Fiery FS700 Pro/FS700 servers

Security White Paper

45266128

8. Dezember 2025

Inhalt

Einführung

Dieses Dokument bietet eine Übersicht über die Sicherheitsfunktionen von Fiery Servern. Ziel ist es, IT-Administratoren und Sicherheitsexperten darüber zu informieren, wie Fiery Lösungen vertrauliche Druckumgebungen absichern. In diesem Dokument werden die Prinzipien und Mechanismen beschrieben, die in Fiery Servern zum Schutz von Daten, zur Verbesserung der Netzwerksicherheit und zur Aufrechterhaltung der Systemintegrität verwendet werden.

Sicherheitsgrundsätze

Fiery servers 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 Server unterstützen u. a. die folgenden Authentifizierungsmethoden:

- Rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC)
- Integration von LDAP und Active Directory
- Multi-Faktor-Authentifizierung (MFA), implementiert über Einmaliges Anmelden (SSO)

Anwenderauthentisierung

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

- Authentifizieren eines Anwenders
- Autorisieren von Aktionen, die auf den Berechtigungen des Anwenders basieren

Der Fiery server unterstützt die folgenden drei Anwenderauthentisierungsmethoden:

- Lokale Authentifizierung für Anwender, die auf dem Fiery Server 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

Der Fiery-Server autorisiert Aktionen von Anwendern in Abhängigkeit von ihrer Gruppenzugehörigkeit. Jeder Gruppe sind bestimmte Berechtigungen zugewiesen, z. B. das Drucken in Farbe oder in Graustufen. 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 Graustufen drucken: erlaubt Gruppenmitgliedern, Aufträge in Graustufen zu drucken. Wenn der Anwender nicht über diese Berechtigung verfügt, druckt der Fiery Server den Auftrag nicht. Wenn es sich bei dem Auftrag um einen Farbauftrag handelt, wird er in Graustufen gedruckt.
- In Farbe und Graustufen drucken: erlaubt Gruppenmitgliedern, Aufträge mit Vollzugriff auf die Farb- und Graustufendruckfunktionen des Fiery Server zu drucken. Ohne diese Berechtigung oder die Berechtigung zum Drucken in Graustufen wird der Druckauftrag nicht gedruckt und Anwender können Aufträge nicht über FTP übermitteln (nur bei Farbgeräten).

- Fiery Mailbox: erlaubt Gruppenmitgliedern jeweils eine eigene Mailbox. Der Fiery Server 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 Server): 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 Server-Software interagiert mit eindeutigen Benutzertypen, die sich von Windows-Benutzern oder -Rollen unterscheiden. Fiery Administratoren sollten nach der Erstinstallation umgehend alle Standardkennwörter ändern. Der Zugriff auf den Fiery Server durch Kennworte muss strikt erzwungen 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-Servers, 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 Servereinstellungen und das Löschen von Auftragsprotokollen.
- Druckproduktionsmitarbeitende (nur Fiery XB Server): Verwalten Aufträge auf der Druckmaschine mit bestimmten, vom Administrator hinzugefügten Berechtigungen.
- Fiery Dienst-Admin (nur Windows-Server): Ein ausgeblendetes Admin-Konto für die Installation des vertrauenswürdigen Zertifikats, kann sich nicht am Fiery Server 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 Server-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

Der Fiery Server 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.

Der Fiery Server 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 FS700 Pro Server 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 server mit ihren bestehenden Entra-ID-Anmeldeinformationen anmelden.

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

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

Datensicherheitsmaßnahmen

Um vertrauliche Informationen zu schützen, implementieren Fiery Server Folgendes:

Verschlüsselte Speicherung: Schützt Druckaufträge und Konfigurationsdaten

Die Verschlüsselung sensibler Kundendaten stellt sicher, dass alle Kennwörter und entsprechende Konfigurationsinformationen sicher auf dem Fiery Server 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 Server entfernt wird. Die Verschlüsselung von Anwenderdaten kann auf Windows-basierten Fiery Servern aktiviert oder deaktiviert werden. Bei Linux-basierten Fiery Servern 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 Server bieten auch die Möglichkeit, das Boot-Laufwerk zu verschlüsseln, das das Betriebssystem enthält. Diese Verschlüsselung dient dazu, Offline-Angriffe auf den Fiery Server 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.

