Fiery FS500 Pro/FS500 servers

Fiery Security White Paper

45234236

3. Juli 2022

Inhalt

Dokumentübersicht

Dieses Dokument enthält Details darüber, wie Sicherheitstechnologie und Funktionen in Fiery FS500 Pro/FS500 servers implementiert werden, und beschreibt Hardwaresicherheit, Netzwerksicherheit, Zugriffssteuerung, Betriebssysteme und Datensicherheit. Ziel des Dokuments ist es, unseren Kunden zu helfen, die Fiery Platform-Sicherheitstechnologie mit ihren eigenen Richtlinien zu kombinieren, um ihre spezifischen Sicherheitsanforderungen zu erfüllen.

Terminologiekonventionen

In diesem Dokument wird die folgende Terminologie verwendet, um Bezug auf Fiery FS500 Pro/FS500 servers, Drucker und Fiery Anwendungen zu nehmen.

Begriff oder Konvention	**Bezieht sich auf**
Fiery server	Fiery FS500 Pro/FS500 servers
Drucker	Drucker, Kopierer, Digitaldruckmaschine, Druckmaschine oder Ausgabegerät
Configure	Fiery Configure
Command WorkStation	Fiery Command WorkStation
WebTools	Fiery WebTools
QuickTouch	Die Software Fiery QuickTouch wird auf dem LCD-Bedienfeld des Fiery Servers ausgeführt

EFI Sicherheitsphilosophie

EFI ist bewusst, dass Sicherheit eines der Hauptanliegen von Organisationen und Unternehmen weltweit ist. Unsere Produkte werden häufig mit verbesserten Sicherheitsfunktionen erweitert, die zum Schutz Ihrer Unternehmensunterlagen vorgesehen sind. EFI Fiery servers werden unter Sicherheitsaspekten als Kernkomponente zum Schutz der Systemdaten entwickelt und hergestellt, wenn sich diese im Ruhezustand befinden, bei der Übertragung und Verarbeitung.

In enger Zusammenarbeit mit unseren globalen EFI Partnern und Lieferanten fühlen wir uns verpflichtet, unsere Kunden kontinuierlich mit Lösungen zu unterstützen, da immer wieder Bedrohungen auftreten. Um die Sicherheit des Gesamtsystems zu erreichen, empfehlen wir Endbenutzern, Fiery Sicherheitsfunktionen mit den organisationseigenen Sicherheitsrichtlinien und bestimmten bewährten Branchenverfahren zu kombinieren, z. B. sichere Kennwörter und strikte physische Sicherheitsverfahren.

EFI Sicherheitsziele

EFI hat sich bei der Umsetzung von Sicherheitsmaßnahmen für den Fiery server die folgenden Ziele gesetzt:

- **Datensicherheit**: Keine unbefugte Offenlegung von Daten während der Verarbeitung, Übertragung (bei der Übertragung) oder Speicherung (im Ruhezustand).
- **Verfügbarkeit**: Leistung wie vorgesehen, frei von unbefugter Manipulation.
- **Zugriffssteuerung**: Kein Denial of Service für autorisierte Benutzer.
- **IT-freundliche Wartung**: Automatische Benachrichtigungen und Downloads, wenn Sicherheitsupdates verfügbar sind.
- **Einhaltung**: Unterstützung der Branchenvorschriften und Sicherheitsframeworks.

Sicherheitsupdates für Fiery Software

Dieser Abschnitt gibt einen allgemeinen Überblick über den Prozess der Fiery server Software-Sicherheitsaktualisierung. Microsoft® Windows™ OS-Sicherheitslücken werden nicht beschrieben, da diese direkt von Microsoft bearbeitet und als Windows-Updates geliefert werden, wenn sie verfügbar sind. Bei Sicherheitsproblemen oder Schwachstellen, die Auswirkungen auf die Fiery Hardwarekernkomponenten, z. B. Motherboard, Prozessor, BIOS usw., haben könnten, arbeitet EFI eng mit den Herstellern zusammen, um die erforderlichen Sicherheitsupdates zu erhalten.

- EFI verfolgt das wöchentliche US-CERT Cyber Security Bulletin von der Cybersecurity and Infrastructure Security Agency (CISA). Das Bulletin enthält eine Zusammenfassung der neuen Schwachstellen, die in den letzten Wochen vom National Institute of Standards and Technology (NIST) aus der National Vulnerability Database (NVD) erfasst wurden. Die Schwachstellen basieren auf dem Namensstandard Common Vulnerabilities and Exposures (CVE, Gemeinsame Schwachstellen und Enthüllungen) und sind gemäß dem Schweregrad (hoch, mittel und niedrig) gegliedert, der anhand des Common Vulnerability Scoring System (CVSS) bestimmt wird.
- EFI stellt so schnell wie möglich Sicherheitskorrekturen für jede Fiery server Plattform bereit.
- Fiery Softwaresicherheitsupdates werden zur Genehmigung an bestimmte EFI Partner gesendet.
- Wenn Sie von den Partnern genehmigt wurden, werden Fiery Softwaresicherheitsupdates zum Download zur Verfügung gestellt.
- Fiery System Update lädt die Sicherheitsupdates herunter und installiert sie, wenn die Option auf dem Fiery server aktiviert ist. Standardmäßig ist diese Option aktiviert und wir empfehlen Kunden, diese aktiviert zu lassen.

Zeitnahe Softwareupdates sind für den optimalen Betrieb der Fiery servers unabdingbar. Die Installation der Sicherheitsupdates für die Software der Fiery und Windows-Betriebssysteme ist wichtig, um Fiery servers in einer bestimmten Druckumgebung zu schützen.

Hinweis: Alle Fiery Updates oder Farbfelder sind digital mit „SHA-2“ signiert.

Konfigurieren der Fiery server Sicherheitsfunktionen

Configure ist das wichtigste Tool zum Konfigurieren der Sicherheitsfunktionen auf Fiery servers. Fiery Administratoren können auf Configure über Command WorkStation oder WebTools zugreifen.

Hinweis: Benutzer müssen über Administratorberechtigungen verfügen, um auf Configure zuzugreifen.

Weitere Informationen zum Konfigurieren des Fiery server finden Sie unter Richtlinien für die sichere Fiery Server-Konfiguration auf Seite 32.

Hardwaresicherheit

Die Sicherheit der Fiery server Hardware konzentriert sich auf die Vermeidung von Datenverlusten bei Stromausfall und unbefugtem Zugriff auf die Daten, die sich auf einem Speichergerät befinden.

Flüchtiger Speicher

Daten, die in den flüchtigen Arbeitsspeicher geschrieben werden, sind nur verfügbar, wenn die Stromversorgung eingeschaltet ist. Wenn die Stromversorgung ausgeschaltet wird, werden alle Daten gelöscht.

Weitere Informationen finden Sie im Abschnitt „Nichtflüchtiger Speicher“ der Tabelle auf Seite 25.

Nichtflüchtiger Speicher und Datenspeicher

Der Fiery server verfügt über verschiedene nichtflüchtige Speichertechnologien, damit beim Ausschalten Daten auf dem Fiery server erhalten bleiben. Zu diesen Daten gehören Informationen zur Systemprogrammierung und Benutzerdaten.

Weitere Informationen finden Sie im Abschnitt „Nichtflüchtiger Speicher“ der Tabelle auf Seite 25.

Flash-Speicher

Der Flash-Speicher speichert das Programm für Eigendiagnose und Booten (BIOS) sowie einige Systemkonfigurationsdaten. Der Flash-Speicher wird im Werk programmiert und kann nur durch das Installieren spezieller, von EFI erstellter Patches umprogrammiert werden. Wenn die Daten beschädigt oder gelöscht sind, startet der Fiery server nicht.

CMOS

Im batteriegepufferten CMOS-Speicher werden die Maschineneinstellungen des Fiery servers gespeichert. Keine dieser Informationen ist als vertraulich oder privat zu betrachten. Wenn der CMOS-Speicher installiert ist, können Benutzer auf diese Einstellungen auf einem Windows 10 IoT Enterprise 2016- oder 2019-basierten Server mithilfe von Monitor, Tastatur und Maus zugreifen.

NVRAM

Im Fiery server sind mehrere kleine NVRAM-Geräte mit funktionsfähiger Firmware vorhanden. Diese Geräte enthalten spezifische betriebsnotwendige Informationen, die aber nicht kundenbezogen sind. Der Benutzer hat keinen Zugriff auf die darauf gespeicherten Daten.

