Fiery FS700 Pro/FS700 servers

Security White Paper

45266127

8 dicembre 2025

Indice

Introduzione 5

Principi di sicurezza 6

Autenticazione e controllo degli accessi 7
Autenticazione utente 7
Privilegi del gruppo 7
Utenti locali 8
Privilegi di accesso e account utente Fiery locali: 8
Autenticazione LDAP 8
Single Sign-On (SSO) 9

Misure di sicurezza dei dati 10
Archiviazione crittografata: protegge i lavori di stampa e i dati di configurazione 10
Eliminazione sicura: garantisce che i dati siano irrecuperabili dopo l'eliminazione 10

Sicurezza di rete 12
Protocolli di rete supportati 12
Porte di rete 12
Porte in entrata 12
Porte in uscita 14
Comunicazione con i servizi cloud 14
Filtraggio IP 15
Autenticazione di rete 15
SNMP v3 16
IEEE 802.1x 16
Crittografia di rete 16
Internet Protocol Security (IPsec) 16
HTTPS 16
Gestione certificati 17
Server Message Block (SMB) 17

Sicurezza dell'hardware 18
Memoria volatile (RAM) 18
Memoria non volatile e Data Storage 18
Memoria flash 18

CMOS eNVRAM 18
Unità di archiviazione 19
Porte fisiche 19

Integrità del sistema e aggiornamenti sicuri 20
Log di verifica sicurezza 20
Avvio protetto 20
aggiornamenti con firma digitale 20
Gestione automatizzata degli aggiornamenti di sicurezza 21

Aggiornamenti della sicurezza software del sever Fiery 22

Conformità e procedure consigliate 23

Linee guida per la configurazione di server Fiery protetti 24
Modifica della password dell'amministratore 24
Procedura consigliata per operazioni sicure ed efficienti 24
Ambienti ad alta sicurezza 24

Conclusioni 25

Novità in FS700, FS700 Pro 26

Introduzione

Questo documento fornisce una panoramica delle funzioni di sicurezza nei server Fiery. Ha lo scopo di informare gli amministratori IT e i professionisti della sicurezza su come le soluzioni Fiery proteggono gli ambienti di stampa protetta. Il documento illustra i principi e i meccanismi utilizzati nei server Fiery per proteggere i dati, migliorare la sicurezza della rete e mantenere l'integrità del sistema.

Principi di sicurezza

Fiery servers sono meticolosamente progettati per aderire alle procedure consigliate del settore, garantendo la conformità alle normative sulla protezione dei dati e ai requisiti di sicurezza aziendale. I principi fondamentali alla base di questa progettazione sono i seguenti:

- Protezione dei dati: crittografia dei dati inattivi e dei dati in transito
- Sicurezza di rete: accesso controllato, protocolli di comunicazione sicuri e meccanismi di autenticazione
- Integrità del sistema: verifica del firmware, avvio protetto e aggiornamenti di sicurezza

In collaborazione con i nostri partner e fornitori globali, forniamo un supporto continuo ai nostri clienti man mano che si evolvono le minacce. Per garantire una sicurezza completa del sistema, si consiglia agli utenti finali di integrare le funzioni di sicurezza Fiery con le politiche sulla sicurezza della propria organizzazione e di attenersi alle procedure consigliate specifiche del settore, tra cui l'implementazione di password protette e solide misure di sicurezza fisica.

Autenticazione e controllo degli accessi

I server Fiery supportano più metodi di autenticazione, tra cui:

- Controllo degli accessi in base al ruolo (RBAC)
- Integrazione LDAP/Active Directory
- Autenticazione a più fattori (MFA) con il Single Sign-on (SSO)

Autenticazione utente

La funzione di autenticazione consente al server Fiery di eseguire le seguenti funzioni:

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

Il Fiery server supporta i seguenti metodi di autenticazione:

- Autenticazione locale per gli utenti definiti sul server Fiery
- Autenticazione a un fattore singolo (SFA) tramite server di autenticazione di rete esterni che utilizzano LDAP (ad es. Microsoft Active Directory)
- Autenticazione a più fattori (MFA) con il Single Sign-on (SSO)

A prescindere dal metodo utilizzato, l'autenticazione per gli account amministratore è sempre necessaria. Non è possibile disabilitare questa modalità.

Privilegi del gruppo

Il server Fiery autorizza le azioni degli utenti in base alla loro appartenenza al gruppo. A ciascun gruppo è associata una serie specifica di privilegi, come ad esempio la stampa a colori o in scala di grigi. Le azioni dei membri del gruppo sono limitate a questi privilegi. L'amministratore Fiery ha l'autorità di modificare i privilegi di un qualsiasi gruppo Fiery, ad eccezione degli account Amministratore e Operatore.

