

# Serviços Remotos na Xerox

## Guia de segurança

Versão 4.0

Março de 2022

Xerox Corporation Todos os direitos reservados. Xerox® é uma marca comercial da Xerox Corporation nos Estados Unidos da América e/ou em outros países. BR35887

Microsoft®, Windows®, Windows Vista®, SQL Server®, Microsoft®.NET, Windows Server®, Internet Explorer®, Windows Media® Center, e Windows NT® também são marcas comerciais registradas ou marcas comerciais da Microsoft Corporation nos Estados Unidos da América e/ou em outros países.

Linux® é uma marca comercial registrada da Linus Torvalds.

Apple®, Macintosh® e Mac OS® são marcas comerciais registradas da Apple Inc.

VMware® é uma marca comercial registrada da VMware Inc. nos Estados Unidos da América e/ou em outras jurisdições.

Cisco® é uma marca comercial registrada da Cisco e/ou suas afiliadas

Parallels Desktop é uma marca comercial registrada da Parallels IP Holdings GmbH.

Mudanças são feitas periodicamente neste documento. Mudanças, imprecisões técnicas e erros tipográficos serão corrigidos em edições subsequentes.



IS 614672/IS 514590

# Índice

<b>1. Público e Finalidade Geral .....</b>	<b>1-4</b>
<b>2. Proposição de valor.....</b>	<b>2-4</b>
<b>3. Serviços Remotos.....</b>	<b>3-5</b>
<b>4. Modelos de Implementação .....</b>	<b>4-6</b>
<b>Modelo de Implementação de Combinação (preferido) .....</b>	<b>4-7</b>
<b>Modelo de Implementação Device Direct .....</b>	<b>4-8</b>
<b>Modelo de Implementação de Aplicativo de Gestão de Dispositivo .....</b>	<b>4-9</b>
<b>5. Transmissão de dados &amp; Cargas .....</b>	<b>5-10</b>
Fontes de dados .....	5-10
Dispositivos Xerox® Office .....	5-10
Dispositivos Xerox® Production.....	5-11
Aplicativos de Gestão de Dispositivo Xerox®.....	5-12
<b>6. Gestão remota de dispositivos de impressão .....</b>	<b>6-14</b>
As exigências de sistema para Aplicativos de Gestão de Dispositivo.....	6-15
<b>7. Serviços e Processos de Negócios Xerox®.....</b>	<b>7-17</b>
<b>8. Detalhes da tecnologia.....</b>	<b>8-18</b>
Design do software .....	8-18
Operabilidade.....	8-18
<b>9. Recursos de segurança.....</b>	<b>9-22</b>
Simple Network Management Protocol (SNMP) para a Xerox® .....	9-22
<b>10. Impacto de rede.....</b>	<b>10-25</b>
Protocolos, portas e outras tecnologias relacionadas .....	10-25
<b>11. Melhores práticas de segurança .....</b>	<b>11-27</b>

# 1. Público e Finalidade Geral

O relatório de segurança dos Serviços Remotos na Xerox é fornecido para ajudar os clientes a entenderem e implementarem a solução de serviços remotos segura que funciona melhor em sua construção de rede e políticas de segurança da informação. Para garantir o método de configuração mais seguro, observe que mudanças no firewall da internet, servidores web proxy ou outra infraestrutura de rede relacionada à segurança pode ser necessária.

O público alvo para este documento inclui fornecedores técnicos, gerenciadores de rede e profissionais de segurança de rede interessados nas capacidades de serviços remotos e na implementação da segurança de tais recursos.

Recomendamos que o documento seja analisado em sua totalidade para certificar o uso dos Produtos e Serviços Xerox® dentro de um ambiente conectado por rede do cliente.

## 2. Proposição de valor

Oferecemos uma forma segura de enviar os dados do dispositivo para nosso sistema certificado ISO visando automatizar tarefas comuns e fornecer um melhor serviço e experiência de suporte.

- O relatório de medidor de faturamento é automatizado e preciso.
- O programa de reposição de suprimentos automatizado fornece toner com base nos níveis de toner comunicados da impressora para que não seja preciso rastrear inventário ou ligar para fornecedores.
- Enviar informações de diagnóstico nos permite fornecer um melhor suporte para seu dispositivo, normalmente permitindo uma resolução de problema mais rápida.
- Certos modelos de impressora podem verificar a existência de atualizações de software importantes e instalar as atualizações de forma programada sem a intervenção do cliente. <sup>Ver nota</sup>
- Nossas capacidades de serviços gerenciados também fornecem uma forma de gerenciar impressoras que não sejam Xerox além de impressoras Xerox.
- Esses serviços permitem que nossos clientes aproveitem o tempo de forma mais eficiente.

Tudo isso é feito com a segurança em mente.

**Nota:** Esta opção pode ser desabilitada em ambientes onde os clientes estão certificando uma versão de software definida e desejam controlar o software de impressão quando as atualizações ocorrerem. Isso pode ser feito sem ter que desabilitar as capacidades de serviços remotos existentes.

### 3. Serviços Remotos

Informação é um ativo-chave e a segurança é primordial para todos os ativos da organização, incluindo dispositivos de impressão multifuncionais (MFPs) em rede. Hoje em dia, administrar uma frota de dispositivos de impressão multifuncionais enquanto garante um nível aceitável de segurança, representa um conjunto de desafios únicos que normalmente são negligenciados. Nós entendemos esta complexidade e é responsiva às necessidades de segurança dos clientes. As ofertas dos Produtos Xerox®, Sistemas Xerox® e serviços remotos são projetadas para se integrarem com segurança aos fluxos de trabalho existentes do nosso cliente enquanto aplicam as últimas tecnologias de segurança.

**Por padrão, nenhuma imagem para impressão, fax, digitalização, ações de cópia ou outras informações sensíveis do cliente são transmitidas para nossos servidores.**

Os servidores Xerox com base nos EUA estão em conformidade com estritas exigências de segurança em relação à Gestão de Segurança da Informação. Nossos data centers e aplicativos de serviços remotos mantêm as exigências de conformidade anuais da Statement on Standards for Attestation (SSAE) No-16, Sarbanes-Oxley Act (SOX) e são certificados pelo ISO 27001:2013.

## 4. Modelos de Implementação

Os clientes podem escolher entre os seguintes modelos igualmente seguros de implementação dos Serviços Remotos Xerox®:

- **Modelo de combinação - (*Modelo preferido*)** A implementação tanto do modelo de aplicativo de gestão de dispositivo quanto do Device Direct é ideal já que proporciona as mais sólidas capacidades de gestão de dispositivo e conjunto de dados.
- **Modelo Device Direct** - O Device Direct permite que os dispositivos de impressão se comuniquem diretamente aos servidores de comunicação remotos da Xerox® através da internet pelo firewall do cliente para dar suporte à Leitura Automática dos Contadores (AMR), Reposição Automática de Suprimentos (ASR) e relatório de diagnósticos do dispositivo. Este modelo de implementação fornece um conjunto de elementos de dados na carga padrão para incluir falhas de dispositivo, alertas, contadores, Itens de Serviço de Alta Frequência (HFSI) e outros atributos de dispositivos de impressão.
- **Modelo de Aplicativo de Gestão de Dispositivo** - Os aplicativos de gestão de dispositivo da Xerox® podem ser implementados na rede de um cliente para coletar um conjunto de atributos de dados de dispositivos de impressão para também dar suporte à Leitura Automática dos Contadores (AMR), Reposição Automática de Suprimentos (ASR) e relatório de diagnósticos do dispositivo. Os atributos do dispositivo de impressão são coletados e então transmitidos de forma segura para os servidores remotos da Xerox. Os atributos de dados dos dispositivos de impressão, da Xerox ou não, podem ser comunicados como uma parte deste modelo de implementação.

