EPSON
EXCEED YOUR VISION

Guía del administrador

Contenido

Guía del administrador

Bienvenido a la *Guía del administrador*.

Para una versión PDF imprimible de esta guía, haga clic aquí.

Nota: No todas las funciones mencionadas es esta *Guía del administrador* están disponibles con cada modelo del producto.

Puede usar dos utilidades de software para configurar los ajustes de red avanzados de su producto: Web Config y EpsonNet Config. Esta guía cubre Web Config en detalle; para obtener información sobre cómo usar EpsonNet Config, consulte la utilidad de ayuda de EpsonNet Config.

Las funciones de red disponibles varían según el producto. (Las funciones que no están disponibles no aparecen en el panel de control del producto o en la pantalla de los ajustes del software). Los productos Epson son compatibles con las siguientes funciones de administración de sistema:

- Comunicación SSL/TLS: utilice el protocolo Secure Sockets Layer/Transport Layer Security (Capa de conexiones seguras/Seguridad de la capa de transporte) para cifrar el tráfico y evitar la suplantación entre el producto y una computadora.
- IPsec/Filtrado de IP: controla el acceso y las comunicaciones seguras entre el producto y una puerta de entrada de red
- Control de protocolo individual: habilita y deshabilita los servicios individuales.
- Configuración remota de destinos de escaneo y fax: utilice un servidor LDAP para buscar contactos de fax y correo electrónico.
- Limitación de las funciones de los usuarios: puede permitir o limitar el acceso a las funciones de impresión, escaneo, fax y copiado que puede utilizar cada usuario.
- Importación y exportación de los ajustes de la impresora: puede copiar los ajustes de un producto a otro.

Cómo usar el software de configuración de red Web Config

Siga las instrucciones de las siguientes secciones para configurar los ajustes de red de administrador de su producto utilizando el software Web Config.

Nota: Antes de que pueda configurar los ajustes de administración de sistema, debe conectar el producto a una red. Consulte el *Manual del usuario* del producto para obtener instrucciones.

Acerca de Web Config

Web Config es una aplicación basada en navegadores que sirve para configurar los ajustes de un producto. Hay páginas de configuración básica y avanzada disponibles.

Nota: Antes de que pueda configurar los ajustes de administración de sistema, debe conectar el producto a una red. Consulte el *Manual del usuario* del producto para obtener instrucciones.

Puede bloquear los ajustes que selecciona configurando una contraseña de administrador para su producto. Consulte el *Manual del usuario* del producto para obtener instrucciones.

Tema principal: Cómo usar el software de configuración de red Web Config

Cómo acceder a Web Config

Puede acceder a Web Config desde su navegador a través de HTTP o HTTPS.

Por defecto, la primera vez que accede a Web Config se utiliza HTTP. Si continúa utilizando HTTP, Web Config no muestra todos los menús disponibles.

1. Imprima una hoja de estado de la red para su producto e identifique la dirección IP del producto. Consulte el *Manual del usuario* del producto para obtener instrucciones.
2. Inicie su navegador web y confirme que JavaScript esté habilitado.
3. Introduzca la dirección IP del producto en el navegador, tal como se indica a continuación, según el protocolo que está utilizando:
   - IPv4: http://*dirección IP del producto*

- IPv6: http://[*dirección IP del producto*]/

Aparece la página Estado:

4. Para utilizar HTTPS, configure su navegador para utilizar HTTPS para la dirección.

   Aparece un mensaje de advertencia acerca del certificado auto-firmado.

Para acceder a Web Config después de configurar HTTPS, introduzca https:// antes de la dirección IP del producto, tal como se muestra en el paso 3.

Nota: Si el nombre del producto está registrado con el servidor DNS, puede utilizar el nombre del producto en lugar de la dirección IP del producto para acceder a Web Config,

Tema principal: Cómo usar el software de configuración de red Web Config

Limitaciones de las funciones disponibles a los usuarios

Siga las instrucciones de las siguientes secciones para impedir que los usuarios utilicen ciertas funciones del producto y para crear una contraseña de administrador para bloquear las limitaciones utilizando el software Web Config.

Limitación de las funciones de los usuarios

Cómo configurar las limitaciones de las funciones de los usuarios

Cómo cambiar la contraseña de administrador en Web Config

Tema principal: Cómo usar el software de configuración de red Web Config

Limitación de las funciones de los usuarios

Puede limitar las funciones disponibles del producto a un máximo de 10 usuarios individuales, con diferentes funciones disponibles para cada usuario. Los usuarios tienen que iniciar sesión en el panel de control del producto con su nombre de usuario y contraseña antes de que puedan usar las funciones del panel de control.

