Fiery FS400 Pro/FS400 servers

Fiery Security White Paper

45211274

30 de junho de 2020

Conteúdo

Visão geral do documento

Este documento fornece detalhes sobre como a tecnologia de segurança e os recursos são implementados dentro do Fiery FS400 Pro/FS400 servers , e abrange segurança de hardware, segurança de rede, controle de acesso, sistemas operacionais e segurança de dados. O objetivo do documento é ajudar nossos clientes a combinar a tecnologia de segurança da plataforma Fiery com suas próprias políticas para atender a seus requisitos de segurança específicos.

Convenções de terminologia

Este documento usa a seguinte terminologia e convenções para se referir ao Fiery FS400 Pro/FS400 servers, à impressora e aos aplicativos Fiery.

Termo ou convenção	**Refere-se a**
Fiery server	Fiery FS400 Pro/FS400 servers
Impressora	Impressora, copiadora, impressora digital, prensa ou dispositivo de saída
Configure	Fiery Configure
Command WorkStation	Fiery Command WorkStation
WebTools	Fiery WebTools

Filosofia de segurança da EFI

A EFI entende que a segurança é uma das principais preocupações para organizações e empresas em todo o mundo. Nossos produtos são frequentemente aprimorados com recursos de segurança avançados destinados a proteger os ativos de empresa. O EFI Fiery servers foi projetado e fabricado com a segurança como um componente essencial para proteger os dados do sistema quando em repouso, em trânsito e durante o processamento.

Trabalhando de perto com nossos parceiros e fornecedores globais da EFI, estamos comprometidos em apoiar continuamente nossos clientes com soluções à medida que as ameaças evoluem. Para obter a segurança geral do sistema, recomendamos que os usuários finais combinem os recursos de segurança do Fiery com as políticas de segurança de suas próprias organizações e as melhores práticas específicas do setor, como senhas seguras e procedimentos de segurança física fortes.

Metas de segurança da EFI

A EFI tem os seguintes objetivos ao implementar medidas de segurança para o Fiery server:

- **Segurança de dados**: não há divulgação não autorizada de dados durante o processamento, transmissão (em trânsito) ou armazenamento (em repouso).
- **Disponibilidade**: desempenho como pretendido, livre de manipulações não autorizadas.
- **Controle de acesso**: sem negação de serviço para usuários autorizados.
- **Manutenção simples de TI**: notificações automáticas e downloads quando houver atualizações de segurança disponíveis.
- **Conformidade**: regulamentos do setor e estruturas de segurança.

Atualizações de segurança do software Fiery

Esta seção descreve o processo de atualizações de segurança do software Fiery server. As vulnerabilidades de segurança do sistema operacional Microsoft® Windows™ não são descritas, pois são tratadas diretamente pela Microsoft e entregues como atualizações do Windows assim que disponíveis. Para problemas de segurança ou vulnerabilidades que podem afetar os principais componentes de hardware do Fiery, por exemplo, placa mãe, processador, BIOS e assim por diante, a EFI trabalha em estreita colaboração com os fabricantes para obter as atualizações de segurança necessárias.

- A EFI monitora o Boletim semanal de segurança cibernética US-CERT da Agência de segurança cibernética e infraestrutura (CISA). O boletim fornece um resumo das novas vulnerabilidades que foram registradas pelo NVD (National Vulnerability Database) do Instituto Nacional de Padrões e Tecnologia (NIST) na semana passada. As vulnerabilidades são baseadas no padrão de nomenclatura de vulnerabilidades e exposições comuns (CVE) e são organizadas de acordo com a gravidade (alta, média e baixa) determinadas pelo sistema de Pontuação comum de vulnerabilidade (CVSS).
- A EFI oferece correções de segurança para cada plataforma Fiery server o mais rápido possível.
- As atualizações de segurança de software do Fiery são entregues a parceiros específicos da EFI para aprovação.
- Quando aprovadas pelos parceiros, as atualizações de segurança do software Fiery são disponibilizadas para download.
- A Atualização do Fiery System baixa e instala as atualizações de segurança se a opção estiver ativada no Fiery server. Por padrão, essa opção está ativada e recomendamos que os clientes a deixem ativada.

Atualizações de software oportunas são essenciais para a operação ideal dos Fiery servers. É importante instalar as atualizações de segurança dos softwares do sistema operacional Fiery e Windows pra manter o Fiery servers seguro em todos os ambientes de impressão.

Configurando os recursos de segurança do Fiery server

O Configure é a principal ferramenta usada para configurar os recursos de segurança do Fiery servers. Os administradores podem acessar o Configure pelo Command WorkStation ou WebTools.

Nota: Os usuários devem ter privilégios de administrador para acessar o Configure.

Para obter informações sobre como configurar o Fiery server, consulte Diretrizes para configuração de servidor Fiery segura na página 28.

Segurança de hardware

A segurança no hardware do Fiery server concentra-se em impedir a perda de dados em caso de falta de energia e acesso não autorizado aos dados localizados em um dispositivo de armazenamento.

Memória volátil

Os dados que são gravados na RAM volátil estão disponíveis somente enquanto a energia estiver ligada. Quando for desligada, todos os dados serão excluídos.

Para obter mais informações, consulte a Seção de memória volátil da tabela na página 24.

Memória não volátil e armazenamento de dados

O Fiery server contém vários tipos de tecnologias de armazenamento de dados não volátil para reter dados no Fiery server quando a energia for desligada. Esses dados incluem informações de programação do sistema e dados do usuário.

Para obter mais informações, consulte a Seção de memória não volátil da tabela na página 24.

Memória flash

A memória flash armazena o autodiagnóstico e o programa de inicialização (BIOS) e alguns dados de configuração do sistema. A memória flash é programada na fábrica e pode ser reprogramada apenas pela instalação de patches especiais criados pela EFI. Se os dados estiverem corrompidos ou forem excluídos, o Fiery server não é iniciado.

CMOS

A memória CMOS, alimentada por bateria, é usada para armazenar as configurações da máquina do Fiery server. Nenhuma dessas informações é considerada confidencial ou privada. Se a memória CMOS estiver instalada, os usuários podem acessar essas configurações em um servidor no Windows 10 IoT Enterprise 2016 ou 2019 por meio de um monitor, teclado e mouse.

