Xerox® Remote Services

Informe sobre seguridad

Versión 2.0

Servicios remotos globales

Administración de información tecnológica de Xerox®

Enero de 2017

BR19369

Se hacen cambios periódicos a este documento. Los cambios, y errores técnicos y tipográficos se corregirán en ediciones posteriores.

IS 614672/IS 514590

Versión del documento: 2.0 (enero de 2017).

Índice

Objetivo general y destinatarios

El objetivo de este documento es servir como guía para implementar Xerox® Remote Services en impresoras conectadas en red tanto de Xerox como de otros fabricantes dentro del entorno del cliente. La intención es proporcionar detalles vinculados con la seguridad y comprender las exhaustivas medidas de seguridad que se implementan a través de Xerox® Remote Services.

Los destinatarios de este documento son los proveedores técnicos, gerentes de redes de TI y profesionales de seguridad informática que estén interesados en las capacidades de Remote Services y la implementación de seguridad de dichas funciones.

Recomendamos que se lea este documento en su totalidad para certificar el uso de los productos y servicios Xerox® dentro del entorno de red del cliente.

Remote Services

La información es un recurso clave, y la seguridad es de importancia crucial para todos los recursos de la empresa, inclusive los dispositivos de impresión multifunción (MFP) conectados en red. Dentro del concepto "todo en uno" de hoy día, administrar un conjunto de dispositivos de impresión multifunción y garantizar, a la vez, un nivel aceptable de seguridad presenta una serie de problemas específicos que suelen ser pasados por alto. Xerox® entiende esta complejidad y brinda respuestas a las necesidades de nuestros clientes con respecto a la seguridad. Las propuestas de productos Xerox®, sistemas Xerox® y Xerox® Remote Services están diseñadas para que se integren en forma segura con los flujos de trabajo actuales de los clientes y, al mismo tiempo, que utilicen las tecnologías de seguridad más actualizadas.

El propósito del Informe sobre seguridad de Xerox® Remote Services es ayudar al cliente a comprender e implementar la solución segura y adecuada de Remote Services que sea compatible con la infraestructura de red del cliente. La construcción de la red del cliente determinará si es necesario hacer cambios al cortafuegos de Internet, servidores proxy de web o cualquier otra infraestructura de red vinculada con la seguridad. La solución de Xerox® Remote Services, el dispositivo y los controles elegidos dependen de las políticas de seguridad informática del cliente y determinarán qué modo de operación hay que usar.

La capacidad de Xerox® Remote Services está disponible en determinados modelos de equipos. Esta capacidad permite que los dispositivos de impresión reciban servicios y asistencia técnica en forma remota a través de los datos de los atributos del dispositivo de impresión que incluyen*: identidad del dispositivo de impresión, propiedades del dispositivo de impresión, estado, niveles de consumibles, datos de uso y datos detallados de diagnósticos*. Los datos de los atributos del dispositivo de impresión se transmiten desde el interior del entorno de red del cliente directamente desde el dispositivo de impresión (Device Direct), a través de una aplicación localizada (aplicación de Device Management) o a través de una combinación de ambos métodos, por medio de la ruta de comunicación segura de Xerox® Remote Services. Tanto los dispositivos Xerox® como las aplicaciones de Xerox® Device Management deben contar con un certificado para autenticarse ante los servidores de comunicaciones de Xerox® antes de poder transmitir los atributos de impresión. Las operaciones de Xerox® Remote Services también se originan desde el interior del entorno del cliente y se envían estrictamente según las autorizaciones del cliente.

Los servidores de comunicaciones de Xerox®, ubicados en los Estados Unidos, cumplen con requisitos de seguridad exigentes en cuanto a la administración de la seguridad informática. Los Xerox® Datacenters y la aplicación Xerox® Remote Services adhieren a la Declaración de Normas para Trabajos de Atestificación (Statement on Standards for Attestation, SSAE) n.º 16, los requisitos de cumplimiento establecidos por la Ley Sarbanes-Oxley (SOX) y, además, cuentan con la certificación ISO 27001:2013.

En forma prefijada, no se transmite a los servidores de comunicación de Xerox® ninguna imagen del cliente derivada de trabajos de impresión, escaneado y copia ni tampoco información confidencial.

Controles del cliente

Las aplicaciones de Xerox® Device Management tienen la capacidad de exhibir registros de datos exportados sobre atributos del dispositivo de impresión con fines de auditoría y verificación antes de realizar el cifrado y la transmisión a los servidores de comunicación remotos de Xerox®. Consulte la Guía del usuario de la aplicación Xerox® Device Management para obtener detalles específicos.

Algunos dispositivos de impresión de oficina pequeños y medianos vienen equipados con una función que les permite a los clientes descargar y ver los datos sobre los atributos del dispositivo de impresión antes de realizar el cifrado y la transmisión a los servidores de comunicación remotos de Xerox® a través del método de activación Device Direct. Para verificar si un dispositivo de impresión en particular tiene esta capacidad, vaya a la página de Centreware Internet Services del dispositivo de impresión; ficha Estado, enlace Smart eSolutions (o Remote Services) y abajo de la ficha Maintenance Assistant (Asistente de mantenimiento).

La solución Xerox® Remote Services se puede adaptar a aquellas políticas de seguridad informática del cliente destinadas a limitar o restringir estrictamente la transmisión de determinados tipos de atributos del dispositivo de impresión por fuera de la red (por ejemplo, atributos vinculados con la dirección de red). Las herramientas de la aplicación Xerox® Device Management cuentan con la capacidad de desactivar la transmisión de determinados campos.

Los clientes también tienen la opción de activar una *Solicitud de excepción* durante las negociaciones contractuales para **"dar de baja"** la solución Remote Services. Esta opción impediría todas las comunicaciones de Remote Services y su capacidad de asistencia técnica remota en los dispositivos de impresión que estén dentro de esa cuenta.

Para facilitar las actividades de asistencia técnica remota que hayan llegado a instancias jerárquicas superiores, los clientes pueden activar, si fuera necesario, la función Acceso remoto para recibir actualizaciones de software del dispositivo de impresión, parches de seguridad y diagnosticar, reparar o modificar en forma remota las configuraciones del dispositivo de impresión para corregir los desperfectos diagnosticados. El Acceso remoto no le permite a Xerox® ver o descargar documentos del cliente, datos u otro tipo de información que están alojados en el dispositivo de impresión o en los sistemas informáticos del cliente o que están pasando por dichos dispositivos o sistemas. Una excepción es cuando un cliente está hablando con el personal de asistencia técnica de Xerox acerca de un inconveniente más complejo, y se determina que puede ser necesario contar con más información para resolver el problema. En tal ocasión, el cliente puede decidir darle permiso a Xerox para acceder a los registros almacenados localmente en el dispositivo que sí incluyen datos confidenciales.

Por lo tanto, se invita a los equipos de TI de la empresa y los expertos en seguridad a leer este documento en su totalidad para comprender correctamente las diversas funciones, requisitos y operaciones de Xerox® Remote Services y de qué manera facilitar el cumplimiento de las políticas de seguridad informática del cliente.