Festplattenlaufwerk und Festkörperlaufwerk

Während des normalen Druck- und Scanbetriebs sowie beim Erstellen von Informationen für das Auftragsmanagement werden Bilddaten in einen Direktzugriffsbereich auf dem Festplattenlaufwerk und Festkörperlaufwerk geschrieben.

Bilddaten und Aufträge in den Warteschlangen können von Benutzern manuell aus Command WorkStation oder einer anderen Warteschlange (z. B. Betrieb über das LCD des Druckers) gelöscht werden. Bilddaten und Objekte können auch automatisch mit dem Befehl **Serverdaten löschen** gelöscht werden, oder wenn die Anzahl der Druckaufträge die zulässigen Parameter überschreitet. Durch Deaktivieren der Warteschlange „Gedruckt“ werden auch die Druckaufträge gelöscht.

EFI verfügt über die Funktion „Sicheres Löschen“, um die Bilddaten vor unbefugtem Zugriff zu schützen. Wenn diese Funktion vom Fiery Administrator aktiviert wird, wird der ausgewählte Betriebsmodus zum entsprechenden Zeitpunkt ausgeführt, um gelöschte Daten sicher vom Festplattenlaufwerk zu entfernen. Die Fiery Funktion „Sicheres Löschen“ unterstützt derzeit nur Festplattenlaufwerke. Bei Festkörperlaufwerken (SSDs) sind vor der Entsorgung des Laufwerks mit dem Hersteller Möglichkeiten der Laufwerkspflege zu klären.

Hinweis: Weitere Informationen zur Funktion „Sicheres Löschen“ finden Sie unter Sicheres Löschen auf Seite 24.

Physikalische Ports

Der Fiery server kann über externe Ports verbunden werden, die in der folgenden Tabelle angegeben sind:

Fiery Ports	Funktion	Zugriff	Zugriffssteuerung
Ethernet RJ-45-Stecker	Ethernet-Konnektivität	Netzwerkverbindungen	Mittels Fiery IP-Filterung für Zugriffssteuerung
Anschluss für Druckerschnittstelle	Drucken und Scannen	Vorgesehen für das Senden/ Empfangen an den/von dem Drucker	n.v.
USB-Port	Anschluss von USB-Geräten Installation der Systemsoftware	Plug-and-Play-Anschluss für die Verwendung mit optionalen Wechseldatenträgern.	Die USB-Druckfunktion kann ausgeschaltet werden. Der Zugriff auf USB-Speichergeräte kann über die Windows-Gruppenrichtlinie ausgeschaltet werden. Der USB-Speicher kann außerdem über Configure deaktiviert werden.
Glasfaserstecker	10 GB Ethernet-Konnektivität	Netzwerkverbindungen	n.v.

Lokale Schnittstelle

Auf einigen Fiery servers kann der Benutzer auf die Fiery Funktionen auf dem Fiery NX Station Monitor, über die Fiery QuickTouch Software auf dem Touchscreen-Display oder über jeden mit dem Fiery server verbundenen

Monitor zugreifen. Der Sicherheitszugriff auf dem Fiery server mit Fiery NX Station wird über ein Windows-Administratorkennwort gesteuert. Das Touchscreen-Display hat sehr begrenzte Funktionen, die kein Sicherheitsrisiko darstellen.

Optionales Kit für Wechselfestplatten

Einige Fiery servers unterstützen ein Options-Kit für Wechselfestplatten bei erhöhten Sicherheitsanforderungen. Mit diesem Kit können Benutzer die Serverlaufwerke bei Normalbetrieb im System verriegeln und nach dem Ausschalten des Fiery server aus dem Gerät entfernen, um sie an einem sicheren Ort aufzubewahren.

Für eigenständige Windows-Server

Eigenständige, auf Windows basierende Fiery servers unterstützen ein Options-Kit für Wechselfestplatten. Ob dieses Options-Kit für ein bestimmtes Fiery Produkt verfügbar ist oder nicht, hängt von den Bedingungen der Vereinbarungen von EFI mit den individuellen Fiery Partnern ab.

Für Fiery XB Server

Die Festplatten- und Festkörperlaufwerke können von den Fiery XB Servern entfernt werden. Die meisten Festplatten- und Festkörperlaufwerke werden in der RAID-Konfiguration miteinander gekoppelt. Es ist wichtig, die Laufwerke wieder in ihrer Originalposition einzubauen, um Datenverluste und eine neue Systemsoftwareinstallation zu vermeiden.

USB-Ports für die Speichernutzung aktivieren

Mit USB-Ports auf Fiery servers sind Maus-, Tastatur- oder Spektralfotometer-Anschlüsse möglich, Verbindungen zu USB-Speichergeräten jedoch nicht, wenn die Option USB-Speicher aktivieren in Configure deaktiviert ist. Diese Option ist standardmäßig aktiviert. Bei Deaktivierung deaktiviert die Option Fiery Funktionen, für die USB-Massenspeicherfunktionalität erforderlich ist, z. B. Sichern und Wiederherstellen.

Netzwerksicherheit

Der Fiery server umfasst eine Vielzahl von Netzwerksicherheitsfunktionen für die Steuerung und Verwaltung des Zugriffs auf den Drucker. Nur autorisierte Benutzer und Gruppen können auf den Fiery server zugreifen und auf dem Drucker drucken. Der Fiery server kann auch so konfiguriert werden, dass er die externe Kommunikation durch die Verwendung von festgelegten IP-Adressen sowie durch Deaktivieren von Netzwerkports und Protokollen einschränkt oder steuert. Fiery servers sollten immer in einer geschützten Netzwerkumgebung eingesetzt werden und die Zugänglichkeit sollte von einem qualifizierten und autorisierten Netzwerkadministrator ordnungsgemäß konfiguriert und verwaltet werden.

Netzwerkports

Standardmäßig sind alle TCP/IP-Ports, die nicht von bestimmten Fiery Diensten verwendet werden, deaktiviert. Der Fiery Administrator kann selektiv Netzwerkports aktivieren und deaktivieren. Das Deaktivieren eines Netzwerkports blockiert die externen Verbindungen über den festgelegten Port. Wenn ein bestimmter Port aktiviert ist, werden externe Verbindungen über diesen Port zugelassen.

TCP	UDP	Portname	Abhängige Dienste
20-21		FTP	FTP
80		HTTP	WebTools, IPP
135		MS RPC	Microsoft® RPC-Dienst (nur Windows 10). Ein weiterer Port im Bereich 49152-65536 wird für den SMB-basierten Point-and-Print-Dienst geöffnet.
137-139		NETBIOS	Windows-Druck
	161, 162	SNMP	Fiery Central, einige ältere Dienstprogramme und andere SNMP-basierte Tools
	427	SLP	SLP
443		HTTPS	WebTools, IPP/s
445		SMB/IP	SMB über TCP/IP
	500	ISAKMP	IPsec
515		LPD	LPR-Druck, einige ältere Dienstprogramme (z. B. ältere Versionen von Command WorkStation)
631		IPP	IPP
3389		RDP	Remote Desktop (nur Windows Fiery Server)

TCP	UDP	Portname	Abhängige Dienste
3702	3702	WS-Discovery	WSD
	4500	IPsec NAT	IPsec
	5353	Multicast DNS	Bonjour
6310 8010 8021-8022 8090 9906 21030 50006-50025	9906	EFI-Ports	Command WorkStation 5 und 6, Fiery Central, EFI SDK-basierte Tools, bidirektionale Funktionen des Fiery Druckertreibers, WebTools, direkter Fiery Mobildruck und Konvertierung nativer Dokumente
9100-9103		Druckport	Port 9100

Hinweis: Die Ports 50006-50025 sind aktiviert, nachdem Command WorkStation Version 6.2 und später auf einem eigenständigen Fiery server installiert wurde.

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.

Der Fiery Administrator kann auch die verschiedenen, vom Fiery server bereitgestellten Netzwerkdienste aktivieren und deaktivieren.

IP-Filterung

Die IP-Filterung lässt Verbindungsanforderungen an den Fiery server von definierten IP-Adressen zu oder weist diese ab. Der Administrator kann Standardrichtlinien definieren, um empfangene Datenpakete zuzulassen oder abzuweisen, und kann auch Filter für maximal 16 IP-Adressen oder Bereiche festlegen, um Verbindungsanforderungen zuzulassen oder abzuweisen.

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

Netzwerkauthentifizierung

SNMP v3

Der Fiery server unterstützt den neuesten SNMPv3-Standard. SNMPv3-Kommunikationspakete können verschlüsselt werden, um Vertraulichkeit, Nachrichtenintegrität und Authentifizierung sicherzustellen.

