Xerox® Remote Services

Lista branca de segurança

Versão 2,0

Serviços Remotos Globais

Gerenciamento de informações de tecnologia Xerox®

Janeiro de 2017

BR19369

Ocorrem alterações periodicamente neste documento. Alterações, imprecisões técnicas e erros tipográficos serão corrigidos em edições posteriores.

IS 614672/IS 514590

Versão do documento: 2.0 (janeiro de 2017).

Índice

Finalidade geral e público

A finalidade deste documento é servir como um guia para a implantação do Xerox® Remote Services para impressoras Xerox e não-Xerox conectadas em rede no ambiente do cliente. Ele foi idealizado para oferecer detalhes relacionados à segurança e inclui medidas de segurança abrangentes que são implementadas no Xerox® Remote Services.

O público-alvo para este documento inclui fornecedores técnicos, gerentes de rede de TI e profissionais de segurança de TI interessados nos recursos do Remote Services (serviços remotos) e na implementação de segurança desses recursos.

Recomendamos que o documento seja revisto na íntegra para certificar o uso dos produtos e serviços Xerox® em um ambiente em rede do cliente.

Remote Services

A informação é um recurso fundamental e a segurança é primordial para todos os equipamentos de empresas, incluindo dispositivos de impressão multifuncionais (MFPs) conectados em rede. No tipo de estrutura "multifuncional", gerenciar um parque de dispositivos de impressão multifuncionais e, ao mesmo tempo, garantir um nível aceitável de segurança apresenta vários desafios específicos que, frequentemente, são ignorados. A Xerox® entende esta complexidade e responde às necessidades de segurança de nossos clientes. Os produtos e sistemas Xerox® e o Xerox® Remote Services foram concebidos para integrar com segurança os fluxos de trabalho existentes de clientes, ao mesmo tempo que empregam as tecnologias de proteção mais recentes.

O documento técnico sobre segurança do Xerox® Remote Services foi idealizado para ajudar o cliente a entender e implementar a solução Remote Services de proteção apropriada, que seja compatível com a infraestrutura da rede. O desenvolvimento da rede do cliente determinará se será necessário fazer mudanças no firewall da Internet, servidores proxy da Web ou qualquer outra infraestrutura de rede relacionada à segurança. A solução Xerox® Remote Services, o dispositivo e os controles escolhidos dependem das políticas de segurança das informações (IS) do cliente e determinarão qual modo de operação será usado.

O recurso Xerox® Remote Services está disponível em determinados modelos de equipamento. Este recurso permite aos dispositivos de impressão serem atendidos remotamente e receberem suporte através dos dados de atributos do dispositivo de impressão, que incluem*: identidade e propriedades dos dispositivos de impressão, status, níveis de consumíveis, dados de uso e dados de diagnósticos detalhados*. Os dados de atributos do dispositivo de impressão são transmitidos do ambiente em rede do cliente, diretamente do dispositivo de impressão (device direct), através de um aplicativo hospedado (aplicativo de gerenciamento de dispositivos), ou através de uma combinação dos dois métodos, utilizando o trajeto de comunicação seguro do Xerox® Remote Services. Os dispositivos Xerox® e os aplicativos de gerenciamento de dispositivos Xerox® têm um certificado para a autenticação com os Xerox® Communication Servers, para que a transmissão dos atributos de impressão possa ocorrer. As transações do Xerox® Remote Services sempre têm origem no ambiente do cliente e são enviadas estritamente com base nas autorizações do cliente.

Os Xerox® Communication Servers com base nos Estados Unidos estão em conformidade com os rigorosos requisitos de segurança para o Gerenciamento de Segurança das Informações. Os datacenters da Xerox® e o aplicativo Xerox® Remote Services mantêm os requisitos de conformidade com o Statement on Standards for Attestation (SSAE) No-16 anual, Lei Sarbanes-Oxley (Sarbanes-Oxley Act ou SOX) e têm certificação ISO 27001:2013.

Por padrão, nenhuma imagem do cliente decorrente de ações de impressão, fax, digitalização e cópia ou informações confidenciais são transmitidas para os Xerox® Communication Servers.

Controles do cliente

Os aplicativos de gerenciamento de dispositivos Xerox® têm capacidade de exibir os registros de dados de atributos do dispositivo de impressão para fins de auditoria e verificação, antes da criptografia e transmissão para os Xerox® Communication Servers remotos. Consulte o Xerox® Device Management Application User Guide (Guia do usuário de aplicativos de gerenciamento de dispositivos Xerox®), para obter detalhes específicos.

Alguns dispositivos de impressão de escritórios de pequeno e médio porte são equipados com um recurso que permite aos clientes baixar e visualizar os dados de atributos do dispositivo de impressão, antes da criptografia e transmissão para os Xerox® Communication Servers remotos através do método de ativação Device Direct. Para verificar se um dispositivo de impressão específico tem esta capacidade, vá até a página do Centreware Internet Services do dispositivo de impressão; guia Status, link Smart eSolutions (ou Remote Services) e guia Maintenance Assistant (Assistente de manutenção).

A solução Xerox® Remote Services pode ser adaptada para atender às políticas de IS do cliente, que limitam ou restringem rigorosamente determinados tipos de atributos do dispositivo de impressão que podem ser transmitidos para fora da rede (por ex.: atributos relacionados ao endereço de rede). As ferramentas do aplicativo de gerenciamento de dispositivos Xerox® têm capacidade para desativar campos selecionados da transmissão.

Os clientes também têm a opção de requerer uma *Solicitação de exceção* durante as negociações de contrato para **"opt-out"** (não adesão) da solução Remote Services. Essa opção impede toda a comunicação do Remote Services e a capacidade de suporte remoto para os dispositivos de impressão nesta conta.

Para facilitar as atividades escalonadas de suporte remoto, os clientes podem, conforme for necessário, ativar o recurso Remote Access (Acesso remoto) para receber versões de software do dispositivo de impressão, correções de segurança e diagnosticar, reparar ou modificar remotamente configurações do dispositivo de impressão para corrigir qualquer mau funcionamento diagnosticado. O Acesso remoto não permitirá à Xerox® visualizar ou fazer download de documentos, dados e outras informações do cliente, que residam em ou passem através do dispositivo de impressão ou por sistemas de informação do cliente. Há uma exceção para esse caso, que ocorre quando um cliente está trabalhando com uma equipe de suporte da Xerox em um problema mais difícil e se determina que informações adicionais podem ser necessárias para a solução do problema. Nessa hora, o cliente pode decidir dar permissão à Xerox para acessar os registros armazenados localmente no dispositivo, que incluem dados confidenciais.

Por isso, as equipes de TI (Tecnologia da Informação) e profissionais de segurança da empresa são incentivados a ler este documento em sua totalidade para efetivamente entenderem os vários recursos, requisitos e operações do Xerox® Remote Services e também se certificarem da conformidade que apresentam com as políticas de IS de nossos clientes.

