Xerox Remote Services

Libro blanco de seguridad

Versión 4.0

Marzo de 2022

Este documento se modifica periódicamente. Los cambios, imprecisiones técnicas y errores tipográficos se corregirán en posteriores ediciones.

IS 614672/IS 514590

Índice

1. Objetivo general y público al que se dirige

El objetivo del libro blanco de seguridad de Xerox Remote Services es ayudar a los clientes a entender y a implementar la solución de servicios remotos seguros que mejor se adapte a la estructura de su red y a sus políticas de seguridad de la información. Para garantizar el método de configuración más seguro, tenga en cuenta que puede ser necesario realizar cambios en el firewall de Internet del cliente, en los servidores proxy de la web o en otra infraestructura de red relacionada con la seguridad.

Los destinatarios de este documento son vendedores técnicos, administradores de redes y profesionales de la seguridad de redes interesados en el potencial de los servicios remotos y la implementación de seguridad de esas características.

Se recomienda revisar el documento en su totalidad para certificar el uso de los productos y servicios Xerox® en el entorno de red del cliente.

2. Propuesta de valor

Ofrecemos una forma segura de enviar los datos de los dispositivos a nuestro sistema con certificación ISO para automatizar las tareas comunes y proporcionar una mejor experiencia de servicio y soporte.

- Los informes de facturación de los contadores están automatizados y son precisos.
- El programa de reposición automática de suministros proporciona tóner en función de los niveles de tóner notificados por la impresora, por lo que no es necesario realizar un seguimiento del inventario ni solicitar suministros.
- El envío de información de diagnóstico nos permite dar un mejor soporte a su dispositivo, lo que a menudo permite una resolución más rápida del problema.
- Algunos modelos de impresoras pueden buscar actualizaciones de software importantes e instalarlas de forma programada sin la intervención del cliente. Ver Nota
- Las funciones de nuestros servicios gestionados también proporcionan una forma de gestionar las impresoras que no son de la marca Xerox, además de las impresoras de la marca Xerox.
- Estos servicios permiten a nuestros clientes un uso más eficiente de su tiempo.

Todo esto se hace pensando en la seguridad.

Nota: Esta opción se puede deshabilitar para entornos en los que los clientes certifican una versión de software determinada y desean controlar el software de impresión cuando se producen actualizaciones. Para ello, no es necesario deshabilitar las demás funciones de servicios remotos.

3. Remote Services

La información es un activo clave y la seguridad es primordial para todos los activos de la organización, incluidos los dispositivos de impresión multifunción (MFP) en red. En la actualidad, la gestión de un conjunto de dispositivos de impresión multifunción, al tiempo que se garantiza un nivel aceptable de seguridad, presenta una serie de retos únicos que a menudo se pasan por alto. Entendemos esta complejidad y respondemos a las necesidades de seguridad de nuestros clientes. Los productos Xerox®, los sistemas Xerox® y las propuestas de servicios remotos están diseñados para integrarse de forma segura con los flujos de trabajo existentes de nuestros clientes, a la vez que emplean las últimas tecnologías seguras.

Por defecto, no se transmiten a nuestros servidores imágenes de clientes procedentes de acciones de impresión, fax, escaneado, copia u otra información sensible.

Los servidores de Xerox con sede en Estados Unidos cumplen con los estrictos requisitos de seguridad para la gestión de la seguridad de la información. Nuestros centros de datos y aplicaciones de servicios remotos conservan los requisitos anuales de la Declaración de Normas de Atestación (SSAE) n.° 16, la Ley Sarbanes-Oxley (SOX) y cuentan con la certificación ISO 27001:2013.

4. Modelos de implantación

Nuestros clientes pueden elegir entre los siguientes modelos de implantación seguros de Xerox® Remote Services:

- **Modelo combinado *(preferido):*** la implementación conjunta del modelo de aplicación Device Direct y Device Management es ideal, ya que proporciona el conjunto de datos más sólido y las capacidades de gestión de dispositivos.

- **Modelo Device Direct:** Device Direct permite que las impresoras de comuniquen directamente con los servidores de comunicación remotos de Xerox® a través de Internet por el firewall del cliente para dar soporte a la reposición automática de suministros (ASR), la lectura automática de contadores (AMR) y los informes de diagnóstico de los dispositivos. Este modelo de implantación ofrece un conjunto de elementos de datos en la carga útil estándar para incluir fallos del dispositivo, alertas, contadores, elementos de servicio de alta frecuencia (HFSI) y otros atributos del dispositivo de impresión.
- **Modelo de Aplicación de Device Management:** las aplicaciones de Xerox® Device Management pueden implantarse en la red del cliente para recoger el conjunto de atributos de datos desde los dispositivos de impresión hasta dar soporte a la reposición automática de suministros (ASR), la lectura automática de contadores (AMR) y los informes de diagnóstico de los dispositivos. Los atributos del dispositivo de impresión se recogen y se transmiten de forma segura a los servidores remotos de Xerox®. Los atributos de datos de los dispositivos de impresión, tanto de Xerox como de otros fabricantes, pueden comunicarse como parte de este modelo de implantación.

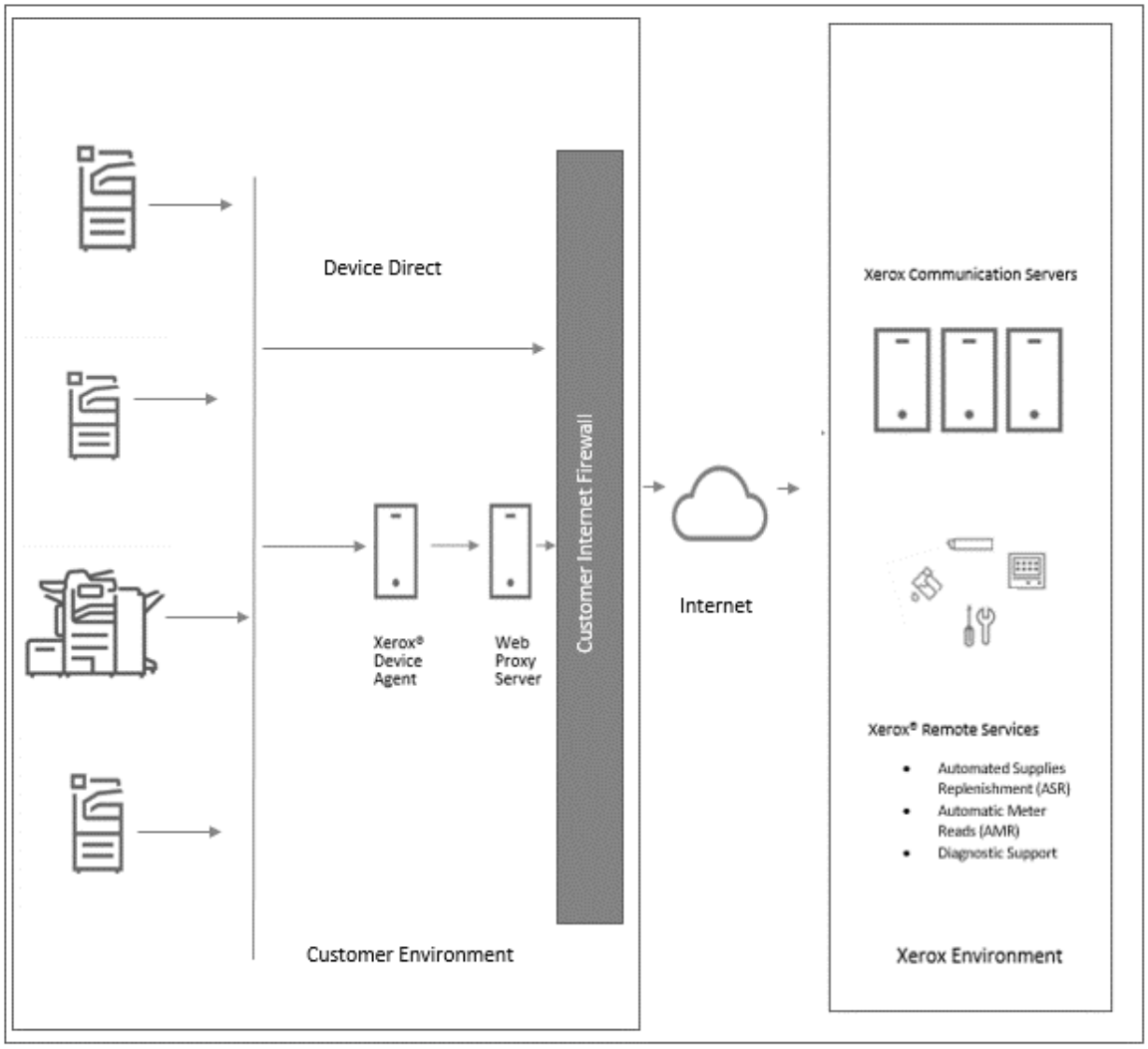
Todos los modelos de implantación de Xerox® Remote Services son igualmente seguros y aprovechan los últimos protocolos y puertos estándar del sector basados en la web para establecer un canal seguro y encriptado al transmitir los atributos de los dispositivos de impresión de forma externa a los servidores remotos de Xerox situados en nuestros centros de datos seguros y redundantes.

