Fiery FS800 Pro/FS800 DFEs

Security White Paper

45271119

6. August 2026

Inhalt

Einführung

Dieses Dokument bietet eine Übersicht über die Sicherheitsfunktionen von digitalen Fiery Front-Ends (DFEs). IT-Administratoren und Sicherheitsexperten erhalten die benötigten Informationen, um zu bewerten, wie Fiery DFEs Druckumgebungen schützen und sichern. In diesem Dokument werden die Prinzipien und Mechanismen beschrieben, die in DFEs zum Schutz von Daten, zur Verbesserung der Netzwerksicherheit und zur Aufrechterhaltung der Systemintegrität verwendet werden.

Sicherheitsgrundsätze

Fiery DFEs wurden sorgfältig für die Einhaltung bewährter Verfahren der Branche entwickelt, um Datenschutzbestimmungen und Unternehmenssicherheitsanforderungen einzuhalten. Die Grundprinzipien, die diesem Design zugrunde liegen, sind wie folgt:

- Datenschutz: Verschlüsselung von Daten im Ruhezustand und während der Übertragung
- Netzwerksicherheit: Kontrollierter Zugriff, sichere Kommunikationsprotokolle und Authentifizierungsmechanismen
- Systemintegrität: Firmware-Verifizierung, Sicheres Booten und Sicherheitsupdates

In Zusammenarbeit mit unseren globalen Partnern und Lieferanten bieten wir unseren Kunden kontinuierliche Unterstützung bei auftretenden Bedrohungen. Um umfassende Systemsicherheit zu gewährleisten, empfehlen wir Endbenutzern, Fiery Sicherheitsfunktionen in die organisationseigenen Sicherheitsrichtlinien zu integrieren und bewährte Branchenverfahren einzuhalten, einschließlich der Implementierung sicherer Kennwörter und robuster physischer Sicherheitsmaßnahmen.

Authentifizierung und Zugriffssteuerung

Fiery DFEs unterstützen u. a. die folgenden Authentifizierungsmethoden:

- Integration von LDAP und Active Directory
- Multi-Faktor-Authentifizierung (MFA), implementiert über Einmaliges Anmelden (SSO)

Anwenderauthentisierung

Mit der Authentifizierungsfunktion können auf dem Fiery DFE die folgenden Funktionen ausgeführt werden:

- Authentifizieren eines Anwenders
- Rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC)

Der Fiery DFE unterstützt die folgenden drei Anwenderauthentisierungsmethoden:

- Lokale Authentifizierung für Anwender, die auf dem Fiery DFE definiert sind
- Ein-Faktor-Authentifizierung (SFA) über externe Netzwerk-Authentifizierungsserver mit LDAP (z. B. Microsoft Active Directory)
- Multi-Faktor-Authentifizierung (MFA) mit Einmaligem Anmelden (SSO)

Die Administratorkonten erfordern unabhängig vom gewählten Verfahren immer eine Authentifizierung. Diese Funktion kann nicht deaktiviert werden.

Gruppenberechtigungen

Das Fiery DFE autorisiert Aktionen von Anwendern in Abhängigkeit von ihrer Gruppenzugehörigkeit. Jeder Gruppe sind bestimmte Berechtigungen zugewiesen, z. B. das Drucken in Farbe oder in Schwarz-weiß (S/W). Die Aktionen von Gruppenmitgliedern sind auf diese Berechtigungen beschränkt. Der Fiery Administrator ist befugt, die Berechtigungen jeder Fiery Gruppe zu ändern, mit Ausnahme der Administrator- und Bediener-Konten.

Bei dieser Methode der Anwenderauthentisierung sind die verschiedenen Berechtigungen, die für eine Gruppe ausgewählt werden können, wie folgt:

- In S/W drucken: erlaubt Gruppenmitgliedern, Aufträge in schwarz-weiß zu drucken. Wenn es sich bei dem Auftrag um einen Farbauftrag handelt, wird er ebenfalls in schwarz-weiß gedruckt.
- In Farbe und S/W drucken: erlaubt Gruppenmitgliedern, Aufträge mit Vollzugriff auf die Farb- und S/W-Druckfunktionen des Fiery DFE zu drucken. Ohne diese Berechtigung oder die Berechtigung zum Drucken in S/W können Anwender den Druckauftrag zwar übermitteln, aber der Druck schlägt fehl.
- Fiery Mailbox: erlaubt Gruppenmitgliedern jeweils eine eigene Mailbox. Das Fiery DFE erstellt für jeden Anwender unter dessen Namen eine Mailbox und erteilt die Zugriffsberechtigung für diese Mailbox. Der Zugriff auf diese Mailbox ist auf Anwender beschränkt, die den Mailbox-Anwendernamen und das zugehörige Kennwort kennen.

- Kalibrierung: Mit dieser Berechtigung können Gruppenmitglieder die Farbkalibrierung durchführen.
- Servervorgaben erstellen: erlaubt Gruppenmitgliedern, Servervorgaben zu erstellen. Gruppenmitglieder haben Zugriff auf diese Servervorgaben.
- Workflows verwalten: Mit dieser Berechtigung können Gruppenmitglieder virtuelle Drucker erstellen, freigeben oder bearbeiten.
- Aufträge bearbeiten (nur Fiery XB DFEs): Mit dieser Berechtigung können Gruppenmitglieder einen Auftrag in der Warteschlange bearbeiten.

Administratoren mit erweiterten Berechtigungen können diese Funktionen anpassen, um unbefugten Zugriff zu verhindern und die Sicherheitsrichtlinien der Organisation durchzusetzen.