Der Fiery Administrator kann zwischen drei SNMP-Sicherheitsstufen wählen: minimal, mittel und maximal. Der Fiery Administrator hat auch die Möglichkeit, eine Authentifizierung vor der Zulassung von SNMP-Transaktionen

anzufordern sowie SNMP-Benutzernamen und -Kennwörter zu verschlüsseln. Der lokale Administrator kann Community-Namen für SNMP-Lese- und Schreibzugriff und andere Sicherheitseinstellungen definieren.

Weitere Informationen finden Sie unter Empfohlene Einstellungen auf Seite 32.

IEEE 802.1 x

802.1x ist ein IEEE-Standardprotokoll für die portbasierte Netzwerkzugriffssteuerung. Dieses Protokoll hat einen Authentifizierungsmechanismus, bevor der Fiery server auf das LAN und dessen Ressourcen zugreifen kann.

Wenn aktiviert, kann der Fiery server so konfiguriert werden, dass er EAP MD5-Challenge, PEAP-MSCHAPv2 oder EAP-TLS für die Authentifizierung an einem 802.1x-Authentifizierungsserver verwendet.

Der Fiery server holt die Authentifizierung beim Starten oder dann ein, wenn das Ethernet-Kabel getrennt und wieder angeschlossen wird.

Netzwerkverschlüsselung

Internet Protocol Security (IPsec)

IPsec (Internet Protocol Security) bietet durch die Verschlüsselung und Authentifizierung jedes einzelnen Datenpakets Sicherheit bei allen über IP-Protokolle kommunizierenden Anwendungen.

Der Fiery server verwendet eine vorinstallierte Schlüsselauthentifizierung, um sichere Verbindungen mit anderen Systemen über IPsec herzustellen.

Nachdem eine sichere Kommunikation über IPsec zwischen einem Client-Computer und einem Fiery server hergestellt wurde, werden alle Kommunikationsdaten — einschließlich Druckaufträgen — sicher über das Netzwerk übertragen.

HTTPS

Der Fiery server erfordert eine sichere Verbindung zwischen Clients und verschiedenen Serverkomponenten. HTTPS über TLS wird verwendet, um die Kommunikation zwischen den beiden Endpunkten zu verschlüsseln. HTTPS ist beim Verbinden mit dem Fiery server von WebTools und Fiery API erforderlich. Diese Kommunikation ist mit TLS 1.3 und 1.2 verschlüsselt.

Zertifikatverwaltung

Fiery servers stellen eine Schnittstelle bereit, um die während der TLS-Kommunikation verwendeten Zertifikate zu verwalten. Fiery servers unterstützen das Zertifikatsformat X.509.

Fiery servers unterstützten RSA-Zertifikate mit einer Schlüssellänge von 4096-, 3072- und 2048-Bit.

Die Zertifikatsverwaltung ermöglicht dem Fiery Administrator Folgendes:

- Selbstsignierte digitale Zertifikate erstellen.
- Ein Zertifikat und dessen entsprechenden privaten Schlüssel für den Fiery server hinzufügen.
- Zertifikate von einer vertrauenswürdigen Zertifikatsstelle hinzufügen, durchsuchen, anzeigen und entfernen.

Hinweis: Selbstsignierte Zertifikate sind nicht sicher. Wir empfehlen Anwendern dringend, ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle (CA) zu verwenden.

Nach Erhalt eines Zertifikats, das von einer vertrauenswürdigen Zertifikatsstelle signiert wurde, können Sie das Zertifikat in den WebTools, im Abschnitt Configure, auf den Fiery server hochladen.

E-Mail-Sicherheit

Der Fiery server unterstützt POP- und SMTP-E-Mail-Kommunikationsprotokolle, wenn eine E-Mail aktiviert ist. (Diese Funktion ist standardmäßig deaktiviert.) Zum Schutz des Dienstes vor Angriffen und nicht ordnungsgemäßer Verwendung kann der Fiery Administrator zusätzliche Sicherheitsfunktionen aktivieren.

POP vor SMTP

Einige E-Mail-Server unterstützen noch das ungesicherte SMTP-Protokoll und damit das Senden von E-Mail-Nachrichten ohne Authentifizierung. Um nicht autorisierte Zugriffe zu verhindern, verlangen einige E-Mail-Server von E-Mail-Clients, sich über POP zu authentifizieren, bevor sie eine E-Mail über SMTP senden können. Für solche E-Mail-Server muss der Fiery Administrator die POP-Authentifizierung vor SMTP aktivieren.

OP25B

Outbound Port 25 Blocking (OP25B) ist eine Antispam-Maßnahme, mit der Internetdienstanbieter Datenpakete, die an Port 25 über ihre Router gesendet wurden, blockieren können. Mit der E-Mail-Konfigurationsschnittstelle kann der Fiery Administrator einen anderen Port festlegen.

Weitere Informationn zum Fiery server Workflow des E-Mail-Druckens finden Sie unter E-Mail-Drucken auf Seite 26.

Server Message Block (SMB)

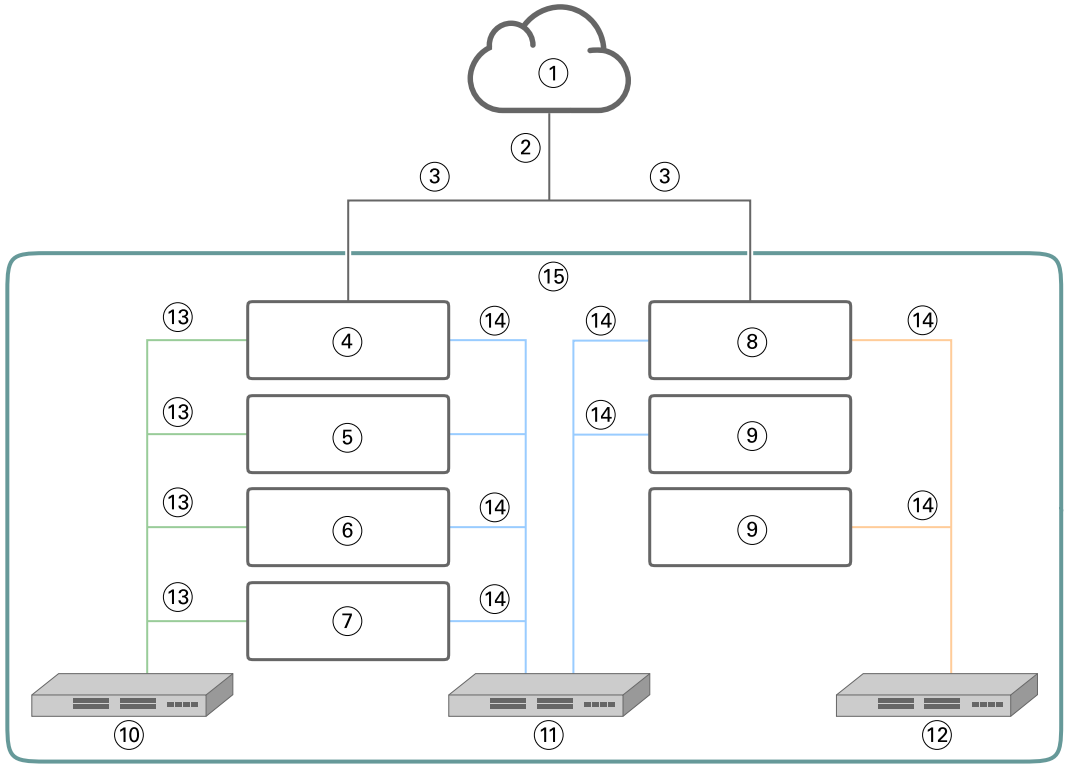
SMB ist ein Netzwerkprotokoll, mit dem ein gemeinsamer Zugriff auf Dateien und Drucker möglich ist. SMB v1 ist auf Fiery servers deaktiviert, da es nicht die aktuellen Branchensicherheitsstandards erfüllt. SMB v2 und V3 werden weiterhin unterstützt.

SMB-Signaturen werden auf dem Fiery server erzwungen. SMB-Signaturen erfordern digital signierte Pakete, damit der Empfänger die Echtheit des Pakets überprüfen kann, um Man-in-the-Middle-Angriffe zu verhindern. Wenn die SMB-Authentifizierung aktiviert ist, muss der Benutzer SMB-Benutzernamen und -Kennwort angeben, um auf die SMB-Ordner und den in den SMB-Ordnern gespeicherten SMB-Inhalt zugreifen zu können.

Hinweis: Das Drucken oder Teilen von Dateien über SMB kann durch Festlegen eines Kennworts in Configure eingeschränkt werden.

