Fiery FS800 Pro/FS800 DFEs

Security White Paper

45271122

2026 年 8 月 6 日

目录

简介

本文档概述了 Fiery 数字前端 (DFEs) 中的安全功能。它为 IT 管理员和安全专业人员提供了评估 Fiery 数字前端如何保护打印环境安全所需的见解。该文档介绍了 Fiery 数字前端中用于保护数据、增强网络安全和维护系统完整性的原则和机制。

安全原则

Fiery 数字前端经过精心设计，遵循行业最佳实践，确保符合数据保护法规和企业安全要求。支持此设计的基本原则如下：

- 数据保护：对静态数据和传输中的数据进行加密
- 网络安全：受控访问、安全通信协议和身份验证机制
- 系统完整性：固件验证、安全启动和安全更新

随着威胁的不断发展，我们与全球合作伙伴和供应商合作，为客户提供连续的支持。为确保全面的系统安全，我们建议最终用户将 Fiery 安全功能与他们自己的组织安全策略集成，并遵守行业最佳做法，包括实施安全密码和强大的物理安全措施。

身份验证和访问控制

Fiery 数字前端支持多种身份验证方法，包括：

- LDAP/Active Directory 集成
- 使用单点登录 (SSO) 实现多因素身份验证 (MFA)

用户身份验证

身份验证功能让 Fiery DFE 能够执行以下操作：

- 验证用户
- 基于角色的访问控制 (RBAC)

Fiery DFE 支持三种用户身份验证方法：

- Fiery DFE 中定义的用户本地身份验证
- 通过使用 LDAP（例如 Microsoft Active Directory）的外部网络身份验证服务器的单因素身份验证 (SFA)
- 使用单点登录 (SSO) 的多因素身份验证 (MFA)

无论使用什么方法，管理员账户始终需要进行身份验证。这是无法禁用的。

群组权限

Fiery DFE 根据用户的群组成员身份授权用户操作。每个群组与一组特定的权限相关联，例如彩色打印或黑白打印。群组成员的操作仅限于这些权限。除管理员和操作员账户之外，Fiery 管理员拥有修改任何 Fiery 群组的权限。

在这种用户身份验证方法中，可以为群组选择的多种权限如下所述：

- 黑白打印：让群组成员能够执行黑白打印作业。如果作业为彩色作业，则会以黑白方式打印。
- 彩色和黑白打印：让群组成员能够完全访问 Fiery DFE 的彩色打印和黑白打印功能来打印作业。如果没有此权限或仅拥有黑白打印权限，用户仍然可以提交打印作业，但打印会失败。
- Fiery 邮箱：允许群组成员拥有独立邮箱。Fiery DFE 将基于具有邮箱权限的用户名创建邮箱。此邮箱的访问权限仅限于有邮箱用户名和密码的用户。
- 校准：此权限允许群组成员执行颜色校准。
- 创建服务器预设：允许群组成员创建服务器预设。群组成员可以访问这些服务器预设。
- 管理工作流程：此权限允许群组成员创建、发布或编辑虚拟打印机。
- 编辑作业（仅限 Fiery XB 数字前端）：此权限允许群组成员编辑队列中的作业。

拥有提升权限的管理员可以自定义这些功能以限制未经授权的访问并强制执行组织安全协议。

本地用户

Fiery DFE 软件与不同的独特用户类型进行交互，这些用户类型不同于 Windows 用户或角色。Fiery 管理员应在初始安装后立即修改所有默认密码。必须严格执行对 Fiery DFE 的密码访问。

- 使用**配置** > **安全性**时，“管理员”和“操作员”的最大密码长度为 64 个字符。
- 使用**配置** > **用户账户**时，本地用户账户的最大密码长度为 64 个字符。
- 可以在**配置** > **用户账户**中更改管理员和操作员密码。