Lokale Anwender

Die Fiery DFE-Software interagiert mit eindeutigen Benutzertypen, die sich von Windows-Benutzern oder -Rollen unterscheiden. Fiery Administratoren sollten nach der Erstinstallation umgehend alle Standardkennwörter ändern. Für den Zugriff auf das Fiery DFE muss zwingend eine Kennwortauthentifizierung verwendet werden.

- Die maximale Kennwortlänge für „Administrator“ und „Operator“ beträgt 64 Zeichen, wenn **Configure** > **Sicherheit** verwendet wird.
- Die maximale Kennwortlänge für lokale Benutzerkonten beträgt 64 Zeichen, wenn **Configure** > **Benutzerkonten** verwendet werden.
- Das Administrator- und Bedienerkennwort kann in **Configure** > **Anwenderkonten** geändert werden.

Lokale Fiery Anwenderkonten und Zugriffsberechtigungen

- Administrator: Vollständige Kontrolle über die Funktionen des Fiery DFE, kann die Berechtigungen der Fiery Gruppe ändern, mit Ausnahme der Administrator- und Bediener-Konten.
- Bediener: Hat dieselben Berechtigungen wie der Administrator, aber keinen Zugriff auf die DFE-Einstellungen und das Löschen von Auftragsprotokollen.
- Druckmaschinenbediener (nur Fiery XB-DFEs): Verwaltet Aufträge auf der Druckmaschine mit bestimmten, vom Administrator hinzugefügten Berechtigungen.
- Fiery DFE-Admin (nur Windows-Server): Ein ausgeblendetes Admin-Konto für die Installation des vertrauenswürdigen Zertifikats, kann sich nicht am Fiery DFE anmelden, wird in den Tools für Netzwerkscans angezeigt und kann entfernt werden.
- Fiery_SMB_User: Standardmäßiges SMB-Konto für Windows-Druckfunktionalität, das Einblick in die Fiery DFE-Druckwarteschlangen in der Netzwerkumgebung bietet.
- Gast (Standard, kein Kennwort): Gleiche Berechtigungen wie Bediener, hat aber keinen Zugriff auf Auftragsprotokolle, kann keine Bearbeitungen vornehmen, keine Statusänderungen vornehmen und kann Aufträge nicht in der Vorschau anzeigen.

LDAP-Authentifizierung

Das Fiery DFE verwendet LDAP Version 3 (RFC 2251-konform) für die Kommunikation mit Unternehmensservern. Über LDAPv3 werden E-Mail-Adressen von Anwendern für Scanfunktionen sowie Anwender- und Gruppeninformationen für die Authentifizierung abgerufen. Diese Funktion wird ausschließlich für LDAP-Verbindungen zu Active Directory-Servern unterstützt.

Das Fiery DFE unterstützt folgende Authentifizierungsmethoden unter Verwendung von LDAP:

- Automatisch
- SIMPLE
- GSSAPI

In der folgenden Tabelle werden die verschiedenen LDAP-Authentifizierungsmethoden beschrieben:

Authentifizierungsmethode	**Beschreibung**	**Active Directory-Server**
Automatisch	Diese Option wählt GSSAPI oder SIMPLE aus, je nachdem, welche Authentifizierungsmethode vom LDAP-Server unterstützt wird.	Unterstützt
SIMPLE	Kennwort ist erforderlich. Wenn LDAP über TLS ausgewählt ist, wird das Kennwort mit TLS verschlüsselt.	Unterstützt
GSSAPI	Bei dieser Methode werden Kerberos-Tickets anstelle von Kennwörtern verwendet, sodass TLS nicht erforderlich ist.	Unterstützt

Einmaliges Anmelden (SSO)

Fiery FS800 Pro DFEs unterstützen das OpenID Connect-Protokoll für die cloudbasierte Anwenderauthentisierung via Einmaliges Anmelden (SSO) mit Microsoft Entra ID (ehemals Azure AD). Anwender können sich bei einem Fiery DFE mit ihren bestehenden Entra-ID-Anmeldeinformationen anmelden.

Diese Authentifizierungsmethode unterstützt die Multi-Faktor Authentifizierung (MFA).

Dieser Identitätsmanagement-Ansatz stellt sicher, dass Fiery DFEs Kennwörter niemals lokal speichern, wodurch die Sicherheit erheblich erhöht wird.

Datensicherheitsmaßnahmen

Um vertrauliche Informationen zu schützen, implementieren Fiery DFEs Folgendes:

Verschlüsselte Speicherung: Schützt Druckaufträge und Konfigurationsdaten

Die Verschlüsselung sensibler Kundendaten stellt sicher, dass alle Kennwörter und entsprechende Konfigurationsinformationen sicher auf dem Fiery DFE gespeichert werden. Diese kritischen Informationen werden entweder verschlüsselt oder mit kryptografischen Algorithmen wie AES-256 und SHA-2 gehasht, die den neuesten Sicherheitsstandards entsprechen.

Auf der Festplatte gespeicherte Kundendaten bleiben unzugänglich, auch wenn die Festplatte aus dem Fiery DFE entfernt wird. Die Verschlüsselung von Anwenderdaten kann auf Windows-basierten Fiery DFEs aktiviert oder deaktiviert werden. Bei Linux-basierten Fiery DFEs ist diese Verschlüsselungsfunktion immer aktiviert.

Im Falle einer vergessenen Passphrase, die für die Datenwiederherstellung verwendet wird, kann FIERY sie nicht zurücksetzen, sodass eine vollständige Neuinstallation der Software erforderlich ist.