In questo metodo di autenticazione utente, i diversi livelli di privilegi che si possono selezionare 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. Se l'utente non dispone di questo privilegio, il server Fiery non stampa il lavoro. Se il lavoro è un lavoro a colori, verrà stampato in scala di grigi.
- Stampa a colori e in scala di grigi: consente ai membri del gruppo di stampare lavori con accesso totale alle funzionalità di stampa a colori e in scala di grigi del server Fiery. 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).

- Mailbox Fiery: 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 nome utente/password mailbox.
- Calibrazione: questo privilegio consente ai membri del gruppo di eseguire la calibrazione del colore.
- Creare preimpostazioni server: consente ai membri del gruppo di creare preimpostazioni server. I membri del gruppo hanno accesso a queste preimpostazioni server.
- 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.

Gli amministratori con privilegi elevati possono personalizzare queste funzionalità per limitare l'accesso non autorizzato e applicare i protocolli di sicurezza dell'organizzazione.

Utenti locali

Il software del server Fiery interagisce con tipi di utenti univoci, distinti dagli utenti o dai ruoli di Windows. Gli amministratori Fiery devono modificare tempestivamente tutte le password predefinite dopo l'installazione iniziale. L'accesso al server Fiery con password deve essere applicato rigorosamente.

- La lunghezza massima della password per "Amministratore" e "Operatore" è di 64 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 **Configura** > **Account utente**.

Privilegi di accesso e account utente Fiery locali:

- Amministratore: pieno controllo della funzionalità del server Fiery, può modificare i privilegi di gruppo Fiery, ad eccezione degli account Amministratore e Operatore.
- Operatore: ha gli stessi privilegi dell'amministratore, ma non ha accesso alla configurazione del server e all'eliminazione del job log.
- Operatore del sistema di stampa (solo server Fiery XB): gestisce i lavori sul sistema di stampa, con privilegi specifici aggiunti dall'amministratore.
- Amministratore del servizio Fiery (solo server Windows): un account admin nascosto per l'installazione del certificato attendibile, non può accedere al server Fiery, appare sugli strumenti di scansione della rete e può essere rimosso.
- Fiery_SMB_User: account di stampa Windows (SMB) predefinito che fornisce visibilità sulle code di stampa del server Fiery tramite la rete vicina.
- Ospite (predefinito; nessuna password): la maggior parte dei privilegi dell'operatore, ma non può accedere al job log, apportare modifiche e cambiare lo stato dei lavori di stampa o visualizzare in anteprima i lavori.

Autenticazione LDAP

Il server Fiery utilizza LDAP versione 3 (conforme alla RFC 2251) per comunicare con i server aziendali. Tramite LDAPv3, recupera gli indirizzi e-mail degli utenti per le funzioni di scansione e le informazioni sugli utenti e sui gruppi per l'autenticazione. Questa funzionalità è supportata esclusivamente per i collegamenti LDAP con i server Microsoft Active Directory.

il server Fiery supporta i seguenti metodi di autenticazione utilizzando PDAP:

- Automatico
- SIMPLE
- GSSAPI

La seguente tabella descrive i diversi metodi di autenticazione LDAP:

Metodo di autenticazione	**Descrizione**	**Server Active Directory**
Automatico	Questa opzione consente di selezionare GSSAPI o SIMPLE in base al metodo di autenticazione supportato dal server LDAP.	Supportato
SIMPLE	La password è obbligatoria. Se si seleziona LDAP su TLS, la password viene crittografata utilizzando TLS.	Supportato
GSSAPI	Questo metodo utilizza i ticket Kerberos al posto delle password, eliminando la necessità di TLS.	Supportato

Single Sign-On (SSO)

I server Fiery FS700 Pro supportano il protocollo OpenID Connect per l'autenticazione utente Single Sign-On (SSO) basata su cloud con ID Microsoft Entra (in precedenza denominato Azure AD). Gli utenti possono accedere a un Fiery server utilizzando le credenziali Entra ID.

Questo metodo di autenticazione supporta l'autenticazione a più fattori (MFA).

Questo approccio alla gestione dell'identità garantisce che i server Fiery non memorizzino mai le password utente in locale, migliorando notevolmente la sicurezza.

Misure di sicurezza dei dati

Per proteggere le informazioni riservate, i server Fiery implementano:

Archiviazione crittografata: protegge i lavori di stampa e i dati di configurazione

La crittografia di informazioni critiche dei clienti garantisce l'archiviazione sicura delle password e le relative informazioni di configurazione sul server Fiery. Queste informazioni critiche vengono crittografate o sottoposte a hashing utilizzando algoritmi crittografici come AES-256 e SHA-2, che aderiscono ai più recenti standard di sicurezza.