NVRAM

Há uma série de pequenos dispositivos NVRAM no Fiery server que contém firmware operacional. Esses dispositivos contêm informações operacionais que não são específicas do cliente. O usuário não tem acesso aos dados contidos neles.

Unidade de disco rígido e unidade de estado sólido

Durante as operações normais de impressão normal e digitalização, bem como durante a criação de informações de gerenciamento de tarefas, os dados da imagem são gravados em uma área aleatória na unidade de disco rígido.

Os dados de imagem e as tarefas nas filas podem ser excluídos manualmente por usuários do Command WorkStation ou de qualquer outra operação de fila (como a operação no LCD da impressora). Os dados e objetos de imagem também podem ser excluídos automaticamente usando o comando **Limpar o servidor** ou quando o número de tarefas impressas exceder os parâmetros permitidos. A desativação da fila de impressos também excluirá as tarefas impressas.

A EFI fornece um recurso de exclusão segura para proteger os dados da imagem contra acesso não autorizado. Quando a exclusão segura é ativada pelo administrador do Fiery, o modo operacional selecionado é executado no momento apropriado para apagar com segurança os dados excluídos na unidade de disco rígido. No momento, o Fiery Secure Erase suporta apenas unidades de disco rígido. Para unidades de estado sólido (SSDs), verifique com o fabricante as opções de limpeza de disco antes de descartar a unidade.

Nota: Para obter mais informações sobre exclusão segura, consulte Exclusão segura na página 22.

Portas físicas

O Fiery server pode ser conectado por meio de portas externas mostradas na seguinte tabela:

Portas Fiery	Função	Acesso	Controle de acesso
Conector Ethernet RJ-45	Conectividade Ethernet	Conexões de rede	Uso do filtro IP do Fiery para controlar o acesso
Conector da interface da impressora	Imprimir e digitalizar	Dedicado a envio/ recebimento de/para a impressora	N/A
Porta USB	Conexão do dispositivo USB Instalação do software do sistema	Conector plug-and-play projetado para uso com dispositivos de mídia removíveis opcionais.	É possível desativar a impressão USB. É possível desativar o acesso a dispositivos de armazenamento USB por meio da Política de grupo do Windows. O armazenamento USB também pode ser desativado no Configure.
Conector de fibra óptica	Conectividade Ethernet de 10 Gb	Conexões de rede	N/A

Interface local

O usuário pode acessar as funções do Fiery no monitor da estação do Fiery NX ou pelo software Fiery QuickTouch na tela sensível ao toque em alguns Fiery servers ou através de qualquer monitor conectado ao Fiery server. O acesso de segurança no Fiery server com a estação do Fiery NX é controlada por uma senha de administrador do Windows. A tela sensível ao toque fornece funções muito limitadas que não impõem qualquer risco à segurança.

Opção de kit de unidade de disco rígido removível

Alguns Fiery servers são compatíveis com um kit opcional de unidade de disco rígido removível para maior segurança. Este kit permite que o usuário bloqueie as unidades do servidor no sistema para operação normal e remova as unidades para um local seguro depois de desligar o Fiery server.

Para servidores Windows independentes

Os Fiery servers independentes baseados no WIndows aceitam um kit de opção de unidade de disco rígido removível. A disponibilidade ou não deste kit opcional para um produto Fiery específico depende dos termos dos contratos da EFI com seus parceiros individuais do Fiery.

Para servidores Fiery XB

As unidades de disco rígido e de estado sólido são removíveis nos servidores Fiery XB. A maioria das unidades disco rígido e de estado sólido são emparelhadas em conjunto na configuração de RAID. É importante colocar as unidades de volta ao seu local original para evitar a perda de dados e uma nova instalação de software de sistema.

Ativar portas USB para uso de armazenamento

Portas USB no Fiery servers permitem conexões de mouse, teclado ou espectrofotômetro, mas impedirá as conexões com dispositivos de armazenamento USB quando a opção Ativar armazenamento USB estiver desativada no Configure. Essa opção é ativada por padrão. Quando desativada, a opção desativa os recursos do Fiery que exigem a funcionalidade de armazenamento em massa USB, como Backup e restaurar.

Segurança da rede

O Fiery server inclui uma variedade de recursos de segurança de rede projetados para controlar e gerenciar o acesso à impressora. Somente usuários e grupos autorizados podem acessar o Fiery server e imprimir na impressora. O Fiery server também pode ser configurado para limitar ou controlar comunicações externas usando endereços IP designados, bem como desativar as portas e os protocolos de rede. O Fiery servers sempre deve ser implantado em um ambiente de rede protegido e a acessibilidade deve ser corretamente configurada e gerenciada por um administrador de rede qualificado e autorizado.

Portas de rede

Por padrão, todas as portas TCP/IP não usadas por serviços específicos do Fiery estão desativadas. O administrador do Fiery pode ativar e desativar seletivamente as portas de rede. Desativar uma porta de rede bloqueia conexões externas usando a porta especificada. Se uma porta específica estiver ativada, conexões externas são permitidas usando essa porta.

TCP	UDP	Nome da porta	Serviços dependentes
20-21		FTP	FTP
80		HTTP	WebTools, IPP
135		MS RPC	Microsoft® RPC Service (somente Windows 10). Uma porta adicional na faixa de 49152-65536 será aberta para fornecer pontos relacionados com SMB e serviços de impressão.
137-139		NETBIOS	Impressão no Windows
	161, 162	SNMP	Fiery Central, alguns utilitários herdados, outras ferramentas baseadas em SNMP
	427	SLP	SLP
443		HTTPS	WebTools, IPP/s
445		SMB/IP	SMB sobre TCP/IP
	500	ISAKMP	IPsec
515		LPD	Impressão LPR, alguns utilitários herdados (como o WebTools, versões mais antigas da Command WorkStation)
631		IPP	IPP

TCP	UDP	Nome da porta	Serviços dependentes
3389		RDP	Área de trabalho remota (apenas Fiery Servers no Windows)
3702	3702	WS-Discovery	WSD
	4500	IPsec NAT	IPsec
	5353	DNS multicast	Bonjour
6310 8010 8021-8022 8090 9906 21030 50006-50025	9906	Portas EFI	Command WorkStation 5 e 6, Fiery Central, Ferramentas baseadas no EFI SDK, funções bidirecionais do Driver de impressora Fiery, WebTools, Fiery Direct Mobile Printing e Conversão de documentos nativos
9100-9103		Porta de impressão	Porta 9100

Nota: As portas 50006-50025 são ativadas após a Command WorkStation versão 6.2 e posterior serem instaladas em um Fiery server independente.