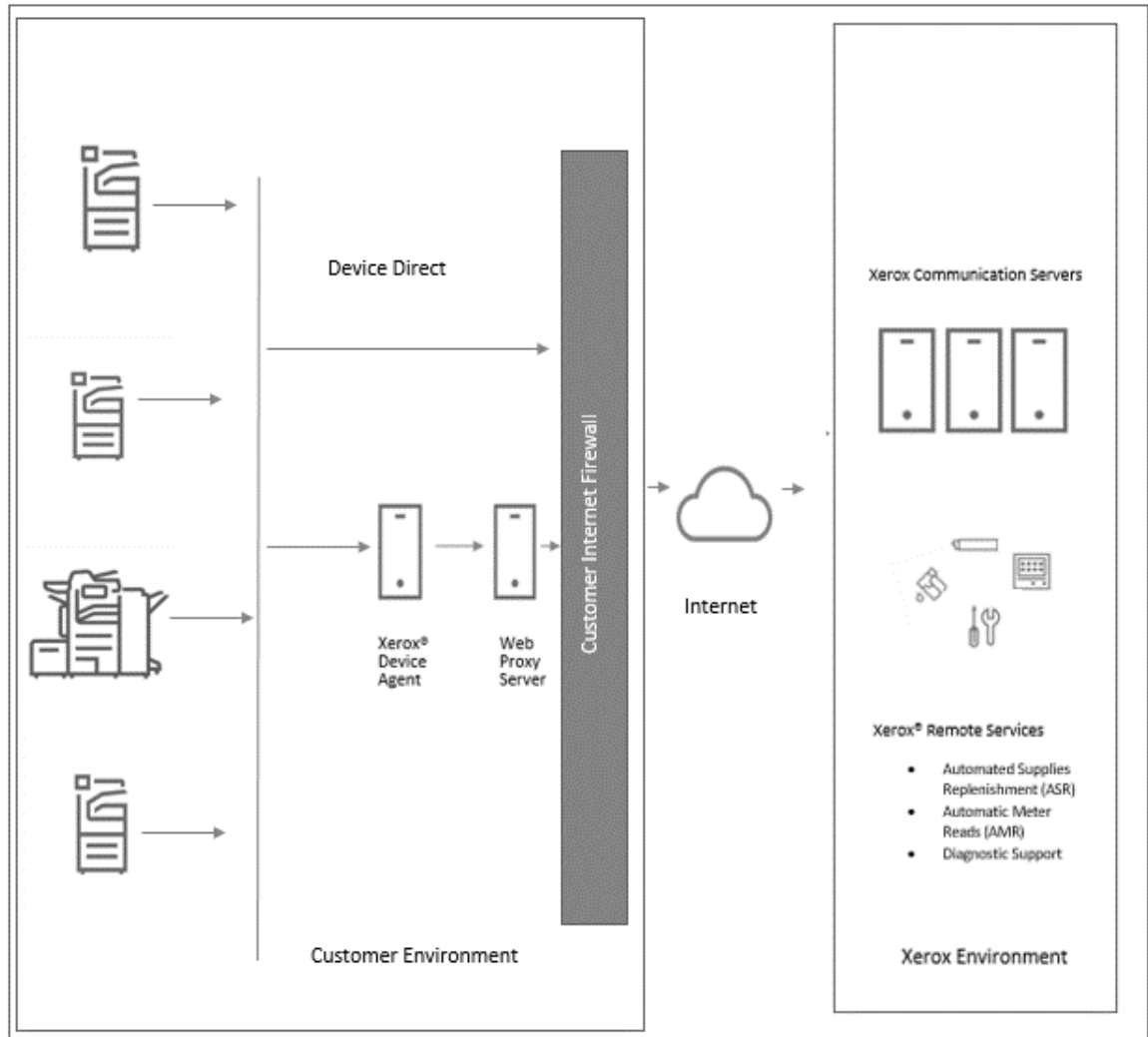
Todos os modelos de implementação para os Serviços Remotos Xerox® são igualmente seguros e utilizam os mais recentes protocolos e portas padrão do setor com base na internet para estabelecer um canal seguro e criptografado ao transmitir atributos do dispositivo de impressão externamente para servidores Xerox remotos localizados em nossos data centers com redundância de segurança.

O modelo de implementação escolhido depende do tipo de solução de serviço de impressão do nosso cliente, das regras e políticas de segurança da informação para processar a transmissão dos atributos de dados da impressora.

## Modelo de Implementação de Combinação (preferido)

A Implementação de Combinação é utilizada quando um cliente compra vários tipos de contratos de manutenção para suas impressoras e para atingir uma solução de serviços remotos mais sólida. Quando uma impressora Xerox® é inicialmente instalada em uma rede, o comportamento dos serviços remotos da Xerox é a impressora tentar se comunicar automaticamente para fora dos nossos servidores de comunicação utilizando um método de conexão seguro e autenticado.

Figura 1



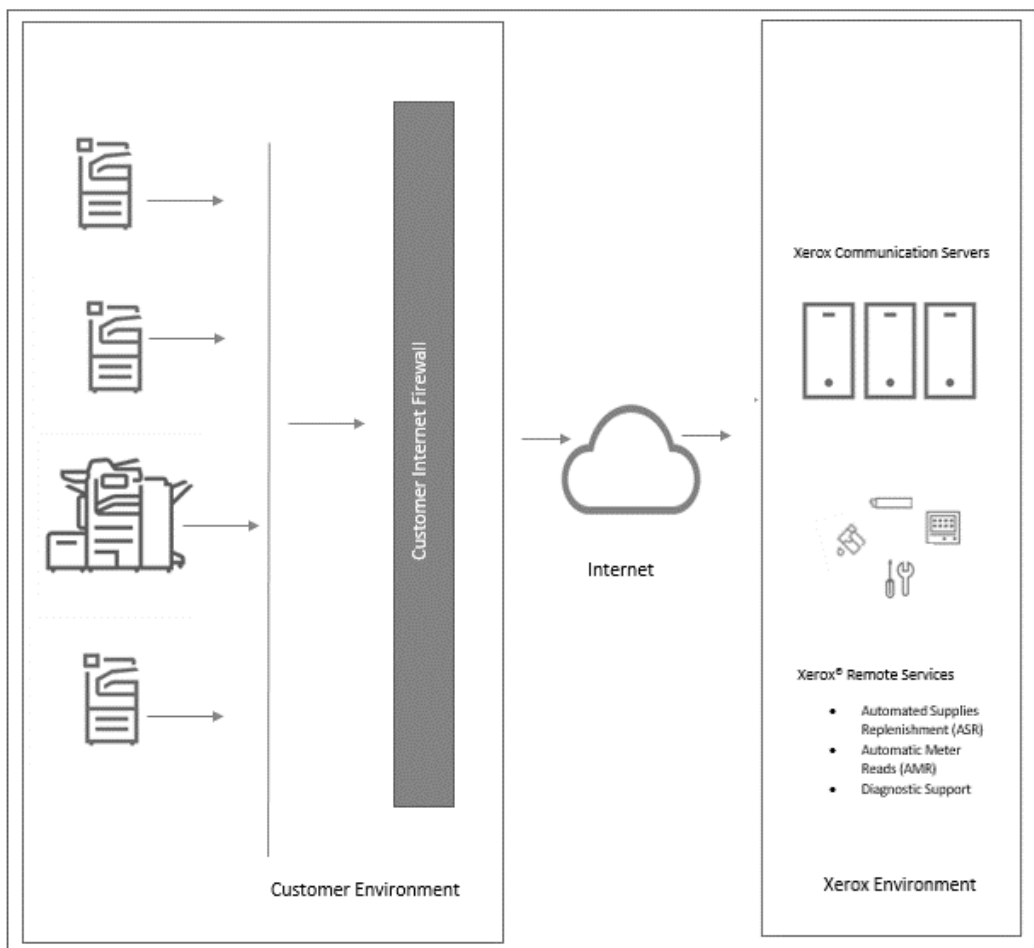
Combination Deployment Model

## Modelo de Implementação Device Direct

Dispositivos Xerox® com capacidade de Serviços Remotos utilizam uma conexão de protocolo Transport Layer Security (TLS) 1.2 na porta 443 segura padrão para a comunicação de saída para nossos servidores seguros.