本地 Fiery 用户账户和访问权限

- 管理员：完全控制 Fiery DFE 功能，可以修改除管理员和操作员账户之外的 Fiery 群组权限。
- 操作员：拥有与管理员相同的权限，但无权访问数字前端设置和删除作业日志。
- 打印机操作员（仅限 Fiery XB 数字前端）：拥有管理员添加的特定权限，管理打印机上的作业。
- Fiery DFE 管理员（仅限 Windows 服务器）：用于安装受信任证书的隐藏管理员账户，无法登录到 Fiery DFE，显示在网络扫描工具上，并且可以将其删除。
- Fiery_SMB_User：默认 Windows 打印 (SMB) 账户，可通过网上邻居查看 Fiery DFE 打印队列。
- 访客（默认，无密码）：与操作员拥有相同的权限，但无法访问作业日志、进行编辑、更改状态或预览作业。

LDAP 身份验证

Fiery DFE 使用 LDAP 版本 3（符合 RFC 2251）与企业服务器通信。通过 LDAPv3，它可以检索用于扫描功能的用户电子邮件地址，以及用于身份验证的用户和群组信息。与 Active Directory 服务器的 LDAP 连接专门支持此功能。

Fiery DFE 支持以下使用 LDAP 的身份验证方法：

- 自动
- 简单
- GSSAPI

下表描述了不同的 LDAP 身份验证方法：

身份验证方法	描述	Active Directory 服务器
自动	此选项根据 LDAP 服务器支持的身份验证方法选择 GSSAPI 或 SIMPLE。	支持
简单	密码为必填字段。如果选择了 LDAP over TLS，将使用 TLS 加密密码。	支持
GSSAPI	此方法使用 Kerberos 票证而不是密码，从而消除了对 TLS 的需求。	支持

单点登录 (SSO)

Fiery FS800 Pro 数字前端支持 OpenID Connect 协议，使用 Microsoft Entra ID（以前称为 Azure AD）进行基于云的单点登录 (SSO) 用户身份验证。用户可以使用现有的 Entra ID 凭据登录 Fiery DFE。

此身份验证方法支持多因素身份验证 (MFA)。

这种身份管理方法可确保 Fiery DFEs 永不将用户密码存储在本地，从而显著增强了安全性。

数据安全措施

为保护敏感信息，Fiery 数字前端实施了以下措施：

加密存储：保护打印作业和配置数据

关键客户数据进行加密可确保密码和相关配置信息在 Fiery DFE 上的安全存储。这些关键信息使用 AES-256 和 SHA-2 等加密算法进行加密或散列处理，这些算法符合最新的安全标准。

即使从 Fiery DFE 移除磁盘，存储在磁盘上的客户数据仍然无法访问。可在基于 Windows 的 Fiery DFEs 启用或禁用用户数据加密。对于基于 Linux 的 Fiery DFEs ，加密功能始终处于启用状态。

如果忘记了用于数据恢复的密码，FIERY 将无法对其进行重置；因此，需要重新安装完整的软件。

基于 Windows 的 Fiery DFEs 还提供加密包含作系统的启动驱动器的选项。这种加密有助于防止对 Fiery DFE 的脱机攻击，并确保启动驱动器不能在其他设备上使用。

安全擦除：确保数据在删除后不可恢复

基于 Windows 的 FS800 Pro 数字前端支持 NIST 800-88 数据清理标准。Fiery 管理员可将此选项配置为 1 次成像或 3 次成像覆盖方法。

注释：基于 Linux 的 Fiery 和 XB 平台或 SSD 上存储的用户数据不支持安全消除功能。

工作流程	安全消除
存储在 Fiery DFE 硬盘驱动器上的作业；安全消除设置为**打开**	是
存储在 Fiery DFE 硬盘驱动器上的作业；安全消除设置为**关闭**	否
在安全消除设置为**打开**后 Fiery DFE 已接收并删除的作业	是
在安全消除设置为**打开**前 Fiery DFE 已接收并删除的作业	否
发送至另一个 Fiery DFE（负载平衡）的作业副本	否
已存档至可移动媒介的作业	否
已存档到网络驱动器的作业	否
客户端设备上的作业	否
清空服务器执行	是
合并或复制到其他作业的页面（例如 Fiery Impose 作业或组合 PDF）	否

工作流程	安全消除
从 SMB 连接接收并保存到 Fiery DFE 硬盘驱动器的作业	否
磁盘交换或磁盘缓存操作期间写入 Fiery DFE 硬盘驱动器的作业部分	否
作业日志条目	否
清空服务器执行后的作业日志条目	是
Fiery DFE 在作业删除完成之前断电	否
删除作业之前对 Fiery DFE 硬盘驱动器进行碎片整理	否