Anche se il disco viene rimosso dal server Fiery, i dati del cliente memorizzati sul disco rimangono inaccessibili. La crittografia dei dati utente può essere abilitata o disabilitata sui server Fiery con Windows. Nel caso dei server Fiery con Linux, la funzione della crittografica è sempre abilitata.

Se si dimentica una passphrase utilizzata per il recupero dei dati, FIERY non può ripristinarla, rendendo necessaria una reinstallazione completa del software.

I server basati su Windows offrono anche un'opzione per crittografare l'unità di avvio, che contiene il sistema operativo. Questa crittografia aiuta a prevenire attacchi offline al server Fiery e garantisce che l'unità di avvio non possa essere utilizzata su un altro dispositivo.

Eliminazione sicura: garantisce che i dati siano irrecuperabili dopo l'eliminazione

Per i Fiery server basati su Linux FS700, quando si elimina 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.

Questa funzione non è supportata sui server Fiery integrati che utilizzano le piattaforme hardware E600 e LX Pro. Queste piattaforme memorizzano i dati dei documenti su un'unità a stato solido (SSD), protetta con crittografia AES-256. Questa crittografia è sempre abilitata e non può essere disabilitata.

I server FS700 Pro basati su Windows supportano lo standard di sanificazione dei dati NIST 800-88. Gli amministratori Fiery possono configurare questa opzione per i metodi di sovrascrittura dell'immagine a 1 o 3 passate.

Nota: La funzione Eliminazione sicura non è supportata sulle piattaforme Fiery XB o per gli utenti con dati archiviati su SSD.

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

Flussi di lavoro	Eliminazione sicura
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

Sicurezza di rete

I server Fiery utilizzano i seguenti meccanismi di sicurezza per proteggere le comunicazioni di rete:

- Filtraggio IP e gestione delle porte
- Configurazione del firewall
- Supporto per SNMP v3 per strumenti di monitoraggio e gestione della rete sicuri

Protocolli di rete supportati

FS700/FS700 Pro supporta un'ampia gamma di protocolli di rete standard del settore per garantire compatibilità, sicurezza e comunicazioni efficienti in ambienti diversi. Questi comprendono:

- **Protocolli principali:** TCP/IP, IPv4, IPv6
- **Protocolli Web:** HTTP/1.1, HTTPS (TLS 1.2/1.3)
- **Servizi file e stampa:** FTP, LPR, IPP 2.0, SMB v2, SMB v3, Port 9100
- **Gestione e monitoraggio:** SNMP v1, v2c e v3
- **Accesso remoto:** RDP (solo server Windows basati su Windows)
- **Sicurezza e autenticazione:** IPSec (IKEv2), LDAP v3, IEEE 802.1X
- **Servizi di rete:** DHCP, DNS
- **Protocolli di rilevamento:** WSD, Bonjour, SLP

Porte di rete

Per impostazione predefinita, tutte le porte TCP/IP inutilizzate sono disabilitate. L'amministratore Fiery può abilitare e disabilitare le porte di rete. La disabilitazione di una porta impedisce in modo efficace le connessioni esterne che richiedono l'utilizzo di quella porta specifica.

Porte in entrata

I server Fiery supervisionano e monitorano i collegamenti di rete in entrata, consentendo l'accesso al server solo al traffico autorizzato e proteggendolo da accessi non autorizzati o attacchi.

TCP	UDP	Nome porta	Servizi dipendenti
20-21		FTP	FTP
80		HTTP	WebTools, IPP

TCP	UDP	Nome porta	Servizi dipendenti
135		MS RPC	Servizio Microsoft RPC. Si aprirà un'altra porta compresa tra 49152 e 65535 per fornire il servizio Point and Print SMB.
137-139		NETBIOS	Stampa Windows Queste porte sono chiuse per impostazione predefinita perché NetBIOS non è sicuro.
	161, 162	SNMP	strumenti basati su SNMP
	427	SLP	Service Location Protocol. Questa porta è bloccata per impostazione predefinita perché SLP non è sicuro.
443		HTTPS	WebTools, IPP/s
445		SMB/IP	SMB su TCP/IP
	500	ISAKMP	IPsec
515		LPD	Stampa LPR
631		IPP	IPP
3389		RDP	Desktop remoto (solo server Windows Fiery basati su Windows)
3702	3702	WS-Discovery	Web Services for Devices (WSD). Consente di rilevare e stampare sul server Fiery su WSD.
	4500	IPsec NAT trasversale	IPsec
	5353	Multicase DNS (mDNS)	Bonjour
6310		Porta DMP	Stampa mobile diretta
8010		Porte FIERY	JDF
8021-8022		Porte FIERY	Fiery Harmony, Fiery HotFolders e Fiery Command WorkStation
8090		Porte FIERY	OFA
9100-9103		Porta di stampa	Porta 9100
	9906	Porte FIERY	Harmony discovery
21030		Porte FIERY	Fiery Image Viewer

Nota: Le porte IPSec (500 e 4500) sono configurabili solo per FS700 (server Fiery basati su Linux).