En Windows, también puede limitar las funciones de impresión y escaneo desde el software del producto. Los usuarios tienen que iniciar sesión en el software de impresión o escaneo y esto permite que el software autentique los usuarios antes de que puedan imprimir o escanear. Para obtener instrucciones sobre cómo configurar las limitaciones del software, consulte la utilidad de ayuda del software de impresión o escaneo.

Tema principal: Limitaciones de las funciones disponibles a los usuarios

Cómo configurar las limitaciones de las funciones de los usuarios

Puede crear un máximo de 10 cuentas de usuario y limitar el acceso a las funciones del panel de control para cada usuario de forma separada.

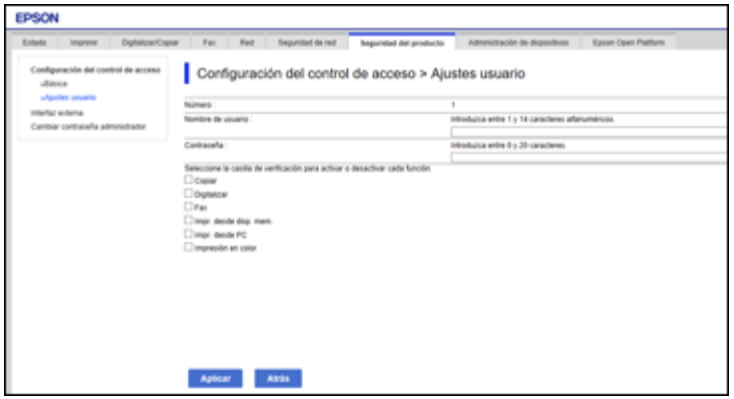
1. Acceda a Web Config y seleccione la ficha **Seguridad del producto**.

   Verá una ventana como esta:

2. Seleccione la casilla **Habilitar control de acceso**.

3. Si ha configurado el producto para un servidor LDAP o una red IEEE 802.1x, puede anular la selección de la casilla **Permite imprimir y digitalizar sin información de autenticación** para prevenir que el producto reciba trabajos enviados de los siguientes orígenes:
   - El driver del sistema operativo predeterminado
   - Un driver de impresora PCL o PostScript
   - Servicos Web, tales como Epson Connect o Google Cloud Print
   - Teléfonos inteligentes y otros dispositivos móviles
4. Haga clic en **Aceptar**.
5. Seleccione **Ajustes usuario**.
6. Haga clic en **Añadir**.

   Verá una ventana como esta:



7. Introduzca un nombre para un usuario en el campo Nombre de usuario siguiendo las directrices que aparecen en la pantalla. Utilice caracteres ASCII (0x20-0x7E).
8. Introduzca una contraseña para el usuario en el campo Contraseña siguiendo las directrices que aparecen en la pantalla.

   Nota: Si necesita reiniciar una contraseña, deje el campo de contraseña vacío.

9. Seleccione la casilla para cada función que desea que el usuario pueda realizar y anule la selección de la casilla para las funciones a las que quiere limitar el acceso.

10. Haga clic en **Aplicar**.

    Nota: Cuando modifica una cuenta de usuario registrada, verá el botón **Eliminar**. Haga clic en el botón para eliminar un usuario, si es necesario.

Nota: Puede importar y exportar una lista de las funciones de usuario a través de EpsonNet Config. Consulte la utilidad de ayuda en el software para obtener instrucciones.

Tema principal: Limitaciones de las funciones disponibles a los usuarios

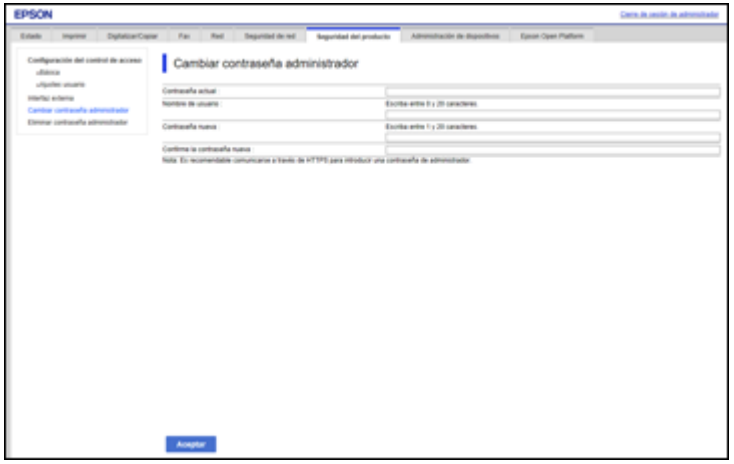
Cómo cambiar la contraseña de administrador en Web Config

Puede configurar una contraseña de administrador utilizando el panel de control del producto, Web Config o EpsonNet Config. Se utiliza la misma contraseña de administrador para todos.