El modelo de implantación elegido depende del tipo de solución de servicio de impresión de nuestros clientes, de las políticas de seguridad de la información y de las normas de gestión de la transmisión de los atributos de los datos del dispositivo de impresión.

Modelos de implantación combinado (preferido)

El modelo de implantación combinado se implanta cuando un cliente adquiere múltiples contratos de mantenimiento con Xerox de sus dispositivos de impresión para conseguir una solución de servicios remotos más sólida. Cuando un dispositivo de impresión de Xerox® se instala inicialmente en una red, el comportamiento predeterminado de los servicios remotos de Xerox es que el dispositivo de impresión intente comunicarse automáticamente con nuestros servidores de comunicación utilizando un método de conexión seguro y autenticado.

Figura 1



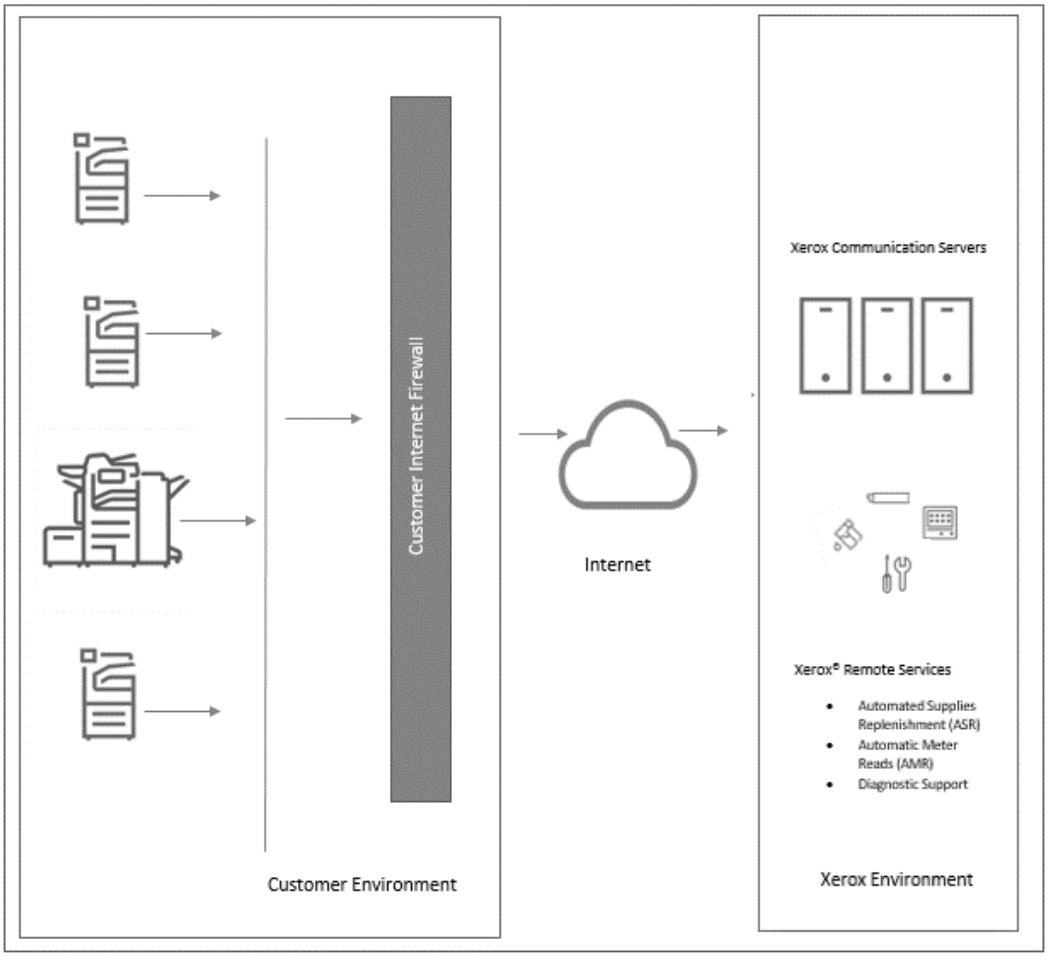
Combination Deployment Model

Modelos de implantación Device Direct

Los dispositivos Xerox® compatibles con los Remote Services utilizan una conexión de protocolo de seguridad de la capa de transporte (TLS) 1.2 a través del puerto estándar seguro 443 para comunicarse con nuestros servidores seguros.

- Los dispositivos de impresión del entorno del cliente inician todas las comunicaciones con los servidores de comunicación. Se requiere una configuración estándar del firewall de la página para permitir la comunicación.
- Se debe utilizar una URL válida para los servidores de comunicación (*.xerox.support.com) para autenticar los dispositivos de impresión en la infraestructura de Xerox.
- El dispositivo solicita un registro con los servidores de comunicación utilizando las credenciales apropiadas de autenticación del certificado.
- Los servidores de comunicación validan las credenciales suministradas por las impresoras y aceptan las solicitudes.
- Los servidores de comunicación están tras un firewall seguro en el entorno de Xerox y no son accesibles desde Internet.