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

O administrador do Fiery pode também ativar e desativar os diferentes serviços de rede fornecidos pelo Fiery server.

Filtro IP

A filtragem de IP permite ou nega solicitações de conexão ao Fiery server de endereços IP definidos. O administrador pode definir políticas padrão para permitir ou negar pacotes de dados recebidos e também pode especificar filtros para um máximo de 16 endereços IP ou intervalos para permitir ou negar solicitações de conexão.

Cada configuração de filtro IP especifica um endereço IP ou um intervalo de endereços IP e a ação correspondente. Se a ação for Negar, os pacotes com um endereço de origem pertencentes aos endereços especificados serão ignorados e, se a ação for Aceitar, os pacotes serão permitidos.

Autenticação de rede

SNMP v3

O Fiery server é compatível com o padrão SNMPv3 mais recente. Os pacotes de comunicação SNMPv3 podem ser criptografados para garantir confidencialidade, integridade da mensagem e autenticação.

O administrador do Fiery pode selecionar entre três níveis de segurança SNMP: Mínimo, Médio ou Máximo. O administrador Fiery tem também a opção de exigir a autenticação antes de permitir operações SNMP e criptografar

nomes de usuário e senhas de SNMP. O administrador local pode definir nomes de comunidade de leitura e gravação SNMP e outras configurações de segurança.

Para obter mais informações, consulte Configurações recomendadas na página 28.

IEEE 802.1x

O 802.1x é um protocolo padrão IEEE para controle de acesso à rede baseado em porta. Esse protocolo fornece um mecanismo de autenticação antes que o Fiery server obtenha acesso à rede local e seus recursos.

Quando ativado, o Fiery server pode ser configurado para usar o EAP MD5-Challenge, PEAP-MSCHAPv2 ou EAP--TLS para autenticar em um servidor de autenticação 802.1x.

O Fiery server busca essa autenticação no momento da inicialização ou quando o cabo Ethernet é desconectado e reconectado.

Criptografia de rede

Segurança de Protocolo IP (IPsec).

O IPsec fornece segurança a todos os aplicativos através de protocolos IP através da criptografia e autenticação de todos os pacotes.

O Fiery server usa a autenticação de chave pré-compartilhada para estabelecer conexões seguras com outros sistemas no IPsec.

Uma vez que a comunicação segura é estabelecida no IPsec entre um computador cliente e o Fiery server, todas as comunicações (incluindo tarefas de impressão) serão transmitidas com segurança pela rede.

HTTPS

O Fiery server requer uma conexão segura entre os clientes e os diferentes componentes do servidor. O HTTPS sobre TLS é usado para criptografar comunicações entre os dois pontos finais. O HTTPS é necessário ao conectar-se ao Fiery server do WebTools e da Fiery API. Essas comunicações são criptografadas com TLS 1.3, 1.2 e 1.1.

Gerenciamento de certificados

O Fiery servers fornece uma interface de certificado para gerenciar os certificados usados durante as comunicações SSL/TLS. O Fiery servers é compatível com o formato de certificado X.509.

O Gerenciamento de certificados permite ao administrador Fiery fazer o seguinte:

- Criar certificados digitais autoassinados.
- Adicionar um certificado e sua chave privada correspondente ao Fiery server.
- Adicionar, navegar, visualizar e remover certificados de uma loja de certificados confiável.

Segurança de e-mail

O Fiery server é compatível com protocolos de comunicação de e-mail POP e SMTP, quando o e-mail é ativado. (O recurso é desativado por padrão.) Para proteger o serviço contra ataques e uso indevido, o administrador do Fiery pode ativar recursos de segurança adicionais, como:

POP antes de SMTP

Alguns servidores de e-mail ainda suportam o protocolo SMTP não seguro, que permite a qualquer pessoa enviar e-mails sem autenticação. Para impedir o acesso não autorizado, alguns servidores de e-mail exigem que os clientes de e-mail autentiquem em POP antes de usar o SMTP para enviar um e-mail. Para esses servidores de e-mail, o administrador Fiery precisaria ativar a autenticação POP antes de SMTP.

OP25B

O bloqueio da porta de saída 25 (OP25B) é uma medida antispam em que provedores podem bloquear pacotes indo até à porta 25 por meio de seus roteadores. A interface de configuração de e-mail permite que o administrador Fiery especifique uma porta diferente.

Para obter mais informações sobre o fluxo de trabalho de e-mail impressão do Fiery server, consulte Impressão de e-mail na página 25.

Bloco de mensagem do servidor (SMB)

