

Xerox® FreeFlow® Core

Guia de Segurança

© 2019 Xerox Corporation. Todos os direitos reservados. Xerox®, Xerox com a marca figurativa® e FreeFlow® são marcas da Xerox Corporation nos Estados Unidos e/ou em outros países.

Este software inclui o software desenvolvido pela Adobe Systems Incorporated.

Adobe, o logotipo Adobe, o logotipo Adobe PDF, PDF Converter SDK, Adobe Acrobat Pro DC, Adobe Reader DC e PDF Library são marcas ou marcas registradas da Adobe Systems Incorporated nos Estados Unidos e/ou em outros países.

O navegador Google Chrome™ é uma marca da Google LLC.

Microsoft®, Windows®, Edge®, Microsoft Language Pack, Microsoft Office 2013, Microsoft Office 2016, Microsoft SQL Server e Internet Explorer® são marcas registradas da Microsoft Corporation nos Estados Unidos e/ou outros países.

Apple®, Macintosh®, Mac®, Mac OS® e Safari® são marcas ou marcas registradas da Apple, Inc., registradas nos Estados Unidos e em outros países.

Mozilla Firefox é uma marca da Mozilla Foundation nos Estados Unidos e em outros países.

BR14707

Índice

1 Visão geral.....	5
Objetivo	6
Público-alvo.....	7
Termo de responsabilidade.....	8
2 Descrição do produto.....	9
Estrutura de software do sistema	10
3 Aspectos de segurança dos recursos selecionados	11
Acesso ao sistema	12
Conexões de rede.....	12
Conformidade com FIPS.....	21
Criptografia de dados.....	22
Processamento de arquivo.....	22
Acesso de conta de usuário e Retenção do trabalho.....	23
Senhas de contas do usuário	23
Bloqueio de conta do usuário	23
Logout de conta do usuário.....	23
Atividade da conta do usuário.....	23
Retenção de Trabalho.....	23
4 Segurança.....	25
Proteção antivírus	26
5 Atualização do software	27

Visão geral

Este capítulo contém:

- Objetivo 6
- Público-alvo 7
- Termo de responsabilidade 8

Objetivo

O objetivo deste documento é divulgar informações pertinentes à segurança dos produtos Xerox® FreeFlow® Core e Xerox® FreeFlow® Cloud.

Os clientes são responsáveis pela segurança de suas redes e 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

