VERSIÓN 8.0.0
AGOSTO 2024
702P09306

# Xerox® FreeFlow® Core

Guía de seguridad

BR40387

# Índice

# Descripción general

Este capítulo incluye:

## Finalidad

El propósito de este Guía de seguridad es proporcionar información relacionada con la seguridad de Xerox® FreeFlow® Core. En este contexto, la Seguridad del producto se refiere a la forma en que los datos se almacenan y transmiten, la manera en que el producto se comporta en un entorno de red y la forma de acceder al producto de manera local y remota. En este documento se describen el diseño, las características y las funciones de Xerox® FreeFlow® Core en cuanto a la seguridad de la información y la protección de la información confidencial del cliente.

Este documento no es una guía informativa sobre la seguridad y la conectividad de las funciones y características de Xerox® FreeFlow® Core. Si desea obtener más información acerca de dichas funciones y características, consulte la *Ayuda de Xerox® FreeFlow® Core*. Se asume que el usuario cuenta con un conocimiento operativo de dichos temas.

Los clientes son responsables de la seguridad de su red y del producto FreeFlow. El producto FreeFlow no refuerza la seguridad de ningún entorno de red.

## Audiencia de destino

El público objetivo de este documento son clientes que requieren más información relacionada con la seguridad sobre Xerox® FreeFlow® Core.

## Declinación de responsabilidades

La información incluida en este documento es correcta en la fecha de publicación y se suministra sin ningún tipo de garantía. En ningún caso Xerox® Corporation será responsable de los daños resultantes del uso o del incumplimiento de la información incluida en este documento como, por ejemplo, daños directos, indirectos, accidentales, derivados, pérdida de beneficios o daños especiales, incluso si se ha informado a Xerox® Corporation de la posibilidad de dichos daños.

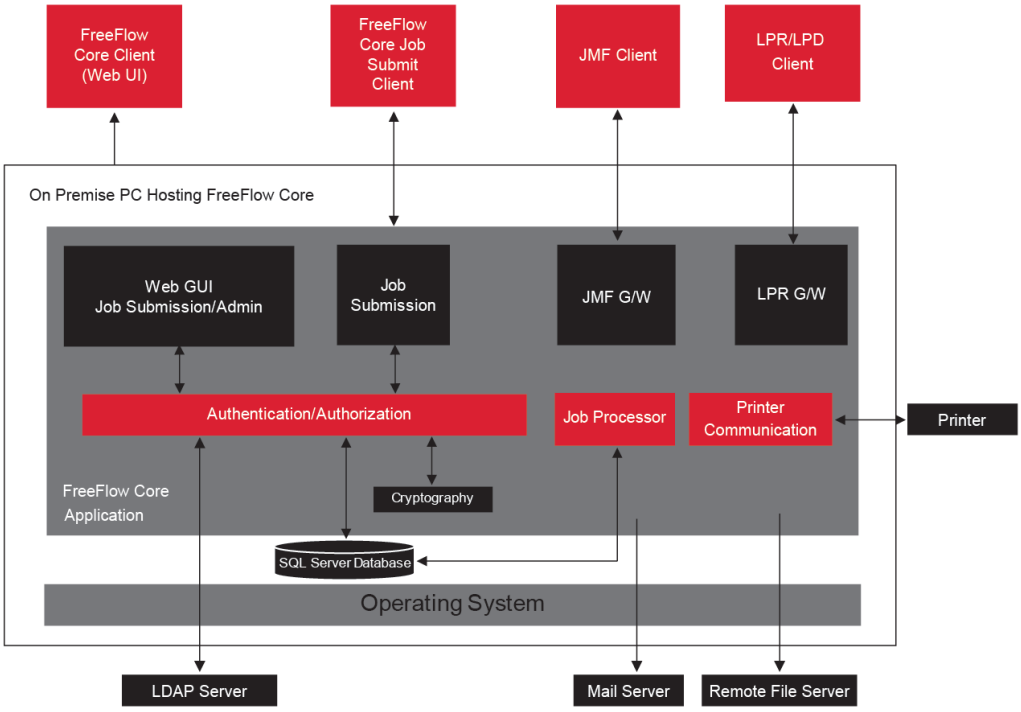
# Descripción del producto

Este capítulo incluye:



Xerox® FreeFlow® Core es la siguiente generación de soluciones de flujos de trabajo de Xerox. FreeFlow Core es una solución basada en el navegador que automatiza e integra el procesamiento de trabajos de impresión de forma inteligente, desde la preparación de los archivos a la producción final. FreeFlow Core proporciona un flujo de trabajo independiente que funciona de forma fácil, se ajusta y adapta rápidamente, y produce resultados homogéneos.

