Fiery FS600 Pro/FS600 servers

Fiery Security White Paper

45263454

6 de outubro de 2025

Conteúdo

Visão geral do documento

Este documento fornece detalhes sobre como a tecnologia de segurança e os recursos são implementados dentro do Fiery FS600 Pro/FS600 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 FS600 Pro/FS600 servers, à impressora e aos aplicativos Fiery.

Termo ou convenção	**Refere-se a**
Fiery server	Fiery FS600 Pro/FS600 servers
Impressora	Impressora, copiadora, impressora digital, prensa ou dispositivo de saída
Configure	Fiery Configure
Command WorkStation	Fiery Command WorkStation
WebTools	Fiery WebTools
QuickTouch	Software Fiery QuickTouch em execução no painel LCD do servidor Fiery

Filosofia de segurança FIERY

A FIERY 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, a fim de proteger os recursos da empresa. Os Fiery servers são projetados e desenvolvidos com foco na segurança, para que os dados do sistema estejam protegidos quando em repouso, em trânsito e durante o processamento.

Trabalhando de perto com nossos parceiros e fornecedores globais, estamos comprometidos em continuar fornecendo novas soluções a nossos clientes 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 que sigam as práticas recomendadas do setor, como o uso de senhas seguras e procedimentos de segurança física robustos.

Abordagem de segurança da FIERY

Os recursos de segurança FIERY são guiados por cinco princípios:

- **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 de TI intuitiva**: notificações automáticas e downloads de atualizações de segurança.
- **Conformidade**: suporte regulamentos do setor e estruturas de segurança.

Atualizações de segurança do software Fiery

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

- A FIERY 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 FIERY oferece correções de segurança para cada plataforma Fiery server o mais rápido possível.
- As atualizações de segurança do software Fiery são entregues a parceiros FIERY 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.

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.

Configurando os recursos de segurança do Fiery server

A maioria dos recursos de segurança dos Fiery servers pode ser gerenciada usando o Configure. O Configure é encontrado no Fiery WebTools e permite que o administrador Fiery ajuste as configurações de segurança dos Fiery servers. O Configure necessita de direitos de administrador e também pode ser acessado a partir pelo Fiery Command WorkStation.

Para obter informações sobre como configurar o Fiery server, consulte Diretrizes para configuração de servidor Fiery segura na página 33.

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 FIERY. Se os dados estiverem corrompidos ou forem excluídos, o Fiery server não será 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 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 FIERY fornece um recurso de exclusão segura para remover os dados de imagem da unidade de disco rígido. Quando a exclusão segura é ativada pelo administrador Fiery, o modo operacional selecionado é executado no momento apropriado para apagar com segurança os dados 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 23.

Portas físicas

Portas físicas comuns disponíveis na maioria dos servidores Fiery:

Portas Fiery	Função	Acesso	Controle de acesso
Conector Ethernet RJ-45	Conectividade Ethernet	Conexões de rede	O filtro IP Fiery pode ser usado para controlar o acesso
Conector da interface da impressora	Imprimir e digitalizar	Dedicado a envio/recebimento de/para a impressora	N/A
Porta(s) USB	Conexão do dispositivo USB Instalação do software do sistema	Conector plug-and-play projetado para uso com dispositivos de mídia removíveis opcionais.	• A impressão USB pode ser desativada em servidores Fiery baseados no Windows. • 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

Em alguns Fiery servers, o usuário pode acessar as funções do Fiery no monitor da estação Fiery NX, por meio do software Fiery QuickTouch na tela sensível ao toque ou por meio 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.

Trusted Platform Module (TPM)

Os servidores Fiery FS600 Pro baseados no Windows são compatíveis com o Trusted Platform Module (TPM). O TPM é usado para habilitar recursos de segurança pagos e opcionais. Servidores Fiery FS600 Pro usam o TPM para criptografar/descriptografar a unidade de inicialização do servidor Fiery (unidade C:). Ele também é usado para armazenar com segurança a chave de recuperação de criptografia da unidade de inicialização. Os módulos TPM Fiery atendem à especificação TPM 2.0, bem como aos padrões FIPS 140-2 e Critérios comuns. Consulte seu provedor de serviços para obter mais informações sobre kits de atualização de segurança Fiery e disponibilidade para o DFE Fiery.

