Whitepaper – Fiery Sicherheit

Fiery FS200 Pro / FS200 Server

Veröffentlichungsdatum: Mai 2018

Whitepaper-Reihe

Whitepaper – Fiery Sicherheit

Inhalt

1 Übersicht über dieses Dokument

Dieses für Kunden konzipierte Dokument beschreibt in Grundzügen die Architektur des Fiery® Servers und funktionale Aspekte, die unter dem Aspekt der Sicherheit und des Datenschutzes für den Fiery FS200 / FS200 Pro Server relevant sind. Dabei kommen Themen wie Hardware, Netzwerksicherheit, Zugriffssteuerung, Betriebssystem und Datensicherheit zur Sprache.

Das Dokument soll über die vielfältigen Sicherheitsvorkehrungen des Fiery Servers und deren Vorteile informieren und helfen, potenzielle Schwachstellen zu erkennen.

1.1 EFI Sicherheitsstrategie

EFI™ ist sich der vordringlichen Bedeutung bewusst, die der Datenschutz und die Datensicherheit für heutige Unternehmensumgebungen haben. Der Fiery Server ist daher mit einer Vielzahl an leistungsstarken Funktionen zum Schutz und zur Sicherheit wichtiger Ressourcen ausgerüstet.

In enger Zusammenarbeit mit OEM-Partnern und interdisziplinären Teams weltweit verfolgt EFI das Ziel, aktuelle und künftige Sicherheitsanforderungen von Unternehmen proaktiv zu bestimmen, um Sicherheitsrisiken für EFI Produkte bereits im Vorfeld auszuschließen.

Trotzdem gilt die Empfehlung, im Interesse der umfassenden Sicherheit für das Gesamtsystem die Fiery Sicherheitsfunktionen durch andere Präventiv- und Schutzmaßnahmen (z. B. sichere Kennwörter und physische Sicherheitssysteme) zu ergänzen.

1.2 Konfigurieren sicherheitsrelevanter Funktionen in Fiery Configure

Ein Anwender, der sich an der Anwendung Fiery Command WorkStation® als Fiery Administrator anmeldet, kann in Fiery Configure auf alle sicherheitsrelevanten Funktionen und Optionen des Fiery Systems zugreifen. Der Zugriff auf Fiery Configure ist zusätzlich auch über die Registerkarte „Konfigurieren“ der WebTools™ möglich.

2 Hardware und physische Sicherheit

2.1 Flüchtiger Arbeitsspeicher

Der Fiery Server nutzt flüchtige Speicherzellen als lokalen CPU-Arbeitsspeicher sowie für das Betriebssystem, die Fiery Systemsoftware und die Bilddatenverarbeitung. In den RAM-Speicher geladene Daten verbleiben dort, nur solange das Gerät mit Strom versorgt wird. Beim Ausschalten werden alle diese Daten gelöscht.

2.2 Nichtflüchtiger Arbeitsspeicher und Datenspeicher

Für Daten, die beim Ausschalten des Fiery Servers erhalten bleiben sollen – hierzu gehören Informationen der Systemprogrammierung sowie Anwenderdaten – kommen beim Fiery Server verschiedene nichtflüchtige Speichertechnologien zum Einsatz.

2.2.1 Flashspeicher

Der Flashspeicher enthält Programmdaten für die Eigendiagnose und für das Booten (BIOS) sowie die Systemkonfiguration betreffende Daten. Diese Baugruppe wird im Werk programmiert und kann nur durch das Installieren spezieller, von EFI bereitgestellter Patches umprogrammiert werden. Wenn diese Daten beschädigt, verfälscht oder gelöscht werden, lässt sich das System nicht starten.

Ein Teil des Flashspeichers wird außerdem verwendet, um optionale Fiery Software mithilfe eines Dongles aktivieren zu können.

In dieser Baugruppe werden keine Anwenderdaten gespeichert, und Anwender haben keinen Zugriff auf die Daten in dieser Baugruppe.

2.2.2 CMOS

Im batteriebetriebenen CMOS-Speicher werden die Maschineneinstellungen des Servers gespeichert. Keine dieser Informationen ist als vertraulich oder personenbezogen zu werten. Bei einem Fiery Server unter Windows 8.1 Pro können Anwender auf die Einstellungen über die Fiery Integrated Workstation (FACI, mit Monitor, Tastatur und Maus) zugreifen, sofern die FACI-Schnittstelle verfügbar ist.

2.2.3 NVRAM

Im Fiery Server befinden sich mehrere kleine NVRAM-Baugruppen mit operativer Firmware. Diese Baugruppen enthalten betriebsnotwendige Informationen, die aber nicht kundenbezogen sind. Anwender haben keinen Zugriff auf die darin gespeicherten Daten.

2.2.4 Festplattenlaufwerk

Während des regulären Druck- und Scanbetriebs sowie beim Generieren der Informationen für die Auftragsverwaltung werden Bilddaten in einen Direktzugriffsbereich auf dem Festplattenlaufwerk (HDD) geschrieben.

Diese Bilddaten und die verwaltungsrelevanten Informationen können manuell vom Operator oder automatisch nach einer gewissen Zeit gelöscht werden. Danach ist kein Zugriff auf die Bilddaten mehr möglich.

Zum Schutz von Bilddaten vor unbefugtem Zugriff bietet EFI die Funktion für das sichere Löschen (siehe Abschnitt 6.2.5). Wird diese Funktion aktiviert, wird die vom Systemadministrator gewählte Aktion zum jeweiligen Zeitpunkt ausgeführt, um gelöschte Daten nicht wiederherstellbar von der Festplatte zu entfernen.