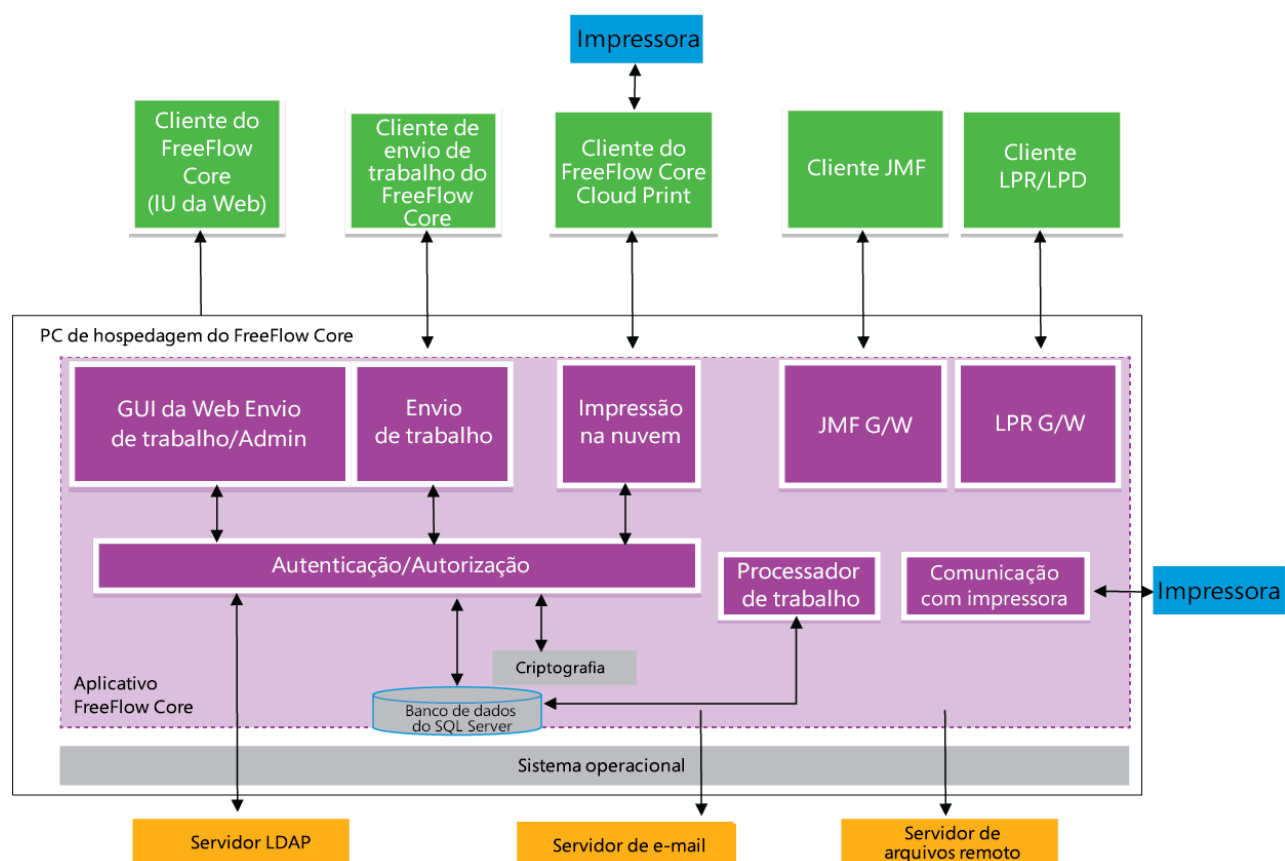
Este capítulo contém:

- [Estrutura de software do sistema.....](#) 10

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.

O Xerox® FreeFlow® Core Cloud é a solução oferecida para a configuração na nuvem. A execução em nuvem significa que a Xerox instala o software nos servidores em nuvem da Xerox. A Xerox configura e gerencia a manutenção da solução. Você pode acessar seu dispositivo dedicado e seguro usando um navegador da Web.

Estrutura de software do sistema



Aspectos de segurança dos recursos selecionados


Este capítulo contém:

- Acesso ao sistema 12
- Conformidade com FIPS..... 21
- Criptografia de dados..... 22
- Acesso de conta de usuário e Retenção do trabalho..... 23

