Documento técnico de segurança da Fiery

Fiery FS200 Pro/FS200 Servers

Data de emissão: Maio de 2018

Série de documentos técnicos

Documento técnico de segurança da Fiery

Índice

1 Visão geral do documento ... 3
1.1 Filosofia de segurança da EFI ... 3
1.2 Configurar o recurso de segurança por meio do Fiery Configure ... 3

2 Segurança física e de hardware ... 4
2.1 Memória volátil ... 4
2.2 Memória não volátil e armazenamento de dados ... 4
2.2.1 Memória Flash ... 4
2.2.2 CMOS ... 4
2.2.3 NVRAM ... 4
2.2.4 Unidade de disco rígido ... 4
2.2.5 Portas físicas ... 4
2.3 Interface local ... 4
2.4 Kit de disco rígido removível opcional ... 5
2.4.1 Para servidores externos ... 5
2.4.2 Para servidores incorporados ... 5

3 Segurança de rede ... 6
3.1 Portas de rede ... 6
3.2 Filtro IP ... 6
3.3 Criptografia de rede ... 6
3.3.1 IPsec ... 6
3.3.2 SSL e TLS ... 6
3.3.3 Gerenciamento de certificados ... 7
3.4 IEEE 802.1X ... 7
3.5 SNMP V3 ... 7
3.6 Segurança de e-mail ... 7
3.6.1 POP antes de SMTP ... 7
3.6.2 OP25B ... 7

4 Controle de acesso ... 8
4.1 Autenticação de usuário ... 8
4.2 Autenticação do software Fiery ... 8

5 Ambiente do sistema operacional ... 9
5.1 Procedimentos de inicialização ... 9
5.2 Linux ... 9
5.2.1 Software antivírus Linux ... 9
5.3 Windows 8.1 Pro ... 9
5.3.1 Patches de segurança da Microsoft ... 9
5.3.2 Ferramentas SMS ... 9
5.3.3 Software antivírus Windows ... 9
5.4 Vírus de e-mail ... 10

6 Segurança de dados ... 11
6.1 Criptografia de informações críticas ... 11
6.2 Impressão padrão ... 11
6.2.1 Filas Em espera, Impressão e Impressão sequencial ... 11
6.2.2 Fila Impressos ... 11
6.2.3 Fila Direta (Conexão direta) ... 11
6.2.4 Exclusão de tarefa ... 11
6.2.5 Exclusão segura ... 11
6.2.6 Memória do sistema ... 12
6.3 Impressão de segurança ... 12
6.3.1 Fluxo de trabalho ... 12
6.4 Impressão por e-mail ... 12
6.5 Gerenciamento de tarefas ... 12
6.6 Registro de tarefas ... 13
6.7 Configuração ... 13
6.8 Digitalização ... 13

7 Conclusão ... 14

Copyright © 2018 Electronics for Imaging, Inc. Todos os direitos reservados.
Esta publicação está protegida por direitos autorais e todos os direitos são reservados. Nenhuma parte dela pode ser copiada, reproduzida, distribuída, divulgada ou transmitida de qualquer forma ou por qualquer meio para qualquer finalidade sem o consentimento prévio por escrito da Electronics For Imaging. As informações contidas neste documento estão sujeitas a alterações sem aviso prévio e não representam um compromisso por parte da Electronics For Imaging. A Electronics For Imaging, Inc. não assume nenhuma responsabilidade por quaisquer erros ou imprecisões, não faz qualquer tipo de garantia (expressa, implícita ou estatutária) no que diz respeito a esta publicação, e renuncia expressamente a todas e quaisquer garantias de comercialização, adequação para fins particulares e não violação de direitos de terceiros. O software descrito nesta publicação é fornecido sob licença e só pode ser utilizado ou copiado de acordo com os termos dessa licença.

1 Visão geral do documento

Este documento dá aos usuários finais uma visão geral dos aspectos funcionais e da arquitetura do Fiery Server®, conforme eles se relacionam com a segurança do dispositivo nos FS200/FS200 Pro Servers. Ele abrange o hardware, a segurança de rede, o controle de acesso, o sistema operacional e a segurança de dados.