2.2.5 Physische Anschlüsse

Verbindungen zum Fiery Server können über die folgenden externen Anschlüsse hergestellt werden:

Anschlüsse am Fiery Server	Funktion	Zugriff	Zugriffssteuerung
Ethernet RJ-45-Anschluss	Ethernet-Konnektivität	Netzwerkverbindungen (vgl. Drucken und Netzwerkverbindungen)	Mittels IP-Adressfilter
Anschluss der Kopierer-schnittstelle	Drucken/ Scannen	Dedizierte Kommunikation (Senden/ Empfangen) mit der Druckmaschine	n. v.
USB-Anschluss	Anschließen von USB-Geräten	Plug-and-Play-Anschluss für optionale Wechseldatenträger	Die USB-Druckfunktionalität kann deaktiviert werden. Der Zugriff auf USB-Speichergeräte kann über die Windows-Gruppenrichtlinie ausgeschaltet werden.

2.3 Lokale Schnittstelle

Bei einem Fiery Server unter Windows 8.1 Pro ist der Zugriff auf die Fiery Funktionen über die FACI- (sofern aktiviert) oder über die LCD-Schnittstelle (Bedienfeld) am Fiery Server möglich. Bei einem Fiery Server mit aktivierter FACI-Schnittstelle wird der Zugriff über die FACI durch das Windows-Administratorkennwort gesteuert. Über die LCD-Schnittstelle am Fiery Server ist der Zugriff auf wenige Funktionen beschränkt, die kein Sicherheitsrisiko bergen.

2.4 Optionales Kit für entfernbare Festplatte

Bei erhöhten Sicherheitsanforderungen unterstützt der Fiery Server ein optionales Kit für entfernbare Festplatten. Das oder die Festplattenlaufwerke können bei Normalbetrieb im System verriegelt und nach dem Ausschalten aus dem Gerät entfernt werden, um an einem sicheren Ort verwahrt zu werden.

2.4.1 Für externe Servercomputer

Der Fiery Server unterstützt ein optionales Kit für entfernbare Festplatten. Für welche Fiery Produkte dieses Kit im Einzelnen angeboten wird, hängt von den vertraglichen Vereinbarungen (EFI Development and Distribution Agreements) mit den OEM-Partnern ab.

2.4.2 Für eingebettete Serverprodukte

Für eingebettete Produkte („Embedded“) ist eine Option für entfernbare Festplatten nur als Gemeinschaftslösung möglich, da Schächte und Halterungen zusammen mit dem OEM gezielt für das jeweilige Multifunktionsgerät (MFP) entwickelt werden müssen. Das optionale Kit sieht vor, dass das eingebaute Festplattenlaufwerk aus dem Chassis des Geräts in eine externe Anlage mit eigener Stromversorgung umgesetzt wird.

3 Netzwerksicherheit

Zu den Standardfunktionen des Fiery Servers im Hinblick auf die Netzwerksicherheit gehört die Möglichkeit, die Druckberechtigung nur autorisierten Anwendern und Gruppen zu erteilen, die Gerätekommunikation auf vorgegebene IP-Adressen zu beschränken und Netzwerkprotokolle und Ports einzeln zu aktivieren oder zu deaktivieren.

Ungeachtet der Tatsache, dass der Fiery Server unterschiedlichste Sicherheitsfunktionen bietet, ist zu beachten, dass er nicht als ein direkt mit dem Internet verbundener Server konzipiert ist. Er sollte in eine geschützte Umgebung integriert werden, und die Methoden und Wege des Zugriffs auf ihn sollten vom Netzwerkadministrator sorgfältig konfiguriert werden.

3.1 Netzwerkports

Der Netzwerkadministrator kann auf dem Fiery Server die folgenden IP-Ports einzeln aktivieren und deaktivieren, sodass unerwünschte Gerätekommunikation und Systemzugriffe über bestimmte Transportprotokolle sehr effizient abgeblockt werden können.

TCP	UDP	Port	Abhängige(r) Dienst(e)
20–21		FTP	
80		HTTP	WebTools, IPP
135		MS RPC	Microsoft® RPC-Dienst (nur Windows 8.1 Pro). Ein weiterer Port im Bereich 49152-65536 wird für den SMB-basierten Point-and-Print-Dienst geöffnet.
137–139		NETBIOS	Windows-Druckunterstützung
	161, 162	SNMP	WebTools, Fiery Central, einige ältere Dienstprogramme und SNMP-basierte Werkzeuge
	427	SLP	
443		HTTPS	WebTools, IPP/s
445		SMB/IP	SMB über TCP/IP
	500	ISAKMP	IPsec
515		LPD	LPR-Druckunterstützung, einige ältere Dienstprogramme (z. B. WebTools und ältere Versionen von CWS)
631		IPP	IPP
3050			Firebird
	4500	IPsec NAT	IPsec
	5353	Multicast-DNS	Bonjour
3389		RDP	Remote Desktop (Windows Fiery servers only)
3702	3702	WS-Discovery	WSD
6310 8010 8021–8022 8090 9906 18021 18022 18081 18082 21030 22000 50006 – 50025*	9906	EFI Ports	Command WorkStation 4 und 5, Fiery Central, EFI SDK-basierte Werkzeuge, bidirektionale Kommunikation des Fiery Druckertreibers, WebTools, direkter Mobildruck und Konvertierung nativer Dokumente.
9100–9103		Druckport	Port 9100

Andere TCP-Ports sind (mit Ausnahme der vom OEM spezifizierten Ports) deaktiviert. Auf einen Dienst, dessen zugewiesener Port deaktiviert ist, kann nicht remote zugegriffen werden.