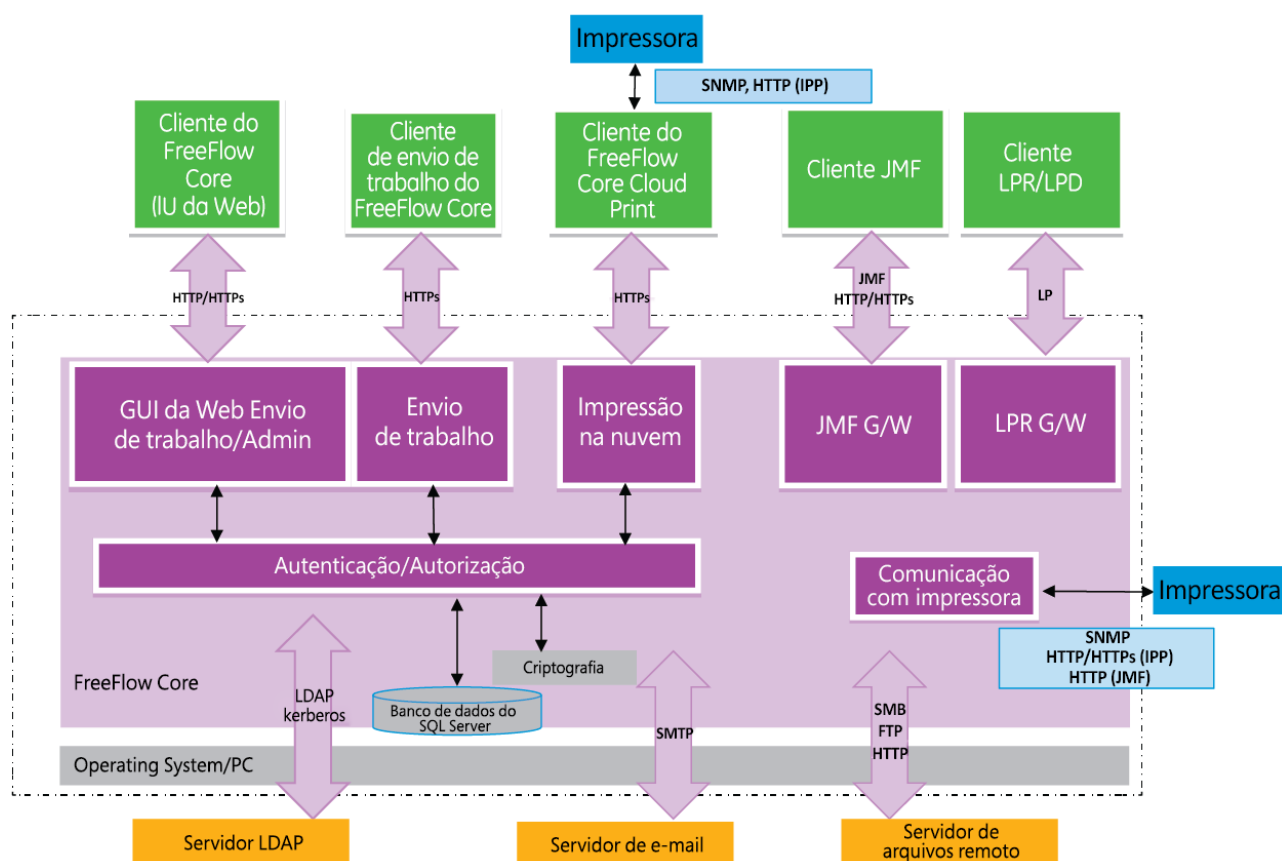
Acesso ao sistema

Conexões de rede

O Xerox® FreeFlow® Core exige conectividade de rede para o processamento de trabalhos e 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 requerido 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 conexões HTTPS, adicione um certificado TLS/SSL ao Internet Information Services (IIS). Siga as instruções na documentação do Windows.
- Para ativar conexões HTTPS, adicione um certificado CA ao gerenciador do Internet Information Services (IIS). Consulte a documentação do Windows.
- FreeFlow Core é compatível com os protocolos criptográficos TLS 1.1 e 1.2. TLS 1.0. Todas as versões de SSL estão desativadas.
- Não há troca de dados do cliente entre o cliente e o servidor do 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 FreeFlow Core no dispositivo.
- 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.

Para atribuir usuários às funções de usuário, consulte a ajuda do FreeFlow Core, tópico *Configuração de acesso ao 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:
 - Configuração da Pasta ativa
 - Configuração de Notificações
 - Configuração de Acesso ao usuário
- Utilitários do Servidor Core disponíveis na área de trabalho do servidor:
 - Xerox® FreeFlow® Core Exchange
 - Xerox® FreeFlow® Core Reports
 - Servidor do Xerox® FreeFlow® Core Cloud Print
 - Certificados do Xerox® FreeFlow® Core
 - Licença do Xerox® FreeFlow® Core
 - Xerox® Core Configure
- Utilitários do cliente Core:
 - Xerox® FreeFlow® Core Submit
 - Cliente do Xerox® FreeFlow® Core Cloud Print



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
- Utilitários do cliente Core:
 - Xerox® FreeFlow® Core Submit
 - Cliente do Xerox® FreeFlow® Core Cloud Print



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 de usuário

As credenciais inseridas para o cliente do navegador do Xerox® FreeFlow® Core são criptografadas com o uso da criptografia AES A128. As credenciais são criptografadas antes que sejam enviadas ao servidor do Xerox® FreeFlow® Core.