A intenção do documento é ajudar os usuários finais a compreenderem todos os recursos de segurança do Fiery Server de que possam se beneficiar e a compreenderem suas possíveis vulnerabilidades.

1.1 Filosofia de segurança da EFI

A EFI™ entende que a segurança é uma das principais preocupações para as empresas em todo o mundo hoje, por isso construímos fortes recursos de segurança para os Fiery Servers, a fim de proteger os ativos mais valiosos das empresas. Também trabalhamos proativamente com parceiros OEM globais e equipes multifuncionais para determinar os requisitos de segurança atuais e futuros das empresas para que a segurança não se torne um problema com nossos produtos.

Como sempre, recomendamos que os usuários finais combinem recursos de segurança do Fiery com outras precauções, como senha segura e procedimentos de segurança física fortes, para obter segurança geral para o sistema.

1.2 Configurar o recurso de segurança por meio do Fiery Configure

Os usuários do Fiery que acessam a segurança do Fiery Server por meio da Fiery Command WorkStation® usando o login do administrador podem configurar todos os recursos do Fiery por meio do Fiery Configure. É possível iniciar o Fiery Configure a partir da Fiery Command WorkStation ou do WebTools™, na guia Configurar.

2 Segurança física e de hardware

2.1 Memória volátil

O Fiery Server usa RAM volátil para a memória local da CPU e para o sistema operacional, o software do sistema Fiery e a memória de trabalho dos dados da imagem. Os dados que são gravados na RAM são mantidos enquanto o aparelho estiver ligado. Quando for desligado, todos os dados serão excluídos.

2.2 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.

2.2.1 Memória Flash

A memória flash armazena o autodiagnóstico e o programa de inicialização (BIOS) e alguns dados de configuração do sistema. Esse dispositivo é programado na fábrica e pode ser reprogramado apenas por instalação de patches especiais criados pela EFI. Se os dados estiverem corrompidos ou forem excluídos, o sistema não inicializará.

Uma parte da memória flash também é utilizada para gravar o uso de dongle para ativar as opções de software do Fiery.

Nenhum dado de usuário é armazenado nesse dispositivo, e o usuário não tem acesso a dados nele.

2.2.2 CMOS

A memória CMOS alimentada por bateria é usada para armazenar as configurações da máquina do servidor. Nenhuma dessas informações é considerada confidencial ou privada. Os usuários podem acessar essas configurações em um Windows 8.1 Pro Server por meio da Fiery Integrated Workstation (kit FACI, incluindo monitor local, teclado e mouse), se estiver instalado.

2.2.3 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.

2.2.4 Unidade de disco rígido

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 (HDD).

Os dados da imagem e as informações de gerenciamento de tarefas podem ser excluídos por um operador ou no final de um período de tempo predefinido, tornando os dados da imagem inacessíveis.

Para proteger os dados da imagem do acesso não autorizado, a EFI fornece um recurso de Exclusão segura (consulte a seção 6.2.5). Uma vez ativada pelo administrador do sistema, a operação selecionada é realizada no momento apropriado para apagar com segurança os dados excluídos do disco rígido.

2.2.5 Portas físicas

É possível conectar o Fiery Server por meio das seguintes portas externas:

Portas Fiery	Função	Acesso	Controle de acesso
Conector Ethernet RJ-45	Conectividade Ethernet	Conexões de rede (consulte impressão e conexões de rede a seguir)	Use o filtro IP do Fiery para controlar o acesso
Conector da interface da copiadora	Imprimir/ Digitalizar	Dedicado a envio/ recebimento de/para o mecanismo de impressão	N/D
Porta USB	Conexão do dispositivo USB	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.

2.3 Interface local

O usuário pode acessar as funções do Fiery no kit FACI (se habilitado em um Windows 8.1 Pro Server) ou no LCD do Fiery nos Fiery Servers. O acesso de segurança no Fiery Server com kit FACI é controlado por meio de uma senha de administrador do Windows, se o kit FACI estiver habilitado. O LCD do Fiery fornece funções muito limitadas que não impõem qualquer risco à segurança.