## Estructura de software del sistema



# Aspectos de seguridad de las funciones seleccionadas

Este capítulo incluye:

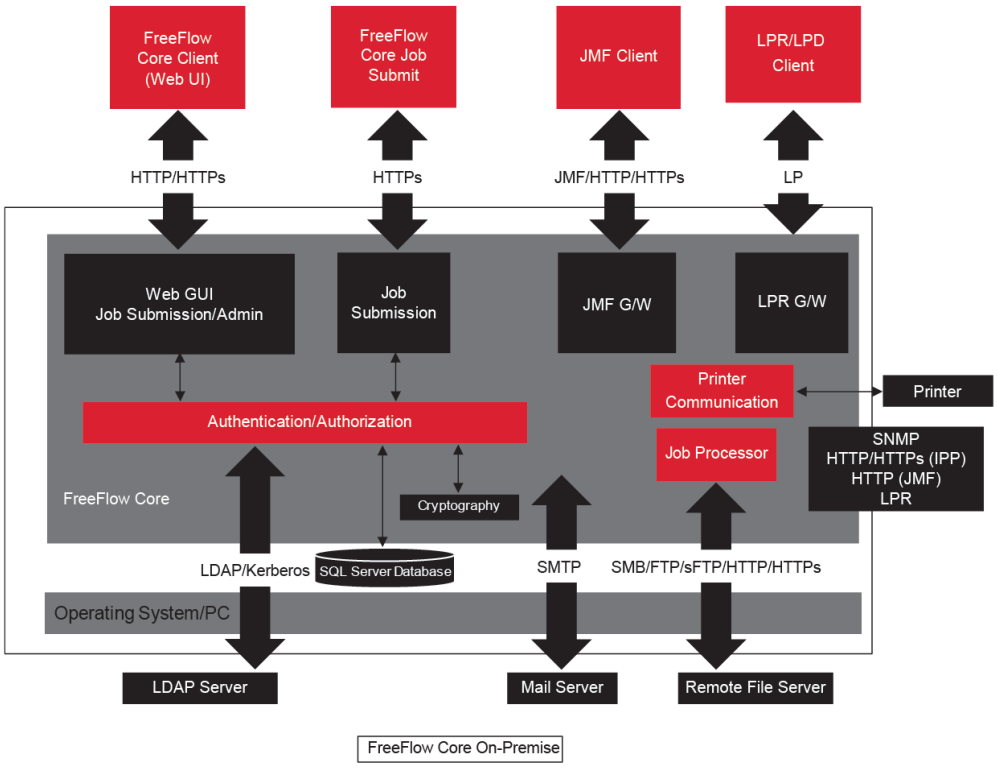
# Acceso al sistema

## CONEXIONES DE RED

Xerox® FreeFlow® Core necesita conectividad de red para el procesamiento de trabajos y para las interacciones de los usuarios. Consulte la información de seguridad de cada conexión de red.

Nota: Para proporcionar una protección y seguridad mejoradas frente los ataques a las vulnerabilidades del sistema, active Windows Firewall en el servidor en el que se instala FreeFlow Core.

FreeFlow Core usa las siguientes conexiones de protocolos de red.




### Cliente de Xerox® FreeFlow® Core

Para conectarse a FreeFlow Core se necesita un navegador web que sea compatible con HTML5 y CSS3. Se necesitan conexiones HTTPS para permitir la descarga segura del cliente de Xerox® FreeFlow® Core y proteger la comunicación entre el cliente y Xerox® FreeFlow® Core.

- Para activar las conexiones HTTPS, agregue un Certificado de servidor a Internet Information Services (IIS). Siga las instrucciones en la documentación de Windows.
- Cuando están activadas las conexiones HTTPS, es necesario activar la opción Requerir SSL en Microsoft Internet Information Services (IIS). Desde el indicativo de comandos de Windows, ejecute el archivo por lotes RequireSSL, situado en el subdirectorio Support del directorio de instalación de FreeFlow Core o en `C:\Program Files\Xerox\FreeFlow Core`.
- FreeFlow Core admite los protocolos criptográficos TLS.

Nota: FreeFlow Core utiliza opciones del sistema operativo que son compatibles con el protocolo TLS. Para garantizar que se utilizan versiones vigentes de protocolos criptográficos, se recomienda que el sistema operativo esté ejecutando la actualización más reciente.

- No se intercambian datos de los usuarios entre el cliente y el servidor de Xerox® FreeFlow® Core a menos que estos descarguen archivos de trabajos.

Nota: El cliente recupera las propiedades del trabajo con datos del usuario.

**Tabla 3.1 Configuración del firewall**

| PUERTO | PROTOCOLO O APLICACIÓN | TIPO DE CONEXIÓN DE FIREWALL |
|---|---|---|
| 80 | HTTP | Entrada<br>Nota: El número de puerto depende de la configuración del servidor de IIS. |
| 443 | HTTPS | Entrada<br>Nota: El número de puerto depende de la configuración del servidor de IIS. |

### Funciones de usuario

Xerox® FreeFlow® Core se abre en una pantalla de inicio de sesión.