Die vom Fiery Server bereitgestellten Netzwerkdienste können vom Fiery Administrator ebenfalls einzeln aktiviert und deaktiviert werden.

Vom lokalen Administrator können darüber hinaus die Namen der Read- und der Write-Community für SNMP und weitere Sicherheitseinstellungen festgelegt werden.

3.2 IP-Adressfilterung

Autorisierte Verbindungen zum Fiery Server können auf Hosts beschränkt werden, deren IP-Adressen in einem vorgegebenen IP-Adressbereich liegen. Von nicht autorisierten IP-Adressen ausgehende Befehle oder Aufträge werden vom Fiery Server ignoriert.

3.3 Netzwerkverschlüsselung

3.3.1 IPsec

IPsec (Internet Protocol security) bietet durch die Verschlüsselung und Authentifizierung jedes einzelnen Datenpakets ein hohes Maß an Sicherheit bei allen über IP-Protokolle kommunizierenden Anwendungsprogrammen.

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 und Fiery Server hergestellt wurde, werden alle Kommunikationsdaten – auch Druckaufträge – sicher über das Netzwerk transferiert.

* Diese Ports sind aktiviert, sobald Fiery Command WorkStationversion 6.2 oder höher auf einem externen Fiery Server installiert wird.

3.3.2 SSL und TLS

SSL/TLS sind auf Anwendungsebene angesiedelte Protokolle für die sichere Übertragung von Nachrichten über das Internet. Der Fiery Server unterstützt die Protokolle SSL v3 und TLS v1.0/v1.1/v1.2.

SSL/TLS wird beim Fiery Server für verschiedene Zwecke genutzt, z. B. um Anwendern den sicheren Zugriff auf die Homepage des Fiery Servers und auf Web-APIs zu ermöglichen. Auch Verbindungen zu LDAP- und E-Mail-Servern können so konfiguriert werden, dass die Kommunikation über SSL/TLS erfolgt.

3.3.3 Zertifikatverwaltung

Der Fiery Server bietet eine Schnittstelle für die Verwaltung von Zertifikaten, die bei der SSL/TLS-Kommunikation zum Einsatz kommen. Zertifikate werden im Format X.509 unterstützt.

Über die Schnittstelle für die Zertifikatverwaltung können Fiery Administratoren:

- Selbstsignierte digitale Zertifikate erstellen
- Ein Zertifikat und dessen privaten Schlüssel zu einem Fiery Server hinzufügen
- Von einer Zertifizierungsstelle ausgegebene Zertifikate hinzufügen, anzeigen und entfernen

3.4 IEEE 802.1x

802.1x ist ein IEEE-Standardprotokoll für die Zugriffssteuerung basierend auf Netzwerkports. Das Protokoll sorgt dafür, dass Geräte authentifiziert werden, ehe sie Zugriff auf ein LAN und dessen Ressourcen erhalten.

Beim Aktivieren der Funktion kann festgelegt werden, ob „EAP MD5-Challenge“ oder „PEAP-MSCHAPv2“ für die Authentifizierung am 802.1x-Authentifizierungsserver verwendet werden soll.

Der Fiery Server wird authentifiziert, wenn er gebootet oder das Ethernet-Kabel abgezogen und neu angeschlossen wird.

3.5 SNMP v3

Mit SNMPv3 unterstützt der Fiery Server ein sicheres Netzwerkprotokoll für die Verwaltung von Geräten in IP-Netzwerken. Zur Wahrung der Vertraulichkeit können SNMPv3-Kommunikationspakete verschlüsselt werden. Außerdem stellt dieses Protokoll die Integrität und Authentifizierung auf Nachrichtenebene sicher.

Der Fiery Administrator kann zwischen drei SNMPv3-Sicherheitsstufen wählen. Er kann auch veranlassen, dass vor SNMP-Transaktionen die Authentifizierung verpflichtend erfolgen muss und dass SNMP-Anwendernamen und Kennwörter verschlüsselt werden.

3.6 E-Mail-Sicherheit

Der Fiery Server unterstützt die Protokolle POP und SMTP. Zum Schutz des Dienstes vor Angriffen und vor Missbrauch kann der Fiery Administrator ergänzende Sicherheitsfunktionen aktivieren, z. B.:

3.6.1 POP before SMTP

Einige E-Mail-Server unterstützen noch immer das ungesicherte SMTP-Protokoll und damit das Senden von E-Mail-Nachrichten ohne Authentifizierung. Um nicht autorisierte Zugriffe zu verhindern, zwingen bestimmte E-Mail-Server ihre Clients, sich über POP zu authentifizieren, bevor sie eine E-Mail-Nachricht über SMTP senden können. Für solche E-Mail-Server muss der Fiery Administrator die Option „POP before SMTP“ aktivieren.

3.6.2 OP25B

OP25B (Outbound port 25 Blocking) ist eine Schutzmaßnahme gegen Spam-Nachrichten, mit der Internetanbieter an Port 25 gesendete Pakete auf ihren Routern blockieren können. Beim Setup kann der Fiery Administrator für die E-Mail-Konfiguration einen anderen Port wählen.

4 Zugriffssteuerung

4.1 Anwenderauthentifizierung

Die Funktion des Fiery Servers für die Anwenderauthentifizierung dient folgenden Zwecken:

- Anwendernamen authentifizieren
- Aktionen ausgehend von den Anwenderberechtigungen zulassen.

Der Fiery Server kann Anwender authentifizieren, deren Konten (Accounts) wie folgt definiert sind:

- In einer Domäne: Der Anwender ist auf einem Unternehmensserver definiert, auf den über LDAP zugegriffen wird.
- Auf dem Fiery Server: Der Anwender ist direkt auf dem Fiery Server definiert.