2.4 Kit de disco rígido removível opcional

O Fiery Server dá suporte a um kit opcional de unidade de disco rígido removível para maior segurança. Esse kit permite ao usuário bloquear as unidades do servidor no sistema para a operação normal e remover as unidades para um local seguro depois de desligar o servidor.

2.4.1 Para servidores externos

Os Fiery Servers dão suporte a um kit opcional de unida de de disco rígido removível. A disponibilidade desse kit opcional para um produto específico Fiery depende dos termos de acordos de desenvolvimento e distribuição da EFI com os seus parceiros OEM individuais.

2.4.2 Para servidores incorporados

Os produtos incorporados podem apenas oferecer disco rígido removível como uma opção coordenada OEM, porque o local de montagem e os suportes para a impressora multifuncional (MFP) devem ser desenvolvidos em conjunto com o OEM. O kit opcional é para tirar o disco rígido interno do chassi incorporado e montar um gabinete externo e alimentado separadamente.

3 Segurança de rede

Os recursos padrão de segurança de rede no Fiery Server incluem a capacidade de permitir que somente usuários autorizados e grupos acessem e imprimam no dispositivo de saída, limitando a comunicação do dispositivo aos endereços IP designados e controlando a disponibilidade de protocolos de rede individuais e portas, como desejado.

Mesmo que os Fiery Servers venham com vários recursos de segurança, não se tratam de servidores voltados para a Internet. Eles devem ser implantados em um ambiente protegido e sua acessibilidade deve ser devidamente configurada pelo administrador da rede.

3.1 Portas de rede

O Fiery Server permite que o administrador de rede ative e desative as portas IP a seguir de forma seletiva. Como resultado, a comunicação não desejada do dispositivo e o acesso ao sistema por meio de protocolos específicos de transporte podem ser bloqueados.

TCP	UDP	Nome da porta	Serviços dependentes
20–21		FTP	
80		HTTP	WebTools, IPP
135		MS RPC	Microsoft® RPC Service (Windows 8.1 Pro apenas). Uma porta adicional na faixa de 49152-65536 será aberta para fornecer pontos relacionados com SMB e serviços de impressão.
137–139		NETBIOS	Impressão do Windows
	161, 162	SNMP	WebTools, Fiery Central, alguns utilitários herdados, outras ferramentas baseadas em SNMP
	427	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 do CWS)
631		IPP	IPP
3050			Firebird
	4500	IPsec NAT	IPsec
	5353	DNS multicast	Bonjour
3389		RDP	Remote Desktop (Windows Fiery servers only)
3702	3702	WS-Discovery	WSD
6310 8010 8021–8022 8090 9906 18021 18022 18081 18082 21030 22000 50006–50025*	9906	Portas EFI	Command WorkStation 4 e 5, Fiery Central, ferramentas baseadas em SDK da EFI, funções bidirecionais do driver de impressora Fiery, WebTools, Fiery Direct Mobile Printing e a conversão de documentos originais.
9100–9103		Porta de impressão	Porta 9100

Outras portas TCP, exceto as especificadas pelo OEM, 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.

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

3.2 Filtro IP

O administrador pode restringir conexões autorizadas com o Fiery Server a partir desses hosts cujos endereços IP estejam dentro de uma faixa IP específica. Os comandos ou as tarefas enviados de endereços IP não autorizados são ignorados pelo Fiery Server.

3.3 Criptografia de rede

3.3.1 IPsec

A segurança IPsec ou de Internet Protocol fornece segurança para todos os aplicativos nos protocolos IP por meio de criptografia e autenticação de cada pacote.

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.

* Essas portas são habilitadas após a instalação da Fiery Command WorkStation versão 6.2 ou posterior em um servidor Fiery externo.

