Fiery FS500 Pro/FS500 servers

Fiery Security White Paper

45234239

2022 年 7 月 3 日

目录

文档概述

此文档提供有关如何在 Fiery FS500 Pro/FS500 servers 中实施安全技术和功能的详细信息 ，并且涵盖了硬件安全、网络安全、访问控制、操作系统和数据安全。文档的目的是帮助客户将 Fiery 平台安全技术与他们自己的策略相结合以满足其特定的安全要求。

术语约定

本文档使用以下术语来表示 Fiery FS500 Pro/FS500 servers、打印机和 Fiery 应用程序。

术语或规范	说明
Fiery server	Fiery FS500 Pro/FS500 servers
打印机	打印机、复印机、数字印刷机、印刷机或输出设备
Configure	Fiery Configure
Command WorkStation	Fiery Command WorkStation
WebTools	Fiery WebTools
QuickTouch	运行在 Fiery 服务器 LCD 面板上的 Fiery QuickTouch 软件

EFI 安全理念

EFI 深知安全是全球各组织和企业最关注的问题之一。我们的产品经常通过改进的安全功能得到加强，以保护您的公司资产。安全性是设计和制造 EFI Fiery servers 的核心组件，以在系统数据静止、传输以及处理期间对其进行保护。

随着威胁的不断发展，我们与全球 EFI 合作伙伴和供应商紧密合作，致力于持续为客户提供解决方案。为了实现整体系统安全，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和特定行业最佳做法（例如安全密码和强大的物理安全程序）相结合。

EFI 安全目标

在为 Fiery server 实施安全措施时，EFI 树立了以下目标：

- **数据安全**：在处理、传输（中转）或存储（静止）期间不得擅自泄露数据。
- **可用性**：达到预期的性能，不受未经授权的操作。
- **访问控制**：不拒绝向授权用户提供服务。
- **IT 友好型维护**：在安全更新可用时自动通知和下载。
- **法规遵从性**：支持行业法规和安全框架。

Fiery 软件安全更新

本节提供了 Fiery server 软件安全更新流程的一般概述。Microsoft® Windows™ 操作系统安全漏洞未被描述，因为这些是由 Microsoft 直接处理的，并在可用时作为 Windows 更新提供。对于可能影响核心 Fiery 硬件组件（如主板、处理器、BIOS 等）的安全问题或漏洞，EFI 与制造商密切协作以获取所需的安全更新。

- EFI 从网络安全和基础结构安全局（CISA）监控每周的美国证书网络安全公报。公报概述了美国国家标准和技术研究所（NIST）国家漏洞数据库（NVD）上周记录的新漏洞。漏洞基于常见的漏洞和暴露（CVE）命名标准，并根据通用漏洞评分系统（CVSS）确定的严重性（高、中、低）进行整理。
- EFI 尽早为每个 Fiery server 平台提供安全补丁。
- Fiery 软件安全更新将交付给特定的 EFI 伙伴批准。
- 在合作伙伴批准后，Fiery 软件安全更新可供下载。
- 如果在 Fiery server 上启用了选项，Fiery System 更新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。

及时更新软件对于发挥 Fiery servers 的最优性能至关重要。安装 Fiery 和 Windows 操作系统软件安全更新对于在任何给定的打印环境中保持 Fiery servers 安全非常重要。

注释：所有 Fiery 更新或补丁都用 SHA-2 进行了数字签名。

配置 Fiery server 安全功能

Configure 是用于在 Fiery servers 上配置安全功能的主工具。Fiery 管理员可以从 Command WorkStation 或 WebTools 访问 Configure。

注释：用户必须具有管理员权限才能访问 Configure。

有关配置 Fiery server 的详细信息，请参阅 安全 Fiery 服务器配置指南（第 27 页）。

硬件安全性

Fiery server 硬件上的安全性侧重于在断电和未授权访问存储设备的数据时防止数据丢失。

易失性内存

写入易失性 RAM 的数据仅在通电期间可用。关闭电源之后，所有数据都将被删除。

有关详细信息，请参阅表格的易失性内存部分（第 21 页）。

非易失性内存和数据存储

Fiery server 采用多种非易失性数据存储技术以在断电之后将数据保存在 Fiery server 上。这些数据包括系统编程信息和用户数据。

有关详细信息，请参阅表格的非易失性内存部分（第 21 页）。

闪存

闪存用于存储自诊断和引导程序 (BIOS) 以及某些系统配置数据。闪存在工厂编程并且只能通过安装 EFI 创建的特殊补丁程序来重新编程。如果这些数据损坏或被删除，Fiery server 将无法启动。

CMOS

电池供电的 CMOS 内存用于存储 Fiery server 的机器设定。此类信息并不被视为机密或私有信息。如果安装了 CMOS 内存，用户可以使用显示器、键盘和鼠标在基于 Windows 10 IoT Enterprise 2016 或 2019 的服务器上访问这些设定。

NVRAM

Fiery server 中有一些较小的 NVRAM 装置，其中包含操作固件。这些设备包含非特定客户操作信息。用户没有访问其中所包含数据的权限。

硬盘驱动器和固态驱动器

正常打印和扫描操作期间以及创建作业管理信息期间，图像数据写入硬盘驱动器和固态驱动器中的随机区域。

用户可以从 Command WorkStation 或任何其他队列操作（例如打印机 LCD 中的操作）手动删除队列中的图像数据和作业。还可以使用**清空服务器**命令自动删除图像数据和对象，或者当已打印作业数量超过允许的参数时，也会自动删除。禁用已打印的队列也将删除打印的作业。