Aktionen werden einem Anwender ausgehend von der Gruppe verfügbar gemacht, der er angehört. Jeder Gruppe sind bestimmte Berechtigungen zugewiesen (z. B. „In S/W drucken“ oder „In Farbe und S/W drucken“), und die für eine Gruppe verfügbaren Aktionen sind durch die ihr zugewiesenen Berechtigungen beschränkt.

Fiery Gruppen sind Anwendergruppen mit spezifischen Berechtigungen. Mithilfe von Fiery Gruppen können bestimmte Berechtigungen kollektiv mehreren Anwendern zugeordnet werden.

Der Fiery Administrator kann die Berechtigungen einer Fiery Gruppe jederzeit ändern. Von Änderungen ausgenommen sind nur die Standardanwender „Administrator“, „Operator“ und „Gast“.

Bei dieser Version der Anwenderauthentifizierung können für Gruppen die folgenden Berechtigungen bearbeitet und gewählt werden:

- In S/W drucken – Die Anwender der Gruppe dürfen nur Schwarzweißaufträge auf dem Fiery Server drucken. Ein Farbauftrag wird automatisch in Schwarzweiß gedruckt, wenn er von einem Anwender stammt, der nicht über die Berechtigung „In Farbe und S/W drucken".
- In Farbe und S/W drucken – Die Anwender der Gruppe dürfen Druckaufträge unter Verwendung aller Farb- und Graustufeneinstellungen des Fiery Servers drucken. Aufträge eines Anwenders, der weder über diese Berechtigung noch über die Berechtigung „In S/W drucken“ verfügt, werden vom Fiery Server generell nicht gedruckt, und auch die Übergabe von Aufträgen per FTP ist ausgeschlossen (nur bei Farbausgabegeräten).
- Fiery Mailbox – Jeder Anwender der Gruppe erhält 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 eine Mailbox ist auf solche Anwender beschränkt, die den Mailbox- bzw. Anwendernamen und das zugehörige Kennwort kennen.
- Kalibrierung – Die Anwender der Gruppe sind berechtigt, die Farbkalibrierung vorzunehmen.
- Servervorgaben erstellen – Die Anwender der Gruppe dürfen Servervorgaben erstellen, um anderen Anwendern des Fiery Servers den unmittelbaren Zugriff auf häufige Kombinationen von Auftragseinstellungen zu ermöglichen.
- Workflows verwalten – Die Anwender der Gruppe dürfen virtuelle Drucker erstellen, veröffentlichen und bearbeiten.

Hinweis: Die Anwenderauthentifizierung ersetzt die bisherige Druckgruppenfunktionen.

4.2 Authentifizierung durch Fiery Software

Der Fiery Server unterstützt mit „Administrator“, „Operator“ und „Gast“ drei Standardanwender mit vordefinierten Berechtigungen. Diese Anwenderkonten sind nicht identisch mit unter Windows definierten Benutzerkonten oder Rollen. Ihr Geltungsbereich ist auf die Fiery Software beschränkt. Es wird empfohlen, dass für Anwender, die als Administrator auf den Fiery Server zugreifen, die Eingabe eines Kennworts verpflichtend ist. EFI empfiehlt außerdem, das standardmäßige Administratorkennwort im Einklang mit den kundeneigenen Sicherheitsrichtlinien durch ein Kennwort eigener Wahl zu ersetzen und turnusmäßig zu ändern.

Die drei Standardanwender haben folgende Berechtigungen:

- Administrator – Der Administrator kann alle Funktionen und Funktionalitäten des Fiery Servers in umfassender Weise steuern.
- Operator – Der Operator hat weniger Berechtigungen als der Administrator. Er hat keinen Zugriff auf die Setup-Optionen und er ist nicht berechtigt, das Auftragsprotokoll zu löschen.
- Gast (Standard; kein Kennwort) – Der Gast hat die wenigsten Berechtigungen. Er hat keinen Zugriff auf das Auftragsprotokoll, er kann keine Änderungen an Aufträgen oder deren Status vornehmen und er kann Aufträge nicht in der Vorschau anzeigen.

5 Betriebssystemumgebung

5.1 Vorgänge beim Systemstart

Beim Starten des Systems werden das Betriebssystem und die Fiery Systemsoftware vom internen Festplattenlaufwerk geladen.

Das BIOS auf der Fiery Hauptplatine (die Informationen zum Booten des Betriebssystems) steht nur im Lesezugriff zur Verfügung. Änderungen am BIOS (oder das Entfernen der BIOS-Daten) verhindern den regulären Betrieb des Fiery Servers.

Die Mehrzahl der beim Setup festgelegten Einstellungen ist auf der Konfigurationsseite vermerkt. Bestimmte Angaben (z. B. die FTP-Proxy-Informationen, Kennwörter und die Namen der SNMP-Gemeinschaften) fehlen aber bewusst auf der gedruckten Konfigurationsseite.

5.2 Linux

Linux-Systeme bieten keine lokale Schnittstelle für den Zugriff auf das Betriebssystem.

5.2.1 Antivirussoftware unter Linux

Das Betriebssystem (OS) Linux wird beim Fiery Server in einer dedizierten, spezifisch angepassten Version verwendet. Diese Version umfasst keine allgemeinen Linux-Systemkomponenten (z. B. Ubuntu), sondern nur die für den Fiery Server notwendigen OS-Komponenten. Diese dedizierte OS-Version bietet zusätzlich zu einer Leistungsoptimierung auch den Vorteil, dass sie weniger virenanfällig ist als handelsübliche Linux- und Microsoft-Betriebssysteme. Antivirussoftware, die für handelsübliche OS-Versionen von Linux ausgelegt sind, kann auf dem Fiery Server möglicherweise nicht ausgeführt werden.

