VERSÃO 8.0.0
AGOSTO DE 2024
702P09306

Xerox® FreeFlow® Core

Guia de Segurança

BR40387

Índice

Visão geral

Este capítulo contém:

Objetivo

O objetivo deste Guia de Segurança é divulgar informações de segurança do produto relacionadas ao Xerox® FreeFlow® Core. Nesse contexto, a segurança do Produto é definida conforme o modo como os dados são armazenados e transmitidos, como o produto se comporta em um ambiente de rede e como acessar o produto localmente e remotamente. Este documento descreve o design, as funções e os recursos do Xerox® FreeFlow® Core relativos à Garantia da Informação (GI) e à proteção de informações sensíveis ao cliente.

Este documento não fornece informações de nível de tutorial sobre a segurança e conectividade de recursos e funções do Xerox® FreeFlow® Core. Para obter mais informações sobre esses recursos e funções, consulte a *Ajuda do Xerox® FreeFlow® Core*. Presume-se que o usuário tenha conhecimento do funcionamento desses tópicos.

Os clientes são responsáveis pela segurança de suas redes e do produto FreeFlow. O produto FreeFlow não impõe segurança a nenhum ambiente de rede.

Público-alvo

O público-alvo para este documento são clientes que exigem mais informações relacionadas à segurança sobre o software Xerox® FreeFlow® Core.

Termo de responsabilidade

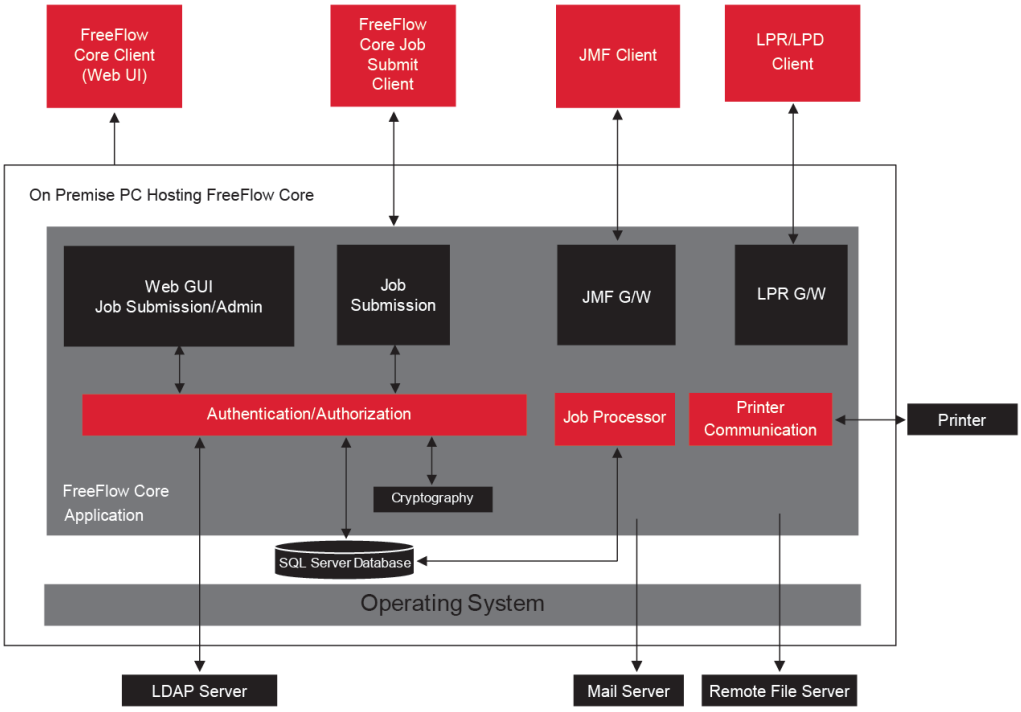
As informações contidas neste documento são corretas e precisas na data de publicação e são oferecidas sem garantias. Em nenhuma circunstância, a Xerox® Corporation será responsabilizada por danos resultantes de uso ou inobservância das informações fornecidas neste documento, incluindo danos diretos, indiretos, incidentais, consequenciais, de lucros cessantes e especiais, mesmo que a Xerox® Corporation tenha sido informada da possibilidade de tais danos.

Descrição do produto

Este capítulo contém:

O Xerox® FreeFlow® Core é a mais nova geração de soluções de fluxo de trabalho da Xerox. O FreeFlow Core é uma solução com base em navegador que automatiza e integra o processamento de trabalhos de impressão de maneira inteligente, desde a preparação do arquivo até a produção final. O FreeFlow Core proporciona um fluxo de trabalho sem uso das mãos, que opera com facilidade, se adapta sem esforço, é rapidamente dimensionável e produz resultados consistentes.