3.3.2 SSL e TLS

Os SSL/TLS são protocolos de nível de aplicativo usados para a transmissão de mensagens pela Internet com segurança. Os Fiery Servers oferecem suporte para protocolos SSL v3 e TLS v1.0/v1.1/v1.2.

Vários recursos do Fiery Server oferecem suporte para SSL/TLS. Os usuários podem acessar a página inicial do Fiery Server e as APIs da Web de forma segura por meio do SSL/TLS. É possível configurar a conexão com servidores LDAP e servidores de e-mail para funcionar em SSL/TLS para garantir uma comunicação segura.

3.3.3 Gerenciamento de certificados

Os Fiery Servers fornecem uma interface de Gerenciamento de certificados para gerenciar os certificados usados em várias comunicações SSL/TLS. Ele suporta 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.

3.4 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 dispositivo obtenha acesso à rede local e seus recursos.

Quando ativado, é possível configurar o Fiery Server para usar o EAP MD5-Challenge ou PEAP-MSCHAPv2 para autenticar um servidor de autenticação 802.1x.

O Fiery Server autentica no momento da inicialização ou quando o cabo Ethernet é desconectado e reconectado.

3.5 SNMP v3

O Fiery Server suporta SNMPv3, pois é um protocolo de rede segura para o gerenciamento de dispositivos em redes IP. É possível criptografar os pacotes de comunicação SNMPv3 para garantir confidencialidade. Ele garante também a integridade das mensagens e a autenticação.

O administrador Fiery pode escolher entre três níveis de segurança em SNMPv3. 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.

3.6 Segurança de e-mail

O Fiery Server suporta os protocolos POP e SMTP. Para proteger o serviço contra ataques e uso indevido, o administrador Fiery pode ativar recursos de segurança adicionais, como:

3.6.1 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.

3.6.2 OP25B

O bloqueio da porta 25 de saída (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.

4 Controle de acesso

4.1 Autenticação de usuário

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

- Autentique nomes de usuários.
- Autorize ações com base em privilégios do usuário.

O Fiery Server pode autenticar os usuários que são:

- Baseados em domínio: usuários definidos em um servidor corporativo e acessados via LDAP.
- Baseados em 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, Imprimir em P&B, Imprimir colorido ou em P&B), e as ações dos membros do grupo são limitadas a esses privilégios.

Grupos Fiery são grupos de usuários com um conjunto predefinido de privilégios. O Grupo Fiery atribui um conjunto de privilégios a um conjunto de usuários.

O administrador Fiery pode modificar os privilégios de qualquer Grupo Fiery com exceção dos usuários Administrador, Operador e Convidado.

Para essa versão de autenticação do usuário, os diferentes níveis de privilégios que podem ser editados ou selecionados para um grupo são os seguintes:

- Imprimir em P&B: esse privilégio permite que os membros do grupo imprimam tarefas no Fiery Server. Se o usuário não tiver o privilégio "Imprimir colorido e em P&B", o Fiery Server forçará a tarefa a imprimir em preto e branco (P&B).
- Imprimir colorido e em P&B: esse privilégio permite que os membros do grupo imprimam tarefas no Fiery Server com pleno acesso aos recursos de impressão em cores e em tons de cinza dos Fiery Servers. Sem esse privilégio ou o privilégio Imprimir em P&B, a tarefa de impressão não é impressa e os usuários não podem enviar a tarefa via FTP (dispositivos de cor apenas).
- 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 nome do usuário/senha da caixa de correio.
- Calibragem: esse privilégio permite que os membros do grupo executem a calibragem de cores.
- Criar predefinições do servidor: esse privilégio permite que os membros do grupo criem predefinições do servidor, a fim de permitir que outros usuários Fiery acessem as predefinições de tarefa geralmente usadas.
- Gerenciar fluxos de trabalho: esse privilégio permite que os membros do grupo criem, publiquem ou editem Impressoras virtuais.

Nota: a autenticação do usuário substitui os recursos Impressão de membro/Impressão de grupos.