- Os dispositivos de impressão dentro do ambiente do cliente iniciam todas as comunicações com os servidores de comunicação. As configurações de firewall padrão no local são necessárias para habilitar a comunicação.
- Um URL válido para os servidores de comunicação devem ser utilizados (\*.xerox.support.com) para autenticar dispositivos de impressão para a infraestrutura da Xerox
- O dispositivo solicita um registro com os servidores de comunicação utilizando as credenciais apropriadas de autenticação de certificado.
- Os servidores de comunicação validam as credenciais fornecidas pelas impressoras e aceitam as solicitações.
- Os servidores de comunicação estão atrás de um firewall seguro e não são acessíveis pela internet.

Figura 2



Device Direct Deployment Model

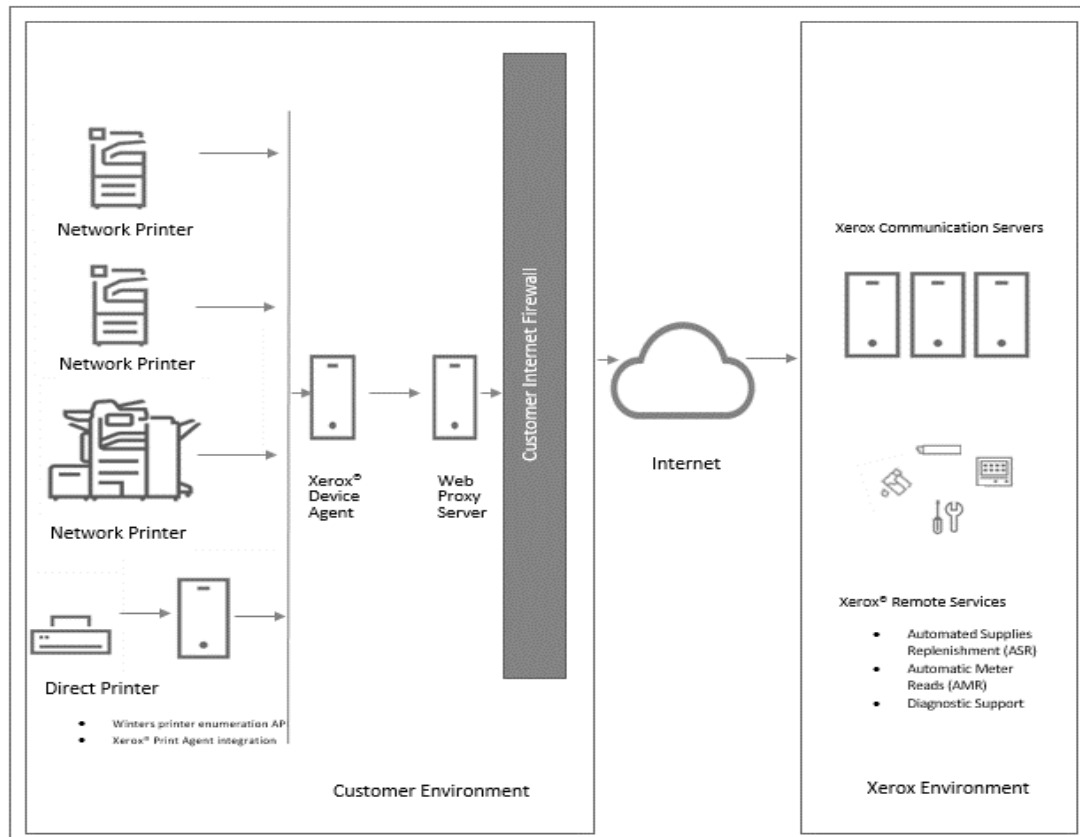


## Modelo de Implementação de Aplicativo de Gestão de Dispositivo

Os Aplicativo de Gestão de Dispositivo (**Xerox Centre Ware® Web, Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition, e Xerox Device Manager**) utilizam uma conexão de protocolo Transport Layer Security (TLS) 1.2 na porta 443 de padrão seguro para uma comunicação externa com os servidores de comunicação. Recursos adicionais são utilizados para aumentar a segurança neste canal e são estabelecidos durante a instalação inicial dos aplicativos de Gestão de Dispositivos que inclui:

- O aplicativo de gestão de dispositivo dentro do ambiente do cliente inicia todas as comunicações com os servidores de comunicação. As configurações de firewall padrão no local são necessárias para habilitar a comunicação.
- Os servidores de comunicação estão atrás de um firewall seguro e não são acessíveis pela internet.
- O aplicativo de gestão de dispositivo solicita um registro com os servidores de comunicação utilizando as credenciais apropriadas de autenticação de certificado.
- Os servidores de comunicação validam as credenciais fornecidas pelas impressoras e aceitam as solicitações.
- O aplicativo de gestão de dispositivo autentica os servidores de comunicação e ativa o serviço.

Figura 3



Device Management Application Deployment Model

## 5. Transmissão de dados & Cargas

### Fontes de dados

Os atributos de dados do dispositivo de impressão enviados como parte da carga transmitida são das seguintes fontes:

- Impressoras de rede Xerox® Office
- Impressoras de rede que não são Xerox
- Impressoras Xerox® Production
- Aplicativos de Gestão de Dispositivo Xerox®

**Nota:** Nem todas as impressoras Xerox Office e Xerox Production tem capacidades de Serviços Remotos Xerox. Você pode encontrar uma lista completa de produtos com tal capacidade [aqui](#). Os atributos do dispositivo de impressão variam de acordo com o produto e solução de implementação de Serviços Remotos Xerox®.

### Dispositivos Xerox® Office

**Tabela 1** Identifica os atributos de dados do dispositivo que podem ser transmitidos para produtos Xerox® Office com capacidade de Serviços Remotos.

Atributos de dados	Descrição detalhada de atributos de dados
<b>Identidade do dispositivo de impressão</b>	Inclui modelo, níveis de firmware do módulo, números de série do módulo, datas de instalação do módulo, dados de licença e localização, se disponível.
<b>Endereço de rede do dispositivo de impressão</b>	Inclui Endereço do Controle de Acesso de Mídia (MAC), endereço de sub-rede.
<b>Propriedades do dispositivo de impressão</b>	Inclui configuração detalhada de componente de hardware, configuração detalhada de módulo de software, recursos/serviços compatíveis etc.
<b>Status do dispositivo de impressão</b>	Inclui status ativos, contagens de histórico de falhas, registro de evento DFE, histórico de transmissão de dados
<b>Contadores do dispositivo de impressão</b>	Inclui medidores de faturamento, contadores relacionados à impressão, contadores relacionados à cópia, contadores relacionados a grandes tarefas, contadores específicos de produção, contadores relacionados à digitalização para o destino em modelos de produção low-end etc.
<b>Consumíveis do dispositivo de impressão</b>	Inclui fabricante, modelo, número de série, nome, tipo, nível, capacidade, status, contadores de tempo de vida útil etc.
<b>Uso de máquina detalhado de impressão</b>	Inclui dados HFSI, dados NVM, substituição de peças, registros DFE, dados de diagnóstico detalhados, resolução de falhas.
<b>Engenharia / Depuração</b>	Inclui dados detalhados e não estruturados relacionados à depuração para uso exclusivo do suporte de 3º nível.

Atributos de dados	Descrição detalhada de atributos de dados
<b>Relacionado à tarefa do cliente</b>	Os produtos de impressão Xerox® Production fornecem a capacidade de reproduzir dados relacionados à tarefa no suporte de cenários de suporte escalados através de PostScript criptografado para a Xerox. O cliente pode controlar se deseja ativar este recurso ou não. Se o cliente escolher transmitir dados relacionados à tarefa (ou seja, PostScript criptografados) de volta à Xerox, esses dados são processados de acordo com os padrões e políticas de segurança da informação (IS) da Xerox.