Windows-basierte Fiery DFEs bieten auch die Möglichkeit, das Boot-Laufwerk zu verschlüsseln, das das Betriebssystem enthält. Diese Verschlüsselung dient dazu, Offline-Angriffe auf den Fiery DFE zu verhindern und sicherzustellen, dass das Boot-Laufwerk nicht auf einem anderen Gerät verwendet werden kann.

Sicheres Löschen: Stellt sicher, dass Daten nach dem Löschen nicht wiederhergestellt werden können.

Windows-basierte FS800 Pro DFEs unterstützen den Standard zur Datenbereinigung NIST 800-88. Fiery Administratoren können diese Option für Methoden zum Überschreiben von Bildern mit 1 Zyklus oder 3 Zyklen konfigurieren.

Hinweis: Die Funktion „Sicheres Löschen“ wird auf Linux-basierten und XB-Plattformen von Fiery oder für Anwenderdaten, die auf SSDs gespeichert sind, nicht unterstützt.

Workflows	Sicheres Löschen
Auf dem Fiery DFE Festplattenlaufwerk gespeicherte Aufträge; Funktion „Sicheres Löschen**eingeschaltet**	Ja
Auf dem Fiery DFE Festplattenlaufwerk gespeicherte Aufträge; Funktion „Sicheres Löschen**ausgeschaltet**	Nein
Aufträge, die vom Fiery DFE empfangen und gelöscht werden, nachdem die Funktion „Sicheres Löschen**eingeschaltet** wird	Ja
Aufträge, die vom Fiery DFE empfangen und gelöscht werden, bevor die Funktion „Sicheres Löschen**eingeschaltet** wird	Nein

Workflows	Sicheres Löschen
Kopien von Aufträgen, die an einen anderen Fiery DFE gesendet wurden (Lastausgleich)	Nein
Auf Wechseldatenträgern archivierte Aufträge	Nein
Auf Netzwerklaufwerken archivierte Aufträge	Nein
Aufträge, die sich auf Client-Geräten befinden	Nein
Ausführung der Funktion „Serverdaten löschen“	Ja
Seiten, die in einen anderen Auftrag übernommen oder kopiert wurden (z. B. Fiery Impose Aufträge oder kombinierte PDF-Dateien)	Nein
Aufträge, die über die SMB-Verbindung empfangen und auf dem Fiery DFE Festplattenlaufwerk gespeichert werden	Nein
Teile eines Auftrags, die während des Festplattenaustauschs oder der Festplatten-Caching-Vorgänge auf die Festplatte des Fiery DFE geschrieben werden	Nein
Auftragsprotokolleinträge	Nein
Auftragsprotokolleinträge nach der Ausführung der Funktion „Serverdaten löschen“	Ja
Fiery DFE wird ausgeschaltet, bevor das Löschen des Auftrags abgeschlossen ist	Nein
Defragmentierung des Fiery DFE Festplattenlaufwerks vor dem Löschen eines Auftrags	Nein

Netzwerksicherheit

Fiery DFEs verwenden die folgenden Sicherheitsmechanismen, um die Netzwerkkommunikation zu schützen:

- Firewall-Konfiguration, einschließlich IP-Filterung und Port-Management
- Transport Layer Security (TLS) für verschlüsselte Kommunikation (z. B. HTTPS, LDAPS)
- IPSec für verschlüsselte sichere Host-to-Host-Kommunikation
- SNMP v3 für sichere Netzwerküberwachung und -verwaltung

Unterstützte Netzwerkprotokolle

FS800/FS800 Pro unterstützt eine Vielzahl von Netzwerkprotokollen nach Industriestandard, um Kompatibilität, Sicherheit und effiziente Kommunikation über verschiedene Umgebungen hinweg zu gewährleisten. Dazu zählen:

- **Kernprotokolle:** TCP/IP, IPv4, IPv6
- **Webprotokolle:** HTTP/1.1, HTTPS (TLS 1.2/1.3)
- **Datei- und Druckdienste:** FTP, LPR, IPP 2.0, SMB v2, SMB v3, Port 9100
- **Verwaltung und Überwachung:** SNMP v1, v2c und v3
- **Remote-Zugriff:** RDP (nur Windows-basierte DFEs)
- **Sicherheit und Authentifizierung:** IPsec (IKEv2), LDAP v3, IEEE 802.1X
- **Netzwerkdienste:** DHCP, DNS
- **Erkennungsprotokolle:** WSD, Bonjour, SLP

Netzwerkports

Standardmäßig sind alle nicht verwendeten TCP/IP-Ports deaktiviert. Der Fiery Administrator kann Netzwerkports nach Bedarf aktivieren und deaktivieren. Das Deaktivieren eines Ports verhindert die externen Verbindungen über diesen Port.

Eingehende Ports

Fiery DFEs überwachen eingehende Netzwerkverbindungen, sodass nur autorisierter Datenverkehr auf das DFE zugreifen kann und es vor unbefugtem Zugriff oder Angriffen geschützt ist.

