Guía de funciones de seguridad

© 2025 Brother Industries, Ltd. Todos los derechos reservados.

Información importante para la seguridad

- La contraseña predeterminada para gestionar la configuración de este equipo se encuentra en la parte inferior del equipo y está marcada como “**Pwd**”. Se recomienda cambiar la contraseña predeterminada de inmediato para proteger el equipo frente al acceso no autorizado.
- Cuando conecte su equipo a una red externa como Internet, asegúrese de que su entorno de red esté protegido por un software cortafuegos independiente u otros medios para evitar fugas de información debido a una configuración inadecuada o a un acceso no autorizado por parte de terceros con malas intenciones.
- Si hay señal en las proximidades, la LAN inalámbrica permite realizar libremente una conexión LAN. Sin embargo, si los ajustes de seguridad no están correctamente configurados, la señal la pueden interceptar terceros con malas intenciones, lo que puede dar como resultado:
  - Robo de información personal o confidencial
  - Transmisión irregular de información a partes que puedan suplantar la identidad de los usuarios
  - Difusión de contenidos de comunicación transcrita interceptados

Información relacionada

- 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

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** 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 con seguridad, use el modo SNMPv3 y, a continuación, configure los ajustes.
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 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 túnel.

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