Nossos dispositivos de impressão da categoria de escritório transmitem os atributos de dados do dispositivo em um formato eXtensible Markup Language (XML) utilizando um arquivo .zip comprimido. Uma vez autenticado, cada arquivo é então transmitido através de um canal criptografado para os servidores de comunicação.

## Dispositivos Xerox® Production

**Tabela 2** Identifica os atributos de dados do dispositivo que podem ser transmitidos para produtos Xerox® Production com capacidade de Serviços Remotos.

Descrição	
<b>Identidade do dispositivo de impressão</b>	Inclui modelo, nível de firmware, números de série do módulo e data de instalação.
<b>Endereço de rede do dispositivo de impressão</b>	Inclui Endereço do Controle de Acesso de Mídia (MAC), endereço de sub-rede.
<b>Propriedades do dispositivo de impressão</b>	Inclui configuração detalhada de componente de hardware, configuração detalhada de módulo de software, recursos/serviços compatíveis, modos de economia de energia etc.
<b>Status do dispositivo de impressão</b>	Inclui status geral, alertas detalhados, histórico das últimas 40 falhas, dados de congestionamento etc.
<b>Contadores do dispositivo de impressão</b>	Inclui medidores de faturamento, contadores relacionados à impressão, contadores relacionados à cópia, contadores relacionados a fax, contadores relacionados a grandes tarefas, estatísticas de uso etc.
<b>Consumíveis do dispositivo de impressão</b>	Inclui nome do consumível, tipo (por ex., imagem, finalização, mídia do papel), nível, capacidade, status, tamanho etc.
<b>Uso de máquina detalhado de impressão</b>	Inclui contadores detalhados relacionados à impressão, estados de energia ligada, quantidades de substituição detalhadas de Unidades de Substituíveis do Cliente (CRU), divulgações e dados de falha detalhados de CRU, uso do recurso integrado de Reconhecimento de Personalidade Ótica (OCR), divulgação da duração de tiragem de impressão, divulgação do uso da bandeja de impressão, divulgação do tamanho da mídia, divulgação do tamanho do documento, divulgação, contagens de pixel, cobertura de área média por cor, falhas/congestionamento, contadores detalhados relacionados à digitalização.
<b>Engenharia / Depuração</b>	Inclui informações detalhadas sobre depuração que podem incluir dados além do conjunto de dados listado acima. Estes dados podem incluir PII como nomes de usuários, endereços de e-mail e dados da tarefa. Estes dados são enviados apenas com a permissão expressa do cliente e com finalidade única para suporte de resolução de problemas encaminhado.

Nossos dispositivos de impressão da categoria de escritório transmitem os atributos de dados do dispositivo em um formato eXtensible Markup Language (XML) utilizando um arquivo .zip comprimido. Uma vez autenticado, cada arquivo é então transmitido através de um canal criptografado para os servidores de serviços remotos.

**Nota:** O arquivo e conteúdo dos dados identificados variam dependendo do modelo do produto.

## Aplicativos de Gestão de Dispositivo Xerox®

Há diversas opções de Aplicativos de Gestão de Dispositivos disponíveis com base no ambiente de rede do cliente e na necessidade de gestão do dispositivo de impressão. Cada uma delas é igualmente segura e possui sólidas capacidades de gestão de dispositivo de impressão.

**Segue uma lista de Aplicativos de Gestão de Dispositivos: Xerox CentreWare® Web, Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition e Xerox Device Manager.**

Cada aplicativo sincroniza, por padrão, pelo menos uma vez ao dia com os servidores de comunicação seguros. Para garantir o máximo de segurança para seus dados, os servidores de comunicação são hospedados em uma instalação em conformidade com o ISO 27001. Os dados enviados são primeiramente níveis de suprimento, alertas de impressora e contadores de faturamento específicos da impressora. Os dados são comprimidos, criptografados e protegidos por diversos mecanismos:

- O Aplicativo de Gestão de Dispositivo inicia todo o contato com os servidores de comunicação da Xerox, configurações de firewall padrão no ambiente do cliente são necessárias para permitir a comunicação.
- Os Aplicativos de Gestão de Dispositivo precisam de um proxy válido, no caso de um proxy ser necessário para a comunicação da internet.
- Os servidores de comunicação encontram-se atrás de um firewall seguro no ambiente da Xerox e não são acessíveis pela internet.
- O acesso da interface do usuário do servidor de comunicação da Xerox precisa de autenticação. A informação de hospedagem do Aplicativo de Gestão de Dispositivo é armazenada em uma conta específica para o local do cliente e o acesso a esses dados da conta nos servidores de comunicação da Xerox é restrito aos gerenciadores de conta dos servidores de comunicação da Xerox.
- Toda a comunicação do servidor de comunicação da Xerox é registrada e fica disponível para visualização.
- Os dados enviados para seus dispositivos de impressão em rede, quando habilitados, consistem principalmente de comandos remotos que permitem que um administrador de suporte de conta solicite a execução de nível de comando do Aplicativo de Gestão de Dispositivo da Xerox durante cenários de suporte encaminhados.
- Solicitações envolvem principalmente atualizações de firmware, reinicialização de impressora, impressão de página de teste e atualizações atuais do status de dispositivos.
- O Aplicativo de Gestão de Dispositivo da Xerox apura periodicamente sua conta de servidores de comunicação em relação a solicitações de comando.
- Resultados de operações de solicitações de comando são enviadas para os servidores de comunicação da Xerox onde eles são analisados.

**Nota:** Há uma solicitação de registro de vez única após a instalação do software. Estas informações de registro incluem um campo para localização de dispositivo e e-mail de contato.

Os Aplicativos de Gestão de Dispositivo da Xerox (**Xerox CentreWare® Web, Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition e Xerox Device Manager**) transmitem os dados de atributo no formato eXtensible Markup Language (XML) utilizando um arquivo .zip comprimido. O arquivo é então criptografado e transmitido através de canais criptografados para os servidores de comunicação remotos.

**Tabela 3** Identifica a lista de atributos de dados do dispositivo e descrição que pode ser enviada através do app de gestão do dispositivo Xerox®.

