Guía de funciones de seguridad

Tabla de contenido

Introducción

Definiciones de notas

En esta Guía del usuario se utilizan los siguientes símbolos y convenciones:

IMPORTANTE	IMPORTANTE indica una situación potencialmente peligrosa que, de no evitarse, puede provocar daños materiales o fallos en el funcionamiento del producto.
NOTA	NOTA especifica el entorno operativo, las condiciones de instalación o las condiciones especiales de uso.
	Los iconos de consejos indican sugerencias útiles e información complementaria.
Negrita	Los caracteres en negrita identifican los botones del panel de control del equipo o de la pantalla del ordenador.
Cursiva	El estilo en cursiva tienen por objeto enfatizar puntos importantes o derivarle a un tema relacionado.

Información relacionada

- Introducción

Marcas comerciales

Adobe® y Reader® son marcas comerciales registradas o marcas comerciales de Adobe Systems Incorporated en Estados Unidos y/o en otros países.

Cada compañía cuyo título de software se menciona en este manual tiene un Contrato de Licencia de software específico de sus programas registrados.

Cualquier nombre comercial y nombre de producto de las compañías que aparecen en los productos de Brother, documentos relacionados y otros materiales, son marcas comerciales o marcas comerciales registradas de las respectivas compañías.

Información relacionada

- Introducción

Copyright

Información relacionada

- Introducción

Antes de utilizar las funciones de seguridad de red

El equipo emplea algunos de los protocolos de seguridad de red y encriptación más recientes disponibles en la actualidad. Estas funciones de red se pueden integrar en su plan general de seguridad de red para ayudar a proteger sus datos y evitar accesos no autorizados al equipo.

Recomendamos desactivar los protocolos FTP y TFTP. El acceso al equipo utilizando estos protocolos no es seguro.

Información relacionada

- Introducción
  - Desactivar protocolos innecesarios

Desactivar protocolos innecesarios

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como "**Pwd**". Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. En la barra de navegación izquierda, haga clic en **Red** > **Red** > **Protocolo**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ≡.
5. Desmarque las casillas de verificación de los protocolos innecesarios para desactivarlos.
6. Haga clic en **Enviar**.
7. Reinicie el equipo Brother para activar la configuración.

Información relacionada

- Antes de utilizar las funciones de seguridad de red

Seguridad de red

- Configurar certificados para la seguridad de los dispositivos
- Utilizar SSL/TLS
- Utilizar SNMPv3
- Utilizar IPsec
- Utilizar Autenticación IEEE 802.1x para la red

Configurar certificados para la seguridad de los dispositivos

Debe configurar un certificado para administrar el equipo incorporado en red mediante SSL/TLS de manera segura. Debe utilizar Administración basada en Web para configurar un certificado.

- Información general de las funciones de los certificados de seguridad
- Cómo crear e instalar un certificado
- Crear un certificado autofirmado
- Creación de una solicitud de firma de certificado (CSR) e instalación de un certificado de una autoridad de certificación (CA)
- Importar y exportar el certificado y la clave privada
- Importar y exportar un certificado de CA

Información general de las funciones de los certificados de seguridad

Su equipo es compatible con el uso de varios certificados de seguridad, lo que permite una autenticación y comunicación seguras con el equipo. Con este equipo pueden utilizarse las siguientes funciones de los certificados de seguridad:

Las funciones, opciones y ajustes compatibles pueden variar en función del modelo.

- Comunicación SSL/TLS
- Autenticación IEEE 802.1x
- IPsec

Su equipo admite lo siguiente:

- Certificado preinstalado

  El equipo tiene un certificado preinstalado autofirmado. Este certificado permite utilizar la comunicación SSL/TLS sin crear o instalar un certificado diferente.

El certificado autoemitido preinstalado protege su comunicación hasta un determinado nivel. Para disfrutar de una mayor seguridad, recomendamos utilizar un certificado emitido por una organización de confianza.

- Certificado autofirmado

  El servidor de impresión emite su propio certificado. Mediante este certificado, puede utilizar fácilmente la comunicación SSL/TLS sin crear o instalar un certificado diferente de una CA.
- Certificado de una autoridad de certificación (CA)

  Existen dos métodos para instalar un certificado de una CA. Si ya dispone de un certificado de una CA o si desea utilizar un certificado de una CA externa de confianza:

  - Al utilizar una solicitud de firma de certificado (CSR) desde este servidor de impresión.
  - Al importar un certificado y una clave privada.
- Certificado de CA (autoridad de certificación)

  Para utilizar un certificado de CA que identifica la CA y posee su clave privada, debe importar ese certificado de CA de la CA antes de configurar las funciones de seguridad de la red.

- Si desea utilizar la comunicación SSL/TLS, es recomendable que se ponga en contacto con el administrador del sistema en primer lugar.
- Si se restablece el servidor de impresión a sus valores predeterminados de fábrica, el certificado y la clave privada que se encuentran instalados se eliminarán. Si desea mantener el mismo certificado y la clave privada después de restablecer el servidor de impresión, expórtelos antes de restablecerlos y vuelva a instalarlos.

Información relacionada

- Configurar certificados para la seguridad de los dispositivos

Información adicional:

- Configurar la autenticación IEEE 802.1x para su red mediante Administración basada en Web (navegador web)

Cómo crear e instalar un certificado

Hay dos opciones al seleccionar un certificado de seguridad: usar un certificado autofirmado o usar un certificado de una autoridad de certificación (CA).

Opción 1

Certificado autofirmado

1. Cree un certificado autofirmado usando Administración basada en Web.
2. Instale el certificado autofirmado en el ordenador.

Opción 2

Certificado emitido por una CA

1. Cree una solicitud de firma de certificado (CSR) con Administración basada en Web.
2. Instale el certificado emitido por la CA en su equipo Brother con Administración basada en Web.
3. Instale el certificado en el ordenador.

Información relacionada

- Configurar certificados para la seguridad de los dispositivos

Crear un certificado autofirmado

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como **"Pwd"**. Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. En la barra de navegación izquierda, haga clic en **Red** > **Seguridad** > **Certificado**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ≡.
5. Haga clic en **Crear certificado autofirmado**.
6. Introduzca un **Nombre común** y una **Fecha válida**.
   - La longitud del **Nombre común** es de menos de 64 bytes. Introduzca un identificador, como una dirección IP, un nombre de nodo o un nombre de dominio, para utilizarlo al acceder a este equipo mediante comunicación SSL/TLS. El nombre del nodo aparece de forma predeterminada.
   - Si utiliza los protocolos IPPS o HTTPS e introduce en la dirección URL un nombre distinto del **Nombre común** utilizado para el certificado autofirmado, aparecerá una advertencia.
7. Seleccione su equipo en la lista desplegable **Algoritmo de clave pública**.
8. Seleccione su equipo en la lista desplegable **Algoritmo implícito**.
9. Haga clic en **Enviar**.

Información relacionada

- Configurar certificados para la seguridad de los dispositivos

Creación de una solicitud de firma de certificado (CSR) e instalación de un certificado de una autoridad de certificación (CA)

Si ya cuenta con un certificado de una autoridad de certificación (CA) externa de confianza, puede almacenar el certificado y la clave privada en el equipo, y gestionarlos mediante importación y exportación. Si no cuenta con un certificado de una CA externa de confianza, cree una solicitud de firma de certificado (CSR), envíela a una CA para su autenticación e instale el certificado devuelto en su equipo.

- Crear una solicitud de firma de certificado (CSR)
- Instalar un certificado en su equipo

Crear una solicitud de firma de certificado (CSR)

Una solicitud de firma de certificado (CSR) es una petición que se envía a una CA para que autentique las credenciales contenidas en el certificado.

Recomendamos instalar un certificado raíz de la CA en su equipo antes de crear la CSR.

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como "**Pwd**". Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. En la barra de navegación izquierda, haga clic en **Red** > **Seguridad** > **Certificado**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ☰.
5. Haga clic en **Crear CSR**.
6. Escriba una **Nombre común** (necesaria) y añada otra información sobre su **Organización** (opcional).

   - Los detalles de su empresa son necesarios para que la CA pueda confirmar su identidad y verificarla a otros.
   - La longitud del **Nombre común** es de menos de 64 bytes. Introduzca un identificador, como una dirección IP, un nombre de nodo o un nombre de dominio, para utilizarlo al acceder a este equipo mediante comunicación SSL/TLS. El nombre del nodo aparece de forma predeterminada. El **Nombre común** es obligatorio.
   - Si introduce en la dirección URL un nombre distinto del nombre común utilizado para el certificado, aparecerá una advertencia.
   - La longitud de **Organización**, **Unidad organizativa**, **Ciudad/Localidad** y **Estado/Provincia** es inferior a 64 bytes.
   - **País/Región** debería ser un código de país ISO 3166 de dos caracteres.
   - Si configura la extensión de certificado X.509v3, seleccione la casilla de verificación **Configurar partición extendida** y, a continuación, seleccione **Automático (Registrar IPv4)** o **Manual**.
7. Seleccione su equipo en la lista desplegable **Algoritmo de clave pública**.
8. Seleccione su equipo en la lista desplegable **Algoritmo implícito**.
9. Haga clic en **Enviar**.

   Aparece la CSR en la pantalla. Guarde la CSR como archivo o copia y péguela en el formulario CSR en línea que la CA le ha proporcionado.
10. Haga clic en **Guardar**.

- Siga la política de su CA relativa al método para enviarle la CSR.
- Si utiliza una CA raíz de empresa en Windows Server, recomendamos utilizar el servidor web para la plantilla de certificado para crear el certificado cliente de forma segura. Si crea un certificado cliente para un entorno IEEE 802.1x con autenticación EAP-TLS, recomendamos utilizar Usuario para la plantilla de certificado.

Información relacionada

- Creación de una solicitud de firma de certificado (CSR) e instalación de un certificado de una autoridad de certificación (CA)

Instalar un certificado en su equipo

Cuando reciba el certificado de una entidad de certificación (CA), siga los pasos a continuación para instalarlo en el servidor de impresión:

> Solo es posible instalar certificados emitidos con la solicitud de firma de certificado (CSR) de este equipo. Si desea crear otra CSR nueva, asegúrese antes de crearla de que el certificado está instalado. Cree otra CSR únicamente después de instalar el certificado en el equipo, de lo contrario, la CSR creada antes de la instalación de la nueva CRS ya no será válida.

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como "**Pwd**". Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. En la barra de navegación izquierda, haga clic en **Red** > **Seguridad** > **Certificado**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ≡.
5. Haga clic en **Instalar certificado**.
6. Busque el archivo que contiene el certificado emitido por la CA y, a continuación, haga clic en **Enviar**.

   El certificado se crea y se guarda en la memoria del equipo.