Nota: Consulte el *Manual del usuario* de su producto para obtener instrucciones sobre cómo configurar una contraseña de administrador utilizando el panel de control. Si olvida la contraseña de administrador, contacte al departamento de soporte técnico de Epson, tal como se describe en el *Manual del usuario* del producto.

1. Acceda a Web Config y seleccione la ficha **Seguridad del producto**.
2. Seleccione **Cambiar contraseña administrador**.

   Verá una ventana como esta:



3. Introduzca un nombre de usuario, si es necesario.
4. Realice una de las siguientes acciones:
   - Si ya había configurado una contraseña de administrador previamente, introduzca la contraseña actual, luego introduzca y confirme la contraseña nueva en los campos indicados.
   - Si no había configurado una contraseña de administrador previamente, introduzca una contraseña nueva y confírmela en los campos indicados.
5. Haga clic en **Aceptar**.

Tema principal: Limitaciones de las funciones disponibles a los usuarios

Cómo utilizar su producto en una red segura

Siga las instrucciones de las siguientes secciones para configurar las funciones de seguridad para su producto en la red utilizando el software Web Config.

Cómo configurar la comunicación SSL/TLS
Cómo configurar el protocolo IPsec/Filtrado de IP
Cómo configurar los ajustes del protocolo SNMPv3
Cómo conectar el producto a una red IEEE 802.1X
Cómo usar un certificado digital
Cómo utilizar un servidor LDAP
Cómo configurar protocolos en Web Config
Cómo utilizar un servidor de correo electrónico

Tema principal: Cómo usar el software de configuración de red Web Config

Cómo configurar la comunicación SSL/TLS

Siga las instrucciones de las siguientes sección para configurar la comunicación SSL/TLS a través de Web Config.

Cómo configurar los ajustes de SSL/TLS
Cómo configurar un certificado de servidor para el producto

Tema principal: Cómo utilizar su producto en una red segura

Cómo configurar los ajustes de SSL/TLS

Si su producto es compatible con HTTPS, puede configurar el protocolo SSL/TLS para codificar las comunicaciones con su producto.

1. Acceda a Web Config y seleccione la ficha **Seguridad de red**.

2. Debajo de **SSL/TLS**, seleccione **Básica**.

   Verá una ventana como esta:

3. Seleccione una de las opciones para el ajuste **Intensidad de cifrado**.
4. Seleccione **Habilitar** o **Deshabilitar** como el ajuste **Rediregir HTTP a HTTPS**, según sea necesario.
5. Haga clic en **Siguiente**.

   Verá un mensaje de confirmación.
6. Haga clic en **Aceptar**.

Tema principal: Cómo configurar la comunicación SSL/TLS

Cómo configurar un certificado de servidor para el producto

Puede configurar un certificado de servidor para su producto.

1. Acceda a Web Config y seleccione la ficha **Seguridad de red**.
2. Debajo de **SSL/TLS**, seleccione **Certificado**.

Verá una ventana como esta:

3. Seleccione una de las siguientes opciones:
   - **Certificado firmado CA**: Seleccione **Importar** si consiguió un certificado firmado por una CA. Elija el archivo que desea importar y haga clic en **Aceptar**.
   - **Certificado auto-firmado**: Seleccione **Actualizar** si no ha obtenido un certificado firmado por una Autoridad de certificados (Certificate Authority o CA, por sus siglas en inglés) y desea que el producto genere un certificado autofirmado.
4. Haga clic en **Siguiente**.

   Verá un mensaje de confirmación.
5. Haga clic en **Aceptar**.

Tema principal: Cómo configurar la comunicación SSL/TLS

Cómo configurar el protocolo IPsec/Filtrado de IP

Siga las instrucciones de las siguientes secciones para configurar el filtrado de tráfico IPsec/IP a través de Web Config.

