Fiery FS700 Pro/FS700 servers

Security White Paper

45266131

2025 年 12 月 8 日

目录

简介

本文档概述了 Fiery 服务器中的安全功能。它旨在向 IT 管理员和安全专业人员介绍 Fiery 解决方案如何保护打印环境。该文档介绍了 Fiery 服务器中用于保护数据、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 servers 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。

验证和访问控制

Fiery 服务器支持多种验证方法，包括：

- 基于角色的访问控制 （RBAC）
- 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

验证功能使 Fiery 服务器能够执行以下功能：

- 验证用户
- 基于用户的权限授权操作

Fiery server 支持以下三种用户验证方法：

- Fiery 服务器中定义的用户本地验证
- 通过使用 LDAP 的外部网络验证服务器的单因素验证 (SFA)（例如 Microsoft Active Directory）
- 使用单一登录 (SSO) 的多因素验证 (MFA)

无论使用什么方法，管理员帐户始终都需要验证。这是无法禁用的。

群组权限

Fiery 服务器根据用户的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，例如彩色或灰度打印。群组成员的操作仅限于这些权限。除管理员和操作员帐户之外，Fiery 管理员拥有修改任何 Fiery 群组的权限。

在该用户认证方法中，可以为群组选择的多种权限如下：

- 灰度打印：允许群组成员将作业打印为灰度。如果用户没有此权限，Fiery 服务器将不会执行打印作业。如果作业为彩色作业，则将打印为灰度。
- 彩色和灰度打印：允许小组成员通过完全访问 Fiery 服务器的彩色和灰度打印功能来打印作业。没有此权限或灰度打印权限，打印作业将无法打印并且用户无法通过 FTP 提交作业（仅彩色设备）。
- Fiery 邮箱：允许群组成员拥有独立邮箱。Fiery Server 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 服务器）：此权限允许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 服务器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 服务器的密码访问。

- 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** > **用户帐户**时，本地用户帐户的最大密码长度为 64 个字符。
- 管理员和操作员密码可以在**配置** > **用户帐户**中更改。

本地 Fiery 用户帐户和访问权限

- 管理员：完全控制 Fiery 服务器功能，可以修改除管理员和操作员帐户之外的 Fiery 群组权限。
- 操作员：拥有与管理员相同的权限，但无权访问服务器设置和删除作业日志。
- 打印机操作员（仅限 Fiery XB 服务器）：使用管理员添加的特定权限管理打印机上的作业。
- Fiery 服务管理员（仅限 Windows 服务器）：用于安装受信任证书的隐藏管理员帐户，无法登录到 Fiery 服务器，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） 帐户，可通过网上邻居查看 Fiery 服务器打印队列。
- 访客（默认，无密码）：与操作员具有相同的权限，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 服务器使用 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 服务器支持以下使用 LDAP 的身份验证方法：

- 自动
- 简单
- GSSAPI

下表描述了不同的 LDAP 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

身份验证方法	描述	Active Directory 服务器
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

单一登录（SSO）

Fiery FS700 Pro 服务器支持 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 server。

此验证方法支持多因素验证（MFA）。

这种身份管理方法可确保 Fiery 服务器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 服务器实施了以下措施：

加密存储：保护打印作业和配置数据

关键客户数据的加密可确保密码和相关配置信息在 Fiery 服务器上的安全存储。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 服务器中移除磁盘，存储在磁盘上的客户数据仍然无法访问。可在基于 Windows 的 Fiery 服务器上启用或禁用用户数据加密。对于基于 Linux 的 Fiery 服务器，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 的服务器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 服务器的脱机攻击，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

对于基于 Linux 的 FS700 Fiery 服务器，删除作业时，每个作业源文件将使用基于 US DoD 5220.22-M 数据擦除方法的算法覆盖 3 次。

使用 E600 和 LX Pro 硬件平台的嵌入式 Fiery 服务器不支持此功能。这些平台将文档数据存储在固态驱动器（SSD） 上，该驱动器受 AES-256 加密保护。此加密始终处于启用状态，无法禁用。

基于 Windows 的 FS700 Pro 服务器支持 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：Fiery 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 server 硬盘驱动器上的作业；安全消除设置为**打开**	是
存储在 Fiery server 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 server 已接收并删除的作业	是
在安全消除设置为**打开**前 Fiery server 已接收并删除的作业	否
发送至另一个 Fiery server（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

工作流程	安全消除
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
从 SMB 连接接收并保存到 Fiery server 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 server 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 server 在作业删除完成之前断电	否
删除作业之前对 Fiery server 硬盘驱动器进行碎片整理	否