Wenn bei Linux-basierten FS700 Fiery Servern ein Auftrag gelöscht wird, wird jede Auftragsquelldatei dreimal mit einem Algorithmus, der auf der US-amerikanischen Datenlöschmethode DoD 5220.22-M basiert, überschrieben.

Diese Funktion wird auf integrierten Fiery Servern mit den Hardwareplattformen E600 und LX Pro nicht unterstützt. Diese Plattformen speichern Dokumentdaten auf einem Solid-State-Laufwerk (SSD), das mit AES-256-Verschlüsselung geschützt ist. Diese Verschlüsselung ist immer aktiviert und kann nicht deaktiviert werden.

Windows-basierte FS700 Pro Server 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 Fiery XB Plattformen oder für Anwenderdaten, die auf SSDs gespeichert sind, nicht unterstützt.

Arbeitsabläufe	Sicheres Löschen
Auf dem Fiery server Festplattenlaufwerk gespeicherte Aufträge; Funktion „Sicheres Löschen**eingeschaltet**	Ja
Auf dem Fiery server Festplattenlaufwerk gespeicherte Aufträge; Funktion „Sicheres Löschen**ausgeschaltet**	Nein

Arbeitsabläufe	Sicheres Löschen
Aufträge, die vom Fiery server empfangen und gelöscht werden, nachdem die Funktion „Sicheres Löschen**eingeschaltet** wird	Ja
Aufträge, die vom Fiery server empfangen und gelöscht werden, bevor die Funktion „Sicheres Löschen**eingeschaltet** wird	Nein
Kopien von Aufträgen, die an einen anderen Fiery server 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 server Festplattenlaufwerk gespeichert werden	Nein
Teile eines Auftrags, die während des Festplattenaustauschs oder der Festplatten-Caching-Vorgänge auf die Festplatte des Fiery server geschrieben werden	Nein
Auftragsprotokolleinträge	Nein
Auftragsprotokolleinträge nach der Ausführung der Funktion „Serverdaten löschen“	Ja
Fiery server wird ausgeschaltet, bevor das Löschen des Auftrags abgeschlossen ist	Nein
Defragmentierung des Fiery server Festplattenlaufwerks vor dem Löschen eines Auftrags	Nein

Netzwerksicherheit

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

- IP-Filterung und Portverwaltung
- Firewall-Konfiguration
- Unterstützung für SNMP v3 für sichere Tools zur Netzwerküberwachung und -verwaltung

Unterstützte Netzwerkprotokolle

FS700/FS700 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 Server)
- **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 aktivieren und deaktivieren. Das Deaktivieren eines Ports verhindert effektiv externe Verbindungen, für die die Nutzung dieses bestimmten Ports erforderlich ist.

Eingehende Ports

Fiery Server überwachen eingehende Netzwerkverbindungen, sodass nur autorisierter Datenverkehr auf den Server zugreifen kann und er vor unbefugtem Zugriff oder Angriffen geschützt ist.

TCP	UDP	Portname	Abhängige Dienste
20–21		FTP	FTP
80		HTTP	WebTools, IPP

TCP	UDP	Portname	Abhängige Dienste
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, IPP/s
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 Server)
3702	3702	WS-Discovery	WSD (Web Services for Devices). Ermöglicht die Erkennung von und das Drucken auf dem Fiery Server über WSD.
	4500	IPSec NAT-Durchgänge	IPsec
	5353	Multicast DNS (mDNS)	Bonjour
6310		DMP-Port	Direkter mobiler Druck
8010		FIERY Ports	JDF
8021–8022		FIERY Ports	Fiery Harmony, Fiery HotFolders und Fiery Command WorkStation
8090		FIERY Ports	OFA
9100–9103		Druckport	Port 9100
	9906	FIERY Ports	Harmony-Erkennung
21030		FIERY Ports	Fiery Image Viewer

Hinweis: Die IPSec-Ports (500 und 4500) sind nur für FS700 (Linux-basierte Fiery Server) 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 Server bereitgestellten unterschiedlichen abhängigen Dienste können vom Fiery Administrator ebenfalls einzeln aktiviert und deaktiviert werden.