Acerca de IPsec/Filtrado de IP

Cómo configurar la política predeterminada de IPsec/Filtrado de IP

Cómo configurar las políticas de grupo de IPsec/Filtrado de IP

Ajustes de política de IPsec/Filtrado de IP

Ejemplos de configuración de IPsec/Filtrado de IP

Cómo configurar un certificado para IPsec/Filtrado de IP

Tema principal: Cómo utilizar su producto en una red segura

Acerca de IPsec/Filtrado de IP

Puede filtrar el tráfico al producto por medio de la red según la dirección IP, el servicio y el puerto configurando una política predeterminada que aplica a todos los usuarios o grupos conectados al producto. Para el control de usuarios individuales o grupos de usuarios, puede configurar políticas de grupo.

Nota: IPsec solo es compatible con computadoras que están ejecutando Windows Vista o posterior, o Windows Server 2008 o posterior.

Tema principal: Cómo configurar el protocolo IPsec/Filtrado de IP

Cómo configurar la política predeterminada de IPsec/Filtrado de IP

Puede configurar la política predeterminada para el filtrado de tráfico IPsec/IP a través de Web Config.

1. Acceda a Web Config y seleccione la ficha **Seguridad de red**.
2. Debajo de **IPsec/Filtrado de IP** y seleccione **Básica**.

   Verá una ventana como esta:

3. Seleccione **Habilitar** para habilitar el protocolo IPsec/Filtrado de IP.
4. Seleccione las opciones de filtrado que desea usar para la política predeterminada.
5. Haga clic en **Siguiente**.

   Verá un mensaje de confirmación.

6. Haga clic en **Aceptar**.

Tema principal: Cómo configurar el protocolo IPsec/Filtrado de IP

Cómo configurar las políticas de grupo de IPsec/Filtrado de IP

Puede configurar las políticas de grupo para el filtrado de tráfico IPsec/IP a través de Web Config.

1. Acceda a Web Config y seleccione la ficha **Seguridad de red**.
2. Debajo de **IPsec/Filtrado de IP**, seleccione **Básica**.
3. Haga clic en una ficha numérica para el número de política que desea configurar.

   Verá una ventana como esta:

4. Seleccione la casilla **Habilitar esta política de grupo**.
5. Seleccione las opciones de filtrado que desea usar para esta política de grupo.
6. Haga clic en **Siguiente**.

   Verá un mensaje de confirmación.
7. Haga clic en **Aceptar**.
8. Si desea configurar políticas de grupo adicionales, haga clic en la siguiente fiche numérica y repita los pasos de configuración, según sea necesario.

Tema principal: Cómo configurar el protocolo IPsec/Filtrado de IP

Ajustes de política de IPsec/Filtrado de IP

Ajustes de políticas predeterminadas

Ajuste	Opciones/Descripción
Control de acceso	**Permitir acceso** para permitir que pasen los paquetes IP configurados. **Denegar acceso** para prohibir que pasen los paquetes IP. **IPsec** para permitir que pasen los paquetes IPsec.
Versión IKE	Seleccione la versión del protocolo de Intercambio de claves en Internet (IKE, por sus siglas en inglés) que coincide con su entorno de red.
Método de autenticación	Seleccione un método de autenticación o seleccione **Certificado** si importó un certificado firmado por una CA.
Clave precompartida	Si es necesario, introduzca una clave precompartida de 1 a 127 caracteres.
Confirmar clave precompartida	Confirme la clave precompartida que introdujo.
Tipo de Identificación (ID)	Si seleccionó **Clave precompartida** como el **Método de autenticación**, seleccione el tipo de identificación de la lista.
Identificación (ID)	Si seleccionó **IKEv2** como el ajuste **Versión IKE**, introduzca la información de identificación necesaria.
Encapsulamiento	Si seleccionó **IPsec** como la opción de **Control de acceso**, seleccione uno de estos modos de encapsulamiento: **Modo de transporte**: si está utilizando el producto en la misma red LAN; se codificarán los paquetes IP de capa 4 o posterior. **Modo túnel**: si está utilizando el producto en una red preparada para Internet, como, por ejemplo, IPsec-VPN; se codificarán las cabeceras y los datos de los paquetes IP.

Ajuste	Opciones/Descripción
Dirección puerta de enlace (Modo túnel)	Si seleccionó **Modo túnel** como la opción de **Encapsulamiento**, introduzca una dirección de puerta de enlace entre 1 y 39 caracteres.
Protocolo de seguridad	Si seleccionó **IPsec** como la opción de **Control de acceso**, seleccione uno de estos protocolos de seguridad: **ESP**: para garantizar la integridad de la autenticación y los datos, además de codificar los datos. **AH** para garantizar la integridad de la autenticación y los datos; puede usar IPsec aunque esté prohibido codificar los datos.
Ajustes de algoritmo	Seleccione los ajustes de algoritmo de codificación para el protocolo de seguridad que seleccionó.