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.

Porte in uscita

I server Fiery gestiscono e limitano il traffico di rete in uscita per garantire che solo le comunicazioni autorizzate lascino il dispositivo, riducendo così l'esposizione alle minacce esterne.

Porte in uscita	Descrizione	Configurazione predefinita/attivata
53	DNS	Predefinito
67	DHCP	Predefinito
80, 443	Aggiornamenti di Fiery System, JDF, PrintMe e altre comunicazioni cloud	Predefinito
161, 162	SNMP	Nella configurazione a doppio IP
21	Scansione su FTP	Alla configurazione
123	NTP	Alla configurazione
389/636	Servizi LDAP	Alla configurazione
445	Scansione su SMB/JobLog su SMB/JDF Percorso globale comune	Alla configurazione
500/4500	IPsec	Alla configurazione
8080/8443	Porta proxy HTTP/HTTPS/FTP	Alla configurazione

Comunicazione con i servizi cloud

Elenca i servizi e le applicazioni Fiery che richiedono una comunicazione con servizi esterni basati su cloud per scaricare gli aggiornamenti di sicurezza Fiery o per l'attivazione della licenza. Questa documentazione è particolarmente utile per i clienti che hanno disabilitato tutte le comunicazioni esterne e stanno tentando di fare eccezioni all'interno del firewall aziendale.

Servizio/ Applicazione Fiery	Nome di dominio completo	Porta	Ubicazione del server	Informazioni d'uso
System Update	https://liveupdate.fiery.com/des/hypatia.asmx	443	Fiery	Scarica gli aggiornamenti di sicurezza Fiery
OFA	https://flexlicensing.fiery.com	443	Fiery	Attivazione licenza
IQ	https://iq.fiery.com/iq	443	AWS	Fiery IQ Cloud
LINQ	https://ews.fiery.com	443	Azure	Dati analitici

Servizio/ Applicazione Fiery	Nome di dominio completo	Porta	Ubicazione del server	Informazioni d'uso
Stampa universale	Domini multipli: •portal.azure.com •print.print.microsoft.com •notification.print.microsoft.com •discovery.print.microsoft.com •graph.print.microsoft.com	80/443	Azure	Proxy IPP e servizio di stampa universale
SSO	login.microsoft.com	80/443	Microsoft	Single Sign-On (SSO)
Servizi di aggiornamento del server di Windows (WSUS)	Domini multipli: •http://windowsupdate.microsoft.com •http://.windowsupdate.microsoft.com •https://.windowsupdate.microsoft.com •http://.update.microsoft.com •https://.update.microsoft.com •http://.windowsupdate.com •http://download.windowsupdate.com •https://download.microsoft.com •http://.download.windowsupdate.com •http://wustat.windows.com •http://ntservicepack.microsoft.com •http://go.microsoft.com •http://dl.delivery.mp.microsoft.com •https://dl.delivery.mp.microsoft.com •http://.delivery.mp.microsoft.com •https://.delivery.mp.microsoft.com	80/443	Microsoft	Aggiornamenti Windows
Command WorkStation	Domini multipli: • https://help.fiery.com •https://learning.fiery.com •https://communities.fiery.com/s/ •https://liveupdate.fiery.com •https://iq.fiery.com	443	Fiery	

Filtraggio IP

Il filtraggio IP consente all'amministratore di controllare le richieste di connessione al server Fiery in base a indirizzi IP predefiniti. Definendo i criteri predefiniti, l'amministratore può specificare se i pacchetti di dati in arrivo devono essere consentiti o negati. Inoltre, possono creare filtri per un massimo di 16 indirizzi o intervalli IP, consentendo o negando le richieste di connessione di conseguenza.

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

Autenticazione di rete

SNMP v3

Il server Fiery supporta il più recente standard SNMPv3, che facilita l'invio di pacchetti di comunicazione 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. A questi livelli, viene eseguito l'hashing delle password utilizzando algoritmi come SHA-1 o SHA-256 e l'intero messaggio SNMP viene crittografato. Inoltre, l'amministratore locale può configurare i nomi delle comunità in scrittura e lettura SNMP e altre impostazioni di sicurezza.

IEEE 802.1x

802.1X è uno standard IEEE per il controllo degli accessi basato sulle porte che garantisce l'autenticazione dei dispositivi prima di accedere alla rete locale e alle relative risorse. Sui server Fiery, lo standard 802.1X può essere configurato per utilizzare EAP-MD5 Challenge o PEAP-MSCHAPv2 per l'autenticazione basata su server o EAP-TLS per l'autenticazione basata su certificati per una maggiore sicurezza. I server Fiery supportano solo il certificato dell'utente (non il certificato del dispositivo) per l'autenticazione basata su certificato EAP-TLS.

