



Fiery FS800 Pro/FS800 DFEs

Security White Paper

© 2026 Fiery, LLC. As informações nesta publicação estão cobertas pelos termos dos Avisos de caráter legal deste produto.

6 de agosto de 2026



Conteúdo

Introdução	5
Princípios de segurança	6
Autenticação e controle de acesso	7
Autenticação do usuário	7
Privilégios de grupo	7
Usuários locais	8
Contas de usuário locais da Fiery e privilégios de acesso	8
Autenticação LDAP	8
Logon único (SSO)	9
Medidas de segurança de dados	10
Armazenamento criptografado: protege as tarefas de impressão e os dados de configuração	10
Exclusão segura: garante que os dados sejam irrecuperáveis após a exclusão	10
Segurança da rede	12
Protocolos de rede compatíveis	12
Portas de rede	12
Portas de entrada	12
Portas de saída	14
Comunicação com serviços em nuvem	14
Filtro IP	16
Autenticação de rede	16
SNMP v3	16
IEEE 802.1x	16
Criptografia de rede	16
Segurança de protocolo IP (IPsec)	17
HTTPS	17
Gerenciamento de certificados	17
Bloco de mensagem do servidor (SMB)	17
Segurança de hardware	19
Memória volátil (RAM)	19
Memória não volátil e armazenamento de dados	19
Memória flash	19

CMOS e NVRAM	19
Unidades de armazenamento	20
Portas físicas	20
Integridade do sistema e atualizações seguras	21
Registro de auditoria de segurança	21
Inicialização segura	21
Atualizações assinadas digitalmente	21
Gerenciamento automatizado de atualizações de segurança	22
Atualizações de segurança do software Fiery DFE	23
Conformidade e boas práticas	24
Diretrizes para configuração segura do Fiery DFE	25
Alterar a senha do Administrador	25
Boas práticas para operar segura e eficientemente	25
Ambientes de alta segurança	25
Conclusão	26
Novidades no FS800, FS800 Pro	27

Introdução

Este documento fornece uma visão geral dos recursos de segurança em front-end digitais (DFEs) Fiery. Ele fornece aos administradores de TI e aos profissionais de segurança as informações necessárias para avaliar como os DFEs Fiery garantem a segurança dos ambientes de impressão. O documento explica os princípios e os mecanismos usados nos DFEs Fiery para proteger dados, melhorar a segurança de rede e manter a integridade do sistema.

Princípios de segurança

Os DFEs Fiery são meticulosamente projetados para aderir às boas práticas do setor, garantindo a conformidade com os regulamentos de proteção de dados e com os requisitos de segurança empresarial. Os princípios fundamentais que sustentam este projeto são os seguintes:

- Proteção de dados: criptografia de dados em repouso e de dados em trânsito
- Segurança de rede: acesso controlado, protocolos de comunicação seguros e mecanismos de autenticação
- Integridade do sistema: verificação de firmware, inicialização segura e atualizações de segurança

Em colaboração com nossos parceiros e fornecedores globais, fornecemos suporte contínuo aos nossos clientes à medida que as ameaças evoluem. Para garantir a segurança total do sistema, recomendamos que os usuários finais integrem os recursos de segurança Fiery com as políticas de segurança de suas próprias organizações e adotem as boas práticas do setor, incluindo a implementação de senhas seguras e medidas robustas de segurança física.

Autenticação e controle de acesso

Os DFEs Fiery aceitam vários métodos de autenticação, incluindo:

- Integração LDAP/Active Directory
- Autenticação Multifator (MFA) implementada por meio de logon único (SSO)

Autenticação do usuário

O recurso de autenticação permite que o Fiery DFE execute as seguintes funções:

- Autenticar um usuário
- Controle de acesso baseado em função (RBAC)

O Fiery DFE é compatível com três métodos de autenticação de usuário:

- Autenticação local para usuários definidos no Fiery DFE
- Autenticação de fator único (SFA) através de servidores de autenticação de rede externos que utilizam o LDAP (por exemplo, Microsoft Active Directory)
- Autenticação de vários fatores (MFA) por meio de logon único (SSO)

Independentemente do método usado, as contas de administrador sempre exigem autenticação. Isso não pode ser desativado.

Privilégios de grupo

O Fiery DFE autoriza as ações dos usuários de acordo com sua participação em grupos. Cada grupo é associado a um conjunto específico de privilégios, como impressão em cores ou em preto e branco (P&B). As ações dos membros do grupo são restritas a esses privilégios. O Administrador Fiery tem autoridade para modificar os privilégios de qualquer grupo Fiery, com exceção de contas de Administrador e Operador.