En http://www.xerox.com/security, se pueden encontrar recursos adicionales sobre seguridad vinculados con la protección de los datos de seguridad de los productos Xerox®, alianzas industriales y certificaciones.

Modelos de implementación

Los clientes pueden optar por cualquiera de los siguientes modelos de implementación de Xerox® Remote Services, ambos igualmente seguros:

- **Modelo Device Direct:** Device Direct activa los dispositivos de impresión para que se comuniquen en forma directa con los servidores de comunicación remotos de Xerox® a través de Internet y del cortafuegos del cliente.

- **Modelo de aplicación de Device Management:** se puede instalar una aplicación de Xerox® Device Management (también conocida como Device Manager) en una red del cliente para recopilar un subconjunto de atributos de datos de los dispositivos de impresión. Se recopilan varios atributos de los dispositivos de impresión y se transmiten, posteriormente y en forma segura, a los servidores de comunicación remotos de Xerox®.

- **Modelo mixto:** consiste en la implementación conjunta del modelo Device Direct y del modelo de aplicación de Device Management.

Todos los modelos de implementación de Xerox® Remote Services se nutren de los protocolos y puertos conformes a las normas de la industria, basados en la web, con el fin de establecer un canal seguro y cifrado para transmitir atributos de los dispositivos de impresión externamente a los servidores de comunicación de Xerox® ubicados en centros de datos Xerox® seguros y redundantes.

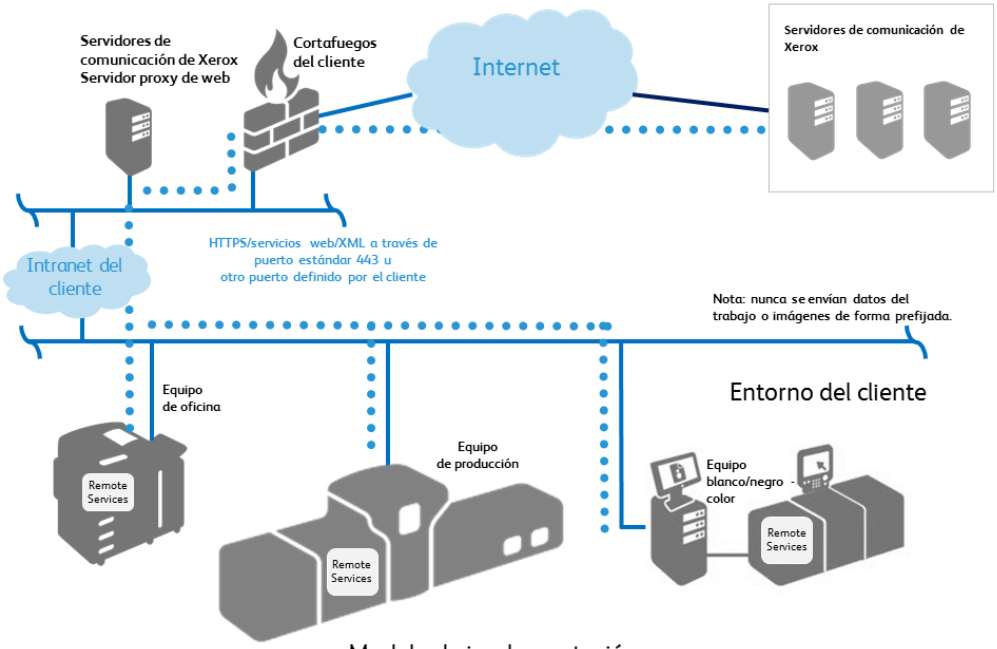
El modelo de implementación elegido depende de las políticas y normas de seguridad informática del cliente para administrar la transmisión de atributos de los dispositivos de impresión, y el tipo de solución de servicio de impresión y dispositivo que se hayan adquirido en Xerox® (servicios de impresión básicos o gestionados).

Modelo de implementación Device Direct

El módulo de servicios remotos (Remote Services) incorporado en los dispositivos Xerox® utiliza una conexión segura de Seguridad de la capa de transporte (TLS) 1.2 a través del puerto estándar 443 para comunicarse externamente con los servidores de comunicación remotos de Xerox®.

- Los dispositivos de impresión dentro del entorno del cliente inician directamente todas las comunicaciones con los servidores de comunicaciones remotos de Xerox®. Se deben establecer en el sitio las configuraciones estándar del cortafuegos para que la comunicación sea posible.
- Debe utilizarse una URL válida para los servidores de comunicaciones remotos de Xerox®.
- Los servidores de comunicaciones de Xerox® están protegidos por un cortafuegos seguro y no se puede acceder a ellos desde Internet.

Figura 1



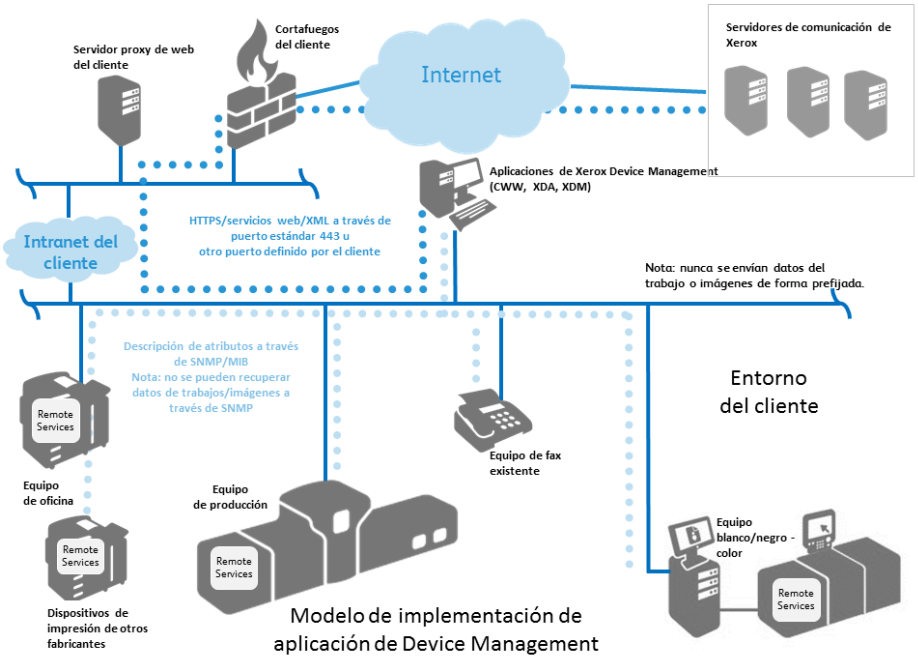
Modelo de implementación Device Direct

Modelo de implementación de aplicación de Device Management

Las aplicaciones de Device Management (es decir, **Xerox® Centre Ware® Web, Xerox® Device Agent, Xerox® Device Agent Partner Edition y Xerox® Device Manager)** también utilizan una conexión cifrada y segura de Seguridad de la capa de transporte (TLS) 1.2 a través del puerto estándar 443 para comunicarse externamente con los servidores de comunicación remotos de Xerox®. Se utilizan funciones adicionales para mejorar la seguridad a través de este canal, que se configuran durante la instalación inicial de las aplicaciones de Device Management:

- La aplicación de Device Management dentro del entorno del cliente inicia todas las comunicaciones con los servidores de comunicaciones remotos de Xerox®. Se deben establecer en el sitio las configuraciones estándar del cortafuegos para que la comunicación sea posible.
- Debe utilizarse una URL válida para los servidores de comunicaciones remotos de Xerox®.
- Los servidores de comunicaciones de Xerox® están protegidos por un cortafuegos seguro y no se puede acceder a ellos desde Internet.
- Debe utilizarse una ID de cuenta válida o un identificador de sitio y una clave de registro de los servidores de comunicaciones de Xerox® para acceder a algunos de los servicios de los servidores de comunicación de Xerox®.
- La aplicación de Device Management solicita el registro en los servidores de comunicaciones remotos de Xerox® mediante las credenciales de autenticación correspondientes.
- Los servidores de comunicaciones remotos de Xerox® validan las credenciales suministradas y aceptan las solicitudes.
- La aplicación de Device Management autentica los servidores de comunicaciones remotos de Xerox® y activa el servicio.

Figura 2

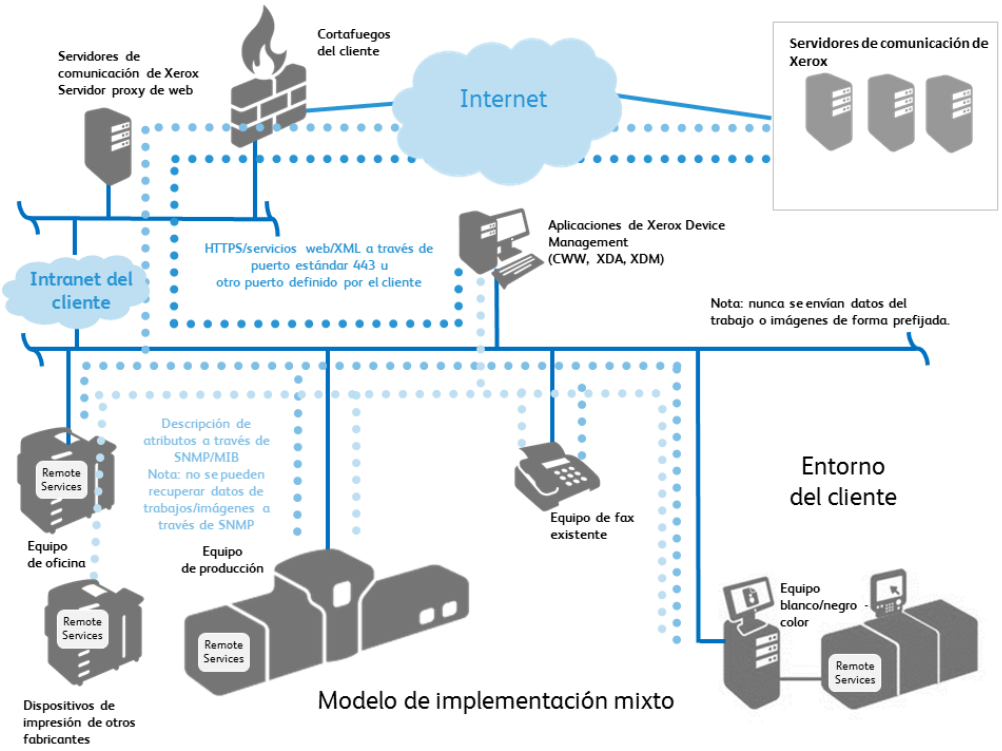


Modelo de implementación de aplicación de Device Management

Modelo de implementación mixto

La implementación mixta es posible cuando un cliente adquiere varios tipos de contratos de mantenimiento de Xerox para sus dispositivos de impresión. Cuando se instala un dispositivo de impresión Xerox® por primera vez en una red, Xerox® Remote Services intenta automáticamente y de forma prefijada que el dispositivo de impresión establezca una conexión directa con los servidores de comunicación de Xerox®.

Figura 3



Transmisión de datos y cargas

Fuentes de datos

Xerox® Remote Services recopila los atributos de datos de dispositivos de impresión de estas fuentes:

- Impresoras de oficina Xerox® conectadas en red
- Dispositivos conectados en red de otros fabricantes
- Impresoras de producción Xerox®
- Aplicaciones de Xerox® Device Management

Dispositivos de oficina Xerox®

Los dispositivos de impresión de oficina Xerox® transmiten los atributos de los datos del dispositivo en formato XML (eXtensible Markup Language), comprimidos en un .zip. Cada archivo se transmite por medio de un canal cifrado a los servidores de comunicación remotos de Xerox®.

Tabla 1: en ella se identifican los atributos de datos del dispositivo que se puedan transmitir y su descripción.

Atributos de datos	Descripción
Identidad del dispositivo de impresión	Incluye el modelo, el nivel de firmware, los números de serie del módulo y la fecha de instalación.
Dirección de red del dispositivo de impresión	Incluye la dirección MAC, dirección de subred.
Propiedades del dispositivo de impresión	Incluye la configuración detallada de los componentes de hardware, la configuración detallada del módulo de software, las funciones y servicios disponibles, los modos de ahorro de energía, etc.
Estado del dispositivo de impresión	Incluye el estado completo, las alertas detalladas, el historial de los 40 últimos errores, información de atascos, etc.
Contadores del dispositivo de impresión	Incluye contadores de facturación, contadores de impresión, contadores de copias, contadores de fax, contadores de trabajos de gran volumen, contadores de escaneado a destino, estadísticas de uso, etc.
Consumibles del dispositivo de impresión	Incluye el nombre del consumible, el tipo (p. ej.: imágenes, acabado, material de impresión), el nivel, la capacidad, el estado, el tamaño, etc.

Atributos de datos	Descripción
Uso detallado de la máquina de impresión	Incluye contadores detallados de impresión, estados de encendido, cantidades detalladas de reposición de CRU, datos detallados de errores de CRU y su distribución, uso de la función integrada OCR, distribución de tiradas, distribución del uso de bandejas, material de impresión instalado, distribución de tipos de materiales de impresión, distribución del tamaño del material de impresión, distribución de longitud de documentos, número fijo, datos de HFSI, datos de MNV, distribución, pixelados establecidos, cobertura media del área por color, errores/atascos, contadores detallados de escaneado.
Ingeniería/ Depuración	Incluye información de depuración detallada que puede incluir datos no abarcados por la lista que provee esta tabla. Estos datos pueden incluir información personal identificable como nombres de usuario, dirección de correo electrónico y datos de trabajos. Estos datos se envían con un permiso expreso del cliente, con la única intención de obtener asistencia técnica en casos que llegaron a instancias jerárquicas superiores.