Il server Fiery esegue l'autenticazione durante l'avvio o ogni volta che il collegamento di rete viene scollegato e ricollegato.

Crittografia di rete

Internet Protocol Security (IPsec)

IPsec migliora la sicurezza delle comunicazioni basate su IP crittografando e autenticando ogni pacchetto a livello di rete, proteggendo così i dati in transito tra tutte le applicazioni che utilizzano IP. Fiery Server utilizza l'autenticazione con codice precondiviso per stabilire collegamenti sicuri con altri sistemi tramite IPsec. Dopo aver stabilito la comunicazione su IPsec tra un computer client e Fiery Server, tutte le comunicazioni, inclusi i lavori di stampa, vengono trasmesse sulla rete in tutta sicurezza.

HTTPS

I server Fiery applicano la protezione delle comunicazioni tra i client e i componenti server tramite HTTPS su TLS. Ciò garantisce che tutti i dati trasmessi, come i lavori di stampa, gli aggiornamenti sullo stato dei lavori e i comandi amministrativi, siano crittografati in transito, proteggendoli da intercettazioni o manomissioni. I server Fiery supportano TLS 1.3 e TLS 1.2 e offrono una protezione crittografica avanzata e moderne funzioni di sicurezza. HTTPS è obbligatorio per i collegamenti a WebTools e Fiery API, garantendo che il traffico amministrativo e operativo venga trasmesso in modo sicuro.

Gestione certificati

I server Fiery offrono un'interfaccia per la gestione dei certificati utilizzati durante le comunicazioni TLS. I server Fiery supportano i certificati X.509 in formato PEM, codificati in Base64, che utilizzano chiavi RSA con lunghezze di 4096, 3072 o 2048 bit.

La gestione dei certificati consente all'amministratore Fiery di eseguire le operazioni seguenti:

- Generare certificati digitali autofirmati.
- Aggiungere un certificato e il codice privato associato per il server Fiery.
- Aggiungere, selezionare, visualizzare e rimuovere i certificati da un'autorità di certificazione attendibile.

I certificati digitali autofirmati forniscono la crittografia, ma non offrono la convalida automatica dell'attendibilità. Per distribuzioni sicure, è consigliabile utilizzare certificati emessi da un'autorità di certificazione (CA) attendibile per garantire la verifica dell'identità corretta.

Una volta che il certificato è stato firmato da una CA attendibile, è possibile caricarlo sul server Fiery nella sezione Configura di WebTools.

Server Message Block (SMB)

SMBv1, il protocollo precedente per la condivisione di file e stampanti, è disabilitato sui server Fiery a causa di vulnerabilità di sicurezza note. I server Fiery supportano invece SMBv2 e SMBv3. La firma SMB viene applicata, garantendo che tutti i pacchetti siano firmati digitalmente per evitare attacchi man-in-the-middle. Quando l'autenticazione SMB è abilitata, gli utenti devono fornire un nome utente e una password validi per accedere alle cartelle e ai contenuti condivisi. È possibile inoltre limitare la stampa o la condivisione dei file tramite SMB per un account guest impostando una password in Fiery Configure.

Sicurezza dell'hardware

I server Fiery sono progettati per garantire la sicurezza dell'hardware di livello enterprise. La protezione delle informazioni sensibili non si limita ai controlli software: i componenti hardware svolgono un ruolo fondamentale nel mantenimento dell'integrità del sistema e della riservatezza dei dati. Di seguito sono descritti i principali elementi hardware e le relative misure di sicurezza.

Memoria volatile (RAM)

I server Fiery utilizzano la memoria volatile (RAM) per memorizzare temporaneamente i dati durante le operazioni attive. Per mitigare il rischio di esposizione dei dati:

- le informazioni sensibili nella RAM vengono cancellate immediatamente dopo l'uso o all'arresto del sistema.
- Le tecniche di pulitura della memoria vengono applicate per impedire la persistenza dei dati residui.
- L'accesso alla RAM è limitato tramite la separazione dei privilegi imposta dal processore e dal sistema operativo.

Memoria non volatile e Data Storage

La memoria non volatile, inclusi dischi rigidi, unità a stato solido (SSD) e altri storage persistenti, conserva i dati anche quando il sistema è spento. Le misure di sicurezza includono:

- User Data Encryption (UDE) per proteggere i dati memorizzati.
- Metodi di eliminazione sicura per rendere irrecuperabili le informazioni riservate quando i file vengono rimossi.