Neste método de autenticação de usuário, os diversos privilégios que podem ser selecionados para um grupo são os seguintes:

- Imprimir em P&B: permite que os membros do grupo imprimam tarefas em P&B. Se a tarefa for colorida, ela será impressa em P&B.
- Imprimir em cores e em P&B: permite que os membros do grupo imprimam tarefas com acesso total aos recursos de impressão em cores e em P&B do Fiery DFE. Sem esse privilégio ou o da impressão em P&B, os usuários ainda podem enviar tarefas de impressão, mas a impressão falhará.
- Caixa de correio do Fiery: permite que os membros do grupo tenham caixas de correio individuais. O Fiery DFE cria uma caixa de correio com base no nome do usuário com um privilégio de caixa de correio. O acesso a essa caixa de correio é limitado a usuários com o nome de usuário e a senha da caixa de correio.

- Calibragem: esse privilégio permite que os membros do grupo realizem a calibragem de cores.
- Criar predefinições de servidor: permite que os membros do grupo criem predefinições de servidor. Os membros do grupo têm acesso a essas predefinições.
- Gerenciar fluxos de trabalho: esse privilégio permite que os membros do grupo criem, publiquem ou editem impressoras virtuais.
- Editar tarefas (somente DFEs Fiery XB): esse privilégio permite que os membros do grupo editem uma tarefa na fila.

Administradores com privilégios elevados podem personalizar esses recursos para restringir o acesso não autorizado e impor protocolos de segurança organizacional.

Usuários locais

O software do Fiery DFE interage com tipos de usuário únicos, diferentes dos usuários ou funções do Windows. Os Administradores Fiery devem alterar imediatamente todas as senhas padrão após a instalação inicial. O acesso por senha ao Fiery DFE deve ser rigorosamente imposto.

- O comprimento máximo da senha para "Administrador" e "Operador" é de 64 caracteres ao usar **Configure > Segurança**.
- O comprimento máximo da senha para contas de usuários locais é de 64 caracteres ao usar **Configure > Contas de Usuário**.
- As senhas do administrador e do operador também podem ser alteradas em **Configurar > Contas de usuário**.

Contas de usuário locais da Fiery e privilégios de acesso

- Administrador: controle total das funcionalidades do Fiery DFE, pode alterar os privilégios de grupos Fiery, com exceção de contas de Administrador e Operador.
- Operador: tem os mesmos privilégios que o Administrador, mas não tem acesso à configuração do DFE e à exclusão do registro de tarefas.
- Operador de impressora (somente DFEs Fiery XB): gerencia tarefas na impressora, com privilégios específicos adicionados pelo Administrador.
- Administrador do Fiery DFE (somente servidores Windows): uma conta de Administrador oculta para instalar o certificado de confiança, não pode fazer login no Fiery DFE, aparece nas ferramentas de varredura de rede e pode ser removida.
- Fiery_SMB_User: conta de impressão padrão do Windows (SMB) que fornece visibilidade das filas de impressão do Fiery DFE por meio do Ambiente de Rede.
- Convidado (padrão, sem senha): tem os mesmos privilégios que o Operador, mas não pode acessar o registro de tarefas, fazer edições, alterar o status ou visualizar as tarefas.

Autenticação LDAP

O Fiery DFE usa o LDAP versão 3 (em conformidade com o RFC 2251) para se comunicar com servidores corporativos. Por meio do LDAPv3, ele recupera endereços de e-mail de usuários para recursos de varredura, bem

como informações de usuários e de grupos para autenticação. Esta funcionalidade é compatível apenas com conexões LDAP para servidores Active Directory.

O Fiery DFE é compatível com os seguintes métodos de autenticação usando LDAP:

- Automático
- SIMPLES
- GSSAPI

A tabela a seguir descreve os diferentes métodos de autenticação LDAP:

Método de autenticação	Descrição	Servidor Active Directory
Automático	Esta opção seleciona GSSAPI ou SIMPLES com base no método de autenticação suportado pelo servidor LDAP.	Suportado
SIMPLES	A senha é obrigatória. Se LDAP sobre TLS estiver selecionado, a senha será criptografada usando TLS.	Suportado
GSSAPI	Este método usa tickets Kerberos em vez de senhas, eliminando a necessidade de TLS.	Suportado

Logon único (SSO)

DFEs Fiery FS800 Pro são compatíveis com o protocolo OpenID Connect para autenticação de usuário por logon único (SSO) na nuvem com o Microsoft Entra ID (antes conhecido como Azure AD). Os usuários podem fazer logon no Fiery DFE usando suas credenciais do Entra ID.

Esse método de autenticação é compatível com a autenticação de vários fatores (MFA).

Essa abordagem de gerenciamento de identidade garante que os Fiery DFEs nunca armazenem senhas de usuário localmente, aumentando significativamente a segurança.