Para utilizar comunicación SSL/TLS, el certificado raíz de la CA debe instalarse en el ordenador. Póngase en contacto con su administrador de red.

Información relacionada

- Creación de una solicitud de firma de certificado (CSR) e instalación de un certificado de una autoridad de certificación (CA)

Importar y exportar el certificado y la clave privada

Puede almacenar el certificado y la clave privada en el equipo y gestionarlos mediante importación y exportación.

- Importar un certificado y una clave privada
- Exportar el certificado y la clave privada

Importar un certificado y una clave privada

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como **"Pwd"**. Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. En la barra de navegación izquierda, haga clic en **Red** > **Seguridad** > **Certificado**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ≡.
5. Haga clic en **Importar certificado y clave secreta**.
6. Navegue para seleccionar el archivo que desea importar.
7. Introduzca la contraseña si el archivo está encriptado y, a continuación, haga clic en **Enviar**.

El certificado y la clave privada se importan en el equipo.

Información relacionada

- Importar y exportar el certificado y la clave privada

Exportar el certificado y la clave privada

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como **"Pwd"**. Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. En la barra de navegación izquierda, haga clic en **Red** > **Seguridad** > **Certificado**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ≡.
5. Haga clic en **Exportar**, que aparece con **Lista de certificados**.
6. Si desea encriptar el archivo, introduzca la contraseña.

   Si deja el campo de contraseña vacío, el archivo no se encriptará.
7. Vuelva a introducir la contraseña a modo de confirmación y, a continuación, haga clic en **Enviar**.
8. Haga clic en **Guardar**.

El certificado y la clave privada se exportan al ordenador.

También puede importar el certificado en su ordenador.

Información relacionada

- Importar y exportar el certificado y la clave privada

Importar y exportar un certificado de CA

Puede importar, exportar y almacenar certificados de CA en el equipo Brother.

- Importar un certificado de CA
- Exportar un certificado de CA

Importar un certificado de CA

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como "**Pwd**". Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. En la barra de navegación izquierda, haga clic en **Red** > **Seguridad** > **Certificado CA**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ≡.
5. Haga clic en **Importar certificado CA**.
6. Busque el archivo que desea importar.
7. Haga clic en **Enviar**.

Información relacionada

- Importar y exportar un certificado de CA

Exportar un certificado de CA

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como "**Pwd**". Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. En la barra de navegación izquierda, haga clic en **Red** > **Seguridad** > **Certificado CA**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ≡.
5. Seleccione el certificado que desea exportar y haga clic en **Exportar**.
6. Haga clic en **Enviar**.

Información relacionada

- Importar y exportar un certificado de CA

Utilizar SSL/TLS

- Administrar el equipo de red mediante SSL/TLS de manera segura
- Imprimir documentos de manera segura mediante SSL/TLS
- Enviar o recibir un correo electrónico de manera segura mediante SSL/TLS

Administrar el equipo de red mediante SSL/TLS de manera segura

- Configurar un certificado para SSL/TLS y los protocolos disponibles
- Acceder a Administración basada en Web mediante SSL/TLS
- Instalar el certificado autofirmado para usuarios de Windows con derechos de administrador
- Configurar certificados para la seguridad de los dispositivos

Configurar un certificado para SSL/TLS y los protocolos disponibles

Configure un certificado en su equipo mediante Administración basada en Web antes de utilizar la comunicación SSL/TLS.

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como "**Pwd**". Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. En la barra de navegación izquierda, haga clic en **Red** > **Red** > **Protocolo**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ≡.
5. Haga clic en **Ajustes de servidor HTTP**.
6. Seleccione el certificado que desee configurar en la lista desplegable de **Seleccionar el certificado**.
7. Haga clic en **Enviar**.
8. Haga clic en **Si** para reiniciar el servidor de impresión.

Información relacionada

- Administrar el equipo de red mediante SSL/TLS de manera segura

Información adicional:

- Imprimir documentos de manera segura mediante SSL/TLS

Acceder a Administración basada en Web mediante SSL/TLS

Para administrar el equipo de red de manera segura, debe utilizar las utilidades de administración con protocolos de seguridad.

- Para utilizar el protocolo HTTPS, este debe estar activado en su equipo. El protocolo HTTPS está activado de forma predeterminada.
- Puede cambiar los ajustes del protocolo HTTPS utilizando la pantalla de administración basada en Web.

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como "**Pwd**". Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. Ahora puede acceder al equipo mediante HTTPS.

Información relacionada

- Administrar el equipo de red mediante SSL/TLS de manera segura

Instalar el certificado autofirmado para usuarios de Windows con derechos de administrador

- Los siguientes pasos se aplican a Microsoft Edge. Si utiliza otro navegador web, consulte la documentación o la ayuda en línea del propio navegador para conocer las instrucciones de instalación de certificados.
- Asegúrese de haber creado el certificado autofirmado utilizando la Administración basada en web.

1. Pulse con el botón derecho el icono **Microsoft Edge** y, a continuación, haga clic en **Ejecutar como administrador**.

   Si aparece la pantalla **Control de cuentas de usuario**, haga clic en **Sí**.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. Si su conexión no es privada, haga clic en el botón **Avanzado** y, a continuación, acceda a la página web.
4. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como "**Pwd**". Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
5. En la barra de navegación izquierda, haga clic en **Red** > **Seguridad** > **Certificado**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ≡.
6. Haga clic en **Exportar**.
7. Para encriptar el archivo de salida, introduzca una contraseña en el campo **Introduzca la contraseña**. Si el campo **Introduzca la contraseña** está vacío, su archivo de salida no se encriptará.
8. Introduzca la contraseña de nuevo en el campo **Volver a introducir la contraseña** y, a continuación, haga clic en **Enviar**.
9. Haga clic en el archivo descargado para abrirlo.
10. Cuando aparezca **Asistente para importación de certificados**, haga clic en **Siguiente**.
11. Haga clic en **Siguiente**.
12. De ser necesario, introduzca una contraseña y, a continuación, haga clic en **Siguiente**.
13. Seleccione **Colocar todos los certificados en el siguiente almacén** y, a continuación, haga clic en **Examinar...**.
14. Seleccione **Entidades de certificación raíz de confianza** y, a continuación, haga clic en **Aceptar**.
15. Haga clic en **Siguiente**.
16. Haga clic en **Finalizar**.
17. Si la huella digital es correcta, haga clic en **Sí**.
18. Haga clic en **Aceptar**.

Información relacionada

- Administrar el equipo de red mediante SSL/TLS de manera segura

Imprimir documentos de manera segura mediante SSL/TLS

- Imprimir documentos mediante IPPS
- Configurar un certificado para SSL/TLS y los protocolos disponibles
- Configurar certificados para la seguridad de los dispositivos

Imprimir documentos mediante IPPS

Para imprimir documentos de manera segura con el protocolo IPP, utilice el protocolo IPPS.

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como **"Pwd"**. Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. En la barra de navegación izquierda, haga clic en **Red** > **Red** > **Protocolo**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ≡.
5. Compruebe que la casilla **IPP** esté marcada.

   Si no está marcada la casilla **IPP**, marque la casilla **IPP** y, a continuación, haga clic en **Enviar**.

   Reinicie el equipo para activar la configuración.

   Una vez que se reinicie el equipo, vuelva a la página web del equipo, introduzca la contraseña y, en la barra de navegación izquierda, haga clic en **Red** > **Red** > **Protocolo**.
6. Haga clic en **Ajustes de servidor HTTP**.
7. Marque la casilla de verificación **HTTPS(Puerto 443)** en el área **IPP** y, a continuación, haga clic en **Enviar**.
8. Reinicie el equipo para activar la configuración.

La comunicación con IPPS no puede impedir el acceso no autorizado al servidor de impresión.

Información relacionada

- Imprimir documentos de manera segura mediante SSL/TLS

Utilizar SNMPv3

- Administrar el equipo de red de manera segura mediante SNMPv3

Administrar el equipo de red de manera segura mediante SNMPv3

La versión 3 del protocolo simple de administración de redes (SNMPv3) ofrece autenticación de usuario y encriptación de datos para administrar dispositivos de red de manera segura.

1. Inicie su navegador web.
2. Escriba “https://nombre común” en la barra de direcciones del navegador (donde “Nombre común” es el nombre común que asignó al certificado; este puede ser su dirección IP, nombre de nodo o nombre de dominio).
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como "**Pwd**". Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.

4. En la barra de navegación izquierda, haga clic en **Red** > **Red** > **Protocolo**.

Si la barra de navegación izquierda no es visible, empiece a navegar desde ≡.

5. Asegúrese de que el ajuste **SNMP** está activado y, a continuación, haga clic en **Configuración avanzada**.
6. Configure los ajustes del modo SNMPv1/v2c.

Opción	Descripción
Acceso de lectura-escritura SNMP v1/v2c	El servidor de impresión utiliza la versión 1 y la versión 2c del protocolo SNMP. En este modo puede utilizar todas las aplicaciones del equipo. No obstante, no es seguro, ya que no autenticará al usuario y los datos no se encriptarán.
Acceso de solo lectura a SNMP v1/v2c	El servidor de impresión utiliza el acceso de solo lectura de la versión 1 y la versión 2c del protocolo SNMP.
Desactivado	Desactive la versión 1 y la versión 2c del protocolo SNMP. Todas las aplicaciones que utilicen SNMPv1/v2c estarán restringidas. Para permitir el uso de aplicaciones SNMPv1/v2c, utilice el modo **Acceso de solo lectura a SNMP v1/v2c** o **Acceso de lectura-escritura SNMP v1/v2c**.

7. Configure los ajustes del modo SNMPv3.

Opción	Descripción
Activada	El servidor de impresión utiliza la versión 3 del protocolo SNMP. Para gestionar el servidor de impresión de forma segura, utilice el modo SNMPv3.
Desactivado	Desactive la versión 3 del protocolo SNMP. Todas las aplicaciones que utilicen SNMPv3 estarán restringidas. Para permitir el uso de aplicaciones SNMPv3, utilice el modo SNMPv3.

8. Haga clic en **Enviar**.

Si el equipo muestra las opciones de configuración del protocolo, seleccione las opciones que desee.

9. Reinicie el equipo para activar la configuración.

Información relacionada

- Utilizar SNMPv3

Utilizar IPsec

Introducción a IPsec

IPsec (protocolo de seguridad de Internet) es un protocolo de seguridad que utiliza una función opcional del protocolo de Internet para evitar la manipulación de datos y garantizar la confidencialidad de los datos transmitidos como paquetes IP. IPsec cifra los datos que se transportan a través de una red, como los datos de impresión que se envían desde los ordenadores a una impresora. Dado que los datos están cifrados en el nivel de red, las aplicaciones que usan un protocolo de nivel superior utilizan IPsec incluso sin que el usuario se percate de ello.