Estrutura de software do sistema



Aspectos de segurança dos recursos selecionados

Este capítulo contém:

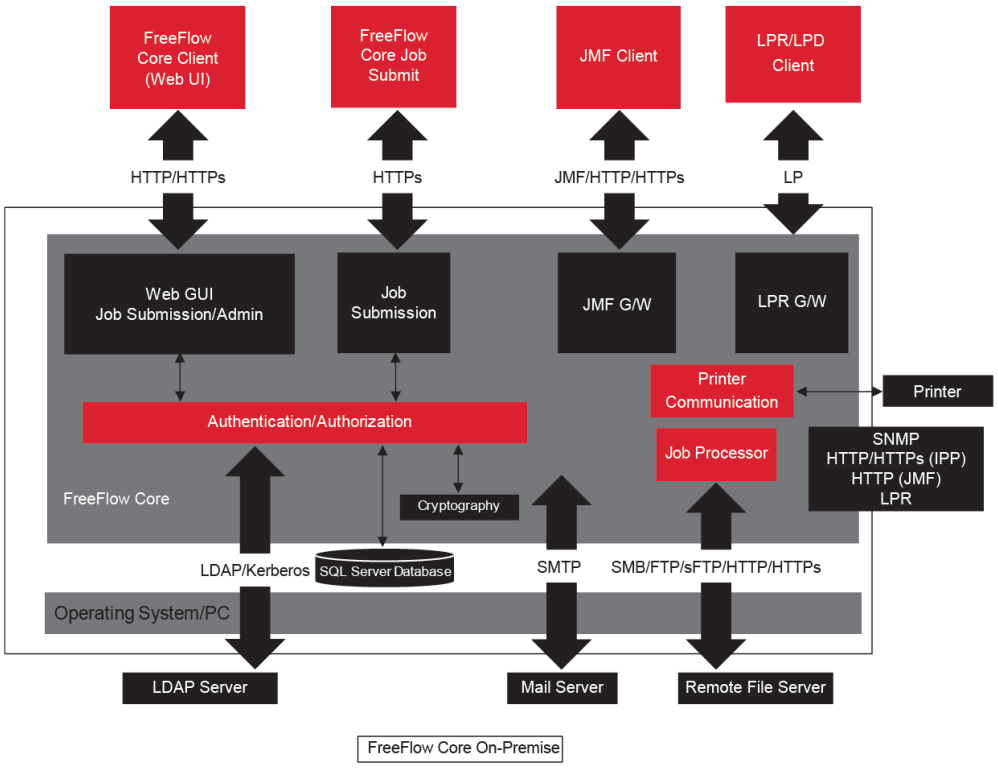
Acesso ao sistema

CONEXÕES DE REDE

O Xerox® FreeFlow® Core requer conectividade de rede para o processamento de trabalhos e as interações do usuário. Consulte as informações de segurança para cada conexão de rede.

Nota: Para oferecer a melhor proteção de segurança contra ataques a vulnerabilidades, ative o firewall do Windows no servidor onde o FreeFlow Core está instalado.

O FreeFlow Core utiliza as seguintes conexões de protocolo de rede.



Cliente Xerox® FreeFlow® Core

Um navegador da Web é compatível com HTML5 e CSS3 é necessário para conectar o FreeFlow Core. As conexões HTTPS são necessárias para fornecer um download seguro do cliente Xerox® FreeFlow® Core e a comunicação segura entre o cliente e o Xerox® FreeFlow® Core.

- Para ativar as conexões HTTPS, adicione um Certificado de servidor ao Internet Information Services (IIS). Siga as instruções na documentação do Windows.
- Se as conexões HTTPS estiverem ativadas, será necessário definir a configuração Requer SSL no Microsoft Internet Information Service (IIS). No prompt de comando do Windows, execute o arquivo em lote RequireSSL, o qual pode ser encontrado no diretório denominado Suporte, dentro do diretório de instalação do FreeFlow Core ou em `C:\Program Files\Xerox\FreeFlow Core`.
- O FreeFlow Core suporta os protocolos criptográficos TLS.

Nota: O FreeFlow Core usa as configurações do sistema operacional que suportam o protocolo TLS. Para assegurar que as versões atuais dos protocolos criptográficos sejam usadas, recomenda-se que o sistema operacional execute as atualizações mais recentes.

- Não há troca de dados do cliente entre o cliente e o servidor Xerox® FreeFlow® Core, a menos que os usuários baixem arquivos de trabalho.