- Ao autenticar usuários com o Xerox® FreeFlow® Core, as informações do usuário serão criptografadas com o uso da criptografia AES 128. As credenciais são armazenadas localmente.
- 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.

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 de usuário  Nota: Os números de portas e serviços dependem da configuração do AD do servidor.
<ul style="list-style-type: none"> • 389 • 636 • 3268 • 3269 	<ul style="list-style-type: none"> • LDAP • LDAP SSL • LDAP GC • LDAP GC SSL 	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 de usuário Enviar trabalho

A interface de usuário (IU) Enviar trabalho usa a conexão de cliente do Xerox® FreeFlow® Core para o envio de trabalhos. Para obter 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, utilize a mesma conta de serviço utilizada na configuração em *Procedimentos de instalação opcionais*. Para obter mais informações, consulte o *Guia de Instalação do 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 ou FTP 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 utilizar o controle de acesso de conta de usuário, use a mesma conta de serviço utilizada para a configuração dos Procedimentos de instalação opcionais. Para obter mais informações, consulte o *Guia de Instalação do FreeFlow Core*, seção *Procedimentos de instalação opcionais*.

Tabela 3.5 Configuração do firewall

Porta	Protocolo ou aplicativo	Tipo de conexão firewall
139, 145	SMB	Saída: recupera arquivos listados no manifesto de diretórios compartilhados
20, 21	FTP	Saída: recupera arquivos listados no manifesto
80	HTTP	Saída: recupera arquivos listados 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

Comandos JMF e sinais de status da impressora

Comandos JMF (Job Messaging Format) aceitam conexões seguras. A recuperação de arquivos JMF utiliza conexões não criptografadas.


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

Os sinais de status da impressora JMF utilizam uma conexão não criptografada. Para o status da impressora JMF seguro, utilize o comando JMF StatusQuery sobre uma conexão segura.

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`. Se JMF seguro estiver configurado corretamente, o navegador exibe uma página de erro HTTP Status 404.

Tabela 3.7 Configuração do firewall

Porta	Protocolo ou aplicativo	Tipo de conexão firewall
775-1	JMF	Entrada: recebe comandos JMF
Va- ria	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.
775-9	sJMF	Entrada: recebe comandos JMF seguros

Xerox® FreeFlow® Core Submit

A conexão entre o Xerox® FreeFlow® Core Submit e o Xerox® FreeFlow® Core é criptografada e exige a instalação de um certificado CA.


- Para instalar o certificado no servidor, adicione o certificado usando o gerenciador do Internet Information Services (IIS).
- TLS 1.2 é usado entre o software Xerox FreeFlow Core Submit e Xerox FreeFlow Core.
- O aplicativo Xerox® FreeFlow® Core Submit e o software de suplementos do Microsoft Office utilizam a mesma conexão segura para o Xerox® FreeFlow® Core.
- As credenciais criptografadas são armazenadas localmente.

Tabela 3.8 Configuração do firewall

Porta	Protocolo ou aplicativo	Tipo de conexão firewall
443	HTTPS	Entrada no servidor: aceita as conexões do cliente Xerox® FreeFlow® Core Submit Saída no cliente: envia trabalhos ao Xerox® FreeFlow® Core Cloud

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 ou FTP URIs.

 **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, utilize a mesma conta de serviço utilizada na configuração em *Procedimentos de instalação opcionais*. Para obter mais informações, consulte o *Guia de Instalação do FreeFlow Core*.