IPsec admite las siguientes funciones:

- Transmisiones de IPsec

  De acuerdo con las condiciones de ajuste de IPsec, el ordenador conectado en red envía datos y los recibe del dispositivo especificado utilizando IPsec. Cuando los dispositivos comienzan a comunicarse con IPsec, las claves primero se intercambian mediante IKE (Internet Key Exchange) y, a continuación, los datos encriptados se transmiten a través de las claves.

  Además, IPsec presenta dos modos de operación: el modo de transporte y el modo de túnel. El modo de transporte se utiliza principalmente para la comunicación entre dispositivos, mientras que el modo de túnel se utiliza en entornos como una VPN (red privada virtual).

  Para las transmisiones IPsec, deben cumplirse las siguientes condiciones:
  - Hay un ordenador conectado a la red que puede comunicarse mediante IPsec.
  - Su equipo está configurado para la comunicación IPsec.
  - El ordenador conectado al equipo se ha configurado para conexiones IPsec.

- Ajustes de IPsec

  Ajustes necesarios para conexiones mediante IPsec. Estos ajustes pueden configurarse mediante Administración basada en Web.

  Para configurar los ajustes IPsec, debe utilizar el navegador de un ordenador que esté conectado a la red.

Información relacionada

- Utilizar IPsec

Configurar IPsec mediante Administración basada en Web

Las condiciones de conexión IPsec comprenden dos tipos de **Plantilla**: **Dirección** y **IPsec**. Puede configurar hasta 10 condiciones de conexión.

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como "**Pwd**". Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. En la barra de navegación izquierda, haga clic en **Red** > **Seguridad** > **IPsec**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ≡.
5. Configure los ajustes.

Opción	Descripción
Estado	Active o desactive IPsec.
Modo de negociación	Seleccione **Modo de negociación** para IKE de fase 1. IKE es un protocolo utilizado para intercambiar claves de encriptación con la finalidad de llevar a cabo una comunicación encriptada mediante IPsec. En el modo **Principal**, la velocidad de procesamiento es baja, pero la seguridad es alta. En el modo **Agresivo**, la velocidad de procesamiento es más rápida que el modo **Principal**, pero la seguridad es inferior.
Todo el tráfico que no sea IPsec	Seleccione la acción que se realizará en paquetes que no sean IPsec. Si utiliza Web Services (Servicios web), debe seleccionar **Permitir** en **Todo el tráfico que no sea IPsec**. Si selecciona **Rechazar**, no es posible utilizar Web Services (Servicios web).
Derivación de difusión/multidifusión	Seleccione **Activada** o **Desactivado**.
Derivación de protocolo	Seleccione las casillas para la opción u opciones que desee.
Reglas	Seleccione la casilla de verificación **Activada** para activar la plantilla. Cuando seleccione varias casillas, las casillas con números inferiores tienen prioridad si los ajustes de las casillas seleccionadas entran en conflicto. Haga clic en la lista desplegable correspondiente para seleccionar la **Plantilla de dirección** que se utiliza para las condiciones de conexión IPsec. Para agregar una **Plantilla de dirección**, haga clic en **Añadir plantilla**. Haga clic en la lista desplegable correspondiente para seleccionar la **Plantilla IPsec** que se utiliza para las condiciones de conexión IPsec. Para agregar una **Plantilla IPsec**, haga clic en **Añadir plantilla**.

6. Haga clic en **Enviar**.

   Si debe reiniciarse el equipo para activar los nuevos ajustes, aparecerá la pantalla de confirmación de reinicio.

Si hay un elemento en blanco en la plantilla que activó en la tabla**Reglas**, aparecerá un mensaje de error. Confirme sus selecciones y haga clic en **Enviar**de nuevo.

Información relacionada

- Utilizar IPsec

Información adicional:

- Configurar certificados para la seguridad de los dispositivos

Configurar una plantilla de dirección para IPsec mediante Administración basada en Web

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como "**Pwd**". Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. En la barra de navegación izquierda, haga clic en **Red** > **Seguridad** > **Plantilla dirección IPsec**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ☰.
5. Haga clic en el botón **Eliminar** para eliminar una **Plantilla de dirección**. Cuando una **Plantilla de dirección** está en uso, no se puede eliminar.
6. Haga clic en la **Plantilla de dirección** que desea crear. Aparece la **Plantilla dirección IPsec**.
7. Configure los ajustes.

Opción	Descripción
Nombre de la plantilla	Escriba un nombre para la plantilla (hasta 16 caracteres).
Dirección IP local	• **Dirección IP** Especifique la dirección IP. Seleccione **TODAS las direcc. IPv4**, **TODAS las direcc. IPv6**, **TODOS los enlaces IPv6 locales**, o **Personalizar** de la lista desplegable. Si selecciona **Personalizar** de la lista desplegable, escriba la dirección IP (IPv4 o IPv6) en el cuadro de texto. • **Intervalo de direcciones IP** Introduzca las direcciones IP inicial y final para el rango de direcciones IP en los cuadros de texto. Si las direcciones IP inicial y final no están estandarizadas para IPv4 o IPv6, o si la dirección IP final es inferior a la dirección inicial, se producirá un error. • **Dirección IP / Prefijo** Especifique la dirección IP utilizando una anotación CIDR. Por ejemplo: 192.168.1.1/24 Como el prefijo se especifica en forma de máscara de subred de 24 bits (255.255.255.0) para 192.168.1.1, las direcciones 192.168.1.### serán válidas.
Dirección IP remota	• **Cualquiera** Si se selecciona **Cualquiera**, todas las direcciones IP quedarán habilitadas. • **Dirección IP** Introduzca la dirección IP especificada (IPv4 o IPv6) en el cuadro de texto. • **Intervalo de direcciones IP** Introduzca las direcciones IP inicial y final para el rango de direcciones IP. Si las direcciones IP inicial y final no están

Opción	Descripción
	estandarizadas para IPv4 o IPv6, o si la dirección IP final es inferior a la dirección inicial, se producirá un error. • **Dirección IP / Prefijo** Especifique la dirección IP utilizando una anotación CIDR. Por ejemplo: 192.168.1.1/24 Como el prefijo se especifica en forma de máscara de subred de 24 bits (255.255.255.0) para 192.168.1.1, las direcciones 192.168.1.### serán válidas.

8. Haga clic en **Enviar**.

Si cambia los ajustes de la plantilla actualmente en uso, reinicie su equipo para activar la configuración.

Información relacionada

- Utilizar IPsec

Configurar una plantilla IPsec mediante Administración basada en Web

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como **"Pwd"**. Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. En la barra de navegación izquierda, haga clic en **Red** > **Seguridad** > **Plantilla IPsec**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ≡.
5. Haga clic en el botón **Eliminar** para eliminar una **Plantilla IPsec**. Cuando una **Plantilla IPsec** está en uso, no se puede eliminar.
6. Haga clic en la **Plantilla IPsec** que desea crear. Aparece la pantalla **Plantilla IPsec**. Los campos de configuración difieren según la configuración de **Utilice la plantilla preconfigurada** y **Intercambio de claves por Internet (IKE)** que selecciona.
7. En el campo **Nombre de la plantilla**, escriba un nombre para la plantilla (hasta 16 caracteres).
8. Si ha seleccionado **Personalizar** en la lista desplegable **Utilice la plantilla preconfigurada**, seleccione las opciones **Intercambio de claves por Internet (IKE)** y, a continuación, cambie los ajustes si es necesario.
9. Haga clic en **Enviar**.

Información relacionada

- Utilizar IPsec
  - Ajustes IKEv1 para una plantilla IPsec
  - Ajustes IKEv2 para una plantilla IPsec
  - Ajustes manuales para una plantilla IPsec

Ajustes IKEv1 para una plantilla IPsec

Opción	Descripción
Nombre de la plantilla	Escriba un nombre para la plantilla (hasta 16 caracteres).
Utilice la plantilla preconfigurada	Seleccione **Personalizar**, **Seguridad alta IKEv1** o **Seguridad media IKEv1**. Los elementos de ajuste varían en función de la plantilla seleccionada.
Intercambio de claves por Internet (IKE)	IKE es un protocolo de comunicación utilizado para intercambiar claves de encriptación con la finalidad de llevar a cabo una comunicación encriptada mediante IPsec. Para poder llevar a cabo la comunicación encriptada una sola vez, se determina el algoritmo de encriptación necesario para IPsec y se comparten las claves de encriptación. En IKE, las claves de encriptación se intercambian con el método de intercambio de clave Diffie-Hellman y la comunicación encriptada que se lleva a cabo se limita a IKE. Si ha seleccionado **Personalizar** en **Utilice la plantilla preconfigurada**, seleccione **IKEv1**.
Tipo de autenticación	• **Grupo Diffie-Hellman** Este método de intercambio de claves permite intercambiar claves secretas de manera segura a través de una red no protegida. El método de intercambio de claves Diffie-Hellman utiliza un problema de logaritmo discreto, y no la clave secreta, para enviar y recibir información abierta generada mediante un número aleatorio y la clave secreta. Seleccione **Grupo1**, **Grupo 2**, **Grupo 5** o **Grupo14**. • **Cifrado** Seleccione **DES**, **3DES**, **AES-CBC 128** o **AES-CBC 256**. • **Hash** Seleccione **MD5**, **SHA1**, **SHA256**, **SHA384** o **SHA512**. • **Vida útil SA** Especifique la vida útil de IKE SA. Introduzca el tiempo (segundos) y el número de kilobytes (KByte).
Seguridad encapsuladora	• **Protocolo** Seleccione **ESP**, **AH** o **AH+ESP**. - ESP es un protocolo para llevar a cabo comunicaciones encriptadas con IPsec. ESP encripta la carga (contenidos comunicados) y agrega información adicional. El paquete IP está formado por el encabezado y la carga encriptada, que sigue a este. Además de los datos encriptados, el paquete IP también incluye información relativa al método de encriptación y la clave, los datos de autenticación, etc. - AH forma parte del protocolo IPsec que autentica el emisor e impide la manipulación de los datos (garantiza la integridad de los datos). En el paquete IP, los datos se insertan inmediatamente tras el encabezado. Además, los paquetes incluyen valores hash, que se calculan mediante una ecuación a partir de los contenidos comunicados, la clave secreta, etc. para impedir la falsificación del emisor y la manipulación de los datos. A diferencia de ESP, los contenidos comunicados no se encriptan y los datos se envían y reciben como texto sin formato. • **Cifrado (No disponible para la opción AH.)** Seleccione **DES**, **3DES**, **AES-CBC 128** o **AES-CBC 256**.