Nota: O cliente recupera as propriedades do trabalho que contêm os dados do cliente.

Tabela 3.1 Configuração do firewall

PORTA	PROTOCOLO OU APLICATIVO	TIPO DE CONEXÃO FIREWALL
80	HTTP	Entrada Nota: O número da porta depende da configuração do servidor IIS.
443	HTTPS	Entrada Nota: O número da porta depende da configuração do servidor IIS.

Funções de usuário

O Xerox® FreeFlow® Core abre em uma tela de login.

- Os usuários fazem login para acessar o sistema FreeFlow Core.
- Após 30 minutos de inatividade, os usuários conectados são desconectados automaticamente.
- Se a autenticação falhar com o software FreeFlow Core, os usuários não serão bloqueados do aplicativo após três tentativas de login.

Nota: Para obter as configurações de contas de usuário adicionais, consulte Acesso de conta de usuário e Retenção do trabalho. O Administrador do FreeFlow Core define as configurações.

Para atribuir usuários às funções de usuário, consulte a *Ajuda do Xerox® FreeFlow® Core*, *Configuração de acesso do usuário*.

Função de Administrador

Os administradores têm acesso a todo o sistema:

- Funções da guia Gerenciamento e status do trabalho: guias da caixa de diálogo Enviar trabalho e Status do trabalho
- Guias de Gerenciamento e Status da impressora
- Configuração do fluxo de trabalho
- Funções da guia Administração:
  - Pasta ativa
  - Notificações
  - Acesso do usuário
  - Região
  - Segurança
  - Relatórios do Core
  - Core Exchange
  - Opções de fila
  - Licença do Core
- Utilitários do Servidor Core disponíveis na área de trabalho do servidor:
  - FreeFlow® Core Exchange
  - FreeFlow® Core Configure
  - FreeFlow® Core Reports para utilitário da linha de comando

Nota: Apenas um administrador de cada vez pode estar conectado ao Xerox® FreeFlow® Core.

Função de Operador

Os operadores têm acesso a:

- Funções da guia Gerenciamento e status do trabalho: guias da caixa de diálogo Enviar trabalho e Status do trabalho
- Guias de Gerenciamento e Status da impressora

Nota: Vários operadores podem estar conectados simultaneamente ao Xerox® FreeFlow® Core.

Função de Monitor de status do trabalho

A função de Monitor de Status de Trabalho oferece acesso somente leitura à janela da guia Status do trabalho.

Nota: Vários usuários que tenham a função de Monitor de Status do Trabalho atribuída podem estar conectados simultaneamente ao Xerox® FreeFlow® Core.

Autenticação do usuário

As credenciais inseridas para o cliente do navegador do Xerox® FreeFlow® Core não são criptografados usando HTTP. Para transmissão segura, ative HTTPS e Requer SSL no IIS para acesso seguro do navegador da Web ao Xerox® FreeFlow® Core.

- Se autenticar usuários com o Xerox® FreeFlow® Core, as informações do usuário não serão criptografadas. As credenciais são armazenadas localmente e criptografadas.
- Se a autenticação de usuários for efetuada com o Active Directory, as credenciais serão descriptografadas antes de serem enviadas ao Active Directory. Quando a autenticação for efetuada com o Active Directory, as credenciais não serão armazenadas localmente.
- É possível configurar a autenticação do Xerox® FreeFlow® Core para usar um Windows Active Directory existente. Essa configuração usa as credenciais da área de trabalho do usuário atual como as credenciais de login para o cliente Xerox® FreeFlow® Core.

A conexão da configuração do Xerox® FreeFlow® Core com o Active Directory é criptografada para a configuração do sistema operacional.

Tabela 3.2 Configuração do firewall

PORTA	PROTOCOLO OU APLICATIVO	TIPO DE CONEXÃO FIREWALL
80	HTTP	Entrada Nota: O número da porta depende da configuração do servidor IIS.
88	Kerberos	Saída: Autenticação do usuário Nota: Os números de portas e serviços dependem da configuração do AD do servidor.
389636 3268 3269	LDAPLDAP TLS LDAP GC LDAP GC TLS	Saída: valida Grupos do AD durante a configuração de autenticação do AD Nota: Os números de portas e serviços dependem da configuração do AD do servidor.

Conexão do SQL Server

O Xerox® FreeFlow® Core se comunica com o SQL Server usando o Microsoft® Entity Framework. A comunicação criptografada entre o Xerox® FreeFlow® Core e o SQL Server é ativada quando o SQL Server é configurado para usar conexões criptografadas.