EFI 提供了一项安全擦除功能，以避免出现未经授权访问图像数据的情况。Fiery 管理员启用安全擦除后，所选操作模式将在适当的时间执行，以安全擦除硬盘驱动器上已删除的数据。Fiery 安全擦除当前仅支持硬盘驱动器。对于固态硬盘（SSD），在处置驱动器之前请与制造商联系以获取磁盘清理选项。

注释：有关安全擦除的详细信息，请参阅 安全擦除（第 20 页） 。

物理端口

Fiery server 可通过下表中显示的外部端口连接：

Fiery 端口	功能	访问权限	访问控制
以太网 RJ-45 接口	以太网连接	网络连接	使用 Fiery IP 过滤功能控制访问
打印机界面连接器	打印和扫描	专门用于和打印机之间发送/接收数据	不适用
USB 端口	USB 设备连接 系统软件安装	即插即用接口，适合与可选的可移除介质设备配合使用。	可以关闭 USB 打印。可通过 Windows 组策略关闭对 USB 存储设备的访问。还可以从 Configure 禁用 USB 存储。
光纤连接器	10Gb 以太网连接	网络连接	不适用

本地接口

在有些 Fiery servers 上，用户可以通过 Fiery NX Station 监视器，触摸屏显示器上的 Fiery QuickTouch 软件，或连接到 Fiery server 的任意显示器访问 Fiery 功能。通过 Windows 管理员密码可控制具有 Fiery NX Station 的 Fiery server 的安全访问。触摸屏显示器提供的功能非常有限，不会出现任何安全风险。

可移动硬盘驱动器套件选项

有些 Fiery servers 支持使用可移动硬盘驱动器选项套件来提高安全性。用户可通过该套件将服务器驱动器锁定于系统中进行正常操作，并可在关闭 Fiery server 之后将驱动器移至安全位置。

对于独立 Windows 服务器

独立的基于 Windows 的 Fiery servers 支持可移动硬盘驱动器选项套件。该选项套件是否可用于特定 Fiery 产品，取决于 EFI 与其各 Fiery 合作伙伴签署的协议条款。

对于 Fiery XB 服务器

硬盘驱动器和固态硬盘可在 Fiery XB 服务器上移除。大多数硬盘驱动器和固态硬盘都在 RAID 配置中配对在一起。将驱动器恢复到原来的位置以防止数据丢失并进行新的系统软件安装很重要。

启用用于存储的 USB 端口

Fiery servers 上的 USB 端口允许鼠标、键盘或分光光度计连接，但在 Configure 中禁用**启用 USB 存储**选项时会阻止连接到 USB 存储设备。此选项默认启用。禁用时，该选项禁用需要 USB 大容量存储功能的 Fiery 功能，例如备份和还原。

网络安全性

Fiery server 包含多种网络安全功能，用于控制和管理对打印机的访问。只有授权用户和组才能访问 Fiery server 并打印到打印机。Fiery server 还可以配置为使用指定的 IP 地址以及禁用网络端口和协议来限制或控制外部通信。Fiery servers 应始终部署在受保护的网络环境中，并应由合格和授权的网络管理员正确配置和管理可访问性。

网络端口

默认情况下，所有未被特定 Fiery 服务使用的 TCP/IP 端口都将被禁用。Fiery 管理员可以有选择地启用和禁用网络端口。禁用网络端口会阻止使用特定端口的外部连接。如果启用特定端口，则允许外部连接使用该端口。

TCP	UDP	端口名称	相关服务
20-21		FTP	FTP
80		HTTP	WebTools，IPP
135		MS RPC	Microsoft® RPC 服务（仅限 Windows 10）。49152-65536 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
	161，162	SNMP	Fiery Central、一些传统的实用程序、其他基于 SNMP 的工具
	427	SLP	SLP
443		HTTPS	WebTools、IPP/s
445		SMB/IP	基于 TCP/IP 的 SMB
	500	ISAKMP	IPSec
515		LPD	LPR 打印，一些传统的实用程序（例如较早版本的 Command WorkStation）
631		IPP	IPP
3389		RDP	远程桌面（仅限 Windows Fiery 服务器）
3702	3702	WS 发现	WSD
	4500	IPSec NAT	IPSec

TCP	UDP	端口名称	相关服务
	5353	多播 DNS	Bonjour
6310 8010 8021-8022 8090 9906 21030 50006-50025	9906	EFI 端口	Command WorkStation 5 和 6、Fiery Central、基于 EFI SDK 的工具、Fiery 打印机驱动程序单纤双向 (bi-di) 功能、WebTools、Fiery 直接移动打印和固有文档转换
9100-9103		打印端口	端口 9100

注释：50006-50025 端口在 Command WorkStation 版本 6.2 和更新版本安装在独立的 Fiery server 上之后启用。

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 管理员也可以启用和禁用 Fiery server 提供的不同网络服务。

IP 过滤

IP 过滤允许或拒绝来自已定义 IP 地址到 Fiery server 的连接请求。管理员可以定义默认策略以允许或拒绝传入数据包，还可以指定最多 16 个 IP 地址或范围的过滤器以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。如果该操作是**拒绝**，则会丢掉源地址属于指定地址的数据包，如果该操作是**接受**，则允许该数据包。