TCP	UDP	Portname	Abhängige Dienste
20–21		FTP	FTP

TCP	UDP	Portname	Abhängige Dienste
80		HTTP	WebTools, IPP
135		MS RPC	Microsoft® RPC Service. Ein weiterer Port im Bereich 49152–65535 wird für den SMB-basierten Point-and-Print-Dienst geöffnet.
137–139		NETBIOS	Windows-Druckfunktionalität Diese Ports sind standardmäßig geschlossen, da NetBIOS unsicher ist.
	161, 162	SNMP	SNMP-basierte Tools
	427	SLP	Service Location Protocol. Dieser Port ist standardmäßig blockiert, da SLP unsicher ist.
443		HTTPS	WebTools, IPPS
445		SMB/IP	SMB über TCP/IP
	500	ISAKMP	IPsec
515		LPD	LPR-Druckfunktionalität
631		IPP	IPP
3389		RDP	Remote Desktop (nur Windows-basierte Fiery DFEs)
3702	3702	WS-Discovery	WSD (Web Services for Devices). Ermöglicht die Erkennung von und das Drucken auf dem Fiery DFE über WSD.
	4500	IPSec NAT-Durchgänge	IPsec
	5353	Multicast DNS (mDNS)	Bonjour
6310		DMP	Direkter mobiler Druck
8010		FIERY Port	JDF
8021–8022		FIERY Ports	Fiery Harmony, Fiery HotFolders und Fiery Command WorkStation
8090		FIERY Port	OFA
9100–9103		Druckports	Port 9100
	9906	FIERY Port	Harmony-Erkennung
21030		FIERY Port	Fiery Image Viewer

Hinweis: Die IPSec-Ports (500 und 4500) sind nur für FS800 (Linux-basierte Fiery DFEs) konfigurierbar.

Andere TCP-Ports, mit Ausnahme der vom Fiery Partner festgelegten Ports, sind deaktiviert. Auf einen von einem deaktivierten Port abhängigen Dienst kann nicht aus der Ferne zugegriffen werden.

Die vom Fiery DFE bereitgestellten unterschiedlichen abhängigen Dienste können vom Fiery Administrator ebenfalls einzeln aktiviert und deaktiviert werden.

Ausgehende Ports

Fiery DFEs verwalten und beschränken den ausgehenden Netzwerkverkehr, damit nur autorisierte Kommunikation das Gerät verlässt und somit die Gefährdung durch externe Bedrohungen verringert wird.

Ausgehende Ports	Zweck	Standard/Ein-Konfiguration
53	DNS	Standard
67	DHCP	Standard
80, 443	Fiery System Updates, Windows Updates, JDF, PrintMe und andere Cloud-Kommunikation	Standard
161, 162	SNMP	In Dual-IP-Konfiguration
21	Scan für FTP	Bei Konfiguration
123	NTP	Bei Konfiguration
389/636	LDAP-Dienste	Bei Konfiguration
445	Scannen nach SMB/JobLog für SMB/JDF allgemeine globale Ressourcen	Bei Konfiguration
500/4500	IPSEC	Bei Konfiguration
8080/8443	HTTP/HTTPS/FTP-Proxy-Port	Bei Konfiguration

Kommunikation mit Cloud-Diensten

Dies listet Fiery Dienste und andere Fiery Anwendungen auf, die Kommunikation mit externen cloudbasierten Diensten erfordern, zum Beispiel Anwendungen zum Herunterladen von Fiery Sicherheitsupdates oder zur Lizenzaktivierung. Diese Dokumentation ist besonders nützlich für Kunden, die die gesamte externe Kommunikation deaktiviert haben und versuchen, Ausnahmen innerhalb ihrer Unternehmensfirewall vorzunehmen.

Fiery Dienst/ Anwendung	Vollqualifizierter Domänenname/URL	Port	Serverstandort	Nutzungshinweise
System-Update	https://liveupdate.fiery.com/des/hypatia.asmx	443	Fiery	Fiery Sicherheitsupdates herunterladen
OFA	https://flexlicensing.fiery.com	443	Fiery	Lizenzaktivierung
IQ	https://iq.fiery.com/iq	443	AWS	Fiery IQ Cloud

Fiery Dienst/ Anwendung	Vollqualifizierter Domänenname/URL	Port	Serverstandort	Nutzungshinweise
LINQ	https://ews.fiery.com	443	Azure	Analysen
Universelles Drucken	Mehrere Domains: • portal.azure.com • print.print.microsoft.com • notification.print.microsoft.com • discovery.print.microsoft.com • graph.print.microsoft.com	80/443	Azure	IPP-Proxy und Druckdienst „Universelles Drucken“
SSO	login.microsoft.com	80/443	Microsoft	Einmaliges Anmelden
Windows Server Update Services (WSUS)	Mehrere Domains: • 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	Windows-Updates

Fiery Dienst/ Anwendung	Vollqualifizierter Domänenname/URL	Port	Serverstandort	Nutzungshinweise
Command WorkStation	Mehrere Domains: • https://help.fiery.com • https://learning.fiery.com • https://communities.fiery.com/s/ • https://liveupdate.fiery.com • https://iq.fiery.com	443	Fiery	Fiery Support, Fiery Updates, Fiery Cloud

IP-Filterung

Mit der IP-Filterung kann der Administrator Verbindungsanfragen an das Fiery DFE anhand vordefinierter IP-Adressen steuern. Durch die Definition von Standardrichtlinien kann der Administrator festlegen, ob empfangene Datenpakete zugelassen oder abgewiesen werden sollen. Darüber hinaus kann er Filter für maximal 16 IP-Adressen oder Bereiche erstellen und Verbindungsanfragen entsprechend zulassen oder ablehnen.

Jede IP-Filtereinstellung legt entweder eine IP-Adresse oder eine Auswahl an IP-Adressen und die entsprechende Aktion fest. Bei der Aktion „Abweisen“ werden Pakete mit einer Quelladresse, die zu den festgelegten Adressen gehört, verworfen. Umgekehrt werden Pakete bei der Aktion „Akzeptieren“ zugelassen.