Nota: el archivo y el contenido de los datos identificados varían en función del modelo de producto.

Dispositivos de producción Xerox®

Los dispositivos de producción Xerox® transmiten los atributos de los datos del dispositivo en formato XML (eXtensible Markup Language), comprimidos en un .zip. Cada archivo se transmite por medio de un canal cifrado a los servicios de comunicación remotos de Xerox®.

Tabla 2: en ella se identifican los atributos de datos del dispositivo que se puedan transmitir y su descripción.

Atributos de datos	Descripción detallada de los atributos de datos
Identidad del dispositivo de impresión	Incluye modelo, niveles del firmware de los módulos, números de serie de los módulos, fechas de instalación de los módulos, datos de contacto del cliente, información sobre la licencia y ubicación, si está disponible.
Dirección de red del dispositivo de impresión	Incluye la dirección MAC, dirección de subred.
Propiedades del dispositivo de impresión	Incluye la configuración detallada de los componentes de hardware, la configuración detallada del módulo de software, las funciones y los servicios disponibles, etc.
Estado del dispositivo de impresión	Incluye estados activos, contadores de historial de errores, registro de eventos del DFE, historial de transmisión de datos.
Contadores del dispositivo de impresión	Incluye contadores de facturación, contadores de impresión, contadores de copias, contadores de trabajos de gran volumen, contadores específicos de producción, contadores de escaneado a destino en modelos de producción de poco volumen, etc.
Consumibles del dispositivo de impresión	Incluye el fabricante, modelo, número de serie, nombre, tipo, nivel, capacidad, estado, contadores de vida útil, etc.
Uso detallado de la máquina de impresión	Incluye información de HFSI, datos de MNV, sustitución de piezas, registros del DFE, datos detallados de diagnósticos, resolución de errores.
Ingeniería/ Depuración	Incluye datos detallados no estructurados sobre depuración solo para uso del servicio de asistencia de tercer nivel.
Relacionados con trabajos del cliente	Los productos de impresión de producción Xerox® proveen la capacidad de reproducir datos relacionados con el trabajo para situaciones de asistencia técnica que lleguen a instancias jerárquicas superiores a través de comandos cifrados PostScript para Xerox. El cliente puede controlar si desea activar esta función o no. Si el cliente elige retransmitir los datos relacionados con un trabajo (es decir, PostScript cifrado) a Xerox, la información se utiliza conforme a las políticas y las normas de seguridad informática de Xerox.

Hay casos de asistencia técnica que llegan a instancias jerárquicas superiores, donde la información de depuración puede incluir atributos de datos por fuera del grupo de datos identificados en las tablas 1-3. Estos datos se envían con el permiso expreso del cliente y se manejan de acuerdo con las políticas y normas de seguridad informática de Xerox.

Nota: el archivo y el contenido de los datos identificados varían en función del modelo de producto.

Aplicaciones de Xerox® Device Management

Las aplicaciones de Xerox® Device Management (es decir, Xerox® Centre Ware® Web (**CWW**), Xerox® Device Agent (**XDA**) , Xerox Device Agent Partner Edition (**XDA PE**) y Xerox® Device Manager (**XDM**) transmiten los datos de atributos de impresión en formato XML (eXtensible Markup Language), comprimidos en un .zip. El archivo se cifra posteriormente y se transmite por medio de canales cifrados a los servidores de comunicaciones remotos de Xerox®.

Tabla 3: en ella se identifican los atributos de datos del dispositivo que se puedan enviar por medio de la aplicación Xerox® Device Management y su descripción.

Atributos de datos	Descripción detallada de los atributos de datos
Identidad del dispositivo de impresión	Incluye fabricante, modelo, descripción, nivel del firmware, número de serie, etiquetas de activos, nombre del sistema, contacto, ubicación, estado de gestión, estación de trabajo (de escritorio), número de fax y nombre de la cola.
Dirección de red del dispositivo de impresión	Incluye la dirección MAC, dirección IP, nombre DNS, máscara de subred, puerta de enlace prefijada de IP, última dirección IP conocida, dirección IP cambiada, zona horaria, dirección IPX, número de red externa de IPX, servidor de impresión de IPX.
Propiedades del dispositivo de impresión	Incluye componentes instalados, descripción de los componentes, funciones y servicios disponibles, velocidad de impresión, compatibilidad de color, opciones de acabado, compatibilidad dúplex, tecnología de marcado, disco duro, RAM, idiomas disponibles, propiedades definidas por el usuario.
Estado del dispositivo de impresión	Incluye estado completo, alertas detalladas, mensajes de la consola local, estado de los componentes, información relacionada con la recuperación del estado, fecha de detección, método/tipo de detección, tiempo de funcionamiento, capturas ("traps") disponibles/habilitadas.
Contadores del dispositivo de impresión	Incluye contadores de facturación, contadores relacionados con la impresión, contadores relacionados con las copias, contadores relacionados con el fax, contadores relacionados con trabajos de gran volumen, contadores relacionados con el escaneado, estadísticas de uso y volumen establecido.
Consumibles del dispositivo de impresión	Incluye el nombre del consumible, el tipo (p. ej.: imágenes, acabado, material de impresión), el nivel, la capacidad, el estado, el tamaño, etc.
Uso detallado del dispositivo de impresión	Información de seguimiento de trabajos del usuario que incluye características del trabajo (ID, nombre del documento, propietario, tipo de documento, tipo de trabajo, color, dúplex, material de impresión requerido, tamaño, páginas, juegos, errores), destino (dispositivo de impresión, modelo, nombre DNS, dirección IP, dirección MAC, número de serie), resultados de impresión del trabajo (hora de envío, tiempo de impresión del trabajo, páginas en color/blanco y negro impresas, modo de color usado, Varias en 1), datos de contabilidad (código de retrofacturación, precio de retrofacturación, fuente de contabilidad), origen del trabajo impreso (estación de trabajo, nombre del servidor de impresión/dirección MAC, nombre de la cola, puerto, nombre de usuario, ID del usuario), información gestionada por Xerox (enviada a Xerox® Services Manager).