Opción	Descripción
	• **Hash** Seleccione **Ninguno**, **MD5**, **SHA1**, **SHA256**, **SHA384** o **SHA512**. **Ninguno** solo se puede seleccionar cuando se ha seleccionado **ESP** en **Protocolo**. • **Vida útil SA** Especifique la vida útil SA de IKE. Introducir la hora (segundos) y el número de kilobytes (KByte). • **Modo de encapsulación** Seleccione **Transporte** o **Túnel**. • **Dirección IP router remoto** Escriba la dirección IP (IPv4 o IPv6) del enrutador remoto. Introduzca esta información únicamente cuando esté seleccionado el modo **Túnel**. SA (Security Association) es un método de comunicación encriptada con IPsec o IPv6 que intercambia y comparte información, como el método de encriptación y la clave, para poder establecer un canal de comunicación seguro antes de que comience la comunicación. SA también puede hacer referencia al canal de comunicación encriptado virtual que se ha establecido. El SA utilizado para IPsec establece el método de encriptación, intercambia las claves y lleva a cabo la autenticación mutua según el procedimiento estándar IKE (Internet Key Exchange). Además, el SA se actualiza periódicamente.
Confidencialidad directa perfecta (PFS)	PFS no deriva claves a partir de claves anteriores utilizadas para encriptar mensajes. Además, si una clave utilizada para encriptar un mensaje se derivó a partir de una clave superior, dicha clave superior no se utilizará para derivar otras claves. Así, si una clave se viera comprometida, el daño se verá limitado únicamente a los mensajes encriptados con esa clave. Seleccione **Activada** o **Desactivado**.
Método de autentificación	Seleccione el método de autenticación. Seleccione **Clave precompartida** o **Certificados**.
Clave precompartida	Al encriptar la comunicación, la clave de encriptación se intercambia y comparte previamente utilizando otro canal. Si seleccionó **Clave precompartida** para el **Método de autentificación**, introduzca la **Clave precompartida** (hasta 32 caracteres). • **Local/Tipo ID/ID** Seleccione el tipo de ID del emisor y, a continuación, escriba el ID. Seleccione **Dirección IPv4**, **Dirección IPv6**, **FQDN**, **Dirección de correo electrónico** o **Certificado** para el tipo. Si selecciona **Certificado**, escriba el nombre común del certificado en el campo **ID**. • **Remoto/Tipo ID/ID** Seleccione el tipo de ID del destinatario y, a continuación, escriba el ID. Seleccione **Dirección IPv4**, **Dirección IPv6**, **FQDN**, **Dirección de correo electrónico** o **Certificado** para el tipo. Si selecciona **Certificado**, escriba el nombre común del certificado en el campo **ID**.
Certificado	Si seleccionó **Certificados** para **Método de autentificación**, seleccione el certificado.

Opción	Descripción
	Puede seleccionar sólo los certificados que fueron creados utilizando la página **Certificado** de la pantalla de configuración de seguridad de la Administración basada en la Web.

Información relacionada

- Configurar una plantilla IPsec mediante Administración basada en Web

Ajustes IKEv2 para una plantilla IPsec

Opción	Descripción
Nombre de la plantilla	Escriba un nombre para la plantilla (hasta 16 caracteres).
Utilice la plantilla preconfigurada	Seleccione **Personalizar**, **Seguridad alta IKEv2** o **Seguridad media IKEv2**. Los elementos de ajuste varían en función de la plantilla seleccionada.
Intercambio de claves por Internet (IKE)	IKE es un protocolo de comunicación utilizado para intercambiar claves de encriptación con la finalidad de llevar a cabo una comunicación encriptada mediante IPsec. Para poder llevar a cabo la comunicación encriptada una sola vez, se determina el algoritmo de encriptación necesario para IPsec y se comparten las claves de encriptación. En IKE, las claves de encriptación se intercambian con el método de intercambio de clave Diffie-Hellman y la comunicación encriptada que se lleva a cabo se limita a IKE. Si ha seleccionado **Personalizar** en **Utilice la plantilla preconfigurada**, seleccione **IKEv2**.
Tipo de autenticación	• **Grupo Diffie-Hellman** Este método de intercambio de claves permite intercambiar claves secretas de manera segura a través de una red no protegida. El método de intercambio de claves Diffie-Hellman utiliza un problema de logaritmo discreto, y no la clave secreta, para enviar y recibir información abierta generada mediante un número aleatorio y la clave secreta. Seleccione **Grupo1**, **Grupo 2**, **Grupo 5** o **Grupo14**. • **Cifrado** Seleccione **DES**, **3DES**, **AES-CBC 128** o **AES-CBC 256**. • **Hash** Seleccione **MD5**, **SHA1**, **SHA256**, **SHA384** o **SHA512**. • **Vida útil SA** Especifique la vida útil de IKE SA. Introduzca el tiempo (segundos) y el número de kilobytes (KByte).
Seguridad encapsuladora	• **Protocolo** Seleccione **ESP**. ESP es un protocolo para llevar a cabo comunicaciones encriptadas con IPsec. ESP encripta la carga (contenidos comunicados) y agrega información adicional. El paquete IP está formado por el encabezado y la carga encriptada, que sigue a este. Además de los datos encriptados, el paquete IP también incluye información relativa al método de encriptación y la clave, los datos de autenticación, etc. • **Cifrado** Seleccione **DES**, **3DES**, **AES-CBC 128** o **AES-CBC 256**. • **Hash** Seleccione **MD5**, **SHA1**, **SHA256**, **SHA384** o **SHA512**. • **Vida útil SA** Especifique la vida útil SA de IKE. Introducir la hora (segundos) y el número de kilobytes (KByte). • **Modo de encapsulación** Seleccione **Transporte** o **Túnel**.

Opción	Descripción
	• **Dirección IP router remoto** Escriba la dirección IP (IPv4 o IPv6) del enrutador remoto. Introduzca esta información únicamente cuando esté seleccionado el modo **Túnel**. SA (Security Association) es un método de comunicación encriptada con IPsec o IPv6 que intercambia y comparte información, como el método de encriptación y la clave, para poder establecer un canal de comunicación seguro antes de que comience la comunicación. SA también puede hacer referencia al canal de comunicación encriptado virtual que se ha establecido. El SA utilizado para IPsec establece el método de encriptación, intercambia las claves y lleva a cabo la autenticación mutua según el procedimiento estándar IKE (Internet Key Exchange). Además, el SA se actualiza periódicamente.
Confidencialidad directa perfecta (PFS)	PFS no deriva claves a partir de claves anteriores utilizadas para encriptar mensajes. Además, si una clave utilizada para encriptar un mensaje se derivó a partir de una clave superior, dicha clave superior no se utilizará para derivar otras claves. Así, si una clave se viera comprometida, el daño se verá limitado únicamente a los mensajes encriptados con esa clave. Seleccione **Activada** o **Desactivado**.
Método de autentificación	Seleccione el método de autenticación. Seleccione **Clave precompartida**, **Certificados**, **EAP - MD5** o **EAP - MS-CHAPv2**. EAP es un protocolo de autenticación que constituye una extensión de PPP. Si utiliza EAP con IEEE802.1x, se usará una clave distinta para la autenticación de usuario durante cada sesión. Los siguientes ajustes sólo son necesarios si se ha seleccionado **EAP - MD5** o **EAP - MS-CHAPv2** en **Método de autentificación**: • **Modo** Seleccione **Modo-Servidor** o **Modo-Cliente**. • **Certificado** Seleccione el certificado. • **Nombre de usuario** Escriba el nombre de usuario (32 caracteres como máximo). • **Contraseña** Escriba la contraseña (32 caracteres como máximo). La contraseña debe introducirse dos veces para confirmarla.
Clave precompartida	Al encriptar la comunicación, la clave de encriptación se intercambia y comparte previamente utilizando otro canal. Si seleccionó **Clave precompartida** para el **Método de autentificación**, introduzca la **Clave precompartida** (hasta 32 caracteres). • **Local/Tipo ID/ID** Seleccione el tipo de ID del emisor y, a continuación, escriba el ID. Seleccione **Dirección IPv4**, **Dirección IPv6**, **FQDN**, **Dirección de correo electrónico** o **Certificado** para el tipo. Si selecciona **Certificado**, escriba el nombre común del certificado en el campo **ID**.

Opción	Descripción
	• **Remoto/Tipo ID/ID** Seleccione el tipo de ID del destinatario y, a continuación, escriba el ID. Seleccione **Dirección IPv4**, **Dirección IPv6**, **FQDN**, **Dirección de correo electrónico** o **Certificado** para el tipo. Si selecciona **Certificado**, escriba el nombre común del certificado en el campo **ID**.
Certificado	Si seleccionó **Certificados** para **Método de autentificación**, seleccione el certificado. Puede seleccionar sólo los certificados que fueron creados utilizando la página **Certificado** de la pantalla de configuración de seguridad de la Administración basada en la Web.

Información relacionada

- Configurar una plantilla IPsec mediante Administración basada en Web

Ajustes manuales para una plantilla IPsec

Opción	Descripción
Nombre de la plantilla	Escriba un nombre para la plantilla (hasta 16 caracteres).
Utilice la plantilla preconfigurada	Seleccione **Personalizar**.
Intercambio de claves por Internet (IKE)	IKE es un protocolo de comunicación utilizado para intercambiar claves de encriptación con la finalidad de llevar a cabo una comunicación encriptada mediante IPsec. Para poder llevar a cabo la comunicación encriptada una sola vez, se determina el algoritmo de encriptación necesario para IPsec y se comparten las claves de encriptación. En IKE, las claves de encriptación se intercambian con el método de intercambio de clave Diffie-Hellman y la comunicación encriptada que se lleva a cabo se limita a IKE. Seleccione **Manual**.
Clave de autenticación (ESP, AH)	Introduzca los valores **Entrada/Salida**. Estos ajustes son necesarios cuando **Personalizar** está seleccionado para **Utilice la plantilla preconfigurada**, **Manual** está seleccionado para **Intercambio de claves por Internet (IKE)**, y un ajuste diferente a **Ninguno** está seleccionado para **Hash** para la sección **Seguridad encapsuladora**. El número de caracteres que se puede establecer varía según el ajuste seleccionado para **Hash** bajo la sección **Seguridad encapsuladora**. Si la longitud de la clave de autenticación especificada es distinta del algoritmo hash seleccionado, se producirá un error. • **MD5**: 128 bits (16 bytes) • **SHA1**: 160 bits (20 bytes) • **SHA256**: 256 bits (32 bytes) • **SHA384**: 384 bits (48 bytes) • **SHA512**: 512 bits (64 bytes) Al especificar la clave en el código ASCII, ponga los caracteres entre comillas dobles (").
Clave de código (ESP)	Introduzca los valores **Entrada/Salida**. Estos ajustes son necesarios al seleccionar **Personalizar** para **Utilice la plantilla preconfigurada**, **Manual** para **Intercambio de claves por Internet (IKE)**, y **ESP** para **Protocolo** en **Seguridad encapsuladora**. El número de caracteres que se puede establecer varía según el ajuste seleccionado para **Cifrado** bajo la sección **Seguridad encapsuladora**. Si la longitud de la clave de código especificada es distinta del algoritmo de encriptación seleccionado, se producirá un error. • **DES**: 64 bits (8 bytes) • **3DES**: 192 bits (24 bytes) • **AES-CBC 128**: 128 bits (16 bytes) • **AES-CBC 256**: 256 bits (32 bytes) Al especificar la clave en el código ASCII, ponga los caracteres entre comillas dobles (").
SPI	Estos parámetros se utilizan para identificar la información de seguridad. En general, un host cuenta con múltiples asociaciones de seguridad (SA) para distintos tipos de comunicación IPsec. Así, es necesario identificar la SA aplicable cuando se recibe un paquete