网络验证

SNMP v3

Fiery server 支持最新的 SNMPv3 标准。可加密 SNMPv3 通信数据包来确保机密性、消息完整性和身份验证。

Fiery 管理员可以从 SNMPv3 的三个安全级别中进行选择：最小、中等或最大另外，Fiery 管理员还可以要求在 SNMP 处理之前进行验证，以及对 SNMP 用户名和密码加密。本地管理员可以定义 SNMP 读写组名和其他安全设置。

有关详细信息，请参阅推荐设定（第 27 页）。

IEEE 802.1x

802.1x 是一个针对基于端口的网络访问控制的 IEEE 标准协议。该协议提供 Fiery server 获得 LAN 及其资源的访问权限之前的验证机制。

在启用之后，Fiery server 可以配置为使用 EAP MD5-Challenge、PEAP-MSCHAPv2 或 EAP-TLS 以验证 802.1x 验证服务器。

Fiery server 在启动时或以太网电缆断开连接后重新连接时验证。

网络加密

Internet 协议安全性 (IPsec)

IPsec 通过对每个数据包进行加密和授权为所有使用 IP 协议的应用程序提供安全性。

Fiery server 使用预先共享的密钥验证来通过 IPsec 建立与其他系统的安全连接。

在通过 IPsec 建立客户端计算机与 Fiery server 之间的安全通信之后，包括打印作业在内的所有通信都将通过网络安全地传输。

HTTPS

Fiery server 需要客户端和不同服务器组件之间的安全连接。基于 TLS 的 HTTPS 用于加密两个端点之间的通信。从 WebTools 和 Fiery API 连接到 Fiery server 时需要 HTTPS。这些通信使用 TLS 1.3 和 1.2 加密。

证书管理

Fiery servers 提供接口以管理 TLS 通信期间使用的证书。Fiery servers 支持 X.509 证书格式。

Fiery servers 支持 4096、3072 和 2048 位密钥长度的 RSA 证书。

证书管理允许 Fiery 管理员执行以下操作：

- 创建自签名数字证书。
- 向 Fiery server 添加证书及其相应的私有密钥。
- 从信赖的证书授权添加、浏览、查看和移除证书。

注释：自签名证书不安全。我们强烈建议用户使用来自受信任的证书管理局 (CA) 的证书。

一旦您获得由受信任的证书管理局签署的证书，您可以在 WebTools 配置部分将证书上传到 Fiery server。

电子邮件安全验证

启用电子邮件时，Fiery server 支持 POP 和 SMTP 电子邮件通信协议。（该功能在默认情况下是禁用的。）为保护服务免受攻击以及不当使用，Fiery 管理员可以启用其他安全功能。

使用 SMTP 前先进行 POP 验证

有些电子邮件服务器仍支持不安全的 SMTP 协议，任何人都可以不经验证发送电子邮件。为避免未经授权的访问，有些电子邮件服务器要求电子邮件客户端在使用 SMTP 发送电子邮件之前先进行 POP 验证。对于此类电子邮件服务器，Fiery 管理员需要在使用 SMTP 之前启用 POP 验证。

OP25B

阻断 25 号端口外发 (OP25B) 是一种防垃圾邮件措施，ISP 可以阻止数据包通过其路由器进入 25 号端口。Fiery 管理员可通过电子邮件配置界面指定一个不同的端口。

有关 Fiery server 电子邮件打印工作流程的详细信息，请参阅 电子邮件打印（第 22 页） 。

服务器消息块（SMB）

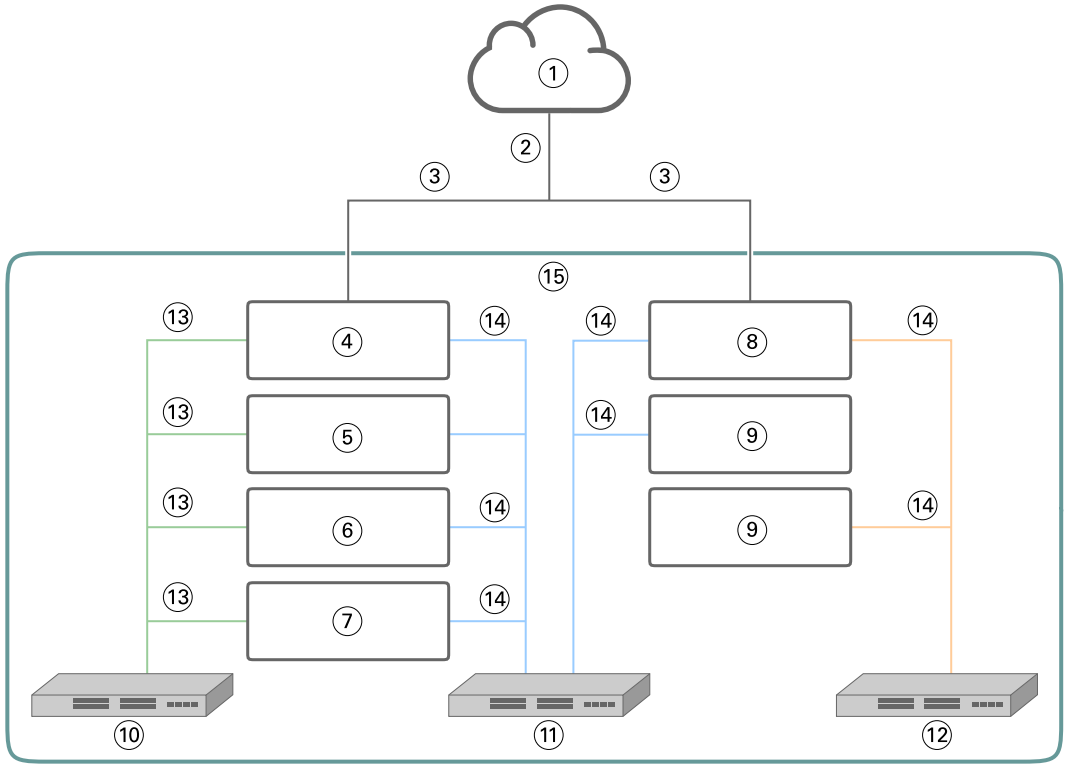
SMB 是为文件和打印机提供共享访问权限的网络协议。SMB v1 在 Fiery servers 上禁用，因为它不符合当前行业安全标准。SMB v2 和 v3 仍然受支持。