Figura 2



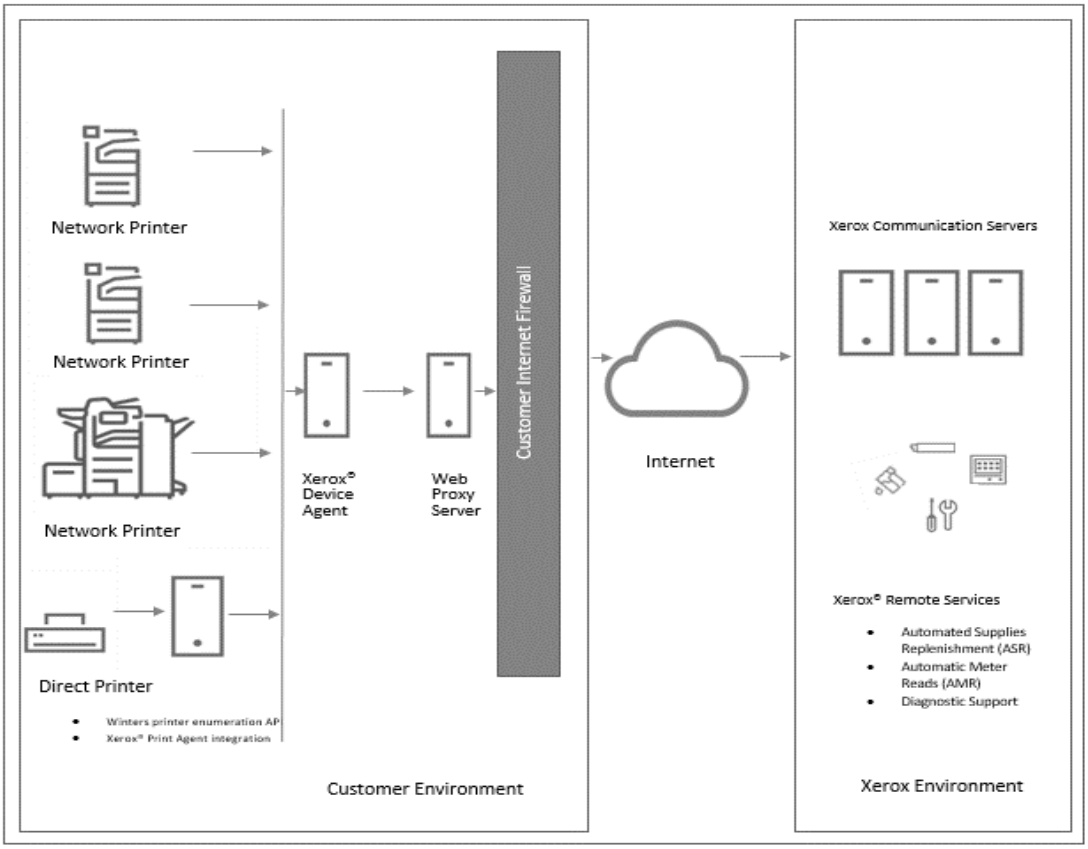
Device Direct Deployment Model

Modelos de implantación de aplicación Device Management

Las aplicaciones de Device Management (como **Xerox Centre Ward® Web, Xerox Device Agent**, **Xerox Device Agent Lite, Xerox Device Agent Partner Edition**, **and Xerox Device Manager)** utilizan una conexión de protocolo de seguridad de la capa de transporte (TLS) 1.2 a través del puerto estándar seguro 443 para comunicarse externamente con los servidores de comunicación. Las funciones adicionales se aprovechan para mejorar la seguridad a través de este canal y se determinan durante la instalación inicial de las aplicaciones de Device Management. que incluyen:

- La aplicación de Device Management del entorno del cliente inicia todas las comunicaciones con los servidores de comunicación. Se requiere una configuración estándar del firewall de la página para permitir la comunicación.
- Los servidores de comunicación están tras un firewall seguro en el entorno de Xerox y no son accesibles desde Internet.
- La aplicación Device Management solicita un registro con los servidores de comunicación utilizando las credenciales apropiadas de autenticación del certificado.
- Los servidores de comunicación validan las credenciales suministradas por las impresoras y aceptan las solicitudes.
- La aplicación de Device Management autentifica los servidores de comunicación y activa el servicio.

Figura3



Device Management Application Deployment Model

5. Transmisión de datos y cargas

Fuentes de datos

Los atributos de datos del dispositivo de impresión que se envían como parte de la carga útil transmitida proceden de las siguientes fuentes:

- Impresoras en red de Xerox® Office
- Impresoras en red de otros fabricantes
- Impresoras de Xerox® Production
- Aplicaciones Xerox® Device Management

Nota: No todas las impresoras Xerox Office y Xerox Production son compatibles con Xerox Remote Services. Consulte la lista completa de productos compatibles aquí. Los atributos del dispositivo de impresión varían según el producto y la solución de implantación de Xerox® Remote Services.

Dispositivos Xerox® Office

Tabla 1: identifica los atributos de datos del dispositivo que pueden ser transmitidos para productos compatibles con Remote Services de Xerox® Office.

Atributos de datos	Descripción detallada de los atributos de datos
Identidad de los dispositivos de impresión	Modelo, niveles de firmware del módulo, números de serie del módulo, fechas de instalación del módulo, datos de la licencia y la ubicación, si está disponible.
Dirección de red de los dispositivos de impresión	Dirección de control de acceso al medio (MAC), dirección de subred.
Propiedades de los dispositivos de impresión	Configuración detallada de los componentes de hardware, configuración detallada de los módulos de software, características/servicios soportados, etc.
Estado de los dispositivos de impresión	estados activos, recuentos del historial de fallos, registro de eventos del DFE, historial de transmisión de datos.
Contadores de los dispositivos de impresión	Contadores de facturación, contadores relacionados con la impresión, contadores relacionados con la copia, contadores relacionados con los trabajos grandes, contadores específicos de producción, contadores relacionados con el escaneo a destino en los modelos de producción de gama baja, etc.
Consumibles de los dispositivos de impresión	Fabricante, modelo, número de serie, nombre, tipo, nivel, capacidad, estado, contadores de vida útil, etc.
Uso detallado de la máquina impresora	Datos FSI, datos NVM, sustitución de piezas, registros DFE, datos de diagnóstico detallados, resolución de fallos.

Atributos de datos	Descripción detallada de los atributos de datos
Ingeniería/ Corrección	Datos no estructurados y detallados relacionados con la corrección, destinados únicamente al soporte de tercer nivel.
Relacionado con el trabajo del cliente	Los productos de impresión de Xerox® Production ofrecen la función de reproducir los datos relacionados con los trabajos como apoyo para los escenarios de soporte escalado a través de PostScript encriptado a Xerox. El cliente puede elegir si quiere activar o no esta función. Si el cliente decide transmitir datos relacionados con el trabajo (es decir, PostScript encriptado) a Xerox, esos datos se manejan de acuerdo con las políticas y normas de seguridad de la información (IS) de Xerox.

Nuestros dispositivos de impresión de oficina transmiten los atributos de los datos del dispositivo en un formato de lenguaje de marcado eXtensible (XML) mediante un archivo comprimido .zip. Una vez autenticado, cada archivo se transmite por un canal cifrado a los servidores de comunicación.

Dispositivos Xerox® Production

Tabla 2: identifica los atributos de datos del dispositivo que pueden ser transmitidos para productos compatibles con Remote Services de Xerox® Production.

	Descripción
Identidad de los dispositivos de impresión	Modelo, nivel de firmware, números de serie del módulo y fecha de instalación.
Dirección de red de los dispositivos de impresión	Dirección de control de acceso al medio (MAC), dirección de subred.
Propiedades de los dispositivos de impresión	Configuración detallada de los componentes de hardware, configuración detallada de los módulos de software, características/servicios soportados, modos de ahorro de energía, etc.
Estado de los dispositivos de impresión	Estado general, alertas detalladas, registro de los 40 últimos fallos, datos de atascos, etc.
Contadores de los dispositivos de impresión	Contadores de facturación, contadores relacionados con la impresión, contadores relacionados con la copia, contadores relacionados con el fax, contadores relacionados con los trabajos grandes, contadores relacionados con el escaneo a destino, estadísticas de uso, etc.
Consumibles de los dispositivos de impresión	nombre del consumible, tipo (por ejemplo, imagen, acabado, soporte de papel), nivel, capacidad, estado, tamaño, etc.
Uso detallado de la máquina impresora	Contadores detallados relacionados con la impresión, estados de encendido, cantidades detalladas de sustitución de las unidades sustituibles por el cliente (CRU), datos y distribuciones detalladas de los fallos de las CRU, uso de la función de reconocimiento óptico de caracteres (OCR) integrada, distribución de la longitud de la tirada de impresión, distribución del uso de la bandeja de papel, soportes instalados, distribución de los tipos de soportes, distribución del tamaño de los soportes, distribución de la longitud de los documentos, número de conjuntos, datos HFSI, datos NVM, distribución, recuentos de píxeles marcados, cobertura media del área por color, fallos/atrancos, contadores detallados relacionados con el escaneado.