As credenciais criptografadas do SQL Server são armazenadas localmente no servidor do Xerox® FreeFlow® Core.

Para instalar o software em um SQL Server remoto sem os privilégios de administração SQLS, crie dois bancos de dados vazios na instância SQLS:

- `OapMasterDatabase`
- `OapPlatformDatabase`

PORTA	PROTOCOLO OU APLICATIVO	TIPO DE CONEXÃO FIREWALL
1433	SQLS	Entrada: recebe conexões do Xerox® FreeFlow® Core Saída: comunica-se com o mecanismo de impressão do banco de dados do SQL Server Nota: O número da porta depende da configuração do servidor SQLS.
1434	Serviço de navegador do SQLS	Entrada: recebe conexões do Xerox® FreeFlow® Core Saída: comunica-se com o mecanismo de impressão do banco de dados do SQL Server Nota: O servidor fornece ao cliente o número da porta para conexão.

Interface com o usuário Enviar trabalho

A interface com o usuário (IU) Enviar trabalho usa a conexão de cliente do Xerox® FreeFlow® Core para o envio de trabalhos. Para obter mais informações, consulte Cliente Xerox® FreeFlow® Core.

Tabela 3.3 Configuração do firewall

PORTA	PROTOCOLO OU APLICATIVO	TIPO DE CONEXÃO FIREWALL
80	HTTP	Entrada Nota: O número da porta depende da configuração do servidor IIS.
443	HTTPS	Entrada Nota: O número da porta depende da configuração do servidor IIS.

Pastas ativas

Use compartilhamentos de arquivos para compartilhar uma pasta ativa local e para acessar uma pasta ativa nas pastas compartilhadas do Windows. Para criptografar pastas do Windows, use o sistema de arquivos do Windows. Para proteger as pastas do Windows, use o controle de acesso de conta de usuário do Windows.

Nota: Quando usar o controle de acesso de conta de usuário, use a mesma conta de serviço usada na configuração em *Procedimentos de instalação opcionais*. Para obter mais informações, consulte o *Guia de Instalação do Xero® FreeFlow® Core*.

Tabela 3.4 Configuração do firewall

PORTA	PROTOCOLO OU APLICATIVO	TIPO DE CONEXÃO FIREWALL
139, 445	SMB	Entrada: Compartilha pastas ativas usando o compartilhamento de arquivos do Windows Saída: Utiliza as pastas ativas em diretórios compartilhados
20, 21	FTP	Entrada: compartilha as pastas ativas usando FTP

Processamento do manifesto

Durante o envio do manifesto, o Xerox® FreeFlow® Core recupera os arquivos listados no manifesto. É possível fazer referência aos arquivos usando unidades mapeadas, caminhos de arquivos UNC, HTTP, HTTPS, FTP ou sFTP URIs.

Nota: HTTP e FTP URIs não são compatíveis com a criptografia.

Use compartilhamentos de arquivos para compartilhar uma pasta ativa local e para acessar uma pasta ativa nas pastas compartilhadas do Windows. Para criptografar pastas do Windows, use o sistema de arquivos do Windows. Para proteger as pastas do Windows, use o controle de acesso de conta de usuário do Windows.

Nota: Ao usar o controle de acesso de conta de usuário, use a mesma conta de serviço usada para a configuração dos Procedimentos de instalação opcionais. Para obter as instruções mais recentes de ativação da conversão do Office, consulte as *Notas da versão do Xerox® FreeFlow® Core*. Para obter o documento, acesse a página da Web do FreeFlow® Core em http://xerox.com/automate. No topo da página, clique em **Recursos do proprietário** e depois clique em **Notas da versão** que incluem os requisitos completos do sistema.

Tabela 3.5 Configuração do firewall

PORTA	PROTOCOLO OU APLICATIVO	TIPO DE CONEXÃO FIREWALL
139, 145	SMB	Saída: recupera os arquivos listados no manifesto de diretórios compartilhados
20, 21	FTP	Saída: recupera arquivos listados no manifesto
80	HTTP	Saída: recupera arquivos listados no manifesto
443	HTTPS	Saída: recupera arquivos usando a URL de HTTPS listada no manifesto
22	sFTP	Saída: recupera arquivos usando o FTP seguro listado no manifesto

LPD (Line Printer Daemon)

Nota: Comandos de LP (Line Printer) não oferecem suporte a conexões seguras.

Tabela 3.6 Configuração do firewall

PORTA	PROTOCOLO OU APLICATIVO	TIPO DE CONEXÃO FIREWALL
515	LP	Entrada: recebe solicitações LPR (Line Printer Remote) e comandos de LP
721 a 731	LPR	Saída: Envia solicitações LPR para uma impressora que suporta LPD.