SMB 签名在 Fiery server 上强制执行。SMB 签名需要数字签名的数据包，以便接收者能够检查数据包的真实性以防止"中间人"攻击。如果启用了 SMB 验证，用户必须提供 SMB 用户名和密码才能访问 SMB 文件夹和存储在其中的内容。

注释：通过在 Configure 中设置密码可以限制通过 SMB 打印或文件共享。

Fiery XB 网络图

下图显示了 Fiery XB 服务器和高速喷墨打印机如何连接到网络。



1	局域网	9	其他印刷机刀片（可选）
2	作业管理网络通信	10	10 GbE 专用网络
3	1 GbE DHCP 或静态	11	1 GbE 专用网络
4	Fiery 主刀片	12	1 GbE 可编程逻辑控制器专用网络
5	Fiery RIP 刀片（可选）	13	10 GbE
6	Fiery 刀片 #1（可选）	14	1 GbE
7	Fiery 刀片 #2（可选）	15	关闭 Fiery XB 环境
8	印刷机刀片		

访问控制

本章介绍了如何配置 Fiery server 以控制对不同用户群组资源的访问。

用户验证

用户验证功能允许 Fiery server 执行以下操作：

- 验证用户
- 基于用户的权限授权操作

Fiery server 可对以下用户进行验证：

- 基于域：在企业服务器上定义并通过 LDAP 访问的用户
- 基于 Fiery：在 Fiery server 上定义的用户

Fiery server 根据群组成员资格授权用户的操作。每个群组与一组权限（例如灰度打印，彩色或灰度打印）相关联，群组成员的操作限于这些权限。除管理员和操作员帐户之外，Fiery 管理员可以修改任何 Fiery 群组的权限。

对于此版本的用户验证，可以为群组选定如下不同的权限：

- **灰度打印**：此权限允许群组成员在 Fiery server 上将作业打印为灰度。如果用户没有此权限，则 Fiery server 不会打印作业。如果作业为彩色作业，则将打印为灰度。
- **彩色及灰度打印**：此权限允许群组成员在 Fiery server 上以 Fiery server 的彩色和灰度打印功能的全部访问权限打印作业。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**：此权限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**：此权限允许群组成员创建服务器预设，以便允许其他 Fiery 服务器访问常用的作业预设。
- **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。

注释：用户验证将取代成员打印和群组打印功能。

Fiery 软件用户验证

Fiery server 与不同类型的用户交互。这些用户特定于 Fiery 软件，并且与 Windows 定义的用户或角色无关。建议 Fiery 管理员提供密码后才可访问 Fiery server。另外，EFI 建议 Fiery 管理员更改默认密码以满足用户打印环境的安全要求。

- 使用**配置** > **安全性**时，“管理员”和“操作员”的密码最多为 15 个字符。
- 使用**配置** > **用户账户**时，本地用户账户的密码最多为 64 个字符。
- 管理员和操作员密码也可以在**配置** > **用户帐户**中更改，最多为 64 个字符。

以下内容描述不同 Fiery 用户类型所允许的权限：

- **管理员**：完全控制 Fiery server 的所有功能。

  除管理员和操作员帐户之外，Fiery 管理员可以修改任何 Fiery 群组的权限。
- **操作员**：拥有与管理员相同的大部分权限，但没有访问某些 Fiery server 功能的权限（例如设置），并且无法删除作业日志。
- **印刷机操作员**（仅限 Fiery XB 服务器）：可以在印刷机上管理作业。管理员可以为此用户类型添加特定权限。
- **Fiery 服务管理员**（仅限基于 Windows 的 Fiery servers）：用于在 Windows 服务器上安装受信任证书的隐藏管理员帐户。此账户不允许用户登录 Fiery server（本地或远程）。此账户可能显示在某些网络扫描工具上，如果有必要，可以删除。可采用替代标准方法安装受信任的证书。

Fiery 安全审计日志

为了帮助符合要求的组织，Fiery 管理员可以收集和分析保存到安全审核日志中的安全相关事件。

默认情况下安全审计日志为启用状态。

每个安全事件以信息、警告或错误进行归类。没有向管理员提供的警告或通知，仅有静态日志。

日志为通用 SIEM 日志收集和分析解决方案支持的格式。有关捕获事件的信息符合 NIST 特别出版物 800-53，*Recommended Security Controls for Federal Information Systems* (SP800-53)。

Fiery 管理员无需 EFI 干预即可读取事件。基于 Windows 和 Linux 的 Fiery servers 事件均采用 JSON 格式，可通过任何日志收集工具进行处理。对于基于 Windows 的 Fiery 服务器，可以在 Windows 事件管理器中查看这些事件。基于 Linux 的 Fiery servers 管理员可以将日志转发到中央日志收集系统 (SysLog)。