Atributos de datos	Descripción detallada de los atributos de datos
Identidad de Device Management	Incluye información del PC host como el nombre DNS, dirección IP, nombre del sistema operativo, tipo de sistema operativo, CPU del PC, tamaños de la RAM (libre/usada), tamaños del disco duro (libre/usado), nombre del sitio, versión de la aplicación, fecha de caducidad de la licencia de la aplicación, versión de .Net, zona horaria, versión del componente de detección, tamaño de la base de datos principal, tamaño de la base de datos de detección, número de impresoras gestionadas o no, servicios críticos ejecutados.
Modo de seguridad de la corporación de Device Manager	**Modo normal** = Xerox® Device Agent se pone en contacto con Xerox® Services Manager todos los días. Los ajustes se pueden modificar en forma remota sin necesidad de recibir la visita del técnico en la empresa, inclusive cuando están desactivados los programas de sondeo. **Modo bloqueado** = Además de la sincronización de los datos relacionados con la impresora, no hay ninguna comunicación con Xerox® Services Manager y los ajustes se deben cambiar en el sitio. Se le informan a Xerox® Services Manager las direcciones IP de la máquina de Xerox® Device Agent y de la impresora.
Política de control de impresión de Device Management	Incluye nombre del PC del usuario final, servidor de impresión usado, cola de impresión usada, fecha y hora de las infracciones, nombre del documento, nombre de usuario final, dúplex del trabajo, color del trabajo, número de impresiones en total del trabajo, precio del trabajo, acción realizada, usuario final notificado, mensaje mostrado, nombre de la política de impresión, norma de la política de impresión.

Administración remota de las dispositivos de impresión

El personal de asistencia técnica de Xerox® puede procesar las siguientes acciones a través de la aplicación Xerox® Device Management. Cuando están permitidas, estas acciones se llevan a cabo para respaldar los esfuerzos que requieren la resolución de una anomalía y se delinean abajo, en la **Tabla 4**.

Datos	Descripción
Acciones para realizar en los dispositivos de impresión	• **Obtener estado del dispositivo** = obtener el último estado del dispositivo de impresión • **Reiniciar dispositivo** = iniciar una secuencia de apagado/encendido en el dispositivo de impresión • **Actualizar dispositivo** = instalar software y/o firmware nuevo en el dispositivo de impresión (.DLM (administrador de descargas) a través del puerto 9100) • **Solución de problemas del dispositivo** = hacer "ping" al dispositivo + recuperar el último estado del dispositivo de impresión • **Imprimir página de prueba** = enviar un trabajo de prueba a un dispositivo de impresión para validar la ruta de impresión (generar un informe de configuración) • **Iniciar administración del dispositivo** = iniciar transferencias de datos del dispositivo de impresión en forma periódica a los servidores de comunicación externos de Xerox® **Nota:** el uso de cada acción se puede desactivar bajo demanda en la parte de configuración de la administración de las aplicaciones de Xerox® Device Management que sean compatibles con esta función.
Acciones para realizar en los dispositivos de impresión	• **Reiniciar dispositivo** = iniciar una secuencia de apagado/encendido en el dispositivo de impresión • **Imprimir página de prueba** = enviar un trabajo de prueba a un dispositivo de impresión para validar la ruta de impresión (generar un informe de configuración)
Acciones para realizar en las aplicaciones de Device Management	Los ajustes que se pueden gestionar en cada aplicación de administración de dispositivos (Device Management) son: operaciones de detección, frecuencia de exportación de los datos, ajustes relacionados con la comunicación SNMP (reintentar, tiempo de espera, nombres de comunidad), perfiles de alerta y frecuencia de actualización automática del software de la aplicación de administración de dispositivos (Device Management).

Requisitos del sistema para aplicaciones de Device Management

Los requisitos mínimos varían ligeramente en función de la oferta. Consulte la Guía del usuario o la guía Security Evaluation Guide (Guía de evaluación de la seguridad) y/o Guía de certificación para conocer los requisitos estándar específicos para la aplicación de administración de dispositivos (Device Management) en cuestión. Si desea obtener detalles adicionales, visite: http://www.support.xerox.com/support/enus.html

Después de la instalación, se incluye un archivo .readme (.léame) para identificar requisitos del sistema adicionales y específicos para la aplicación de administración de dispositivos (Device Management) que se desea instalar.

- Se recomienda que los PC host tengan un sistema operativo provisto por Microsoft® Corporation que sea compatible. Sin embargo, las aplicaciones de Xerox® Device Management se pueden ejecutar con un sistema operativo de Macintosh si tienen un emulador de Parallels Desktop. (No puede ejecutar la aplicación Xerox® Device Management en un entorno Macintosh nativo). Consulte las Guías del usuario de la aplicación Xerox® Device Management para obtener detalles adicionales.
- Se recomienda que los PC host tengan instalados los parches y actualizaciones importantes más recientes de Microsoft® Corporation.
- Debe estar instalado y activado el protocolo de control de transmisiones en red/protocolo de Internet (TCP/IP).
- Se debe tener conexión a Internet.
- Se deben tener privilegios administrativos para instalar el software de la aplicación Device Management en la máquina cliente.
- Se requieren dispositivos habilitados para SNMP y la capacidad para encaminar SNMP por la red. No es necesario habilitar SNMP en el PC donde se instalarán las aplicaciones de Xerox® Device Management u otros PC conectados en red.
- Debe instalar Microsoft®.NET Framework 4.6 (versión completa) antes de instalar la aplicación.
- La aplicación no debe instalarse en un PC donde estén instaladas otras aplicaciones basadas en SNMP u otras herramientas de Xerox® Device Management, dado que ello podría interferir en su funcionamiento.

Configuraciones no admitidas

- La instalación de la aplicación en un PC con otra aplicación de Xerox® Device Management, como Xerox® Device Manager
- Cualquier sistema operativo Unix® o Linux®
- Los sistemas operativos Microsoft® que estén al final de su vida útil, como Windows NT® 4.0, Windows® Media Center, Windows® XP y Windows® Server 2000 y 2003.
- Entornos virtuales diferentes a VMware® Lab Manager™/Workstation/vSphere Hypervisor™. La aplicación puede funcionar con otros entornos virtuales; sin embargo, no se han hecho pruebas al respecto.

Procesos y servicios empresariales de Xerox®

Los datos recibidos por los servidores de comunicación de Xerox® de dispositivos de impresión de oficina Xerox®, dispositivos de impresión de producción Xerox® y las aplicaciones de Xerox® Device Management son utilizados por los siguientes procesos empresariales de Xerox:

Nombre del proceso empresarial	Descripción
Lecturas automáticas de contadores	Se genera automáticamente una factura a partir de los datos del contador recibidos desde los dispositivos de impresión.
Reposición automática de suministros/piezas	El tóner se envía automáticamente a los clientes cuando se recibe el estado "agotado" del consumible desde los dispositivos de impresión. Los componentes reemplazables se envían automáticamente a los clientes cuando es necesario para los dispositivos de impresión. Estas opciones solo están disponibles para clientes que disponen de contratos de suministros por contador.
Mantenimiento (Maintenance Assistant)	El personal de servicio de Xerox puede ver información detallada sobre los errores, siempre que sea necesario, para agilizar la preparación de una visita a las instalaciones o realizar un diagnóstico en forma remota y revolver los problemas.
Asistencia de nivel 3 (Ingeniería/depuración)	El personal de asistencia del producto puede solucionar problemas difíciles cuando se le proporciona acceso a los registros detallados de ingeniería y depuración.

Los datos básicos del dispositivo de impresión se comprimen, transmiten, conservan y archivan en un centro de datos de Xerox® certificado por la norma ISO-27001 y según la política corporativa de manejo de datos de Xerox®.