Opción	Descripción
	IPsec. El parámetro SPI, que identifica la SA, se incluye en el encabezado de autenticación (AH) y el encabezado de carga de seguridad encapsuladora (ESP). Estos ajustes son necesarios cuando **Personalizar** está seleccionado para **Utilice la plantilla preconfigurada**, y **Manual** está seleccionado para **Intercambio de claves por Internet (IKE)**. Introduzca los valores **Entrada/Salida**. (3-10 caracteres)
Seguridad encapsuladora	• **Protocolo** Seleccione **ESP** o **AH**. - ESP es un protocolo para llevar a cabo comunicaciones encriptadas con IPsec. ESP encripta la carga (contenidos comunicados) y agrega información adicional. El paquete IP está formado por el encabezado y la carga encriptada, que sigue a este. Además de los datos encriptados, el paquete IP también incluye información relativa al método de encriptación y la clave, los datos de autenticación, etc. - AH forma parte del protocolo IPsec que autentica el emisor e impide la manipulación de los datos (garantiza la integridad de los datos). En el paquete IP, los datos se insertan inmediatamente tras el encabezado. Además, los paquetes incluyen valores hash, que se calculan mediante una ecuación a partir de los contenidos comunicados, la clave secreta, etc. para impedir la falsificación del emisor y la manipulación de los datos. A diferencia de ESP, los contenidos comunicados no se encriptan y los datos se envían y reciben como texto sin formato. • **Cifrado (No disponible para la opción AH.)** Seleccione **DES**, **3DES**, **AES-CBC 128** o **AES-CBC 256**. • **Hash** Seleccione **Ninguno**, **MD5**, **SHA1**, **SHA256**, **SHA384** o **SHA512**. **Ninguno** solo se puede seleccionar cuando se ha seleccionado **ESP** en **Protocolo**. • **Vida útil SA** Especifique la vida útil SA de IKE. Introducir la hora (segundos) y el número de kilobytes (KByte). • **Modo de encapsulación** Seleccione **Transporte** o **Túnel**. • **Dirección IP router remoto** Escriba la dirección IP (IPv4 o IPv6) del enrutador remoto. Introduzca esta información únicamente cuando esté seleccionado el modo **Túnel**. SA (Security Association) es un método de comunicación encriptada con IPsec o IPv6 que intercambia y comparte información, como el método de encriptación y la clave, para poder establecer un canal de comunicación seguro antes de que comience la comunicación. SA también puede hacer referencia al canal de comunicación encriptado virtual que se ha establecido. El SA utilizado para IPsec establece el método de encriptación, intercambia las claves y lleva a cabo la autenticación mutua según el procedimiento estándar IKE (Internet Key Exchange). Además, el SA se actualiza periódicamente.

Información relacionada

- Configurar una plantilla IPsec mediante Administración basada en Web

Utilizar Autenticación IEEE 802.1x para la red

- ¿Qué es la autenticación IEEE 802.1x?
- Configurar la autenticación IEEE 802.1x para su red mediante Administración basada en Web (navegador web)
- Métodos de autenticación IEEE 802.1x

¿Qué es la autenticación IEEE 802.1x?

IEEE 802.1x es un estándar IEEE que limita el acceso desde dispositivos de red no autorizados. Su equipo Brother envía una solicitud de autenticación a un servidor RADIUS (servidor de autenticación) a través del punto de acceso o hub. Una vez verificada la solicitud por el servidor RADIUS, el equipo puede acceder a la red.

Información relacionada

- Utilizar Autenticación IEEE 802.1x para la red

Configurar la autenticación IEEE 802.1x para su red mediante Administración basada en Web (navegador web)

- Si configura el equipo con la autenticación EAP-TLS, deberá instalar el certificado de cliente emitido por una CA antes de iniciar la configuración. Póngase en contacto con el administrador de red para obtener información sobre el certificado de cliente. Si ha instalado varios certificados, se recomienda anotar el nombre del certificado que desea utilizar.
- Antes de verificar el certificado de servidor, debe importar el certificado de CA emitido por la CA que firmó el certificado de servidor. Póngase en contacto con el administrador de red o con su proveedor de servicios de Internet (ISP) para comprobar si es necesario importar un certificado de CA.

También puede configurar la autenticación IEEE 802.1x mediante el asistente de configuración inalámbrica desde el panel de control (red inalámbrica).

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como **"Pwd"**. Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.

4. En la barra de navegación izquierda, haga clic en **Red**.

Si la barra de navegación izquierda no es visible, empiece a navegar desde ≡.

5. Realice una de las siguientes acciones:
   - Para la red cableada

     Haga clic en **Cableada** > **Estado de 802.1x autentificación**.
   - Para la red inalámbrica

     Haga clic en **Inalámbrica** > **Inalámbrica (Empresa)**.
6. Configure los ajustes de autenticación IEEE 802.1x.

- Si desea activar la autenticación IEEE 802.1x para redes cableadas, seleccione **Activada** para **Estado de 802.1x cableada** en la página **Estado de 802.1x autentificación**.
- Si utiliza autenticación **EAP-TLS**, debe seleccionar el certificado de cliente instalado (se muestra con el nombre del certificado) para su verificación en la lista desplegable **Certificado de cliente**.
- Si selecciona autenticación **EAP-FAST**, **PEAP**, **EAP-TTLS** o **EAP-TLS**, seleccione el método de verificación en la lista desplegable **Verificación del certificado del servidor**. Verifique el certificado del servidor utilizando el certificado de CA, importado previamente en el equipo, que emitió la CA y que firmó el certificado del servidor.

Seleccione uno de los siguientes métodos de verificación en la lista desplegable **Verificación del certificado del servidor**:

Opción	Descripción
No verificar	Siempre se puede confiar en el certificado del servidor. No se lleva a cabo la verificación.
Cert. CA	El método de verificación para comprobar la fiabilidad de CA del certificado del servidor, utilizando el certificado de CA emitido por la CA y que firmó el certificado de servidor.
Cert. CA + ID servidor	El método de verificación para comprobar el valor de nombre común del [1] certificado del servidor, además de la fiabilidad de CA del certificado del servidor.

7. Una vez finalizada la configuración, haga clic en **Enviar**.

   Para redes cableadas: después de la configuración, conecte su equipo a la red IEEE 802.1x compatible. Al cabo de unos minutos, imprima el informe de configuración de la red para comprobar el estado de <**Wired IEEE 802.1x**>.

Opción	Descripción
Success	La función IEEE 802.1x para redes cableadas se habilita y la autenticación ha finalizado con éxito.
Failed	La función IEEE 802.1x para redes cableadas se habilita, pero la autenticación ha fallado.
Off	La función IEEE 802.1x para redes cableadas no está disponible.

Información relacionada

- Utilizar Autenticación IEEE 802.1x para la red

Información adicional:

- Información general de las funciones de los certificados de seguridad
- Configurar certificados para la seguridad de los dispositivos

1 La verificación del nombre común compara el nombre común del certificado de servidor con la cadena de caracteres configurada para **ID del servidor**. Antes de utilizar este método, póngase en contacto con su administrador del sistema para conocer el nombre común del certificado de servidor y, a continuación, configure **ID del servidor**.

Métodos de autenticación IEEE 802.1x

EAP-FAST

Extensible Authentication Protocol-Flexible Authentication via Secured Tunneling (EAP-FAST) ha sido desarrollado por Cisco Systems, Inc., y utiliza un ID de usuario y una contraseña para la autenticación, así como algoritmos de clave simétrica, para lograr un proceso de autenticación en tunneled.

El equipo Brother es compatible con los siguientes métodos de autenticación interna:

- EAP-FAST/NINGUNO
- EAP-FAST/MS-CHAPv2
- EAP-FAST/GTC

EAP-MD5 (red cableada)

Extensible Authentication Protocol-Message Digest Algorithm 5 (EAP-MD5) utiliza un ID de usuario y una contraseña para la autenticación de desafío-respuesta.

PEAP

El protocolo de autenticación extensible protegida (PEAP) es una versión del método EAP desarrollada por Cisco Systems, Inc., Microsoft Corporation y RSA Security. El protocolo PEAP crea un túnel de capa de sockets seguros (SSL)/seguridad de la capa de transporte (TLS) encriptado entre un cliente y un servidor de autenticación, para enviar un ID de usuario y una contraseña. PEAP proporciona autenticación mutua entre el servidor y el cliente.

El equipo Brother es compatible con los siguientes métodos de autenticación interna:

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

Protocolo de autenticación extensible-Seguridad de la capa de transporte en túnel (EAP-TTLS) se ha desarrollado por Funk Software y Certicom. EAP-TTLS crea un túnel SSL encriptado, similar a PEAP, entre un cliente y un servidor de autenticación para enviar un ID de usuario y una contraseña. EAP-TTLS proporciona autenticación mutua entre el servidor y el cliente.

El equipo Brother es compatible con los siguientes métodos de autenticación interna:

- EAP-TTLS/CHAP
- EAP-TTLS/MS-CHAP
- EAP-TTLS/MS-CHAPv2
- EAP-TTLS/PAP

EAP-TLS

Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) requiere autenticación de certificado digital tanto en el cliente como en el servidor de autenticación.

Información relacionada

- Utilizar Autenticación IEEE 802.1x para la red

Autenticación del usuario

- Utilizar autenticación Active Directory
- Utilizar autenticación LDAP
- Utilizar Bloqueo seguro de funciones 3.0

Utilizar autenticación Active Directory

- Introducción a la autenticación Active Directory
- Configurar la autenticación Active Directory mediante Administración basada en Web
- Iniciar sesión para cambiar los ajustes del equipo utilizando el panel de control del mismo (autenticación Active Directory)

Introducción a la autenticación Active Directory

La autenticación de Active Directory limita el uso del equipo. Si la autenticación Active Directory está activada, el panel de control del equipo quedará bloqueado. No se podrán cambiar los ajustes del equipo hasta que introduzca un ID de usuario y la contraseña.