Ingeniería/ Corrección	Información de corrección detallada que puede incluir información que no se encuentra en la lista anterior. Estos datos pueden incluir datos que permitan la identificación personal como nombres de usuario, direcciones de correo electrónico y datos de trabajo. Estos datos solo se envían con el permiso expreso del cliente y están destinados a un uso de apoyo para la resolución de problemas.

Nuestros dispositivos de impresión de producción transmiten los atributos de los datos del dispositivo en un formato de lenguaje de marcado eXtensible (XML) mediante un archivo comprimido .zip. Una vez autenticado, cada archivo se transmite por un canal cifrado a los servidores de comunicación.

Nota: El archivo y contenido de los datos identificados varía según el modelo de producto.

Aplicaciones Xerox® Device Management

Existen varias opciones de aplicaciones Device Management disponibles basadas en entornos de red de clientes y en la necesidad de gestión de los dispositivos de impresión. Todas son igual de seguras y cuentan con sólidas capacidades de gestión de dispositivos de impresión.

A continuación, se presenta una lista de aplicaciones de gestión de dispositivos: Xerox CentreWare® Web, Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition, y Xerox Device Manager.

Cada aplicación se sincroniza, por defecto, al menos diariamente con los servidores de comunicación segura. Para garantizar la máxima seguridad de sus datos, los servidores de comunicación están alojados en unas instalaciones que cumplen la norma ISO 27001. Los datos que se envían son principalmente contadores de facturación específicos de la impresora, niveles de suministro y alertas de la impresora. Los datos se comprimen, encriptan y protegen mediante varios mecanismos:

- La aplicación de Xerox Device Management inicia el contacto con los servidores de Xerox. Se requiere contar con una configuración estándar del firewall en el entorno del cliente para habilitar la comunicación.
- Las aplicaciones de Xerox Device Management requieren un proxy válido, en el caso de que sea requerido para la comunicación por Internet.
- Los servidores de comunicación de Xerox están tras un firewall seguro en el entorno de Xerox y no son accesibles desde Internet.
- El acceso a la interfaz de usuario del servidor de comunicación Xerox requiere autenticación. La información del host de la aplicación de Xerox Device Management se almacena en una cuenta específica en el sitio del cliente y el acceso a los datos de dicha cuenta en los servidores de comunicación de Xerox se restringe a los administradores de cuenta de los servidores de comunicación de Xerox.
- Queda registro de toda la comunicación del servidor de comunicaciones Xerox y está disponible para su visualización.
- Los datos enviados a sus dispositivos de impresión en red, cuando están habilitados, consisten principalmente en comandos remotos que permiten a un administrador de soporte de cuentas solicitar la ejecución del nivel de comandos de la aplicación de Xerox Device Management durante escenarios de soporte escalado.

- Las solicitudes se refieren principalmente a la actualización del firmware, el reinicio de la impresora, la impresión de páginas de prueba y la actualización del estado actual del dispositivo.
- La aplicación de Xerox Device Management sondea periódicamente su cuenta de servidores de comunicación de Xerox en busca de solicitudes de comandos.
- Los resultados de las operaciones de las solicitudes de comandos se envían a los servidores de comunicación de Xerox, donde son revisados.

Nota: Se requiere un registro único al instalar el software. Esta información de registro incluye un campo para la ubicación del dispositivo y el correo electrónico de contacto.

Las aplicaciones de Xerox Device Management **(Xerox CentreWare® Web, Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition y Xerox Device Manager** transmiten los datos del atributo de impresión en formato de lenguaje marcado extensible (XML) mediante un archivo .zip comprimido. A continuación, el archivo se cifra y transmite a través de canales cifrados a los servidores de comunicación remotos.

Tabla 3 Identifica una lista de atributos de datos del dispositivo y una descripción que puede enviarse a través de la aplicación de gestión de dispositivos de Xerox®.

Atributos de datos	Descripción detallada de los atributos de datos
Identidad de los dispositivos de impresión	Incluye fabricante, modelo, descripción, nivel de firmware, número de serie, etiquetas de activos, nombre del sistema, contacto, ubicación, estación de trabajo del estado de gestión (escritorio), número de fax y nombre de la cola.
Dirección de red de los dispositivos de impresión	Incluye dirección MAC, dirección IP, nombre de DNS, máscara de subred, puerta de enlace IP predeterminada, última dirección IP conocida, dirección IP cambiada, zona horaria, dirección IPS, número de red externa IPX, servidor de impresión IPX.
Propiedades de los dispositivos de impresión	Incluye componentes instalados, descripciones de componentes, funciones/servicios compatibles, velocidad de impresión, compatibilidad con la impresión a color, opciones de acabado, compatibilidad con la impresión a doble cara, tecnología de marcado, disco duro, memoria RAM, soporte de idioma, propiedades definidas por el usuario.
Estado de los dispositivos de impresión	Incluye estado general, alertas detalladas, mensajes de la consola local, estado de los componentes, datos relativos a la recuperación del estado, fecha de detección, método/tipo de detección, disponibilidad del dispositivo, reventados compatibles/activados.
Contadores de los dispositivos de impresión	Incluye contadores de facturación; contadores relativos a la impresión, copia, fax, trabajos grandes y escaneo; estadísticas de uso; y volumen objetivo.
Consumibles de los dispositivos de impresión	Incluye nombre de los consumibles, tipo (p. ej., imágenes, acabado, papel), nivel, capacidad, estado, tamaño y atributos relacionados
Uso detallado de los dispositivos de impresión	Datos de seguimiento de trabajos basados en el usuario que incluyen características del trabajo (ID, nombre del documento, propietario, tipo de documento, tipo de trabajo, color, impresión a dos caras, medios necesarios, tamaño, páginas, conjuntos, errores), destino (dispositivo de impresión, modelo, nombre de DNS, dirección IP, dirección MAC, número de serie), resultados de la impresión del trabajo (hora de envío, hora de impresión del trabajo, páginas impresas, páginas impresas a color o en blanco y negro, modo de color empleado, N-up), datos contables (código de contracargo, precio de contracargo, fuente contable), fuente del trabajo de impresión (estación de trabajo, nombre del servidor de impresión/dirección MAC, nombre de la cola, puerto, nombre de usuario, ID de usuario), datos de gestión de Xerox (enviados a Xerox Services Manager).

