

## Umfassender Schutz für digitale Dokumente und Geräte

Angesichts der explosionsartigen Zunahme von Viren und Sicherheitsverstößen ist der Schutz von Unternehmensdaten von entscheidender Bedeutung. Fiery® Security stellt Administratoren eine umfassende Werkzeugpalette für die Dokumenten- und Gerätesicherheit bereit. Diese Tools bieten die umfassendsten Sicherheitsmaßnahmen in der Druckindustrie.

### Bessere Kontrollfunktionen für Administratoren

Die Funktionen von Fiery Security ermöglichen Systemadministratoren mehr Kontrolle über den persönlichen und elektronischen Zugriff auf Fiery Funktionen. Durch die **3-stufige Zugriffskontrolle** können Administratoren verschiedene Benutzerebenen definieren – jede mit anderen Zugriffsrechten.

Mit der **IP-Filterung** können Administratoren den Fiery-Zugriff im Netzwerk beschränken. Dabei werden autorisierte Verbindungen auf bestimmte IP-Adressen bzw. einen IP-Adressbereich beschränkt.

Die Funktion **Druckgruppen (Group Printing)** beschränkt die Möglichkeit des Druckens auf eine bestimmte Benutzergruppe, indem ein gültiges Gruppenkennwort eingegeben werden muss.

Mit der Funktion zum **Drucken per E-Mail (Email Printing)** steuern Administratoren, welche Anwender Aufträge per E-Mail an den Fiery senden können. Darüber hinaus können Administratoren autorisierte E-Mail-Adresslisten auf dem Fiery speichern.

Die **Port-Blockierung** ermöglicht es Administratoren, eine beliebige Anzahl von Ports und die damit verbundenen Fiery Funktionen in Echtzeit zu deaktivieren.

Die **LDAP-Unterstützung** bietet zusätzliche Sicherheit, da sie es dem Fiery ermöglicht, auf E-Mail-Adressen zuzugreifen, E-Mail-Adressen zu authentifizieren und Anwenderkennwörter zu validieren.

### Einhaltung strenger Richtlinien zur Datensicherheit

Bei der Entwicklung von Fiery Security wurde auf die Einhaltung der strengsten MIS/IT-Regierungs- und Unternehmensrichtlinien zur Datensicherheit geachtet. Sie entspricht auf Industriestandards beruhenden Zertifizierungsrichtlinien wie dem IP Sec-, SSL v2/v3- und X509-Zertifikatmanagement. IP Security Protocol stellt Verschlüsselungs- und Authentifizierungsmechanismen bereit und bietet dadurch Sicherheit für IP-Protokolle.

Mit der Funktion für **sicheres Löschen<sup>1</sup>** werden elektronische Daten und versteckte Dateien auf der Festplatte des Fiery entfernt.

Dank der **Anwenderauthentifizierung** und dem **Deaktivieren von Netzwerkanschlüssen und -diensten** kann unerwünschten Anwendern der Zugriff auf das System verwehrt werden.

Für Fiery Systeme mit **erweiterter Controller-schnittstelle (FACI)** wird zudem der Einsatz von Antivirussoftware unterstützt.

Real-time Fiery Systemsoftware- und Microsoft XPe-Updates werden in Echtzeit direkt über EFI WebTools implementiert, um den höchsten Sicherheitsstand zu gewährleisten.

Dank der **Anwenderauthentifizierung** und dem **Deaktivieren von Netzwerkanschlüssen und -diensten** kann unerwünschten Anwendern der Zugriff auf das System verwehrt werden.

Für Fiery Systeme mit **erweiterter Controller-schnittstelle (FACI)** wird zudem der Einsatz von Antivirussoftware unterstützt.

Fiery Systemsoftware- und Microsoft XPe-Updates werden in Echtzeit direkt über EFI WebTools implementiert, um zu gewährleisten, dass die Sicherheitsfunktionen stets auf dem neuesten Stand sind.