Kits de segurança de unidade de disco Fiery

Alguns Fiery servers são compatíveis com um kit opcional de segurança de unidade de disco para aumentar a proteção. 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 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

As portas USB dos Fiery servers permitem conexões de mouse, teclado ou espectrofotômetro. As portas USB podem ser desativadas para evitar conexões com dispositivos de armazenamento USB externos, como pendrives. Essa opção está disponível no Configure. Quando desativada, os recursos Fiery que exigem a gravação de dados em uma unidade USB externa não estão disponíveis.

Segurança da rede

O Fiery server inclui uma variedade de recursos de segurança projetados para controlar e gerenciar o acesso à rede. 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 e desativando as portas e os protocolos de rede. Os Fiery servers sempre devem ser implantados 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	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
	161, 162	SNMP	Ferramentas baseadas em SNMP
	427	SLP	Service Location Protocol
443		HTTPS	WebTools, IPP/s
445		SMB/IP	SMB sobre TCP/IP
	500	ISAKMP	IPsec
515		LPD	Impressão LPR
631		IPP	IPP
3389		RDP	Área de trabalho remota (apenas servidores Fiery no Windows)

TCP	UDP	Nome da porta	Serviços dependentes
3702	3702	WS-Discovery	WSD. Descubra as impressoras de rede habilitadas para WSD, que aparecem na seção Rede do Windows Explorer e podem ser instaladas com um clique duplo.
	4500	IPsec NAT traversal	IPsec
	5353	DNS multicast (mDNS)	Bonjour
6310 8010 8021-8022 8090 9906 21030 50006-50025	9906	Portas FIERY	Command WorkStation, Fiery Central, Ferramentas baseadas no SDK Fiery, Fiery Printer Driver, Fiery WebTools, Impressão móvel direta 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.

Nota: As portas IPSec (500 e 4500) só podem ser configuradas para FS600 (servidores Fiery 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 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 33.

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 e 1.2.

Gerenciamento de certificados

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

O Fiery servers é compatível com Certificados RSA com comprimento de chave de 4096, 3072 e 2048 bits.

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 autoridade de certificados confiável.

Nota: Certificados autoassinados não são seguros. Recomendamos fortemente que os usuários usem um certificado de uma Autoridade de Certificados (CA) confiável.

Uma vez obtido um certificado assinado por uma Autoridade de Certificado confiável, você pode carregar o certificado no Fiery server na seção Configurar do WebTools.

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 26.

Bloco de mensagem do servidor (SMB)

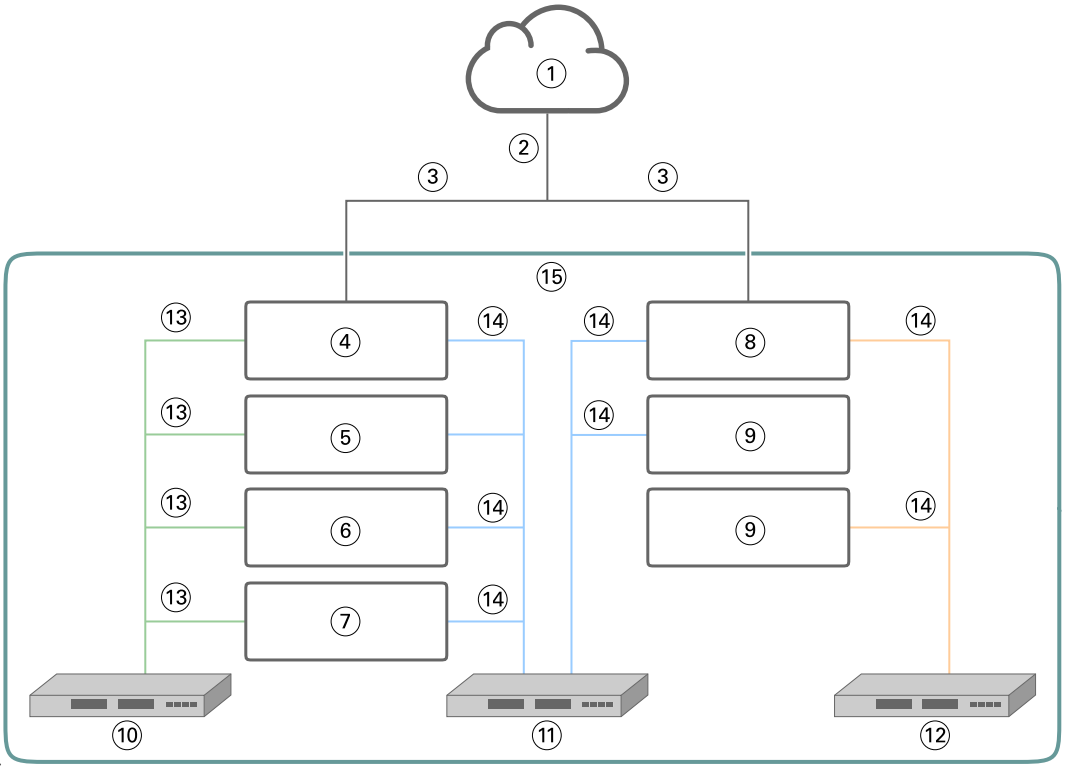
O SMB é um protocolo de rede que fornece acesso compartilhado a arquivos e impressoras. O SMB v1 é desativado no Fiery servers porque não atende aos padrões atuais de segurança do setor. O SMB v2 e v3 são compatíveis.