Comandos JMF e sinais de status da impressora

Os comandos JMF (Formato de mensagens do trabalho) e sinais para um cliente JMF suportam conexões seguras. A recuperação de arquivos JMF suporta conexões HTTPS.

Nota: Para envios JMF seguros, envie um pacote MIME com os arquivos JMF, JDF e PDF.

Para ativar a comunicação HTTPS para comandos JMF:

1. Para adicionar um certificado ao armazenamento de chaves Java, no diretório de instalação do Xerox® FreeFlow® Core, utilize o utilitário `installJMFCertificate.bat`.
2. Reinicie o serviço Xerox® FreeFlow® Core JMF Server.
3. Para testar a instalação, acesse `http://<nome_do_host>:7759/FreeFlowCore`. Se JMF seguro estiver configurado corretamente, o navegador exibirá uma página de erro `HTTP Status 404`.

Tabela 3.7 Configuração do firewall

PORTA	PROTOCOLO OU APLICATIVO	TIPO DE CONEXÃO FIREWALL
7751	JMF	Entrada: recebe comandos JMF
Varia	JMF	Saída: retorna sinais de status da impressora JMF Nota: O cliente que solicita os sinais de status da impressora JMF ou o sinal de retorno JMF define o número da porta solicitada.
7759	sJMF	Entrada: recebe comandos JMF seguros

Nós do fluxo de trabalho

Os componentes de fluxo de trabalho que recuperam ou salvam arquivos de trabalho podem usar unidades mapeadas, caminhos de arquivo UNC, HTTP, HTTPS ou URI sFTP. A URI sFTP suporta a recuperação do arquivo de trabalho como MAX, JMF.

Nota: HTTP e FTP URIs não são compatíveis com a criptografia.

Para criptografar compartilhamentos de arquivos para compartilhar, use o sistema de arquivos do Windows. Para proteger os compartilhamentos de arquivos, use o controle de acesso de conta de usuário do Windows.

Nota: Quando usar o controle de acesso de conta de usuário, use a mesma conta de serviço usada na configuração em *Procedimentos de instalação opcionais*. Para obter mais informações, consulte o *Guia de Instalação do Xero® FreeFlow® Core*.

Tabela 3.8 Configuração do firewall

PORTA	PROTOCOLO OU APLICATIVO	TIPO DE CONEXÃO FIREWALL
139, 445	SMB	Entrada: recupera arquivos especificados em uma predefinição de componente de fluxo de trabalho Saída: salva arquivos em diretórios compartilhados
20, 21	FTP	Saída: recupera arquivos especificados em uma predefinição de componente de fluxo de trabalho
80	HTTP	Saída: recupera arquivos especificados em uma predefinição de componente de fluxo de trabalho
443	HTTPS	Saída: recupera arquivos especificados em uma predefinição de componente de fluxo de trabalho

Impressão com o Xerox® FreeFlow® Core

O Xerox® FreeFlow® Core usa SNMP e HTTP com os comandos IPP, JMF ou XBDS para determinar o tipo de DFE (Digital Front End) por meio de uma conexão não criptografada. A sequência de caracteres da comunidade pública SNMP na impressora ou no DFE requer a configuração padrão. Se a sequência de caracteres da comunidade pública SNMP na impressora ou no DFE foi modificada na configuração padrão, assegure-se de que a configuração atualizada esteja registrada no FreeFlow Core. Verifique se todas as impressoras registradas no FreeFlow Core têm a mesma sequência de caracteres da comunidade pública SNMP. Para obter instruções sobre como atualizar a sequência de caracteres da comunidade pública SNMP, consulte as Notas da versão do Xerox FreeFlow Core.

As seguintes operações utilizam uma conexão não criptografada:

- Recupere a lista de filas de DFE.
- Recupere a lista de impressoras virtuais no EFI DFE.
- Recupere os recursos da impressora.

- Operações de trabalho no DFE.
- Recupere informações de contabilidade do trabalho. Esta operação não é aplicável ao JMF.
- Envio de um trabalho de impressão para uma impressora usando LPR.

Quando conectado a um DFE configurado para suportar IPP seguro, o envio para impressão é criptografado. Para ativar o IPP seguro, use a opção Impressão protegida na configuração de Destino da Impressora. A criptografia TLS e SHA256 é usada entre o FreeFlow Core e o DFE.