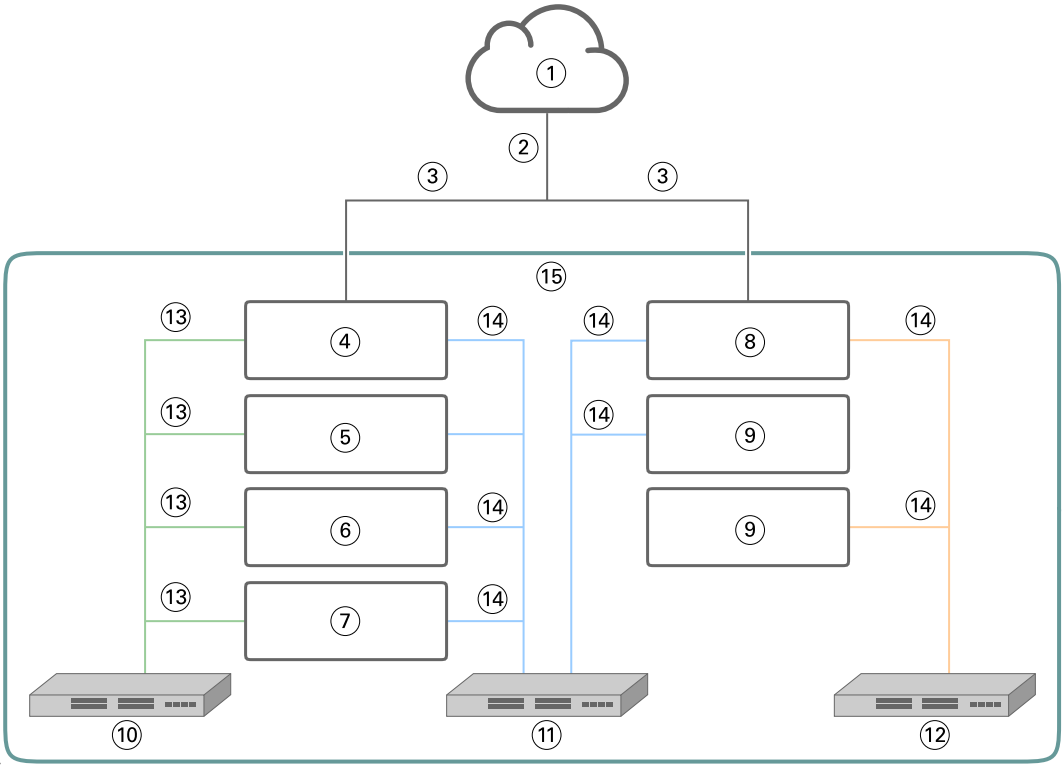
O SMB é um protocolo de rede que fornece acesso compartilhado a arquivos e impressoras. O SMB v1 é desativado no Fiery servers porque não atende aos padrões atuais de segurança do setor. O SMB v2 e v3 são compatíveis.

A assinatura de SMB é executada no Fiery server. A assinatura de SMB requer pacotes assinados digitalmente para permitir que o destinatário verifique a autenticidade do pacote para evitar ataques "Man in the middle". Se a autenticação de SMB estiver ativada, o usuário deverá fornecer o nome de usuário e a senha de SMB para acessar as pastas e o conteúdo armazenados nas pastas SMB.

Nota: A impressão ou o compartilhamento de arquivos pelo SMB pode ser restringido definindo uma senha no Configure.

Diagrama de rede do Fiery XB

A tabela a seguir mostra como os servidores Fiery XB e as impressoras jato de tinta de alta velocidade se conectam à rede.



1	LAN	9	Outras impressoras blade (opcional)
2	Tráfego de rede de gerenciamento de tarefas	10	Rede privada de 10 GbE
3	DHCP de 1 GbE ou estático	11	Rede privada de 1 GbE
4	Blade principal do Fiery	12	Rede privada de 1 GbE PLC
5	Blade RIP opcional (opcional)	13	10 GbE
6	Blade do Fiery nº 1 (opcional)	14	1 GbE
7	Blade do Fiery nº 2 (opcional)	15	Ambiente fechado do Fiery XB
8	Blade da impressora		

Controle de acesso

Este capítulo descreve como o Fiery server pode ser configurado para controlar o acesso aos recursos para grupos de usuários diferentes.

Autenticação do usuário

O recurso de autenticação de usuário permite que o Fiery server faça o seguinte:

- Autenticar um usuário
- Autorizar ações com base em privilégios do usuário

O Fiery server pode autenticar usuários que são:

- Baseados em domínio: usuários definidos em um servidor corporativo e acessados via LDAP
- Baseados no Fiery: usuários definidos no Fiery server

O Fiery server autoriza as ações de um dos usuários com base em sua participação no grupo. Cada grupo é associado a um conjunto de privilégios (por exemplo, impressão em escala de cinza ou impressão em cores), e as ações dos membros do grupo são limitadas a esses privilégios. O administrador Fiery pode modificar os privilégios de qualquer grupo do Fiery com exceção dos usuários Administrador, Operador e Convidado.

Para esta versão da autenticação do usuário, os diferentes privilégios que podem ser selecionados para um grupo são os seguintes:

- **Imprimir em escala de cinza**: este privilégio permite que os membros do grupo imprimam tarefas em escala de cinza no Fiery server . Se o usuário não tiver esse privilégio, o Fiery server não imprimirá a tarefa. Se a tarefa for colorida, ela será impressa em escala de cinza.
- **Imprimir em cores e em escala de cinza**: esse privilégio permite que os membros do grupo imprimam tarefas no Fiery server com acesso total aos recursos de impressão em cores e em escala de cinza do Fiery server. Sem esse privilégio ou a impressão em escala de cinza, a tarefa de impressão não é impressa e os usuários não podem enviar a tarefa via FTP (somente dispositivos coloridos).
- **Caixa de correio do Fiery**: esse privilégio permite que os membros do grupo tenham caixas de correio individuais. O Fiery server 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 definições do servidor**: esse privilégio permite que os membros do grupo criem predefinições do servidor para permitir que outros usuários do Fiery acessem as predefinições de tarefas usadas com frequência.

- **Gerenciar fluxos de trabalho**: esse privilégio permite que os membros do grupo criem, publiquem ou editem impressoras virtuais.
- **Editar tarefas** (somente servidores Fiery XB): esse privilégio permite que os membros do grupo editem uma tarefa na fila.

Nota: A autenticação do usuário substitui os recursos de impressão por membro e impressão em grupo.

Autenticação de usuário do software Fiery

O Fiery server interage com diferentes tipos de usuários. Esses usuários são específicos para o software Fiery e não estão relacionados a usuários ou funções definidos do Windows. É recomendável que os administradores do Fiery exijam senhas para acessar o Fiery server. Além disso, a EFI recomenda que o administrador do Fiery altere a senha padrão para atender aos requisitos de segurança nesse ambiente de impressão.

A seguir, os privilégios permitidos para os diferentes tipos de usuário Fiery são descritos:

- **Administrador**: tem controle total sobre todas as funcionalidades do Fiery server.