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 é compatível com três métodos de autenticação de usuário:

1. Autenticação local para usuários definidos no servidor Fiery
2. Autenticação de fator único (SFA) através de servidores de autenticação de rede externos que utilizam o LDAP (por exemplo, Microsoft Active Directory)
3. 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.

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**: permite que os membros do grupo imprimam tarefas em escala de cinza. 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**: permite que os membros do grupo imprimam tarefas 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 não é impressa e os usuários não podem enviá-la via FTP (somente dispositivos coloridos).
- **Caixa de correio do Fiery**: 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 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 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 software do 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 recomendado que administradores Fiery alterem todas as senhas padrão imediatamente após a primeira instalação. O uso de senhas para acessar o servidor Fiery deve ser obrigatório.

- A senha máxima permitida para "Administrador" e "Operador" é de até 15 caracteres ao usar **Configurar** > **Segurança**.
- Para contas de usuário locais, o tamanho máximo de senha permitido é de até 64 caracteres ao usar a opção **Configurar** > **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**: 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 os mesmos privilégios que o administrador, mas não tem acesso a algumas funções do Fiery server, como configuração, e não pode excluir o registro 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.
- **Administrador de serviços Fiery** (Fiery servers apenas no Windows): uma conta de administrador oculta usada para instalar o certificado confiável em servidores Windows. Esta conta não permite que os usuários façam login no Fiery server (local ou remoto). Esta conta pode aparecer em algumas ferramentas de varredura de rede e pode ser removida se necessário. Métodos padrão alternativos podem ser usados para instalar o certificado confiável.
- **Fiery_SMB_User**: esta é a conta de usuário padrão na Impressão do Windows (SMB). Permite que usuários do SMB do Windows "vejam" o servidor Fiery no "Ambiente de rede".
- **Convidado** (padrão; sem senha): tem os mesmos privilégios que o operador, mas não pode acessar o registro de tarefas, nem fazer edições ou alterar o status das tarefas de impressão e de visualização.

Logon único (SSO)

Servidores Fiery FS600 Pro são compatíveis com o protocolo OpenID Connect para autenticação de usuário por logon único na nuvem com o Microsoft Entra ID (Azure Active Directory). Os usuários podem fazer logon no Fiery server usando suas credenciais AAD.

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

O benefício adicional dessa abordagem de gerenciamento de identidade é que os servidores Fiery não armazenam nenhuma senha de usuário localmente, o que ajuda a melhorar a segurança.

Registro de auditoria de segurança do Fiery

Para ajudar as organizações com os requisitos de conformidade, os administradores do Fiery podem coletar e analisar eventos relacionados à segurança, que são salvos no Registro de auditoria de segurança.

O Registro de auditoria de segurança é ativado por padrão.

Cada evento de segurança é classificado como informação, Aviso ou Erro. Não há alertas ou notificações fornecidas ao administrador, somente um registro estático.

Os registros estão em um formato compatível com soluções comuns de coleta e análise de registros SIEM. As informações captadas sobre eventos estão de acordo com a Publicação Especial NIST 800-53, *Recommended Security Controls for Federal Information Systems* (SP800-53).