La autenticación Active Directory incluye las siguientes funciones:

Las funciones, opciones y ajustes compatibles pueden variar en función del modelo.

- Almacenamiento de datos de impresión entrantes
- Almacenamiento de datos de fax entrantes
- Obtiene la dirección de correo electrónico del servidor Active Directory en función de su ID de usuario, al enviar datos escaneados a un servidor de correo electrónico.

  Para utilizar esta función, seleccione la opción **Sí** para el ajuste **Obtener dirección de correo electrónico** y el método de autenticación **LDAP + kerberos** o **LDAP + NTLMv2**. Su dirección de correo electrónico se establecerá como emisor al enviar el equipo datos escaneados a un servidor de correo electrónico, o como destinatario si desea enviar los datos escaneados a su dirección de correo electrónico.

Cuando la autenticación Active Directory está activada, el equipo almacena todos los datos de fax entrantes. Una vez iniciada sesión, el equipo imprime los datos de fax almacenados.

Puede cambiar los ajustes de autenticación de Active Directory mediante Administración basada en Web.

Información relacionada

- Utilizar autenticación Active Directory

Configurar la autenticación Active Directory mediante Administración basada en Web

La autenticación Active Directory admite autenticación Kerberos y autenticación NTLMv2. Para la autenticación, debe configurar el protocolo SNTP (servidor de hora de red) y configuración de servidor DNS.

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como "**Pwd**". Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. En la barra de navegación izquierda, haga clic en**Administrador** > **Función de restricción de usuario** o **Administración de restricciones**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ☰.
5. Seleccione **Autenticación de Active Directory**.
6. Haga clic en **Enviar**.
7. Haga clic en **Autenticación de Active Directory**.
8. Configure los siguientes ajustes:

   Las funciones, opciones y ajustes compatibles pueden variar en función del modelo.

Opción	Descripción
Almacenamiento de datos recibidos de fax	Seleccione esta opción para almacenar los datos de fax entrantes. Podrá imprimir todos los datos de fax entrantes una vez haya iniciado una sesión en el equipo.
Recordar ID de usuario	Seleccione esta opción para guardar el ID de usuario.
Dirección del servidor de Active Directory	Escriba la dirección IP o el nombre del servidor (por ejemplo: ad.example.com) del servidor Active Directory.
Nombre de dominio de Active Directory	Escriba el nombre de dominio de Active Directory.
Protocolo y método de autenticación	Seleccione el protocolo y el método de autenticación.
SSL/TLS	Seleccione la opción **SSL/TLS**.
Puerto del servidor LDAP	Escriba el número de puerto para conectar el servidor Active Directory a través de LDAP (disponible solo para el método de autenticación **LDAP + kerberos** o **LDAP + NTLMv2**).

Opción	Descripción
Raíz de búsqueda LDAP	Escriba la raíz de búsqueda LDAP (disponible solo para el método de autenticación **LDAP + kerberos** o **LDAP + NTLMv2**).
Obtener dirección de correo electrónico	Seleccione esta opción para obtener la dirección de correo electrónico del usuario que inició sesión desde el servidor Active Directory. (disponible solo para el método de autenticación **LDAP + kerberos** o **LDAP + NTLMv2**)
Obtener el directorio inicial del usuario	Seleccione esta opción para obtener su directorio principal como el destino de escaneado a red. (disponible solo para el método de autenticación **LDAP + kerberos** o **LDAP + NTLMv2**)

9. Haga clic en **Enviar**.

Información relacionada

- Utilizar autenticación Active Directory

Iniciar sesión para cambiar los ajustes del equipo utilizando el panel de control del mismo (autenticación Active Directory)

Cuando la autenticación Active Directory está activada, el panel de control del equipo queda bloqueado hasta que introduzca el ID de usuario y la contraseña en el panel de control del equipo.

1. En el panel de control del equipo, introduzca su ID de usuario y contraseña para iniciar sesión.
2. Si la autenticación es correcta, el panel de control del equipo se desbloqueará.

Información relacionada

- Utilizar autenticación Active Directory

Utilizar autenticación LDAP

- Introducción a autenticación LDAP
- Configurar autenticación LDAP mediante Administración basada en Web
- Iniciar sesión para cambiar los ajustes del equipo utilizando el panel de control del mismo (autenticación LDAP)

Introducción a autenticación LDAP

La autenticación LDAP limita el uso del equipo. Si la autenticación LDAP está activada, el panel de control del equipo quedará bloqueado. No se podrán cambiar los ajustes del equipo hasta que introduzca un ID de usuario y la contraseña.

La autenticación LDAP ofrece las siguientes funciones:

Las funciones, opciones y ajustes compatibles pueden variar en función del modelo.

- Almacenamiento de datos de impresión entrantes
- Almacenamiento de datos de fax entrantes
- Obtiene la dirección de correo electrónico del servidor LDAP en función de su ID de usuario, al enviar datos escaneados a un servidor de correo electrónico.

  Para utilizar esta función, seleccione la opción **Sí** para el ajuste **Obtener dirección de correo electrónico**. Su dirección de correo electrónico se establecerá como emisor al enviar el equipo datos escaneados a un servidor de correo electrónico, o como destinatario si desea enviar los datos escaneados a su dirección de correo electrónico.

Cuando la autenticación LDAP está activada, el equipo almacena todos los datos de fax entrantes. Una vez iniciada sesión, el equipo imprime los datos de fax almacenados.

Puede cambiar los ajustes de autenticación LDAP con Administración basada en Web.

Información relacionada

- Utilizar autenticación LDAP

Configurar autenticación LDAP mediante Administración basada en Web

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como "**Pwd**". Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. En la barra de navegación izquierda, haga clic en**Administrador** > **Función de restricción de usuario** o **Administración de restricciones**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ☰.
5. Seleccione **Autenticación LDAP**.
6. Haga clic en **Enviar**.
7. Haga clic en el menú **Autenticación LDAP**.
8. Configure los siguientes ajustes:

   Las funciones, opciones y ajustes compatibles pueden variar en función del modelo.

Opción	Descripción
Almacenamiento de datos recibidos de fax	Seleccione esta opción para almacenar los datos de fax entrantes. Podrá imprimir todos los datos de fax entrantes una vez haya iniciado una sesión en el equipo.
Recordar ID de usuario	Seleccione esta opción para guardar el ID de usuario.
Dirección del servidor LDAP	Escriba la dirección IP o el nombre del servidor (por ejemplo: ldad.example.com) del servidor LDAP.
SSL/TLS	Seleccione la opción **SSL/TLS** para usar LDAP con SSL/TLS.
Puerto del servidor LDAP	Escriba el número de puerto del servidor LDAP.
Raíz de búsqueda LDAP	Escriba el directorio raíz de búsqueda LDAP.
Atributo de nombre (clave de búsqueda)	Escriba el atributo que desea utilizar como clave de búsqueda.
Obtener dirección de correo electrónico	Seleccione esta opción para obtener la dirección de correo electrónico registrada del usuario desde el servidor LDAP.
Obtener el directorio inicial del usuario	Seleccione esta opción para obtener su directorio principal como el destino de escaneado a red.

9. Haga clic en **Enviar**.

Información relacionada

- Utilizar autenticación LDAP

Iniciar sesión para cambiar los ajustes del equipo utilizando el panel de control del mismo (autenticación LDAP)

Si la autenticación LDAP está activada, el panel de control del equipo quedará bloqueado hasta que introduzca el ID de usuario y la contraseña en el panel de control del equipo.

1. En el panel de control del equipo, introduzca su ID de usuario y contraseña para iniciar sesión.
2. Si la autenticación es correcta, el panel de control del equipo se desbloqueará.

Información relacionada

- Utilizar autenticación LDAP

Utilizar Bloqueo seguro de funciones 3.0

Bloqueo seguro de funciones (Secure Function Lock) 3.0 aumenta la seguridad al limitar las funciones disponibles en el equipo.

Antes de utilizar Bloqueo seguro de funciones (Secure Function Lock) 3.0

Utilice Bloqueo seguro de funciones para configurar contraseñas, especificar límites de páginas de usuarios específicos y permitir el acceso a algunas o a todas las funciones indicadas aquí.

Puede configurar y cambiar los siguientes ajustes de Bloqueo seguro de funciones 3.0 mediante Administración basada en Web:

Las funciones, opciones y ajustes compatibles pueden variar en función del modelo.

- **Imprimir**
- **Copia**
- **Escanear**
- **Fax**
- **Soporte**
- **Web Connect**
- **Aplicaciones**
- **Límites de página**
- **Contadores de páginas**
- **ID de tarjeta (ID de NFC)**

Modelos de pantalla LCD táctil:

Cuando Bloqueo seguro de funciones está activado, el equipo entra automáticamente en modo público y algunas de las funciones del equipo quedan restringidas solamente a usuarios autorizados. Para acceder a las funciones restringidas del equipo, pulse , seleccione su nombre de usuario e introduzca la contraseña.

Información relacionada

- Utilizar Bloqueo seguro de funciones 3.0

Configurar Bloqueo seguro de funciones (Secure Function Lock) 3.0 mediante Administración basada en Web

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como "**Pwd**". Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. En la barra de navegación izquierda, haga clic en**Administrador** > **Función de restricción de usuario** o **Administración de restricciones**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ≡.
5. Seleccione **Bloqueo de funciones seguro**.
6. Haga clic en **Enviar**.
7. Haga clic en el menú **Funciones restringidas**.
8. Configure los ajustes para gestionar las restricciones por usuario o grupo.
9. Haga clic en **Enviar**.
10. Haga clic en el menú **Lista de usuarios**.
11. Configure la lista de usuario.
12. Haga clic en **Enviar**.

   También puede modificar los ajustes de bloqueo de la lista de usuario en el menú **Bloqueo de funciones seguro**.

Información relacionada

- Utilizar Bloqueo seguro de funciones 3.0

Escanear con Bloqueo seguro de funciones (Secure Function Lock) 3.0

Las funciones, opciones y ajustes compatibles pueden variar en función del modelo.

Configurar restricciones de escaneado (para administradores)

Bloqueo seguro de funciones permite al administrador limitar a los usuarios que tienen permiso para escanear. Cuando la función de escaneado está desactivada para usuarios públicos, solo los usuarios que tengan activada la casilla **Escanear** podrán escanear.