<b>Atributos de dados</b>	<b>Descrição detalhada de atributos de dados</b>
<b>Identidade do dispositivo de impressão</b>	Inclui fabricante, modelo, descrição, nível de firmware, número de série, identificações de ativos, nome do sistema, contato, localização, estação de trabalho (desktop) do estado de gestão, número de telefone e fax e nome da fila.
<b>Endereço de rede do dispositivo de impressão</b>	Inclui endereço MAC, endereço IP, nome DNS, máscara de sub-rede, gateway padrão de IP, último endereço IP conhecido, endereço IP modificado, fuso horário, endereço IPX, número de rede externo IPX, servidor de impressão IPX.
<b>Propriedades do dispositivo de impressão</b>	Inclui componentes instalados, descrição de componentes, recursos/serviços compatíveis, velocidade de impressão, suporte de cor, opções de finalização, suporte duplex, tecnologia de marcação, disco rígido, RAM, suporte de idioma, propriedades definidas pelo usuário.
<b>Status do dispositivo de impressão</b>	Inclui status geral, alertas detalhados, mensagens de console local, status de componente, dados relacionados à recuperação de status, data de busca, tipo/método de busca, tempo de operação do dispositivo, traps compatíveis/habilitadas.
<b>Contadores do dispositivo de impressão</b>	Inclui medidores de faturamento, contadores relacionados à impressão, contadores relacionados à cópia, contadores relacionados a fax, contadores relacionados a grandes tarefas, contadores relacionados à digitalização, estatísticas de uso e volume-alvo.
<b>Consumíveis do dispositivo de impressão</b>	Inclui nome do consumível, tipo (por ex., imagem, finalização, mídia de papel), nível, capacidade, status, tamanho e atributos relacionados
<b>Uso detalhado do dispositivo de impressão</b>	Dados de monitoramento de tarefa com base no usuário que incluem características da tarefa (ID, nome do documento, proprietário, tipo do documento, tipo de tarefa, cor, duplex, mídia necessária, tamanho, páginas, grupos, erros), destino (dispositivo de impressão, modelo, nome DNS, endereço IP, endereço MAC, número de série), resultados das tarefas de impressão (tempo de envio, tempo de impressão da tarefa, páginas impressas, páginas impressas cor/PB, modo de cor utilizado, N-up), dados de contabilidade (código de estorno, preço de estorno, fonte contábil), fonte da tarefa de impressão (estação de trabalho, nome do servidor de impressão/endereço MAC, nome da fila, porta, nome de usuário, ID do usuário), dados de gestão Xerox (enviados para o Xerox Services Manager).
<b>Identidade de gestão do dispositivo</b>	Inclui informações de PC de hospedagem do aplicativo como nome DNS, endereço IP, nome do SistOp, tipo de SistOp, CPU PC, tamanhos da RAM (livre X usada), tamanhos de discos rígidos (livre X usado), nome do local, versão do app, data de validade da licença do app, versão .Net, fuso horário, versão do componente de busca, tamanho da principal base de dados, tamanho da base de dados da busca, nº de impressoras dentro e fora do âmbito, execução de serviços críticos.
<b>Device Manager Modo de segurança corporativo</b>	Modo normal = Xerox Device Agent contata o Xerox Services Manager, diariamente. Configurações podem ser alteradas remotamente sem a necessidade de visitas ao local, mesmo quando as programações de apuração são desligadas. Modo lock down = Além da sincronização de dados relacionados à impressora, não há comunicação com o Xerox Services Manager e as configurações devem ser alteradas no local. Os endereços IP da impressora e equipamento Xerox Device Agent são reportados ao Xerox Services Manager.
<b>Política de controle de impressão da gestão do dispositivo</b>	Inclui nome do PC do usuário final, servidor de impressão utilizado, fila de impressão utilizada, indicação da hora da violação, nome do documento, nome do usuário final, duplex da tarefa, cor da tarefa, impressões totais da tarefa, preço da tarefa, ação tomada, usuário final notificado, mensagem exibida, nome da política de impressão, regra da política de impressão.

## 6. Gestão remota de dispositivos de impressão

O pessoal de suporte encaminhado da Xerox pode processar as seguintes ações através do device direct ou Aplicativo de gestão do dispositivo Xerox.

A Tabela 4 mostra esforços de resolução aprimorados, permitidos pelo cliente em um cenário de suporte encaminhado. A permissão pelo cliente para realizar essas funções deve ser obtida explicitamente.

Dados	Descrição
<p>Ações para realizar em Dispositivos de impressão</p>	<ul style="list-style-type: none"> <li>• Obter status do dispositivo = recuperar o status mais recente do dispositivo de impressão</li> <li>• Reinicializar dispositivo = iniciar uma sequência de desligar e ligar o dispositivo de impressão</li> <li>• Atualizar dispositivo = instalar novo software/firmware no dispositivo de impressão (.DLM na porta 9100)</li> <li>• Dispositivo de resolução de problemas = realizar ping no dispositivo + recuperar último status do dispositivo de impressão</li> <li>• Página de teste de impressão = enviar uma tarefa de teste para um dispositivo de impressão para validar o caminho de impressão (gerar um relatório de configuração)</li> <li>• Iniciar dispositivo de gestão = iniciar transferências periódicas de dados do dispositivo de impressão para os servidores de comunicação externos da Xerox®</li> </ul> <p><b>Nota: O uso de cada ação pode ser desabilitado sob demanda dentro da parte de configuração da administração dos Aplicativos de Gestão de Dispositivo Xerox® compatíveis com este recurso.</b></p>
<p><b>Ações para realizar nos Aplicativos de Gestão de Dispositivo</b></p>	<p>As configurações dentro de cada aplicativo de gestão de dispositivo que podem ser gerenciadas incluem operação de busca, frequência de exportação de dados, configurações relacionadas à comunicação SNMP (tentativas, tempo esgotado, nomes de comunidade), perfis de alerta e frequência de atualização de software do aplicativo de gestão de dispositivo automática.</p>
<p><b>Gestão de software remota</b></p>	<p>Certos dispositivos são equipados com capacidades de gestão de software remota automatizadas. Esses dispositivos enviam uma consulta para o ambiente Xerox para ver se há alguma nova atualização de software disponível para o dispositivo. Se houver, o dispositivo poderá então enviar uma solicitação para essa atualização de software e ele será atualizado no tempo pré-definido. Entretanto, se seu ambiente proíbe atualizações de software automáticas; a opção de gestão de software remota pode ser desmarcada apenas sem a interrupção dos serviços remotos padrão.</p>

## As exigências de sistema para Aplicativos de Gestão de Dispositivo

As exigências mínimas variam ligeiramente de acordo com as ofertas. Consulte o Guia do usuário, Guia de avaliação de segurança e/ou guia de Certificação para exigências básicas específicas para os respectivos aplicativos de gestão de dispositivo.

Após a instalação, um arquivo de leitura é incluído para tratar das exigências adicionais e específicas do sistema para o respectivo aplicativo de gestão de dispositivo ser instalado.

- Os aplicativos de Gestão de Dispositivo são compatíveis com os recursos de segurança desenvolvidos dentro do sistema operacional do Windows®. Eles se baseiam em um serviço Windows® em segundo plano sob as credenciais de conta do sistema local para habilitar o monitoramento proativo de impressoras e a carga de atributos de dados de impressão que será transmitida para a Xerox. A interface do usuário que mostra a carga de atributos de dados de impressão só está acessível por usuários e administradores com acesso ao SistOp Windows®.
- Para evitar uma interrupção das comunicações de serviços remotos automáticos, é recomendado que o aplicativo de gestão do dispositivo seja carregado em um cliente que esteja continuamente ligado ou durante as horas de trabalho padrão.
- Recomendamos que computadores de hospedagem estejam executando um sistema operacional compatível da Microsoft® Corporation. Entretanto, os aplicativos de gestão de dispositivo da Xerox podem ser executados no SistOp Apple® 10.9.4 ou posterior utilizando o software emulador Parallels Desktop. O aplicativo não funcionará em ambiente nativo Macintosh. Veja os respectivos guias de usuário para suporte detalhado. Exigências para executar em um sistema operacional Macintosh podem ser encontradas
- Recomendamos que computadores de hospedagem estejam atualizados com os últimos serviços e patches fundamentais lançados pela Microsoft® Corporation.
- O Network Transmission Control Protocol/Internet Protocol (TCP/IP) deve ser carregado e estar funcionando.
- Privilégios administrativos são necessários para instalar o software do aplicativo de gestão de dispositivo no equipamento do cliente.
- São necessários dispositivos com SNMP habilitados e a possibilidade de rotear SNMP na rede. Não é necessário habilitar SNMP no computador onde os Aplicativos de Gestão de Dispositivo Xerox® serão instalados ou qualquer outro computador de rede.
- Microsoft®.NET Framework deve ser instalado antes de instalar o aplicativo.
- O aplicativo não deve ser instalado em um PC onde outros aplicativos com base em SNMP ou outras ferramentas de gestão Xerox® Print são instaladas, já que interferem nas operações um do outro.

## Configurações de base de dados

- O aplicativo instala arquivos de base de dados e um mecanismo de base de dados SQL Server Compact Edition (SQL CE) que armazena os dados da impressora e configurações do aplicativo dentro do diretório de instalação. Nenhuma licença de base de dados é necessária para o aplicativo. O Xerox® Device Agent também é compatível com instalações existentes de SQL Server, como descrito acima.

## Configurações não compatíveis

Esta seção descreve as configurações que não são compatíveis.