Fiery XB Netzwerkdiagramm

Die folgende Grafik zeigt, wie sich Fiery XB Server und Highspeed-Inkjet-Drucker mit dem Netzwerk verbinden.



1	LAN	9	Andere Druckblätter (optional)
2	Auftragsmanagement Netzwerkdatenverkehr	10	10 GbE Privates Netzwerk
3	1 GbE DHCP oder statisch	11	1 GbE Privates Netzwerk
4	Fiery Hauptblatt	12	1 GbE PLC Privates Netzwerk
5	Fiery RIP Blatt (optional)	13	10 GbE
6	Fiery Blatt Nr. 1 (optional)	14	1 GbE
7	Fiery Blatt Nr. 2 (optional)	15	Geschlossene Fiery XB Umgebung
8	Druckblatt		

Zugriffssteuerung

In diesem Kapitel wird beschrieben, wie der Fiery server konfiguriert werden kann, um den Zugriff auf die Ressourcen für verschiedene Benutzergruppen zu steuern.

Benutzerauthentifizierung

Mit der Funktion „Benutzerauthentifizierung“ ist Folgendes auf dem Fiery server möglich:

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

Der Fiery server kann Benutzer mit folgendem Status authentifizieren:

- In einer Domäne: Benutzer, die auf einem Unternehmensserver definiert sind, auf den über LDAP zugegriffen werden kann
- Auf dem Fiery Server: Auf dem Fiery server definierte Benutzer

Der Fiery server autorisiert die Aktionen der Benutzer basierend auf der Gruppe, zu der sie gehören. Jeder Gruppe sind bestimmte Berechtigungen zugewiesen (z. B. „In Graustufen drucken“, „In Farbe oder Graustufen drucken“) und die Aktionen der Gruppenmitglieder sind auf diese Berechtigungen beschränkt. Der Fiery Administrator kann die Berechtigungen jeder Fiery Gruppe ändern, mit Ausnahme der Administrator- und Bediener-Konten.

Bei dieser Version der Benutzerauthentifizierung sind die Berechtigungen, die für eine Gruppe ausgewählt werden können, wie folgt:

- **In Graustufen drucken**: Mit dieser Berechtigung können Gruppenmitglieder Aufträge in Graustufen auf dem Fiery server drucken. Wenn der Benutzer 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**: Mit dieser Berechtigung können Gruppenmitglieder Aufträge auf dem Fiery server mit Vollzugriff auf die Farb- und Graustufendruckfunktionen des Fiery server drucken. Ohne diese Berechtigung oder die Berechtigung zum Drucken in Graustufen wird der Druckauftrag nicht gedruckt und Benutzer können den Auftrag nicht über FTP übermitteln (nur bei Farbgeräten).
- **Fiery Mailbox**: Mit dieser Berechtigung erhalten Gruppenmitglieder jeweils eine eigene Mailbox. Der Fiery server erstellt für jeden Benutzer unter dessen Namen eine Mailbox und erteilt die Zugriffsberechtigung für diese Mailbox. Der Zugriff auf diese Mailbox ist auf Benutzer beschränkt, die den Mailbox-Benutzernamen und das zugehörige Kennwort kennen.
- **Kalibrierung**: Mit dieser Berechtigung können Gruppenmitglieder die Farbkalibrierung durchführen.
- **Servervorgaben erstellen**: Mit dieser Berechtigung können Gruppenmitglieder Servervorgaben erstellen, damit andere Fiery Benutzer Zugriff auf häufig verwendete Auftragsvorgaben erhalten.

- **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.

Hinweis: Die Benutzerauthentifizierung ersetzt die Druckfunktionen für Mitglieder und Gruppen.

Benutzerauthentifizierung für Fiery Software

Der Fiery server interagiert mit unterschiedlichen Benutzertypen. Diese Benutzer sind für die Fiery Software festgelegt und sind nicht mit Windows-definierten Benutzern oder Rollen verknüpft. Es wird empfohlen, dass Fiery Administratoren Kennwörter anfragen, um auf den Fiery server zugreifen zu können. Darüber hinaus empfiehlt EFI, dass der Fiery Administrator das Standardkennwort ändert, um den Sicherheitsanforderungen in der Druckumgebung des Anwenders zu entsprechen.

- Das Kennwort für den „Administrator“ und den „Bediener“ darf höchstens 15 Zeichen betragen, wenn Configure > Sicherheit verwendet wird.
- Das Kennwort für lokale Benutzerkonten darf höchstens 64 Zeichen betragen, wenn Configure > Benutzerkonten verwendet werden.
- Das Administrator- und Bedienerkennwort kann auch in Configure > Benutzerkonten geändert werden. Die maximale Zeichenlänge beträgt in diesem Fall 64 Zeichen.

Im Folgenden werden die für die verschiedenen Fiery Benutzertypen zulässigen Berechtigungen beschrieben:

- **Administrator**: Hat die volle Kontrolle über alle Funktionen des Fiery server .

  Der Fiery Administrator kann die Berechtigungen jeder Fiery Gruppe ändern, mit Ausnahme der Administrator- und Bedienerkonten.
- **Bediener**: Hat fast dieselben Berechtigungen wie der Administrator, aber keinen Zugriff auf einige Fiery server Funktionen, z. B. Setup, und er kann das Auftragsprotokoll nicht löschen.
- **Druckproduktionsmitarbeiter** (nur Fiery XB Server): Kann Aufträge auf der Druckmaschine verwalten. Der Administrator kann zu diesem Benutzertyp bestimmte Berechtigungen hinzufügen.
- **Fiery Dienst-Admin** (Fiery servers nur unter Windows): Ein ausgeblendetes Admin-Konto, das für die Installation des vertrauenswürdigen Zertifikats auf Windows-Servern verwendet wird. Dieses Konto erlaubt es Anwendern nicht, sich bei (lokalen oder entfernten) Fiery server anzumelden. Dieses Konto kann von gewissen Tools für das Netzwerkscannen angezeigt werden und kann bei Bedarf entfernt werden. Mit alternativen Standardmethoden können Sie das vertrauenswürdige Zertifikat installieren.

Protokoll des Fiery Sicherheitsaudits

Um Unternehmen mit Konformitätsanforderungen zu helfen, können Fiery Administratoren sicherheitsrelevante Ereignisse sammeln und analysieren, die im Protokoll des Sicherheitsaudits gespeichert werden.

Das Sicherheitsaudit-Protokoll ist standardmäßig aktiviert.

Jedes Sicherheitsereignis wird als Information, Warnung oder Fehler eingestuft. Dem Administrator werden keine Warnungen oder Benachrichtigungen zur Verfügung gestellt, sondern nur ein statisches Protokoll.

Die Protokolle haben ein Format, das von gängigen SIEM-Lösungen für die Protokollsammlung und -analyse unterstützt wird. Die Informationen zu den erfassten Ereignissen entsprechen der NIST Sonderveröffentlichung 800-53, *Recommended Security Controls for Federal Information Systems* (SP800-53).

Der Fiery Administrator kann Ereignisse ohne Eingriffe durch EFI lesen. Ereignisse sowohl von Windows- als auch von Linux-basierten Fiery servers liegen im JSON-Format vor und können von jedem Protokollierungswerkzeug verarbeitet werden. Auf Windows-basierten Fiery Servern können die Ereignisse im Windows Ereignis-Manager eingesehen werden. Administratoren von Linux-basierten Fiery servers können Protokolle an ein zentrales Protokollierungssystem (SysLog) weiterleiten.

Sicherheitsereignisse werden basierend auf der Speicherkapazität der zugewiesenen Festplatte aufbewahrt. Wenn die Protokollgröße den maximalen Speicherplatz erreicht (400 MB), werden ältere Ereignisse gelöscht.

Betriebssysteme

EFI arbeitet eng mit den Herstellern der in Fiery servers verwendeten Betriebssysteme zusammen, um die erforderlichen Sicherheitsupdates in Bezug auf Sicherheitsprobleme oder Schwachstellen zu erhalten, die Auswirkungen auf die Fiery server Kernkomponenten, z. B. Motherboard, Prozessor, BIOS usw., haben könnten. Darüber hinaus werden Fiery Softwareupdates von EFI digital signiert, um eine unzulässige Änderung zu verhindern, einschließlich der Einfügung von Schadsoftware.

Linux (FS500)

FS500 Fiery servers sind Linux-basierte Server, die mit geschlossener Architektur entwickelt wurden. Eine eingeschränkte Sichtbarkeit des Netzwerks verhindert einen unbefugten Zugriff.