Atributos de datos	Descripción detallada de los atributos de datos
Identidad de Device Management	Incluye información del equipo host de la aplicación como nombre de DNS, dirección IP, nombre del SO, tipo de SO, CPU del equipo, tamaños de memoria RAM (libres y en uso), tamaños de disco duro (libres y en uso), nombre del sitio, versión de la aplicación, fecha de vencimiento de la licencia de la aplicación, versión .NET, zona horaria, versión de la detección de componentes, tamaño de la base de datos principal, tamaño de la base de datos de detección, número de impresoras en el ámbito y fuera del ámbito, servicios fundamentales en ejecución.
Modo de seguridad de la empresa de Device Manager	Modo Normal = Xerox Device Agent a diario se pone en contacto con Xerox Services Manager. Los ajustes se pueden cambiar de forma remota sin la necesidad de realizar visitas in situ, incluso cuando los programas de *polling* están desactivados. Modo Bloqueado = aparte de la sincronización de datos relacionados con la impresora, no existe comunicación con Xerox Services Manager y los ajustes se deben cambiar in situ. El dispositivo de Xerox Device Agent y las direcciones IP de la impresora se comunican a Xerox Services Manager.
Política de control de impresión de Device Management	Incluye nombre del equipo del usuario final, servidor de impresión utilizado, cola de impresión utilizada, fecha y hora de la infracción, nombre del documento, nombre de usuario del usuario final, impresión a doble cara del trabajo, color del trabajo, impresiones totales del trabajo, precio del trabajo, medidas adoptadas, usuario final notificado, mensaje mostrado, nombre de la política de impresión, regla de la política de impresión.

6. Gestión remota de los dispositivos de impresión

El personal de asistencia ampliada de Xerox puede procesar las siguientes acciones a través de Device Direct o la aplicación de Xerox® Device Management.

La tabla 4 muestra las iniciativas de resolución mejoradas que permite el usuario en una situación de asistencia ampliada. Debe obtenerse el permiso explícito del cliente para realizar estas funciones.

Datos	Descripción
Acciones para llevar a cabo en los dispositivos de impresión	• Obtener el estado del dispositivo = recuperar el último estado del dispositivo de impresión • Reiniciar el dispositivo = iniciar una secuencia de apagado/encendido en el dispositivo de impresión • Actualizar el dispositivo = instalar software/firmware nuevo en el dispositivo de impresión (.DLM a través del puerto 9100) • Resolución de problemas del dispositivo = comprobar la disponibilidad del dispositivo + recuperar el último estado del dispositivo de impresión • Impresión de la página de prueba = enviar un trabajo de prueba al dispositivo de impresión para validar la ruta de impresión (generar un informe de configuración) • Empezar a gestionar el dispositivo = iniciar transferencias de datos periódicas del dispositivo de impresión a los servidores de comunicación de Xerox® externos **Nota: Cada acción se puede deshabilitar en el uso bajo demanda desde la configuración de administración de las aplicaciones Xerox® Device Management que admiten esta función.**
Acciones para llevar a cabo en las aplicaciones de Device Management	Entre los ajustes de cada aplicación de gestión de dispositivos que se pueden gestionar se incluye la operación de detección, frecuencia de exportación de datos, ajustes relativos a la comunicación SNMP (reintento, tiempo de espera, nombres de la comunidad), perfiles de alerta y frecuencia de actualización de software automática de la aplicación de Device Management.
Gestión remota del software	Algunos dispositivos están equipados con capacidades de gestión remota del software. Estos dispositivos envían una solicitud al entorno de Xerox para comprobar si hay nuevas actualizaciones de software disponibles para el dispositivo. En caso afirmativo, el dispositivo después podrá enviar una solicitud de actualización del sistema y esta se llevará a cabo a la hora indicada. No obstante, si su entorno no permite realizar actualizaciones de software automáticas; la opción de gestión remota del software se puede desmarcar únicamente sin la interrupción de los servicios remotos estándar.

Requisitos del sistema para las aplicaciones de Device Management

Los requisitos mínimos varían ligeramente en función de las propuestas. Consulte la Guía de usuario, la Guía de evaluación y seguridad o la Guía de certificación para descubrir los requisitos básicos específicos para las aplicaciones correspondientes de Device Management.

Durante la instalación se incluye un archivo de lectura que aborda requisitos adicionales y específicos del sistema para la aplicación de Device Management que se está instalando.

- Las aplicaciones de Device Management son compatibles con las funciones de seguridad integradas en el sistema operativo de Windows®. Dependen de un servicio de Windows® que se ejecuta en segundo plano con las credenciales de la cuenta del sistema local para habilitar la supervisión proactiva de impresoras y la carga de atributos de datos de impresión que se transmitirán a Xerox. La interfaz de usuario que muestra la carga de atributos de datos de impresión solo está accesible para los usuarios avanzados y administradores con acceso al SO de Windows®.

- Para evitar la interrupción de las comunicaciones automáticas de servicios remotos, se recomienda que la aplicación de Device Management se cargue en un cliente que funciona continuamente o durante las principales horas de trabajo.

- Recomendamos que los equipos host ejecuten un sistema operativo admitido de Microsoft® Corporation. Aun así, las aplicaciones de Xerox Device Management se pueden ejecutar en Apple® OS 10.9.4 o versiones posteriores utilizando el software de emulación Parallels Desktop. La aplicación no se ejecutará en un entorno Macintosh nativo. Consulte las guías de usuario correspondientes para un soporte más detallado. Se pueden encontrar los requisitos para la ejecución en un sistema operativo Macintosh

- Recomendamos que los equipos host estén actualizados con los últimos parches críticos y versiones de mantenimiento de Microsoft® Corporation.

- El Protocolo de control de transmisión/Protocolo de Internet (TCP/IP) debe cargarse y estar en funcionamiento.

- Se requieren privilegios de administrador para instalar el software de la aplicaciones de Device Management en el dispositivo del cliente.

- Requiere dispositivos habilitados por SNMP y la capacidad de enrutar SNMP en la red. No es necesario habilitar SNMP en el equipo donde se van a instalar las aplicaciones de Xerox® Device Management ni en ningún otro equipo de la red.

- Microsoft® .NET Framework debe instalarse antes que la aplicación.

- La aplicación no debe instalarse en un equipo donde estén instaladas otras aplicaciones basadas en SNMP u otras herramientas de gestión de la impresión de Xerox®, puesto que pueden interferir entre sí.

Configuraciones de la base de datos

- La aplicación instala el motor y los archivos de base de datos de SQL Server Compact Edition (SQL CE) que almacenan datos de la impresora y ajustes de la aplicación en el directorio de instalación. No se requieren licencias de base de datos para la aplicación. Xerox® Device Agent también es compatible con instancias existentes de SQL Server, como se ha descrito anteriormente.

Configuraciones no compatibles

Esta sección describe las configuraciones no compatibles.

- Instalación de la aplicación en un equipo con otra aplicación de Xerox Device Management, como Xerox Device Manager.

- Software nativo del sistema operativo de Mac OS® (Xerox Device Agent solo se puede ejecutar en la plataforma Apple Mac cuando se instala el software de emulación Parallels).

- Cualquier versión de los sistemas operativos de UNIX®, sistemas operativos de Linux®, sistemas de Windows® que ejecutan el cliente Novell, Windows® 7, Windows® XP, Windows® Vista, Windows NT® 4.0, Windows Media® Center, Windows® 2000, Windows® Server 2008 y 2008 R2, Windows® Server 2003, Windows® 8 RT, sistemas operativos que ejecutan servicios de terminal para aplicaciones y la instalación en sistemas de Windows que ejecutan controladores de dominio.

Dado que esta aplicación solo se ha probado en un entorno de VMware® Lab Manager/Workstation, otros entornos virtuales no son compatibles.

7. Procesos y servicios de Xerox® Business

Los siguientes procesos de Xerox Business utilizan los datos recibidos de los dispositivos de impresión basados en Xerox® Office y Xerox® Production, y de aplicaciones de Xerox Device Management como parte de la solución de servicios remotos:

La tabla 5 indica el nombre y la descripción de los procesos y servicios de Xerox Business que están admitidos como parte de la solución de Remote Services.