O administrador Fiery pode ler eventos sem a intervenção da FIERY. Os eventos dos Fiery servers para Windows e Linux estão no formato JSON e podem ser processados por qualquer ferramenta de coleta de registros. Para servidores Fiery em Windows, os eventos podem ser visualizados no Windows Event Manager. Os administradores de registros baseados no Linux Fiery servers podem encaminhar regitros para um sistema central de coleta de registros (SysLog).

Os eventos de segurança são retidos com base na capacidade de armazenamento de disco alocada. Quando o tamanho do registro atinge o limite máximo de armazenamento (400 MB), eventos mais antigos são removidos.

Sistemas operacionais

A FIERY trabalha em estreita colaboração com os fabricantes dos sistemas operacionais usados nos Fiery servers para obter as atualizações de segurança necessárias que possam afetar os componentes principais do Fiery server.

Linux (FS600)

Os servidores FS600 baseados em Linux são sistemas fechados. A visibilidade limitada da rede impede o acesso não autorizado.

Sobre os Fiery servers baseados em Linux:

- Não incluem uma interface local que permita o acesso ao sistema operacional.
- Não são compatíveis com SSH e Telnet, o que impede o acesso ao shell do sistema operacional.
- Não permitem a instalação de programas não autorizados que possam expor o sistema a vulnerabilidades.
- O sistema operacional Linux usado no Fiery servers FS600 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 e aplicativos de usuário final encontrados em sistemas Linux comuns.
- Pode ser definido na Configuração do Fiery no painel de controle da impressora ou através do Configure no Fiery WebTools. O Fiery WebTools é um aplicativo interno baseado em navegador usado pelos administradores Fiery para acessar a configuração do Fiery server e outras atividades de administração do sistema. O Fiery WebTools é executado na mais recente estrutura segura da web, que é compatível com a maioria dos navegadores web modernos.

Windows 10 (FS600 Pro)

Os Fiery servers FS600 Pro são executados no Windows 10 IoT Enterprise 2021 LTSC. Esta versão do Windows contém as mais recentes medidas de segurança e inclui os aprimoramentos de recursos cumulativos fornecidos até a versão 21H2 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 2021 LTSC é um equivalente binário ao Windows 10 Enterprise versão 21H2.

O Windows 10 IoT Enterprise 2021 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 atualizações de segurança por até 10 anos após o lançamento.
- Não inclui aplicativos orientados para o consumidor, como Calendário, Tempo, 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

Os Fiery servers usam o software antivírus Microsoft 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. O administrador Fiery deve trabalhar diretamente com o fabricante do software antivírus para obter 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. Os clientes devem trabalhar 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. Os Fiery servers também podem ser configurados para imprimir documentos a partir de endereços de e-mail específicos.

Sistema de proteção de invasão de host (HIPS) e controle de aplicativos

Devido à natureza complexa do HIPS 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 podem coexistir 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". Revise 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, arquivos executáveis de aplicativos, arquivos de configuração, arquivos temporários e assim por diante.

Lista de permissões e lista de bloqueio
As funcionalidades de lista de permissões e lista de bloqueio normalmente não devem ter efeitos adversos sobre o Fiery server. A FIERY recomenda enfaticamente que os clientes configurem essas funcionalidades para que os módulos do servidor Fiery não sejam bloqueados.

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, bem como 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 26.

Segurança de dados

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

Criptografia de informações críticas

A criptografia de dados importantes de clientes garante que todas as senhas e informações de configuração relacionadas sejam armazenadas com segurança no Fiery server. As informações essenciais são criptografadas ou colocadas em hash. Os algoritmos criptográficos implementados são o AES256, Diffie-Hellman e SHA-2, e estão em conformidade com os mais recentes padrões de segurança.

Dados de clientes armazenados no disco não podem ser lidos, 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 usada para recuperar dados for esquecida, não há como redefini-la e a FIERY não poderá recuperá-la. O software teria que ser reinstalado.

Os servidores do Windows também têm uma opção para criptografar a unidade de inicialização. A unidade de inicialização inclui o sistema operacional e o software do sistema Fiery. A criptografia da unidade de inicialização impede que o servidor Fiery seja inicializado com outro sistema operacional a fim de burlar a aplicação de permissões de arquivos do sistema operacional.

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.

Para ambientes com muitos requisitos de segurança, recomenda-se não imprimir na fila direta. O Fiery server exclui todas as tarefas enviadas por conexão direta após a impressão. No entanto, não há garantia de que todos os arquivos temporários relacionados à 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. Depois que a tarefa é excluída, suas informações não podem ser recuperadas do disco rígido do servidor Fiery.