Medidas de segurança de dados

Para proteger informações confidenciais, os DFEs Fiery implementam:

Armazenamento criptografado: protege as tarefas de impressão e os dados de configuração

A criptografia de dados críticos de clientes garante o armazenamento seguro de senhas e informações de configuração relacionadas no Fiery DFE. Essas informações críticas são criptografadas ou codificadas em hash usando algoritmos criptográficos, como AES-256 e SHA-2, que aderem aos mais recentes padrões de segurança.

Dados de clientes armazenados no disco permanecem inacessíveis mesmo que o disco seja removido do Fiery DFE. A criptografia de dados do usuário pode ser ativada ou desativada em Fiery DFEs baseados em Windows. Para Fiery DFEs baseados em Linux, o recurso de criptografia está sempre ativado.

Caso a senha usada para recuperação de dados seja esquecida, a FIERY não poderá redefini-la, exigindo uma reinstalação completa do software.

Fiery DFEs baseados em Windows também fornecem uma opção para criptografar a unidade de inicialização que contém o sistema operacional. Essa criptografia ajuda a evitar ataques off-line ao Fiery DFE e garante que a unidade de inicialização não possa ser usada em outro dispositivo.

Exclusão segura: garante que os dados sejam irrecuperáveis após a exclusão

Os DFEs FS800 Pro baseados em Windows são compatíveis com o padrão de sanitização de dados NIST 800-88. Os administradores Fiery podem configurar essa opção para métodos de substituição de imagem de 1 ou 3 passagens.

Nota: O recurso de exclusão segura não é compatível com plataformas Fiery baseadas em Linux e XB ou com dados de usuário armazenados em SSDs.

Fluxos de trabalho	Exclusão segura
Tarefas armazenadas na unidade de disco rígido do Fiery DFE; Exclusão segura definida como Ativada	Sim
Tarefas armazenadas na unidade de disco rígido do Fiery DFE; Exclusão segura definida como Desativada	Não
Tarefas recebidas pelo Fiery DFE e excluídas após a opção Exclusão segura ser definida como Ativada	Sim
Tarefas recebidas pelo Fiery DFE e excluídas antes de a opção Exclusão segura ser definida como Ativada	Não
Cópias de tarefas enviadas para outro Fiery DFE (balanceamento de carga)	Não
Tarefas arquivadas para mídia removível	Não
Tarefas arquivadas em unidades de rede	Não

Fluxos de trabalho	Exclusão segura
Tarefas localizadas em dispositivos cliente	Não
Limpar a execução do servidor	Sim
Páginas mescladas ou copiadas em outra tarefa (por exemplo, tarefas do Fiery Impose ou PDFs combinados)	Não
Tarefas recebidas da conexão de SMB e salvas na unidade de disco rígido do Fiery DFE	Não
Partes de uma tarefa gravada na unidade de disco rígido do Fiery DFE durante operações de troca ou armazenamento em cache de disco	Não
Entradas do registro de tarefas	Não
Entradas do registro de tarefas após a execução de limpeza do servidor	Sim
O Fiery DFE foi desligado antes de a exclusão da tarefa ser concluída	Não
Desfragmentar a unidade disco rígido do Fiery DFE antes de excluir uma tarefa	Não

Segurança da rede

Os Fiery DFEs utilizam os seguintes mecanismos de segurança para proteger as comunicações de rede:

- Configuração de firewall, incluindo filtros IP e gerenciamento de portas
- Transport Layer Security (TLS) para comunicação criptografada (por exemplo, HTTPS, LDAPS)
- IPSec para comunicação segura criptografada de host a host
- SNMP v3 para monitoramento e gerenciamento seguro da rede

Protocolos de rede compatíveis

O FS800/FS800 Pro é compatível com uma variedade de protocolos de rede padrão do setor para garantir compatibilidade, segurança e comunicação eficiente em diversos ambientes. Estes incluem:

- **Protocolos principais:** TCP/IP, IPv4 IPv6
- **Protocolos web:** HTTP/1.1, HTTPS (TLS 1.2/1.3)
- **Serviços de impressão e de arquivos:** FTP, LPR, IPP 2.0, SMB v2, SMB v3, Porta 9100
- **Gerenciamento e monitoramento:** SNMP v1, v2c e v3
- **Acesso remoto:** RDP (apenas DFEs Fiery baseados em Windows)
- **Segurança e autenticação:** IPSec (IKEv2), LDAP v3, IEEE 802.1X
- **Serviços de rede:** DHCP, DNS
- **Protocolos de descoberta:** WSD, Bonjour, SLP

Portas de rede

Por padrão, todas as portas TCP/IP não utilizadas são desativadas. O Administrador Fiery pode ativar ou desativar as portas de rede conforme necessário. Desativar uma porta impede conexões externas por meio dela.

Portas de entrada

Os Fiery DFEs supervisionam e monitoram as conexões de rede recebidas, permitindo que apenas o tráfego autorizado acesse o DFE e protegendo-o contra acessos não autorizados ou ataques.