Netzwerkauthentifizierung

SNMP v3

Das Fiery DFE unterstützt den neuesten SNMPv3-Standard und ermöglicht verschlüsselte Kommunikationspakete, um Vertraulichkeit, Nachrichtenintegrität und Authentifizierung zu gewährleisten.

Der Fiery Administrator kann zwischen drei SNMP-Sicherheitsebenen wählen: minimal, mittel und maximal. Auf diesen Ebenen werden Kennwörter mithilfe von Algorithmen wie SHA-1 oder SHA-256 gehasht, und die gesamte SNMP-Nachricht wird verschlüsselt. Zusätzlich kann der lokale Administrator Community-Namen für SNMP-Lese- und Schreibzugriffe sowie andere Sicherheitseinstellungen konfigurieren.

IEEE 802.1 x

802.1X ist ein IEEE-Standard für die portbasierte Netzwerkzugriffssteuerung, der sicherstellt, dass sich Geräte authentifizieren, bevor sie auf das lokale Netzwerk und dessen Ressourcen zugreifen. Auf Fiery DFEs kann 802.1X so konfiguriert werden, dass EAP-MD5 Challenge oder PEAP-MSCHAPv2 als anmeldeinformationsbasierte Authentifizierungsmethoden oder EAP-TLS für die zertifikatbasierte Authentifizierung verwendet werden. Fiery DFEs unterstützen nur Benutzerzertifikate (keine Gerätezertifikate) für die EAP-TLS-Authentifizierung. Die EAP-MD5 Challenge wird aus Gründen der Kompatibilität bereitgestellt und ist weniger sicher als PEAP-MSCHAPv2 und EAP-TLS.

Das Fiery DFE führt die 802.1X-Authentifizierung beim Start und immer dann durch, wenn die Netzwerkverbindung wiederhergestellt wird.

Netzwerkverschlüsselung

Internet Protocol Security (IPsec)

IPsec erhöht die Sicherheit der IP-basierten Kommunikation, indem jedes Paket auf der Netzwerkebene verschlüsselt und authentifiziert wird, wodurch Daten während der Übertragung in allen Anwendungen, die IP verwenden, geschützt werden. Für die Authentifizierung und den Aufbau der sicheren Verbindung zu einem anderen System auf Basis von IPsec verwendet das Fiery DFE einen vorinstallierten Schlüssel (PSK). Nachdem die Kommunikation über IPsec zwischen Client-Computer und dem Fiery DFE hergestellt wurde, werden alle Kommunikationsdaten sicher über das Netzwerk transferiert, auch Druckaufträge.

Es gibt Protokolle wie LPR, Port 9100, FTP, WSD und Harmony (das proprietäre Protokoll von Fiery), die für die Übermittlung von Druckaufträgen, Auftragsstatusaktualisierungen und Verwaltungsbefehle verwendet werden. Diese Protokolle durchlaufen keinen sicheren Kanal, daher sollten Organisationen, die Vertraulichkeit und Integritätsschutz für solche Funktionen benötigen, IPsec zwischen dem Client-Computer und dem Fiery DFE einsetzen.

HTTPS

Fiery DFEs verwenden HTTPS über TLS, um die webbasierte und API-Kommunikation zwischen Clients und Serverkomponenten zu sichern. Fiery DFEs unterstützen TLS 1.3 und TLS 1.2 und bieten starken kryptografischen Schutz und moderne Sicherheitsfunktionen. HTTPS ist für Verbindungen zu WebTools- und Fiery-APIs obligatorisch und stellt sicher, dass der über diese Schnittstellen übertragene administrative und betriebliche Datenverkehr während der Übertragung verschlüsselt und vor Abfangen oder Manipulation geschützt ist. Nicht die gesamte Client-Server-Kommunikation wird über HTTPS übertragen.

Zertifikatsverwaltung

Fiery DFEs bieten eine Schnittstelle zur Verwaltung von Zertifikaten, die während der TLS-Kommunikation verwendet werden. Fiery DFEs unterstützen X.509-Zertifikate im PEM-Format, codiert im Base64, unter Verwendung von RSA-Schlüsseln mit einer Länge von 4096, 3072 oder 2048 Bit.

Die Zertifikatsverwaltung ermöglicht dem Fiery Administrator folgende Aktionen:

- Selbstsignierte digitale Zertifikate erstellen.
- Ein Zertifikat und dessen assoziierten privaten Schlüssel zu einem Fiery DFE hinzufügen.
- Zertifikate von einer vertrauenswürdigen Zertifikatsstelle hinzufügen, durchsuchen, anzeigen und entfernen.

Selbstsignierte digitale Zertifikate bieten Verschlüsselung, aber keine automatische Vertrauensüberprüfung. Für sichere Bereitstellungen empfehlen wir die Verwendung von Zertifikaten, die von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt wurden, um eine ordnungsgemäße Identitätsüberprüfung zu gewährleisten.

Nachdem ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde, kann es in den WebTools unter „Configure“ auf das Fiery DFE hochgeladen werden.

Server Message Block (SMB)

SMBv1, das frühere Protokoll für die Datei- und Druckerfreigabe, ist auf Fiery DFEs aufgrund bekannter Sicherheitslücken deaktiviert. Fiery DFEs unterstützen stattdessen SMBv2 und SMBv3. SMB-Signaturen werden erzwungen, sodass alle Pakete digital signiert werden, um Mittelsmann-Angriffe zu verhindern. Wenn die SMB-Authentifizierung aktiviert ist, müssen Anwender einen gültigen Benutzernamen und ein Kennwort angeben, um auf freigegebene Ordner und Inhalte zugreifen zu können. Das Drucken oder Teilen von Dateien über SMB für ein Gastkonto kann auch durch Festlegen eines Kennworts in Fiery Configure eingeschränkt werden.