根据分配的磁盘存储容量保留安全事件。当日志大小达到最大存储限制 (400 MB) 时，旧事件将被移除。

操作系统

对于可能影响核心 Fiery server 组件（如主板、处理器、BIOS 等）的安全问题或漏洞，EFI 与 Fiery servers 所用操作系统的制造商密切协作以获取所需的安全更新。此外，Fiery 软件更新通过 EFI 进行数字签名，以防止未经授权的修改，包括插入恶意软件。

Linux (FS500)

FS500 Fiery servers 是使用封闭式架构设计的基于 Linux 的服务器。有限的网络可见性可防止未授权访问。

基于 Linux 的 Fiery servers 特性如下:

- 基于 Linux 的 Fiery servers 不包含可能用于访问操作系统的本地接口。
- 基于 Linux 的 Fiery servers 不支持 SSH 和 Telnet，这会阻止访问操作系统外壳。
- 基于 Linux 的 Fiery servers 不允许安装可能会将系统暴露于漏洞之下的非授权程序。
- FS500 Fiery servers 上使用的 Linux 操作系统是自定义操作系统，仅供 Fiery servers 使用。它具有 Fiery server 需要的全部操作系统组件，但是没有常用 Liunx 系统的一些通用组件和最终用户应用程序。

访问系统

基于 Linux 的 Fiery servers 可通过打印机控制面板的 Fiery 设置或通过 WebTools 中的 Configure 进行配置。WebTools 是一组基于浏览器的页面，允许 Fiery 管理员访问 Fiery server 进行配置和其他系统管理相关的活动。WebTools 在最新的安全 Web 框架上运行，这是大多数现代 Web 浏览器支持的。

Windows 10 (FS500 Pro)

FS500 Pro 独立 Fiery servers 使用 Windows 10 IoT Enterprise 2019 LTSC 作为其操作系统。该 Windows 版本包含最新安全保护功能，具有 Windows 10 1703、1709、1803 和 1809 版提供的所有增强功能。Microsoft 支持每个 LTSC 版本，并在发布后十年内对其进行安全更新。

注释：Windows 10 IoT Enterprise 2019 LTSC 是一个二进制版本，相当于 Windows 10 企业版 1809。

Windows 10 IoT Enterprise 2019 LTSC 包含以下功能:

- 用于特定系统，如 Fiery servers 。
- 集成了许多威胁、信息和身份保护方面的安全改进。
- 提供许多安全更新。
- 不包括面向消费者的应用程序，例如日历、天气、照片等。

Microsoft Windows Update

Microsoft 定期通过 Windows Update 发布安全修补程序以解决潜在的操作系统安全威胁和漏洞。Fiery servers 上 Windows Update 的默认设定会通知用户有修补发布但不下载它们。在 Windows **控制面板**中选择 Windows Update 下的**检查更新**可启用自动更新并开始更新过程。

Windows Update 工具

基于 Windows 的 Fiery servers 能够使用标准 Microsoft 方法更新所有适用的 Microsoft 安全补丁。Fiery server 不支持任何其他第三方更新工具检索安全补丁。

Windows 防病毒软件

Fiery servers 使用 Microsoft 防病毒软件和 Windows 10 Defender 进行保护。通常，第三方防病毒软件可以与 Fiery server 搭配使用。防病毒软件有许多种类，并且可能会包含许多组件和功能来消除威胁。

注意，在 Fiery server 本身上安装、配置和运行防病毒软件非常有用。对于没有本地配置的 Fiery servers，仍可以在远程客户端计算机上启动防病毒软件并扫描共享的 Fiery server 硬盘驱动器。但是，EFI 建议 Fiery 管理员直接与防病毒软件制造商联系，以获取操作支持。

防病毒引擎扫描

即使已安排扫描，防病毒引擎扫描 Fiery server 可能会影响 Fiery 性能。

防间谍软件

防间谍软件程序可能会在文件进入 Fiery server 时影响性能。例如，正在传入的打印作业、在 Fiery server 系统更新期间下载的文件或在 Fiery server 上运行的应用程序的自动更新。

内置防火墙

由于 Fiery server 有防火墙，因此通常不需要防病毒防火墙。EFI 建议客户咨询自己的 IT 部门，确定是否需要安装和运行防病毒软件附带的内置防火墙。有关可用端口的列表，请参阅 网络端口（第 10 页）。

反垃圾邮件

Fiery server 支持通过电子邮件打印和扫描到电子邮件功能。我们建议使用基于服务器的垃圾邮件过滤机制。Fiery servers 还可以配置为从指定的电子邮件地址打印文档。不需要防垃圾邮件组件，因为 Fiery server 上不支持运行独立的电子邮件客户端（如 Outlook）。

HIPS 和应用程序控制

由于主机入侵保护 (HID) 和应用程序控制的复杂性，必须对防病毒配置进行测试并在使用其中任意功能时小心确认。在适当调整后，HIPS 和应用程序控制是卓越的安全措施并可以与 Fiery server 共存。但是，错误的 HIPS 参数设定和错误的文件排除很容易造成 Fiery server 问题 — 许多时候是“接受默认值”导致的。解决方法是查看 HIPS 中选择的选项或应用程序控制设定以及 Fiery server 设定，例如网络端口、网络协议、应用程序可执行文件、配置文件、临时文件等。