Quando uma tarefa é excluída em servidores Fiery FS600 baseados no Linux, cada arquivo de origem é substituído três vezes, usando um algoritmo baseado no método de limpeza de dados 5220.22-M do Departamento de Defesa dos EUA.

Os servidores FS600 Pro baseados no Windows são compatíveis com o padrão de higienização de dados NIST 800-88. Os administradores Fiery podem configurar essa opção para métodos de substituição de imagem de 1 ou 3 passagens.

Fluxos de trabalho	Exclusão segura
Tarefas armazenadas na unidade de disco rígido do Fiery server; Exclusão segura definida como **Ativada**	Sim

Fluxos de trabalho	Exclusão segura
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 ou com dados de usuário armazenados em SSDs.

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

Memória volátil			
Tipo (SRAM, DRAM e assim por diante)	**Usuário modificável (Sim ou não)**	**Função ou uso**	**Processar para limpar**
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*. Ferramentas de limpeza de disco de terceiros ou de fabricantes de equipamento original (OEM) também podem ser usadas para remover completamente os dados desses 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.

*Usar métodos de substituição de várias passagens para tarefas armazenadas em SSDs não é recomendado devido ao desgaste de memória. Todas as SSDs têm um número limitado de ciclos de gravação, portanto, sobrescrevê-las múltiplas vezes diminui bastante a vida útil da unidade. Os servidores Fiery armazenam dados de tarefas em unidades de disco rígido.

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 de impressão segura

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.

Usuários remotos podem ver o registro de tarefas no locatário do Portal do IQ da empresa se o servidor Fiery estiver conectado ao FIERY IQ.

Configuração

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

Comunicação da Fiery com os serviços em nuvem

Alguns serviços Fiery internos e aplicativos Fiery exigem a comunicação com serviços externos baseados em nuvem; por exemplo, para baixar atualizações de segurança ou ativar licenças.

As informações fornecidas abaixo são destinadas à equipe de TI ou de administração da rede e podem ser usadas para configurar o Fiery server por trás de firewalls corporativos.

#	Serviço/aplicativo Fiery	URLs remotos	Porta	Uso
1	System Update	https://liveupdate.fiery.com	443	Fazer o download de patches Fiery
2	OFA	https://flexlicensing.fiery.com	443	Para a ativação de licenças
3	IQ	https://iq.fiery.com	443	Comunicação com o Fiery IQ
4	LINQ	https://ews.fiery.com	443	Dados analíticos
5	Impressão Universal da Microsoft	https://portal.azure.com https://print.print.microsoft.com https://notification.print.microsoft.com https://discovery.print.microsoft.com https://graph.print.microsoft.com	443	Comunicação com a Impressão Universal da Microsoft
6	Logon único (SSO)	https://login.microsoft.com	443	Logon único (SSO)

#	Serviço/aplicativo Fiery	URLs remotos	Porta	Uso
7	Atualização do Windows	https://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://*.dl.delivery.mp.microsoft.com https://*.dl.delivery.mp.microsoft.com	80 443	Atualizações do Windows
8	Command WorkStation	https://help.fiery.com https://learning.fiery.com https://communities.fiery.com/s/ https://liveupdate.fiery.com https://iq.fiery.com	443	Acessar serviços e recursos Fiery
9	Fiery Driver	https://help.fiery.com	443	Acessar recursos de ajuda on-line da Fiery
10	Fiery Updater	https://liveupdate.fiery.com	443	Verificar atualizações do Fiery na Command WorkStation

#	Serviço/aplicativo Fiery	URLs remotos	Porta	Uso
11	Fiery Software Manager	https://liveupdate.fiery.com https://www.fiery.com https://solutions.fiery.com/estore/downloads https://assistance.fiery.com/ffc/whatsnew/ https://assistance.fiery.com/ffc/overview/ https://assistance.fiery.com/cws_cs/whatsnew/ https://assistance.fiery.com/cws/CRNs/ https://assistance.fiery.com/frs/CRNs/ https://assistance.fiery.com/jobflow/overview/ https://assistance.fiery.com/cps/whyupgrade/ https://assistance.fiery.com/cps/renewsmsa/ https://assistance.fiery.com/cps/spectros/ https://assistance.fiery.com/cps/CRNs/ https://assistance.fiery.com/cps/getthelatest/	443	Procurar atualizações de software
12	Fiery Software Manager	https://diumxs9ckzarso.cloudfront.net	443	Fazer download de aplicativos Fiery
13	Fiery JobFlow	https://help.fiery.com/ https://assistance.fiery.com/jobflow/productsupport/ https://solutions.fiery.com/jobflow-cookbook	443	Acessar serviços e recursos Fiery
14	Fiery Color Profiler Suite	https://help.fiery.com/cps/ https://communities.fiery.com/s/ https://www.fiery.com/products/color-imaging/fiery-color-profiler-suite/#resources https://activation.fiery.com/fulfillment/cps/?lang=pt https://flexlicensing.fiery.com	443	