- Instalação do aplicativo em um computador com outro aplicativo de gestão de dispositivo Xerox, como o Xerox Device Manager.
- Software de sistema operacional Mac OS® nativo (ou seja, Xerox Device Agent só pode ser executado na plataforma Mac da Apple quando o software Parallels Emulation estiver instalado.)
- Qualquer versão de sistemas operacionais UNIX®, sistemas operacionais Linux®, sistemas Windows® rodando o cliente Novell, Windows® 7, Windows® XP, Windows® Vista, Windows N® 4.0, Windows Media® Center, Windows® 2000, Windows® Server 2008 e 2008 R2, Windows20® Server 2003, Windows® 8 RT, sistemas operacionais executando Serviços Terminais para aplicativos e instalação em sistemas Windows executando controladores de domínio.

Já que este aplicativo foi testado apenas em ambiente de estação de trabalho/VMware® Lab Manager, outros ambientes virtuais não são compatíveis.



## 7. Serviços e Processos de Negócios Xerox®

Os dados recebidos dos dispositivos de impressão com base no Xerox® Office, dispositivos de impressão com base no Xerox® Production e Aplicativos de Gestão de Dispositivo da Xerox como parte de uma solução de serviços remotos são utilizados pelos processos de negócios Xerox listados abaixo:

A Tabela 5 detalha o nome e descrição dos serviços e processos de negócios que são compatíveis como parte de uma solução de Serviços Remotos.

Nome do processo de negócios	Descrição
<b>Leituras Automáticas dos Contadores</b>	Dados de leitura dos contadores são utilizados no processo de faturamento.
<b>Reposição Automática de Suprimentos / Reposição Automática de Peças</b>	O toner é automaticamente enviado para clientes com base no status de esgotamento de consumíveis recebido dos dispositivos de impressão. Certos componentes substituíveis são enviados automaticamente aos clientes conforme necessidade de seus dispositivos de impressão.  Essas opções estão disponíveis apenas aos clientes que optam por contratos de suprimento medido.
<b>Operacionalidade (Assistente de manutenção)</b>	A Gestão remota do dispositivo fornece informações de falha detalhadas que podem ser visualizadas pelo pessoal de serviço da Xerox, quando necessário, para agilizar a preparação para uma visita local ou diagnosticar e resolver problemas.
<b>Suporte de 3º nível (Engenharia / Depuração)</b>	O pessoal de suporte de produto pode depurar problemas difíceis ao dar acesso a registros de depuração e engenharia detalhados.
<b>Desenvolvimento de produto</b>	Desempenho de impressora e dados de uso são utilizados para identificar melhorias de produtos para lançamentos futuros.

Dados básicos do dispositivo de impressão são agregados, transmitidos, retidos e arquivados dentro de um data center da Xerox certificado pelo ISO-27001 e é mantido de acordo com as políticas de retenção de processamento de dados.

As práticas e processos de trabalho que são compatíveis e protegem os sistemas de software de serviços remotos são baseados nas melhores práticas e Políticas de segurança da informação da Xerox que alinha-se diretamente com os padrões do sistema de gestão de segurança da informação da Organização de Padrões Internacionais ISO 27002. Os clientes podem ter a certeza de que a gestão, proteção e armazenamento dos dados do dispositivo compreendem os princípios básicos da segurança da informação: confidencialidade, integridade, disponibilidade, autenticação e não rejeição.

## 8. Detalhes da tecnologia

Esta seção fornece detalhes técnicos adicionais que normalmente são necessários pelas equipes de Tecnologia da Informação (TI) e agentes de segurança que gerenciam riscos ao obter a garantia de práticas de desenvolvimento seguras. Tal garantia permite que eles certifiquem nossos dispositivos de impressão e aplicativos de gestão de dispositivo para uso dentro do ambiente de rede do cliente.

### Design do software

Nosso compromisso com a segurança dos produtos Xerox começa no início do desenvolvimento do produto onde os desenvolvedores da Xerox seguem um ciclo de vida de desenvolvimento de segurança formal que gerencia problemas de segurança através da identificação, análise, priorização, codificação e testagem. Muitos dispositivos de impressão Xerox® têm certificação Common Criteria ISO IEC 15408 ou estão ativamente sob análise de certificação.

### Operabilidade

Os serviços remotos da Xerox realizam os seguintes tipos de operações em uma rede. Essas operações dependem do método de implementação configurado.

Tabela 6.

Método de implementação	Aplicativo utilizado	Fluxo de dados na rede	Operabilidade aplicada em uma rede
Dispositivo Direto	Nenhum	Interno	Dispositivo de Impressão Xerox® tenta detectar um servidor web proxy (automático ou direcionado para um endereço específico)
		Interno	Dispositivos de Impressão Xerox® podem ser programados para gerar solicitações para um servidor Simple Mail Transport Protocol (SMTP) para enviar mensagens de e-mail com notificações de alerta para uma lista de destinatários definidos
		Externo à rede	O Dispositivo de Impressão Xerox® atravessa o firewall da empresa para acessar a Internet (HTTPS na porta 443)
		Externo à rede	O Dispositivo de Impressão Xerox® autentica com seu certificado para o servidor de comunicação remoto da Xerox para transmitir qualquer atributo de dados
		Externo à rede	O Dispositivo de Impressão Xerox® transmite automaticamente dados de atributos do dispositivo de impressão através de um canal criptografado (HTTPS na porta 443) para os servidores de comunicação da Xerox® em um momento específico diariamente ou após solicitação do cliente.

Método de implementação	Aplicativo utilizado	Fluxo de dados na rede	Operabilidade aplicada em uma rede
		Externo à rede	O Dispositivo de Impressão Xerox® consulta automaticamente os servidores de comunicação da Xerox® através de um canal criptografado (HTTPS na porta 443) em um momento específico todos os dias para uma lista de ações a realizar (por ex., enviar dados de faturamento agora, adicionar serviço etc.)
		Externo à rede	Transmissões sob demanda de via única dos dados de registro de engenharia de dispositivo de impressão da Xerox® através de um canal criptografado (HTTPS na porta 443) para o servidor de comunicação da Xerox®
Dispositivo Direto	Nenhum	Saída, iniciado por dispositivo para puxar último software	O dispositivo envia uma consulta para o servidor de gestão de software remota para verificar a existência de atualizações de segurança / software. Se o ambiente do cliente proíbe atualizações de software automáticas, a opção de gestão de software remota pode ser desmarcada apenas sem a interrupção dos serviços remotos padrão.
Aplicativos de gestão do dispositivo	Centre Ware® Web	Interno	Cada app detecta um servidor web proxy (automático ou direcionado para um endereço específico)
		Interno	Cada app recupera as capacidades do dispositivo de impressão na frota via SNMP
		Interno	Cada app recupera as configurações do dispositivo de impressão na frota via SNMP
		Interno	Cada app recupera o status do dispositivo de impressão na frota via SNMP
		Interno	Cada app recupera os dados de suprimentos do dispositivo de impressão na frota via SNMP
		Interno	Cada app reinicia um dispositivo de impressão via SNMP ou via Interface do Usuário na internet do dispositivo de impressão
		Interno	Cada app pode enviar uma página de teste para um dispositivo de impressão específico
		Interno	Cada app pode iniciar uma página da internet do dispositivo de impressão
		Externo (apenas saída)	Cada app atravessa o firewall da empresa para acessar a Internet (HTTPS na porta 443)
		Externo (apenas saída)	Cada app autentica com seu certificado para o servidor de comunicação remoto da Xerox para transmitir qualquer atributo de dados
		Externo (apenas saída)	Cada app transmite automaticamente dados de atributos do dispositivo de impressão através de um canal criptografado (HTTPS na porta 443) para os servidores de comunicação da Xerox® em um momento específico todos os dias
		Externo (apenas saída)	Cada app consulta automaticamente os servidores de comunicação da Xerox® através de um canal criptografado (HTTPS na porta 443) em um momento específico todos os dias para uma lista de ações a realizar