5.3 Windows 8.1 Pro

Beim Betriebssystem Windows 8.1 wird der Fiery Server mit einem Standardkennwort für das Administratorkonto ausgeliefert. Es wird empfohlen, dieses Standardkennwort schon bei der Installation durch ein eigenes Kennwort zu ersetzen.

Außerdem sollte das Kennwort regelmäßig und gemäß den unternehmenseigenen IT-Richtlinien geändert werden.

Das Administratorkennwort ermöglicht – sowohl bei lokaler Anmeldung als auch von einer remoten Workstation – den umfassenden Zugriff auf den Fiery Server: auf das Dateisystem, auf die Sicherheitsrichtlinien und auf die Registrierungseinträge (ohne darauf beschränkt zu sein).

Außerdem kann der Administrator das Administratorkennwort ändern und allen Anwendern den Zugriff auf den Fiery Server verwehren.

5.3.1 Microsoft Sicherheitspatches

Zum Schließen potenzieller Sicherheitslücken im Betriebssystem Windows 8.1 veröffentlicht Microsoft regelmäßig Sicherheitspatches. Windows Update ist standardmäßig so konfiguriert, dass eine Benachrichtigung angezeigt wird, wenn ein Patch verfügbar ist, die Patchsoftware aber nicht automatisch geladen wird. Der Fiery Administrator kann dieses Standardverhalten von Windows Update ändern oder die Patches manuell laden.

5.3.2 SMS-Werkzeuge

Für einen Windows-basierten Fiery Server stellt EFI ein eigenes Werkzeug zum Aktualisieren der Systemsoftware bereit, mit dem sich der Abruf von Updates für die Fiery Software und auch von Microsoft-Sicherheitspatches steuern lässt. Der Fiery Server unterstützt keine SMS-Werkzeuge von Drittanbietern für den Abruf oder die Push-Bereitstellung von Updates für den Fiery Server.

5.3.3 Antivirussoftware unter Windows

Antivirussoftware kann i. d. R. auf dem Fiery Server ausgeführt werden. Allerdings wird Antivirussoftware in vielen Varianten und gelegentlich in Kombination mit Funktionen für spezifische Bedrohungsszenarien angeboten. Bei der Wahl der Antivirussoftware sollten daher die folgenden Aspekte berücksichtigt werden. Eine Antivirussoftware ist bei einem Fiery Server mit lokaler FACI-Schnittstelle sinnvoll, da hier das Risiko einer Infizierung infolge von Windows-Standardaktionen am größten ist. Bei einem Fiery Server ohne FACI-Schnittstelle kann dessen internes Festplattenlaufwerk mit einer Antivirussoftware von einem remoten PC aus gescannt werden. EFI empfiehlt bei Fragen zur Vorgehensweise die Rücksprache mit dem Hersteller der Antivirussoftware.

Für die Komponenten einer Antivirussoftware für Windows gelten vonseiten EFI die folgenden Richtlinien:

Engine der Antivirussoftware – Das Scannen des Fiery Servers (ob geplant oder manuell) kann zu Leistungseinbußen des Fiery Systems führen.

Antispyware – Ein Antispyware-Programm kann die Leistung des Fiery Servers beim Empfang von Dateien beeinträchtigen. Zu beobachten ist dies ist z. B. beim Senden von Druckaufträgen und beim Laden von Daten, mit denen das Fiery System oder auf dem Fiery Server ausgeführte Anwendungsprogramme aktualisiert werden sollen.

Integrierte Firewall – Da der Fiery Server selbst über eine Firewall verfügt, ist eine Firewall der Antivirussoftware i. d. R. nicht nötig. EFI empfiehlt, nach Rücksprache mit der eigenen IT-Abteilung und anhand der Informationen im Abschnitt 3.1 zu entscheiden, ob eine durch die Antivirussoftware bereitgestellte Firewall sinnvoll und zweckmäßig ist.

Antispam – Das Fiery System unterstützt die Funktionalitäten „Drucken per E-Mail" und „Scannen für E-Mail", weshalb der Einsatz eines serverbasierten Filters für Spammail empfohlen wird. Der Fiery Server lässt sich außerdem so konfigurieren, dass Aufträge per E-Mail nur akzeptiert werden, wenn sie von vorgegebenen E-Mail-Absenderadressen stammen. Die Antispam-Komponente ist nicht erforderlich, da der Fiery Server die Ausführung einer E-Mail-Client-Software (z. B. Outlook) nicht unterstützt.

Positiv- und Negativlisten – Die Verwendung einer Positivliste (Whitelist) und (oder einer Negativliste (Blacklist) hat i. d. R. keine nachteiligen Auswirkungen auf den Fiery Server. EFI rät dringend zur Konfiguration dieser Funktionalität durch den Kunden, um zu verhindern, dass Fiery Module unbeabsichtigt auf die Negativliste gesetzt werden.