### Gewährleistet Datenvertraulichkeit

Die Fiery Datensicherheit gewährleistet mithilfe der folgenden Optionen und Funktionen die Vertraulichkeit von digitalen und gedruckten Dokumenten:

Die Funktion für **sicheres Drucken** setzt voraus, dass Anwender auftragspezifische Kennwörter eingeben, um zu verhindern, dass nicht autorisierte Anwender vertrauliche oder private Dokumente drucken.

**Herausnehmbare Festplatten** bieten Administratoren mit externen Fiery Servern auf Wunsch maximale Festplattensicherheit, da archivierte Dateien entnommen und an einem sicheren Ort aufbewahrt werden können.

Durch die **Verschlüsselung** von Daten wird sichergestellt, dass alle Kennwörter und zugehörigen Konfigurationsinformationen auf dem Fiery sicher sind. Die Verschlüsselungstechnologie beruht auf der gemeinhin akzeptierten TwoFish-Verschlüsselungsmethode.

### Kontrolle über die Anwender im System

Durch die **Fakturierung per Fiery Auftragsprotokoll** können Administratoren nachvollziehen, wer das System verwendet. Diese Funktion erfasst unveränderliche Anwenderdaten und erlaubt es nur dem Administrator, einzelne Aufträge oder das gesamte Auftragsprotokoll vom System zu löschen.

### Bietet Schutz auf dem neuesten Stand

Durch die Benachrichtigung in Echtzeit und den Download von Fiery System-Software, darunter Fiery Dienstprogramme und wichtige Microsoft-Updates, wird sichergestellt, dass die Software stets auf dem neuesten Stand ist, ohne dass Sie sich an den technischen Support wenden oder CDs bzw. DVDs einlesen müssen.

<sup>1</sup>Dies ist eine optionale Funktion für integrierte Fiery Server und eine Standardfunktion für externe Fiery Server.



# Fiery Security

## SERVER & CONTROLLER SOLUTIONS



Das Portfolio der integrierten Lösungen von EFI erhöht Ihre Produktivität und verbessert Ihr Geschäftsergebnis. Weitere Informationen sind unter [www.efi.com](http://www.efi.com) erhältlich.

### Funktionen von Fiery Security

#### Auftragsverwaltung/-übergabe:

**3-stufige Zugriffskontrolle**—Definiert Anwendertypen mit verschiedenen Berechtigungen.

**Sicheres Auftragsprotokoll / Secure Job Log**—Setzt voraus, dass Anwender bei Auswahl der zu druckenden Seiten/des Auftragsprotokolls das Administratorkennwort eingeben.

**Dokumentenfluss**—Wird verwendet, wenn Aufträge über eine der folgenden Warteschlangen an den Fiery übergeben werden:

- Warteschlange „Halten“
- Warteschlange „Drucken“
- Warteschlange „Direktdruck“

**Drucken per E-Mail**—Empfängt und druckt per E-Mail gesendete Aufträge.

- E-Mails werden anhand einer autorisierten E-Mail-Adressliste validiert.
- Nicht autorisierte E-Mails von nicht autorisierten Adressen werden gelöscht.

**Sicheres Drucken**—Setzt voraus, dass Anwender ein auftragsspezifisches Kennwort am Fiery eingeben, bevor der Auftrag gedruckt wird.

**Anwenderauthentifizierung**—Ermöglicht Administratoren das Definieren von autorisierten Anwendern für bestimmte Funktionen/Aufgaben auf dem Fiery.

**Herausnehmbare Festplatte<sup>2</sup>**—Ermöglicht das Aufbewahren der Festplatte an einem sicheren Ort.

**Sichern und Wiederherstellen**—Ermöglicht das Sichern und Wiederherstellen von kundenspezifischen Einstellungen auf demselben Fiery.

#### Scannen:

**Kennwortgeschützte Mailboxen**—Verhindert unberechtigte Zugriffe durch zusätzlichen Kennwortschutz.

#### Daten löschen:

**Aufträge löschen**—Löscht Aufträge vom Fiery automatisch oder mithilfe der Fiery Tools.

**Sicheres Löschen<sup>3</sup>**—Entfernt die Auftragsdatei von der Fiery Festplatte durch mehrfaches Überschreiben.

#### Netzwerkzugriff:

**LDAP-Authentifizierung**—Lightweight Directory Access Protocol (LDAP) v3, Kommunikation mit firmeninternen Servern auf Basis von RFC2251.