Hardwaresicherheit

Fiery DFEs sind auf Hardware-Sicherheit auf Unternehmensebene ausgelegt. Der Schutz sensibler Informationen ist nicht auf Softwarekontrollen beschränkt. Hardwarekomponenten spielen eine entscheidende Rolle bei der Aufrechterhaltung der Systemintegrität und der Vertraulichkeit von Daten. Die wichtigsten Hardwareelemente und ihre Sicherheitsmaßnahmen werden im Folgenden beschrieben.

Flüchtiger Speicher (RAM)

Fiery DFEs verwenden flüchtigen Speicher (RAM), um Daten während des aktiven Betriebs vorübergehend zu speichern. So mindern Sie das Risiko einer Offenlegung von Daten:

- Vertrauliche Informationen im Arbeitsspeicher werden sofort nach der Verwendung oder beim Herunterfahren des Systems gelöscht.
- Speicherbereinigungsverfahren werden angewendet, um zu verhindern, dass Restdaten bestehen bleiben.
- Der Zugriff auf den Arbeitsspeicher wird durch die vom Prozessor und Betriebssystem erzwungene Privilegientrennung eingeschränkt.

Nichtflüchtiger Speicher und Datenspeicher

Nichtflüchtiger Speicher, einschließlich Festplatten, Solid-State-Laufwerke (SSDs) und anderer persistenter Speicher, behält Daten auch dann bei, wenn das System ausgeschaltet ist. Zu den Sicherheitsmaßnahmen gehören:

- User Data Encryption (UDE) zum Schutz gespeicherter Daten.
- Sichere Löschmethoden, um sicherzustellen, dass sensible Daten nach dem Löschen nicht wiederhergestellt werden können.

Flash-Speicher

Flash-Speicher wird zum Speichern von Firmware, Konfigurationsdateien und Systemeinstellungen verwendet. Folgendes wird unternommen, um die Sicherheit zu gewährleisten:

- Die Firmware wird digital signiert, um Manipulationen zu verhindern.
- Firmware-Updates werden vor der Installation anhand kryptografischer Prüfsummen verifiziert.
- Schreibschutzmechanismen verhindern unbefugte Änderungen während der Laufzeit.

CMOS und NVRAM

Kritische Systemparameter, wie Hardwarekonfigurationen und Boot-Einstellungen, werden im CMOS und im nichtflüchtigen RAM (NVRAM) gespeichert. So sichern Sie diese Daten:

- Der Zugriff ist auf autorisierte administrative Prozesse beschränkt.
- Sicheres Booten stellt sicher, dass nur vertrauenswürdige Firmware und Startkomponenten geladen werden.
- Kritische NVRAM-Variablen werden durch Integritätskontrollen vor Beschädigung und unbefugter Änderung geschützt.

Speicherlaufwerke

Fiery DFEs verwenden Speicherlaufwerke für das Host-Betriebssystem, Systemdateien, Auftragsspooling, Protokolle und temporäre Dateien.

Die folgenden Sicherheitsfunktionen werden bereitgestellt, um Kundendaten zu schützen:

- Verschlüsselung auf Laufwerksebene.
- Zugriffssteuerungslisten (Access Control Lists, ACLs), um nicht autorisierte Lese-/Schreibvorgänge einzuschränken.
- Laufwerkssicherheitskits (optional für externe Fiery DFEs) ermöglichen es, Laufwerke während des normalen Betriebs sicher zu sperren.

Physische Ports

Physische Ports wie USB, Netzwerkschnittstellen und Serviceanschlüsse sind potenzielle Vektoren für unbefugten Zugriff. Die Fiery Hardwaresicherheit begegnet diesem Risiko durch:

- Deaktivieren nicht verwendeter Ports durch Hardware- und Firmware-Steuerelemente.
- Einschränken des Zugriffs auf externe Geräte durch administrative Steuerelemente und Systemkonfiguration.
- Protokollieren sicherheitsrelevanter Ereignisse mit kritischen physikalischen Schnittstellen.

Durch die Integration dieser Hardware-Sicherheitsmaßnahmen mit Software- und Netzwerkschutzmaßnahmen bieten Fiery DFEs eine umfassende Defense-in-Depth-Strategie, die die Vertraulichkeit, Integrität und Verfügbarkeit sensibler Daten in Druckumgebungen sicherstellt.

Systemintegrität und sichere Updates

Die Aufrechterhaltung der Systemintegrität ist für die Gewährleistung der Sicherheit von größter Bedeutung. Fiery DFEs bieten folgende Unterstützung:

- Protokolle des Sicherheitsaudits
- Sicheres Booten: Stellt sicher, dass nur vertrauenswürdige Software geladen wird.
- Digital signierte Updates: Verhindert die Manipulation von Softwareupdates.
- Automatisierte Verwaltung von Sicherheitsupdates: Vereinfacht das Anwenden von Sicherheitsupdates.

Protokoll des Sicherheitsaudits

Administratoren mit erweiterten Berechtigungen können auf die im Sicherheitsüberwachungsprotokoll aufgezeichneten Sicherheitsereignisse zugreifen und diese überprüfen. Dieses Protokoll ist standardmäßig aktiviert.

Jedes Sicherheitsereignis wird als Information, Warnung oder Fehler eingestuft. Der Administrator erhält keine Warnungen oder Benachrichtigungen. Stattdessen wird ihnen ein statisches Protokoll angezeigt.