HID und Anwendungssteuerung – Aufgrund der Komplexität der HID-Geräteklasse (Human Device Interface) und der Anwendungssteuerung muss (bei Verwendung einer dieser Funktionalitäten) die Konfiguration der Antivirussoftware sorgfältig getestet und austariert werden. Bei sorgsamer Feinabstimmung sind HID und Anwendungssteuerung exzellente Schutzmaßnahmen, die problemlos mit dem Fiery Server genutzt werden können. Falsche HID-Parametereinstellungen und falsche Dateiausschlüsse können aber leicht zu Fehlfunktionen des Fiery Servers führen – oft auch in Fällen, in denen der „Standardwert beibehalten" wird. Zum Beheben eventueller Konflikte müssen die HID-Einstellungen und/oder die Einstellungen der Anwendungssteuerung im Kontext der Einstellungen des Fiery Servers geprüft und getestet werden (z. B. Netzwerkports, Netzwerkprotokolle, ausführbare Dateien, Konfigurationsdateien, temporäre Dateien usw.).

5.4 E-Mail-Viren

In E-Mail-Nachrichten versteckte Viren erfordern i. d. R. eine Aktion durch den Anwender, um sich ausbreiten zu können. Vor diesem Hintergrund werden Anhänge, die keine PDL-Dateien sind, vom Fiery Server abgewiesen. Der Fiery Server ignoriert außerdem auch E-Mail-Nachrichten in den Formaten RTF oder HTML und deren gesamten JavaScript-Inhalt.

Mit Ausnahme einiger weniger Nachrichten, die ein Anwender als Antwort auf eine Befehlsanfrage erhält, werden generell alle per E-Mail empfangenen Dateien als PDF-Aufträge behandelt. Weitere Hinweise zur E-Mail-Druckfunktionalität finden Sie im Abschnitt 6.4.

6 Datensicherheit

6.1 Verschlüsselung kritischer Informationen

Kritische Informationen wie Kennwörter und konfigurationsbezogene Informationen werden auf dem Fiery Server in verschlüsselter Form gespeichert, wobei NIST 2010-konforme Algorithmen zum Verschlüsseln verwendet werden.

6.2 Standarddruckverbindungen

Aufträge können an folgende Warteschlangen oder Druckverbindungen gesendet werden (sofern diese auf dem Fiery Server freigegeben sind):

- Warteschlange „Halten“
- Warteschlange „Drucken“
- Warteschlange „Sequenziell drucken“
- Warteschlange „Direkt“ (Direktverbindung)
- Virtuelle Drucker (vom Fiery Administrator definierte Warteschlangen)

Soll das automatische Drucken eingeschränkt werden, kann der Fiery Administrator die Warteschlangen „Halten“ und „Drucken“ deaktivieren. Bei aktiviertem Kennwortschutz bedeutet dies, dass nur Fiery Operatoren und Administratoren Aufträge drucken können.

6.2.1 Warteschlangen „Halten“, „Drucken“ und „Sequenziell drucken“

Ein an die Warteschlange „Halten“ oder „Drucken“ gesendeter Auftrag wird auf die Festplatte im Fiery Server gespoolt. Ein Auftrag in der Warteschlange „Halten“ verbleibt auf der Festplatte im Fiery Server, bis er in einer Software für die Auftragsverwaltung (z. B. Anwendung Fiery Command WorkStation oder Fiery Command WorkStation ME) zum Drucken freigegeben oder (mit der Option „Server löschen“) gelöscht wird.

Bei der Warteschlange „Sequenziell drucken“ werden die Aufträge strikt in der Reihenfolge verarbeitet und gedruckt, in der sie über das Netzwerk empfangen werden. Dieser Workflow wird als „First In, First Out“ (FIFO) bezeichnet. Die Reihenfolge von Aufträgen, die nicht an die Warteschlange „Sequenziell drucken“ gesendet werden, kann durch verschiedene Faktoren verändert werden, z. B. wenn kleinere Aufträge gedruckt werden können, solange ein umfangreicher Auftrag noch gespoolt wird. (Die entsprechende Option kann beim Setup aktiviert werden.)

6.2.2 Warteschlange „Gedruckt“

An die Warteschlange „Drucken“ gesendete Aufträge werden nach Abschluss der Druckausgabe in die Warteschlange „Gedruckt“ transferiert, sofern diese Warteschlange aktiviert ist. Die Anzahl der Aufträge, die in der Warteschlange „Gedruckt“ maximal enthalten sein dürfen, kann vom Fiery Administrator festgelegt werden. Ist die Warteschlange „Gedruckt“ nicht verfügbar, werden Aufträge nach Abschluss der Druckausgabe automatisch gelöscht.

6.2.3 Warteschlange „Direkt“ (direkte Druckverbindung)

Die direkte Druckverbindung ist zum Laden von Schriften und für Anwendungsprogramme konzipiert, die eine direkte Verbindung zum Fiery PostScript-Modul benötigen.

EFI rät davon ab, die direkte Verbindung zum Drucken von Aufträgen zu verwenden. Aufträge, die an die Warteschlange „Direkt“ gesendet werden, werden nach Abschluss der Druckausgabe automatisch vom Fiery Server gelöscht. EFI übernimmt allerdings keine Gewähr dafür, dass alle für einen Auftrag angelegten temporären Daten restlos entfernt werden.

VDP-, PDF- und TIFF-Dateien, die an die direkte Verbindung gesendet werden, werden automatisch an die Warteschlange „Drucken“ umgeleitet. Bei entsprechender Konfiguration können auch Aufträge, die über den SMB-Netzwerkdienst an die direkte Verbindung gesendet werden, an die Warteschlange „Drucken“ umgeleitet werden.

6.2.4 Löschen von Auftragsdaten

Wenn ein Auftrag (automatisch oder in einem Fiery Anwendungsprogramm) vom Fiery Server gelöscht wird, kann er mit den Mitteln der Fiery Software nicht mehr angezeigt oder wiederhergestellt werden. Bei einem Auftrag, der auf die Festplatte im Fiery Server gespoolt wurde, können aber Teile auf der Festplatte verbleiben, die theoretisch mit Spezialwerkzeugen (z. B. mit Werkzeugen für die Festplattenforensik) wiederhergestellt werden können.