网络安全性

Fiery 服务器采用以下安全机制来保护网络通信：

- IP 过滤和端口管理
- 防火墙配置
- 支持 SNMP v3 的安全网络监控和管理工具

支持的网络协议

FS700/FS700 Pro 支持广泛的行业标准网络协议，以确保跨不同环境的兼容性、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
- **快速访问：** RDP（仅限基于 Windows 的服务器）
- **安全与认证：** 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 管理员可以启用和禁用网络端口。禁用端口可有效防止需要使用该特定端口的外部连接。

入站端口

Fiery 服务器监督和监控传入的网络连接，仅允许经授权的流量访问服务器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，此端口是 bloacked，因为 SLP 不安全。
443		HTTPS	WebTools、IPP/s
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 服务器）
3702	3702	WS 发现	装置网络服务 (WSD)。可通过 WSD 发现和打印到 Fiery 服务器。
	4500	IPSec NAT 穿透	IPSec
	5353	多播 DNS (mDNS)	Bonjour
6310		DMP 端口	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 FS700（基于 Linux 的 Fiery 服务器）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 服务器提供的各种相关服务。

出站端口

Fiery 服务器可管理和限制出站网络流量，以确保只有经过授权的通信才能离开设备，从而减少受到外部威胁的风险。

出站端口	用途	默认/开配置
53	DNS	默认值
67	DHCP	默认值
80, 443	Fiery 系统更新、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	关于配置
123	NTP	关于配置
389/636	LDAP 服务	关于配置
445	扫描至 SMB/JobLog 到 SMB/JDF 通用全局路径	关于配置
500/4500	IPSEC	关于配置
8080/8443	HTTP/HTTPS/FTP 代理端口	关于配置

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	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	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	单一登录
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.com	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	

IP 过滤

IP 过滤使管理员能够根据预定义的 IP 地址控制对 Fiery 服务器的连接请求。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 地址范围和相应的操作。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，当作为接受时，则允许数据包。

网络验证

SNMP v3

Fiery 服务器支持最新的 SNMPv3 标准，便于加密通信数据包以保证机密性、消息完整性和真实性。

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 服务器上，可以将 802.1X 配置为使用 EAP-MD5 Challenge 或 PEAP-MSCHAPv2 进行基于服务器的验证，或者使用 EAP-TLS 进行基于证书的验证以增强安全性。Fiery 服务器仅支持用户证书（而非设备证书）进行基于 EAP-TLS 证书的验证。

Fiery 服务器在启动期间或网络连接断开并重新连接时执行验证。

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 服务器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和 Fiery 服务器之间建立了 IPsec 通信，所有通信（包括打印作业）都将通过网络安全传输。

HTTPS

Fiery 服务器使用 TLS 上的 HTTPS 强制客户端和服务器组件之间进行安全通信。这可确保传输的所有数据（如打印作业、作业状态更新和管理命令）在传输过程中都经过加密，从而防止被拦截或篡改。Fiery 服务器支持 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 WebTools 和 Fiery API 时必须使用 HTTPS，以确保安全传输管理和作流量。

证书管理

Fiery Server 提供用于管理 TLS 通信期间使用的证书的接口。Fiery 服务器支持采用 Base64 编码的 PEM 格式的 X.509 证书，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 服务器添加证书及其关联的私钥。
- 从信赖的证书授权添加、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管理机构（CA） 颁发的证书，以确保正确的身份验证。

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 服务器。

服务器消息块 (SMB)

SMBv1 是文件和打印机共享的传统协议，由于已知的安全漏洞，已在 Fiery 服务器上禁用。Fiery 服务器支持 SMBv2 和 SMBv3。强制执行 SMB 签名，确保所有数据包都经过数字签名，以防止中间人攻击。启用 SMB 验证后，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通过 SMB 为客人帐户打印或文件共享。

硬件安全

Fiery 服务器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。

易失性内存（RAM）

Fiery 服务器利用易失性内存（RAM）在活动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 和 NVRAM

硬件配置和启动设定等关键系统参数存储在 CMOS 和非易失性 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。
- 安全启动机制可确保只有受信任的固件才能读取和写入这些区域。
- 关键 NVRAM 变量将进行备份和完整性检查，以防止损坏或恶意更改。

存储驱动器

Fiery 服务器使用存储驱动器存储作系统和系统文件。这些驱动器还用于作业假脱机处理、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） 以限制未经授权的读/写作。
- 磁盘驱动器安全套件（外部 Fiery 服务器可选），允许用户在正常作期间安全锁定服务器驱动器，从而增强系统安全性。