网络安全性

Fiery DFEs 采用以下安全机制来保护网络通信：

- 防火墙配置，包括 IP 过滤与端口管理
- 传输层安全性 (TLS) 协议，用于加密通信（例如 HTTPS、LDAPS）
- IPSec，用于加密主机间安全通信
- SNMP v3，用于安全网络监控和管理

支持的网络协议

FS800/FS800 Pro 支持广泛的行业标准网络协议，确保在各种环境中实现兼容性、安全性和高效通信。这些功能包括：

- **核心协议：**TCP/IP、IPv4、IPv6
- **Web 协议：**HTTP/1.1、HTTPS (TLS 1.2/1.3)
- **文件和打印服务：**FTP、LPR、IPP 2.0、SMB v2、SMB v3、端口 9100
- **管理和监控：**SNMP v1、v2c 和 v3
- **远程访问：**RDP（仅限基于 Windows 的数字前端）
- **安全与身份验证：**IPSec (IKEv2)、LDAP v3、IEEE 802.1X
- **网络服务：**DHCP、DNS
- **发现协议：**WSD、Bonjour、SLP

网络端口

默认情况下，所有未使用的 TCP/IP 端口都将被禁用。Fiery 管理员可以启用或禁用网络端口。禁用端口可阻止通过该端口的外部连接。

入站端口

Fiery DFEs 监督和监控传入的网络连接，仅允许已获授权的流量访问数字前端，并保护其免受未经授权的访问或攻击。

TCP	UDP	端口名称	相关服务
20-21		FTP	FTP
80		HTTP	WebTools，IPP

TCP	UDP	端口名称	相关服务
135		MS RPC	Microsoft® RPC 服务。49152-65535 范围内的一个额外端口将打开，提供 SMB 相关的指向和打印服务。
137-139		NETBIOS	Windows 打印。默认情况下，这些端口处于关闭状态，因为 NetBIOS 不安全。
	161、162	SNMP	基于 SNMP 的工具
	427	SLP	服务定位协议。默认情况下，此端口被封锁，因为 SLP 不安全。
443		HTTPS	WebTools、IPPS
445		SMB/IP	基于 TCP/IP 的 SMB
	500	ISAKMP	IPSec
515		LPD	LPR 打印
631		IPP	IPP
3389		RDP	远程桌面（仅限基于 Windows 的 Fiery DFEs）
3702	3702	WS 发现	装置网络服务 (WSD)。通过 WSD 启用发现并打印到 Fiery DFE。
	4500	IPSec NAT 穿透	IPSec
	5353	多播 DNS (mDNS)	Bonjour
6310		DMP	直接移动打印
8010		FIERY 端口	JDF
8021-8022		FIERY 端口	Fiery Harmony、Fiery HotFolders 和 Fiery Command WorkStation
8090		FIERY 端口	OFA
9100-9103		打印端口	端口 9100
	9906	FIERY 端口	Harmony discovery
21030		FIERY 端口	Fiery Image Viewer

注释：IPSec 端口（500 和 4500）只能针对 FS800（基于 Linux 的 Fiery DFEs）进行配置 。

除 Fiery 合作伙伴指定的端口之外，其他 TCP 端口已禁用。无法远程访问与所禁用端口相关的任何服务。Fiery 管理员还可以启用或禁用 Fiery DFE 提供的各种相关服务。

出站端口

Fiery DFEs 管理和限制出站网络流量，确保只有已获授权的通信才能离开设备，从而减少遭受外部威胁的风险。

出站端口	用途	默认/开启配置
53	DNS	默认值
67	DHCP	默认值
80, 443	Fiery 系统更新、Windows 更新、JDF、PrintMe 和其他云通信	默认值
161、162	SNMP	在双 IP 配置中
21	扫描到 FTP	开启配置
123	NTP	开启配置
389/636	LDAP 服务	开启配置
445	扫描至 SMB/JobLog 到 SMB/JDF 通用全局路径	开启配置
500/4500	IPSEC	开启配置
8080/8443	HTTP/HTTPS/FTP 代理端口	开启配置