Conformidade com regulamentos e estruturas

A tabela abaixo fornece regulamentos e estruturas de conformidade para servidores Fiery que executam o software de sistema FS600 Pro/FS600.

Regulamentos/estruturas	Escopo	Série NX (FS600 Pro)	Série A/E (FS600)
FIPS 140-2	• EUA, Canadá • Requisitos de segurança para módulos criptográficos	Em conformidade Windows 10 2021 LTSC	Não está em conformidade
Referência CIS	• Configuração de linhas de base e melhores práticas para configurar um sistema com segurança	Em conformidade Referência do Microsoft Windows 10 Enterprise (Versão 21H2)	N/D*
Guia de implementação técnica de segurança (STIG)	Padrão de configuração de segurança para hardwares e softwares usados por agências do Departamento de Defesa dos EUA (DOD).	Em conformidade Windows 10 STIG versão 2, R4	N/D*
Critérios comuns	• Critérios de avaliação de técnicas de segurança da informação para segurança de TI	Em conformidade	Não está em conformidade
Proteger matriz de avaliação de segurança do computador (SCSEM)	• Governo dos EUA (Federal e Estadual) • Diretrizes de segurança da informação fiscal para agências federais, estaduais e locais	Em conformidade Os requisitos de resistência e detecção precisam do kit de segurança de unidade de disco Fiery opcional	Não está em conformidade
DoD 522.22-M	Padrão de higienização de dados.	N/A	Em conformidade 3 passagens
NIST 800-88	Padrão de higienização de dados.	Em conformidade 1 ou 3 passagens	Não está em conformidade

*Fora do escopo da regulamentação ou da estrutura. Os servidores baseados em Linux séries A e E são sistemas fechados sem acesso direto ao sistema de arquivos. A visibilidade limitada da rede impede o acesso não autorizado.

Conformidade com o FIPS 140-2

Quando configurados corretamente, os servidores Fiery que executam o FS600 Pro no Windows 10 2021 LTSC atendem às diretrizes de criptografia de dados FIPS 140-2. Um servidor Fiery no *Modo FIPS 140-2*, usa apenas algoritmos criptográficos validados e certificados sob o Programa de Validação de Algoritmos Criptográficos (CAVP) do Governo Federal dos EUA para criptografar dados em repouso e em trânsito.

Habilitar o *Modo FIPS 140-2* no Fiery exige o uso de serviços de fortalecimento profissionais e certificados pela Fiery.

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 configuração pela primeira vez em WebTools : **Configurar** > **Segurança** > **Senha do Administrador** (ou Operador, respectivamente). A configuração de senha também está disponível em **Configurar** > **Contas de usuário** > **Lista de contatos Fiery**.

A senha de administrador fornece acesso completo 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 em **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 do SNMP **Nome d 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**.

  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. Desativar comunicações de porta 80 (HTTP) não seguras.

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 definições de acessibilidade 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	Desativado
LPD	Ativado
Impressão do Windows	Desativado
IPP	Ativado
Web Services for Devices (WSD)	Desativado
Imprimir via e-mail	Desativado
Impressão FTP	Desativado
Impressão móvel direta	Desativado

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

Conclusão

A FIERY oferece um conjunto robusto de recursos de segurança padrão e opcionais para servidores Fiery. Esses recursos de segurança abrangentes e personalizáveis são adequados para todos os tamanhos de empresa, incluindo clientes com requisitos de segurança rigorosos. A FIERY tem o compromisso de fornecer recursos de segurança avançados para proteger os dados do cliente e servidores Fiery contra vulnerabilidades e uso malicioso ou não intencional, tudo sem impactar a eficiência.

Informações de direitos autorais