Memoria flash

La memoria flash viene utilizzata per memorizzare il firmware, i file di configurazione e le impostazioni di sistema. Per mantenerne la sicurezza:

- il firmware è firmato digitalmente per evitare manomissioni.
- Gli aggiornamenti del firmware vengono verificati tramite checksum crittografici prima dell'installazione.
- I meccanismi di protezione da scrittura impediscono modifiche non autorizzate durante il runtime.

CMOS eNVRAM

I parametri critici del sistema, come ad esempio le configurazioni hardware e le impostazioni di avvio, vengono memorizzati in CMOS e RAM non volatile (NVRAM). Per proteggere questi dati:

- l'accesso è limitato ai processi amministrativi autorizzati.
- I meccanismi di avvio sicuro garantiscono che solo il firmware attendibile legga e scriva in queste aree.
- Le variabili NVRAM critiche vengono sottoposte a backup e vengono verificate l'integrità per evitare danneggiamenti o alterazioni dannose.

Unità di archiviazione

I server Fiery utilizzano unità di archiviazione per archiviare il sistema operativo e i file di sistema. Queste unità vengono utilizzate anche per lo spool dei lavori, i log e i file temporanei.

Per proteggere i dati dei clienti sono disponibili le seguenti funzioni di sicurezza:

- Crittografia a livello di unità.
- Elenchi di controllo di accesso (ACL) per limitare le operazioni di lettura/scrittura non autorizzate.
- Kit di sicurezza dell'unità disco (opzionale per i server Fiery esterni) che migliorano la sicurezza del sistema consentendo agli utenti di bloccare in modo sicuro le unità del server durante il normale funzionamento.

Porte fisiche

Le porte fisiche, come USB, interfacce di rete e connettori di servizio, sono potenziali vettori per l'accesso non autorizzato. La sicurezza dell'hardware Fiery affronta questo rischio nei seguenti modi:

- Disabilitazione delle porte inutilizzate a livello hardware o firmware.
- Richiesta di autorizzazione amministrativa per il collegamento di dispositivi esterni.
- Monitoraggio e registrazione di tutte le interazioni con interfacce fisiche critiche.

Integrando queste misure di sicurezza hardware con le protezioni software e di rete, i server Fiery offrono una strategia di difesa completa e approfondita, garantendo la riservatezza, l'integrità e la disponibilità dei dati sensibili negli ambienti di stampa.

Integrità del sistema e aggiornamenti sicuri

Mantenere l'integrità del sistema è fondamentale per garantire la sicurezza. I server Fiery forniscono il seguente supporto:

- Log di verifica sicurezza
- Avvio protetto: garantisce che venga caricato solo software attendibile.
- Aggiornamenti con firma digitale: impedisce la manomissione degli aggiornamenti software.
- Gestione automatizzata degli aggiornamenti di sicurezza: semplifica il processo di applicazione degli aggiornamenti di sicurezza.

Log di verifica sicurezza

Gli amministratori con privilegi elevati possono accedere ed esaminare gli eventi di sicurezza registrati nel log di verifica sicurezza. Questo log è abilitato per impostazione predefinita.

Ogni evento di sicurezza è classificato come informazione, avviso o errore. L'amministratore non riceve avvisi o notifiche, al contrario, viene presentato un log statico.

I log sono formattati per garantire la compatibilità con gli strumenti SIEM (Security Information and Event Management) comunemente utilizzati per la raccolta e l'analisi dei log. Tutti i dati degli eventi acquisiti sono conformi agli standard delineati in NIST SP 800-53.

L'amministratore Fiery può accedere al log di verifica sicurezza senza bisogno dell'intervento di FIERY. I log per i server basati su Linux vengono forniti in formato syslog (RFC 5424 o RFC 3164). Per i server basati su Windows, i log vengono salvati nel formato standard Windows EVTX e possono essere letti da Gestione log eventi di Windows e da molte soluzioni commerciali disponibili che utilizzano l'API del log eventi di Windows. I server Fiery basati su Linux offrono la possibilità di inoltrare i log a un sistema di raccolta centralizzato come Syslog.

I log di sicurezza vengono mantenuti in base alla capacità di archiviazione locale allocata. Quando la dimensione del log supera il limite di archiviazione predefinito (400 MB), gli eventi meno recenti vengono rimossi automaticamente.