Ajustes de políticas de grupo

Ajuste	Opciones/Descripción
Control de acceso	**Permitir acceso** para permitir que pasen los paquetes IP configurados. **Denegar acceso** para prohibir que pasen los paquetes IP. **IPsec** para permitir que pasen los paquetes IPsec.
Dirección local(impresora)	Seleccione una dirección IPv4 o IPv6 adecuada para su entorno de red; si la dirección IP se asigna automáticamente, seleccione **Usar dirección IPv4 obtenida automáticamente**.
Dirección remota(host)	Escriba la dirección IP del dispositivo (entre 0 y 43 caracteres) para controlar el acceso, o déjelo en blanco para controlar todas las direcciones; si la dirección IP se asigna automáticamente (como, por ejemplo, por DHCP), es posible que la conexión no esté disponible. En ese caso, configure una dirección estática.
Método de elección de puerto	Seleccione el método que desea usar para especificar los puertos.

Ajuste	Opciones/Descripción
Nombre del servicio	Si seleccionó **Nombre del servicio** como el **Método de elección de puerto**, seleccione una opción de nombre de servicio aquí; consulte la siguiente tabla para obtener más información.
Protocolo de transporte	Si seleccionó **Número de puerto** como el **Método de elección de puerto**, seleccione uno de estos modos de encapsulamiento: **Cualquier protocolo** **TCP** **UDP** **ICMPv4** Consulte la tabla Directrices para políticas de grupo para obtener más información.
Puerto local	Si seleccionó **Número de puerto** como el **Método de elección de puerto** y **TCP** o **UDP** como el **Protocolo de transporte**, introduzca los números de puerto para controlar la recepción de paquetes (hasta 10 puertos), separándolos con comas, por ejemplo, **25,80,143,5220**; deje este ajuste en blanco para controlar todos los puertos; consulte la siguiente tabla para obtener más información.
Puerto remoto	Si seleccionó **Número de puerto** como el **Método de elección de puerto** y **TCP** o **UDP** como el **Protocolo de transporte**, introduzca los números de puerto para controlar el envío de paquetes (hasta 10 puertos), separándolos con comas, por ejemplo, **25,80,143,5220**; deje este ajuste en blanco para controlar todos los puertos; consulte la siguiente tabla para obtener más información.
Versión IKE	Seleccione **IKEv1** o **IKEv2** dependiendo del dispositivo a que el producto está conectado.
Método de autenticación	Si seleccionó **IPsec** como la opción de **Control de acceso**, seleccione un método de autenticación aquí.

Ajuste	Opciones/Descripción
Clave precompartida	Si seleccionó **Clave precompartida** como el **Método de autenticación**, introduzca una clave precompartida entre 1 y 127 caracteres aquí y en el campo **Confirmar clave precompartida**.
Tipo de Identificación (ID)	Si seleccionó **Clave precompartida** como el **Método de autenticación**, seleccione el tipo de identificación de la lista.
Identificación (ID)	Si seleccionó **IKEv2** como el ajuste **Versión IKE**, introduzca la información de identificación necesaria.
Encapsulamiento	Si seleccionó **IPsec** como la opción de **Control de acceso**, seleccione uno de estos modos de encapsulamiento: **Modo de transporte**: si está utilizando el producto en la misma red LAN; se codificarán los paquetes IP de capa 4 o posterior. **Modo túnel**: si está utilizando el producto en una red preparada para Internet, como, por ejemplo, IPsec-VPN; se codificarán las cabeceras y los datos de los paquetes IP.
Dirección puerta de enlace (Modo túnel)	Si seleccionó **Modo túnel** como la opción de **Encapsulamiento**, introduzca una dirección de puerta de enlace entre 1 y 39 caracteres.
Protocolo de seguridad	Si seleccionó **IPsec** como la opción de **Control de acceso**, seleccione uno de estos protocolos de seguridad: **ESP**: para garantizar la integridad de la autenticación y los datos, además de codificar los datos. **AH** para garantizar la integridad de la autenticación y los datos; puede usar IPsec aunque esté prohibido codificar los datos.
Ajustes de algoritmo	Seleccione los ajustes de algoritmo de codificación para el protocolo de seguridad que seleccionó.