Nombre del proceso de Xerox Business	Descripción
Lecturas automáticas de los contadores	Los datos de las lecturas de contadores se utilizan en el proceso de facturación.
Reabastecimiento automático de suministros/reabastecimiento automático de las partes	Los tóneres se envían automáticamente a los clientes en función del estado de agotamiento de los consumibles recibido de los dispositivos de impresión. Algunos componentes reemplazables se envían automáticamente a los clientes cuando los necesitan para sus dispositivos de impresión. Estas opciones están disponibles para clientes que optan solo por contratos de consumibles medidos.
Capacidad de servicio (asistente de mantenimiento)	La gestión remota del dispositivo ofrece información detallada de errores que puede consultar el personal de servicio, cuando sea necesario, para agilizar la preparación de una visita in situ o diagnosticar y resolver problemas.
Asistencia de tercer nivel (tecnología/corrección)	El personal de asistencia de productos puede corregir problemas difíciles cuando se le otorga acceso a registros técnicos y de corrección detallados.
Desarrollo de productos	Los datos de uso y rendimiento de la impresora se utilizan para identificar mejoras de producto para futuras versiones.

Los datos básicos del dispositivo de impresión se agregan, transmiten, conservan y archivan en un centro de datos de Xerox® certificado por la norma ISO-27001 y se almacenan de acuerdo con las políticas de retención y gestión de datos corporativos de Xerox.

Los procesos y prácticas de trabajo que admiten y protegen los sistemas de software de Remote Services se basan en las prácticas recomendadas de ITIL y las políticas de seguridad de la información de Xerox que se alinean directamente con las normas del sistema de gestión de la seguridad de la información de la Organización Internacional de Normalización (ISO 27002). Los clientes pueden estar seguros de que la gestión, protección y almacenamiento de los datos del dispositivo abarca los principios básicos de la seguridad de la información: confidencialidad, integridad, disponibilidad, autenticación y no repudio.

8. Detalles tecnológicos

Esta sección ofrece detalles técnicos adicionales que normalmente requieren los equipos de tecnología de la información (TI) y profesionales de seguridad que gestionan riesgos mediante la obtención de la garantía de seguridad de las prácticas de desarrollo. Esta garantía les permite certificar nuestros dispositivos de impresión y las aplicaciones de Device Management para su uso en el entorno de red del cliente.

Diseño de software

Nuestro compromiso con la seguridad de los productos de Xerox comienza temprano en el desarrollo de productos, donde los desarrolladores de Xerox siguen un ciclo de vida formal del desarrollo de la seguridad que gestiona los problemas de seguridad mediante la identificación, análisis, priorización, codificación y realización de pruebas. Muchos dispositivos de impresión de Xerox® cuentan con la certificación Common Criteria (ISO IEC 15408) o se encuentran de forma activa en revisión de certificación.

Funcionamiento

Xerox® Remote Services realiza los siguientes tipos de operaciones en la red. Estas operaciones dependen del método de implementación configurado.

Tabla 6.

Método de implemen-tación	Aplicación utilizada	Flujo de datos en la red	Funcionamiento impuesto en la red
Device Direct	Ninguno	Interno	El dispositivo de impresión de Xerox® intenta detectar un servidor proxy web (automático o dirigido a una dirección específica)
		Interno	Los dispositivos de impresión de Xerox® se pueden programar para generar solicitudes a un servidor del protocolo para transferencia simple de correo (SMTP) para enviar notificaciones de alerta por correo electrónico a una lista de destinatarios definida
		Externo a la red	Cada dispositivo de impresión de Xerox® atraviesa el firewall de la empresa para acceder a Internet (HTTPS a través del puerto 443)
		Externo a la red	Cada dispositivo de impresión de Xerox® realiza la autenticación con su certificado en el servidor de comunicación de Xerox remoto antes de transmitir los atributos de datos
		Externo a la red	El dispositivo de impresión de Xerox® transmite automáticamente datos de atributo del dispositivo de impresión por un canal cifrado (HTTPS a través del puerto 443) a los servidores de comunicación de Xerox® a una hora específica cada día o a petición del cliente.

Método de implemen-tación	Aplicación utilizada	Flujo de datos en la red	Funcionamiento impuesto en la red
		Externo a la red	El dispositivo de impresión de Xerox® automáticamente envía solicitudes a los servidores de comunicación de Xerox® por un canal cifrado (HTTPS a través del puerto 443) a una hora específica cada día para que realicen una serie de acciones (p. ej., enviar datos de facturación ahora, añadir servicio, etc.)
		Externo a la red	Transmisión unidireccional bajo demanda de los datos de registro técnicos del dispositivo de impresión de Xerox® por un canal cifrado (HTTPS a través del puerto 443) al servidor de comunicación de Xerox®
Device Direct	Ninguno	Salida, iniciado por desarrolla-dores para obtener el software más reciente	El dispositivo encía una solicitud al servidor de gestión remota del software para buscar actualizaciones de software/seguridad. Si el entorno del cliente no permite realizar actualizaciones de software automáticas, la opción de gestión remota del software se puede desmarcar únicamente sin la interrupción de los servicios remotos estándar.
Aplicaciones de Device Management	Centre Ware® Web	Interno	Cada aplicación detecta un servidor proxy web (automático o dirigido a una dirección específica)
		Interno	Cada aplicación recupera las capacidades de los dispositivos de impresión de la flota mediante SNMP
		Interno	Cada aplicación recupera la configuración de los dispositivos de impresión de la flota mediante SNMP
		Interno	Cada aplicación recupera el estado de los dispositivos de impresión de la flota mediante SNMP
		Interno	Cada aplicación recupera los datos de los consumibles de los dispositivos de impresión de la flota mediante SNMP
		Interno	Cada aplicación puede reiniciar un dispositivo de impresión mediante SNMP o a través de la IU web del dispositivo de impresión
		Interno	Cada aplicación puede enviar una página de prueba a un dispositivo de impresión específico
		Interno	Cada aplicación puede lanzar la página web de un dispositivo de impresión
		Externo **(solo de salida)**	Cada aplicación atraviesa el firewall de la empresa para acceder a Internet (HTTPS a través del puerto 443)
		Externo **(solo de salida)**	Cada aplicación realiza la autenticación con su certificado en el servidor de comunicación de Xerox remoto antes de transmitir los atributos de datos
		Externo **(solo de salida)**	Cada aplicación transmite automáticamente datos de atributo del dispositivo de impresión por un canal cifrado (HTTPS a través del puerto 443) a los servidores de comunicación de Xerox® a una hora específica cada día