TCP	UDP	Nome da porta	Serviços dependentes
20-21		FTP	FTP
80		HTTP	WebTools, IPP

TCP	UDP	Nome da porta	Serviços dependentes
135		MS RPC	Serviço RPC da Microsoft*. Uma porta adicional no intervalo de 49152-65535 será aberta para fornecer o serviço de ponto e impressão relacionado ao SMB.
137-139		NETBIOS	Impressão no Windows. Essas portas são fechadas por padrão porque o NetBIOS não é seguro.
	161, 162	SNMP	Ferramentas baseadas em SNMP
	427	SLP	Service Location Protocol. Essa porta é bloqueada por padrão pois o SLP não é seguro.
443		HTTPS	WebTools, IPPS
445		SMB/IP	SMB sobre TCP/IP
	500	ISAKMP	IPsec
515		LPD	Impressão LPR
631		IPP	IPP
3389		RDP	Área de trabalho remota (apenas Fiery DFEs baseados em Windows)
3702	3702	WS-Discovery	Web Services for Devices (WSD). Permite a descoberta e a impressão no Fiery DFE através do WSD.
	4500	IPsec NAT traversal	IPsec
	5353	DNS multicast (mDNS)	Bonjour
6310		DMP	Impressão móvel direta
8010		Porta FIERY	JDF
8021-8022		Portas FIERY	Fiery Harmony, Fiery HotFolders e Fiery Command WorkStation
8090		Porta FIERY	OFA
9100-9103		Portas de impressão	Porta 9100
	9906	Porta FIERY	Descoberta do Harmony
21030		Porta FIERY	Fiery Image Viewer

Nota: As portas IPsec (500 e 4500) só podem ser configuradas para o FS800 (Fiery DFEs baseados em Linux).

Outras portas TCP, exceto as especificadas pelo parceiro Fiery, são desativadas. Nenhum serviço dependente em uma porta desativada pode ser acessado remotamente.

O Administrador Fiery também pode ativar ou desativar os vários serviços dependentes fornecidos pelo Fiery DFE.

Portas de saída

Os Fiery DFEs gerenciam e restringem o tráfego de rede de saída para garantir que apenas comunicações autorizadas saiam do dispositivo, reduzindo a exposição a ameaças externas.

Portas de saída	Objetivo	Padrão/Ativado na configuração
53	DNS	Padrão
67	DHCP	Padrão
80, 443	Atualizações do Sistema Fiery, Atualizações do Windows, JDF, PrintMe e outras comunicações na nuvem	Padrão
161, 162	SNMP	Em configuração de IP dupla
21	Digitalização para FTP	Ativado na configuração
123	NTP	Ativado na configuração
389/636	Serviços LDAP	Ativado na configuração
445	Digitalizar para SMB/Registro de tarefas para SMB/Caminho global comum JDF	Ativado na configuração
500/4500	IPSEC	Ativado na configuração
8080/8443	Porta proxy HTTP/HTTPS/FTP	Ativado na configuração

Comunicação com serviços em nuvem

Esta lista enumera os serviços e os aplicativos Fiery que exigem comunicação com serviços externos baseados em nuvem para, por exemplo, baixar atualizações de segurança Fiery ou ativar licenças. Esta documentação é particularmente útil para clientes que desabilitaram todas as comunicações externas e estão tentando abrir exceções no firewall corporativo.

Serviço/aplicativo Fiery	Nome de domínio/URL totalmente qualificado	Porta	Localização do servidor	Informações de uso
Atualização do sistema	https://liveupdate.fiery.com/des/hypatia.asmx	443	Fiery	Faça o download das atualizações de segurança Fiery
OFA	https://flexlicensing.fiery.com	443	Fiery	Ativação da licença
IQ	https://iq.fiery.com/iq	443	AWS	Nuvem do Fiery IQ

Serviço/ aplicativo Fierly	Nome de domínio/URL totalmente qualificado	Porta	Localização do servidor	Informações de uso
LINQ	https://ews.fierly.com	443	Azure	Dados analíticos
Impressão Universal	Vários domínios: - portal.azure.com - print.print.microsoft.com - notification.print.microsoft.com - discovery.print.microsoft.com - graph.print.microsoft.com	80/443	Azure	Serviço de Proxy IPP e Impressão Universal
SSO	login.microsoft.com	80/443	Microsoft	Logon único
Windows Server Update Services (WSUS)	Vários domínios: - 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	Atualizações do Windows

Serviço/ aplicativo Fiery	Nome de domínio/URL totalmente qualificado	Porta	Localização do servidor	Informações de uso
Command WorkStation	Vários domínios: • https://help.fiery.com • https://learning.fiery.com • https://communities.fiery.com/s/ • https://liveupdate.fiery.com • https://iq.fiery.com	443	Fiery	Suporte Fiery, atualizações do Fiery, Fiery Cloud

Filtro IP

O filtro IP permite que o Administrador controle as solicitações de conexão ao Fiery DFE com base em endereços IP predefinidos. Ao definir políticas padrão, o Administrador pode especificar se os pacotes de dados recebidos devem ser permitidos ou negados. Além disso, podem criar filtros para até 16 intervalos ou endereços IP, permitindo ou negando solicitações de conexão de acordo com a necessidade.