- Los usuarios inician sesión en el sistema FreeFlow Core.
- Después de 30 minutos de inactividad, los usuarios conectados se desconectan automáticamente.
- Si se produce un error de autenticación en el software de FreeFlow Core, la aplicación bloquea a los usuarios tras tres intentos de inicio de sesión fallidos.

Nota: En cuanto a las opciones de la cuenta del usuario, consulte Retención de trabajos y acceso a cuentas de usuario. Las opciones las configura el administrador de FreeFlow Core.

Para asignar usuarios a roles de usuarios, consulte en la *Ayuda de Xerox® FreeFlow® Core Configuración de acceso del usuario*.

### Rol Administrador

Los administradores tienen acceso a la totalidad del sistema:

- Roles Administración de trabajos y Estado de trabajos: Cuadro de diálogo Enviar trabajo y pestañas Estado de trabajos.
- Pestañas Administración y Estado de impresoras
- Configuración del flujo de trabajo
- Funciones de la pestaña Administración:
  - Carpeta activa
  - Notificaciones
  - Acceso de usuario
  - Región
  - Seguridad
  - Informes de Core
  - Intercambio de Core
  - Opciones de cola
  - Licencia de Core
- Utilidades del servidor Core disponibles en el escritorio del servidor:
  - Intercambio de FreeFlow® Core
  - Configuración de FreeFlow® Core
  - Informes de FreeFlow® Core para utilidad de línea de comandos

Nota: Un solo administrador puede iniciar sesión simultáneamente en Xerox® FreeFlow® Core.

### Rol Operador

Los operadores tienen acceso a lo siguiente:

- Roles Administración de trabajos y Estado de trabajos: Cuadro de diálogo Enviar trabajo y pestañas Estado de trabajos
- Pestañas Administración y Estado de impresoras

Nota: Varios operadores pueden conectarse simultáneamente a Xerox® FreeFlow® Core.

### Rol Supervisor de estado de trabajos

El rol Supervisor de estado de trabajos tiene acceso de solo lectura a la ventana de la pestaña Estado de trabajos.

Nota: Varios usuarios asignados al rol de supervisor de estado de trabajos pueden conectarse simultáneamente a Xerox® FreeFlow® Core.

### Autenticación de usuario

Las credenciales que se introducen en el cliente del navegador de Xerox® FreeFlow® Core no están cifradas cuando se utiliza HTTP. Para proteger la transmisión, active HTTPS y Requerir SSL en IIS a fin de asegurar el acceso del navegador web a Xerox® FreeFlow® Core.

- Cuando los usuarios se autentican con Xerox® FreeFlow® Core, se descifra la información del usuario. Las credenciales se guardan localmente y se cifran.
- Si los usuarios se autentican con Active Directory, las credenciales no se cifran antes de enviarse a Active Directory. Si la autenticación se realiza a través de Active Directory, las credenciales no se guardan de forma local.
- Puede configurar la autenticación de Xerox® FreeFlow® Core para que emplee un Windows Active Directory existente. Esta configuración emplea las credenciales de escritorio del usuario actual como credenciales de inicio de sesión del cliente Xerox® FreeFlow® Core.

La conexión de la configuración de Xerox® FreeFlow® Core a Active Directory se cifra para la configuración del sistema operativo.

**Tabla 3.2 Configuración del firewall**

| PUERTO | PROTOCOLO O APLICACIÓN | TIPO DE CONEXIÓN DE FIREWALL |
|---|---|---|
| 80 | HTTP | Entrada<br>Nota: El número de puerto depende de la configuración del servidor de IIS. |
| 88 | Kerberos | Salida: Autenticación de usuario<br>Nota: Los números de puerto y los servicios dependen de la configuración de AD del servidor. |
| 389636<br>3268<br>3269 | LDAPLDAP TLS<br>LDAP GC<br>LDAP GC TLS | Salida: Valida grupos de AD durante la configuración de la autenticación de AD<br>Nota: Los números de puerto y los servicios dependen de la configuración de AD del servidor. |

### Conexión de SQL Server

Xerox® FreeFlow® Core se comunica con el servidor SQL mediante Microsoft® Entity Framework. La comunicación cifrada entre Xerox® FreeFlow® Core y el servidor SQL se activa cuando el servidor SQL se configura para usar conexiones cifradas.

Las credenciales cifradas del servidor SQL se guardan de forma local en el servidor de Xerox® FreeFlow® Core.