4.2 Autenticação do software Fiery

O Fiery Server define os usuários Administrador, Operador e Convidado com diferentes privilégios. Esses usuários são específicos para o software Fiery e não estão relacionados a usuários ou funções definidos do Windows. Recomenda-se que os administradores exijam senhas para acessar o Fiery Server. Além disso, a EFI recomenda que o administrador altere a senha padrão para uma senha diferente, conforme definido pelos requisitos de segurança do usuário final.

Os três níveis de senhas no Fiery Server permitem acessar os seguintes privilégios:

- Administrador: obtém o controle total sobre todas as funcionalidades do Fiery Server.
- Operador: tem a maioria dos mesmos privilégios do administrador, mas não tem acesso a algumas funções do servidor, como configurações, e não pode excluir o registro de tarefa.
- Convidado (padrão; sem senha): tem a maioria dos mesmos privilégios que o operador, mas não pode acessar o registro de tarefa, não pode fazer edições e não pode fazer alterações de status das tarefas de impressão e de visualização.

5 Ambiente do sistema operacional

5.1 Procedimentos de inicialização

O sistema operacional e o software do sistema Fiery são carregados do disco rígido local durante a inicialização.

O residente BIOS na placa-mãe Fiery é somente leitura e armazena as informações necessárias para inicializar o sistema operacional. As alterações na BIOS (ou a remoção da BIOS) impedirão que o Fiery Server funcione corretamente.

A página de configuração lista os valores especificados durante a instalação. Algumas informações, como informações de proxy FTP, de senha e nomes de comunidade SNMP, não estão incluídas na página de configuração.

5.2 Linux

Os sistemas Linux não incluem uma interface local que permita o acesso ao sistema operacional.

5.2.1 Software antivírus Linux

O sistema operacional Linux usado em Fiery Servers é um sistema operacional dedicado somente a 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 o Ubuntu. Além de ter um melhor desempenho, esse sistema operacional dedicado não está sujeito à mesma vulnerabilidade do vírus como um sistema Linux de uso geral e sistema operacional Microsoft. O software antivírus projetado para um sistema operacional Linux de uso geral pode não conseguir operar em Fiery Servers.

5.3 Windows 8.1 Pro

O Fiery Server é fornecido com uma senha de administrador padrão do Windows 8.1. Recomenda-se que o administrador altere a senha após a instalação. Também é altamente recomendável alterar a senha regularmente de acordo com a política de TI da organização. A senha de administrador dá acesso completo do usuário ao Fiery Server no nível local e/ou de uma estação de trabalho remota.
Isso inclui, sem limitação, o sistema de arquivos, a política de segurança do sistema e entradas de registro. Além disso, esse usuário pode alterar a senha de administrador, negando acesso a qualquer outra pessoa ao Fiery Server.

5.3.1 Patches de segurança da Microsoft.

A Microsoft publica regularmente atualizações de segurança para lidar com possíveis falhas de segurança no sistema operacional Windows 8.1. A configuração padrão de atualizações do Windows é para notificar os usuários de patches sem baixá-los. O administrador Fiery pode alterar a configuração padrão no Windows Update ou instalar manualmente os patches de segurança.

5.3.2 Ferramentas SMS

A EFI tem sua própria ferramenta de atualização de sistema dedicada aos seus sistemas baseados em Windows. Essa ferramenta lida com a recuperação de todos os patches de segurança da Microsoft aplicáveise atualizações de software do Fiery. O Fiery Server não suporta todas as ferramentas SMS de terceiros para recuperar e impulsionar as atualizações para o Fiery Server.

5.3.3 Software antivírus Linux

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 específica.
Aqui estão algumas orientações para ajudar os clientes a confiar no software antivírus que escolherem. Observe que o software antivírus é mais útil em uma configuração de kit FACI local, em que os usuários têm o potencial para infectar o Fiery Server com um vírus por meio de ações padrão do Windows. Para os Fiery Servers sem um kit FACI, ainda é possível lançar um software antivírus em um PC remoto e digitalizar 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. A seguir, estão as diretrizes EFI para cada um dos componentes do software antivírus Windows:

Mecanismo de vírus: quando um mecanismo antivírus verifica o Fiery Server, independentemente de se tratar de uma verificação agendada ou não, ele pode afetar o desempenho do Fiery.