Cada configuração de filtro IP especifica um endereço IP ou um intervalo de endereços IP e a ação correspondente. Quando a ação é Negar, os pacotes com endereço de origem pertencente aos endereços especificados são ignorados. Por outro lado, quando a ação é Aceitar, os pacotes são permitidos.

Autenticação de rede

SNMP v3

O Fiery DFE é compatível com o padrão SNMPv3 mais recente, facilitando a comunicação criptografada de pacotes para garantir confidencialidade, integridade da mensagem e autenticação.

O Administrador Fiery pode selecionar entre três níveis de segurança SNMP: Mínimo, Médio e Máximo. Nesses níveis, as senhas são codificadas em hash usando algoritmos como SHA-1 ou SHA-256, e toda a mensagem SNMP é criptografada. Além disso, o Administrador local pode configurar nomes de comunidade de leitura e gravação SNMP com outras configurações de segurança.

IEEE 802.1x

802.1X é um padrão IEEE para controle de acesso à rede baseado em porta que garante que os dispositivos sejam autenticados antes de acessarem a rede local e seus recursos. No Fiery DFEs, o 802.1X pode ser configurado para usar EAP-MD5 Challenge ou PEAP-MSCHAPv2 como métodos de autenticação baseados em credenciais, ou EAP-TLS para autenticação baseada em certificado. Os Fiery DFEs são compatíveis apenas com certificados de usuário (não certificados de dispositivo) para autenticação EAP-TLS. O EAP-MD5 Challenge é fornecido para compatibilidade e é menos seguro que o PEAP-MSCHAPv2 e o EAP-TLS.

O Fiery DFE executa a autenticação 802.1X na inicialização e sempre que a conexão de rede é restabelecida.

Criptografia de rede

Segurança de protocolo IP (IPsec).

O IPsec aumenta a segurança das comunicações baseadas em IP criptografando e autenticando cada pacote na camada de rede, protegendo assim os dados em trânsito em todos os aplicativos que usam IP. O Fiery DFE utiliza a autenticação de chave pré-compartilhada para estabelecer conexões seguras com outros sistemas via IPsec. Uma vez que a comunicação IPsec é estabelecida entre um computador cliente e um Fiery DFE, todas as comunicações, incluindo tarefas de impressão, serão transmitidas com segurança pela rede.

Há protocolos, como LPR, porta 9100, FTP, WSD e Harmony (protocolo proprietário da Fiery), usados para o envio de tarefas de impressão, atualizações de status da tarefa e comandos administrativos. Esses protocolos não passam por um canal seguro, portanto, as organizações que exigem confidencialidade e proteção de integridade para essas funções devem utilizar o IPsec entre o computador cliente e o Fiery DFE.

HTTPS

Os Fiery DFEs usam HTTPS sobre TLS para proteger comunicações baseadas na Web e de API entre clientes e componentes do servidor. Os Fiery DFEs são compatíveis com TLS 1.3 e TLS 1.2, fornecendo forte proteção criptográfica e recursos de segurança modernos. O HTTPS é obrigatório para conexões com o WebTools e com APIs da Fiery, garantindo que o tráfego administrativo e operacional transportado por essas interfaces seja criptografado em trânsito e protegido contra interceptação ou adulteração. Nem toda comunicação entre cliente e servidor é transportada por HTTPS.

Gerenciamento de certificados

Os Fiery DFEs oferecem uma interface para gerenciar os certificados utilizados em comunicações TLS. Os Fiery DFEs oferecem suporte a certificados X.509 em formato PEM, codificados em Base64, usando chaves RSA com comprimentos de 4096, 3072 ou 2048 bits.

O gerenciamento de certificados permite que o Administrador Fiery faça as seguintes ações:

- Gerar certificados digitais autoassinados.
- Adicionar um certificado e sua chave privada associada ao Fiery DFE.
- Adicionar, navegar, visualizar e remover certificados de uma autoridade de certificados confiável.

Os certificados digitais autoassinados fornecem criptografia, mas não oferecem validação automática de confiabilidade. Para implantações seguras, recomendamos o uso de certificados emitidos por uma Autoridade de Certificação (CA) confiável para garantir uma verificação de identidade adequada.