  O administrador Fiery pode modificar os privilégios de qualquer grupo do Fiery com exceção dos usuários Administrador, Operador e Convidado.
- **Operador**: tem quase os mesmos privilégios que o administrador, mas não tem acesso a algumas funções do Fiery server, como configuração, e não pode excluir o log de tarefas.
- **Operador de impressora** (somente servidores Fiery XB): pode gerenciar tarefas na impressora. O administrador pode adicionar privilégios específicos a este tipo de usuário.

Sistemas operacionais

A EFI trabalha em estreita colaboração com os fabricantes dos sistemas operacionais usados no Fiery servers para obter as atualizações de segurança necessárias para problemas ou vulnerabilidades de segurança que possam afetar os componentes principais do Fiery server, como a placa-mãe, processador, BIOS e assim por diante. Além disso, as atualizações de software do Fiery são assinadas digitalmente pela EFI para impedir modificações não autorizadas, incluindo a inserção de malware.

Linux (FS400)

Fiery servers FS400 são servidores baseados em Linux projetados com uma arquitetura fechada. A visibilidade limitada da rede impede o acesso não autorizado.

As características do Fiery servers baseado em Linux são as seguintes:

- Os Fiery servers baseados em Linux não incluem uma interface local que permita o acesso ao sistema operacional.
- O SSH e o Telnet não são compatíveis com o Fiery servers baseado em Linux, o que impede o acesso ao shell do sistema operacional.
- O Fiery servers baseado em Linux não permite a instalação de programas não autorizados que possam expor o sistema a vulnerabilidades.
- O sistema operacional Linux usado no Fiery servers FS400 é um sistema operacional personalizado somente para o Fiery servers. Ele tem todos os componentes do sistema operacional necessários para um Fiery server, mas não alguns dos componentes de uso geral para sistemas Linux, como Ubuntu e Fedora.

Acesso ao sistema

O Fiery servers baseado no Linux pode ser configurado no Fiery no painel de controle da impressora ou por meio do Configure no WebTools. O WebTools é um conjunto de páginas baseadas no navegador que permite ao administrador do Fiery acessar o Fiery server para configuração e outras atividades relacionadas à administração do sistema. O WebTools é executado na mais recente estrutura segura da web, suportada pela maioria dos navegadores modernos.

Windows 10 (FS400 Pro)

O Fiery servers FS400 Pro independente usa o Windows 10 IOT Enterprise 2019 LTSC como sistema operacional. Esta edição do Windows contém as mais recentes proteções de segurança e inclui os aprimoramentos de recursos cumulativos fornecidos nas versões 1703, 1709, 1803 e 1809 do Windows 10. Cada compilação LTSC é compatível com a Microsoft com atualizações de segurança por dez anos após o lançamento.

Nota: O Windows 10 IoT Enterprise 2019 LTSC é um equivalente binário ao Windows 10 Enterprise versão 1809. A principal diferença entre essas duas versões é o modelo de licenciamento e distribuição.

O Windows 10 IoT Enterprise 2019 LTSC inclui os seguintes recursos:

- Destinado ao uso em sistemas especializados como Fiery servers.
- Inclui muitas melhorias de segurança para proteção contra ameaças, informações e identidade.
- Fornece inúmeras atualizações de segurança.
- Não inclui aplicativos orientados para o consumidor, como o navegador Edge, Calendário, Clima, Fotos e outros.

Microsoft Windows Update

A Microsoft emite periodicamente patches de segurança por meio do Windows Update para atender às possíveis ameaças e vulnerabilidades de segurança do sistema operacional. A configuração padrão do Windows Update no Fiery servers notifica os usuários de patches sem baixá-los. Selecionar Verificar atualizações no Windows Update no Painel de controle do Windows permite atualizações automáticas e inicia o processo de atualização.

Ferramentas do Windows Update

O Fiery servers baseado no Windows usa métodos padrão da Microsoft para atualizar todos os patches de segurança aplicáveis da Microsoft. O Fiery server não é compatível com nenhuma outra ferramenta de atualização de terceiros para recuperar patches de segurança.

Software antivírus do Windows

O Fiery servers usa o software antivírus da Microsoft e o Windows 10 Defender para proteção. Em geral, o software antivírus pode ser usado com um Fiery server. O software antivírus vem em muitas variedades e pode compactar muitos componentes e recursos para lidar com uma ameaça.

Observe que o software antivírus é mais útil quando instalado, configurado e executado no próprio Fiery server. Para Fiery servers sem uma configuração local, ainda é possível iniciar o software antivírus em um PC remoto e verificar um disco rígido do Fiery server compartilhado. No entanto, a EFI sugere que o administrador Fiery trabalhe diretamente com o fabricante do software antivírus para suporte operacional.

Verificação do mecanismo antivírus

Uma verificação do mecanismo antivírus do Fiery server pode afetar o desempenho do Fiery, mesmo se a verificação tiver sido programada.

Antispyware

Um programa antispyware pode afetar o desempenho do Fiery quando os arquivos estiverem entrando em um Fiery server. Exemplos disso são as tarefas de impressão de entrada, arquivos baixados durante uma atualização do sistema Fiery server ou uma atualização automática de aplicativos executadas em um Fiery server.

Firewall integrado

Como o Fiery server tem um firewall, os firewalls dos antivírus geralmente não são necessários. A EFI recomenda que os clientes trabalhem com seu próprio departamento de TI se houver necessidade de instalar e executar um firewall interno que faça parte do software antivírus. Consulte Portas de rede na página 11 para ver uma lista de portas disponíveis.

Antispam
O Fiery server é compatível com os recursos de impressão por e-mail e digitalização para e-mail. Recomendamos que um mecanismo de filtragem de spam baseado em servidor seja usado. O Fiery servers também pode ser configurado para imprimir documentos a partir de endereços de e-mail especificados. O componente antispam não é necessário porque a execução de um cliente de e-mail separado (como o Outlook) no Fiery server não é uma operação compatível.