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 ou uma atualização automática de aplicativos executadas em um Fiery Server.

Firewall embutido: uma vez que o Fiery Server tem um firewall, os firewalls antivírus geralmente não são necessários. A EFI recomenda que os clientes trabalhem com seu próprio departamento de TI e consultem a seção 3.1 deste documento, se existir a necessidade de instalar e executar um firewall embutido, fornecido como parte do software antivírus.

Antispam: o Fiery suporta recursos Impressão via e-mail e Digitalizar para e-mail. Recomendamos que um mecanismo de filtragem de spam baseado em servidor seja utilizado. Também é possível configurar os Fiery Servers para imprimirem 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 suportada.

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 que o cliente configure essa funcionalidade de modo que não barre os módulos Fiery.

Controle de aplicativo e HID: por causa da natureza complexa de controle de aplicativos e HID, a configuração de antivírus deve ser testada e cuidadosamente confirmada quando qualquer um desses recursos estiver em uso. Quando ajustados corretamente, o controle de aplicativos e o HID são excelentes medidas de segurança e coexistem com o Fiery Server. No entanto, é muito fácil causar problemas de servidor com as configurações de parâmetro erradas do HID e exclusões do arquivo errado, muitas vezes causados por "aceitar os padrões". A solução é rever as opções selecionadas nas configurações de controle de aplicativos e/ou HID em conjunto com as configurações do Fiery Server, como portas de rede, protocolos de rede, executáveisde aplicativos, arquivos de configuração, arquivos temporários e assim por diante.

5.4 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. Consulte os detalhes sobre o fluxo de trabalho de impressão de e-mail do Fiery na Seção 6.4 deste documento.

6 Segurança de dados

6.1 Criptografia de informações críticas

A criptografia de informações críticas no Fiery Server garante que todas as senhas e informações de configuração relacionadas fiquem seguras quando armazenadas no Fiery Server. São usados algoritmos de criptografia compatíveis com o NIST 2010.

6.2 Impressão padrão

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

- Fila Em espera
- Fila Impressão
- Fila Impressão sequencial
- Conexão direta da fila 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. Com senhas ativadas no Fiery Server, esse recurso limita a impressão para operadores e administradores do Fiery.

6.2.1 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 Fiery Command WorkStation, Fiery Command WorkStation ME ou Limpar servidor.

A fila Impressão sequencial permite que o Fiery 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 podem ficar fora de ordem devido a vários fatores, como o Fiery permitindo que tarefas menores passem à frente, enquanto as tarefas maiores são colocadas em spool.

6.2.2 Fila Impressos

As tarefas enviadas para a fila Impressão são armazenadas na fila Impressos no Fiery Server, se habilitado. 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.

6.2.3 Fila Direta (Conexão direta)

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

A EFI não recomenda a impressão na fila Direta. O Fiery 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 de tipos de arquivos VDP, PDF ou TIFF são reencaminhadas para a fila Impressão quando enviadas para a fila Direta. As tarefas enviadas pelo serviço de rede SMB podem ser encaminhadas para a fila Impressão, quando enviadas para a fila Direta.

6.2.4 Exclusão de tarefa

Quando uma tarefa é excluída do Fiery automaticamente ou usando ferramentas Fiery, não será possível visualizar ou recuperar a tarefa usando as ferramentas do Fiery. Se a tarefa tiver sido colocada em spool no disco rígido Fiery, 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.

6.2.5 Exclusão segura

O recurso Exclusão segura foi projetado para remover o conteúdo de uma tarefa enviada do disco rígido do Fiery sempre que uma função Fiery excluir uma tarefa. No caso de exclusão, cada arquivo de origem de tarefa é substituído três vezes usando um algoritmo com base na especificação DoD5220.22M do Departamento de Defesa dos EUA.