Depois que um certificado for assinado por uma CA confiável, ele poderá ser carregado no Fiery DFE, na seção Configure do WebTools.

Bloco de mensagem do servidor (SMB)

O SMBv1, protocolo legado para compartilhamento de arquivos e impressoras, está desativado nos Fiery DFEs devido a vulnerabilidades de segurança conhecidas. Em vez disso, os Fiery DFEs são compatíveis com o SMBv2 e o SMBv3. A assinatura SMB é obrigatória, garantindo que todos os pacotes sejam assinados digitalmente para evitar ataques do tipo man-in-the-middle. Quando a autenticação SMB está ativada, os usuários devem fornecer nome de

usuário e senha válidos para acessar pastas e conteúdo compartilhados. A impressão ou o compartilhamento de arquivos via SMB para uma conta de convidado também podem ser restringidos ao definir uma senha no Fiery Configure.

Segurança de hardware

Os Fiery DFEs são projetados com segurança de hardware de nível empresarial em mente. A proteção de informações confidenciais não se limita aos controles de software. Os componentes de hardware desempenham um papel crítico na manutenção da integridade do sistema e da confidencialidade dos dados. Os principais elementos de hardware e suas medidas de segurança são descritos abaixo.

Memória volátil (RAM)

Os Fiery DFEs utilizam memória volátil (RAM) para armazenar dados temporariamente durante operações ativas. Para mitigar o risco de exposição de dados:

- As informações confidenciais na RAM são apagadas imediatamente após o uso ou após o desligamento do sistema.
- Técnicas de limpeza de memória são aplicadas para evitar que dados residuais persistam.
- O acesso à RAM é restrito por meio da separação de privilégios imposta pelo processador e pelo sistema operacional.

Memória não volátil e armazenamento de dados

A memória não volátil, incluindo discos rígidos, unidades de estado sólido (SSDs) e outros armazenamentos persistentes, retém dados mesmo quando o sistema está desligado. As medidas de segurança incluem:

- Criptografia de dados do usuário (UDE) para proteger os dados armazenados.
- Métodos de exclusão seguros para tornar informações confidenciais irre recuperáveis quando os arquivos são removidos.

Memória flash

A memória flash é usada para armazenar firmware, arquivos de configuração e configurações do sistema. Para manter sua segurança:

- O firmware é assinado digitalmente para evitar violação.
- As atualizações de firmware são verificadas por meio de somas de verificação criptográficas antes da instalação.
- Os mecanismos de proteção contra gravação impedem modificações não autorizadas durante o tempo de execução.

CMOS e NVRAM

Parâmetros críticos do sistema, como configurações de hardware e configurações de inicialização, são armazenados em CMOS e NVRAM (RAM Não Volátil). Para proteger esses dados:

- O acesso é restrito a processos administrativos autorizados.
- A inicialização segura ajuda a garantir que apenas os firmware confiáveis e os componentes de inicialização sejam carregados.
- As variáveis críticas da NVRAM são protegidas contra corrupção e modificação não autorizada por meio de controles de integridade.

Unidades de armazenamento

Os Fiery DFEs utilizam unidades de armazenamento para o sistema operacional do host, arquivos do sistema, tarefas em spool, registros e arquivos temporários.

Os seguintes recursos de segurança são fornecidos para proteger os dados do cliente:

- Criptografia a nível de unidade.
- Listas de controle de acesso (ACLs) para restringir operações de leitura/gravação não autorizadas.
- Kits de segurança de unidade de disco (opcionais para Fiery DFEs externos) permitem que as unidades sejam bloqueadas com segurança durante a operação.

Portas físicas

Portas físicas, como USB, interfaces de rede e conectores de serviço, são vetores potenciais de acesso não autorizado. A segurança de hardware Fiery lida com esse risco ao:

- Desativar portas não utilizadas por meio de controles de hardware e firmware.
- Restringir o acesso de dispositivos externos por meio de controles administrativos e configuração do sistema.
- Registrar eventos relevantes para a segurança envolvendo interfaces físicas críticas.

Ao integrar essas medidas de segurança de hardware com proteções de software e rede, os Fiery DFEs fornecem uma estratégia abrangente de defesa profunda, garantindo a confidencialidade, a integridade e a disponibilidade de dados confidenciais em ambientes de impressão.

Integridade do sistema e atualizações seguras

Manter a integridade do sistema é fundamental para garantir a segurança. Os Fiery DFEs oferecem suporte aos seguintes itens:

- Registro de auditoria de segurança
- Inicialização segura: garante que apenas softwares confiáveis sejam carregados.
- Atualizações assinadas digitalmente: impede a adulteração de atualizações de software.
- Gerenciamento automatizado de atualizações de segurança: simplifica o processo de aplicação das atualizações de segurança.