HIPS e controle do aplicativo
Devido à natureza complexa do HIPS (Host Intrusion Protection System) e do controle de aplicativos, a configuração do antivírus deve ser testada e cuidadosamente confirmada quando um desses recursos estiver em uso. Quando ajustados adequadamente, o HIPS e o controle de aplicativos são excelentes medidas de segurança e coexistem com o Fiery server. No entanto, é muito fácil causar problemas de Fiery server com as configurações de parâmetro erradas do HIPS e exclusões do arquivo errado, muitas vezes causados por "aceitar os padrões". A solução é revisar as opções selecionadas no HIPS ou nas configurações de controle de aplicativos em conjunto com as configurações do Fiery server, como portas de rede, protocolos de rede, executáveis de aplicativos, arquivos de configuração, arquivos temporários e assim por diante.

Lista de permissões e lista negra
As funcionalidades de lista de permissões e lista negra normalmente não devem ter efeitos adversos sobre o Fiery server. A EFI recomenda enfaticamente que o cliente configure essas funcionalidades para que os módulos do Fiery não fiquem na lista negra.

Vírus de e-mail

Normalmente, os vírus transmitidos por e-mail precisam de algum tipo de execução pelo destinatário. Os arquivos anexados que não são arquivos PDL são descartados pelo Fiery server. O Fiery server também ignora e-mails em formato RTF ou HTML ou qualquer JavaScript incluído. Além de uma resposta de e-mail a um usuário específico com base em um comando recebido, todos os arquivos recebidos por e-mail são tratados como tarefas PDL.

Nota: Para obter mais informações sobre o fluxo de trabalho de e-mail impressão do Fiery server, consulte Impressão de e-mail na página 25.

Segurança de dados

Essa seção descreve os controles de segurança projetados para proteger os dados do usuário residentes no Fiery server e os controles de segurança para dados em trânsito.

Criptografia de informações críticas

A criptografia de informações críticas no Fiery server garante que todas as senhas e informações de configuração relacionadas sejam seguras quando armazenadas no Fiery server. As informações essenciais são criptografadas ou colocadas em hash. Os algoritmos criptográficos usados são AES256, Diffie-Hellman e SHA-2 para atender aos mais recentes padrões de segurança.

As informações do usuário armazenadas no disco não podem ser lidas, mesmo que o disco seja removido do Fiery server. A criptografia de dados do usuário pode ser ativada ou desativada no Fiery servers baseado no Windows usando o Configure. Para Fiery servers baseados no Linux, o recurso está sempre ativado.

Se a senha inserida para recuperar dados for esquecida, não há como redefini-la e a EFI não poderá recuperá-la. O software teria que ser reinstalado.

Nota: Com a criptografia de dados, o disco é particionado e somente a partição de dados do usuário é criptografada. As partições do sistema operacional não podem ser criptografadas.

Padrão de criptografia avançado (AES)

O Fiery server protege os dados em repouso do acesso não autorizado. Ele criptografa tarefas, imagens e dados de cliente usando o algoritmo AES de 256 bits.

O AES é um padrão de criptografia pequeno, rápido e difícil de ser quebrado, adequado para uma grande variedade de dispositivos e aplicativos. Ele oferece nível extra de proteção contra roubo de dados, ao mesmo tempo em que atende a políticas de segurança corporativas.

Impressão padrão

As tarefas enviadas para o Fiery server podem ser enviadas para uma das seguintes filas de impressão publicadas pelo Fiery server:

- Fila de espera
- Fila de impressão
- Fila de impressão sequencial
- Fila direta (conexão direta)
- Impressoras virtuais (filas personalizadas definidas pelo administrador Fiery)

O administrador Fiery pode desativar a fila Impressão e a fila Direta para limitar a impressão automática.

Filas Em espera, Impressão e Impressão sequencial

Quando uma tarefa é impressa na fila Impressão ou na fila Em espera, a tarefa é colocada em spool no disco rígido do Fiery server. As tarefas enviadas para a fila Em espera são mantidas no disco rígido do Fiery até que o usuário envie a tarefa para impressão ou exclua a tarefa usando um utilitário de gerenciamento de tarefas, como a Command WorkStation.

A fila Impressão sequencial permite que o Fiery server mantenha a ordem de tarefas em determinadas tarefas enviadas pela rede. O fluxo de trabalho será "Primeiro a entrar, primeiro a sair", respeitando a ordem na qual as tarefas foram recebidas na rede. Sem a fila Impressão sequencial ativada, as tarefas de impressão enviadas pelo Fiery server podem ficar fora de ordem devido a vários fatores, como o Fiery server permitindo que tarefas menores passem à frente, enquanto as tarefas maiores são colocadas em spool.

Fila de impressos

As tarefas enviadas para a fila de impressão são armazenadas na fila impressos no Fiery server após impressão, caso a fila de impressos esteja ativada. O administrador pode definir o número de tarefas mantidas na fila Impressos. Quando a fila Impressos está desativada, as tarefas são excluídas automaticamente depois de serem impressas.

Fila direta (conexão direta)

A fila direta é projetada para download de fontes e aplicativos que requerem conexão direta com módulo de PostScript em Fiery servers.

A EFI não recomenda a impressão na fila direta. O Fiery server exclui todas as tarefas enviadas por conexão direta após a impressão. No entanto, a EFI não garante que todos os arquivos temporários relacionados com a tarefa sejam excluídos.

As tarefas dos tipos de arquivo VDP (Impressão de dados variáveis), PDF ou TIFF são redirecionados para a fila de impressão quando enviados para a fila direta. As tarefas enviadas pelo serviço de rede SMB podem ser encaminhados para a fila de impressão quando enviados para a fila direta.

Exclusão de tarefa

Uma tarefa não pode ser visualizada ou recuperada quando ela é excluída automaticamente do Fiery server ou apagada usando ferramentas do Fiery. Se a tarefa tiver sido colocada em spool no disco rígido do Fiery server, os elementos da tarefa poderão permanecer no disco rígido e poderão, teoricamente, ser recuperados com determinadas ferramentas, como as ferramentas de análise forense do disco.

Exclusão segura

O recurso Exclusão segura foi projetado para remover o conteúdo de uma tarefa enviada do disco rígido do Fiery server sempre que uma função Fiery excluir uma tarefa. Quando uma tarefa é excluída, cada arquivo de origem do

trabalho é substituído três vezes, usando um algoritmo baseado no método de limpeza de dados do DoD 5220.22-M dos EUA.