Recursos de segurança adicionais para a proteção de dados de segurança de produtos Xerox®, parcerias do setor e certificações podem ser localizados em http://www.xerox.com/security.

Modelos de implantação

Os clientes podem escolher entre os seguintes modelos, igualmente seguros, de implantação do Xerox® Remote Services:

- **Modelo Device Direct** - a opção Device Direct habilita os dispositivos de impressão a se comunicarem diretamente com os Xerox® Communication Servers remotos por meio da Internet e através do firewall do cliente.

- **O modelo de aplicativo de gerenciamento de dispositivo** - um aplicativo de gerenciamento de dispositivos Xerox® (também conhecido como gerenciamento de dispositivos) pode ser implantado em uma rede do cliente para coletar um subconjunto de atributos de dados dos dispositivos de impressão. Vários atributos de dispositivos de impressão são coletados e depois transmitidos com segurança para os Xerox® Communication Servers remotos.

- **Modelo combinado** – a implementação de ambos os modelos de aplicativos Device Direct e Gerenciamento de dispositivos

Todos os modelos de implementação para o Xerox® Remote Services se beneficiam dos protocolos com base na Web e portas padrão da indústria para estabelecer um canal seguro e criptografado para transmitir atributos de dispositivos de impressão aos Xerox® Communication Servers, localizados nos datacenters protegidos e redundantes da Xerox®.

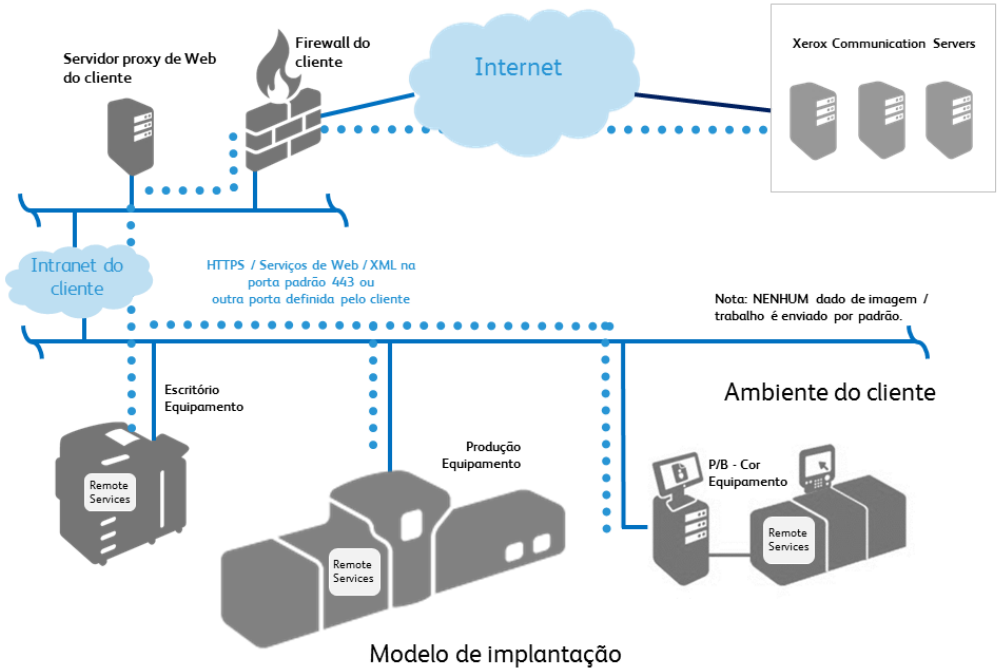
O modelo de implantação escolhido depende das políticas e regras de IS de nossos clientes para lidar com a transmissão dos atributos de dispositivos de impressão e o tipo de solução de serviço de impressão e dispositivos adquiridos da Xerox® (serviços de impressão básicos ou gerenciados).

Modelo de implantação Device Direct

O módulo de serviços remotos integrado nos dispositivos Xerox® utiliza uma conexão TLS (Transport Layer Security) 1.2 na porta padrão 443 para se comunicar externamente com os Xerox® Communication Servers remotos.

- Os dispositivos de impressão no ambiente do cliente iniciam diretamente todas as comunicações com os Xerox® Communications Servers remotos. Para ativar a comunicação, são necessárias as configurações do firewall padrão no local.
- Um URL válido para os Xerox® Communications Servers remotos deve ser utilizado.
- Os Xerox® Communication Servers ficam atrás de um firewall seguro e não são acessíveis pela Internet.

Figura 1



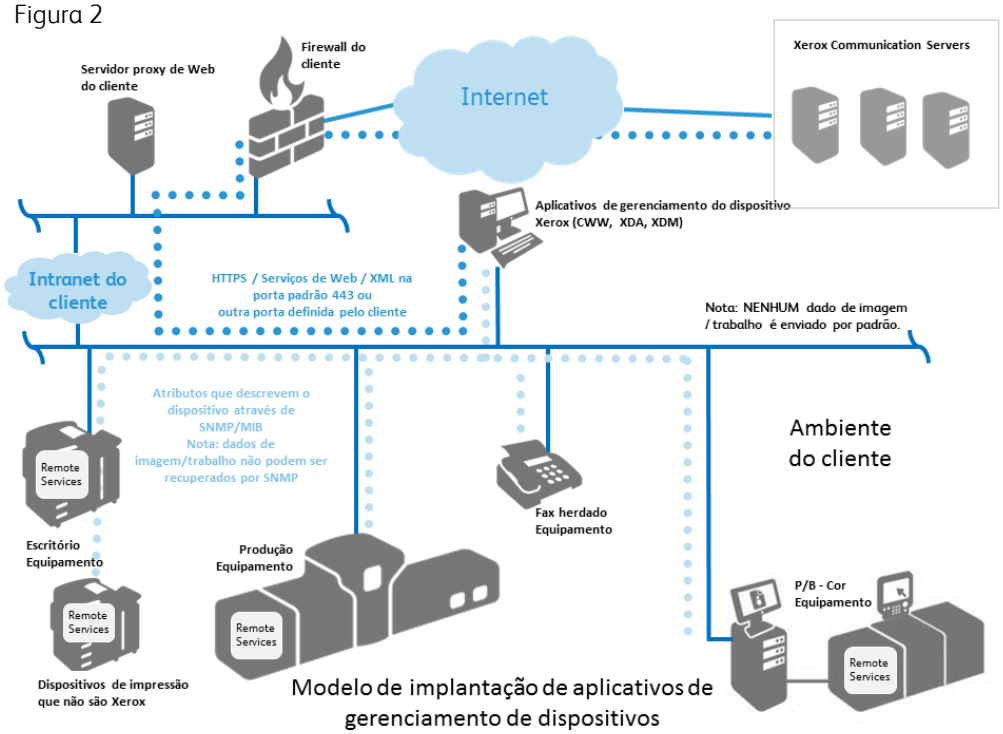
Modelo de implantação Device Direct

Modelo de implantação de aplicativos de gerenciamento de dispositivos

Os aplicativos de Gerenciamento de Dispositivos (isto é: **Xerox® Centre Ware® Web, Xerox® Device Agent, Xerox® Device Agent Partner Edition e Xerox® Device Manager)** também utilizam uma conexão criptografada segura TLS (Transport Layer Security) 1.2 sobre a porta 443 padrão para se comunicar externamente com os Xerox® Communication Servers remotos. Recursos adicionais, que são potencializados para aprimorar a segurança por este canal e são estabelecidos durante a instalação inicial dos aplicativos de Gerenciamento de Dispositivos, incluem:

- O aplicativo de Gerenciamento de Dispositivos no ambiente do cliente inicia todas as comunicações com os Xerox® Communications Servers remotos. Para ativar a comunicação, são necessárias as configurações do firewall padrão no local.
- Um URL válido para os Xerox® Communications Servers remotos deve ser utilizado.
- Os Xerox® Communication Servers ficam atrás de um firewall seguro e não são acessíveis pela Internet.
- Um ID de conta válido ou um identificador de local e a chave de registro do Xerox® Communications Server devem ser utilizados para acessar alguns serviços nos Xerox® Communication Servers.
- O aplicativo de gerenciamento de dispositivos solicita um registro com os Xerox® Communications Servers remotos utilizando as credenciais apropriadas de autenticação do certificado.
- Os Xerox® Communications Servers remotos validam as credenciais fornecidas e aceitam as solicitações.
- O aplicativo de Gerenciamento de Dispositivos autentica os Xerox® Communications Servers remotos e ativa o serviço.

Figura 2

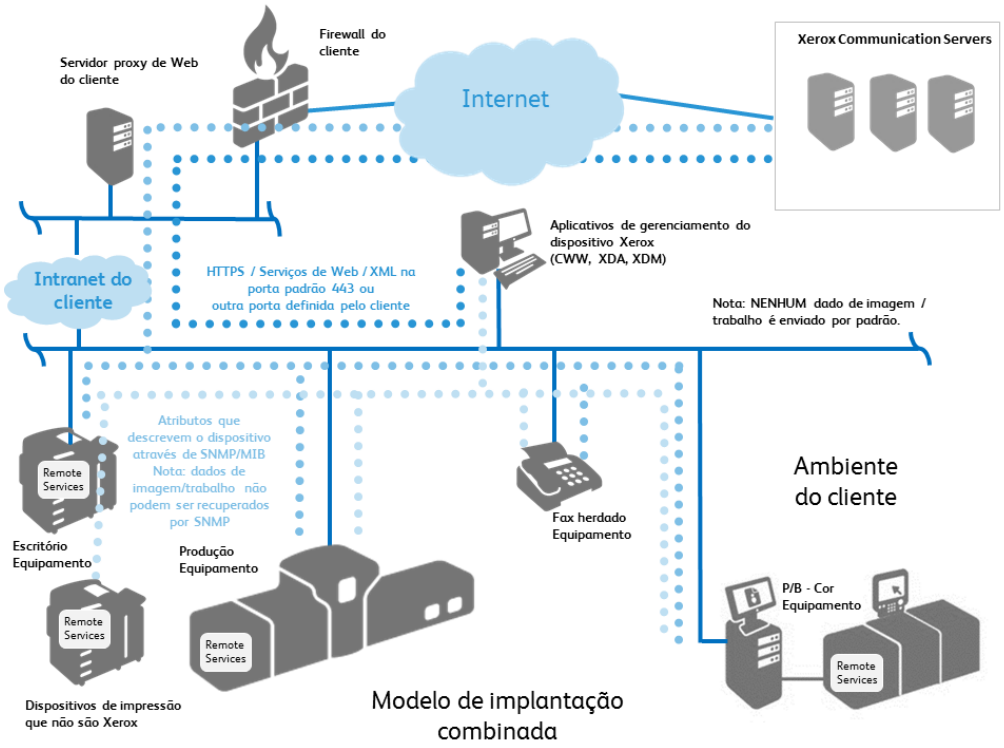


Modelo de implantação de aplicativos de gerenciamento de dispositivos

Modelo de implantação combinada

A implantação combinada é implementada sempre que um cliente adquire vários tipos de contratos de manutenção Xerox para os dispositivos de impressão. Quando um dispositivo de impressão Xerox® é inicialmente instalado em uma rede, o comportamento padrão do Xerox® Remote Services é para o dispositivo de impressão tentar automaticamente estabelecer uma conexão direta com os Xerox® Communication Servers.

Figura 3



Transmissão e cargas de dados

Fontes de dados

Os atributos de dados dos dispositivos de impressão são coletados para o Xerox® Remote Services a partir das seguintes origens:

- Impressoras Office Xerox® em rede
- Impressoras não-Xerox® em rede
- Impressoras de produção Xerox®
- Aplicativos de gerenciamento de dispositivos Xerox®

Dispositivos Office Xerox®

Os dispositivos de impressão da classe Office Xerox® transmitem os atributos de dados do dispositivo no formato XML (eXtensible Markup Language), utilizando um arquivo compactado .zip. Cada arquivo é então transmitido através de um canal criptografado para os Xerox® Communication Servers remotos.

A Tabela 1 identifica os atributos de dados do dispositivo que podem ser transmitidos e sua descrições.

Atributos de dados	Descrição
Identidade do dispositivo de impressão	Inclui o modelo, nível do firmware, números de série dos módulos e data de instalação.
Endereço de rede do dispositivo de impressão	Inclui o endereço MAC (Media Access Control) e o endereço de sub-rede.
Propriedades do dispositivo de impressão	Incluem a configuração detalhada de componentes de hardware e de módulos de software, recursos/serviços compatíveis, modos de economia de energia etc.
Status do dispositivo de impressão	Inclui o status geral, alertas detalhados, histórico de falhas dos últimos 40 dias, dados de atolamento etc.
Contadores do dispositivo de impressão	Incluem os medidores de faturamento; contadores de impressão, cópia, fax, trabalhos grandes; e de digitalizações para destino; estatística de uso etc.
Consumíveis do dispositivo de impressão	Incluem o nome, tipo (por ex,: imagem, acabamento, papel), nível, capacidade, status, tamanho do consumível etc.

Atributos de dados	Descrição
Uso detalhado da máquina de impressão	Inclui os contadores de impressão detalhados, estados de alimentação ligada, quantidades detalhadas de substituições de USCs (unidades substituíveis pelo cliente), dados e distribuições detalhados de falha de USCs, uso da função de OCR (Reconhecimento óptico de caractere) integrada, distribuição da tiragem de impressão, distribuição do uso da bandeja do papel, material instalado, distribuição dos tipos e dos tamanhos do material, distribuição do comprimento do documento, número de jogos, dados de IAMF e da MNV, distribuição, contagem de pixels marcados, cobertura média de área por cor, falhas/atolamentos, contadores detalhados de digitalizações.
Engenharia/correção de falhas	Inclui informações detalhadas de correção de falhas que podem incluir dados fora do conjunto de dados listado acima. Esses dados podem incluir PII, como nomes de usuários, endereços de e-mail e dados do trabalho. Eles são enviados com a permissão expressa do cliente e são destinados somente para uso do suporte escalonado.