与云端服务的通信

此列表列举了需要与外部基于云的服务进行通信的 Fiery 服务和应用程序；例如，下载 Fiery 安全更新或许可证激活。本文档对于已禁用所有外部通信并试图在其公司防火墙内进行例外处理的客户特别有用。

Fiery 服务/应用程序	完全限定域名/URL	端口	服务器位置	使用信息
系统更新	https://liveupdate.fiery.com/des/hypatia.asmx	443	Fiery	下载 Fiery 安全更新
OFA	https://flexlicensing.fiery.com	443	Fiery	许可证激活
IQ	https://iq.fiery.com/iq	443	AWS	Fiery IQ 云
LINQ	https://ews.fiery.com	443	Azure	分析

Fiery 服务/应用程序	完全限定域名/URL	端口	服务器位置	使用信息
通用打印	多个域： • portal.azure.com • print.print.microsoft.com • notification.print.microsoft.com • discovery.print.microsoft.com • graph.print.microsoft.com	80/443	Azure	IPP 代理和通用打印服务
SSO	login.microsoft.com	80/443	Microsoft	单点登录
Windows Server Update Services (WSUS)	多个域： • http://windowsupdate.microsoft.com • http://.windowsupdate.microsoft.com • https://.windowsupdate.microsoft.com • http://.update.microsoft.com • https://.update.microsoft.com • http://.windowsupdate.com • http://download.windowsupdate.com • https://download.microsoft.com • http://.download.windowsupdate.com • http://wustat.windows.com • http://ntservicepack.microsoft.com • http://go.microsoft.com • http://dl.delivery.mp.microsoft.com • https://dl.delivery.mp.microsoft.com • http://.delivery.mp.microsoft.com • https://.delivery.mp.microsoft.co	80/443	Microsoft	Windows 更新
Command WorkStation	多个域： • https://help.fiery.com • https://learning.fiery.com • https://communities.fiery.com/s/ • https://liveupdate.fiery.com • https://iq.fiery.com	443	Fiery	Fiery 支持、Fiery 更新、Fiery Cloud

IP 过滤

IP 过滤让管理员能够根据预定义的 IP 地址控制对 Fiery DFE 的连接请求。通过定义默认策略，管理员可以指定是允许还是拒绝传入数据包。此外，他们可以为最多 16 个 IP 地址或范围创建过滤器，从而相应地允许或拒绝连接请求。

每个 IP 过滤器设定均指定 IP 地址或 IP 地址范围及相应的操作。当操作为拒绝时，源地址属于指定地址的数据包将被丢弃。相反，当操作为接受时，则允许数据包。

网络验证

SNMP v3

Fiery DFE 支持最新的 SNMPv3 标准，便于加密通信数据包以保证机密性、消息完整性和身份验证。

Fiery 管理员可以从三个 SNMP 安全级别中进行选择：最低、中等和最高。在这些级别上，使用 SHA-1 或 SHA-256 等算法对密码进行哈希处理，并对整个 SNMP 消息进行加密。此外，本地管理员可以配置 SNMP 读取和写入社区名称以及其他安全设置。

IEEE 802.1x

802.1X 是一个针对基于端口的网络访问控制的 IEEE 标准，可确保设备在访问本地网络及其资源之前进行身份验证。在 Fiery DFEs 上，可以将 802.1X 配置为使用 EAP-MD5 质询或 PEAP-MSCHAPv2 作为基于凭证的身份验证方法，或者使用 EAP-TLS 作为基于证书的身份验证方法。Fiery DFEs 仅支持用户证书（而不是设备证书）进行 EAP-TLS 身份验证。提供 EAP-MD5 质询是出于兼容性考量，其安全性低于 PEAP-MSCHAPv2 和 EAP-TLS 方法。

Fiery DFE 在启动时以及每次重新建立网络连接时，都会执行 802.1X 身份验证。

网络加密

Internet 协议安全性 (IPsec)

IPsec 通过在网络层对每个数据包进行加密和授权来增强基于 IP 的通信的安全性，从而保护跨所有使用 IP 的应用程序传输的数据。Fiery DFE 采用预共享密钥身份验证通过 IPsec 与其他系统建立安全连接。一旦在客户端计算机与 Fiery DFE 之间建立了 IPsec 通信，所有通信（包括打印作业）都将通过网络安全传输。