Die Protokolle sind so formatiert, dass sie mit SIEM(Security Information and Event Management)-Tools kompatibel sind, die häufig für die Protokollsammlung und -analyse verwendet werden. Alle erfassten Ereignisdaten entsprechen den in NIST SP 800-53 beschriebenen Standards.

Der Fiery Administrator kann auf das Protokoll des Sicherheitsaudits zugreifen, ohne dass FIERY eingreifen muss. Protokolle für Linux-basierte DFEs werden im Syslog-Format (RFC 5424 oder RFC 3164) bereitgestellt. Bei Windows-basierten DFEs werden Protokolle im standardmäßigen Windows EVTX-Format gespeichert und können vom Windows-Ereignisprotokoll-Manager und vielen verfügbaren gewerblichen Lösungen, die die Windows-Ereignisprotokoll-API verwenden, gelesen werden. Linux-basierte Fiery DFEs bieten die Möglichkeit, Protokolle an ein zentrales Erfassungssystem wie Syslog weiterzuleiten.

Sicherheitsprotokolle werden basierend auf der zugewiesenen lokalen Speicherkapazität bis zu einer vordefinierten Obergrenze aufbewahrt. Bei Windows-basierten Fiery DFEs werden die ältesten Einzelereignisse nach Bedarf entfernt. Auf Linux-basierten Fiery DFEs werden Überwachungsprotokolle nach Dateigröße rotiert. Rotierte Protokolldateien werden bis zur konfigurierten Rotationsanzahl beibehalten, danach werden die ältesten rotierten Dateien gelöscht.

Sicheres Booten

Sicheres Booten schützt das Betriebssystem während des Starts, indem nur vertrauenswürdige, digital signierte Komponenten geladen werden können. Bei unterstützten Windows-basierten Fiery DFEs verhindert diese Funktion, dass nicht autorisierter oder bösartiger Code beim Booten ausgeführt wird, wodurch das Risiko einer Kompromittierung verringert wird. Damit die Funktion „Sicheres Booten“ wirksam wird, muss sie in den BIOS-Einstellungen aktiviert und eingeschaltet werden.

Digital signierte Updates

Fiery DFEs verwenden digital signierte Updates, um die Integrität und Authentizität aller Software- und Firmware-Installationen sicherzustellen. Jedes Update wird von Fiery oder autorisierten Partnern kryptografisch signiert, sodass das DFE prüfen kann, ob der Inhalt verändert oder manipuliert wurde. Dieser Prozess schützt vor der Einführung von bösartigem Code und garantiert, dass nur vertrauenswürdige Updates angewendet werden, wodurch die Sicherheit und Zuverlässigkeit des Systems gewährleistet wird.

Automatisierte Verwaltung von Sicherheitsupdates

Zeitnahe Softwareupdates sind für den optimalen Betrieb von Fiery DFEs unabdingbar. Die Installation aller Softwaresicherheitsupdates ist wichtig, um Fiery DFEs in einer bestimmten Druckumgebung zu schützen.

Updates für Fiery System lädt die Sicherheitsupdates herunter und installiert sie, wenn die Option auf dem Fiery DFE aktiviert ist. Standardmäßig ist diese Option aktiviert und wir empfehlen Kunden, sie aktiviert zu lassen.

Sicherheitslücken des Betriebssystems Microsoft® Windows™ werden in diesem Dokument nicht beschrieben, da diese direkt von Microsoft verwaltet und als **Windows-Updates** an die Kunden verteilt werden, wenn sie verfügbar sind.

Um Sicherheitsbedenken oder Schwachstellen zu beheben, die Auswirkungen auf die Fiery Kern-Hardwarekomponenten, darunter Motherboard, Prozessor und Firmware, haben könnten, arbeitet FIERY eng mit den Herstellern zusammen, um die erforderlichen Sicherheitsupdates zu erhalten. Diese Sicherheitsupdates werden anschließend den Kunden bereitgestellt, wenn dies erforderlich ist.

Hinweis: Fiery Softwareupdates werden unter Verwendung des sicheren Hash-Algorithmus (SHA-2) digital signiert, um eine unzulässige Änderung zu verhindern, einschließlich der Einfügung von Schadsoftware.

Fiery DFE Sicherheitsupdates für Software

Die zeitnahe Installation von Updates und Patches ist für den optimalen Betrieb des Fiery DFE unabdingbar. Durch die Anwendung der neuesten Fiery DFE Softwaresicherheitsupdates wird die Systemintegrität gewährleistet, Schwachstellen werden minimiert und die Einhaltung der Branchensicherheitsstandards gewahrt.

Das Fiery DFE-Sicherheitsteam überwacht und verfolgt Sicherheitslücken sorgfältig über ein umfassendes Netzwerk vertrauenswürdiger und zuverlässiger Quellen, wie z. B.:

- Warnungen und Hinweise der US-amerikanischen Behörde für Cybersicherheit und Infrastruktursicherheit (CISA)
- Nationale Schwachstellendatenbank des US-amerikanischen National Institute for Standards and Technology (NIST)
- CVE(Common Vulnerabilities and Exposures)-Datensätze
- Berichte und Hinweise des CERT Coordination Center (CERT/CC) zu Software- und Hardware-Schwachstellen
- Regionale Regierungs- und Regulierungsbehörden
- Sicherheitshinweise von Software- und Hardwareanbietern

Fiery priorisiert Sicherheitskorrekturen basierend auf dem Schweregrad (Kritisch, Hoch, Mittel und Niedrig), der anhand des Common Vulnerability Scoring System (CVSS) bestimmt wird. Diese Korrekturen werden nach Erhalt der entsprechenden Genehmigung durch den OEM(Original Equipment Manufacturer)-Partner freigegeben. Nach der Genehmigung werden Fiery Softwaresicherheitsupdates zum Download zur Verfügung gestellt. Alle Fiery Softwareupdates werden unter Verwendung des sicheren Hash-Algorithmus (SHA-2) digital signiert, um eine unzulässige Änderung zu verhindern, einschließlich der Einfügung von Schadsoftware.