Método de implemen-tación	Aplicación utilizada	Flujo de datos en la red	Funcionamiento impuesto en la red
		Externo **(solo de salida)**	Cada aplicación automáticamente envía una solicitud a los servidores de comunicación de Xerox® por un canal cifrado (HTTPS a través del puerto 443) a una hora específica cada día para que realicen una serie de acciones
Aplicaciones de Device Management	Xerox Device Agent Partner Edition para la supervisión de dispositivos de impresión conectados a la red	Interno	Cada aplicación de Xerox Device Agent detecta un servidor proxy web (automático o dirigido a una dirección específica)
		Interno	Cada aplicación de Xerox® Device Agent recupera capacidades de los dispositivos de impresión de la flota mediante SNMP
		Interno	Cada aplicación de Xerox® Device Agent recupera la configuración de los dispositivos de impresión de la flota mediante SNMP
		Interno	Cada aplicación de Xerox Device Agent recupera el estado de los dispositivos de impresión de la flota mediante SNMP.
		Interno	Cada aplicación de Xerox Device Agent recupera los datos de los consumibles de los dispositivos de impresión de la flota mediante SNMP
		Interno	Cada aplicación de Xerox Device Agent puede solicitar que el dispositivo imprima un informe de configuración
		Interno	Cada aplicación de Xerox Device Agent puede lanzar la página web de un dispositivo de impresión
		Interno	Cada aplicación de Xerox Device Agent puede actualizar el software del dispositivo de impresión mediante el envío de un trabajo de impresión. (Archivo .DLM a través del puerto 9100)
		Externo **(solo de salida)**	Cada aplicación de Xerox Device Agent atraviesa el firewall de la empresa para acceder a Internet (HTTPS a través del puerto 443)
		Externo **(solo de salida)**	Cada aplicación realiza la autenticación con su certificado en el servidor de comunicación de Xerox remoto antes de transmitir los atributos de datos
		Externo **(solo de salida)**	Cada aplicación de Xerox Device Agent transmite automáticamente datos de atributo del dispositivo de impresión por un canal cifrado (HTTPS a través del puerto 443) a los servidores de comunicación de Xerox® a una hora específica cada día
		Externo **(solo de salida)**	Cada aplicación de Xerox Device Agent automáticamente envía solicitudes a los servidores de comunicación por un canal cifrado (HTTPS a través del puerto 443) a una hora específica cada día para que realicen una serie de acciones
Aplicaciones de Device Management	Xerox® Device Manager para la supervisión de dispositivos	Interno	Las aplicaciones Xerox Device Manager y Xerox Device Agent detectan un servidor proxy web (automático o dirigido a una dirección específica)
		Interno	Las aplicaciones Xerox Device Manager y Xerox Device Agent recuperan capacidades de los dispositivos de impresión de la flota mediante SNMP
		Interno	Las aplicaciones Xerox Device Manager y Xerox Device Agent recuperan la configuración de los dispositivos de impresión de la flota mediante SNMP

Método de implemen-tación	Aplicación utilizada	Flujo de datos en la red	Funcionamiento impuesto en la red
	de impresión conectados a la red	Interno	Las aplicaciones Xerox Device Manager y Xerox Device Agent recuperan el estado de los dispositivos de impresión de la flota mediante SNMP.
		Interno	Las aplicaciones Xerox Device Manager y Xerox Device Agent recuperan los datos de los consumibles de los dispositivos de impresión de la flota mediante SNMP.
		Interno	Las aplicaciones Xerox Device Manager y Xerox Device Agent pueden solicitar que el dispositivo imprima un informe de configuración
		Interno	Las aplicaciones Xerox Device Manager y Xerox Device Agent pueden lanzar la página web de un dispositivo de impresión
		Interno	Las aplicaciones Xerox Device Manager y Xerox Device Agent pueden actualizar el software del dispositivo de impresión mediante el envío de un trabajo de impresión
		Interno	La aplicación Xerox Device Manager es admite las comunicaciones de SNMPv3 con dispositivos de impresión
		Interno	La aplicación Xerox Device Manager puede realizar cambios en la configuración del dispositivo de impresión mediante SNMP y la IU web
		Interno	La aplicación Xerox Device Manager recupera registros contables basados en el trabajo de determinados equipos multifunción de Xerox®
		Interno	La aplicación Xerox Device Manager gestiona/aplica políticas de control de impresión
		Externo **(solo de salida)**	Las aplicaciones Xerox Device Manager y Xerox Device Agent atraviesan el firewall de la empresa para acceder a Internet (HTTPS a través del puerto 443)
		Externo **(solo de salida)**	Cada aplicación realiza la autenticación con su certificado en el servidor de comunicación de Xerox remoto antes de transmitir los atributos de datos
		Externo **(solo de salida)**	Las aplicaciones Xerox Device Manager y Xerox Device Agent automáticamente transmiten los datos del dispositivo de impresión a los servidores de comunicación de Xerox® por un canal cifrado (HTTPS a través del puerto 443) a una hora específica cada día
		Externo **(solo de salida)**	Las aplicaciones Xerox Device Manager y Xerox Device Agent automáticamente envían una solicitud a los servidores de comunicación de Xerox por un canal cifrado (HTTPS a través del puerto 443) a una hora específica cada día para que realicen una serie de acciones
	Aplicación de Device Management	Externo, bidireccio-nal	Xerox Device Manager se pone en contacto con Xerox Services Manager a diario y permite a los administradores cambiar de forma remota los ajustes, eliminando la necesidad de realizar llamadas de servicio in situ.

9. Funciones de seguridad

PROTOCOLO SIMPLE DE ADMINISTRACIÓN DE REDES (SNMP) PARA XEROX®

El protocolo simple de administración de redes (SNMP) es la herramienta de gestión de redes más utilizada para la comunicación entre sistemas de gestión de red e impresoras de la red. Las aplicaciones de Device Management utilizan SNMP durante las operaciones de detección para recuperar información detallada del dispositivo de impresión. Las aplicaciones de Xerox® Device Management son compatibles con los protocolos SNMP v1/v2 y v3. Consulte las guías de certificación de la aplicación de Xerox® Device Management correspondientes para obtener datos específicos.

El marco de SNMPv3 es compatible con muchos modelos de seguridad, que pueden coexistir en una entidad SNMP. SNMPv3 ofrece mayor seguridad al añadir seguridad criptográfica a SNMPv2. Además, SNMPv3 es compatible con versiones anteriores y se utiliza ampliamente en redes sólidas.

Las aplicaciones de Xerox® Device Management (Centre Ware® Web/Xerox Device Manager, Xerox Device Agent) puede comunicarse con las plataformas de dispositivos que cumplan con lo dispuesto en Federal Information Processing Standard FIPS 140-2 con respecto a sus implementaciones de SNMPv3.

Las aplicaciones de Xerox® Device Management no utilizan el servicio SNMP de Windows ni el servicio de captura de SNMP de Windows. Si ya estaban instalados, estos servicios **deben** deshabilitarse en cualquier equipo personal o servidor donde la aplicación de Xerox Device Management esté instalada.

Las aplicaciones de Xerox Device Management utilizan un agente SNMP desarrollado por Xerox que:

- Contiene un mecanismo especial de codificación/descodificación
- Está completamente gestionado por .NET
- Usa un ejecutable .NET de tiempo de funcionamiento: esto ofrece una seguridad mejorada para evitar los ataques contra las vulnerabilidades del software, como la manipulación de punteros no válida, los desbordamientos de búfer y las comprobaciones de límites.

Las aplicaciones de Xerox Device Management utilizan funciones de seguridad disponibles en el sistema operativo (SO) de Windows, entre las que se incluyen:

- Autenticación y autorización de usuarios
- Configuración y administración de servicios
- Despliegue y administración de política de grupos

Firewall de conexión a Internet (ICF) de Windows, por ejemplo:

- Configuraciones de registro de seguridad
- Configuraciones ICMP

Aplicaciones de Xerox Device Management: **Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition,** la aplicación SQL CE de Microsoft® SQL Server y **Xerox Device Manager** utilizan Microsoft® SQL Server.

Las aplicaciones de Xerox Device Management se pueden configurar para aprovechar las funciones de seguridad adicionales de Microsoft® para incluir, cuando proceda:

- Habilitación del registro de la cuenta de usuario
- Cifrado del sistema de nombres de dominio (DNS)
- Limitación de los privilegios de la cuenta de usuario para acceder a la base de datos, es decir, los derechos del propietario de la base de datos
- Implementación de números de puerto definidos por el usuario

Se requiere una clave de registro de Xerox y una cuenta válida de Xerox para transmitir datos a los servidores de comunicación de Xerox remotos.