Ativação de um envio de impressão por IPP seguro para o Servidor de Impressão FreeFlow

Para ativar o envio de impressão por IPP seguro para o Servidor de Impressão FreeFlow, faça o seguinte:

1. Adicione um certificado TLS ao Servidor de Impressão FreeFlow.
2. Selecione **Ativar TLS** na configuração do Servidor de Impressão Xerox® FreeFlow®.
3. Para recuperar o certificado TLS/SSL no Servidor de Impressão FreeFlow, use o Xerox® FreeFlow® Core Certificado.

Nota: Após a configuração bem-sucedida do IPP seguro, a mensagem `Certificado instalado com sucesso` será exibida.

Ativação de um envio de impressão por IPP (Protocolo de impressão via Internet) seguro para o Fiery

Para ativar um envio de impressão por IPP seguro para o Fiery, faça o seguinte:

1. Para ativar a interface com o usuário do Fiery, insira o endereço IP do Fiery em qualquer navegador da Web.
2. Selecione **Configuração do Fiery** no painel esquerdo.
3. Faça login com as credenciais da controladora Fiery.
4. Selecione **Segurança** e, em seguida, crie o certificado autoassinado ou preencha os detalhes com os certificados do CA.
5. Ative **SSL\TLS** na tela de interface com o usuário de configuração.
6. Quando SSL\TLS está ativado, uma mensagem de confirmação aparece para reiniciar a controladora.
7. Selecione **Sim**.
8. Ative o **Utilitário Windows de Configuração do Core** no Xerox® FreeFlow® Core.
9. Selecione a guia **Certificado do Core**, forneça o endereço IP da Controladora Fiery e selecione **Recuperar certificado**.

   A mensagem `Certificado instalado com sucesso` é exibida.
10. Configure a impressora no Xerox® FreeFlow® Core com a opção de impressão protegida na tela Gerenciamento de impressora.

O Xerox® FreeFlow® Core não suporta comunicação com o DFE usando JMF seguro.

Tabela 3.9 Configuração do firewall

PORTA	PROTOCOLO OU APLICATIVO	TIPO DE CONEXÃO FIREWALL
161, 162	SNMP v1/v2	Saída: identifica o tipo de DFE durante uma configuração de Destino da impressora e a Recuperação do certificado
80	HTTP	Entrada: a impressora JDF recupera o arquivo de impressão usando HTTP. Saída: identifica o tipo de DFE durante uma configuração de Destino da impressora e a Recuperação do certificado
N/D	ICMP	Saída: verifica a disponibilidade do dispositivo antes da Recuperação do certificado
631	IPP v1.0/v1.1	Saída: envia trabalhos para DFEs, obtém o status do trabalho e envia os comandos de trabalho para o DFE
4004	JMF	Entrada: Recebe a mensagem JMF `ReturnQueueEntry` da impressora
8010 ou impressora definiu a porta JMF	JMF v1.3/v1.4	Saída: Identifica o tipo de DFE durante o Registro da impressora e envia o trabalho para o DFE.
443	HTTPS	Saída: comunicação da impressora com o DFE
515, 721 a 731	LPR	Saída: Envia solicitações LPR para uma impressora que suporta LPD

Notificação por e-mail

O Xerox® FreeFlow® Core é um cliente de e-mail que se conecta ao servidor de e-mail SMTP acessível ou a um servidor de e-mail do Google. Você pode criptografar notificações por e-mail e então se conectar a um servidor de e-mail que suporta criptografia. O TLS ativa a criptografia das comunicações entre o serviço de notificação e o servidor SMTP.

As credenciais criptografadas são armazenadas localmente.

Tabela 3.10 Configuração do firewall

PORTA	PROTOCOLO OU APLICATIVO	TIPO DE CONEXÃO FIREWALL
25, 465, 587	SMTP	Saída: Envia notificações de e-mail Nota: O número da porta solicitada e o uso de conexão segura dependem da configuração do servidor SMTP.

Compatível com FIPS e GDPR

O Xerox® FreeFlow® Core é executado no sistema operacional Windows habilitado para conformidade com FIPS 140-2. Para ativar a conformidade com FIPS, consulte a documentação da Microsoft. Por padrão, o FreeFlow Core é executado no modo de conformidade com FIPS.

O FreeFlow Core desativa o suporte para criptografia DES/3DES.

Se a impressão IPP segura com Autenticação Digest for solicitada, desative o modo de conformidade com FIPS. Assim, o FreeFlow Core não estará mais em conformidade com os requisitos de criptografia.

O FreeFlow Core é compatível com o GDPR (Regulamento Geral sobre Proteção de Dados) da União Europeia.