Los procesos y prácticas de trabajo que respaldan y protegen los sistemas de software de Xerox® Back office Remote Services se basan en las mejores prácticas de ITIL y en las políticas de seguridad informática de Xerox que se basan, a su vez, en las normas ISO 27001. Los clientes pueden estar seguros de que la gestión de la integridad, privacidad y protección de los datos se corresponde con los más elevados estándares.

Información sobre la tecnología

Esta sección permite identificar detalles técnicos adicionales que requieren, por lo general, los equipos de TI y los expertos en seguridad con el propósito de administrar los riesgos, garantizando el cumplimiento de prácticas de desarrollo seguras y, así, permitir la certificación de los dispositivos de impresión y las aplicaciones de Device Management para su uso en el entorno de red del cliente.

Diseño de software

En Xerox®, nuestro compromiso con la seguridad del producto comienza en las primeras fases de desarrollo del producto, ya que adherimos a las mejores prácticas del sector en cuanto a técnicas de codificación seguras, pruebas exhaustivas y análisis para eliminar vulnerabilidades. Xerox® participa activamente en los procesos de certificación, por ejemplo de Common Criteria y en las nuevas normas como P2600 Working Group y Security Development Lifecycle (SDLC).

Operabilidad

Xerox® Remote Services realiza los siguientes tipos de operaciones en una red:

Método de implementación	Aplicación usada	Flujo de datos en la red	Operabilidad impuesta en una red
Device Direct	Ninguna	Interno	El dispositivo de impresión Xerox® intenta detectar un servidor proxy de web (automático o dirigido a una dirección específica)
		Interno	Los dispositivos de impresión Xerox® se pueden programar para que generen solicitudes a un servidor de protocolo simple de transferencia de correo (SMTP) para que envíe una notificación de alerta por correo electrónico a una lista de destinatarios definida
		Externo a la red	El dispositivo de impresión de Xerox® atraviesa el cortafuegos de la empresa para acceder a Internet (HTTPS por el puerto 443)
		Externo a la red	El dispositivo de impresión Xerox® se autentica con su certificado ante el servidor de comunicación remoto de Xerox antes de transmitir cualquier atributo de datos.
		Externo a la red	El dispositivo de impresión Xerox® transmite automáticamente los datos de los atributos del dispositivo de impresión a través de un canal cifrado (HTTPS por el puerto 443) a los servidores de comunicación de Xerox® a una determinada hora de cada día o cuando lo solicite el cliente.

Método de implementación	Aplicación usada	Flujo de datos en la red	Operabilidad impuesta en una red
		Externo a la red	El dispositivo de impresión Xerox® les envía consultas automáticamente a los servidores de comunicación de Xerox® a través de un canal cifrado (HTTPS por el puerto 443), a una determinada hora de cada día, acerca de una lista de acciones que se deben realizar (por ejemplo, enviar ahora la información de facturación, añadir un servicio, etc.)
		Externo a la red	La transmisión unidireccional bajo demanda de los datos del registro de ingeniería del dispositivo de impresión Xerox® a través de un canal cifrado (HTTPS por el puerto 443) al servidor de comunicación de Xerox®
Aplicaciones de Device Management	Centre Ware® Web	Interno	Cada aplicación detecta un servidor proxy de web (automático o dirigido a una dirección específica)
		Interno	Cada aplicación recupera las funciones de los dispositivos de impresión de toda la flota a través de SNMP
		Interno	Cada aplicación recupera la configuración de los dispositivos de impresión de toda la flota a través de SNMP
		Interno	Cada aplicación recupera el estado de los dispositivos de impresión de toda la flota a través de SNMP
		Interno	Cada aplicación recupera los datos de consumibles de los dispositivos de impresión de toda la flota a través de SNMP
		Interno	Cada aplicación puede reiniciar un dispositivo de impresión a través de SNMP o a través de la IU de 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 cortafuegos de la empresa para acceder a Internet (HTTPS por el puerto 443)
		Externo **(solo de salida)**	Cada aplicación se autentica con su certificado ante el servidor de comunicación remoto de Xerox antes de transmitir cualquier atributo de datos
		Externo **(solo de salida)**	Cada aplicación transmite automáticamente los datos de atributos del dispositivo de impresión a través de un canal cifrado (HTTPS por el puerto 443) a los servidores de comunicación de Xerox® a una determinada hora de cada día

Método de implementación	Aplicación usada	Flujo de datos en la red	Operabilidad impuesta en una red
		Externo **(solo de salida)**	Cada aplicación les envía consultas automáticamente a los servidores de comunicación de Xerox® a través de un canal cifrado (HTTPS por el puerto 443), a una determinada hora de cada día, acerca de una lista de acciones que se deben realizar
Aplicaciones de Device Management	Aplicación Xerox® Device Agent Partner Edition para supervisar dispositivos de impresión conectados en red	Interno	Cada aplicación Xerox® Device Agent detecta un servidor proxy de web (automático o dirigido a una dirección específica)
		Interno	Cada aplicación Xerox® Device Agent recupera las capacidades de los dispositivos de impresión de toda la flota a través de SNMP
		Interno	Cada aplicación Xerox®Device Agent recupera la configuración de los dispositivos de impresión de toda la flota a través de SNMP
		Interno	Cada aplicación Xerox®Device Agent recupera el estado de los dispositivos de impresión de toda la flota a través de SNMP
		Interno	Cada aplicación Xerox®Device Agent recupera los datos sobre consumibles de los dispositivos de impresión de toda la flota a través de SNMP
		Interno	Cada aplicación Xerox® Device Agent puede solicitar que el dispositivo imprima un informe de configuración
		Interno	Cada aplicación Xerox® Device Agent puede lanzar la página web de un dispositivo de impresión
		Interno	Cada aplicación Xerox® Device Agent puede actualizar el software del dispositivo de impresión a través del envío del trabajo de impresión. (archivo .DLM por el puerto 9100)
		Externo (**solo de salida)**	Cada aplicación Xerox® Device Agent atraviesa el cortafuegos de la empresa para acceder a Internet (HTTPS por el puerto 443)
		Externo **(solo de salida)**	Cada aplicación se autentica con su certificado ante el servidor de comunicación remoto de Xerox antes de transmitir cualquier atributo de datos
		Externo **(solo de salida)**	Cada aplicación Xerox® Device Agent transmite automáticamente los datos de atributos del dispositivo de impresión a través de un canal cifrado (HTTPS por el puerto 443) a los servidores de comunicación de Xerox® a una determinada hora de cada día