- Der Fiery greift auf E-Mail-Adressen und Anwendernamen zu
- Der Fiery unterstützt nachfolgende Authentifizierungsmethoden unter Verwendung von LDAP auf Exchange-, Novell- und Domino-Systemen:
  - Anonymous
  - SIMPLE
  - GSSAPI
  - Nicht für Domino oder Novell verfügbar

**Port-Blockierung**—Kann IP-Ports am Fiery deaktivieren.

**IP-Filterung**—Lässt Verbindungen von einer bestimmten IP-Adresse oder einem bestimmten IP-Adressenbereich mit dem Fiery zu oder lehnt diese ab.

**SNMP v3**—Bietet Fiery Administratoren die Wahl zwischen drei Sicherheitsstufen.

**SNTP**—Ermöglicht dem Fiery das Abfragen der exakten Standardzeit.

**IP Sec-Unterstützung**—Bietet IP-Protokollsicherheit durch Verschlüsselung und Authentifizierung.

**SSL/TLS-Unterstützung**—SSL ist ein Protokoll zur Übertragung privater Dokumente über das Internet. TLS ist ein Protokoll, das die Datensicherheit zwischen miteinander kommunizierenden Anwendungen und deren Anwendern im Internet sicherstellt.

**Zertifikatmanagement**—Ein Verfahren, mit dem sich Netzwerk-Clients in Netzwerkaktivitäten authentifizieren, bei denen Identitätsüberprüfungen durchgeführt werden.

**Verschlüsselung sensibler Informationen**—Stellt sicher, dass alle Kennwörter und zugehörigen Konfigurationsinformationen sicher sind.

**MAC-Filterung**—Lässt Verbindungsanfragen zu Fiery über Ethernet basierend auf der MAC-Adresse (Media Access Control) des Verbindungsabsenders zu bzw. lehnt sie ab.

**802.1x-Authentifizierung**—Ermöglicht Fiery den autorisierten Zugriff auf das LAN basierend auf der Zugriffssteuerung für den Port 802.1x.

<sup>2</sup> Optionale Funktion für externe Fiery Server

<sup>3</sup> Standardfunktion für externe Fiery Server und optionale Funktion für integrierte Fiery Server

ColorWise, Command WorkStation, DocBuilder Pro, DocStream, EDOX, EFI, Fiery, das Fiery Logo, Fiery Driven, das Fiery Driven Logo, OneFlow, PrinterSite, PrintFlow, PrintMe, PrintSmith, PrintSmith Site, Prograph, Proteus, RIP-While-Print und VUTEK sind eingetragene Marken der Electronics for Imaging, Inc., die in den USA und/oder einigen anderen Ländern patentrechtlich geschützt sind. Bestcolor ist eine eingetragene Marke der Electronics For Imaging GmbH, die in den USA durch Copyright urheberrechtlich geschützt ist. ADS, AutoCal, Auto-Count, Balance, BioVu, Build, ColorCal, Digital StoreFront, Estimate, Fiery Link, Fiery Prints, Fiery Spark, FreeForm, Hagen, Intelligent Device Management, Jetrion das Jetrion logo, Logic, MicroPress, Printcafe, PSI, PSI Flexo, RIPChips, Scan, SendMe, Splash, Spot-On, VisualCal, WebTools, das EFI Logo, das Fiery Prints Logo und Essential to Print sind Marken der Electronics for Imaging, Inc. Best, das Best Logo, Colorproof, PhotoXposure, Remoteproof und Screenproof sind Marken der Electronics For Imaging GmbH. Alle anderen Bezeichnungen und Produktnamen können Marken oder eingetragene Marken der jeweiligen Rechtsinhaber sein und werden hiermit anerkannt. © 2007 Electronics for Imaging