有一些协议，例如 LPR、端口 9100、FTP、WSD 和 Harmony（Fiery 的专有协议）用于打印作业提交、作业状态更新和管理命令。这些协议不通过安全通道传输，因此，那些需要此类功能提供保密性和完整性保护的组织，应在客户端计算机与 Fiery DFE 之间部署 IPsec。

HTTPS

Fiery DFEs 使用基于 TLS 的 HTTPS 来保护客户端与服务器组件之间的 Web 和 API 通信。Fiery DFEs 支持 TLS 1.3 和 TLS 1.2，提供强大的加密保护和现代安全功能。连接到 WebTools 和 Fiery API 时必须使用

HTTPS，以确保通过这些接口传输的管理和操作流量在传输过程中得到加密，并防止流量被拦截或篡改。客户端与服务器之间的通信并非全部通过加密的 HTTPS 协议进行。

证书管理

Fiery DFEs 提供一个接口，用于管理 TLS 通信期间使用的各种证书。Fiery DFEs 支持 PEM 格式的 X.509 证书，采用 Base64 编码，使用长度为 4096、3072 或 2048 位的 RSA 密钥。

证书管理允许 Fiery 管理员执行以下操作：

- 生成自签名数字证书。
- 为 Fiery DFE 添加证书及其关联的私钥。
- 从受信任的证书颁发机构添加、浏览、查看和移除证书。

自签名数字证书提供加密，但不提供自动信任验证。对于安全部署，我们建议使用受信任的证书颁发机构 (CA) 颁发的证书，确保执行适当的身份核验流程。

由受信任的 CA 签署证书后，即可在 WebTools 的 Configure 部分将其上传到 Fiery DFE。

服务器消息块 (SMB)

SMBv1 是文件和打印机共享的传统协议，由于存在已知的安全漏洞，已在 Fiery DFEs 上已禁用该协议。Fiery DFEs 反而支持 SMBv2 和 SMBv3。强制执行 SMB 签名，确保所有数据包都经过数字签名，以防范中间人攻击。如果启用 SMB 身份验证，用户必须提供有效的用户名和密码才能访问共享文件夹和内容。在 Fiery Configure 中设置密码，也可以限制访客账户通过 SMB 进行打印或文件共享。

硬件安全

Fiery DFEs 在设计时充分考虑了企业级硬件安全性。保护敏感信息不仅限于软件控制；硬件组件在维护系统完整性和数据机密性方面发挥着关键作用。关键硬件元素及其安全措施概述如下。

易失性存储器 (RAM)

Fiery DFEs 利用易失性存储器 (RAM) 在活动操作期间临时存储数据。为降低数据泄露风险，请执行以下操作：

- RAM 中的敏感信息会在使用后或系统关闭后立即清除。
- 应用内存清理技术来防止残留数据持久存在。
- 对 RAM 的访问通过处理器和操作系统强制的权限分离受到限制。

非易失性内存和数据存储

非易失性内存，包括硬盘驱动器、固态驱动器 （SSD） 和其他持久性存储，即使在系统关闭时也能保留数据。安全措施包括：

- 用户数据加密 （UDE） 用于保护存储的数据。
- 安全删除方法，用于在删除文件时使敏感信息无法恢复。

闪存

闪存用于存储固件、配置文件和系统设定。要维护其安全性，请执行以下操作：

- 固件经过数字签名以防止篡改。
- 固件更新在安装前通过加密校验和进行验证。
- 写保护机制可防止在运行时进行未经授权的修改。

CMOS 与 NVRAM

硬件配置和启动设定等关键系统参数存储在 CMOS 与非易失性 RAM (NVRAM) 中。要保护此数据，请执行以下操作：

- 访问仅限于授权的管理进程。
- 安全启动有助于确保仅加载受信任的固件和启动组件。
- 通过完整性控制措施，保护关键 NVRAM 变量免受已损坏和未经授权的修改。