Proteção de segurança geral

AUTENTICAÇÃO DE CONTA DO SERVIÇO, UTILITÁRIOS E INTERFACE DA LINHA DE COMANDOS (CLI)

As contas do serviço do FreeFlow Core, os utilitários e a CLI agora usam a autenticação Windows. Para realizar a autenticação adicione a conta do serviço ou a conta do usuário conectado atualmente a um grupo local do Windows denominado Segurança do FreeFlow Core. Para obter mais informações, consulte as *notas de versão do Xerox FreeFlow Core*.

PROTEÇÃO DE DADOS DO USUÁRIO

Segurança de documentos e arquivos

O FreeFlow Core não criptografa explicitamente os arquivos enviados para processamento antes de serem armazenados no sistema de arquivos do computador.

O conteúdo de origem do documento possui Informações de identificação pessoal (PII) ou outro conteúdo sensível. Portanto, é responsabilidade do usuário lidar com as informações digitais de acordo com as melhores práticas de proteção de informações.

Informações de identificação pessoal (PII)

Quando você se registra para obter uma licença de software do FreeFlow Core, as informações PII são coletadas. As informações contêm o seguinte:

- Nome da empresa
- Chave de ativação e número de série
- ID do host/UUID do sistema
- Nome do usuário
- Endereço (Rua, Cidade, Estado, CEP, País)
- Endereço de e-mail (opcional)

Essas informações são transmitidas de forma segura para o host de licenças da Xerox.

As informações PII, especialmente o endereço de e-mail do usuário que é usado para recuperação de senha, são armazenadas no sistema FreeFlow Core. As informações são criptografadas.

Acesso de conta de usuário e Retenção do trabalho

SENHAS DE CONTAS DO USUÁRIO

A reutilização de uma senha é permitida por até 10 vezes. O número de vezes que uma senha pode ser reutilizada é configurável.

BLOQUEIO DE CONTA DO USUÁRIO

Se a autenticação falhar ao usar o Cliente do Xerox FreeFlow Core, os usuários serão bloqueados após três tentativas de login por um período de 30 minutos. O número de tentativas de login com falha e o período de bloqueio são configuráveis.

LOGOUT DE CONTA DO USUÁRIO

Após 30 minutos de atividade, os usuários que fizeram login no Cliente do Xerox® FreeFlow® Core serão desconectados automaticamente. A duração do período de inatividade não é configurável.

ATIVIDADE DA CONTA DO USUÁRIO

O registro de auditoria de transações de login do usuário para o FreeFlow Core está localizado no Visualizador de Eventos do Windows, na seção **Aplicativo** na pasta **Logs do Windows**.

RETENÇÃO DE TRABALHO

Após a conclusão do processamento de um trabalho, o período de retenção para os trabalhos no FreeFlow Core é de 24 horas.

A impressora FreeFlow Core é configurada para alterar o período de retenção, antes que os trabalhos concluídos sejam removidos automaticamente. Após 24 horas, o dispositivo FreeFlow Core remove os trabalhos concluídos.

Para remover os trabalhos manualmente, use o FreeFlow Core Web GUI.

PROPRIEDADES DO TRABALHO

Ativa a restrição de download de arquivos encontrados em Propriedades do trabalho para um trabalho exibido em Gerenciamento e Status do Trabalho do FreeFlow Core.

Direitos da conta do usuário

Para configurar a conta do serviço Xerox® FreeFlow® Core, você pode usar uma conta de administrador local ou uma conta que não seja de administrador. Quando você usar uma conta que não seja um membro do grupo de administradores locais, nenhuma ação especial será necessária.

Quando você usar uma conta que não seja de administrador, serão necessários direitos adicionais, além dos direitos do grupo de usuários padrão. O FreeFlow® Core Configure inclui direitos adicionais automaticamente, conforme listados na tabela a seguir:

CONFIGURAÇÃO DA POLÍTICA DE GRUPO	NOME CONSTANTE
Atua como parte do sistema operacional	SeTcbPrivilege
Ajustar cotas de memória para um processo	SeIncreaseQuotaPrivilege
Permitir login localmente	SeInteractiveLogonRight
Faze backup de arquivos e diretórios	SeBackupPrivilege
Criar um objeto de token	SeCreateTokenPrivilege
Criar objetos globais	SeCreateGlobalPrivilege
Criar objetos compartilhados permanentes	SeCreatePermanentPrivilege
Depurar programas	SeDebugPrivilege
Carregar e descarregar drivers de impressão	SeLoadDriverPrivilege
Fazer login como um trabalho em lote	SeBatchLogonRight
Fazer login como um serviço	SeServiceLogonRight
Gerenciar registro de auditoria e segurança	SeSecurityPrivilege
Executar tarefas de manutenção de volume	SeManageVolumePrivilege
Perfil de único processo	SeProfileSingleProcessPrivilege
Perfil de desempenho do sistema	SeSystemProfilePrivilege
Substituir um token de nível de processo	SeAssignPrimaryTokenPrivilege

Nota: Os direitos listados na tabela são definidos no site https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-rights-assignment.