Para instalar software en el servidor SQL sin privilegios administrativos de SQLS, cree dos bases de datos vacías en la instancia de SQLS:

- `OapMasterDatabase`
- `OapPlatformDatabase`

| PUERTO | PROTOCOLO O APLICACIÓN | TIPO DE CONEXIÓN DE FIREWALL |
|---|---|---|
| 1433 | SQLS | Entrada: Recibe conexiones de Xerox® FreeFlow® Core<br>Salida: Se comunica con el motor de impresión de la base de datos del servidor SQL<br>Nota: El número de puerto depende de la configuración del servidor de SQLS. |
| 1434 | Servicio de explorador SQLS | Entrada: Recibe conexiones de Xerox® FreeFlow® Core<br>Salida: Se comunica con el motor de impresión de la base de datos del servidor SQL<br>Nota: El servidor proporcionará al cliente el número de puerto para la conexión. |

### Interfaz de usuario Enviar trabajo

La interfaz de usuario Enviar trabajo usa la conexión del cliente de Xerox® FreeFlow® Core para realizar el envío de trabajos. Si desea más información, consulte Cliente de Xerox® FreeFlow® Core.

**Tabla 3.3 Configuración del firewall**

| PUERTO | PROTOCOLO O APLICACIÓN | TIPO DE CONEXIÓN DE FIREWALL |
|---|---|---|
| 80 | HTTP | Entrada<br>Nota: El número de puerto depende de la configuración del servidor de IIS. |
| 443 | HTTPS | Entrada<br>Nota: El número de puerto depende de la configuración del servidor de IIS. |

### Carpetas activas

Use recursos compartidos de archivos para compartir carpetas activas locales y para acceder a las carpetas activas en carpetas compartidas de Windows. Use el sistema de archivos de Windows para cifrar carpetas de Windows. Para proteger las carpetas de Windows, use el control de acceso de cuentas de usuarios de Windows.

Nota: Al usar el control de acceso de cuentas de usuario, utilice la misma cuenta de servicio que se usó al realizar la configuración de los *procedimientos de instalación opcionales*. Para obtener más información, consulte la *Guía de instalación de Xerox® FreeFlow® Core*.

Tabla 3.4 Configuración del firewall

| PUERTO | PROTOCOLO O APLICACIÓN | TIPO DE CONEXIÓN DE FIREWALL |
|---|---|---|
| 139, 445 | SMB | Entrada: Comparte carpetas activas mediante el uso compartido de archivos de Windows<br>Salida: Usa carpetas activas en directorios compartidos |
| 20, 21 | FTP | Entrada: Comparte carpetas activas mediante FTP |

### Procesamiento de manifiesto

Durante el envío del manifiesto, Xerox® FreeFlow® Core recupera los archivos incluidos en el manifiesto. Puede hacer referencia a los archivos mediante unidades asignadas, rutas de archivos UNC, URI de sFTP, FTP, HTTP o HTTPS.

Nota: Los URI de HTTP y FTP no son compatibles con el cifrado.

Use recursos compartidos de archivos para compartir carpetas activas locales y para acceder a las carpetas activas en carpetas compartidas de Windows. Use el sistema de archivos de Windows para cifrar carpetas de Windows. Para proteger las carpetas de Windows, use el control de acceso de cuentas de usuarios de Windows.

Nota: Al usar el control de acceso de cuentas de usuario, utilice la misma cuenta de servicio que utilizara al realizar la configuración de los procedimientos de instalación opcionales. Encontrará las últimas instrucciones de activación de la conversión a Office en las *Notas de la versión de Xerox® FreeFlow® Core*. Para obtener el documento, acceda a la página web de FreeFlow® Core en https://xerox.com/automate. En la parte superior de la página, haga clic en **Owner Resources** (Recursos propietario) y, a continuación, en **Notas de la versión**, donde se incluyen todos los requisitos del sistema.

Tabla 3.5 Configuración del firewall

| PUERTO | PROTOCOLO O APLICACIÓN | TIPO DE CONEXIÓN DE FIREWALL |
|---|---|---|
| 139, 145 | SMB | Salida: Recupera archivos que figuran en el manifiesto de directorios compartidos |
| 20, 21 | FTP | Salida: Recupera archivos indicados en el manifiesto |
| 80 | HTTP | Salida: Recupera archivos indicados en el manifiesto |
| 443 | HTTPS | Salida: Recupera archivos mediante la URL HTTPS indicada en el manifiesto |
| 22 | sFTP | Salida: Recupera archivos mediante la FTP segura indicada en el manifiesto |

### Line Printer Daemon (LPD)

Nota: Los comandos LP (Line Printer) no admiten conexiones seguras.

**Tabla 3.6 Configuración del firewall**

| PUERTO | PROTOCOLO O APLICACIÓN | TIPO DE CONEXIÓN DE FIREWALL |
|---|---|---|
| 515 | LP | Entrada: Recibe solicitudes LPR (Line Printer Remote) y comandos LP |
| 721 a 731 | LPR | Salida: Envía solicitudes LPR a una impresora que admita LPD. |

### Señales de estado de la impresora y comandos de JMF

Los comandos de JMF (formato de mensajes de trabajos) y las señales a un cliente JMF admiten conexiones protegidas. La recuperación de archivos JMF admite conexiones HTTPS.