存储驱动器

Fiery DFEs 使用存储驱动器来存放主机操作系统、系统文件、作业假脱机处理、日志和临时文件。

提供以下安全功能来保护客户数据：

- 驱动器级加密。
- 访问控制列表 (ACL)，限制未经授权的读取/写入操作。
- 磁盘驱动器安全套件（外部 Fiery DFEs 可选）支持用户在正常操作期间安全锁定驱动器。

物理端口

物理端口（如 USB、网络接口和服务连接器）是未经授权访问的潜在媒介。Fiery 硬件安全性通过以下方式解决此风险：

- 通过硬件和固件控制，禁用未使用的端口。
- 通过管理控制和系统配置，限制外部设备访问。
- 记录涉及重要物理接口的安全相关事件。

通过将这些硬件安全措施与软件和网络保护集成，Fiery DFEs 可提供全面的纵深防御策略，确保打印环境中敏感数据的机密性、完整性和可用性。

系统完整性和安全更新

维护系统完整性是确保安全的关键。Fiery DFEs 提供以下支持：

- 安全审核日志
- 安全启动：确保仅加载受信任的软件。
- 数字签名更新：防止篡改软件更新。
- 自动安全更新管理：简化应用安全更新的过程。

安全审计日志

具有提升权限的管理员可以访问和检查安全审计日志中记录的安全事件。该日志默认启用。

每个安全事件都分类为信息、警告或错误。管理员不会收到任何警告或通知；相反，它们将显示静态日志。

日志的格式与通常用于日志收集和分析的安全信息和事件管理 (SIEM) 工具兼容。所有捕获的事件数据均符合 NIST SP 800-53 中概述的标准。

Fiery 管理员无需 FIERY 干预即可访问安全审核日志。基于 Linux 的数字前端的日志以 Syslog 格式（RFC 5424 或 RFC 3164）提供。对于基于 Windows 的数字前端，日志以标准 Windows EVTX 格式保存，并且可从 Windows 事件日志管理器以及许多使用 Windows 事件日志 API 的可用商业解决方案中读取。基于 Linux 的 Fiery 数字前端提供将日志转发到 Syslog 等集中式收集系统的选项。

根据分配的本地存储容量保留安全日志，但不超过预定义的保留期限限制。在基于 Windows 的 Fiery DFEs 上，系统会根据需要删除最早的单个事件。在基于 Linux 的 Fiery DFEs 上，审计日志按文件大小进行轮换；轮换后的日志文件将保留到配置的轮换计数，之后系统会删除最早的轮换文件。

安全启动

安全启动通过仅允许加载受信任的、经过数字签名的组件，在启动期间保护操作系统。在受支持的基于 Windows 的 Fiery 数字前端上，这项功能可防止未经授权的或恶意代码在启动时执行，从而降低遭到入侵的风险。若要使安全启动功能生效，必须在 BIOS 设定中启用并激活这项功能。

数字签名更新

Fiery DFEs 使用数字签名更新来确保所有软件和固件安装的完整性和真实性。每次更新均由 Fiery 或其授权合作伙伴进行加密签名，使数字前端能够验证内容尚未被更改或篡改。此过程可防止引入恶意代码，并保证仅应用受信任的更新，从而维护系统安全性和可靠性。

自动化安全更新管理

及时更新软件对于发挥 Fiery DFEs 的最优性能至关重要。安装所有安全更新是确保 Fiery DFEs 在任何给定的打印环境中维持安全的关键。

如果在 Fiery DFE 上启用了此选项，**Fiery 系统更新**会下载并安装安全更新。此选项已默认启用，我们建议客户保留启用。

本文档中未详细介绍 Microsoft® Windows™ 操作系统安全漏洞，因为它们由 Microsoft 直接管理，并在发布时通过 **Windows 更新**分发给客户。

为了解决可能影响核心 Fiery 硬件组件（包括主板、处理器和固件）的安全问题和漏洞，FIERY 与制造商密切合作以获得必要的安全更新。这些安全更新随后会根据需要提供给客户。

注释：Fiery 软件更新采用安全哈希算法 (SHA-2) 进行数字签名，以防止未经授权的修改，包括插入恶意软件。

Fiery DFE 软件安全更新

及时更新软件对于 Fiery DFE 的最佳运行至关重要。通过应用最新的 Fiery DFE 软件安全更新，可确保系统完整性，缓解漏洞，并保持对行业安全标准的合规性。