安全列表和阻止列表

安全列表和阻止列表功能通常不会对 Fiery server 产生不良影响。EFI 强烈建议客户配置这些功能，以免阻止 Fiery 模块。

电子邮件病毒

一般情况下，通过电子邮件传播的病毒需要收件人做出某种类型的执行操作才会发作。Fiery server 会丢弃 PDL 文件之外的附加文件。 Fiery server 还会忽略 RTF 或 HTML 格式的电子邮件或者包含的任何 JavaScript。除了基于所收到命令发送给特定用户的电子邮件回复之外，通过电子邮件收到的所有文件都会被作为 PDL 作业处理。

注释：有关 Fiery server 电子邮件打印工作流程的详细信息，请参阅 电子邮件打印（第 22 页） 。

数据安全

本节描述旨在保护驻留在 Fiery server 中的用户数据和传输中的数据的安全控件。

关键信息加密

对 Fiery server 中的关键信息进行加密可确保所有密码和相关配置信息存储在 Fiery server 中时都是安全的。关键信息不是加密就是散列。使用的加密算法为 AES256、Diffie-Hellman 和 SHA-2 以符合最新的安全标准。

存储在磁盘上的用户信息无法读取，即使磁盘已从 Fiery server 移除。可使用 Configure 在基于 Windows 的 Fiery servers 上启用或禁用用户数据加密。对于基于 Linux 的 Fiery servers，该功能始终启用。

如果忘记了为恢复数据而输入的密码，则无法重置它，并且 EFI 无法恢复它。必须重新安装软件。

注释：使用数据加密时，磁盘会被分区，只有用户数据分区被加密。无法加密操作系统分区。

高级加密标准 (AES)

可通过 Fiery server 保护静态数据不受未经授权的访问。它使用 256 位 AES 算法加密作业、图像和客户数据。

AES 是一种小巧、快速且不易破解的加密标准，适用于多种设备和应用。它在遵守公司安全策略的同时提供了额外的保护以防止数据窃取。

标准打印

提交至 Fiery server 的作业可发送至 Fiery server 发布的以下打印队列之一：

- 保留队列
- 打印队列
- 按序打印队列
- 直接队列直接连接
- 虚拟打印机（Fiery 管理员定义的自定义队列）

Fiery 管理员可以禁用打印队列和直接队列以限制自动打印。

保留队列、打印队列和按序打印队列

当作业打印到打印队列或保留队列时，作业以假脱机的方式发送到 Fiery server 上的硬盘驱动器。发送到保留队列的作业将保留在 Fiery 硬盘驱动器上，直到用户提交作业进行打印或使用作业管理实用程序删除作业，如 Command WorkStation。

按序打印队列使 Fiery server 能够保持从网络发送的特定作业的作业顺序。工作流程将保持“先入先出”(FIFO) 状态，即根据网络接收作业的顺序执行。不启用按序打印队列，通过 Fiery server 提交的打印作业可能会因诸多因素而弄乱顺序，例如 Fiery server 会在假脱机处理较大的作业时跳过较小的作业。

打印队列

如果已启用已打印队列，则发送至打印队列的作业将在打印后存储在 Fiery server 上的已打印队列中。管理员可以定义已打印队列中保留的作业数量。禁用已打印队列之后，作业将在打印之后自动删除。

直接队列（直接连接）

直接队列设计用于字体下载和需要直接连接到 Fiery servers 中 PostScript 模块的应用程序。

EFI 不建议打印到直接队列。打印之后，Fiery server 会删除通过直接连接发送的全部作业。但是，EFI 并不保证与作业相关的所有临时文件都会被删除。

VDP（可变数据印刷）、PDF 或 TIFF 文件类型的作业发送到直接队列之后重新传送到打印队列。通过 SMB 网络服务发送的作业可以在发送到直接队列之后传送到打印队列。

作业删除

如果从 Fiery server 自动删除或使用 Fiery 工具擦除了作业，则无法查看或取回该作业。如果作业以假脱机方式传送到 Fiery server 硬盘驱动器，则作业元素会保存在硬盘驱动器上，理论上可以通过特定工具恢复，例如司法取证磁盘分析工具。

安全擦除

安全擦除设计用于在 Fiery 功能删除作业时从 Fiery server 硬盘驱动器移除所提交作业的内容。删除作业时，每个作业源文件使用基于美国 DoD 5220.22 M 数据擦除方法的算法覆盖三次。

工作流程	安全消除
存储在 Fiery server 硬盘驱动器上的作业；安全擦除设置为**打开**	是
存储在 Fiery server 硬盘驱动器上的作业；安全擦除设置为**关闭**	否
在安全擦除设置为**打开**后 Fiery server 已接收并删除的作业	是
在安全擦除设置为**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

工作流程	安全消除
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
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

注释：Fiery XB 平台或使用 SSD 的 Fiery servers 不支持安全擦除功能。

系统内存

处理某些文件时会将一些作业数据写入到操作系统内存。在某些情况下，内存中的这些数据可能已经交换到硬盘驱动器并且不会被特别地覆盖。

易失性内存			
类型（SRAM、DRAM 等）	**用户可修改（是或否）**	**功能或用途**	**净化工艺**
DRAM	是	主系统内存（接收发送至直接队列的作业）	关闭 Fiery server 电源
SDRAM（显卡上）	是	显存	关闭 Fiery server 电源