Registro de auditoria de segurança

Administradores com privilégios elevados podem acessar e examinar eventos de segurança registrados no Registro de Auditoria de Segurança. Esse registro está ativado por padrão.

Cada evento de segurança é categorizado como Informação, Aviso ou Erro. O administrador não recebe alertas ou notificações; em vez disso, é apresentado a eles um registro estático.

Os registros são formatados para serem compatíveis com as ferramentas de Gerenciamento de eventos e informações de segurança (SIEM), comumente usadas para coleta e análise de registros. Todos os dados de eventos capturados estão em conformidade com os padrões descritos no NIST SP 800-53.

O Administrador Fiery pode acessar o registro de auditoria de segurança sem a necessidade de intervenção da FIERY. Os registros para DFEs baseados em Linux são fornecidos no formato Syslog (RFC 5424 ou RFC 3164). Para DFEs baseados em Windows, os registros são salvos no formato EVTX padrão do Windows e podem ser lidos no Visualizador de Eventos do Windows e em muitas soluções comerciais disponíveis que usam a API do Visualizador de Eventos do Windows. Os DFEs Fiery baseados em Linux oferecem a opção de encaminhar registros para um sistema de coleta centralizado, como o Syslog.

Os registros de segurança são retidos com base na capacidade de armazenamento local, até um limite predefinido. Em Fiery DFEs baseados em Windows, os eventos individuais mais antigos são removidos conforme necessário. Em Fiery DFEs baseados em Linux, os registros de auditoria são substituídos com base no tamanho do arquivo; arquivos de registro substituídos são retidos até a contagem de substituição configurada, após a qual os arquivos substituídos mais antigos são excluídos.

Inicialização segura

A inicialização segura protege o sistema operacional ao permitir que apenas componentes confiáveis e assinados digitalmente sejam carregados. Em DFEs Fiery baseados em Windows e compatíveis, ela impede que códigos não autorizados ou maliciosos sejam executados na inicialização, reduzindo assim o risco de comprometimento. Para que a inicialização segura seja eficaz, ela deve estar habilitada nas configurações do BIOS e estar ativada.

Atualizações assinadas digitalmente

Os Fiery DFEs usam atualizações assinadas digitalmente para garantir a integridade e autenticidade de todas as instalações de software e firmware. Cada atualização é assinada criptograficamente pela Fiery ou por seus parceiros autorizados, permitindo que o DFE verifique se o conteúdo não foi alterado ou adulterado. Esse processo é uma proteção contra a introdução de códigos maliciosos e garante que apenas atualizações confiáveis sejam aplicadas, mantendo a segurança e a confiabilidade do sistema.

Gerenciamento automatizado de atualizações de segurança

Atualizações de software oportunas são essenciais para a operação ideal dos Fiery DFEs. É importante instalar todas as atualizações de segurança para manter os Fiery DFEs seguros em todos os ambientes de impressão.

A **Atualização do Sistema Fiery** baixa e instala atualizações de segurança se a opção estiver ativada no Fiery DFE. Por padrão, essa opção está ativada e recomendamos que os clientes a deixem ativada.

As vulnerabilidades de segurança do sistema operacional Microsoft® Windows™ não são detalhadas neste documento, pois são gerenciadas diretamente pela Microsoft e distribuídas aos clientes através de **atualizações do Windows** conforme ficam disponíveis.

Para resolver questões de segurança e vulnerabilidades que possam afetar os principais componentes do hardware Fiery, incluindo a placa-mãe, o processador e o firmware, a FIERY colabora diretamente com os fabricantes para obter as atualizações de segurança necessárias. Essas atualizações de segurança são posteriormente fornecidas aos clientes, conforme necessário.

Nota: As atualizações de software Fiery são assinadas digitalmente usando o Secure Hash Algorithm (SHA-2) para impedir modificações não autorizadas, incluindo a inserção de malware.

Atualizações de segurança do software Fiery DFE

Atualizações de software regulares são essenciais para a operação ideal dos Fiery DFE. Ao aplicar as atualizações de segurança de software mais recentes do Fiery DFE, a integridade do sistema é garantida, as vulnerabilidades são atenuadas e a conformidade com os padrões de segurança do setor é mantida.