Avvio protetto

Questa funzionalità garantisce l'integrità dei file del sistema operativo durante l'avvio consentendo il caricamento solo dei componenti con firma digitale e attendibili. Sui server Fiery, blocca l'esecuzione di codice non autorizzato o dannoso durante l'avvio, migliorando la sicurezza e riducendo il rischio di compromissione. Per impostazione predefinita, l'Avvio protetto è disabilitato.

aggiornamenti con firma digitale

I server Fiery utilizzano aggiornamenti con firma digitale per garantire l'integrità e l'autenticità di tutte le installazioni di software e firmware. Ogni aggiornamento è firmato crittograficamente da Fiery o dai suoi partner autorizzati, consentendo al server di verificare che il contenuto non sia stato alterato o manomesso. Questo processo protegge dall'introduzione di codice dannoso e garantisce che vengano applicati solo aggiornamenti attendibili, mantenendo la sicurezza e l'affidabilità del sistema.

Gestione automatizzata degli aggiornamenti di sicurezza

Gli aggiornamenti software sono fondamentali per garantire il funzionamento ottimale dei server Fiery. L'installazione degli aggiornamenti per la sicurezza è importante per garantire che i server Fiery siano protetti in ogni ambiente di stampa specificato.

Fiery System Update scarica e installa gli aggiornamenti per la sicurezza se l'opzione è abilitata sul server Fiery. Per impostazione predefinita, questa opzione è abilitata e si consiglia ai clienti di lasciarla abilitata.

Le vulnerabilità di sicurezza del sistema operativo Microsoft® Windows™ non sono descritte in dettaglio in questo documento in quanto sono gestite direttamente da Microsoft e distribuite ai clienti come **aggiornamenti di Windows** mano a mano che sono disponibili.

Per affrontare problemi di sicurezza o vulnerabilità che potrebbero avere un impatto sui componenti hardware Fiery chiave, tra cui scheda madre, processore e firmware, FIERY collabora strettamente con i produttori per ottenere gli aggiornamenti di sicurezza richiesti. Questi aggiornamenti per la sicurezza vengono successivamente forniti ai clienti in base alle necessità.

Nota: Gli aggiornamenti del software Fiery sono firmati digitalmente con l'algoritmo SHA-2 (Secure Hash Algorithm) per evitare modifiche non autorizzate, incluso l'inserimento di malware.

Aggiornamenti della sicurezza software del sever Fiery

Gli aggiornamenti software tempestivi sono essenziali per il funzionamento ottimale del server Fiery. Applicando i più recenti aggiornamenti per la sicurezza del software Fiery Server, viene garantita l'integrità del sistema, le vulnerabilità vengono mitigate e viene mantenuta la conformità con gli standard di sicurezza del settore.

Il team di sicurezza dei server Fiery monitora e tiene traccia diligentemente delle vulnerabilità di sicurezza attraverso una rete completa di fonti attendibili e affidabili, come ad esempio:

- Avvisi e raccomandazioni della CyberSecurity and Infrastructure Security Agency (CISA) degli Stati Uniti
- Database nazionale delle vulnerabilità del National Institute for Standards and Technology (NIST) degli Stati Uniti
- Record di vulnerabilità ed esposizioni comuni (CVE)
- Rapporti e raccomandazioni del Centro di coordinamento CERT (CERT/CC) sulle vulnerabilità di software e hardware
- Governo regionale e agenzie di regolamentazione
- Avvisi di sicurezza dei fornitori di software e hardware

Fiery assegna la priorità alle correzioni relative alla sicurezza in base alla gravità (Critica, Alta, Media e Bassa) in base al Common Vulnerability Scoring System (CVSS). Queste correzioni vengono rilasciate dopo aver ottenuto l'approvazione corrispondente da parte del partner OEM (Original Equipment Manufacturer). Una volta approvati, gli aggiornamenti per la sicurezza per il software Fiery sono disponibili per il download. Tutti gli aggiornamenti del software Fiery sono firmati digitalmente con l'algoritmo SHA-2 (Secure Hash Algorithm) per evitare modifiche non autorizzate, incluso l'inserimento di malware.

Quando è abilitato, Fiery System Update scarica e installa automaticamente gli aggiornamenti per la sicurezza sul server Fiery. Per impostazione predefinita, questa opzione è abilitata e si consiglia vivamente ai clienti di mantenerne lo stato attivo.

Conformità e procedure consigliate

Solide implementazioni di sicurezza sono conformi agli standard di settore e ai quadri normativi fondamentali, tra cui:

- GDPR, Legge UE sui dati
- ISO/IEC 27001 (solo FS700 Pro)
- FIPS 140-2
- NIST 800-88. Linee guida per la sanificazione dei supporti (solo FS700 Pro)
- NIST 800-52. Linee guida per la selezione, la configurazione e l'utilizzo delle implementazioni di Transport Layer Security (TLS)
- NIST 800-171. Protezione delle informazioni non classificate controllate in sistemi e organizzazioni non federali (solo FS700 Pro)
- Certificazione del modello di maturità della sicurezza informatica (CMMC) del Dipartimento della Difesa degli Stati Uniti. Livello 2: ampia protezione delle informazioni non classificate controllate (CUI) (solo FS700 Pro)
- NIST 800-193. Linee guida per la resilienza del firmware della piattaforma (solo FS700 Pro)
- NIST 800-53. Controlli di sicurezza e privacy per i sistemi informativi e le organizzazioni
- Profilo di protezione Common Criteria per sistemi operativi generici (solo FS700 Pro)

