disabilitato
IPP	Abilitato
Web Services for Devices (WSD)	Disabilitato
Stampa tramite e-mail	Disabilitato
Stampa FTP	Disabilitato
Stampa mobile diretta	Disabilitato

EFI consiglia di utilizzare il profilo di sicurezza Elevato per gli ambienti con i requisiti di sicurezza massimi.

Conclusioni

EFI mette a disposizione dei clienti una solida serie di funzioni standard e di sicurezza opzionali su Fiery server, offrendo soluzioni complete e personalizzabili per la sicurezza di ogni ambiente. EFI si impegna a garantire che Fiery server sia efficacemente protetto da una vulnerabilità a un uso dannoso o involontario, in modo che i nostri clienti possano gestire le proprie aziende con la massima efficienza.