Die Merkmale von Linux-basierten Fiery servers sind wie folgt:

- Linux-basierte Fiery servers enthalten keine lokale Schnittstelle, die den Zugriff auf das Betriebssystem zulassen könnte.
- SSH und Telnet werden auf Linux-basierten Fiery servers nicht unterstützt, wodurch kein Zugriff auf die Betriebssystem-Shell möglich ist.
- Linux-basierte Fiery servers lassen keine Installation von nicht autorisierten Programmen zu, die das System gegenüber Sicherheitslücken anfällig machen könnten
- Das Linux-Betriebssystem, das auf FS500 Fiery servers verwendet wird, ist ein angepasstes Betriebssystem nur für Fiery servers. Es verfügt über alle Betriebssystemkomponenten, die für einen Fiery server notwendig sind, jedoch nicht über einige allgemeine Komponenten und Endnutzeranwendungen von gängigen Linux-Systemen.

Zugriff auf das System

Linux-basierte Fiery servers können über Fiery Setup auf dem Druckerbedienfeld oder über Configure in WebTools konfiguriert werden. WebTools ist ein Satz browserbasierter Seiten, mit denen der Fiery Administrator auf den Fiery server für die Konfiguration und andere Aktivitäten in Bezug auf die Systemverwaltung zugreifen kann. WebTools läuft unter dem neuesten sicheren Webframework, das von den meisten modernen Webbrowsern unterstützt wird.

Windows 10 (FS500 Pro)

Die eigenständigen FS500 Pro Fiery servers verwenden Windows 10 IoT Enterprise 2019 LTSC als Betriebssystem. Diese Windows-Edition umfasst die aktuellsten Sicherheitsverfahren und kumulativen Funktionserweiterungen, die in Windows 10, Versionen 1703, 1709, 1803 und 1809, enthalten sind. Jedes LTSC Build wird von Microsoft mit Sicherheitsupdates für zehn Jahre nach dem Release unterstützt.

Hinweis: Windows 10 IoT Enterprise 2019 LTSC ist ein binäres Äquivalent zu Windows 10 Enterprise Version 1809.

Windows 10 IoT Enterprise 2019 LTSC enthält die folgenden Funktionen:

- Für die Verwendung in spezialisierten Systemen wie Fiery servers vorgesehen.
- Umfasst viele Sicherheitsverbesserungen im Hinblick auf Bedrohungen, Informationen und Identitätsschutz.
- Verfügt über zahlreiche Sicherheitsupdates.
- Enthält keine verbraucherorientierten Anwendungen, z. B. Kalender, Wetter, Fotos und andere.

Microsoft Windows Update

Microsoft gibt regelmäßig Sicherheitspatches über Windows Update aus, um potenzielle Sicherheitsbedrohungen und Schwachstellen des Betriebssystems zu beheben. Die Standardeinstellung von Windows Update auf Fiery servers soll Benutzer über Patches benachrichtigen, ohne diese herunterzuladen. Das Auswählen von Nach Updates suchen unter Windows Update in der Windows-Systemsteuerung aktiviert automatische Updates und startet den Updatevorgang.

Windows Update-Tools

Windows-basierte Fiery servers verwenden Microsoft-Standardmethoden zur Aktualisierung aller anwendbaren Microsoft-Sicherheitspatches. Der Fiery server unterstützt keine anderen Update-Tools Dritter zum Abrufen von Sicherheitspatches.

Windows-Antivirussoftware

Fiery servers verwenden Microsoft Antivirussoftware und Windows 10 Defender zum Schutz. Im Allgemeinen kann die Antivirussoftware Dritter mit einem Fiery server verwendet werden. Die Antivirussoftware wird in vielen Varianten angeboten und kann zahlreiche Komponenten und Funktionen enthalten, um einer Bedrohung entgegenzuwirken.

Bitte beachten Sie, dass die Antivirussoftware am besten funktioniert, wenn sie direkt auf dem Fiery server installiert, konfiguriert und ausgeführt wird. Bei Fiery servers ohne lokale Konfiguration ist es weiterhin möglich, die Antivirussoftware auf einem Remote-Client-Computer zu starten und ein gemeinsam genutztes Fiery server Festplattenlaufwerk zu scannen. EFI empfiehlt bei Fragen zur Vorgehensweise die Rücksprache mit dem Hersteller der Antivirussoftware.

Antivirenscan bei Druckmaschinen

Ein Antivirenscan bei Druckmaschinen des Fiery server kann sich auf die Fiery Leistung auswirken, selbst wenn der Scan geplant wurde.

Antispyware

Ein Antispyware-Programm kann die Leistung beeinträchtigen, wenn Dateien auf einem Fiery server empfangen werden. Beispiele dafür sind empfangene Druckaufträge, Dateien, die während eines Fiery server Systemupdates heruntergeladen werden, oder ein automatisches Update der auf dem Fiery server ausgeführten Anwendungen.

Integrierte Firewall

Da der Fiery server über eine Firewall verfügt, sind Firewalls der Antivirussoftware im Allgemeinen nicht erforderlich. EFI empfiehlt, nach Rücksprache mit der eigenen IT-Abteilung zu entscheiden, ob es notwendig ist,

eine integrierte Firewall, die mit der Antivirussoftware zur Verfügung gestellt wird, zu installieren und auszuführen. Unter Netzwerkports auf Seite 11 finden Sie eine Liste der verfügbaren Ports.

Antispam
Der Fiery server unterstützt die Funktionen „Drucken über E-Mail“ und „Scannen über E-Mail“. Wir empfehlen, einen serverbasierten Spam-Filter-Mechanismus zu verwenden. Der Fiery servers kann auch so konfiguriert werden, dass Dokumente von bestimmten E-Mail-Adressen gedruckt werden. Die Antispam-Komponente ist nicht erforderlich, da die Ausführung eines separaten E-Mail-Clients (z. B. Outlook) auf dem Fiery server nicht unterstützt wird.

HIPS und Anwendungssteuerung
Aufgrund der Komplexität des Host Intrusion Protection System (HIPS) und der Anwendungssteuerung muss die Konfiguration der Antivirussoftware sorgfältig geprüft und bestätigt werden, wenn eine dieser Funktionen verwendet wird. Bei ordnungsgemäßer Feinabstimmung sind HIPS und Anwendungssteuerung hervorragende Sicherheitsmaßnahmen, die problemlos mit dem Fiery server genutzt werden können. Falsche HID-Parametereinstellungen und falsche Dateiausschlüsse können aber leicht zu Fehlfunktionen des Fiery server führen — oft durch „Akzeptieren der Standardeinstellungen“. Die Lösung besteht darin, die ausgewählten Optionen in den HIPS- oder Anwendungssteuerungseinstellungen in Verbindung mit den Einstellungen des Fiery server zu überprüfen, z. B. Netzwerkports, Netzwerkprotokolle, ausführbare Dateien der Anwendungen, Konfigurationsdateien, temporäre Dateien usw.

Liste sicherer Einträge und Liste blockierter Einträge
Die Verwendung einer Liste sicherer Einträge und einer Liste blockierter Einträge sollte normalerweise keine nachteiligen Auswirkungen auf den Fiery server haben. EFI empfiehlt dringend die Konfiguration dieser Funktionalität durch den Kunden, sodass Fiery Module nicht auf die Liste blockierter Einträge gesetzt werden.

E-Mail-Viren

Normalerweise erfordern über E-Mail übertragene Viren Aktivitäten durch den Empfänger. Angehängte Dateien, die keine PDL-Dateien sind, werden vom Fiery server ignoriert. Der Fiery server ignoriert auch E-Mails in RTF- oder HTML-Formaten oder mit integriertem JavaScript. Abgesehen von einer E-Mail-Antwort an einen bestimmten Benutzer aufgrund eines empfangenen Befehls werden alle per E-Mail empfangenen Dateien als PDL-Aufträge behandelt.

Hinweis: Weitere Informationen zum Fiery server Workflow des E-Mail-Druckens finden Sie unter E-Mail-Drucken auf Seite 26.

Datensicherheit

In diesem Abschnitt werden Sicherheitskontrollen beschrieben, die die im Fiery server vorhandenen Benutzerdaten schützen, sowie Sicherheitskontrollen für Daten während der Übertragung.

Verschlüsselung sensibler Informationen

Die Verschlüsselung sensibler Informationen im Fiery server stellt sicher, dass alle Kennwörter und entsprechende Konfigurationsinformationen sicher sind, wenn sie im Fiery server gespeichert werden. Sensible Informationen werden entweder verschlüsselt oder mit Hash versehen. Die verwendeten kryptografischen Algorithmen sind AES256, Diffie-Hellman und SHA-2, um den neuesten Sicherheitsstandards zu entsprechen.