Nota: o arquivo e o conteúdo dos dados identificados variam, dependendo do modelo do produto.

Dispositivos de Produção Xerox®

Os dispositivos da classe de produção da Xerox® transmitem os atributos de dados do dispositivo no formato XML (eXtensible Markup Language), utilizando um arquivo compactado .zip. Cada arquivo é então transmitido através de um canal criptografado para os Xerox® Communication Services remotos.

A Tabela 2 identifica os atributos de dados do dispositivo e as descrições que podem ser transmitidas.

Atributos de dados	Descrição detalhada dos atributos de dados
Identidade do dispositivo de impressão	Inclui o modelo, níveis de firmware do módulo, números de série e datas de instalação dos módulos, informações de contato do cliente, dados da licença e local, se estiverem disponíveis.
Endereço de rede do dispositivo de impressão	Inclui o endereço MAC (Media Access Control) e o endereço de sub-rede.
Propriedades do dispositivo de impressão	Incluem a configuração detalhada de componentes de hardware e de módulos de software, recursos/serviços compatíveis etc.
Status do dispositivo de impressão	Inclui os status ativos, contagens de histórico de falhas, registro de eventos do DFE, histórico de transmissão de dados
Contadores do dispositivo de impressão	Incluem os medidores de faturamento; contadores de impressão, cópia, trabalhos grandes; contadores específicos da produção e de digitalizações para destino em modelos de produção mais acessíveis etc.
Consumíveis do dispositivo de impressão	Incluem o fabricante, modelo, número de série, nome, tipo, nível, capacidade, status, contadores de vida útil etc.
Uso detalhado da máquina de impressão	Inclui dados de IAMF e da MNV, substituição de peças, registros de DFE, dados de diagnóstico detalhados, resolução de falhas.
Engenharia/correção de falhas	Inclui dados relacionados à correção de falhas, não estruturados e detalhados, destinados somente para uso do suporte de 3° nível.
Relacionado ao trabalho do cliente	Os produtos de impressão de produção da Xerox® oferecem a capacidade de reprodução de dados relacionados ao trabalho para benefício dos cenários do suporte escalonado através de PostScript criptografado para a Xerox. O cliente pode controlar se deseja ou não ativar esse recurso. Se o cliente escolher transmitir dados relacionados ao trabalho (isto é, o PostScript criptografado) à Xerox, esses dados serão manuseados de acordo com as políticas e padrões de IS da Xerox.

Existem cenários de suporte escalonado, onde informações de correção de falhas detalhadas podem incluir atributos de dados fora do conjunto de dados identificado nas tabelas 1-3. Esses dados são enviados com a permissão expressa do cliente e são manuseados de acordo com as políticas e padrões de IS da Xerox

Nota: o arquivo e o conteúdo dos dados identificados variam, dependendo do modelo do produto.

Aplicativos de gerenciamento de dispositivos Xerox®

Os aplicativos de gerenciamento de dispositivos Xerox® (isto é: Xerox® Centre Ware® Web (**CWW**), Xerox® Device Agent (**XDA**), Xerox Device Agent Partner Edition (**XDA PE**) e Xerox® Device Manager (**XDM**) transmitem os dados de atributos de impressão no formato XML (eXtensible Markup Language) utilizando um arquivo .zip compactado. O arquivo é então criptografado e transmitido através de canais criptografados para os Xerox® Communication Servers remotos.

A Tabela 3 identifica os atributos de dados do dispositivo e as descrições que podem ser enviadas através do aplicativo de gerenciamento de dispositivos Xerox®.

Atributos de dados	Descrição detalhada dos atributos de dados
Identidade do dispositivo de impressão	Inclui o fabricante, modelo, descrição, nível de firmware, número de série, etiquetas de ativos, nome do sistema, contato, local, estação de trabalho (desktop) do estado de gerenciamento, número do fax e nome da fila.
Endereço de rede do dispositivo de impressão	Inclui o endereço MAC, endereço IP, nome de DNS, máscara de sub-rede, gateway do IP padrão, último endereço IP conhecido, endereço IP alterado, fuso horário, endereço IPX, número de rede IPX externa, servidor de impressão IPX.
Propriedades do dispositivo de impressão	Incluem os componentes instalados, descrições de componentes, recursos/serviços compatíveis, velocidade de impressão, suporte de cor, opções de acabamento, suporte para frente e verso, tecnologia de marcação, disco rígido, RAM, suporte de idioma, propriedades definidas pelo usuário.
Status do dispositivo de impressão	Inclui o status geral, alertas detalhados, mensagens do console local, status de componentes, dados de recuperação de status, data de localização, método/tipo de localização, tempo do dispositivo em operação, capturas compatíveis/ativadas.
Contadores do dispositivo de impressão	Incluem os medidores de faturamento; contadores de impressão, cópia, fax, trabalhos grandes e digitalizações; estatística de uso; e volume de destino.
Consumíveis do dispositivo de impressão	Incluem o nome, tipo (por ex,: imagem, acabamento, papel), nível, capacidade, status, tamanho do consumível etc.
Uso detalhado do dispositivo de impressão	Dados de rastreamento do trabalho com base no usuário que incluem as características do trabalho (ID, nome do documento, proprietário, tipo de documento, tipo de trabalho, cor, frente e verso, material solicitado, tamanho, páginas, jogos, erros), destino (dispositivo de impressão, modelo, nome de DNS, endereço IP, endereço MAC, número de série), resultados da impressão do trabalho (tempo de envio, tempo de impressão do trabalho, páginas impressas, páginas impressas em cores/P&B, modo de cor usado, N em 1), dados de contabilidade (código e preço de chargeback, origem da contabilidade), origem do trabalho de impressão (estação de trabalho, nome do servidor de impressão, endereço MAC, nome da fila, porta, nome do usuário, ID do usuário), dados de gerenciamento da Xerox (enviados para o Xerox® Services Manager).