A equipe de segurança do Fiery DFE monitora e rastreia diligentemente as vulnerabilidades de segurança por meio de uma rede abrangente de fontes confiáveis, como:

- Alertas e avisos da Agência de Segurança Cibernética e de Infraestrutura dos EUA (CISA)
- Banco de dados nacional de vulnerabilidades do Instituto Nacional de Padrões e Tecnologia dos EUA (NIST)
- Registros de Vulnerabilidades e Exposições Comuns (CVE)
- Relatórios e avisos do Centro de Coordenação CERT (CERT/CC) sobre vulnerabilidades de software e hardware
- Governo regional e agências reguladoras
- Avisos de segurança de fornecedores de software e hardware

A Fiery prioriza correções de segurança com base na gravidade (Crítica, Alta, Média e Baixa), conforme determinado pelo Sistema de Pontuação Comum de Vulnerabilidade (CVSS). Essas correções são liberadas após a obtenção da aprovação correspondente do parceiro OEM (Fabricante de equipamento original). Quando aprovadas, as atualizações de segurança do software Fiery são disponibilizadas para download. Todas as atualizações de software Fiery são assinadas digitalmente usando o Secure Hash Algorithm (SHA-2) para impedir modificações não autorizadas, incluindo a inserção de malware.

Quando ativada, a Atualização do Sistema Fiery baixa e instala as atualizações de segurança automaticamente no Fiery DFE. Por padrão, essa opção está ativada e é altamente recomendável que os clientes a mantenham assim.

Conformidade e boas práticas

Implementações de segurança robustas estão em conformidade com os padrões fundamentais da indústria e com os quadros regulamentares, incluindo:

- Regulamento Geral de Proteção de Dados, Lei de Dados da UE
- FIPS 140-3
- NIST 800-88. Diretrizes para higienização de mídia (somente FS800 Pro)
- NIST 800-52. Diretrizes para seleção, configuração e uso de implementações TLS (Transport Layer Security)
- Certificação de Modelo de Maturidade de Cibersegurança (CMMC) do Departamento de Segurança Cibernética dos EUA. Nível 2: Ampla proteção de informações controladas não classificadas (CUI) (somente FS800 Pro)
- NIST 800-193. Diretrizes de resiliência de firmware da plataforma (somente FS800 Pro)
- NIST 800-53. Controles de segurança e privacidade para sistemas de informação e organizações
- Perfil de proteção de critérios comuns para sistemas operacionais de uso geral (somente FS800 Pro)

Para reforçar a postura de segurança, os administradores de TI são responsáveis por implementar as seguintes medidas:

- Aplicar atualizações de segurança regularmente
- Impor políticas de autenticação robustas
- Realizar auditorias periódicas de segurança
- Implementar segmentação de rede para ambientes de impressão

Diretrizes para configuração segura do Fiery DFE

Administradores Fiery podem seguir estas diretrizes para reforçar a segurança ao configurar o Fiery DFE:

Alterar a senha do Administrador

Os Fiery DFEs são enviados da fábrica com uma senha padrão para a conta de Administrador. Essa senha concede acesso completo ao Fiery DFE, tanto localmente quanto de um cliente remoto. Esse acesso inclui, mas não está limitado a:

- Sistema de arquivos (somente Fiery DFEs no Windows)
- Configurações de segurança do sistema
- Configurações de aplicativos
- Entradas de registro

Recomendamos fortemente alterar a senha padrão do Administrador Fiery logo após a instalação e em intervalos regulares, de acordo com as políticas de segurança da sua organização. A senha do Administrador Fiery deve ser modificada na plataforma Fiery.

Boas práticas para operar segura e eficientemente

- Restrinja o SNMP à Versão 3 para segurança máxima.
- Desative o WSD para envio de tarefas a fim de impedir seu uso em fluxos de trabalho de impressão.
- Desative os Protocolos de impressão do Windows (LPR, porta 9100, IPP), a menos que sejam explicitamente necessários.
- Ative o Filtro de porta TCP/IP para bloquear portas não utilizadas e reduzir os riscos.
- Feche as portas 137–139 e 445 se não forem necessárias para a impressão no Windows ou para o compartilhamento de arquivos.
- Desative o HTTP na porta 80 para prevenir comunicações não seguras.
- Ative a Impressão segura para que apenas o proprietário da tarefa possa liberar tarefas de impressão.

Ambientes de alta segurança

Administradores com privilégios elevados podem facilmente definir configurações de alta segurança selecionando o perfil de alta segurança disponível em **WebTools > Configure > Segurança**.

Conclusão

Os Fiery DFEs, embora equipados com recursos de segurança robustos, não são destinados a serem conectados à internet. Eles devem ser implantados em ambientes de rede seguros com acesso cuidadosamente controlado pelo administrador de rede. Criados para atender aos mais recentes padrões do setor, os Fiery DFEs fornecem segurança de nível empresarial para proteger os ambientes de impressão contra ameaças cibernéticas em evolução. Os administradores podem garantir a conformidade e proteger dados confidenciais ao aproveitar totalmente os recursos de segurança da Fiery.

Novidades no FS800, FS800 Pro

- Módulos principais do sistema atualizados para resolver vulnerabilidades de segurança.
- As conexões de área de trabalho remota com os Fiery DFEs baseados em Windows 11 são compatíveis com o TLS 1.3, fornecendo criptografia avançada e melhor segurança de conexão.