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：

- 在硬件或固件级别禁用未使用的端口。
- 连接外部设备需要管理授权。
- 监控和记录与关键物理接口的所有交互。

通过将这些硬件安全措施与软件和网络保护集成，Fiery 服务器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

维护系统完整性对于确保安全性至关重要。Fiery 服务器提供以下支持：

- 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 的服务器的日志以 Syslog 格式（RFC 5424 或 RFC 3164）提供。对于基于 Windows 的服务器，日志以标准 Windows EVTX 格式保存，可以从 Windows 事件日志管理器和许多使用 Windows 事件日志 API 的可用商业解决方案中读取。基于 Linux 的 Fiery 服务器提供将日志转发到 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。当日志大小超过预定义的存储限制 (400MB) 时，较早的事件将被自动删除。

安全启动

此功能通过仅允许加载经过数字签名和信任的组件来确保启动期间作系统文件的完整性。在 Fiery 服务器上，它可以阻止未经授权或恶意代码在启动期间运行，从而增强安全性并降低泄露风险。默认情况下，安全启动处于禁用状态。

数字签名的更新

Fiery 服务器使用数字签名的更新来确保所有软件和固件安装的完整性和真实性。每次更新都由 Fiery 或其授权合作伙伴进行加密签名，使服务器能够验证内容是否未被更改或篡改。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。

自动安全更新管理

及时更新软件对于发挥 Fiery 服务器的最优性能至关重要。安装所有安全更新对于 Fiery 服务器在任何给定的打印环境中保持安全非常重要。

如果在 Fiery 服务器上启用了此选项，**Fiery 系统更新**即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 软件更新用安全散列算法 (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 Server 软件安全更新

及时的软件更新对于 Fiery 服务器的最佳运行至关重要。通过应用最新的 Fiery 服务器软件安全更新，可以确保系统完整性，缓解漏洞，并保持对行业安全标准的合规性。

Fiery 服务器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。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 软件更新均使用安全哈希算法 (SHA-2) 进行数字签名，以防止未经授权的修改，包括恶意软件的插入。

启用后，Fiery System Update 会自动在 Fiery 服务器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。

合规性和最佳实践

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
- ISO/IEC 27001（仅限 FS700 Pro）
- FIPS 140-2
- NIST 800-88。媒体清理指南（仅限 FS700 Pro）
- NIST 800-52。传输层安全性 （TLS） 实施的选择、配置和使用指南
- NIST 800-171。保护非联邦系统和组织中的受控非机密信息（仅限 FS700 Pro）
- 美国国防部网络安全成熟度模型认证 （CMMC）。级别 2：对受控非机密信息 （CUI） 的广泛保护（仅限 FS700 Pro）
- NIST 800-193。平台固件复原指南（仅限 FS700 Pro）
- NIST 800-53。信息系统和组织的安全和隐私控制
- 通用操作系统的通用标准保护特性档（仅限 FS700 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 服务器配置指南

配置 Fiery 服务器时，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 服务器出厂时带有管理员帐户的默认密码。此密码授予本地和从远程客户端对 Fiery 服务器的完全访问权限。此访问包括但不限于：

- 文件系统（仅限 Windows 上的 Fiery 服务器）
- 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 服务器虽然配备了强大的安全功能，但并非面向互联网。应将它们部署在安全的网络环境中，并由网络管理员仔细控制访问权限。Fiery 服务器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，确保合规性并保护敏感数据。

FS700、FS700 Pro 的新功能

- 已更新核心系统模块以解决安全漏洞。
- 电子邮件功能已弃用，以防止电子邮件攻击并确保符合安全法规。
- 现在可以使用 TLS 1.3 加密与 Fiery 服务器的所有通信。当前，连接运行 Windows 10 的 Fiery 服务器的远程桌面支持 TLS 1.2。
- 添加了对以下 Fiery 应用程序和模块的 TLS 1.3 支持：
  - 许可服务器和客户端组件
  - IPP 代理：Microsoft 通用打印所必需的
  - 802.1x 网络认证协议
  - EFI LINQ：用于 Fiery 服务器崩溃报告
  - JDF
  - 系统更新
  - FCC – Fiery Cloud Connector
- Linux 服务器上使用的 IPsec 工具已替换为更新、更安全的工具。
- 添加了对 SNMPv3 通信的高级加密标准 （AES） 的支持，并使 AES 128 成为新的默认值：
  - AES 128（默认值）
  - AES 192（用户可以从“配置”中选择）
  - AES 256（用户可以从“配置”中选择）
  - 虽然 DES 不再是默认选项，但仍受支持。用户可以根据需要选择它。