Atributos de dados	Descrição detalhada dos atributos de dados
Identidade de gerenciamento de dispositivos	Inclui as informações do computador host do aplicativo, como o nome de DNS, endereço IP, nome e tipo de sistema operacional, CPU do computador pessoal, tamanhos da RAM (livre versus usada), tamanhos dos discos rígidos (livre versus usado), nome do local, versão do aplicativo, data de expiração da licença do aplicativo, versão .Net, fuso horário, versão do componente de localização, tamanho do banco de dados principal, tamanho do banco de dados de localização, número de impressoras/no escopo/fora do escopo, execução de serviços essenciais.
Device Manager Modo de segurança corporativo	**Modo Normal** = Xerox® Device Agent contata o Xerox® Services Manager diariamente. As configurações podem ser remotamente alteradas, sem a necessidade de visitas no local, mesmo quando as programações de busca estão desligadas. **Modo de Bloqueio** = além da sincronização de dados da impressora, não existe comunicação com o Xerox® Services Manager e as configurações têm que ser alteradas no local. Os endereços IP da máquina do Xerox® Device Agent e da impressora são informados para o Xerox® Services Manager.
Política de controle de impressão do gerenciamento de dispositivos	Inclui o nome do computador do usuário final; servidor de impressão utilizado; fila de impressão utilizada; carimbo de violação; nome do documento; nome de usuário do usuário final; frente e verso, cor, total de impressões, preço do trabalho; ação tomada, usuário final notificado, mensagem exibida, nome e regra da política de impressão.

Gerenciamento remoto de dispositivos de impressão

A equipe de suporte Xerox® pode processar as seguintes ações através do aplicativo de gerenciamento de dispositivos Xerox®. Quando existe permissão, estas ações são realizadas em suporte aos esforços de resolução de falhas e estão descritas na **Tabela 4** a seguir.

Data	Descrição
Ações a serem executadas nos dispositivos de impressão	• **Obter status do dispositivo** = recuperar o último status do dispositivo de impressão • **Reinicializar o dispositivo** = iniciar uma sequência de desligar/ligar o dispositivo de impressão • **Atualizar o dispositivo** = instalar um novo software/firmware no dispositivo de impressão (DJM na porta 9100) • **Solucionar problemas do dispositivo** = fazer um ping no dispositivo + recuperar o último status do dispositivo de impressão • **Imprimir uma página de teste** = enviar um trabalho de teste para um dispositivo de impressão para validar o trajeto da impressão (gerar um relatório de configuração) • **Iniciar o gerenciamento de dispositivos** = iniciar as transferências periódicas de dados do dispositivo de impressão para os Xerox® Communication Servers **Nota:** Cada ação pode ser desativada por demanda na parte de configuração da administração dos aplicativos de gerenciamento de dispositivos Xerox®, que são compatíveis com esta função.
Ações a serem executadas nos dispositivos de impressão	• **Reinicializar o dispositivo** = iniciar uma sequência de desligar/ligar o dispositivo de impressão • **Imprimir uma página de teste** = enviar um trabalho de teste para um dispositivo de impressão para validar o trajeto da impressão (gerar um relatório de configuração)
Ações a serem executadas nos aplicativos de gerenciamento de impressão	As configurações em cada aplicativo de gerenciamento de dispositivos que podem ser gerenciadas incluem configurações de operação de localização, frequência de exportação de dados, configurações relacionadas à comunicação SNMP (nova tentativa, tempo limite, nomes de comunidade), perfis de alerta e frequência de atualização automática do software do aplicativo de gerenciamento de dispositivos.

Requisitos do sistema para aplicativos de gerenciamento de dispositivos

Os requisitos mínimos variam levemente, de acordo com as ofertas. Consulte o guia do usuário, guia de avaliação de segurança e/ou guia de certificação para os requisitos da linha básica, específicos para o aplicativo de gerenciamento do dispositivo Detalhes adicionais podem ser encontrados em: http://www.support.xerox.com/support/enus.html

Na instalação, um arquivo .readme (.leiame) é incluído para cuidar dos requisitos adicionais e específicos do sistema para o respectivo aplicativo de gerenciamento do dispositivo sendo instalado.

- Recomenda-se que os computadores host executem um sistema operacional compatível da Microsoft® Corporation. Entretanto, os aplicativos de gerenciamento de dispositivos Xerox® podem ser executados em um ambiente de OS Macintosh, se estiverem usando o software de emulação Parallels Desktop. (Não é possível executar atualmente o aplicativo de gerenciamento de dispositivos Xerox® em um ambiente Macintosh nativo.) Consulte os respectivos guias do usuário dos aplicativos de gerenciamento de dispositivos Xerox®, para obter detalhes específicos.
- Recomenda-se que os computadores host estejam atualizados com as últimas versões de correções essenciais e serviços da Microsoft® Corporation.
- Um protocolo TCP/IP (Network Transmission Control Protocol/Internet Protocol) tem que ser carregado e estar operacional.
- Uma conexão de Internet é necessária.
- Necessita-se de privilégios administrativos para instalar o software do aplicativo de gerenciamento de dispositivos na máquina do cliente.
- Exige dispositivos habilitados para SNMP e a capacidade de rotear SNMP através da rede. Não é necessário ativar SNMP no computador onde os aplicativos de gerenciamento de dispositivos Xerox® serão instalados ou em qualquer outro computador da rede.
- Você deve instalar o Microsoft®.NET Framework 4.6 (versão completa), para instalar o aplicativo.
- O aplicativo não deverá ser instalado em um computador onde outros aplicativos com base em SNMP ou outras ferramentas Xerox® de gerenciamento de dispositivos estejam instalados, já que podem interferir com a atuação do outro aplicativo.

Configurações não compatíveis

- Instalação do aplicativo em um computador com outro aplicativo Xerox® de gerenciamento de dispositivos, como o Xerox® Device Manager.
- Qualquer sistema operacional Unix® ou Linux®
- Sistemas operacionais Microsoft® no final de sua vida útil, como o Windows NT® 4.0, Windows® Media Center, Windows® XP e Windows® Server 2000 e 2003.
- Ambientes virtuais diferentes do VMware® Lab Manager™/Workstation/vSphere Hypervisor™. Esse aplicativo pode funcionar em outros ambientes virtuais; entretanto, esses ambientes ainda não foram testados.

Processos de negócios e serviços Xerox®

Os dados recebidos pelos Xerox® Communication Servers de dispositivos de impressão Xerox® com base em escritório, dispositivos de impressão Xerox® com base na produção e aplicativos de gerenciamento de dispositivos Xerox® são utilizados pelos seguintes processos de negócios da Xerox:

Nome do processo de negócio	Descrição
Leituras automáticas do medidor	Um faturamento é gerado automaticamente dos dados recebidos do medidor a partir dos dispositivos de impressão.
Reabastecimento automático de suprimentos/peças	O toner é automaticamente enviado aos clientes quando o status de fim do consumível é recebido dos dispositivos de impressão. Os componentes para substituição são enviados automaticamente para os clientes, quando necessário, para os dispositivos de impressão. Essas opções estão disponíveis somente para os clientes que optam por contratos de suprimentos medidos.
Facilidade de manutenção (assistente de manutenção)	Informações detalhadas de falhas podem ser visualizadas pela equipe de atendimento técnico da Xerox, quando necessário, para agilizar a preparação para uma visita no local ou diagnosticar e solucionar problemas remotamente.
Suporte de 3º Nível (engenharia/correção de falhas)	A equipe de suporte do produto pode solucionar problemas difíceis quando recebe acesso para os registros detalhados de engenharia e de correção de falhas.