Auf der Festplatte gespeicherte Benutzerinformationen können nicht gelesen werden, auch wenn die Festplatte aus dem Fiery server entfernt wurde. Die Verschlüsselung von Benutzerdaten kann auf Windows-basierten Fiery servers mithilfe von Configure aktiviert oder deaktiviert werden. Bei Linux-basierten Fiery servers ist diese Funktion immer aktiviert.

Wenn die Passphrase, die eingegeben wird, um Daten wiederherzustellen, nicht gespeichert wird, besteht keine Möglichkeit, sie zurückzusetzen, und EFI kann sie nicht wiederherstellen. Die Software muss dann neu installiert werden.

Hinweis: Bei der Datenverschlüsselung wird die Festplatte partitioniert und nur die Benutzerdatenpartition wird verschlüsselt. Betriebssystempartitionen können nicht verschlüsselt werden.

Advanced Encryption Standard (AES)

Der Fiery server schützt ruhende Daten vor unbefugtem Zugriff. Er verschlüsselt Aufträge, Bilder und Kundendaten mithilfe des 256-Bit-AES-Algorithmus.

AES ist ein schneller und schwer zu knackender Verschlüsselungsstandard mit kleinem Umfang, der für eine Vielzahl von Geräten und Anwendungen geeignet ist. Er bietet einen zusätzlichen Schutz vor Datendiebstahl und gleichzeitige Einhaltung der für Unternehmen geltenden Sicherheitsrichtlinien.

Standarddruck

An den Fiery server übermittelte Aufträge können an eine der folgenden Druckwarteschlangen, die vom Fiery server freigegeben wurden, gesendet werden:

- Warteschlange „Halten“
- Warteschlange „Drucken“
- Warteschlange „Sequenzielles Drucken“

- Warteschlange „Direkt“ – direkte Verbindung
- Virtuelle Drucker (vom Fiery Administrator festgelegte benutzerdefinierte Warteschlangen)

Der Fiery Administrator kann die Warteschlangen „Drucken“ und „Direkt“ deaktivieren, um das automatische Drucken einzuschränken.

Warteschlangen „Halten“, „Drucken“ und „Sequenzielles Drucken“

Ein an die Warteschlange „Halten“ oder „Drucken“ gesendeter Auftrag wird auf der Festplatte auf dem Fiery server gespoolt. An die Warteschlange „Halten“ gesendete Aufträge bleiben auf dem Fiery Festplattenlaufwerk, bis der Benutzer den Auftrag zum Drucken sendet oder den Auftrag mithilfe eines Dienstprogramms für Auftragsmanagement, z. B. Command WorkStation, löscht.

Bei der Warteschlange „Sequenzielles Drucken“ kann der Fiery server die Auftragsreihenfolge für bestimmte, über das Netzwerk gesendete Aufträge beibehalten. Der Workflow ist „First In, First Out“ (FIFO) unter Berücksichtigung der Reihenfolge, in der die Aufträge über das Netzwerk empfangen wurden. Ohne aktivierte Warteschlange „Sequenzielles Drucken“ kann die Reihenfolge der Druckaufträge, die über den Fiery server gesendet wurden, aufgrund vieler Faktoren geändert werden, z. B. wenn der Fiery server zulässt, dass kleinere Aufträge vorgezogen werden, während größere Aufträge gespoolt werden.

Warteschlange „Gedruckt“

Aufträge, die an die Warteschlange „Drucken“ gesendet werden, werden nach dem Drucken in der Warteschlange „Gedruckt“ auf dem Fiery server gespeichert, sofern die Warteschlange „Gedruckt“ aktiviert ist. Der Administrator kann die Anzahl der Aufträge festlegen, die sich in der Warteschlange „Gedruckt“ befinden. Wenn die Warteschlange „Gedruckt“ deaktiviert wird, werden Aufträge automatisch gelöscht, nachdem sie gedruckt wurden.

Warteschlange „Direkt“ (direkte Verbindung)

Die Warteschlange „Direkt“ ist zum Herunterladen von Schriften und Anwendungen vorgesehen, für die eine direkte Verbindung zum PostScript-Modul in Fiery servers erforderlich ist.

EFI empfiehlt nicht, die Warteschlange „Direkt“ zum Drucken zu verwenden. Vom Fiery server werden alle von der direkten Verbindung gesendeten Aufträge nach dem Drucken gelöscht. EFI garantiert jedoch nicht, dass alle für den Auftrag angelegten temporären Daten gelöscht werden.

Aufträge mit VDP (Variable Data Printing)-, PDF- oder TIFF-Dateien, die an die Warteschlange „Direkt“ gesendet wurden, werden an die Druckwarteschlange umgeleitet. Über den SMB-Netzwerkdienst gesendete Aufträge können an die Warteschlange „Drucken“ weitergeleitet werden, wenn sie an die Warteschlange „Direkt“ gesendet wurden.

Auftragslöschung

Ein Auftrag kann nicht angezeigt oder abgerufen werden, wenn er automatisch vom Fiery server oder mit Fiery Tools gelöscht wird. Wenn der Auftrag auf dem Festplattenlaufwerk des Fiery server gespoolt wurde, können Auftragselemente auf dem Festplattenlaufwerk bleiben und theoretisch mit bestimmten Tools, z. B. forensischen Analysetools für Laufwerke, wiederhergestellt werden.

Sicheres Löschen

Mit der Funktion „Sicheres Löschen“ wird der Inhalt eines gesendeten Auftrags vomFiery server Festplattenlaufwerk entfernt, sobald ein Auftrag über eine Fiery Funktion gelöscht wird. Wenn ein Auftrag gelöscht wird, wird jede Auftragsquelldatei dreimal mit einem Algorithmus, der auf der US-amerikanischen Datenlöschmethode DoD 5220.22-M basiert, überschrieben.

Workflows	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
Aufträge, die vom Fiery server empfangen und gelöscht werden, nachdem die Funktion „Sicheres Löschen“ eingeschaltet wurde	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 Wechseldatenträger 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 beim Disk Swapping oder Disk Caching auf das Fiery server Festplattenlaufwerk geschrieben wurden	Nein
Auftragsprotokolleinträge	Nein
Auftragsprotokolleinträge nach der Ausführung der Funktion „Serverdaten löschen“	Ja
Fiery server ausgeschaltet, bevor das Löschen des Auftrags abgeschlossen ist	Nein
Defragmentierung des Fiery server Festplattenlaufwerks vor dem Löschen eines Auftrags	Nein

Hinweis: Die Funktion „Sicheres Löschen“ wird auf Fiery XB Plattformen oder Fiery servers mit SSDs nicht unterstützt.

Systemspeicher

Beim Verarbeiten einiger Dateien können manche Auftragsdaten in den Arbeitsspeicher des Betriebssystems geschrieben werden. In einigen Fällen wird der Inhalt des Arbeitsspeichers beim Disk Swapping möglicherweise auf die Festplatte ausgelagert und nicht explizit überschrieben.

Flüchtiger Speicher			
Typ (SRAM, DRAM usw.)	**Vom Benutzer modifizierbar (Ja oder Nein)**	**Funktion oder Verwendung**	**Vorgang zum Bereinigen**
DRAM	Ja	Hauptsystemspeicher (empfängt an die Warteschlange „Direkt“ gesendete Aufträge)	Fiery server ausschalten
SDRAM (auf Videokarte)	Ja	Videospeicher	Fiery server ausschalten

Nichtflüchtiger Speicher			
Typ (SRAM, DRAM usw.)	**Vom Benutzer modifizierbar (Ja oder Nein)**	**Funktion oder Verwendung**	**Vorgang zum Bereinigen**
BIOS	Nein	BIOS-Funktionen	Aus der Steckbuchse entfernen und zerstören, aber das System wird dann nicht mehr funktionieren.
Ethernet-EPROM	Nein	Firmware für Ethernet-Chip	Ablöten und zerstören, aber das System wird dann nicht mehr funktionieren.
CMOS NVRAM	Nein	Speicher für BIOS-Einstellungen	Systembatterie für 30 Sekunden entfernen.
Festplattenlaufwerk (HDD) oder Festkörperlaufwerk (SSD)	Ja	Betriebssystem Fiery Anwendungen (möglicherweise mit Benutzerdaten) Fiery Systemsoftware Druckaufträge, Scanaufträge und andere Benutzerdaten Sicherungsbild für Werksstandardeinstellung	Die Systemsoftware neu installieren. Die meisten Aufträge können mit der Funktion „Sicheres Löschen“* sicher entfernt werden. Mit den Tools für die Systembereinigung von Dritten und Fiery Partnern können Daten auf diesen Geräten gelöscht werden.