6.2.5 Sicheres Löschen

Mit der Funktion für das sichere Löschen ist gewährleistet, dass inhaltliche Daten eines Auftrags unwiederbringlich von der Festplatte im Fiery Server entfernt wird, sobald der Auftrag in einem Fiery Anwendungsprogramm gelöscht wird. Mithilfe eines Algorithmus, der auf der Spezifikation US DoD5220.22M basiert, wird zu diesem Zweck zum Zeitpunkt des Löschvorgangs jede Quelldatei dreimal mit zufälligen Daten überschrieben.

Im Hinblick auf das sichere Löschen sind die folgenden Einschränkungen zu beachten:

- Die Funktion hat keine Auswirkung auf Dateien, die sich nicht auf dem Fiery Server, sondern an einer anderen Stelle im Gesamtsystem befinden, z. B.:
  – Kopien eines Auftrags, die im Zuge der Lastverteilung auf einen anderen Fiery Server transferiert wurden.
  – Kopien eines Auftrags, die auf Wechselmedien oder Netzwerklaufwerken archiviert wurden.
  – Kopien eines Auftrags auf Client-Workstations.
  – Seiten, die aus einem Auftrag in einen anderen Auftrag übernommen oder kopiert wurden.
- Die Funktion löscht keine Einträge aus dem Auftragsprotokoll.
- Wenn das System vor dem Ende des Löschvorgangs manuell ausgeschaltet wird, besteht keine Gewähr dafür, dass die Auftragsdaten restlos entfernt werden.
- Die Funktion löscht keine Auftragsdaten, die bei einer Auslagerung (Disk Swapping) oder Zwischenspeicherung (Disk Caching) auf die Festplatte geschrieben werden.
- Aufträge, die über einen FTP-Server geleitet werden, werden u. U. auf dem FTP-Clientsystem gespeichert, bevor sie an die Fiery Systemsoftware übergeben werden. Da die Fiery Systemsoftware keine Kontrolle über diesen Vorgang hat, können Aufträge, die auf dem FTP-Clientsystem gespeichert sind, nicht sicher gelöscht werden.
- Über SMB gedruckte Aufträge werden mithilfe des Spoolers auf den Fiery Server transferiert und auf dessen Festplatte geschrieben. Da die Fiery Systemsoftware keine Kontrolle über diesen Vorgang hat, können diese Aufträge nicht sicher gelöscht werden.

Hinweis: Durch Disk Swapping kann mehr virtueller Arbeitsspeicher bereitgestellt werden, als physisch vorhanden ist. Dieser Vorgang erfolgt auf Betriebssystemebene, weshalb der Fiery Server keine Kontrolle darüber hat. Der für das Disk Swapping genutzte Festplattenbereich wird aber häufig überschrieben, wenn bei OS-Operationen unterschiedliche Segmente aus dem Arbeitsspeicher auf die Festplatte ausgelagert und von dort zurück in den Arbeitsspeicher transferiert werden. Der Vorgang kann dazu führen, dass Segmente eines Auftrags kurzzeitig auf die Festplatte ausgelagert werden.

6.2.6 Systemspeicher

Beim Verarbeiten bestimmter Dateien werden u. U. Auftragsdaten in den Arbeitsspeicher des Betriebssystems geschrieben. In einigen Fällen wird der Inhalt des Arbeitsspeichers beim Disk Caching auf die Festplatte ausgelagert, wo er möglicherweise nicht explizit überschrieben wird.

6.3 Vertrauliches Drucken

Damit ein vertraulicher Auftrag tatsächlich gedruckt wird, muss vor Ort am Fiery Server ein für den Auftrag spezifisches Kennwort eingegeben werden. Diese Funktionalität erfordert eine lokale LCD-Schnittstelle zum Fiery System.

Die Funktionalität beschränkt den Zugriff auf ein Dokument auf Personen, die (a) das Auftragskennwort kennen und (b) physischen Zugang zum Fiery Server haben und vor Ort das Kennwort eingeben können.

6.3.1 Workflow

Der Anwender gibt im Fiery Druckertreiber ein Kennwort seiner Wahl in das Feld „Vertraulich drucken“ ein. Nachdem der Auftrag an die Warteschlange „Drucken“ oder „Halten“ gesendet wurde, verbleibt er in dieser Warteschlange, bis er durch die Eingabe des Kennworts zum Drucken freigegeben wird.

Hinweis: Der Inhalt eines Auftrags, dem mit der Option „Vertraulich drucken“ ein spezifisches Kennwort zugeordnet wurde, kann in der Anwendung Fiery Command WorkStation bzw. Fiery Command WorkStation ME nicht angezeigt werden.

Über die LCD-Schnittstelle zum Fiery System gibt der Anwender das Kennwort für seinen Auftrag ein. Der Anwender erhält dadurch Zugriff auf alle Aufträge, die unter Verwendung des eingegebenen Kennworts gesendet wurde. Er kann alle diese Aufträge drucken und/oder löschen.

Ein vertraulich gedruckter Auftrag wird nach Abschluss der Druckausgabe nicht in die Warteschlange „Gedruckt“ transferiert. Nach dem Ende des Druckvorgangs wird der Auftrag automatisch gelöscht.