非易失性内存			
类型（SRAM、DRAM 等）	**用户可修改（是或否）**	**功能或用途**	**清除工艺**
BIOS	否	BIOS 功能	从插槽中移除并销毁，但系统将停止运行。
以太网 Eprom	否	以太网芯片固件	退焊并销毁，但系统将停止运行。
CMOS NVRAM	否	Bios 设定存储	卸下系统电池 30 秒。

非易失性内存			
类型（SRAM、DRAM 等）	**用户可修改（是或否）**	**功能或用途**	**清除工艺**
硬盘驱动器 (HDD) 或固态驱动器 (SSD)	是	操作系统 Fiery 应用程序（可能带有用户数据） Fiery 系统软件 打印作业、扫描作业和其他用户数据 出厂默认值的备份映像	重新安装系统软件。 大多数作业都可以使用安全擦除功能*安全删除。第三方和 Fiery 合作伙伴清除工具可用于完全擦除这些设备的数据。
注释：易失存储器和 RAM 可在处理客户的数据时包含客户数据。BIOS、CMOS 和 NVRAM 等非易失性存储器中不存储客户数据。 * 由于发生内存磨损映射，安全擦除多路覆盖方法无法完全清理固态硬盘。另外，尝试这样做也会大大削弱固态驱动器的操作寿命。Fiery XB 平台不支持此功能。			

安全打印

安全打印功能需要用户在 Fiery server 和打印机 上输入作业特定的密码才能打印作业。

此功能需要访问打印机控制面板。该功能的目的是将对文档的访问限制为具有作业密码的用户，而且可以在打印机控制面板本地输入。

安全打印工作流程

用户在 Fiery Driver 中的 **安全打印**字段中输入密码。当此作业发送到 Fiery server 的打印或保留队列时，该作业排队并保留等待输入密码。

注释：使用安全打印密码发送的作业无法从 Command WorkStation 查看。

在打印机控制面板中，用户访问安全打印窗口并输入密码。然后，用户可以查找使用该密码发送的作业并打印，然后删除该作业。

已打印的安全作业未移动到已打印队列，打印后会自动删除。

注释：部分数据可能暂时保留在操作系统文件中。

电子邮件打印

Fiery server 可接收和打印通过电子邮件发送的作业。管理员可以在 Fiery server 上存储已授权电子邮件地址的列表。如果某个电子邮件地址不在授权电子邮件地址列表中，则从该电子邮件地址接收的所有邮件都将被删除。默认情况下，电子邮件打印功能是关闭的。管理员可以打开及关闭电子邮件打印功能。

作业管理

对提交给 Fiery server 的作业执行作业操作需要具有管理员或操作员访问权限的 Fiery 作业管理实用程序。

作业日志

作业日志存储在 Fiery server 上。作业日志的单个记录是无法删除的。作业日志包含打印和扫描作业的信息，例如启动作业的用户、执行作业的时间，以及作业所用纸张和颜色等特点。作业日志可用于检查 Fiery server 的作业活动。

具有操作员访问权限的用户可以从 Command WorkStation 查看、导出或打印作业日志。具有管理员访问权限的用户可以从 Command WorkStation 删除作业日志。

设置

设置需要提供管理员密码。Fiery server 可从 WebTools 中的 Configure 工具或 Command WorkStation 或打印机控制面板上的“设置”功能设置。

扫描

Fiery server 允许将打印机玻璃上的图像扫描回启动扫描的工作站。在扫描功能从工作站启动之后，原始位图图像将直接发送至工作站。

用户可以将文档扫描到 Fiery server 以供分发、存储和检索。所有扫描的文档都将写入磁盘。管理员可以配置 Fiery server 在预定义的时间段之后自动删除扫描作业。

分发扫描的作业

扫描作业可以通过多种方法分发。

电子邮件

带有扫描作业附件的电子邮件将发送至邮件服务器，在其中路由到所需的目的地。

注释：如果扫描作业的文件大小超过管理员定义的最大文件大小，作业将存储在 Fiery server 硬盘驱动器上，可通过 URL 进行访问。

FTP

文件将发送至 FTP 目的地。包括目的地在内的传输记录保存在 FTP 日志中，可通过打印机控制面板打印页面命令访问该记录。FTP 代理服务器可定义为穿过防火墙发送作业。

Fiery server 保留队列

文件将发送至 Fiery server 保留队列，但不会保留为扫描作业。

有关 Fiery server 保留队列的详细信息，请参阅 保留队列、打印队列和按序打印队列（第 20 页）。

互联网传真

文件将发送至邮件服务器，然后从其中转发到所需的互联网传真目的地。

邮箱

文件存储在 Fiery server 上并赋予一个邮箱代码。用户需要输入正确的邮箱代码才能访问存储的扫描作业。用户可以选择设置密码以保护其扫描邮箱内容免受未经授权访问。扫描作业可通过 URL 检索。

法规和框架合规性

下表为运行 FS500 Pro/FS500 系统软件的 Fiery 服务器提供了法规和框架合规性。

法规/框架	范围	NX 系列 (FS500 Pro)	A/E 系列 (FS500)
FIPS 140-2	• 美国政府（联邦和州） • 加密模块的安全要求	合规 Windows 10 2019 LTSC FIPS 证书： • #3197 • #3196 • #3092	不合规
CIS 基准	• 整体 • 政府/私营部门 • 配置基线和安全配置系统的最佳实践	合规 Microsoft Windows 10 Enterprise（第 1809 版）基准	不适用*
安全技术实施指南 (STIG)	• 美国政府（联邦和州）配置标准，包括特定产品的网络安全要求	部分合规 Windows 10 STIG 版本 2，R3 例外：CCI-000366：受信任的平台模块 (TPM) 不可用	不适用*
ISO/IEC-15408	• 整体 • 常用标准 • IT 安全的信息技术安全技术评价标准	部分合规 • 访问控制需要 LDAP/AD 验证 • 不支持 TPM 和安全启动	不合规
IEEE 2600.2-2009	• 整体 • 政府/私营部门 • 硬拷贝设备环境 B 的常用标准特性档	部分合规 • 不支持 TPM 和安全启动 • 阻力和检测要求需要可选的 Fiery 磁盘驱动器安全套件	不合规