Os dados do dispositivo de impressão básico são compactados, transmitidos, retidos e arquivados no datacenter Xerox® com certificação ISO-27001 e são mantidos de acordo com as políticas de retenção e manuseio de dados corporativos da Xerox®.

Os processos e práticas de trabalho que oferecem suporte e protegem os sistemas de software Xerox® Back Office Remote Services têm como base as melhores práticas ITIL e Políticas de Segurança das Informações da Xerox, que têm como base os padrões da ISO 27001. Pode-se garantir aos clientes que o gerenciamento da integridade, privacidade e proteção dos dados estão em conformidade com as melhores práticas.

Detalhes de tecnologia

Esta seção oferece detalhes técnicos adicionais, que geralmente são exigidos pela equipe de TI e profissionais de segurança com o objetivo de controlar os riscos através da obtenção de garantia de práticas de desenvolvimento seguras; ativando assim a certificação dos dispositivos de impressão e aplicativos de gerenciamento de dispositivos para uso no ambiente de rede do cliente.

Design do software

Nosso compromisso com a segurança dos produtos Xerox® começa cedo no desenvolvimento do produto com as melhoras práticas padrão da indústria para a codificação protegida, testes extensivos e análise para eliminar vulnerabilidades. A Xerox® ativamente assume práticas de certificação, como o Common Criteria (Critérios comuns) e os padrões emergentes, como P2600 Working Group e Security Development Lifecycle (SDLC).

Operabilidade

O Xerox® Remote Services executa os seguintes tipos de operações em uma rede:

Método de implantação	Aplicativo utilizado	Fluxo de dados na rede	Operabilidade imposta em uma rede
Device Direct	Nenhum	Interno	O dispositivo de impressão Xerox® tenta detectar um servidor proxy de Web (de forma automática ou direta para um endereço específico)
		Interno	Os dispositivos de impressão Xerox® podem ser programados para gerar solicitações para um servidor SMTP (Simple Mail Transport Protocol) para enviar mensagens de e-mail de notificações de alertas para uma lista definida de destinatários.
		Externo para a rede	Os dispositivos de impressão Xerox® atravessam o firewall da empresa para acessar a Internet (HTTPS na porta 443)
		Externo para a rede	O dispositivo de impressão Xerox® é autenticado com o seu certificado para um Xerox Communication Server remoto antes da transmissão de quaisquer atributos de dados.
		Externo para a rede	O dispositivo de impressão Xerox® automaticamente transmite dados de atributos do dispositivo de impressão através de um canal criptografado (HTTPS na porta 443) para os Xerox® Communication Servers, em uma hora específica, diariamente, ou a pedido do cliente.

Método de implantação	Aplicativo utilizado	Fluxo de dados na rede	Operabilidade imposta em uma rede
		Externo para a rede	O dispositivo de impressão Xerox® automaticamente solicita aos Xerox® Communication Servers, através de um canal criptografado (HTTPS na porta 443) em uma determinada hora, todos os dias, uma lista de ações a serem executadas (por ex.: enviar dados de faturamento agora, adicionar serviços etc.)
		Externo para a rede	Transmissão unidirecional por demanda dos dados de registro de engenharia do dispositivo de impressão Xerox® através de um canal criptografado (HTTPS na porta 443) para o Xerox® Communication Server
Aplicativos de gerenciamento de dispositivos	Centre Ware® Web	Interno	Cada aplicativo detecta um servidor proxy da Web (de forma automática ou direta para um endereço específico)
		Interno	Cada aplicativo recupera os recursos do dispositivo de impressão no parque via SNMP
		Interno	Cada aplicativo recupera a configuração do dispositivo de impressão no parque via SNMP
		Interno	Cada aplicativo recupera o status do dispositivo de impressão no parque via SNMP
		Interno	Cada aplicativo recupera os dados dos consumíveis do dispositivo de impressão no parque via SNMP
		Interno	Cada aplicativo reinicializa um dispositivo de impressão via SNMP ou através da IU da Web do dispositivo de impressão
		Interno	Cada aplicativo pode enviar uma página de teste a um dispositivo de impressão específico
		Interno	Cada aplicativo pode lançar uma página de Web do dispositivo de impressão
		Externo **(somente para fora)**	Cada aplicativo atravessa o firewall da empresa para acessar a Internet (HTTPS na porta 443)
		Externo **(somente para fora)**	Cada aplicativo é autenticado com o seu certificado para um Xerox Communication Server remoto antes da transmissão de quaisquer atributos de dados
		Externo **(somente para fora)**	Cada aplicativo transmite automaticamente os dados de atributos do dispositivo de impressão através de um canal criptografado (HTTPS na porta 443) para os Xerox® Communication Servers, diariamente, em uma hora determinada

Método de implantação	Aplicativo utilizado	Fluxo de dados na rede	Operabilidade imposta em uma rede
		Externo **(somente para fora)**	Cada aplicativo automaticamente solicita aos Xerox® Communication Servers, através de um canal criptografado (HTTPS na porta 443) em uma determinada hora, todos os dias, uma lista de ações a serem executadas
Aplicativos de gerenciamento de dispositivos	Xerox® Device Agent Partner Edition para monitoramento de dispositivos de impressão conectados na rede	Interno	Cada aplicativo Xerox® Device Agent detecta um servidor proxy de Web (de forma automática ou direta para um endereço específico)
		Interno	Cada aplicativo Xerox® Device Agent recupera os recursos do dispositivo de impressão no parque via SNMP
		Interno	Cada aplicativo Xerox® Device Agent recupera a configuração do dispositivo de impressão no parque via SNMP
		Interno	Cada aplicativo Xerox® Device Agent recupera o status do dispositivo de impressão no parque via SNMP
		Interno	Cada aplicativo Xerox® Device Agent recupera os dados dos consumíveis do dispositivo de impressão no parque via SNMP
		Interno	Cada aplicativo Xerox® Device Agent pode solicitar que o dispositivo imprima um relatório de configuração
		Interno	Cada aplicativo Xerox® Device Agent pode lançar uma página de Web do dispositivo de impressão
		Interno	Cada aplicativo Xerox® Device Agent pode atualizar o software do dispositivo de impressão através do envio do trabalho de impressão. (Arquivo .DLM na porta 9100)
		Externo (**somente para fora)**	Cada aplicativo Xerox® Device Agent atravessa o firewall da empresa para acessar a Internet (HTTPS na porta 443)
		Externo **(somente para fora)**	Cada aplicativo é autenticado com o seu certificado para um Xerox Communication Server remoto antes da transmissão de quaisquer atributos de dados
		Externo **(somente para fora)**	Cada aplicativo Xerox® Device Agent transmite automaticamente os dados de atributos do dispositivo de impressão através de um canal criptografado (HTTPS na porta 443) para os Xerox® Communication Servers, em uma hora determinada, todos os dias
		Externo **(somente para fora)**	Cada aplicativo Xerox® Device Agent automaticamente solicita aos Xerox® Communication Servers, através de um canal criptografado (HTTPS na porta 443) em uma determinada hora, todos os dias, uma lista de ações a serem executadas