Utilizar la función Escanear (para usuarios restringidos)

- Para escanear utilizando el panel de control del equipo:

  Los usuarios restringidos deben introducir sus contraseñas en el panel de control del equipo para acceder al modo de escaneado.
- Para escanear desde un equipo:

  Los usuarios restringidos deben introducir sus contraseñas en el panel de control del equipo antes de escanear desde sus ordenadores. Si no se introduce la contraseña en el panel de control del equipo, aparece un mensaje de error en el ordenador del usuario.

Si el equipo es compatible con la autenticación con tarjetas IC, los usuarios restringidos también podrán acceder al modo de escaneado pasando sus tarjetas IC registradas por el símbolo de NFC del panel de control del equipo.

Información relacionada

- Utilizar Bloqueo seguro de funciones 3.0

Configurar el modo público para Bloqueo seguro de funciones (Secure Function Lock) 3.0

Utilice la pantalla Bloqueo seguro de funciones para configurar el modo público, que limita las funciones disponibles a los usuarios públicos. Los usuarios públicos no tendrán que introducir una contraseña para acceder a las funciones disponibles mediante la configuración de modo público.

El modo público incluye los trabajos de impresión enviados mediante Brother iPrint&Scan y Brother Mobile Connect.

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como "**Pwd**". Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. En la barra de navegación izquierda, haga clic en**Administrador** > **Función de restricción de usuario** o **Administración de restricciones**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ≡.
5. Seleccione **Bloqueo de funciones seguro**.
6. Haga clic en **Enviar**.
7. Haga clic en el menú **Funciones restringidas**.
8. En la fila **Modo público**, marque o desmarque una casilla de verificación para permitir o restringir, respectivamente, la función indicada.
9. Haga clic en **Enviar**.

Información relacionada

- Utilizar Bloqueo seguro de funciones 3.0

Configurar los ajustes de la pantalla de inicio personal mediante Administración basada en Web

Como administrador, puede especificar qué pestañas pueden ver los usuarios en sus pantallas de inicio personales. Estas pestañas proporcionan acceso rápido a los accesos directos favorite de los usuarios, que pueden asignar a sus pestañas de la pantalla de inicio personal desde el panel de control del equipo.

Las funciones, opciones y ajustes compatibles pueden variar en función del modelo.

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como "**Pwd**". Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.

4. En la barra de navegación izquierda, haga clic en**Administrador** > **Función de restricción de usuario** o **Administración de restricciones**.

Si la barra de navegación izquierda no es visible, empiece a navegar desde ☰.

5. Seleccione **Bloqueo de funciones seguro**.
6. En el campo **Configuración de pestañas**, seleccione **Personal** para los nombres de pestañas que desee usar como su página de inicio personal.
7. Haga clic en **Enviar**.
8. Haga clic en el menú **Funciones restringidas**.
9. Configure los ajustes para gestionar las restricciones por usuario o grupo.
10. Haga clic en **Enviar**.
11. Haga clic en el menú **Lista de usuarios**.
12. Configure la lista de usuario.
13. Seleccione **Lista de usuarios / Funciones restringidas** para cada usuario en la lista desplegable.
14. Seleccione el nombre de la pestaña de la lista desplegable **Pantalla de inicio** para cada usuario.
15. Haga clic en **Enviar**.

Información relacionada

- Utilizar Bloqueo seguro de funciones 3.0

Funciones adicionales de Bloqueo seguro de funciones (Secure Function Lock) 3.0

Configure las siguientes funciones en la pantalla Bloqueo seguro de funciones:

Las funciones, opciones y ajustes compatibles pueden variar en función del modelo.

Reajuste de todos los contadores

Haga clic en **Reajuste de todos los contadores**, en la columna **Contadores de páginas**, para poner a cero el contador de páginas.

Exportar a archivo CSV

Haga clic en **Exportar a archivo CSV** para exportar el contador de número de páginas actual y más reciente, incluida la información sobre **Lista de usuarios / Funciones restringidas** como archivo CSV.

ID de tarjeta (ID de NFC)

Haga clic en el menú **Lista de usuarios** y, a continuación, escriba la identificación de un usuario en el campo **ID de tarjeta (ID de NFC)**. Puede utilizar su tarjeta IC de autenticación.

Salida

Si la unidad Clasificador está instalada en su equipo, seleccione la bandeja de salida para cada usuario de la lista desplegable.

Registro de último contador

Haga clic en **Registro de último contador** si desea que el equipo conserve el recuento de páginas después de poner a cero el contador.

Restablecer automáticamente el contador

Haga clic en **Restablecer automáticamente el contador** para configurar el intervalo de tiempo que desee entre cada reinicio de contador de páginas. Elija un intervalo diario, semanal o mensual.

Información relacionada

- Utilizar Bloqueo seguro de funciones 3.0

Registrar una nueva tarjeta IC utilizando el panel de control del equipo

Puede registrar tarjetas de circuito integrado (tarjetas IC) en su equipo.

Las funciones, opciones y ajustes compatibles pueden variar en función del modelo.

1. Toque el símbolo de transmisión de datos en proximidad (NFC) del panel de control del equipo con una tarjeta de circuito integrado (tarjeta IC) registrada.
2. Seleccione su ID de usuario en la pantalla LCD.
3. Pulse el botón Registrar tarjeta.
4. Pase una nueva tarjeta IC por el símbolo de NFC.

   El número de la nueva tarjeta IC se registra a continuación en el equipo.
5. Pulse el botón OK.

Información relacionada

- Utilizar Bloqueo seguro de funciones 3.0

Registrar un lector de tarjetas de identificación externo

Cuando conecte un lector de tarjetas IC (circuito integrado) externo, utilice Administración basada en Web para registrarlo. El equipo puede utilizar lectores de tarjetas IC externos compatibles con controlador de clase HID.

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como "**Pwd**". Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. En la barra de navegación izquierda, haga clic en **Administrador** > **Lector de tarjetas externo**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ≡.
5. Introduzca la información necesaria y, a continuación, haga clic en **Enviar**.
6. Reinicie el equipo Brother para activar la configuración.
7. Conecte el lector de tarjetas al equipo.
8. Acerque la tarjeta al lector de tarjetas cuando utilice la autenticación de tarjetas.

Información relacionada

- Utilizar Bloqueo seguro de funciones 3.0

Enviar o recibir un correo electrónico de manera segura

- Configurar el envío o recepción de correos electrónicos mediante Administración basada en Web
- Enviar un correo electrónico con autenticación de usuario
- Enviar o recibir un correo electrónico de manera segura mediante SSL/TLS

Configurar el envío o recepción de correos electrónicos mediante Administración basada en Web

- La función Recibir correos electrónicos solamente está disponible para ciertos modelos.
- Se recomienda utilizar Administración basada en Web para configurar el envío de correos electrónicos seguros con autenticación del usuario o el envío y la recepción de correos electrónicos mediante SSL/TLS (solamente modelos compatibles).

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como "**Pwd**". Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. En la barra de navegación izquierda, haga clic en **Red** > **Red** > **Protocolo**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ≡.
5. En el campo **Cliente POP3/IMAP4/SMTP**, haga clic en **Configuración avanzada** y asegúrese de que el estado de **Cliente POP3/IMAP4/SMTP** sea **Activada**.

   - Los protocolos disponibles pueden diferir en función del equipo.
   - Si aparece la pantalla de selección **Método de autentificación**, seleccione el método de autenticación y siga las instrucciones que aparecen en la pantalla.
6. Establezca la configuración de **Cliente POP3/IMAP4/SMTP**.
   - Confirme si la configuración de correo electrónico es correcta después de haberla establecido mediante el envío de un correo electrónico de prueba.
   - Si no conoce la configuración de los servidores POP3/IMAP4/SMTP, póngase en contacto con su administrador de red o proveedor de servicios de Internet (ISP).
7. Cuando finalice la configuración, haga clic en **Enviar**.

   Aparecerá el cuadro de diálogo **Probar configuración de envío/recepción de correo electrónico**.
8. Siga las instrucciones del cuadro de diálogo para probar la configuración actual.

Información relacionada

- Enviar o recibir un correo electrónico de manera segura

Información adicional:

- Enviar o recibir un correo electrónico de manera segura mediante SSL/TLS

Enviar un correo electrónico con autenticación de usuario

Su equipo envía mensajes de correo electrónico a través de un servidor de correo electrónico que requiere la autenticación del usuario. Este método evita que usuarios no autorizados puedan acceder al servidor de correo electrónico.

Puede enviar notificaciones por correo electrónico, informes por correo electrónico e I-Fax (disponible solo para determinados modelos) utilizando la autenticación de usuario.

- Los protocolos disponibles pueden diferir en función del equipo.
- Se recomienda utilizar Administración basada en Web para configurar el método de autenticación SMTP.

Configuración del servidor de correo electrónico

Deberá configurar el método de autenticación SMTP del equipo para que coincida con el método utilizado por su servidor de correo electrónico. Para obtener más información sobre la configuración del servidor de correo electrónico, póngase en contacto con el administrador de red o con su proveedor de servicios de Internet (ISP).

Para activar la autenticación del servidor SMTP usando la Administración basada en Web, seleccione el método de autenticación en **Método de autenticación de servidor** en la pantalla **Cliente POP3/IMAP4/SMTP**.

Información relacionada

- Enviar o recibir un correo electrónico de manera segura

Enviar o recibir un correo electrónico de manera segura mediante SSL/TLS

Su equipo es compatible con los métodos de comunicación SSL/TLS. Para utilizar un servidor de correo electrónico que utilice comunicación SSL/TLS, debe configurar los siguientes ajustes.

- La función Recibir correos electrónicos solamente está disponible para ciertos modelos.
- Se recomienda utilizar Administración basada en Web para configurar SSL/TLS.

Verificar el certificado de servidor

En **SSL/TLS**, si selecciona **SSL** o **TLS**, la casilla de verificación **Verificar certificado del servidor** se activará automáticamente.

- Antes de verificar el certificado de servidor, debe importar el certificado de CA emitido por la CA que firmó el certificado de servidor. Póngase en contacto con el administrador de red o con su proveedor de servicios de Internet (ISP) para comprobar si es necesario importar un certificado de CA.
- Si no necesita verificar el certificado de servidor, desactive la casilla **Verificar certificado del servidor**.

Número de puerto

Si selecciona **SSL** o **TLS**, el valor **Puerto** cambiará para coincidir con el protocolo. Para cambiar el número de puerto manualmente, introduzca el número de puerto después de configurar **SSL/TLS**.

Debe configurar el método de comunicación del equipo de modo que se corresponda con el método utilizado por el servidor de correo electrónico. Para obtener más información sobre la configuración del servidor de correo electrónico, póngase en contacto con el administrador de red o con su ISP.

En la mayoría de casos, los servicios de correo web seguros requieren la siguiente configuración:

Las funciones, opciones y ajustes compatibles pueden variar en función del modelo.