Método de implementación	Aplicación usada	Flujo de datos en la red	Operabilidad impuesta en una red
		Externo **(solo de salida)**	Cada aplicación Xerox® Device Agent les envía consultas automáticamente a los servidores de comunicación de Xerox® a través de un canal cifrado (HTTPS por el puerto 443), a una determinada hora de cada día, acerca de una lista de acciones que se deben realizar
Aplicaciones de Device Management	Xerox® Device Manager para supervisar dispositivos de impresión conectados en red	Interno	Las aplicaciones Xerox® Device Manager/Xerox® Device Agent detectan un servidor proxy de web (automático o dirigido a una dirección específica)
		Interno	Las aplicaciones Xerox® Device Manager/Xerox® Device Agent recuperan las capacidades de los dispositivos de impresión de toda la flota a través de SNMP
		Interno	Las aplicaciones Xerox® Device Manager/Xerox® Device Agent recuperan la configuración de los dispositivos de impresión de toda la flota a través de SNMP
		Interno	Las aplicaciones Xerox® Device Manager/Xerox® Device Agent recuperan el estado de los dispositivos de impresión de toda la flota a través de SNMP
		Interno	Las aplicaciones Xerox® Device Manager/Xerox® Device Agent recuperan los datos sobre consumibles de los dispositivos de impresión de toda la flota a través de SNMP
		Interno	Las aplicaciones Xerox® Device Manager/Xerox® Device Agent pueden solicitar que el dispositivo imprima un informe de configuración
		Interno	Las aplicaciones Xerox® Device Manager/Xerox® Device Agent pueden lanzar la página web de un dispositivo de impresión
		Interno	Las aplicaciones Xerox® Device Manager/Xerox® Device Agent pueden actualizar el software del dispositivo de impresión a través del envío del trabajo de impresión
		Interno	La aplicación Xerox® Device Manager admite comunicaciones SNMPv3 con dispositivos de impresión
		Interno	La aplicación Xerox® Device Manager puede hacer cambios a la configuración del dispositivo de impresión a través de SNMP y la IU de web
		Interno	La aplicación Xerox® Device Manager recupera los registros de contabilidad basados en el trabajo de determinadas impresoras multifunción Xerox®
		Interno	La aplicación Xerox® Device Manager gestiona y hace cumplir las políticas de control de impresiones
		Externo **(solo de salida)**	Las aplicaciones Xerox® Device Manager/Xerox® Device Agent atraviesan el cortafuegos de la empresa para acceder a Internet (HTTPS por el puerto 443)

Método de implementación	Aplicación usada	Flujo de datos en la red	Operabilidad impuesta en una red
		Externo **(solo de salida)**	Cada aplicación se autentica con su certificado ante el servidor de comunicación remoto de Xerox antes de transmitir cualquier atributo de datos
		Externo **(solo de salida)**	Las aplicaciones Xerox® Device Manager/Xerox® Device Agent transmiten automáticamente datos del dispositivo de impresión a los servidores de comunicación de Xerox® a través de un canal cifrado (HTTPS por el puerto 443) a una determinada hora de cada día
		Externo **(solo de salida)**	Las aplicaciones Xerox® Device Manager/Xerox® Device Agent les envían consultas automáticamente a los servidores de comunicación de Xerox® a través de un canal cifrado (HTTPS por el puerto 443), a una determinada hora de cada día, acerca de una lista de acciones que se deben realizar

Protocolo simple de administración de redes (SNMP)

El protocolo simple de administración de redes (SNMP) es la herramienta de administración de redes más usada para las comunicaciones entre los sistemas de administración de redes y las impresoras conectadas en red. Las aplicaciones de Device Management utilizan el protocolo SNMP durante las operaciones de detección para recuperar información detallada sobre el dispositivo de impresión que se encuentra en la red. Las aplicaciones de Xerox® Device Management admiten los protocolos SNMP v1/v2 y v3. Consulte las guías de certificación correspondientes a la aplicación de Xerox® Device Management que corresponda para comprender detalles específicos.

La estructura de SNMP v3 admite varios modelos de seguridad, que pueden coexistir dentro de una estructura de SNMP. SNMPv3 incluye medidas de seguridad más rigurosas, dado que le añade protocolos de seguridad criptográficos a SNMPv2. Además, SNMPv3 es compatible en forma retroactiva con versiones anteriores y se usa ampliamente en varias redes seguras.

Las aplicaciones de Xerox® Device Management (Centre Ware® Web/Xerox® Device Manager) tienen la capacidad de comunicarse con plataformas de dispositivos que adhieren a la norma FIPS 140-2 para la implementación de SNMPv3.

Las aplicaciones de Xerox® Device Management no utilizan el servicio SNMP de Windows o el servicio de Captura de SNMP (SNMP Trap) de Windows. Si estos servicios estuvieran instalados previamente, **deben** desactivarse en cualquier PC o servidor donde se instale la aplicación de Xerox® Device Management.

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

- Contiene un mecanismo de codificación y decodificación especial

- Está completamente administrado por .NET

- Utiliza el archivo ejecutable .NET que proporciona una seguridad mejorada para impedir un ataque a las vulnerabilidades del software como manipulaciones del puntero no válidas, desbordamiento de búfer y comprobación de límites.

Las aplicaciones de Xerox® Device Management utilizan funciones de seguridad disponibles en el sistema operativo Windows, por ejemplo:

- Autenticación y autorización de usuarios

- Configuración y administración de servicios

- Implementación y gestión de políticas de grupos

Cortafuegos de conexión a Internet (ICF) de Windows, que incluye:

- Ajustes para recopilar registros de seguridad

- Ajustes de ICMP

Aplicaciones de Xerox® Device Management: **Xerox® Device Agent, Xerox® Device Agent Partner Edition o Xerox® Device Manager** utilizan Microsoft® SQL Server, una aplicación de SQL CE

La aplicación de Xerox® Device Management se puede configurar para aprovechar las funciones de seguridad adicionales de Microsoft® SQL Server, entre las cuales se incluyen:

- Activación del registro de cuenta de usuario

- Cifrado del sistema de nombres de dominios (DNS)

- Privilegios de cuenta de usuario limitados para acceder a la base de datos (es decir, derechos del propietario de la base de datos)

- Implementación de números de puerto definidos por el usuario

Se requieren una clave de registro y una cuenta válida de Xerox para transmitirles datos a los servidores de comunicaciones remotos de Xerox®.

Las comunicaciones externas de las aplicaciones de Xerox® Device Management pueden verse afectadas por el cortafuegos de conexión a Internet de Windows. (Les **recomendamos** a los clientes que permitan la URL de Xerox en el cortafuegos del cliente y que especifiquen la dirección IP desde la cual se puede acceder a la URL).

Las aplicaciones de Xerox® Device Management se ejecutan como un proceso en segundo plano y usan credenciales de cuenta del sistema local para enviar consultas automáticamente a los dispositivos de impresión conectados en red a través de SNMP y para transmitirles regularmente a los servidores de comunicaciones de Xerox® los atributos de los dispositivos de impresión

El acceso a las interfaces de usuario y las funciones de la aplicación Xerox® Device Manager (XDM) se controla mediante los siguientes privilegios basados en funciones (por ejemplo, administradores de Centre Ware® Web, usuarios avanzados de Centre Ware® Web, usuarios de Centre Ware® Web SQL, administradores de Centre Ware® Web de clientes y grupos de clientes de Centre Ware® Web proporcionados).