Método de implantação	Aplicativo utilizado	Fluxo de dados na rede	Operabilidade imposta em uma rede
Aplicativos de gerenciamento de dispositivos	Xerox® Device Manager para monitoramento de dispositivos de impressão conectados na rede	Interno	Os aplicativos Xerox® Device Manager/Xerox® Device Agent detectam um servidor proxy de Web (de forma automática ou direta para um endereço específico)
		Interno	Os aplicativos Xerox® Device Manager/Xerox® Device Agent recuperam os recursos do dispositivo de impressão no parque via SNMP
		Interno	Os aplicativos Xerox® Device Manager/Xerox® Device Agent recuperam a configuração do dispositivo de impressão no parque via SNMP
		Interno	Os aplicativos Xerox® Device Manager/Xerox® Device Agent recuperam o status do dispositivo de impressão no parque via SNMP
		Interno	Os aplicativos Xerox® Device Manager/Xerox® Device Agent recuperam os dados dos consumíveis do dispositivo de impressão no parque via SNMP
		Interno	Os aplicativos Xerox® Device Manager/Xerox® Device Agent podem solicitar que o dispositivo imprima um relatório de configuração
		Interno	Os aplicativos Xerox® Device Manager/Xerox® Device Agent podem lançar uma página de Web do dispositivo de impressão
		Interno	Os aplicativos Xerox® Device Manager/Xerox® Device Agent podem atualizar o software do dispositivo de impressão através do envio de trabalhos de impressão
		Interno	O aplicativo Xerox® Device Manager é compatível com a comunicação SNMPv3 com os dispositivos de impressão
		Interno	O aplicativo Xerox® Device Manager pode fazer alterações na configuração do dispositivo de impressão através de SNMP e da IU da Web
		Interno	O aplicativo Xerox® Device Manager recupera os registros de contabilidade com base em trabalhos de determinadas MFPs Xerox®
		Interno	O aplicativo Xerox® Device Manager gerencia/reforça as políticas de controle de impressão
		Externo **(somente para fora)**	Os aplicativos Xerox® Device Manager/Xerox® Device Agent atravessam o firewall da empresa para acessar a Internet (HTTPS na porta 443)
		Externo **(somente para fora)**	Cada aplicativo é autenticado com o seu certificado para um Xerox Communication Server remoto antes da transmissão de quaisquer atributos de dados

Método de implantação	Aplicativo utilizado	Fluxo de dados na rede	Operabilidade imposta em uma rede
		Externo **(somente para fora)**	Os aplicativos Xerox® Device Manager/Xerox® Device Agent transmitem automaticamente os dados do dispositivo de impressão para os Xerox® Communication Servers através de um canal criptografado (HTTPS na porta 443) em uma determinada hora, todos os dias
		Externo **(somente para fora)**	Os aplicativos Xerox® Device Manager/Xerox® Device Agent automaticamente solicitam aos Xerox® Communication Servers, através de um canal criptografado (HTTPS na porta 443) em uma determinada hora, todos os dias, uma lista de ações a serem executadas

SNMP (Simple Network Management Protocol)

O protocolo SNMP é a ferramenta de gerenciamento de rede utilizada amplamente para comunicação entre os sistemas de gerenciamento de rede e impressoras da rede. Os aplicativos de gerenciamento de dispositivos utilizam o SNMP durante as operações de localização para recuperar informações detalhadas dos dispositivos de impressão encontradas na rede. Os aplicativos de gerenciamento de dispositivo Xerox® são compatíveis com os protocolos SNMP v1/v2 e v3. Consulte os guias respectivos de certificação dos aplicativos de gerenciamento de dispositivos Xerox® para entender 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 rígida pela adição da segurança criptográfica ao protocolo SNMPv2. Além disso, SNMPv3 é compatível com versões anteriores e é amplamente utilizado em redes robustas.

Os aplicativos de gerenciamento de dispositivos Xerox® (CentreWare® Web/Xerox® Device Manager) têm a capacidade de se comunicar com plataformas de dispositivos que estão em conformidade com FIPS 140-2 em suas implementações de SNMPv3.

Os aplicativos de gerenciamento de dispositivos Xerox® não utilizam o serviço Windows SNMP ou Windows SNMP Trap. Se instalados anteriormente, estes serviços **devem** ser desativados no computador pessoal ou servidor onde o aplicativo de gerenciamento de dispositivos Xerox® estiver instalado.

Os aplicativos de gerenciamento de dispositivos Xerox® utilizam um agente SNMP desenvolvido pela Xerox que:

- Contém um mecanismo de codificação/decodificação especial
- É completamente gerenciado pelo .NET
- Utiliza o executável de tempo de execução .NET. Ele proporciona segurança aprimorada para impedir ataques contra os pontos vulneráveis do software, como manipulações inválidas do apontador; sobrecargas de buffer e verificação vinculada.

Os aplicativos de gerenciamento de dispositivos Xerox® utilizam as funções de segurança disponíveis do sistema operacional (OS) Windows, incluindo:

- Autenticação e autorização do usuário
- Configuração e gerenciamento de serviços
- Implantação e gerenciamento de políticas de grupo

Firewall de conexão com a Internet (ICF) do Windows, incluindo:

- Configurações de log de segurança
- Configurações de ICMP

Aplicativos de gerenciamento de dispositivos Xerox®: **Xerox® Device Agent, Xerox® Device Agent Partner Edition ou Xerox® Device Manager** utilizam o aplicativo Microsoft® SQL Server Compact

O aplicativo de gerenciamento de dispositivos Xerox® pode ser configurado para aumentar as funções de segurança adicionais do aplicativo Microsoft® SQL Server, incluindo:

- Ativar o registro de conta do usuário
- Criptografar o DNS (Domain Name System)
- Limitar os privilégios de conta do usuário para acessar o banco de dados (isto é, direitos do proprietário do banco de dados)
- Implementação de números de porta definidas pelo usuário

Uma chave de registro e uma conta Xerox válida são necessárias para a transmissão dos dados para os Xerox® Communications Servers remotos.

As comunicações externas dos aplicativos de gerenciamento de dispositivos Xerox® podem ser impactadas pelo firewall de conexão com a Internet do Windows. (**Recomendamos** que os clientes incluam a lista branca do URL Xerox no firewall do cliente e especifiquem os endereços IP que podem acessar o URL.)

Os aplicativos de gerenciamento de dispositivos Xerox® executam um processo em segundo plano, utilizando as credenciais de conta do sistema local para consultar automaticamente os dispositivos de impressão em rede através de SNMP e transmitir periodicamente os atributos do dispositivo de impressão para os Xerox® Communications Servers.

O acesso à interface do usuário (IU) e funções do aplicativo Xerox® Device Manager (XDM) são controlados através dos seguintes privilégios com base em função (por ex.: Centre Ware® Web Administrators, Centre Ware® Web Power Users, Centre Ware® Web SQL Users, Centre Ware® Web Customer Administrators e Centre Ware® Web Customers Groups fornecidos).