Fiery DFE 安全团队通过由可信和可靠来源组成的全面网络，认真监控和跟踪安全漏洞，例如：

- 美国网络安全和基础设施安全局 (CISA) 警报和建议
- 美国国家标准与技术研究院 (NIST) 国家漏洞数据库
- 常见漏洞与披露 (CVE) 记录
- CERT 协调中心 (CERT/CC) 关于软件和硬件漏洞的报告和建议
- 地区政府和监管机构
- 软件和硬件供应商的安全公告

Fiery 根据通用漏洞评分系统 (CVSS) 确定的严重性（严重、高、中和低）对安全修复进行优先级排序。这些修复程序将在获得原始设备制造商 (OEM) 合作伙伴的相应批准后发布。获得批准后，Fiery 软件安全更新可供下载。所有 Fiery 软件更新采用安全哈希算法 (SHA-2) 进行数字签名，以防止未经授权的修改，包括插入恶意软件。

启用后，Fiery 系统更新会自动在 Fiery DFE 上下载并安装安全更新。此选项已默认启用，我们强烈建议客户保持其活动状态。

合规与最佳实践

强大的安全实施符合基本的行业标准和监管框架，包括：

- GDPR、欧盟数据法案
- FIPS 140-3
- NIST 800-88。介质清理指南（仅限 FS800 Pro）
- NIST 800-52。传输层安全性 (TLS) 实施的选择、配置和使用指南
- 美国国防部网络安全成熟度模型认证 (CMMC)。级别 2：受控非密信息 (CUI) 的广泛保护（仅限 FS800 Pro）
- NIST 800-193。平台固件韧性恢复指南（仅限 FS800 Pro）
- NIST 800-53。信息系统和组织的安全与隐私控制
- 通用操作系统的通用标准保护特性档（仅限 FS800 Pro）

若要加强安全态势，IT 管理员有责任实施以下措施：

- 定期应用安全更新
- 实施可靠的身份验证策略
- 进行定期安全审计
- 为打印环境实施网络分段

安全 Fiery DFE 配置指南

配置 Fiery DFE 时，Fiery 管理员可以遵循以下指南以加强安全性：

更改管理员密码

Fiery DFEs 出厂时带有管理员账户的默认密码。此密码授予本地以及从远程客户端对 Fiery DFE 的完全访问权限。此访问权限包括但不限于：

- 文件系统（仅限 Windows 上的 Fiery DFEs）
- 系统安全性设定
- 应用程序设定
- 注册表项

我们强烈建议您在安装后立即更改默认 Fiery 管理员密码，并根据您组织的安全策略定期更改。必须在 Fiery 平台内修改 Fiery 管理员密码。

安全高效的运营最佳实践

- 将 SNMP 限制为版本 3 以获得最大安全性。
- 禁用 WSD 进行作业提交以防止其在打印工作流程中使用。
- 除非明确要求，否则禁用 Windows 打印协议（LPR、端口 9100、IPP）。
- 启用 TCP/IP 端口过滤以阻止未使用的端口并降低风险。
- 如果不是 Windows 打印或文件共享需要，则关闭 Ports 137 – 139 和 445。
- 禁用端口 80 上的 HTTP 以防止不安全的通信。
- 启用安全打印，因此只有作业所有者才能发布打印作业。

高安全性环境

具有提升权限的管理员可以通过选择 **WebTools** > **配置** > **安全性**中提供的“高安全性”特性档来轻松配置高安全性设定。

结语

Fiery DFEs 虽然配备了强大的安全功能，但并非面向互联网。应将其部署在安全的网络环境中，并由网络管理员严格控制访问权限。Fiery DFEs 专为满足最新行业标准而构建，可提供企业级安全性，保护打印环境免受不断变化的网络威胁。管理员可以充分利用 Fiery 的安全功能，确保合规并保护敏感数据。

FS800、FS800 Pro 中的新功能

- 核心系统模块更新，以解决安全漏洞。
- 远程桌面连接到基于 Windows 11 的 Fiery DFEs 支持 TLS 1.3，从而增强加密并提高连接安全性。