Nota: Para el envío de JMF seguro se requiere el envío de un paquete MIME con archivos JMF, JDF y PDF.

Para habilitar la comunicación HTTPS para los comandos JMF:

1. Para agregar un certificado al depósito de claves de Java, desde el directorio de instalación de Xerox® FreeFlow® Core, use la utilidad `installJMFCertificate.bat`.
2. Reinicie el servicio del servidor JMF de Xerox® FreeFlow® Core.
3. Para probar la instalación, acceda a `http://<nombrehost>:7759/FreeFlowCore`. Si JMF seguro se configura correctamente, el navegador muestra una página de error `HTTP Status 404`.

**Tabla 3.7 Configuración del firewall**

| PUERTO | PROTOCOLO O APLICACIÓN | TIPO DE CONEXIÓN DE FIREWALL |
|---|---|---|
| 7751 | JMF | Entrada: Recibe comandos JMF |
| Varía | JMF | Salida: Devuelve señales de estado JMF de la impresora<br>Nota: El cliente que solicita las señales de estado de la impresora de JMF o la señal de retorno de JMF define el número de puerto requerido. |
| 7759 | sJMF | Entrada: Recibe comandos de JMF seguro |

### Nodos de flujo de trabajo

Componentes de flujo de trabajo que recuperan o guardan archivos de trabajo que pueden usar unidades asignadas, rutas de archivos UNC, URI de FTP o HTTP y HTTPS. Los URI de SFTP admiten la recuperación de archivos de trabajos tipo MAX o JMF.

Nota: Los URI de HTTP y FTP no son compatibles con el cifrado.

Para cifrar recursos compartidos de archivos, use el sistema de archivos de Windows. Para proteger recursos compartidos de archivos, use el control de acceso de cuentas de usuarios de Windows.

Nota: Al usar el control de acceso de cuentas de usuario, utilice la misma cuenta de servicio que se usó al realizar la configuración de los *procedimientos de instalación opcionales*. Para obtener más información, consulte la *Guía de instalación de Xerox® FreeFlow® Core*.

**Tabla 3.8 Configuración del firewall**

| PUERTO | PROTOCOLO O APLICACIÓN | TIPO DE CONEXIÓN DE FIREWALL |
|---|---|---|
| 139, 445 | SMB | Entrada: Recupera archivos especificados en la configuración predefinida de componentes del flujo de trabajo<br>Salida: Almacena archivos en directorios compartidos |
| 20, 21 | FTP | Salida: Recupera archivos especificados en la configuración predefinida de componentes del flujo de trabajo |
| 80 | HTTP | Salida: Recupera archivos especificados en la configuración predefinida de componentes del flujo de trabajo |
| 443 | HTTPS | Salida: Recupera archivos especificados en la configuración predefinida de componentes del flujo de trabajo |

### Impresión Xerox® FreeFlow® Core

Xerox® FreeFlow® Core usa SNMP y HTTP con los comandos IPP, JMF o XBDS para determinar el tipo de servidor de impresión mediante una conexión cifrada. La cadena de comunidad pública de SNMP en el servidor de impresión o la impresora requiere la configuración predeterminada. Si se modificó la cadena de comunidad pública de SNMP en la impresora o el servidor de impresión de la configuración predeterminada, asegúrese de que la opción actualizada esté registrada en FreeFlow Core. Asegúrese de que todas las impresoras registradas en FreeFlow Core tengan la misma cadena de comunidad pública de SNMP. Para obtener instrucciones sobre cómo actualizar la cadena de comunidad pública de SNMP, consulte las Notas de la versión de Xerox FreeFlow Core.

Las siguientes operaciones utilizan una conexión no cifrada:

- Recuperación de la lista de colas del servidor de impresión.
- Recuperación de la lista de impresoras virtuales del servidor de impresión EFI.
- Recuperación de las capacidades de la impresora.

- Operaciones de trabajos en el servidor de impresión.
- Recuperación de información de contabilidad de trabajos. Operación no aplicable a JMF.
- Envío de un trabajo de impresión a una impresora mediante LPR.

El envío de la impresión se cifra si se conecta a un servidor de impresión que está configurado para admitir IPP protegido. Para activar el IPP protegido, use la opción Impresión protegida en la configuración de Destino de impresora. El cifrado TLS y SHA256 se usa entre FreeFlow Core y el servidor de impresión.