Tabela 3.9 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: você pode criptografar arquivos nas pastas ativas. Para pastas compartilhadas do Windows, é possível criptografar os arquivos usando o sistema de arquivo do Windows ou proteger os arquivos usando o controle de acesso de conta do usuário do Windows. Recupera arquivos especificados em uma predefinição de componente de fluxo de trabalho.

Impressão com o Xerox® FreeFlow® Core

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

Quando conectado a um DFE configurado para oferecer suporte a 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 1.2 e SHA256 é usada entre o FreeFlow Core e o DFE.

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

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



Nota: Quando IPP seguro estiver configurado corretamente, é exibida a mensagem *Certificado instalado com sucesso*.

O FreeFlow Core não oferece suporte à comunicação com DFE usando JMF seguro.

Tabela 3.10 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	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
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: envia trabalhos ao DFE

Xerox® FreeFlow® Core Cloud Print

A conexão entre o servidor do Xerox® FreeFlow® Core Cloud Print e o cliente é criptografada e exige a instalação de um certificado CA. TLS 1.2 é usado entre o servidor e o cliente FreeFlow Core Cloud Print.

Para instalar o certificado no servidor, use o gerenciador do Internet Information Services (IIS). Para obter mais informações, consulte a documentação do Windows.

Para determinar o tipo de DFE (Digital Front End) usando uma conexão não criptografada, o cliente Xerox® FreeFlow® Core Cloud Print usa SNMP ou HTTP. A cadeia de caracteres da comunidade pública SNMP na impressora ou no DFE é definida com a configuração padrão.

A conexão entre o cliente Xerox® FreeFlow® Core Cloud Print e o DFE (Digital Front End) não oferece suporte a IPP seguro.

Tabela 3.11 Configuração do firewall


Porta	Protocolo ou aplicativo	Tipo de conexão firewall
161, 162	SNMP (v1/v2)	Saída: identifica o tipo de DFE durante a configuração do Destino da impressora
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
443	HTTPS	Entrada no servidor: aceita as conexões do cliente Xerox® FreeFlow® Core Cloud Print Saída no cliente: conecta-se ao servidor do Xerox® FreeFlow® Core Cloud Print
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.

Notificação por e-mail

O Xerox® FreeFlow® Core é um cliente de e-mail que se conecta ao servidor de e-mail do cliente. Você pode criptografar notificações por e-mail e então se conectar a um servidor de e-mail compatível com criptografia. O protocolo SSL permite criptografar as comunicações entre o serviço de notificação e o servidor SMTP.

As credenciais criptografadas são armazenadas localmente.

Tabela 3.12 Configuração do firewall

Porta	Protocolo ou aplicativo	Tipo de conexão firewall
25, 2525, 465, 475, 587	SMTP	Saída: envia notificações por e-mail  Nota: O número da porta solicitada e o uso de conexão segura dependem da configuração do servidor SMTP.

Conformidade com FIPS

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.

Criptografia de dados

Processamento de arquivo

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

Acesso de conta de usuário e Retenção do trabalho

Senhas de contas do usuário

A reutilização de senhas é permitida.

Bloqueio de conta do usuário

Se a autenticação falhar com o FreeFlow Core, os usuários não são bloqueados após tentativas malsucedidas.

Logout de conta do usuário

Após 30 minutos de inatividade, os usuários conectados são desconectados automaticamente. A duração do período de inatividade não é configurada.

Atividade da conta do usuário

O registro de auditoria de transações de login do usuário no FreeFlow Core não está disponível.

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.

Segurança

Este capítulo contém:

- **Proteção antivírus..... 26**

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. Os especialistas do setor de computadores pessoais recomendam a Xerox para todos que buscam um software de detecção de vírus. Para proteger a sua impressora contra vírus, é imperativo que o software de detecção de vírus seja mantido atualizado.

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

Recomenda-se que os clientes mantenham o software atualizado em todos os dispositivos de software instalados no servidor do Xerox® FreeFlow® Core. Execute uma atualização do Microsoft Windows pelo menos uma vez por mês.

Você encontra 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.