As seguintes limitações e restrições se aplicam à exclusão segura:

- Não é aplicável a arquivos de tarefas localizados em sistemas que não sejam o Fiery Server, como os seguintes:
  – Cópias da carga de tarefa equilibrada para outro Fiery Server.
  – Cópias da tarefa arquivada nas unidades de rede ou de mídia.
  – Cópias da tarefa localizada em estações de trabalho cliente.
  – Páginas de uma tarefa mescladas ou copiadas inteiramente em outra tarefa.
- Não exclui nenhuma entrada do registro de tarefa.
- Se o sistema for desligado manualmente antes da conclusão de uma exclusão de tarefa, não haverá nenhuma garantia de que a tarefa seja totalmente excluída.
- Não exclui todos os dados da tarefa que podem ter sido gravados no disco devido à troca de disco e armazenamento em cache de disco.
- As tarefas enviadas por um servidor FTP podem ser salvas pelo cliente FTP antes de serem passadas para o software do sistema Fiery. Como o software do sistema Fiery não tem controle sobre esse processo, o sistema não pode excluir com segurança as tarefas salvas pelo cliente FTP.
- As tarefas impressas por SMB passam pelo spooler no Fiery, que salva as tarefas no disco. Como o software do sistema Fiery não tem controle sobre esse processo, o sistema não pode excluir com segurança essas tarefas.

Nota: a troca de disco ocorre para criar mais memória virtual do que há memória física. Esse processo é tratado na camada do sistema operacional e o Fiery Server não tem controle sobre ele. No entanto, o espaço de troca de disco é regularmente regravado durante a operação do sistema operacional, pois vários segmentos da memória são movidos entre a memória e o disco. Esse processo pode fazer com que alguns segmentos de tarefa sejam armazenados no disco temporariamente.

6.2.6 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 armazenada em cache no disco rígido e não é especificamente substituída.

6.3 Impressão de segurança

A função Impressão de segurança requer que o usuário insira uma senha específica da tarefa no Fiery Server para permitir que a tarefa seja impressa. Esse recurso requer um local de interface LCD para o Fiery Server.

O objetivo do recurso é limitar o acesso a um documento a um usuário que (a) tenha a senha para a tarefa e (b) possa entrar localmente no Fiery Server.

6.3.1 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 são visíveis na Fiery Command WorkStation ou na Fiery Command WorkStation ME.

No LCD do Fiery, o usuário entra em uma janela Impressão segura e digita uma senha. O usuário pode, em seguida, acessar as tarefas enviadas com essa senha e imprimir e/ou excluir as tarefas.

A tarefa segura impressa não é movida para a fila Impressos. A tarefa é excluída automaticamente, assim que a impressão for concluída.

6.4 Impressão por 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 de e-mail que não esteja na lista de endereços de e-mail autorizados será excluído. O administrador pode desativar o recurso de impressão por e-mail. O recurso de impressão por e-mail está desativado por padrão.

6.5 Gerenciamento de tarefas

As tarefas enviadas ao Fiery Server só poderão ser usadas por meio de um utilitário de gerenciamento de tarefas Fiery com acesso de administrador ou operador. Os usuários convidados (usuários sem senha) podem ver os nomes de arquivos e os atributos da tarefa, mas não podem usar nem visualizar essas tarefas.

6.6 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 Fiery Command WorkStation. Um usuário com acesso de administrador pode excluir o registro de tarefas da Fiery Command WorkStation. Um usuário com acesso de convidado poderá imprimir o registro de tarefas do LCD do Fiery somente se esse acesso for concedido pelo administrador.

6.7 Configuração

A configuração requer uma senha de administrador. É possível configurar o Fiery Server a partir da ferramenta Fiery Configure ou da Configuração no LCD do Fiery. É possível iniciar a ferramenta Fiery Configure a partir do Fiery WebTools e da Fiery Command WorkStation.

6.8 Digitalização

O Fiery Server permite que uma imagem colocada no vidro da copiadora seja digitalizada de volta para a estação de trabalho que iniciou a digitalização usando um plug-in Fiery TWAIN. O plug-in é compatível com os aplicativos Adobe® Photoshop e Textbridge. 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.