**Activación de un envío de impresión con IPP protegido al servidor de impresión FreeFlow**

Para activar el envío de impresión con IPP protegido al servidor de impresión FreeFlow:

1. Agregue un certificado TLS al servidor de impresión FreeFlow.
2. Seleccione **Usar TLS** en la configuración del servidor de impresión Xerox® FreeFlow®.
3. Use el certificado de Xerox® FreeFlow® Core para recuperar el certificado TLS del servidor de impresión FreeFlow.

Nota: Tras una configuración de IPP protegida, se muestra el mensaje El certificado se instaló correctamente.

**Activación de un envío de impresión con IPP protegido a Fiery**

Para activar el envío de impresión con IPP protegido a Fiera, siga estos pasos:

1. Introduzca la dirección IP de Fiery en el navegador web para abrir la IU de Fiery.
2. Seleccione **Fiery Configure** (Configuración de Fiery) en el panel izquierdo.
3. Conéctese con las credenciales del controlador de Fiery.
4. Seleccione **Security** (Seguridad) y cree un certificado autofirmado o rellene los datos con certificados de una autoridad de certificación (CA).
5. Active **SSL\TLS** en la pantalla de configuración.
6. Cuando se activa SSL\TLS, se muestra un mensaje de confirmación para reiniciar el controlador.
7. Seleccione **Sí**.
8. Inicie la **Core Configure Windows Utility** (Utilidad Windows de Configuración de Core) en Xerox® FreeFlow® Core.
9. Seleccione la pestaña **Core Certificate** (Certificado de Core), proporcione la dirección IP del controlador Fiery y seleccione **Recuperar certificado**.

   Se muestra el mensaje El certificado se instalado correctamente.
10. Configure la impresora de Xerox® FreeFlow® Core con la opción de impresión protegida en la pantalla de administración de impresoras.

Xerox® FreeFlow® Core no admite la comunicación con el servidor de impresión mediante JMF seguro.

**Tabla 3.9 Configuración del firewall**

| PUERTO | PROTOCOLO O APLICACIÓN | TIPO DE CONEXIÓN DE FIREWALL |
|---|---|---|
| 161, 162 | SNMP v1/v2 | Salida: Identifica el tipo de servidor de impresión durante la configuración de destino de impresora y la recuperación del certificado. |
| 80 | HTTP | Entrada: La impresora de JDF recupera el archivo de impresión mediante HTTP.<br>Salida: Identifica el tipo de servidor de impresión durante la configuración de destino de impresora y la recuperación del certificado. |
| N/A | ICMP | Salida: Verifica la disponibilidad del dispositivo antes de la recuperación del certificado. |
| 631 | IPP v1.0/v1.1 | Salida: Envía trabajos al servidor de impresión, obtiene el estado de los trabajos y envía comandos de los trabajos al servidor de impresión. |
| 4004 | JMF | Entrada: Recibe el mensaje `ReturnQueueEntry` de JMF de la impresora. |
| Puerto 8010 o JMF definido por impresora | JMF v1.3/v1.4 | Salida: Identifica el tipo de servidor de impresión durante el registro de la impresora y envía un trabajo al servidor de impresión. |
| 443 | HTTPS | Salida: Comunicación de la impresora con el servidor de impresión |
| 515, y de 721 a 731 | LPR | Salida: Envía solicitudes LPR a una impresora que admita LPD. |

### Notificación de correo electrónico

Xerox® FreeFlow® Core es un cliente de correo electrónico que se conecta a un servidor de correo electrónico SMTP accesible o a un servidor de correo electrónico de Google. Las notificaciones de correo electrónico pueden cifrarse y, a continuación, puede conectarse a un servidor de correo compatible con el cifrado. TLS permite el cifrado de las comunicaciones entre el servicio de notificaciones y el servidor SMTP.

Las credenciales cifradas se guardan de forma local.

**Tabla 3.10 Configuración del firewall**

| PUERTO | PROTOCOLO O APLICACIÓN | TIPO DE CONEXIÓN DE FIREWALL |
|---|---|---|
| 25, 465, 587 | SMTP | Salida: Envía notificaciones de correo electrónico<br>Nota: El número de puerto necesario y el uso de la conexión protegida dependen de la configuración del servidor SMTP. |

## Cumplimiento con FIPS y RGPD

Xerox® FreeFlow® Core ejecuta un sistema operativo Windows compatible con FIPS 140-2. Para habilitar la compatibilidad con FIPS, consulte la documentación de Microsoft. De manera prefijada, FreeFlow Core se ejecuta en modo compatible con FIPS.

FreeFlow Core desactiva la compatibilidad con los cifrados DES/3DES.

Si se requiere la impresión con IPP protegido y autenticación implícita, desactive el modo compatible con FIPS para que FreeFlow Core deje de ser compatible con requisitos criptográficos.

Freeflow Core cumple con el Reglamento General de Protección de Datos (RGPD) de la UE.