Wenn aktiviert, lädt Updates für Fiery System Sicherheitsupdates herunter und installiert sie automatisch auf dem Fiery DFE. Standardmäßig ist diese Option aktiviert, und wir empfehlen Kunden dringend, den aktiven Status beizubehalten.

Compliance und bewährte Verfahren

Robuste Sicherheitsimplementierungen entsprechen grundlegenden Industriestandards und regulatorischen Rahmenbedingungen, einschließlich:

- DSGVO, EU-Datenschutzgesetz
- FIPS 140-3
- NIST 800-88. Richtlinien für die Medienbereinigung (nur FS800 Pro)
- NIST 800-52. Richtlinien für die Auswahl, Konfiguration und Verwendung von TLS-Implementierungen (Transport Layer Security)
- Zertifizierung des US DOD Cybersecurity Maturity Model (CMMC). Stufe 2: Umfassender Schutz kontrollierter nicht klassifizierter Informationen (CUI) (nur FS800 Pro)
- NIST 800-193. Richtlinien zur Ausfallsicherheit der Plattform-Firmware (nur FS800 Pro)
- NIST 800-53. Sicherheits- und Datenschutzkontrollen für Informationssysteme und Organisationen
- Common Criteria-Schutzprofil für allgemeine Betriebssysteme (nur FS800 Pro)

Um die Sicherheitslage zu verbessern, sind IT-Administratoren für die Implementierung der folgenden Maßnahmen verantwortlich:

- Regelmäßiges Anwenden von Sicherheitsupdates
- Erzwingen robuster Authentifizierungsrichtlinien
- Durchführung regelmäßiger Sicherheitsaudits
- Implementieren der Netzwerksegmentierung für Druckumgebungen

Richtlinien für die sichere Fiery DFE-Konfiguration

Fiery Administratoren können diese Richtlinien befolgen, um die Sicherheit bei der Konfiguration des Fiery DFE zu erhöhen:

Administratorkennwort ändern

Fiery DFEs werden werksseitig mit einem Standardkennwort für das Administratorkonto ausgeliefert. Mit diesem Kennwort können Sie sowohl lokal als auch über einen Remote-Client uneingeschränkten Zugriff auf das Fiery DFE erhalten. Dieser Zugriff umfasst unter anderem:

- Dateisystem (nur Fiery DFEs unter Windows)
- System-Sicherheitseinstellungen
- Anwendungseinstellungen
- Registrierungseinträge

Wir empfehlen Ihnen dringend, das Fiery Administrator-Standardkennwort direkt nach der Installation und in regelmäßigen Abständen gemäß den Sicherheitsrichtlinien Ihrer Organisation zu ändern. Das Fiery Administratorkennwort muss innerhalb der Fiery Plattform geändert werden.

Bewährte Verfahren für einen sicheren und effizienten Betrieb

- Beschränken Sie SNMP auf Version 3, um maximale Sicherheit zu gewährleisten.
- Deaktivieren Sie WSD für die Auftragsübergabe, um die Verwendung in Druck-Workflows zu verhindern.
- Deaktivieren Sie Windows-Druckprotokolle (LPR, Port 9100, IPP), wenn diese nicht explizit vorgeschrieben sind.
- Aktivieren Sie die TCP/IP-Port-Filterung, um ungenutzte Ports zu blockieren und Risiken zu verringern.
- Schließen Sie die Ports 137–139 und 445, wenn sie nicht für Windows-Druckfunktionalität oder Dateifreigabe benötigt werden.
- Deaktivieren Sie HTTP auf Port 80, um eine ungesicherte Kommunikation zu verhindern.
- Aktivieren Sie die Option „Sicheres Drucken“, damit nur der Auftragsbesitzer Druckaufträge freigeben kann.

Hochsicherheitsumgebungen

Administratoren mit erweiterten Berechtigungen können mühelos Hochsicherheitseinstellungen konfigurieren, indem sie das Hochsicherheitsprofil auswählen, das in **WebTools** > **Configure** > **Security** verfügbar ist.

Schlussfolgerung

Fiery DFEs sind zwar mit robusten Sicherheitsfunktionen ausgestattet, aber nicht für den Internetzugang vorgesehen. Sie sollten in einer sicheren Netzwerkumgebung eingesetzt werden, wobei der Zugriff sorgfältig vom Netzwerkadministrator kontrolliert wird. Fiery DFEs sind so konzipiert, dass sie den neuesten Branchenstandards entsprechen und Sicherheit auf Unternehmensebene bieten, um Druckumgebungen vor sich entwickelnden Cyberbedrohungen zu schützen. Administratoren können Compliance sicherstellen und sensible Daten schützen, indem sie die Sicherheitsfunktionen von Fiery in vollem Umfang nutzen.

Neu in FS800, FS800 Pro

- Die Kernsystemmodule wurden aktualisiert, um Sicherheitslücken zu schließen.
- Remotedesktopverbindungen mit Windows 11-basierten Fiery DFEs unterstützen TLS 1.3 und bieten erweiterte Verschlüsselung und verbesserte Verbindungssicherheit.