Nichtflüchtiger Speicher			
Typ (SRAM, DRAM usw.)	**Vom Benutzer modifizierbar (Ja oder Nein)**	**Funktion oder Verwendung**	**Vorgang zum Bereinigen**
Hinweis: Der flüchtige Speicher und der Arbeitsspeicher könnten Kundendaten enthalten, während die Daten der Kunden verarbeitet werden. Es werden keine Kundendaten im nichtflüchtigen Speicher, z. B. BIOS, CMOS und NVRAM, gespeichert. *Festkörperlaufwerke können durch Multi-Pass-Überschreibungsmethoden für sicheres Löschen aufgrund der Zuordnung für den Speicherverschleiß nicht vollständig bereinigt werden. Darüber hinaus würden Versuche, dies durchzuführen, auch die Lebensdauer des Festkörperlaufwerks erheblich vermindern. Diese Funktion wird auf Fiery XB Plattformen nicht unterstützt.			

Vertraulich drucken

Die Funktion „Vertraulich drucken“ fordert den Benutzer auf, ein auftragsspezifisches Kennwort auf dem Fiery server und dem Drucker einzugeben, damit der Auftrag gedruckt werden kann.

Für diese Funktion ist der Zugriff auf das Druckerbedienfeld erforderlich. Der Zweck der Funktion besteht darin, den Zugriff auf ein Dokument auf einen Benutzer zu beschränken, der über das Kennwort für den Auftrag verfügt und dieses lokal auf dem Druckerbedienfeld eingeben kann.

W orkflow „Vertraulich Drucken“

Der Benutzer gibt im Fiery Treiber ein Kennwort in das Feld Vertraulich drucken ein. Wenn dieser Auftrag an die Fiery server Warteschlange „Drucken“ oder „Halten“ gesendet wird, bleibt der Auftrag so lange in der Warteschlange, bis das Kennwort eingegeben wird.

Hinweis: Aufträge, die mit einem Kennwort für „Vertraulich drucken“ gesendet werden, können nicht über Command WorkStation angezeigt werden.

Über das Druckerbedienfeld greift der Benutzer auf das Fenster „Vertraulich drucken“ zu und gibt ein Kennwort ein. Der Benutzer kann dann die mit diesem Kennwort gesendeten Aufträge suchen und drucken und anschließend diese löschen.

Der gedruckte vertrauliche Auftrag wird nicht in die Warteschlange „Gedruckt“ verschoben und wird nach dem Drucken automatisch gelöscht.

Hinweis: Ein Teil der Daten kann vorübergehend in den Betriebssystemdateien verbleiben.

E-Mail-Drucken

Der Fiery server empfängt und druckt Aufträge, die per E-Mail gesendet wurden. Der Administrator kann eine Liste mit autorisierten E-Mail-Adressen auf dem Fiery server speichern. Eine E-Mail, die von einer E-Mail-Adresse empfangen wurde, die nicht in der Liste mit autorisierten E-Mail-Adressen vorhanden ist, wird gelöscht. Die E-Mail-Druckfunktion ist standardmäßig ausgeschaltet. Der Administrator kann die E-Mail-Druckfunktion ein- und ausschalten.

Auftragsmanagement

Für die Durchführung von Auftragsaktionen für Aufträge, die an den Fiery server gesendet werden, ist ein Fiery Dienstprogramm für das Auftragsmanagement entweder mit Administrator- oder Bediener-Zugriff erforderlich.

Auftragsprotokoll

Das Auftragsprotokoll wird auf dem Fiery server gespeichert. Einzelne Einträge im Auftragsprotokoll können nicht gelöscht werden. Das Auftragsprotokoll enthält Informationen zu Druck- und Scanaufträgen, z. B. den Namen des Benutzers, der den Auftrag ausgelöst hat, den Auftragsausführungszeitpunkt und bestimmte Auftragsmerkmale in Bezug auf verwendetes Papier, Farbe usw. Mit dem Auftragsprotokoll kann die Auftragsaktivität auf dem Fiery server überprüft werden.

Ein Benutzer mit Bediener-Zugriff kann das Auftragsprotokoll über Command WorkStation anzeigen, exportieren oder drucken. Ein Benutzer mit Administrator-Zugriff kann das Auftragsprotokoll über Command WorkStation löschen.

Setup

Für das Setup ist ein Administratorkennwort erforderlich. Der Fiery server kann über das Tool Configure in WebTools oder Command WorkStation bzw. über die Funktion „Setup“ auf dem Druckerbedienfeld eingerichtet werden.

Scannen

Der Fiery server ermöglicht, dass ein Bild, das sich auf dem Druckerglas befindet, an die Workstation zurückgescannt wird, die den Scan ausgelöst hat. Wenn eine Scanfunktion von einer Workstation aus ausgelöst wurde, wird ein Bitmap-Bild im RAW-Format direkt an die Workstation gesendet.

Der Benutzer kann Dokumente auf dem Fiery server scannen, um sie zu verteilen, zu speichern oder abzurufen. Alle gescannten Dokumente werden auf die Festplatte geschrieben. Der Administrator kann den Fiery server so konfigurieren, dass Scanaufträge nach einem vorgegebenen Zeitrahmen automatisch gelöscht werden.

Verteilen gescannter Aufträge

Scanaufträge können mithilfe verschiedener Methoden verteilt werden.

E-Mail

Eine E-Mail mit einem Anhang des gescannten Auftrags wird an einen Mailserver gesendet und von dort an das gewünschte Ziel weitergeleitet.

Hinweis: Wenn die Dateigröße des gescannten Auftrags die vom Administrator definierte Maximalgröße überschreitet, wird der Auftrag auf dem Fiery server Festplattenlaufwerk gespeichert, das über eine URL zugänglich ist.

FTP

Die Datei wird an ein FTP-Ziel gesendet. Die Übertragung, einschließlich des Ziels, wird im FTP-Protokoll aufgezeichnet, das über den Befehl „Seiten drucken“ über das Druckerbedienfeld zugänglich ist. Ein FTP-Proxy-Server kann definiert werden, um den Auftrag über eine Firewall zu senden.

Fiery server Warteschlange „Halten“

Die Datei wird an die Warteschlange „Halten“ des Fiery server gesendet und nicht mehr als Scanauftrag behandelt.

Weitere Informationen zur Warteschlange „Halten“ des Fiery server finden Sie unter Warteschlangen „Halten“, „Drucken“ und „Sequenzielles Drucken“ auf Seite 23.

Internetfax

Die Datei wird an einen Mailserver gesendet und von dort an das gewünschte Internetfax-Ziel weitergeleitet.

Mailbox

Die Datei wird auf dem Fiery server mit einer Mailbox-Codenummer gespeichert. Benutzer müssen die richtige Mailboxnummer eingeben, um auf den gespeicherten Scanauftrag zugreifen zu können. Benutzer haben die Möglichkeit, Kennwörter festzulegen, um den Inhalt Ihrer Scanmailboxen vor unbefugtem Zugriff zu schützen. Der Scanauftrag kann über eine URL abgerufen werden.

Konformität mit Verordnungen und Rahmenbedingungen

In der folgenden Tabelle finden Sie Informationen zur Konformität von Fiery Servern mit der Systemsoftware FS500 Pro/FS500 mit den entsprechenden Verordnungen und Rahmenbedingungen.