Segurança

Este capítulo contém:

Na Xerox, as questões de segurança são muito importantes. Como líder no desenvolvimento de tecnologia digital, a Xerox demonstra o seu compromisso em manter informações digitais seguras e protegidas, identificar possíveis vulnerabilidades e tratar problemas proativamente para limitar os riscos.

A Xerox se esforça para oferecer os dispositivos de software mais seguros possível, com base nas informações e nas tecnologias disponíveis, enquanto mantém o desempenho, o valor, a funcionalidade e a produtividade do dispositivo.

A segurança dos componentes do Xerox® FreeFlow® Core é avaliada com as ferramentas de varredura comercialmente disponíveis para verificação de vulnerabilidades e penetração. As vulnerabilidades dos aplicativos são tratadas com base nos resultados das verificações da Xerox.

Quando necessário, a Xerox distribui boletins de segurança. As informações dos boletins de segurança são comunicadas no site de Segurança da Xerox em http://www.xerox.com/security para Orientação de segurança de produtos. O site contém o status atualizado de vulnerabilidades de segurança da impressora, white papers, Certificação Common Criteria, Informações do Intel Security McAfee e um portal para enviar dúvidas sobre segurança à Xerox.

Proteção antivírus

A Xerox toma precauções especiais para garantir que o software Xerox seja enviado sem contaminação por vírus de computador. A Xerox recomenda que a Detecção antivírus e a Detecção e prevenção de intrusão de ponto de extremidade sejam instaladas no Servidor FreeFlow Core. Esse software e o sistema operacional são mantidos atualizados com os patches de segurança mais recentes, conforme recomendado pelos respectivos fornecedores.

Para melhorar o desempenho, recomenda-se que você exclua os diretórios de instalação do Xerox® FreeFlow® Core e do SQL Server das varreduras do antivírus.

Você excluir os seguintes arquivos da varredura do antivírus:

- `<diretório de instalação do FreeFlow Core>\Logs`
- `<diretório de instalação do FreeFlow Core>\Platform\Logs`
- `<diretório de instalação do FreeFlow Core>\JobSubmit\Logs`
- `<diretório de instalação do FreeFlow Core>\Config`
- `<diretório de instalação do FreeFlow Core>\Platform\Config`
- `<diretório de dados do usuário do FreeFlow Core>\`
- Pastas fora do diretório de dados do usuário do FreeFlow Core que são usadas pelo FreeFlow Core

Atualização do software

A Xerox não se responsabiliza pelo estado do sistema operacional que executa o Xerox® FreeFlow® Core. É responsabilidade do cliente manter o sistema atualizado e garantir que ele esteja adequadamente corrigido e configurado. Execute uma atualização do Microsoft® Windows® pelo menos uma vez por mês.

Use a opção **Windows Update** para aplicar a atualização, quando executar as atualizações do Windows. É recomendado não instalar as atualizações opcionais de versão prévia, porque elas podem afetar a confiabilidade do servidor do Xerox® FreeFlow® Core.

Você pode encontrar as atualizações de software para o FreeFlow Core em http://www.support.xerox.com/support/core/software/enus.html. Os clientes podem instalar a atualização do software.

Informações e recursos adicionais

Segurança na Xerox

A Xerox mantém um página da Web pública atualizada que contém as informações de segurança mais recentes pertencentes aos seus produtos. Consulte www.xerox.com/security.

Respostas às vulnerabilidades conhecidas

A Xerox criou um documento que detalha a Política de gerenciamento e divulgação de vulnerabilidades da Xerox, que é usada na descoberta e correção de vulnerabilidades no software e hardware da Xerox. É possível fazer download desse documento nesta página: https://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html.

Recursos adicionais

RECURSO DE SEGURANÇA	URL
Perguntas frequentes	www.xerox.com/en-us/information-security/frequently-asked-questions
Boletins, Assistentes e Atualizações de segurança	www.xerox.com/security
Arquivos de novidades de segurança	security.business.xerox.com/en-us/news/
Centro de confiabilidade Xerox	https://trust.corp.xerox.com/