6.4 E-Mail-Druckfunktionalität

Der Fiery Server ist in der Lage, per E-Mail gesendete Aufträge zu empfangen und zu drucken. Der Administrator kann für diesen Zweck auf dem Fiery Server eine Liste autorisierter E-Mail-Absenderadressen erstellen. Ein Auftrag, der nicht von einer dieser autorisierten E-Mail-Adressen stammt, wird automatisch gelöscht. Der Administrator kann die E-Mail-Druckfunktionalität auch komplett deaktivieren. Standardmäßig ist die E-Mail-Druckfunktionalität aktiviert.

6.5 Auftragsverwaltung

An den Fiery Server übergebene Aufträge können mit den Mitteln der Fiery Anwendersoftware nur verwaltet und bearbeitet werden, wenn die Anmeldung als Administrator oder als Operator erfolgt. Bei der Anmeldung als Gast (ohne Eingabe eines Kennworts) sind nur die Dateinamen und Attribute der Aufträge zu sehen. Es ist einem Gast nicht möglich, Aktionen für die Aufträge auszuführen oder die Aufträge in der Vorschau anzuzeigen.

6.6 Auftragsprotokoll

Das Auftragsprotokoll wird auf dem Fiery Server gespeichert. Es ist nicht möglich, einzelne Einträge aus dem Auftragsprotokoll zu löschen. Das Auftragsprotokoll enthält Angaben zu Druck- und Scanaufträgen, u. a. den Anwendernamen des Initiators eines Auftrags, den Ausführungszeitpunkt und bestimmte Auftragsmerkmale (z. B. das verwendete Papier und die Information, ob die Ausgabe in Farbe oder in S/W erfolgte). Anhand des Auftragsprotokolls lassen sich auftragsbezogene Aktivitäten auf dem Fiery Server nachverfolgen.

Der Operator kann in der Anwendung Fiery Command WorkStation das Auftragsprotokoll anzeigen, exportieren und drucken. Der Administrator kann das Auftragsprotokoll zusätzlich auch löschen. Ein Gast kann das Auftragsprotokoll über die LCD-Schnittstelle zum Fiery System nur drucken (sofern dieser Zugang vom Administrator eingerichtet wurde).

6.7 Setup

Zum Konfigurieren der Setup-Optionen für den Fiery Server muss das Administratorkennwort eingegeben werden. Das Setup kann mit Fiery Configure oder über die LCD-Schnittstelle zum Fiery Server erfolgen. Der Zugriff auf Fiery Configure ist über die Fiery WebTools oder die Anwendung Fiery Command WorkStation möglich.

6.8 Scannen

Der Fiery Server bietet die Möglichkeit, mithilfe eines TWAIN-Zusatzmoduls ein Papierdokument auf dem Vorlagenglas eines Kopierers zu scannen und den Scan auf die anfordernde Workstation zu transferieren. Dieses Zusatzmodul wird für Adobe® Photoshop und für Textbridge Anwendungsprogramme unterstützt. Wird ein Scanvorgang von einer Workstation aus initiiert, wird eine Bitmap-Datei im RAW-Format direkt an die anfordernde Workstation transferiert.

Scans, die verteilt oder später abgerufen werden sollen, können direkt auf dem Fiery Server gespeichert werden. Alle Scans werden auf die Festplatte geschrieben. Der Administrator kann den Fiery Server so konfigurieren, dass Scans nach Ablauf einer vorgegebenen Zeitspanne automatisch gelöscht werden.

Scans können mit den folgenden Methoden verteilt werden:

- E-Mail – Der Scan wird als Anhang einer E-Mail-Nachricht an den Mailserver gesendet und von dort an die Empfängeradresse geleitet. Hinweis: Wenn die Dateigröße eines Scans die vom Administrator definierte Maximalgröße überschreitet, wird der Scan auf der Festplatte im Fiery Server gespeichert und in Form seiner URL zugänglich gemacht.
- FTP – Der Scan wird in ein FTP-Zielverzeichnis transferiert. Der Transfer wird unter Angabe des Zielverzeichnisses im FTP-Protokoll aufgezeichnet, das mit der Option „Seiten drucken" über die LCD-Schnittstelle zum Fiery Server gedruckt werden kann. Damit Scans über eine Firewall hinweg transferiert werden können, kann ein FTP-Proxyserver eingerichtet werden.
- Fiery Warteschlange „Halten" – Die Scandatei wird an die Warteschlange „Halten" gesendet (siehe Abschnitt 6.2.1) und ab diesem Zeitpunkt nicht mehr als Scanauftrag behandelt.
- Internetfax – Der Scan wird als Anhang einer E-Mail-Nachricht an den Mailserver gesendet und von dort an die gewünschte Internetfax-Adresse geleitet.
- Mailbox – Der Scan wird in einer Mailbox auf dem Fiery Server gespeichert. Der Anwender muss die Zugangsnummer zu dieser Mailbox eingeben, um auf den gespeicherten Scanauftrag zugreifen zu können. Bei einigen Versionen erfordert der Fiery Server zusätzlich die Eingabe eines Kennworts. Der Scanauftrag kann über seine URL abgerufen werden.

7 Schlussbemerkung

Mit den Standardfunktionen und -optionen des Fiery Servers als solider Basis lässt sich für jede Umgebung eine umfassende und skalierbare Lösung realisieren, die den jeweiligen Sicherheitsanforderungen gerecht wird. EFI setzt alles daran, dass in Kundenumgebungen geschäftsrelevante und betriebliche Abläufe mit maximaler Effizienz erfolgen und der Fiery Server effektiv gegen Schwachstellen abgesichert ist, die für böswillige oder unbefugte Zwecke missbraucht werden könnten. EFI entwickelt daher kontinuierlich neue Technologien, mit denen sich der Rundumschutz und die Sicherheit des Fiery Servers weiter verbessern lassen.

TL035.07.18_DE