Ausgehende Ports

Fiery Server 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	Updates für Fiery System, JDF, PrintMe und andere Cloud-Kommunikation	Standard
161, 162	SNMP	In Dual-IP-Konfiguration
21	Scan für FTP	Ein-Konfiguration
123	NTP	Ein-Konfiguration
389/636	LDAP-Dienste	Ein-Konfiguration
445	Scannen nach SMB/JobLog für SMB/JDF allgemeine globale Ressourcen	Ein-Konfiguration
500/4500	IPSEC	Ein-Konfiguration
8080/8443	HTTP/HTTPS/FTP-Proxy-Port	Ein-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	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
LINQ	https://ews.fiery.com	443	Azure	Analysen

Fiery Dienst/ Anwendung	Vollqualifizierter Domänenname	Port	Serverstandort	Nutzungshinweise
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
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	

IP-Filterung

Mit der IP-Filterung kann der Administrator Verbindungsanfragen an den Fiery Server 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

Der Fiery Server 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 Servern kann 802.1X so konfiguriert werden, dass EAP-MD5 Challenge oder PEAP-MSCHAPv2 für die serverbasierte Authentifizierung oder EAP-TLS für die zertifikatbasierte Authentifizierung für erhöhte Sicherheit verwendet wird. Fiery Server unterstützen nur das Anwenderzertifikat (nicht das Gerätezertifikat) für die auf dem EAP-TLS-Zertifikat basierende Authentifizierung.

Der Fiery Server nimmt die Authentifizierung beim Systemstart sowie immer dann vor, wenn die Verbindung getrennt und neu hergestellt 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 Authentifzierung und den Aufbau der sicheren Verbindung zu einem anderen System auf Basis von IPsec verwendet der Fiery Server einen vorinstallierten Schlüssel (PSK). Nachdem die Kommunikation über IPsec zwischen Client-Computer und Fiery Server hergestellt wurde, werden alle Kommunikationsdaten sicher über das Netzwerk transferiert, auch Druckaufträge.

HTTPS

Fiery Server erzwingen die sichere Kommunikation zwischen Clients und Serverkomponenten mithilfe von HTTPS über TLS. Dadurch wird sichergestellt, dass alle übertragenen Daten – wie Druckaufträge, Aktualisierungen des Auftragsstatus und Administratorbefehle – während der Übertragung verschlüsselt werden, um sie vor Abfangen oder Manipulationen zu schützen. Fiery Server unterstützen TLS 1.3 und TLS 1.2 und bieten damit einen starken kryptografischen Schutz und moderne Sicherheitsfunktionen. HTTPS ist für Verbindungen zu WebTools und Fiery APIs zwingend erforderlich, um sicherzustellen, dass administrativer und betrieblicher Datenverkehr sicher übertragen wird.

Zertifikatsverwaltung

Fiery Server bieten eine Schnittstelle zur Verwaltung von Zertifikaten, die während der TLS-Kommunikation verwendet werden. Fiery Server unterstützen X.509-Zertifikate im PEM-Format, codiert in 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 Server 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 den Fiery Server hochgeladen werden.

Server Message Block (SMB)

SMBv1, das frühere Protokoll für die Datei- und Druckerfreigabe, ist auf Fiery Servern aufgrund bekannter Sicherheitslücken deaktiviert. Fiery Server 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 Server sind mit Blick auf Hardware-Sicherheit auf Unternehmensniveau konzipiert. 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 Server 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.
- Sichere Boot-Mechanismen stellen sicher, dass nur vertrauenswürdige Firmware-Lese- und Schreibvorgänge in diesen Bereichen erfolgen.
- Kritische NVRAM-Variablen werden gesichert und einer Integritätsprüfung unterzogen, um eine Beschädigung oder böswillige Änderung zu verhindern.

Speicherlaufwerke

Fiery Server verwenden Speicherlaufwerke, um das Betriebssystem und Systemdateien zu speichern. Diese Laufwerke werden auch für das Spoolen von Aufträgen, für Protokolle und für temporäre Dateien verwendet.

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 Server), die die Systemsicherheit erhöhen, indem sie es Anwendern ermöglichen, Serverlaufwerke 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 auf Hardware- oder Firmware-Ebene.
- Erfordernis einer Administratorberechtigung für das Verbinden externer Geräte.
- Überwachung und Protokollierung aller Interaktionen mit kritischen physischen Schnittstellen.

Durch die Integration dieser Hardware-Sicherheitsmaßnahmen mit Software- und Netzwerkschutzmaßnahmen bieten Fiery Server 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 Server 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 Server werden im Syslog-Format (RFC 5424 oder RFC 3164) bereitgestellt. Bei Windows-basierten Servern 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-Server bieten die Möglichkeit, Protokolle an ein zentrales Erfassungssystem wie Syslog weiterzuleiten.