Método de implementação	Aplicativo utilizado	Fluxo de dados na rede	Operabilidade aplicada em uma rede
Aplicativos de gestão do dispositivo	Xerox	Interno	Cada app Xerox Device Agent detecta um servidor web proxy (automático ou direcionado para um endereço específico)
		Interno	Cada app Xerox Device Agent recupera as capacidades do dispositivo de impressão na frota via SNMP
		Interno	Cada app Xerox® Device Agent recupera as configurações do dispositivo de impressão na frota via SNMP
		Interno	Cada app Xerox Device Agent recupera o status do dispositivo de impressão na frota via SNMP
		Interno	Cada app Xerox Device Agent recupera os dados de suprimentos do dispositivo de impressão na frota via SNMP
		Interno	Cada app Xerox Device Agent pode solicitar que o dispositivo imprima um relatório de configuração
		Interno	Cada app Xerox Device Agent pode iniciar uma página da internet do dispositivo de impressão
		Interno	Cada app Xerox Device Agent pode atualizar o software do dispositivo de impressão através do envio de tarefa de impressão. (. Arquivo DLM na porta 9100)
		Externo (apenas saída)	Cada app Xerox Device Agent atravessa o firewall da empresa para acessar a Internet (HTTPS na porta 443)
		Externo (apenas saída)	Cada app autentica com seu certificado para o servidor de comunicação remoto da Xerox para transmitir qualquer atributo de dados
		Externo (apenas saída)	Cada app Xerox Device Agent transmite automaticamente dados de atributos do dispositivo de impressão através de um canal criptografado (HTTPS na porta 443) para os servidores de comunicação da Xerox® em um momento específico todos os dias
		Externo (apenas saída)	Cada app Xerox Device Agent consulta automaticamente os servidores de comunicação através de um canal criptografado (HTTPS na porta 443) em um momento específico todos os dias para uma lista de ações a realizar
		Interno	Aplicativos Xerox Device Manager / Xerox Device Agent detectam um servidor web proxy (automático ou direcionado para um endereço específico)
		Interno	Aplicativos Xerox Device Manager / Xerox Device Agent recuperam as capacidades do dispositivo de impressão na frota via SNMP
		Interno	Aplicativos Xerox Device Manager / Xerox Device Agent recuperam a configuração do dispositivo de impressão na frota via SNMP
		Interno	Aplicativos Xerox Device Manager / Xerox Device Agent recuperam o status do dispositivo de impressão na frota via SNMP

Método de implementação	Aplicativo utilizado	Fluxo de dados na rede	Operabilidade aplicada em uma rede
Aplicativos de gestão do dispositivo	Xerox® Device Manager para monitorar dispositivos de impressão conectados por rede	Interno	Aplicativos Xerox Device Manager / Xerox Device Agent recuperam os dados de suprimentos do dispositivo de impressão na frota via SNMP
		Interno	Aplicativos Xerox Device Manager / Xerox Device Agent podem solicitar que o dispositivo imprima um relatório de configuração
		Interno	Aplicativos Xerox Device Manager / Xerox Device Agent podem iniciar uma página da internet do dispositivo de impressão
		Interno	Aplicativos Xerox Device Manager / Xerox Device Agent podem atualizar o software do dispositivo de impressão através do envio de tarefa de impressão
		Interno	O app Xerox Device Manager é compatível com comunicações SNMPv3 com dispositivos de impressão
		Interno	O app Xerox Device Manager pode realizar mudanças na configuração do dispositivo de impressão através de SNMP e Interface do Usuário na Internet
		Interno	O app Xerox Device Manager recupera registros de contabilidade de certos MFPs da Xerox®
		Interno	O app Xerox Device Manager gerencia / aplica as políticas de controle de impressão
		Externo (apenas saída)	Aplicativos Xerox Device Manager / Xerox Device Agent atravessam o firewall da empresa para acessar a Internet (HTTPS na porta 443)
		Externo (apenas saída)	Cada app autentica com seu certificado para o servidor de comunicação remoto da Xerox para transmitir qualquer atributo de dados
		Externo (apenas saída)	Aplicativos Xerox Device Manager / Xerox Device Agent transmitem automaticamente dados do dispositivo de impressão para os servidores de comunicação da Xerox® através de um canal criptografado (HTTPS na porta 443) em um momento específico todos os dias
		Externo (apenas saída)	Aplicativos Xerox Device Manager / Xerox Device Agent consultam automaticamente os servidores de comunicação da Xerox através de um canal criptografado (HTTPS na porta 443) em um momento específico todos os dias para uma lista de ações a realizar
	Aplicativo de gestão do dispositivo	Externo, bidirecional	O Xerox Device Manager contata o Xerox Services Manager diariamente e permite que os administradores alterem as configurações remotamente, evitando a necessidade de chamadas de serviço no local.

## 9. Recursos de segurança

### **SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) PARA A XEROX®**

O Simple Network Management Protocol (SNMP) é a ferramenta de gerenciamento de rede mais utilizada para comunicações entre sistemas de gerenciamento de rede e impressoras em rede. Os Aplicativos de gestão do dispositivo utilizam o SNMP durante operações de busca para recuperar informações detalhadas do dispositivo de impressão. Os Aplicativos de Gestão de Dispositivo Xerox® são compatíveis com protocolos SNMP v1/v2 e v3. Consulte o respectivo guia de certificação do Aplicativo de Gestão de Dispositivo Xerox® para obter detalhes específicos.

A estrutura SNMP v3 é compatível com vários modelos de segurança, que podem existir simultaneamente em uma entidade SNMP. SNMPv3 inclui uma segurança mais restrita adicionando segurança criptográfica à SNMPv2. Além disso, SNMPv3 é compatível com versões anteriores e é amplamente utilizada em redes robustas.

Aplicativos de gestão do dispositivo da Xerox (Centre Ware® Web / Xerox Device Manager, Xerox Device Agent) podem se comunicar com plataformas de dispositivos que estão em conformidade com o Federal Information Processing Standard FIPS 140-2 em suas implementações de SNMPv3.

Os Aplicativos de gestão do dispositivo da Xerox não utilizam o serviço SNMP do Windows ou o serviço SNMP Trap do Windows. Se instalados anteriormente, esses serviços devem ser desabilitados em qualquer computador pessoal (PC) ou servidor onde o Aplicativo de gestão do dispositivo da Xerox estiver instalado.

Os Aplicativos de gestão do dispositivo da Xerox utilizam um agente SNMP desenvolvido pela Xerox que:

- Contém um mecanismo especial de codificação/decodificação
- É completamente gerenciado por .NET
- Utiliza executáveis de tempo de duração .NET - fornece maior segurança para prevenir ataques contra vulnerabilidades de softwares como manipulações de cursor inválido, buffer excedido e verificação de limites.

Os Aplicativos de gestão do dispositivo da Xerox utilizam os recursos de segurança disponíveis do sistema operacional (OS) Windows incluindo:

- Autorização e autenticação do usuário
- Gestão e configuração de serviços
- Gestão e implantação de política de grupo

Internet Connection Firewall (ICF) do Windows incluindo:

- Configurações de registro de segurança
- Configurações ICMP

Aplicativos de Gestão de Dispositivo da Xerox: **Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition**, SQL CE application Microsoft® SQL Server e **Xerox Device Manager** utilizam Microsoft® SQL Server.

Os Aplicativos de Gestão de Dispositivo da Xerox podem ser configurados para trazer os recursos de segurança adicionais da Microsoft® para incluir, se aplicável:

- Habilitar registro de conta do usuário
- Criptografia de Domain Name System (DNS)
- Limite de privilégios de conta do usuário para acessar a base de dados (ou seja, direitos de proprietário da base de dados)
- Implementação de números de porta definidos por usuário

Uma chave de registro da Xerox e uma conta Xerox válida para transmitir dados para os servidores de comunicação da Xerox.