Los nombres de usuarios y claves de las aplicaciones no atraviesan la red; en su lugar se usan llaves de acceso ("token") (según el diseño del sistema operativo Windows®).

La aplicación Xerox® Device Manager (XDM) ofrece seguridad basada en el control del envío de impresiones mediante la restricción de trabajos según la política de uso de color, tipo de documentos, costo del trabajo, hora del día, control de acceso de grupo de usuarios, política en cuanto a dúplex, impresiones de trabajos permitidas y cuotas de impresión.

Notas: el uso de SNMP por parte de cualquier aplicación de Xerox® Remote Services no debería implicar un riesgo en cuanto a la seguridad en perjuicio del entorno informático del cliente porque todo el tráfico basado en SNMP generado o consumido por estas aplicaciones se desarrolla en la Intranet del cliente, protegida por el cortafuegos. Los servicios SNMP de Windows y Captura de SNMP de Windows no están habilitados en el sistema operativo Windows en forma prefijada.

Modo de seguridad de la corporación

Además de cualquier sincronización programada de las aplicaciones de Xerox® Device Management con Xerox® Services Manager, hay una sincronización diaria que se hace en forma prefijada. Los dos modos de seguridad de la corporación que existen son **Normal** y **Bloqueado.**

En el modo **normal**, la aplicación de Device Management se pone en contacto con Xerox® Services Manager todos los días cuando todas las demás sincronizaciones programadas hayan sido canceladas ***(modo recomendado***).

En el modo **bloqueado**, además de la sincronización de datos relacionados con la impresora, no hay comunicación con Xerox® Services Manager. Los cambios en estos ajustes deben hacerse en el sitio. (***La sincronización de los datos*** garantiza que la información del dispositivo de impresión enviada desde la aplicación de Xerox® Device Management y lo que se captura en Xerox® Services Manager sean iguales).

En forma prefijada, la aplicación de Xerox® Device Management se pone en contacto con Xerox® Services Manager todos los días y les permite a los administradores cambiar los ajustes en forma remota y así evitar una visita del personal técnico a la empresa. Le recomendamos que no cambie este ajuste. Si el cliente impide que el personal de Xerox brinde asistencia a los dispositivos de impresión en forma remota, la comunicación del dispositivo con Xerox® Services Manager se puede bloquear, excepto la sincronización de los datos de la impresora. En este modo, la aplicación no le envía a Xerox® Services Manager ningún informe sobre un PC o direcciones IP de impresoras o ajustes del sitio, y cualquier cambio de ajuste exige una visita del personal técnico a la empresa directamente.

Nota: si Xerox® Device Agent no contiene la ficha Modo de seguridad de la corporación, funciona en modo Normal.

Protocolos, puertos y otras tecnologías relacionadas

En la siguiente tabla, se identifican los protocolos, puertos y tecnologías que se utilizan en Xerox® Remote Services:

Número de puerto	Protocolo	Descripción de 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/D	Protocolo de mensajes de control de Internet (ICMP)	Detección de dispositivos de impresión + solución de problemas	Interno

Número de puerto	Protocolo	Descripción de uso	Flujo de datos en la red
25	Protocolo simple de transferencia de correo (SMTP)	Dispositivo de impresión + alertas de notificación por correo electrónico de la aplicación de proxy remoto	Interno
53	Servicios de nombres de dominio (DNS)	Se usa para operaciones de detección de dispositivos de impresión basados en DNS	Interno
80	Protocolo de transporte de hipertexto (HTTP)	Consultas de páginas web del dispositivo de impresión + consultas de páginas web de la aplicación de Device Management	Interno
135	Llamada a procedimiento remoto (RPC)	Detección de dispositivos de impresión	Interno
137, 139	NetBIOS	Detección de servidores de impresión	Interno
161	Protocolo simple de administración de redes (SNMP v1/v2C/v3)	Protocolo estándar del sector, utilizado para detectar dispositivos de impresión conectados en red + Recuperar estado, contadores y datos de suministros + Recuperar y aplicar la configuración de los dispositivos de impresión. Nombres de comunidad prefijados = “públicos” (GET), “privados” (SET)	Interno
162	Capturas de SNMP	Nombre de comunidad prefijado = “SNMP_trap”	Interno
389	Protocolo ligero de acceso a directorios (LDAP)	Detección de dispositivos de impresión a través de enumeración de particiones de MS Active Directory + Conjunto de valores de configuración de escaneado + Importación del cliente de Active Directory + Configuraciones de grupos de clientes	Interno
443	Protocolo de transporte de hipertexto seguro (HTTPS)	Consultas de páginas web seguras de los dispositivos de impresión (si están configuradas) + consultas de páginas web seguras de la aplicación de proxy remoto (si están configuradas) + Transferencia de datos de los dispositivos de impresión a los servidores de comunicación de Xerox® + comunicaciones de controles de impresión a Xerox® Device Manager	Interno + Externo (solo de salida)
452	Protocolo de anuncio de servicios (SAP) de Netware	Consultas de detección de dispositivos de impresión por medio del servidor Novell a través de IPX	Interno

Número de puerto	Protocolo	Descripción de uso	Flujo de datos en la red
515, 9100, 2000, 2105	TCP/IP LPR y envío de trabajos de impresión a puerto Raw	Actualización del software del dispositivo de impresión + Diagnóstico de página de prueba de impresión	Interno
631	Protocolo de impresión de Internet (IP)	Detección de dispositivos de impresión	Interno

Las mejores prácticas de seguridad

Mantenga siempre los dispositivos de impresión actualizados con los últimos niveles de firmware/software. Utilice la interfaz de usuario web del dispositivo de impresión o la aplicación de administración de la impresora proporcionada por Xerox® y otros proveedores de impresión para actualizar el firmware/software del dispositivo de impresión.

Deshabilite los puertos y protocolos no usados de los dispositivos de impresión siempre que sea posible. Esto se hace normalmente en la interfaz de usuario web de los dispositivos de impresión de oficina y la interfaz de usuario local de los dispositivos de impresión de producción.

Utilice las funciones relacionadas con el control de acceso de los usuarios en los dispositivos de impresión, si están disponibles. Esto se hace normalmente en la interfaz de usuario web de los dispositivos de impresión de oficina y la interfaz de usuario local de los dispositivos de impresión de producción.

Utilice los protocolos seguros cuando sea posible. Esto se hace normalmente en la interfaz de usuario web de los dispositivos de impresión de oficina y la interfaz de usuario local de los dispositivos de impresión de producción.

Habilite las funciones de seguridad integradas en el dispositivo (p. ej. sobrescritura de imágenes, cifrado de discos, impresión segura, etc.)

Asegúrese de que el cortafuegos de la empresa pueda encaminar los paquetes HTTPS a través del puerto 443 de acuerdo con las políticas de seguridad de la empresa.