# Protección de seguridad general

## AUTENTICACIÓN DE CUENTAS DE SERVICIO, UTILIDADES Y LA INTERFAZ DE LÍNEA DE COMANDOS (CLI)

Las cuentas de servicio de FreeFlow Core, Utilidades y CLI ahora utilizan la autenticación de Windows. Para ello, se agrega la cuenta de servicio, o la cuenta de usuario que se encuentre conectada en ese momento, a un grupo de Windows denominado FreeFlow Core Security. Si desea más información, consulte las *Notas de la versión de Xerox FreeFlow Core*.

## PROTECCIÓN DE DATOS DE USUARIOS

### Seguridad de archivos y documentos

FreeFlow Core no cifra explícitamente los archivos enviados para el procesamiento antes de que se almacenen en el sistema de archivos del equipo.

El contenido de origen del documento contiene información de identificación personal u otro tipo de contenido sensible. Por tanto, es responsabilidad del usuario gestionar la información digital de acuerdo con las mejores prácticas de protección de la información.

### Información de identificación personal

Cuando se realiza el registro para obtener una licencia de software de FreeFlow Core, se recopila información de identificación personal. La información es la siguiente:

- Nombre de la empresa
- Clave de activación y número de serie
- ID del host/UUID del sistema
- Nombre del usuario
- Dirección (Calle, Ciudad, Provincia, Código postal, País)
- Dirección de correo electrónico (opcional)

Esta información se transmite de forma segura al host de licencias de Xerox.

La información de identificación personal, en concreto la dirección de correo electrónico del usuario que se utiliza para la recuperación de la clave, se almacena en el sistema FreeFlow Core. La información está cifrada.

## Retención de trabajos y acceso a cuentas de usuario

### CONTRASEÑAS DE CUENTAS DE USUARIO

Se permite la reutilización de una contraseña hasta 10 veces. La cantidad de veces que se puede reutilizar una contraseña es configurable.

### BLOQUEO DE CUENTAS DE USUARIO

Si se produce un error de autenticación mientras se utiliza el cliente de Xerox FreeFlow Core, la aplicación bloquea a los usuarios por 30 minutos tras tres intentos de inicio de sesión fallidos. La cantidad de inicios de sesión fallidos y la duración del bloqueo son configurables.

### CIERRE DE SESIÓN DE CUENTA DE USUARIO

Después de 30 minutos de inactividad, los usuarios conectados al cliente Xerox® FreeFlow® Core se desconectan automáticamente. La duración del periodo de inactividad es configurable.

### ACTIVIDAD DE CUENTAS DE USUARIO

El registro de auditoría de transacciones de inicio de sesión del usuario en FreeFlow Core se ubica en el Visor de eventos de Windows, en la sección **Aplicación** de la carpeta **Registros de Windows**.

### RETENCIÓN DE TRABAJOS

Después de completar el procesamiento de los trabajos, su periodo de retención en FreeFlow Core es de 24 horas.

La impresora FreeFlow Core se configura para cambiar el periodo de retención antes de que los trabajos completados se eliminen automáticamente. Transcurridas 24 horas, el dispositivo FreeFlow Core elimina los trabajos completados.

Para quitar los trabajos de forma manual, use la interfaz gráfica de usuario web de FreeFlow Core.

### PROPIEDADES DEL TRABAJO

Activa la restricción de descarga de archivos definida en Propiedades del trabajo de los trabajos que se muestran en Administración y estado de trabajos de FreeFlow Core.

## Derechos de cuentas de usuario

Para configurar su cuenta de servicio Xerox® FreeFlow® Core, puede utilizar una cuenta local de administrador o bien una cuenta que no sea de administrador. Si utiliza una cuenta que sea miembro del grupo administrador local, no es necesario realizar ninguna acción especial.

Si utiliza una cuenta que no sea de administrador, se le exigirán derechos adicionales, además de los derechos del grupo de usarios estándar. El Configurador de FreeFlow® Core añade los derechos adicionales de manera automática, tal como se enumera en la siguiente tabla:

| CONFIGURACIÓN DE DIRECTIVA DE GRUPO | NOMBRE DE CONSTANTE |
|---|---|
| Actuar como parte del sistema operativo | SeTcbPrivilege |
| Ajustar las cuotas de la memoria para un proceso | SeIncreaseQuotaPrivilege |
| Permitir el inicio de sesión local | SeInteractiveLogonRight |
| Realizar copia de seguridad de archivos y directorios | SeBackupPrivilege |
| Crear un objeto símbolo (token) | SeCreateTokenPrivilege |
| Crear objetos globales | SeCreateGlobalPrivilege |
| Crear objetos compartidos permanentes | SeCreatePermanentPrivilege |
| Depurar programas | SeDebugPrivilege |
| Cargar y descargar controladores de dispositivo | SeLoadDriverPrivilege |
| Iniciar sesión como proceso por lotes | SeBatchLogonRight |
| Iniciar sesión como servicio | SeServiceLogonRight |
| Administrar registro de seguridad y auditoría | SeSecurityPrivilege |
| Realizar tareas de mantenimiento del volumen | SeManageVolumePrivilege |
| Analizar un solo proceso | SeProfileSingleProcessPrivilege |
| Analizar el rendimiento del sistema | SeSystemProfilePrivilege |
| Reemplazar un símbolo (token) de nivel de proceso | SeAssignPrimaryTokenPrivilege |

Nota: Los derechos enumerados en esta tabla se definen en https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-rights-assignment.