Las comunicaciones externas de las aplicaciones de Xerox Device Management pueden verse afectadas por el firewall de conexión a Internet de Windows. (**Recomendamos** a los clientes que incluyan la URL de Xerox en la lista blanca su firewall (*.support.xerox.com) y especifiquen la dirección IP que puede acceder a la URL)**.**

Las aplicaciones de Xerox Device Management se ejecutan en segundo plano utilizando credenciales de la cuenta del sistema local para enviar solicitudes automáticas a los dispositivos de impresión de la red mediante SNMP y transmitir de forma periódica atributos del dispositivo de impresión a los servidores de comunicación de Xerox

El acceso a la interfaz de usuario (IU) de la aplicación de gestión de dispositivos de Xerox y las funciones están controladas por los siguientes privilegios basados en tareas:

- administradores de Centre Ware® Web, usuarios avanzados de Centre Ware® Web, usuarios de SQL de Centre Ware® Web, administradores de clientes de Centre Ware® Web y grupos de clientes de Centre Ware® Web.
- Los nombres de usuario para las aplicaciones no atraviesan la red; se utilizan tokens de acceso en su lugar (debido al diseño del SO de Windows®).
- La aplicación de Xerox Device Manager ofrece seguridad basada en el control del envío de impresión mediante la restricción de trabajos en función de la política de uso del color, tipo de documento, coste del trabajo, hora, control de acceso de grupos de usuarios, política de impresión a doble capa, impresiones permitidas del trabajo y cuotas de impresión.

Nota: El uso de SNMP de cualquier aplicación de Xerox® Remote Services no supone un riesgo para la seguridad del entorno TI de un cliente, dado que todo el tráfico basado en SNMP generado o consumido por estas aplicaciones se produce en la red interna del cliente, detrás del firewall. El servicio SNMP de Windows y el servicio de captura de SNMP de Windows no están habilitados en el SO de Windows de forma predeterminada.

Modo de seguridad de la empresa

La sincronización ***programada*** por la aplicación de Xerox Device Agent para asegurar el servidor de comunicaciones está configurada de forma predeterminada como *a diario*. Tenga en cuenta que puede configurar la hora a su gusto.

Existen dos modos de seguridad de la empresa: **Normal** y **Bloqueado.**

Cuando está configurada en modo **Normal**, la aplicación de Device Management a diario se pone en contacto con Xerox Services Manager. Los ajustes se pueden cambiar sin la necesidad de realizar visitas in situ, incluso cuando los programas de *polling* están desactivados. ***(Modo recomendado***).

En el modo **Bloqueado**, aparte de la sincronización de datos relacionados con la impresora, no existe comunicación con los servidores de comunicación y los ajustes se deben cambiar in situ. Además, el dispositivo de Xerox Device Agent y las direcciones IP de la impresora no se comunican al servidor de comunicación. Este modo limita los demás beneficios de los servicios remotos para incluir la facturación y el reabastecimiento automatizado, así como los datos de diagnóstico utilizados para el soporte técnico.

Nota: Si una versión de Xerox Device Agent no contiene la pestaña Modo de seguridad de la empresa, funciona en modo Normal.

10. Impacto de la red

Las directrices de la red empresarial normalmente habilitan o deshabilitan puertos de red específicos en enrutadores o servidores. La mayoría de los departamentos de TI se preocupan por los puertos que emplea la aplicación para el tráfico saliente. La inhabilitación de puertos específicos puede afectar a la funcionalidad de la aplicación. Consulte la siguiente tabla para descubrir los puertos específicos que utilizan los procesos de la aplicación. Si se requiere que la aplicación escanee múltiples segmentos de red o subredes, los enrutadores deben permitir los protocolos asociados con estos números de puerto.

Protocolos, puertos y otras tecnologías relacionadas

La tabla 7 identifica los protocolos, puertos y tecnologías que se utilizan en Xerox® Remote Services:

Número de puerto	Protocolo	Descripción del uso	Flujo de datos en la red
Depende de los protocolos de las capas superiores	**Protocolo de Internet (IP)**	**Transporte subyacente para todas las comunicaciones de datos**	**Interno + Externo (solo de salida)**
N/A	Protocolo de mensajes de control de Internet (ICMP)	Detección de un dispositivo de impresión + Resolución de problemas	Interno
25	Servidor del protocolo para transferencia simple de correo (SMTP)	Dispositivo de impresión + Alertas de notificación de correo electrónico de la aplicación proxy remota	Interno
53	Servicios de nombres de dominio (DNS)	Se utiliza para las operaciones de detección de dispositivos de impresión basadas en DNS	Interno
80	Protocolo de transferencia de hipertexto (HTTP)	Consultas de la página web del dispositivo de impresión + Consultas de la página web de la aplicación de Device Management	Interno
135	Llamada a procedimiento remoto (RPC)	Detección de un dispositivo de impresión	Interno

Número de puerto	Protocolo	Descripción del uso	Flujo de datos en la red
161	Protocolo simple de administración de redes (SNMP v1/v2C/v3)	Protocolo estándar del sector que se utiliza para detectar dispositivos de impresión de la red + Recuperación del estado, contadores y datos de consumibles + Recuperación y aplicación de la configuración del dispositivo de impresión. Nombres de la comunidad predeterminados = «público» (GET), «privado» (SET)	Interno
443	Protocolo seguro de transferencia de hipertexto (HTTPS)	Consultas de la página web del dispositivo de impresión (si están configuradas) + Consultas de la página web segura de la aplicación proxy remota (si están configuradas) + Transferencia de los datos del dispositivo de impresión a los servidores de comunicación de Xerox® + Comunicaciones de los controles de impresión a Xerox® Device Manager	Interno + Externo (solo de salida)
515, 9100, 2000, 2105	Envío de un trabajo de impresión de TCP/IP LPR y el puerto RAW	Actualización del software del dispositivo de impresión + Diagnóstico de la impresión de la página de prueba	Interno

11. Prácticas recomendadas de seguridad

- Mantenga siempre actualizados los dispositivos de impresión con el firmware/software más reciente. Xerox supervisa de cerca las vulnerabilidades y proporciona a los clientes de forma proactiva parches y actualizaciones de seguridad en caso necesario.
- Deshabilite los puertos y protocolos sin utilizar en los dispositivos de impresión cuando sea posible. Esto se realiza generalmente en la interfaz de usuario (IU) web de los dispositivos de impresión de oficina y en la interfaz de usuario (IU) local de los dispositivos de impresión de producción.
- Utilice las funciones relativas al control de acceso de los usuarios en los dispositivos de impresión, si están disponibles. Esto se realiza generalmente en la interfaz de usuario (IU) web de los dispositivos de impresión de oficina y en la interfaz de usuario (IU) local de los dispositivos de impresión de producción.
- Utilice protocolos seguros cuando sea posible. Esto se realiza generalmente en la interfaz de usuario (IU) web de los dispositivos de impresión de oficina y en la interfaz de usuario (IU) local de los dispositivos de impresión de producción.
- Habilite las funciones de seguridad integradas en el dispositivo (p. ej., sobreescritura de imágenes, cifrado de datos de escaneo, cifrado del flujo de impresión, cifrado del disco, impresión segura, .pdf cifrado, autenticación de acceso CAC/PIV).

Para obtener información adicional sobre Xerox® Remote Services, visite Xerox.com/RemoteServices.

Para obtener información adicional y específica sobre los mecanismos y las capacidades de seguridad del conjunto de aplicaciones de Xerox Device Management, consulte sus guías correspondientes:

Xerox Device Agent

Xerox Device Manager

Centre Ware Web

Tanto si se trata de la seguridad de dispositivos como de contenido, Xerox está a la cabeza con seguridad proactiva para las nuevas amenazas que surgen en la actualidad. Visite www.xerox.com/security para acceder a toda la información de seguridad, actualizaciones, boletines, libros blancos, parches y mucho más.