法规/框架	范围	NX 系列 (FS500 Pro)	A/E 系列 (FS500)
保护计算机安全评估矩阵 (SCSEM)	• 美国政府（联邦和州） • 联邦、州和地方机构的税收信息安全指南	部分合规 • 不支持 TPM 和安全启动 • 阻力和检测要求需要可选的 Fiery 磁盘驱动器安全套件	不合规
DoD 522.22-M	数据清理标准，3 次成像	合规	合规
NIST 800-88	数据清理标准，1 次成像	不合规	不合规
军队 RMF 认证	• 美国政府 • 军队信息技术风险管理框架	部分合规 • 不支持 TPM 和安全启动	部分合规 • 不支持 TPM 和安全启动

*超出监管或框架范围。A 和 E 系列基于 Linux 的服务器是封闭的系统，不提供直接访问文件系统的权限。有限的网络可见性可防止未授权访问。

FIPS 140-2 合规性

正确配置后，在 Windows 10 2019 LTSC 下运行的 FS500 Pro 的 Fiery 服务器符合 FIPS 140-2 数据加密指南的要求。*FIPS 140-2 模式*下的 Fiery 服务器仅会使用在美国联邦政府的加密算法验证程序 (CAVP) 中验证和注册过的加密算法，来加密非活动和传输中的数据。

若要在 Fiery 中启用 *FIPS 140-2 模式*，需要用户遵循高级配置过程来增强服务器安全性。

安全 Fiery 服务器配置指南

以下指南可帮助 Fiery 管理员在配置 Fiery server 时提高安全性。

更改管理员密码

我们建议您在安装时以及根据组织的安全策略要求定期更改默认 Fiery 管理员密码。管理员默认密码应在第一次设置期间在 **Fiery 设置向导**中更改。可通过在 WebTools 中进行首次设置后更改管理员和操作员密码，具体路径为：**配置** > **安全** > **管理员密码**（或操作员密码）。**用户帐户**也提供密码设置。

管理员密码为用户提供本地或从远程客户端访问 Fiery server 的全部权限。完全访问包括但不限于:

- 文件系统
- 系统安全策略
- 注册表项
- 管理员密码，它拒绝匿名用户访问 Fiery server

推荐设定

- 在 **Network** > **SNMP** 中为 SNMP 选择**最大**安全级别：

  选择“最大安全”将限制 Fiery server 仅支持 SNMP v3。

  如果 SNMP 管理员仅使用 SNMP v1/v2c，请更改**读取组名**字段的值。Fiery server 允许您从 WebTools（具体路径为：**配置** > **网络** > **SNMP**）和打印机控制面板（具体路径为：**网络** > **SNMP**）更改 SNMP **读取组名**和**写入组名**字段的值。
- 在作业提交中禁用 WSD 。
- 如果使用 lpr、端口 9100 或 IPP 进行打印，则在作业提交中禁用 Windows 打印。
- 在**安全** > **TCP/IP** 端口过滤中启用 TCP/IP 端口过滤器以拦截端口。

  如果您没有使用 Windows 打印，并且不需要访问或共享文件文件夹，则清除端口 137-139 和 445。 禁用不安全的 80 (HTTP) 端口通信。

除了操作系统级别的保护外，Fiery server 还有以下附加的安全功能以帮助保护您的数据:

- Fiery servers 具有安全打印功能，确保用户仅获取自己的打印作业。
- Fiery servers 与领先的作业会计解决方案集成，通过后续打印来包含额外的安全性。

Fiery servers 具有许多安全功能，但不是面向互联网的服务器。应将它们置于受保护的环境中，并需要网络管理员正确配置其可访问性。

选择高安全性特性档

Fiery server 根据不同的风险和威胁级别（**标准**、**高**、**当前**）提供预先定义的安全建议。此功能称为**安全特性档**，可从以下位置访问：

- Fiery 软件向导
- **WebTools** > **配置** > **安全**

高安全特性档让 Fiery server 更安全并启用最常用的安全功能。

选项	高
TCP/IP 端口过滤	已启用
Service Location Protocol (SLP)	禁用
Bonjour	禁用
安全消除	已启用
远程桌面	禁用
SMB 密码	已启用
USB 存储设备	禁用
PostScript 安全	已启用
端口 9100	已禁用
LPD	已启用
Windows 打印	禁用
IPP	已启用
Web Services for Devices (WSD)	禁用
通过电子邮件打印	禁用
FTP 打印	禁用
直接移动打印	禁用

EFI 建议对具有最大安全要求的环境使用**高**安全性特性档。

结论

EFI 在 Fiery server 上提供了一套强大的标准和可选安全功能，可针对任何环境为客户提供全面、可定制的安全解决方案。EFI 致力于确保 Fiery server 得到有效保护，免受恶意或无意使用的漏洞，以便我们的客户能够以最大效率运营公司。