Per rafforzare il livello di sicurezza, gli amministratori IT sono responsabili dell'implementazione delle misure seguenti:

- Applicazione regolare degli aggiornamenti della sicurezza
- Applicazione di criteri di autenticazione solidi
- Esecuzione di controlli di sicurezza periodici
- Implementazione della segmentazione di rete per gli ambienti di stampa

Linee guida per la configurazione di server Fiery protetti

Gli amministratori Fiery possono seguire queste linee guida per rafforzare la sicurezza durante la configurazione del server Fiery:

Modifica della password dell'amministratore

I server Fiery vengono forniti dalla fabbrica con una password predefinita per l'account amministratore. Questa password garantisce l'accesso completo al server Fiery, sia in locale che da un client remoto. Questo accesso comprende, ma senza limitazione:

- File system (solo server Fiery su Windows)
- Impostazioni di sicurezza del sistema
- Impostazioni delle applicazioni
- Voci di registro

Si consiglia di modificare la password predefinita dell'amministratore Fiery subito dopo l'installazione e, a intervalli regolari, come richiesto dalle politiche sulla sicurezza dell'azienda. La password dell'amministratore Fiery deve essere modificata all'interno della piattaforma Fiery.

Procedura consigliata per operazioni sicure ed efficienti

- Limitare SNMP alla versione 3 per la massima sicurezza.
- Disabilitare WSD per l'inoltro dei lavori per impedirne l'utilizzo nei flussi di lavoro di stampa.
- Disabilitare i protocolli di stampa Windows (LPR, porta 9100, IPP) a meno che non sia esplicitamente richiesto.
- Abilitare il filtro porta TCP/IP per bloccare le porte inutilizzate e ridurre i rischi.
- Chiudere le porte 137-139 e 445 se non sono necessarie per la stampa su Windows o la condivisione di file.
- Disabilitare HTTP sulla porta 80 per impedire comunicazioni non protette.
- Abilitare la stampa protetta in modo che solo il proprietario del lavoro possa rilasciare i lavori di stampa.

Ambienti ad alta sicurezza

Gli amministratori con privilegi elevati possono configurare facilmente le impostazioni di sicurezza elevata selezionando il profilo di sicurezza elevata disponibile in **WebTools** > **Configure** > **Security**.

Conclusioni

I server Fiery, pur essendo dotati di solide funzioni di sicurezza, non sono progettati per essere connessi a Internet. Deve essere installato in un ambiente di rete protetto con accesso attentamente controllato dall'amministratore di rete. Progettati per soddisfare i più recenti standard del settore, i server Fiery offrono un livello di sicurezza di livello enterprise per proteggere gli ambienti di stampa dalle minacce informatiche in continua evoluzione. Gli amministratori possono garantire la conformità e salvaguardare i dati sensibili sfruttando appieno le funzionalità di sicurezza di Fiery.

Novità in FS700, FS700 Pro

- Moduli di sistema principali aggiornati per risolvere le vulnerabilità di sicurezza.
- La funzionalità e-mail è stata dichiarata obsoleta per prevenire attacchi e-mail e garantire la conformità alle norme di sicurezza.
- Tutte le comunicazioni con il server Fiery possono ora essere crittografate utilizzando TLS 1.3. I collegamenti del desktop remoto ai server Fiery che eseguono Windows 10 attualmente supportano TLS 1.2.
- È stato aggiunto il supporto TLS 1.3 alle seguenti applicazioni e moduli Fiery:
  - Licenze per i componenti server e client
  - Proxy IPP: necessario per Microsoft Universal Print
  - Protocollo di autenticazione di rete 802.1x
  - EFI LINQ: utilizzato per la segnalazione di arresti anomali di server Fiery
  - JDF
  - System Update
  - FCC – Fiery Cloud Connector
- Gli strumenti IPsec utilizzati sui server Linux sono stati sostituiti con strumenti più recenti e sicuri.
- È stato aggiunto il supporto per Advanced Encryption Standard (AES) per le comunicazioni SNMPv3 e AES 128 è stato reso il nuovo valore predefinito:
  - AES 128 (valore predefinito)
  - AES 192 (l'utente può selezionare da Configure)
  - AES 256 (l'utente può selezionare da Configure)
  - DES è ancora supportato, anche se non è più l'opzione predefinita. Gli utenti possono selezionarla se necessario.