Verordnungen/ Rahmenbedingungen	**Umfang**	**NX-Serie (FS500 Pro)**	**A/E-Serie (FS500)**
FIPS 140-2	• US-Regierung (Bundesregierung und Staat) • Sicherheitsanforderungen für kryptografische Module	Konform mit den Verordnungen Windows 10 2019 LTSC FIPS-Zertifikate: • #3197 • #3196 • #3092	Nicht konform mit den Verordnungen
CIS-Benchmarks	• Global • Regierung/Privatsektor • Basiskonfiguration und bewährte Verfahren für die sichere Konfiguration eines Systems	Konform mit den Verordnungen Microsoft Windows 10 Enterprise (Release 1809) Benchmark	n.v.*
Leitfaden für die sicherheitstechnische Implementierung (STIG)	• Konfigurationsstandard der US-Regierung (Bundesregierung und Staat) bestehend aus Cybersicherheitsanforderungen für ein bestimmtes Produkt	Teilweise konform Windows 10 STIG Version 2, R3 Ausnahmen: CCI-000366: Vertrauenswürdiges Plattformmodul (Trusted Platform Module, TPM) nicht verfügbar	n.v.*

Verordnungen/ Rahmenbedingungen	Umfang	NX-Serie (FS500 Pro)	A/E-Serie (FS500)
ISO/IEC-15408	• Global • Allgemeine Kriterien • Bewertungskriterien für informationstechnische Sicherheitstechniken für IT-Sicherheit	Teilweise konform • LDAP-/AD-Authentifizierung für die Zugriffssteuerung erforderlich • TPM und sicheres Booten werden nicht unterstützt	Nicht konform mit den Verordnungen
IEEE 2600.2-2009	• Global • Regierung/Privatsektor • Allgemeines Kriterienprofil für Hardcopy-Geräte, Umgebung B	Teilweise konform • TPM und sicheres Booten werden nicht unterstützt • Die Anforderungen an Widerstandsfähigkeit und Erkennung erfordern ein optionales Fiery Laufwerkssicherheitskit	Nicht konform mit den Verordnungen
Safeguard Computer Security Evaluation Matrix (SCSEM)	• US-Regierung (Bundesregierung und Staat) • Steuerinformationssicherheitsleitlinien des Bundes, der Staaten und der lokalen Behörden	Teilweise konform • TPM und sicheres Booten werden nicht unterstützt • Die Anforderungen an Widerstandsfähigkeit und Erkennung erfordern ein optionales Fiery Laufwerkssicherheitskit	Nicht konform mit den Verordnungen
DoD 522.22-M	Standard für Datenbereinigung. 3 Zyklen	Konform mit den Verordnungen	Konform mit den Verordnungen
NIST 800-88	Standard für Datenbereinigung. 1 Zyklus	Nicht konform mit den Verordnungen	Nicht konform mit den Verordnungen
RMF-Zertifizierung der Armee	• US-Regierung • Rahmen für das Risikomanagement in der Informationstechnologie der Armee	Teilweise konform • TPM und sicheres Booten werden nicht unterstützt	Teilweise konform • TPM und sicheres Booten werden nicht unterstützt

* Außerhalb des Anwendungsbereichs der Verordnung oder der Rahmenbedingung. Linux-basierte Server der A- und E-Serie sind geschlossene Systeme, die keinen direkten Zugriff auf das Dateisystem haben. Eine eingeschränkte Sichtbarkeit des Netzwerks verhindert einen unbefugten Zugriff.

FIPS 140-2-Konformität

Bei ordnungsgemäßer Konfiguration erfüllen Fiery Server, auf denen FS500 Pro unter Windows 10 2019 LTSC ausgeführt wird, die Richtlinien zur Datenverschlüsselung nach FIPS 140-2. Ein Fiery Server im *FIPS 140-2-Modus* verwendet ausschließlich kryptografische Algorithmen, die im Rahmen des Cryptographic Algorithm Validation Program (CAVP) der US-Bundesregierung validiert und zertifiziert wurden, um Daten im Ruhezustand und bei der Übertragung zu verschlüsseln.

Um den *FIPS 140-2-Modus* in Fiery zu aktivieren, muss der Benutzer einen erweiterten Konfigurationsprozess zur Absicherung des Servers durchführen.

Richtlinien für die sichere Fiery Server-Konfiguration

Anhand der folgenden Richtlinien können Fiery Administratoren die Sicherheit bei der Konfiguration des Fiery server verbessern.

Ändern des Administratorkennworts

Wir empfehlen Ihnen, das Fiery Administrator-Standardkennwort bei der Installation und in regelmäßigen Abständen gemäß den Sicherheitsrichtlinien Ihrer Organisation zu ändern. Das Administrator-Standardkennwort sollte beim erstmaligen Setup in Assistent für Fiery Setup geändert werden. Das Administrator- und Operator-Kennwort kann nach der erstmaligen Einrichtung in den WebTools geändert werden: Configure > Sicherheit > Administrator-Kennwort (bzw. Bediener-Kennwort). Die Kennworteinrichtung ist auch unter Benutzerkontenverfügbar.

Mit dem Administratorkennwort hat der Benutzer Vollzugriff auf den Fiery server, sowohl lokal als auch über einen Remote-Client. Der Vollzugriff umfasst unter anderem:

- Dateisystem
- Systemsicherheitsrichtlinien
- Registrierungseinträge
- Administratorkennwort, das anonymen Benutzern den Zugriff auf den Fiery server verweigert

Empfohlene Einstellungen

- Wählen Sie die Sicherheitsstufe Maximum für SNMP in Netzwerk > SNMP:

  Das Auswählen der maximalen Sicherheitsstufe beschränkt die Unterstützung auf dem Fiery server lediglich auf SNMP V3.

  Wenn der SNMP Manager nur mit SNMP v1/v2c arbeitet, ändern Sie den Wert des Felds Community-Name lesen. Der Fiery server ermöglicht es Ihnen, die Werte der SNMP-Felder Community-Name lesen und Community-Name schreiben in WebTools (Configure > Netzwerk > SNMP) und über das Druckerbedienfeld (Netzwerk > SNMP) zu ändern.
- Deaktivieren Sie WSD in „Auftragsübergabe“.
- Deaktivieren Sie Windows-Druck in „Auftragsübergabe“, wenn Sie LPR, Port 9100 oder IPP zum Drucken verwenden.
- Blockieren Sie Ports durch das Aktivieren des TCP/IP-Port-Filters in Sicherheit > TCP/IP Port-Filterung.

  Löschen Sie die Ports 137-139 und 445, wenn Sie Windows-Druck nicht verwenden und es nicht notwendig ist, auf Dateiordner zuzugreifen oder diese zu teilen. Deaktivieren Sie die ungesicherte Kommunikation über Port 80 (HTTP).

Zusätzlich zu den Schutzmaßnahmen auf Betriebssystemebene verfügt der Fiery server über die folgenden zusätzlichen Sicherheitsfunktionen, um Ihre Daten zu schützen:

- Fiery servers verfügen über die Funktion „Vertraulich drucken“, um sicherzustellen, dass der Benutzer nur seinen Druckauftrag annimmt.
- Fiery servers binden die maßgeblichen Auftragsabrechnungslösungen mit ein, um zusätzliche Sicherheit durch FollowMe Printing zu bieten.

Fiery servers verfügen über zahlreiche Sicherheitsfunktionen, sind aber keine mit dem Internet verbundenen Server. Sie sollten in einer geschützten Umgebung aufgestellt werden und ihre Zugänglichkeit sollte vom Netzwerkadministrator entsprechend konfiguriert werden.

Auswählen des Sicherheitsprofils Hoch

Der Fiery server stellt vordefinierte Sicherheitsempfehlungen bereit, die auf verschiedenen Risiken und Bedrohungsstufen basieren (Standard, Hoch, Aktuell). Diese Funktion wird als Sicherheitsprofile bezeichnet und kann über die folgenden Programme aufgerufen werden:

- Fiery Software Assistent
- WebTools > Configure > Sicherheit

Das Sicherheitsprofil Hoch ermöglicht dem Fiery server, noch sicherer zu sein, und aktiviert die am häufigsten verwendeten Sicherheitsfunktionen.

Option	Hoch
TCP/IP-Port-Filterung	Aktiviert
Service Location Protocol (SLP)	Deaktiviert
Bonjour	Deaktiviert
Sicheres Löschen	Aktiviert
Remote Desktop	Deaktiviert
SMB-Kennwort	Aktiviert
USB-Speichergeräte	Deaktiviert
PostScript-Sicherheit	Aktiviert
Port 9100	Deaktiviert
LPD	Aktiviert
Windows-Druck	Deaktiviert
IPP	Aktiviert
WSD (Web Services for Devices)	Deaktiviert
Per E-Mail drucken	Deaktiviert

Option	Hoch
Drucken über FTP	Deaktiviert
Direkter Mobildruck	Deaktiviert

EFI empfiehlt, das Sicherheitsprofil Hoch für Umgebungen mit maximalen Sicherheitsanforderungen zu verwenden.

Schlussfolgerung

EFI verfügt über mehrere solide Standard- und optionale Sicherheitsfunktionen auf dem Fiery server, um unseren Kunden umfassende und individuell anpassbare Sicherheitslösungen für jede Umgebung zu bieten. EFI sorgt dafür, dass der Fiery server vor Anfälligkeiten gegenüber schädlicher oder unbeabsichtigter Nutzung effektiv geschützt ist, damit unsere Kunden in ihren Unternehmen mit maximaler Effizienz arbeiten können.