Nomes de usuário e senhas para os aplicativos não atravessam a rede; em vez disso, utiliza-se os tokens de acesso (por design de SO do Windows®).

O aplicativo Xerox® Device Manager (XDM) proporciona segurança baseada no controle do envio de impressão ao restringir trabalhos com base na política de uso da cor, tipo do

documento, custo do trabalho, hora do dia, controle de acesso de grupos de usuário, política de frente e verso, impressões do trabalho permitidas e cotas de impressão.

Notas: o uso do protocolo SNMP por qualquer aplicativo Xerox® Remote Services não representa um risco à segurança para o ambiente de TI de um cliente, porque todo o tráfego com base em SNMP gerado ou consumido por estes aplicativos ocorre na Intranet do cliente, por trás do firewall. O serviço Windows SNMP e o serviço Windows SNMP Trap não são ativados por padrão no sistema operacional Windows.

Modo de segurança corporativo

Além de qualquer sincronização programada pelos aplicativos de gerenciamento de dispositivos Xerox® para o Xerox® Services Manager, existe uma sincronização diária executada por padrão. Os dois modos de segurança corporativa que existem são os modos **Normal** e **Bloqueado.**

No modo **normal**, o aplicativo de gerenciamento de dispositivo entra em contato diário com o Xerox® Services Manager, quando todas as outras sincronizações programadas tiverem sido desativadas ***(modo recomendado***).

No modo **bloqueado**, além da sincronização de dados relacionada à impressora, não há comunicação com o Xerox® Services Manager. As alterações nesta configuração devem ser feitas no local. (A ***sincronização de dados*** garante que as informações do dispositivo de impressão enviadas pelo aplicativo de gerenciamento de dispositivos Xerox® e as que são capturadas no Xerox® Services Manager sejam as mesmas.)

Por padrão, o aplicativo de gerenciamento de dispositivos Xerox® contata diariamente o Xerox® Services Manager e permite aos administradores alterar configurações remotamente, evitando a necessidade de chamadas para atendimento técnico no local. Recomendamos que esta configuração não seja alterada. Se um cliente restringe a equipe Xerox de oferecer suporte remoto aos dispositivos de impressão, a comunicação do dispositivo com o Xerox® Services Manager pode ser bloqueada, exceto para a sincronização de dados da impressora. Neste modo, o aplicativo não reporta quaisquer endereços IP do computador ou impressora ou configurações do local ao Xerox® Services Manager e qualquer alteração de configuração exigirá uma visita no local.

Nota: se o Xerox® Device Agent não contiver a guia de Modo de segurança corporativo, ele irá operar no modo Normal.

Protocolos, portas e outras tecnologias relacionadas

A tabela a seguir identifica os protocolos, portas e tecnologias que são utilizados no Xerox® Remote Services:

Número da porta	Protocolo	Descrição do uso	Fluxo de dados na rede
Depende dos protocolos de camada superior	**IP (Internet Protocol ou Protocolo de Internet)**	**Transporte básico para todas as comunicações de dados**	**Interno + Externo (somente para fora)**
NA	ICMP (Internet Control Message Protocol)	Localização + solução de problemas do dispositivo de impressão	Interno
25	SMTP (Simple Mail Transport Protocol)	Dispositivo de impressão + alertas de notificação de e-mail de aplicativo de proxy remoto	Interno

Número da porta	Protocolo	Descrição do uso	Fluxo de dados na rede
53	DNS (Domain Name Services)	Utilizado por operações de localização de dispositivos de impressão com base em DNS	Interno
80	HTTP (Hyper Text Transport Protocol)	Consultas de página de Web do dispositivo de impressão + consultas de página de Web do aplicativo de gerenciamento de dispositivos	Interno
135	RPC (Remote Procedure Call)	Localização do dispositivo de impressão	Interno
137, 139	NetBIOS	Localização do servidor de impressão	Interno
161	Simple Network Management Protocol (SNMP v1 / v2C / v3)	Protocolo padrão da indústria usado para localizar dispositivos de impressão na rede + Recuperar status, contadores e dados de suprimentos + Recuperar e aplicar a configuração de dispositivos de impressão. Nomes de comunidade padrão = "pública" (GET), "privada" (SET)	Interno
162	Capturas de SNMP	Nome de comunidade padrão = "SNMP_trap"	Interno
389	LDAP (Lightweight Direct Access Protocol)	Localização de dispositivo de impressão através de enumeração de partição do MS Active Directory + Definição da configuração do serviço de digitalização + Importação de clientes do Active Directory + Configurações de grupos do cliente	Interno
443	HTTPS (Hyper Text Transport Protocol Secure)	Consultas seguras de páginas de Web do dispositivo de impressão (se configurado) + consultas seguras de páginas de Web do aplicativo de proxy remoto (se configurado) + Transferência de dados do dispositivo de impressão para os Xerox® Communication Servers + transmissão de comunicação de controles de impressão para o Xerox® Device Manager	Interno + Externo (somente para fora)
452	SAP (Netware Service Advertising Protocol)	Localização do dispositivo de impressão utilizando consultas do Servidor Novell via IPX	Interno
515, 9100, 2000, 2105	Envio do trabalho de impressão por TCP/IP, LPR e Porta Raw	Atualização de software do dispositivo de impressão + Diagnóstico da página do teste de impressão	Interno
631	IPP (Internet Printing Protocol)	Localização do dispositivo de impressão	Interno

Melhores práticas de segurança

Sempre mantenha os dispositivos de impressão atualizados com os firmware/software mais recentes. Utilize a interface de usuário (IU) da Web do dispositivo de impressão ou o aplicativo de gerenciamento de impressora fornecidos pela Xerox® e outros fornecedores de impressão para atualizar o firmware/software do dispositivo de impressão.

Desative as portas e protocolos não utilizados nos dispositivos de impressão, sempre que possível. Geralmente, isso é feito na interface de usuário (IU) da Web nos dispositivos de impressão da classe de escritório e interface de usuário (IU) local de dispositivos de impressão da classe de produção.

Utilize as funções de controle de acesso do usuário nos dispositivos de impressão, se disponíveis. Geralmente, isso é feito na interface de usuário (IU) da Web nos dispositivos de impressão da classe de escritório e interface de usuário (IU) local de dispositivos de impressão da classe de produção.

Utilize protocolos seguros, quando possível Geralmente, isso é feito na interface de usuário (IU) da Web nos dispositivos de impressão da classe de escritório e interface de usuário (IU) local de dispositivos de impressão da classe de produção.

Ative as funções de segurança incorporadas no dispositivo (por ex.: sobregravação de imagem, criptografia de disco, impressão protegida etc.).

Certifique-se de que o firewall da empresa possa rotear os pacotes HTTPS pela porta 443, de acordo com as políticas de segurança corporativa.