É possível distribuir as tarefas de digitalização pelos seguintes métodos:

- E-mail: nesse processo, um e-mail é enviado para um servidor de correio, onde é encaminhado para o destino desejado. Nota: se o tamanho do arquivo for maior do que o máximo definido pelo administrador, a tarefa será armazenada no disco rígido do Fiery, que é acessível por meio de uma URL.
- FTP: o arquivo será enviado para um destino de FTP. Um registro da transferência, incluindo o destino, é mantido no registro de FTP, que é acessível a partir do menu Imprimir páginas do LCD. É possível definir um servidor proxy FTP para enviar a tarefa por meio de um firewall.
- Fila Em espera do Fiery: o arquivo será enviado para a fila Em espera do Fiery (consulte a seção 6.2.1 acima) e não será mantido como uma tarefa de digitalização.
- Fax da Internet: o arquivo será enviado para um servidor de correio de onde é encaminhado para o destino desejado de fax da Internet.
- Caixa de correio: o arquivo será armazenado no Fiery Server com um número de código de caixa de correio. O usuário precisa digitar o número da caixa de correio correto para acessar a tarefa de digitalização armazenada. Algumas versões do Fiery Server também requerem uma senha. A tarefa de digitalização é recuperável por meio de uma URL.

7 Conclusão

A EFI oferece um conjunto robusto de recursos e opções padrão no Fiery Server para ajudar os clientes a atenderem a necessidade de uma solução de segurança abrangente e personalizável para qualquer ambiente. A EFI está empenhada em garantir que os negócios dos clientes sejam realizados com a máxima eficiência e em proteger efetivamente o Fiery Server contra vulnerabilidades do uso mal-intencionado ou não intencional. Portanto, a EFI está continuamente desenvolvendo novas tecnologias para fornecer soluções de segurança abrangentes e confiáveis para o Fiery Server.

Nothing herein should be construed as a warranty in addition to the express warranty statement provided with EFI products and services.

The APPS logo, AutoCal, Auto-Count, Balance, BESTColor, BioVu, BioWare, ColorPASS, Colorproof, ColorWise, Command WorkStation, CopyNet, Cretachrom, Cretaprint, the Cretaprint logo, Cretaprinter, Cretaroller, Digital StoreFront, DocBuilder, DocBuilder Pro, DockNet, DocStream, DSFdesign Studio, Dynamic Wedge, EDOX, EFI, the EFI logo, Electronics For Imaging, Entrac, EPCount, EPPhoto, EPRegister, EPStatus, Estimate, ExpressPay, FabriVU, Fast-4, Fiery, the Fiery logo, Fiery Driven, the Fiery Driven logo, Fiery JobFlow, Fiery JobMaster, Fiery Link, Fiery Navigator, Fiery Prints, the Fiery Prints logo, Fiery Spark, FreeForm, Hagen, Inktensity, Inkware, LapNet, Logic, Metrix, MicroPress, MiniNet, Monarch, OneFlow, Pace, Pecas, Pecas Vision, PhotoXposure, PressVu, Printcafe, PrinterSite, PrintFlow, PrintMe, the PrintMe logo, PrintSmith, PrintSmith Site, PrintStream, Print to Win, Prograph, PSI, PSI Flexo, Radius, Remoteproof, RIPChips, RIP-While-Print, Screenproof, SendMe, Sincrolor, Splash, Spot-On, TrackNet, UltraPress, UltraTex, UltraVu, UV Series 50, VisualCal, VUTEk, the VUTEk logo, and WebTools are trademarks of Electronics For Imaging, Inc. and/or its wholly owned subsidiaries in the U.S. and/or certain other countries.

All other terms and product names may be trademarks or registered trademarks of their respective owners, and are hereby acknowledged.

© 2018 ELECTRONICS FOR IMAGING, INC. ALL RIGHTS RESERVED. | WWW.EFI.COM

TL035.07.18_BP