Fluxos de trabalho	Exclusão segura
Tarefas armazenadas na unidade de disco rígido do Fiery server; Exclusão segura definida como Ativada	Sim
Tarefas armazenadas na unidade de disco rígido do Fiery server; Exclusão segura definida como Desativada	Não
Tarefas recebidas pelo Fiery server e excluídas após a opção Exclusão segura ser definida como Ativada	Sim
Tarefas recebidas pelo Fiery server e excluídas antes de a opção Exclusão segura ser definida como Ativada	Não
Cópias de tarefas enviadas para outro Fiery server (balanceamento de carga)	Não
Tarefas arquivadas para mídia removível	Não
Tarefas arquivadas em unidades de rede	Não
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 server	Não
Partes de uma tarefa gravada na unidade de disco rígido do Fiery server 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 server foi desligado antes de a exclusão da tarefa ser concluída	Não
Desfragmentar a unidade disco rígido do Fiery server antes de excluir uma tarefa	Não

Nota: O recurso de exclusão segura não é compatível com plataformas Fiery XB.

Memória do sistema

O processamento de alguns arquivos pode gravar alguns dados de tarefas na memória do sistema operacional. Em alguns casos, essa memória pode ser trocada para a unidade de disco rígido e não é substituída especificamente.

Memória volátil			
Tipo (SRAM, DRAM e assim por diante)	**Usuário modificável (Sim ou não)**	**Função ou uso**	**Processar para limpar**
DRAM	Sim	Memória do sistema principal (recebe tarefas enviadas para a fila direta)	Desligar Fiery server
SDRAM (em placa de vídeo)	Sim	Memória de vídeo	Desligar Fiery server

Memória não volátil			
Tipo (SRAM, DRAM e assim por diante)	**Usuário modificável (Sim ou não)**	**Função ou uso**	**Processar para limpar**
BIOS	Não	Funções de BIOS	Retire do soquete e destrua, mas o sistema deixará de funcionar.
EPROM Ethernet	Não	Firmware de chip Ethernet	Dessolde e destrua, mas o sistema deixará de funcionar.
CMOS NVRAM	Não	Armazenamento de configurações do BIOS	Remova a bateria do sistema por 30 segundos.
Unidade de disco rígido (HDD) e unidade de estado sólido (SSD)	Sim	Sistema operacional Aplicativos Fiery (possivelmente com dados do usuário) Software do sistema Fiery Tarefas de impressão, tarefas de digitalização e outros dados do usuário Imagem de backup para o padrão de fábrica	Reinstale o software do sistema. A maioria das tarefas pode ser removida com segurança com o recurso Exclusão segura*. As ferramentas de limpeza de terceiros e parceiros Fiery podem ser usadas para concluir a limpeza de dados nesses dispositivos.

Nota: A memória volátil e a RAM podem conter dados do cliente durante o processamento dos dados do cliente. Nenhum dado cliente é armazenado na memória não volátil, como BIOS, CMOS e NVRAM.

*As unidades de estado sólido não podem ser completamente limpas pelos métodos de substituição de múltiplas passagens do recurso exclusão segura, devido ao desgaste de memória que ocorre. Além disso, as tentativas de fazê-lo também prejudicariam bastante a vida útil operacional da unidade de estado sólido. Este recurso não é compatível com as plataformas do Fiery XB.

Impressão segura

A função de impressão segura exige que o usuário digite uma senha específica da tarefa no Fiery server e na impressora para permitir a impressão da tarefa.

Este recurso requer acesso ao painel de controle da impressora. A intenção do recurso é limitar o acesso a um documento a um usuário que tem a senha do trabalho e pode inseri-la localmente no painel de controle da impressora.

Fluxo de trabalho

O usuário digita uma senha no campo Impressão de segurança no Fiery Driver. Quando essa tarefa é enviada para a fila Em espera ou Impressão do Fiery server , a tarefa fica na fila e espera pela senha.

Nota: As tarefas enviadas com uma senha de impressão segura não podem ser visualizadas no Command WorkStation.

No painel de controle da impressora, o usuário acessa uma janela de impressão segura e insere uma senha. O usuário pode, em seguida, localizar as tarefas enviadas com essa senha e imprimir e excluir as tarefas.

A tarefa segura impressa não é movida para a fila impressa e é excluído automaticamente após a impressão.

Nota: Parte dos dados pode permanecer temporariamente nos arquivos do sistema operacional.

Impressão de e-mail

O Fiery server recebe e imprime tarefas enviadas por e-mail. O administrador pode armazenar uma lista de endereços de e-mail autorizados no Fiery server. Qualquer e-mail recebido de um endereço que não esteja na lista de endereços de e-mail autorizados será excluído. O recurso de impressão por e-mail está desativado por padrão. O administrador pode ativar e desativar o recurso de impressão por e -mail.

Gerenciamento de tarefas

Executar ações nas tarefas enviadas para o Fiery server requer um utilitário de gerenciamento de tarefas do Fiery com acesso de administrador ou operador.

Registro de tarefas

O registro de tarefas está armazenado no Fiery server. Não é possível excluir registros individuais do registro de tarefas. O registro de tarefas contém informações de tarefas de impressão e de digitalização, como o usuário que iniciou a tarefa, o momento em que a tarefa foi executada e as características da tarefa em termos de papel usado, cor e assim por diante. É possível usar o registro de tarefas para inspecionar a atividade da tarefa do Fiery server.

Um usuário com acesso de operador pode visualizar, exportar ou imprimir o registro de tarefas da Command WorkStation. Um usuário com acesso de administrador pode excluir o registro de tarefas da Command WorkStation.

Configuração

A configuração requer uma senha de administrador. O Fiery server pode ser configurado na ferramenta do Configure no WebTools ou Command WorkStation ou no recurso Configuração no painel de controle da impressora.