As comunicações externas dos Aplicativos de Gestão de Dispositivo da Xerox podem ser impactadas pelo Windows Internet Connection Firewall. (**Recomendamos** que os clientes coloquem o URL da Xerox na lista de autorizações do firewall do cliente (\*.support.xerox.com) e especifique o endereço IP que pode acessar o URL.)

Os Aplicativos de Gestão de Dispositivo da Xerox rodam como um processo em segundo plano utilizando credenciais de conta de sistema local para automaticamente consultar dispositivos de impressão de rede via SNMP e transmitir periodicamente atributos de dispositivo de impressão de volta para os servidores de comunicação da Xerox.

O acesso à interface do usuário (UI) e recursos do aplicativo de gestão do dispositivo da Xerox são controlados através dos seguintes privilégios com base em funções:

- Centre Ware® Web Administrators, Centre Ware® Web Power Users, Centre Ware® Web SQL Users, Centre Ware® Web Customer Administrators e grupos Centre Ware® Web Customers.
- Nomes de usuários e senhas para os aplicativos não atravessam a rede; ao invés disso, tokens de acesso são utilizados (design do SistOp Windows)
- Os Aplicativos de Gestão de Dispositivo da Xerox fornecem segurança com base no controle do envio de impressão ao restringir tarefas com base em política de uso de cor, tipo de documento, custo da tarefa, hora do dia, controle de acesso a grupo de usuário, política de duplex, impressões da tarefa permitida e cotas de impressão.

**Nota:** O uso de SNMP pelo aplicativo de Serviços Remotos da Xerox® não representam um risco de segurança para o ambiente de TI de um cliente porque todo o tráfego gerado com base em SNMP ou consumido por esses aplicativos ocorre dentro da intranet do cliente, atrás do firewall. O serviço de SNMP do Windows e o serviço SNMP Trap do Windows não é habilitado dentro do SistOp do Windows por padrão.

## Modo de segurança corporativa

A sincronização **programada** pelo aplicativo Xerox Device Agent para o servidor de comunicação seguro é definida como diária, por padrão. Observe que a hora do dia pode ser definida para um horário escolhido.

Há dois modos de segurança corporativa existentes: **Normal** e **Lock Down**.

Quando definido para **Normal**, o Aplicativo de gestão do dispositivo contata o Xerox Services Manager diariamente. Configurações podem ser alteradas sem a necessidade de visitas ao local, mesmo quando as programações de apuração são desligadas. (**Modo recomendado**)

No modo **Lock down**, além da sincronização de dados relacionados à impressora, não há comunicação com os servidores de comunicação e as configurações devem ser alteradas no local. Além disso, os endereços IP da impressora e equipamento Xerox Device Agent não são reportados ao servidor de comunicação. Este modo limita todos os outros benefícios de serviços remotos para incluir faturamento automático e fornecimentos, bem como dados de diagnóstico utilizados para suporte técnico.

**Nota:** Se uma versão do Xerox Device Agent não contiver a aba de Modo de segurança corporativa, ela opera no modo Normal.



## 10. Impacto de rede

As diretrizes de rede da empresa normalmente habilitarão ou desabilitarão portas de rede específicas em roteadores e/ou servidores. A maioria dos departamentos de TI se preocupa com as portas utilizadas pelo aplicativo para tráfego enviado. Desabilitar portas específicas podem impactar a funcionalidade do aplicativo. Consulte a tabela abaixo para saber sobre portas específicas utilizadas pelos processos do aplicativo. Se o aplicativo precisa escanear em vários segmentos de rede ou sub-redes, os roteadores devem permitir os protocolos associados com esses números de porta.

### Protocolos, portas e outras tecnologias relacionadas

Tabela 7 Identifica os protocolos, portas e tecnologias utilizadas dentro dos Serviços Remotos da Xerox®:

Número da porta	Protocolo	Descrição da utilização	Fluxo de dados na rede
Dependente de protocolos de camadas superiores	(Protocolo de Internet)	Transporte subjacente para todas as comunicações de dados	Interno + Externo (apenas saída)
NA	protocolo de mensagens de controlo da Internet	Busca de dispositivo de impressão + resolução de problemas	Interno
25	Protocolo de Transferência de Correio Simples (Simple Mail Transport Protocol)	Dispositivo de impressão + alertas de notificação por e-mail de app Proxy remoto	Interno
53	Serviços de nome de domínio (DNS)	Utilizado para operações de busca de dispositivos de impressão com base em DNS	Interno
80	Protocolo de Transporte de Hipertexto (HTTP)	Consultas de páginas da internet de dispositivos de impressão + consultas de páginas da internet de Aplicativo de gestão do dispositivo	Interno
135	chamada de procedimentos remotos	Busca de dispositivo de impressão	Interno

<b>Número da porta</b>	<b>Protocolo</b>	<b>Descrição da utilização</b>	<b>Fluxo de dados na rede</b>
<b>161</b>	Protocolo de Gerenciamento de Rede Simples SNMP v1/v2c/v3	Protocolo padrão do setor utilizado para buscar dispositivos de impressão na rede + Recuperar status, medidores e dados de suprimento + Recuperar e aplicar configurações de dispositivo de impressão. Nomes de comunidade padrão = "público" (GET), "privado" (SET)	Interno
<b>443</b>	Protocolo de Transporte de Hipertexto Seguro (HTTPS)	Consultas de página da internet seguras de dispositivo de impressão (se configurado) + Consultas de página da internet seguras de app Proxy remoto (se configurado) + Transferência de dados do dispositivo de impressão de volta para os servidores de comunicação da Xerox® + comunicações de controle de impressão de volta para o Xerox® Device Manager	Interno + Externo (apenas saída)
<b>515, 9100, 2000, 2105</b>	TCP/IP LPR e Envio de tarefa de impressão de Raw Port	Atualização de software do dispositivo de impressão + Diagnóstico de página de teste de impressão	Interno

## 11. Melhores práticas de segurança

- Sempre manter dispositivos de impressão atualizados com o software/firmware mais recente. A Xerox monitora de perto as vulnerabilidades e fornece proativamente aos clientes atualizações e patches de segurança, quando necessário.
- Desabilitar protocolos e portas não utilizadas em dispositivos de impressão onde possível. Isso normalmente é feito na interface do usuário (UI) na internet de dispositivos de impressão de categoria de escritório e interfaces de usuário (UI) locais de dispositivos de impressão de categoria de produção.
- Utilize recursos relacionados a controle do acesso de usuário em dispositivos de impressão, se disponível. Isso normalmente é feito na interface do usuário (UI) na internet de dispositivos de categoria de escritório e interfaces de usuário (UI) locais de dispositivos de impressão de categoria de produção.
- Utilize protocolos seguros quando possível. Isso normalmente é feito na interface do usuário (UI) na internet de dispositivos de impressão com base em escritório e interfaces de usuário (UI) locais de dispositivos de impressão com base em produção.
- Habilite recursos de segurança integrados do dispositivo (por ex., sobreposição de imagem, criptografia de dados de escaneamento, criptografia de fluxo de impressão, criptografia de disco, impressão segura, pdf criptografado, autenticação de acesso CAC/PIV.)

Para encontrar informações adicionais em relação a serviços remotos na Xerox, visite o site [Xerox.com/RemoteServices](https://www.xerox.com/RemoteServices).

Para informações adicionais e específicas em relação às capacidades e mecanismos de segurança dentro do conjunto de Aplicativos de Gestão de Dispositivo da Xerox, veja seus respectivos guias:

[Xerox Device Agent](#)

[Xerox Device Manager](#)

[Centre Ware Web](#)

Seja para a segurança do dispositivo ou do conteúdo, a Xerox está na linha de frente com uma segurança proativa para as iminentes ameaças de hoje em dia. Visite [www.xerox.com/security](https://www.xerox.com/security) para acessar uma grande variedade de informações de segurança, atualizações, boletins, documentos, patches e mais.