SMTP	**Puerto**	587
	Método de autenticación de servidor	**SMTP-AUTH**
	SSL/TLS	**TLS**
POP3	**Puerto**	995
	SSL/TLS	**SSL**
IMAP4	**Puerto**	993
	SSL/TLS	**SSL**

Información relacionada

- Enviar o recibir un correo electrónico de manera segura

Información adicional:

- Configurar el envío o recepción de correos electrónicos mediante Administración basada en Web
- Configurar certificados para la seguridad de los dispositivos

Almacenamiento del registro de impresión en red

Descripción general del almacenamiento del registro de impresión en la red

La función de almacenamiento del registro de impresión en red permite guardar el archivo de registro de impresión desde el equipo en un servidor de red mediante el protocolo del sistema común de archivos de Internet (CIFS). Puede guardar el ID, el tipo de trabajo de impresión, el nombre de trabajo, el nombre de usuario, la fecha, la hora y el número de páginas impresas por cada trabajo de impresión. CIFS es un protocolo que se ejecuta sobre TCP/IP permitiendo a los ordenadores de una red compartir archivos a través de una red interna o de Internet.

En el registro de impresión se guardan las siguientes funciones de impresión:

Las funciones, opciones y ajustes compatibles pueden variar en función del modelo.

- Trabajos de impresión desde el ordenador
- Impresión directa por USB
- Copia
- Fax recibido
- Impresión Web Connect

- La función de almacenamiento del registro de impresión en red admite autenticación Kerberos y NTLMv2. Debe configurar el protocolo SNTP (servidor de tiempo de red) o bien la fecha, hora y zona horaria correctamente en el panel de control para la autenticación.
- Al almacenar un archivo en el servidor puede establecer el tipo de archivo TXT o CSV.

Información relacionada

- Almacenamiento del registro de impresión en red

Configurar los ajustes de almacenamiento del registro de impresión en red mediante Administración basada en Web

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como "**Pwd**". Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.

4. En la barra de navegación izquierda, haga clic en **Administrador** > **Guardar registro de impr. en red**.

Si la barra de navegación izquierda no es visible, empiece a navegar desde ≡.

5. En el campo **Registro de impresión**, haga clic en **Sí**.
6. Configure los siguientes ajustes:

Las funciones, opciones y ajustes compatibles pueden variar en función del modelo.

Opción	Descripción
Ruta de carpeta de red	Escriba la carpeta de destino en la que se guardará su registro de impresión dentro del servidor CIFS (por ejemplo, \\ComputerName\SharedFolder).
Nombre de archivo	Introduzca el nombre de archivo que desee utilizar para el registro de impresión (hasta 32 caracteres).
Tipo de archivo	Seleccione la opción **TXT** o **CSV** para el tipo de archivo de registro de impresión.
Origen de hora para el registro	Seleccione la fuente de tiempo para el registro de impresión.
Método de autenticación	Seleccione el método de autenticación necesario para acceder al servidor CIFS: **Automático**, **Kerberos**, o **NTLMv2**. Kerberos es un protocolo de autenticación que permite a dispositivos o individuos demostrar su identidad de manera segura en servidores de red utilizando un único registro. NTLMv2 es el método de autenticación utilizado por Windows para iniciar sesión en servidores. • **Automático**: si selecciona **Automático**, NTLMv2 se utilizará para el método de autenticación. • **Kerberos**: seleccione la opción **Kerberos** para utilizar únicamente la autenticación Kerberos. • **NTLMv2**: seleccione la opción **NTLMv2** para utilizar únicamente la autenticación NTLMv2.

Opción	Descripción
	• Para la autenticación **Kerberos** y **NTLMv2**, también debe configurar los ajustes de **Fecha y hora** o el protocolo SNTP (servidor de tiempo de red) y servidor DNS. • También puede configurar los ajustes de fecha y hora desde el panel de control del equipo.
Nombre de usuario	Introduzca el nombre de usuario para la autenticación (hasta 96 caracteres). Si el nombre de usuario forma parte de un dominio, introduzca el nombre de usuario de una de las siguientes maneras: usuario@dominio o dominio\usuario.
Contraseña	Introduzca la contraseña para la autenticación (hasta 32 caracteres).
Dirección del servidor Kerberos (si fuera necesario)	Introduzca la dirección de host Key Distribution Center (KDC) (por ejemplo: kerberos.ejemplo.com; hasta 64 caracteres) o la dirección IP (por ejemplo: 192.168.56.189).
Error de detección de ajuste	Elija qué acción se llevará a cabo cuando el registro de impresión no se pueda almacenar en el servidor debido a un error de red.

7. En el campo **Estado de la conexión**, confirme el último estado de registro.

También puede confirmar el estado del error en la pantalla LCD de su equipo.

8. Haga clic en **Enviar** para ver la página **Registro de impresión de prueba a red**.

   Para probar los ajustes, haga clic en **Si** y, a continuación, vaya al siguiente paso.

   Para omitir la prueba, haga clic en **No**. La configuración se enviará automáticamente.
9. El equipo comprobará la configuración.
10. Si la configuración es aceptada, en la pantalla aparece **Prueba OK**.

    Si aparece **Error de prueba**, compruebe todos los ajustes y, a continuación, haga clic en **Enviar** para que vuelva a aparecer la página de prueba.

Información relacionada

- Almacenamiento del registro de impresión en red

Usar el ajuste de detección de errores del almacenamiento del registro de impresión en red

Usar los ajustes de detección de errores para determinar qué acción debe tomarse cuando el registro de impresión no puede almacenarse en el servidor debido a un error de red.

1. Inicie su navegador web.
2. Introduzca “https://dirección IP del equipo” en la barra de direcciones del navegador (donde “dirección IP del equipo” es la dirección IP de su equipo).

   Por ejemplo:

   https://192.168.1.2

   La dirección IP de su equipo puede encontrarse en el Informe de configuración de la red.
3. En caso necesario, introduzca la contraseña en el campo **Iniciar sesión** y, a continuación, haga clic en **Iniciar sesión**.

   La contraseña predeterminada para gestionar los ajustes de este equipo se encuentra en la parte posterior o en la base del equipo y está marcada como "**Pwd**". Cambie la contraseña predeterminada siguiendo las instrucciones que aparecen en la pantalla al iniciar sesión por primera vez.
4. En la barra de navegación izquierda, haga clic en **Administrador** > **Guardar registro de impr. en red**.

   Si la barra de navegación izquierda no es visible, empiece a navegar desde ≡.
5. En la sección **Error de detección de ajuste**, seleccione la opción **Cancel impresión** o **Ignorar regist e imprim**.

   Las funciones, opciones y ajustes compatibles pueden variar en función del modelo.

Opción	Descripción
Cancel impresión	Si selecciona la opción **Cancel impresión**, los trabajos de impresión se cancelarán cuando el registro de impresión no se pueda almacenar en el servidor. Aunque seleccione la opción **Cancel impresión**, su equipo imprimirá los faxes recibidos.

Ignorar regist e imprim	Si selecciona la opción **Ignorar regist e imprim**, el equipo imprime la documentación aunque el registro de impresión no se pueda almacenar en el servidor.
	Cuando la función de almacenamiento del registro de impresión se haya recuperado, el registro de impresión se grabará tal y como se muestra a continuación:
	`Id, Type, Job Name, User Name, Date, Time, Print Pages`
	`1, Print(xxxxxxx), “Document01.doc”, “user01”, 03/03/20xx, 14:01:32, 52`
	`2, Print(xxxxxxx), “Document02.doc”, “user01”, 03/03/20xx, 14:45:30, ?` (a)
	`3, <Error>, ?, ?, ?, ?, ?` (b)
	`4, Print(xxxxxxx), “Report01.xls”, “user02”, 03/03/20xx, 19:30:40, 4`
	a. Si el registro de impresión no se puede almacenar al final de la impresión, no se grabará el número de páginas impresas.
	b. Si el registro no se puede almacenar al comienzo y al final de la impresión, el registro de impresión del trabajo no se grabará. Una vez recuperada la función, el error queda reflejado en el registro de impresión.

6. Haga clic en **Enviar** para ver la página **Registro de impresión de prueba a red**.

Para probar los ajustes, haga clic en **Si** y, a continuación, vaya al siguiente paso.

Para omitir la prueba, haga clic en **No**. La configuración se enviará automáticamente.

7. El equipo comprobará la configuración.
8. Si la configuración es aceptada, en la pantalla aparece **Prueba OK**.

   Si aparece **Error de prueba**, compruebe todos los ajustes y, a continuación, haga clic en **Enviar** para que vuelva a aparecer la página de prueba.

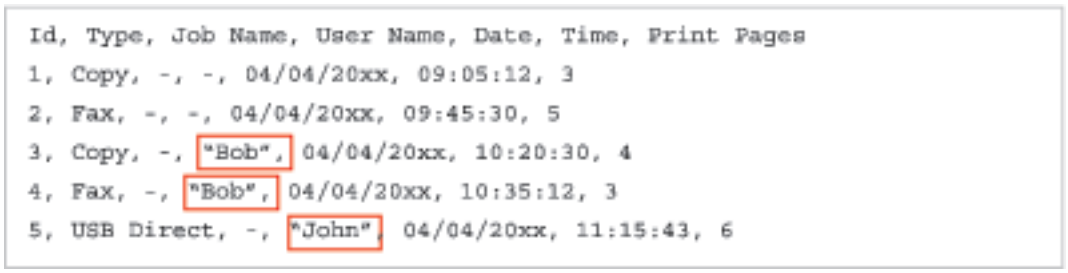
Información relacionada

- Almacenamiento del registro de impresión en red

Usar el almacenamiento del registro de impresión en red con Bloqueo seguro de funciones (Secure Function Lock) 3.0

Cuando Secure Function Lock 3.0 está activa, los nombres de los usuarios registrados para copia, recepción de faxes, impresión Web Connect e impresión USB directa se grabarán en el informe de almacenamiento del registro de impresión en red. Una vez la autenticación Active Directory está activada, se grabará el nombre de usuario en el informe de almacenamiento del registro de impresión en red:

Las funciones, opciones y ajustes compatibles pueden variar en función del modelo.



```
Id, Type, Job Name, User Name, Date, Time, Print Pages
1, Copy, -, -, 04/04/20xx, 09:05:12, 3
2, Fax, -, -, 04/04/20xx, 09:45:30, 5
3, Copy, -, "Bob", 04/04/20xx, 10:20:30, 4
4, Fax, -, "Bob", 04/04/20xx, 10:35:12, 3
5, USB Direct, -, "John", 04/04/20xx, 11:15:43, 6
```

Información relacionada

- Almacenamiento del registro de impresión en red

brother

Brother Earth

www.brotherearth.com

SPA
Versión 0