Digitalização

O Fiery server permite que uma imagem colocada no vidro da impressora seja digitalizada de volta para a estação de trabalho que iniciou a digitalização. Quando uma função de digitalização é iniciada a partir de uma estação de trabalho, a imagem bitmap bruta é enviada diretamente para a estação de trabalho.

O usuário pode digitalizar documentos para o Fiery server para distribuição, armazenamento e recuperação. Todos os documentos digitalizados serão gravados no disco. O administrador pode configurar o Fiery server para excluir tarefas de digitalização automaticamente após um período de tempo predefinido.

Distribuição de tarefas digitalizadas

As tarefas de digitalização podem ser distribuídas por diversos métodos.

E-mail

Um e-mail com um anexo do trabalho digitalizado é enviado para um servidor de e-mail, onde é encaminhado para o destino desejado.

Nota: Se o tamanho do arquivo do trabalho digitalizado for maior que o máximo definido pelo administrador, o trabalho será armazenado na unidade de disco rígido do Fiery server, que pode ser acessada por meio de um URL.

FTP

O arquivo será enviado para um destino de FTP. Um registro da transferência, incluindo o destino, é mantido no log FTP, acessível no comando imprimir páginas do painel de controle da impressora. É possível definir um servidor proxy FTP para enviar a tarefa por meio de um firewall.

Fila de espera do Fiery server

O arquivo é enviado à fila de espera do Fiery server e não é mantido como uma tarefa de digitalização.

Para obter mais informações sobre a fila de espera do Fiery server, consulte Filas Em espera, Impressão e Impressão sequencial na página 22.

Fax da Internet

O arquivo é enviado para um servidor de e-mail, onde é encaminhado para o destino de fax da Internet desejado.

Caixa de correio

O arquivo é armazenado no Fiery server com um número de código da caixa postal. Os usuários precisam digitar o número correto da caixa de correio para acessar a tarefa de digitalização armazenada. Os usuários têm a opção de definir senhas para proteger o conteúdo de suas caixas de correio de digitalização contra acesso não autorizado. A tarefa de digitalização é recuperável por meio de um URL.

Diretrizes para configuração de servidor Fiery segura

As diretrizes a seguir podem ajudar os administradores do Fiery a melhorar a segurança ao configurar o Fiery server.

Alteração da senha do administrador

Recomendamos que você altere a senha padrão do administrador do Fiery na instalação e em intervalos regulares, conforme exigido pelas políticas de segurança da sua organização. A senha padrão do administrador deve ser alterada no Assistente de configuração do Fiery durante a primeira configuração. As senhas do administrador e do operador podem ser alteradas após a primeira configuração no WebTools: Configure > Segurança > Senha de administrador (ou operador, respectivamente). A configuração de senha também está disponível em Contas de usuário.

A senha de administrador dá acesso completo do usuário ao Fiery server no nível local ou de uma estação de trabalho remota. O acesso total inclui, mas não está limitado a:

- Sistema de arquivos
- Política de segurança de sistema
- Entradas de registro
- Senha do administrador, que nega ao usuário anônimo acesso ao Fiery server

Configurações recomendadas

- Escolha o nível de segurança máximo para SNMP na Rede > SNMP:

  A escolha da segurança máxima restringe o suporte ao Fiery server para SNMP v3 somente.

  Se o gerenciador SNMP funcionar apenas com o SNMP v1/ v2c, altere o valor do campo Nome da comunidade de leitura. O Fiery server permite alterar os valores dos campos SNMP Nome da comunidade de leitura e Nome da comunidade de gravação no WebTools (Configure > Rede > SNMP) e painel de controle da impressora (Rede > SNMP).
- Desative o WSD no envio de tarefas.
- Desative a impressão do Windows no envio de tarefas se estiver usando lpr, porta 9100 ou IPP para imprimir.
- Bloqueie portas ativando o filtro de porta TCP/IP em Segurança > TCP/IP filtragem de porta.

  Desmarque as portas 137-139 e 445 se você não estiver usando a impressão do Windows e não precisar acessar ou compartilhar pastas de arquivos.

Além das proteções de nível operacional do sistema, o Fiery server tem os seguintes recursos de segurança adicionais para ajudar a proteger seus dados:

- O Fiery servers vem com impressão segura para garantir que o usuário pegue apenas sua tarefa de impressão.
- O Fiery servers integra-se às principais soluções de contabilidade de tarefas para incluir segurança adicional através da impressão siga-me.

O Fiery servers vem com inúmeros recursos de segurança, mas não são servidores voltados para a Internet. Eles devem ser implantados em um ambiente protegido e as acessibilidades devem ser devidamente configuradas pelo Administrador da rede.

Seleção de um perfil de alta segurança

O Fiery server oferece recomendações de segurança predefinidas com base em diferentes riscos e níveis de ameaça (Padrão, Alta, Atual). Esse recurso é chamado de Perfis de segurança e pode ser acessado nos seguintes locais:

- Assistente do software Fiery
- WebTools > Configure > Segurança

O perfil de segurança alta permite que o Fiery server seja ainda mais seguro e habilita os recursos de segurança mais usados.

Opção	Alto
Filtro de porta TCP/IP	Ativado
Service Location Protocol (SLP)	Desativado
Bonjour	Desativado
Exclusão segura	Ativado
Área de trabalho remota	Desativado
Senha SMB	Ativado
Dispositivos de armazenamento USB	Desativado
Segurança de PostScript	Ativado
Porta 9100	Ativado
LPD	Ativado
Impressão do Windows	Desativado
IPP	Ativado
Web Services for Devices (WSD)	Desativado
Imprimir via e-mail	Desativado
Impressão FTP	Desativado

Opção	Alto
Impressão móvel direta	Desativado

A EFI recomenda usar o perfil de segurança alta para ambientes com requisitos de segurança máximos.

Conclusão

A EFI oferece um conjunto robusto de recursos de segurança padrão e opcionais no Fiery server para fornecer aos nossos clientes soluções de segurança abrangentes e personalizáveis para qualquer ambiente. A EFI tem o compromisso de garantir que o Fiery server esteja efetivamente protegido contra a vulnerabilidade de uso mal-intencionado ou não intencional, de modo que nossos clientes possam operar suas empresas com a máxima eficiência.