Sicherheitsprotokolle werden basierend auf der zugewiesenen lokalen Speicherkapazität aufbewahrt. Wenn die Protokollgröße den vordefinierten Speicherplatz überschreitet (400 MB), werden ältere Ereignisse automatisch gelöscht.

Sicheres Booten

Diese Funktion stellt die Integrität von Betriebssystemdateien während des Starts sicher, indem nur digital signierte und vertrauenswürdige Komponenten geladen werden können. Auf Fiery Servern blockiert dies die Ausführung von nicht autorisiertem oder bösartigem Code während des Bootens, wodurch die Sicherheit erhöht und das Risiko einer Kompromittierung verringert wird. Standardmäßig ist „Sicheres Booten“ deaktiviert.

Digital signierte Updates

Fiery Server 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 der Server 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

Die zeitnahe Installation von Updates und Patches ist für den optimalen Betrieb der Fiery Server unabdingbar. Die Installation aller Softwaresicherheitsupdates ist wichtig, um Fiery Server in einer bestimmten Druckumgebung zu schützen.

Fiery System Update lädt Sicherheitsupdates herunter und installiert sie, wenn die Option auf dem Fiery Server 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.

Sicherheitsupdates für Fiery Server-Software

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

Das Fiery Server 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 Fiery System Update Sicherheitsupdates herunter und installiert sie automatisch auf dem Fiery Server. 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
- ISO/IEC 27001 (nur FS700 Pro)
- FIPS 140-2
- NIST 800-88. Richtlinien für die Medienbereinigung (nur FS700 Pro)
- NIST 800-52. Richtlinien für die Auswahl, Konfiguration und Verwendung von TLS-Implementierungen (Transport Layer Security)
- NIST 800-171. Schutz kontrollierter, nicht klassifizierter Informationen in nichtstaatlichen Systemen und Organisationen (nur FS700 Pro)
- Zertifizierung des US DOD Cybersecurity Maturity Model (CMMC). Stufe 2: Umfassender Schutz kontrollierter nicht klassifizierter Informationen (CUI) (nur FS700 Pro)
- NIST 800-193. Richtlinien zur Ausfallsicherheit der Plattform-Firmware (nur FS700 Pro)
- NIST 800-53. Sicherheits- und Datenschutzkontrollen für Informationssysteme und Organisationen
- Common Criteria-Schutzprofil für allgemeine Betriebssysteme (nur FS700 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 Server-Konfiguration

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

Administratorkennwort ändern

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

- Dateisystem (nur Fiery Server 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 Server 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 Server sind so konzipiert, dass sie den neuesten Branchenstandards entsprechen und Unternehmenssicherheit 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 FS700, FS700 Pro

- Die Kernsystemmodule wurden aktualisiert, um Sicherheitslücken zu schließen.
- Die E-Mail-Funktionalität wurde eingestellt, um E-Mail-Angriffe zu verhindern und die Einhaltung von Sicherheitsbestimmungen zu gewährleisten.
- Die gesamte Kommunikation mit dem Fiery Server kann nun mit TLS 1.3 verschlüsselt werden. Remotedesktopverbindungen mit Fiery Servern, auf denen Windows 10 ausgeführt wird, unterstützen derzeit TLS 1.2.
- Unterstützung für TLS 1.3 wurde für die folgenden Fiery Anwendungen und Module hinzugefügt:
  - Lizenzierungsserver und Client-Komponenten
  - IPP-Proxy: erforderlich für Microsoft Universal Print
  - Netzwerkauthentifizierungsprotokoll 802.1x
  - EFI LINQ: Wird für die Fiery Server-Absturzberichterstattung verwendet
  - JDF
  - System-Update
  - FCC – Fiery Cloud Connector
- Die auf Linux-Servern verwendeten IPsec-Tools wurden durch neuere, sicherere Tools ersetzt.
- Unterstützung für Advanced Encryption Standard (AES) für SNMPv3-Kommunikation wurde hinzugefügt und AES 128 wurde als neuer Standard festgelegt:
  - AES 128 (Standard)
  - AES 192 (Benutzer kann über Configure auswählen)
  - AES 256 (Benutzer kann über Configure auswählen)
  - DES wird weiterhin unterstützt, obwohl es nicht mehr die Standardoption ist. Benutzer können sie bei Bedarf auswählen.