# Seguridad

Este capítulo incluye:



Para Xerox, la seguridad es fundamental y prioritaria. Como líder en el desarrollo de tecnología digital, Xerox se compromete a garantizar la seguridad de la información digital mediante la identificación de posibles vulnerabilidades y su resolución para minimizar los riesgos.

Xerox proporciona dispositivos de software con el mayor nivel de seguridad posible, en función de la información y las tecnologías disponibles, a la vez que mantiene el rendimiento, el valor, la productividad y la funcionalidad de los dispositivos.

Para comprobar que los componentes de Xerox® FreeFlow® Core cumplen los requisitos de seguridad correspondientes, se usan herramientas de análisis de vulnerabilidad y penetración comerciales. Las vulnerabilidades de las aplicaciones se tratan a partir de los resultados de los análisis de Xerox.

Xerox distribuye boletines de seguridad según sea necesario. Esta información se comunica en la página web de seguridad de Xerox, en https://www.xerox.com/security (Guía de seguridad del producto). El sitio web contiene el estado de vulnerabilidades de seguridad de la impresora actualizado, notas del producto, certificación Common Criteria, Información de McAfee sobre seguridad de Intel, y un portal para enviar preguntas sobre seguridad a Xerox.

## Protección antivirus

Xerox adopta precauciones especiales para garantizar que el software no incorpora ningún tipo de virus. Xerox recomienda instalar software de detección antivirus y de intrusiones en los puntos de conexión del servidor de FreeFlow Core. Este software y el sistema operativo se mantienen actualizados con las últimas revisiones de seguridad conforme a las recomendaciones de cada distribuidor.

Para mejorar el rendimiento, se recomienda excluir los directorios de instalación de Xerox® FreeFlow® Core y SQL Server del análisis del antivirus.

Puede excluir los archivos siguientes de los análisis antivirus:

- `<Directorio de instalación de FreeFlow Core>\Logs`
- `<Directorio de instalación de FreeFlow Core>\Platform\Logs`
- `<Directorio de instalación de FreeFlow Core>\JobSubmit\Logs`
- `<Directorio de instalación de FreeFlow Core>\Config`
- `<Directorio de instalación de FreeFlow Core>\Platform\Config`
- `<Directorio de datos de usuarios de FreeFlow Core>\`
- Carpetas fuera del directorio de datos de usuarios de FreeFlow Core usadas por freeFlow Core

# Actualización de software

Xerox no es responsable del estado del sistema operativo que ejecuta Xerox® FreeFlow® Core. Es responsabilidad del cliente mantener el sistema actualizado y asegurarse de que tiene las revisiones adecuadas y se ha configurado correctamente. Actualice Microsoft® Windows® como mínimo una vez al mes.

Cuando actualice Windows, para aplicar la actualización, utilice la opción **Windows Update**. Se recomienda no instalar actualizaciones de versiones preliminares opcionales, ya que pueden afectar a la fiabilidad del servidor de Xerox® FreeFlow® Core.

Puede encontrar actualizaciones de software de FreeFlow Core en https://www.support.xerox.com/support/core/software/enus.html. Los clientes pueden instalar la actualización del software.

# Información y recursos adicionales

### Seguridad en Xerox

Xerox mantiene una página web pública actualizada que contiene la información más actualizada en materia de seguridad relacionada con sus productos. Consulte www.xerox.com/security.

### Respuesta frente a vulnerabilidades conocidas

Xerox ha creado un documento que describe en detalle la gestión de vulnerabilidades de Xerox y la política de divulgación que se emplea para detectar y solucionar las vulnerabilidades en el hardware y software de Xerox. Puede descargarlo desde esta página: https://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html.

### Recursos adicionales

| RECURSO DE SEGURIDAD | URL |
|---|---|
| Preguntas frecuentes relacionadas con la seguridad | www.xerox.com/en-us/information-security/frequently-asked-questions |
| Boletines, avisos y actualizaciones de seguridad | www.xerox.com/security |
| Archivo de noticias de seguridad | security.business.xerox.com/en-us/news/ |
| Xerox Trust Center | https://trust.corp.xerox.com/ |