Directrices para políticas de grupo

Nombre del servicio	Tipo de protocolo	Número del puerto local/remoto	Funciones controladas
ENPC	UDP	3289/cualquier puerto	Búsqueda de un producto desde aplicaciones, tales como un driver de impresora o escáner, o EpsonNet Config
SNMP	UDP	161/cualquier puerto	Adquisición y configuración de MIB desde aplicaciones, tales como un driver de impresora o escáner, o EpsonNet Config
LPR	TCP	515/cualquier puerto	Reenvíio de datos LPR
RAW (Puerto9100)	TCP	9100/cualquier puerto	Reenvío de datos RAW
IPP/IPPS	TCP	631/cualquier puerto	Reenvío de datos AirPrint (impresión IPP/IPPS)
WSD	TCP	Cualquier puerto/5357	Control de WSD
WS-Discovery	UDP	3702/cualquier puerto	Búsqueda de un producto desde WSD
Digitalización red	TCP	1865/cualquier puerto	Reenvío de datos de escaneo desde Document Capture Pro
Network Push Scan	TCP	Cualquier puerto/2968	Adquisición de datos de trabajos de escaneo por medio de la función de escaneo directo desde Document Capture Pro
Network Push Scan Discovery	UDP	2968/cualquier puerto	Búsqueda de una computadora cuando se ejecuta un escaneo directo desde Document Capture Pro
Datos FTP (local)	TCP	20/cualquier puerto	Reenvío de datos de impresión FTP a servidor FTP
Control FTP (local)	TCP	21/cualquier puerto	Control de impresión FTP a servidor FTP

Nombre del servicio	Tipo de protocolo	Número del puerto local/remoto	Funciones controladas
Datos FTP (remoto)	TCP	Cualquier puerto/20	Reenvío de datos de escaneo y datos de fax recibidos a cliente FTP; solamente puede controlar un servidor FTP que utiliza el número de puerto remoto 20
Control FTP (remoto)	TCP	Cualquier puerto/21	Reenvío de datos de escaneo y datos de fax recibidos a cliente FTP
CIFS (local)*	TCP	445/cualquier puerto	Uso compartido de una carpeta de red en un servidor CIFS
CIFS (remoto)*	TCP	Cualquier puerto/445	Reenvío de datos de escaneo y datos de fax recibidos a una carpeta en un servidor CIFS
NetBIOS Name Service (local)	UDP	137/cualquier puerto	Uso compartido de una carpeta de red en un servidor CIFS
NetBIOS Datagram Service (local)	UDP	138/cualquier puerto	
NetBIOS Session Service (local)	TCP	139/cualquier puerto	
NetBIOS Name Service (remoto)	UDP	Cualquier puerto/137	Reenvío de datos de escaneo y datos de fax recibidos a una carpeta en un servidor CIFS
NetBIOS Datagram (remoto)	UDP	Cualquier puerto/138	
NetBIOS Session Service (remoto)	TCP	Cualquier puerto/139	
HTTP (local)	TCP	80/cualquier puerto	Reenvío de datos de Web Config y WSD a un servidor HTTP o HTTPS
HTTPS (local)	TCP	443/cualquier puerto	
HTTP (remoto)	TCP	Cualquier puerto/80	Comunicación con Epson Connect o Google Cloud Print, actualización de firmware y actualización de certificado raíz en un cliente HTTP o HTTPS
HTTPS (remoto)	TCP	Cualquier puerto/443	

* Para controlar las funciones que reenvían de datos de escaneo y datos de fax recibidos, compartir una carpeta de red o recibir datos de fax desde PC-Fax, seleccione **Número de puerto** como el **Método de elección de puerto** y especifique los números de puerto para CIFS y NetBIOS.

Tema principal: Cómo configurar el protocolo IPsec/Filtrado de IP

Ejemplos de configuración de IPsec/Filtrado de IP

Puede configurar el filtrado de IPsec y IP de varias formas, tal como se muestra en los siguientes ejemplos.

Para recibir paquetes IPsec solamente

Utilice este ejemplo solo para configurar una política predeterminada.

- **IPsec/Filtrado de IP**: **Habilitar**
- **Control de acceso**: **IPsec**
- **Método de autenticación**: **Clave precompartida**
- **Clave precompartida**: Introduzca una clave de hasta 127 caracteres.

Para recibir datos de impresión y ajustes de la impresora

Utilice este ejemplo para permitir la comunicación de datos de impresión y los ajustes de la impresora desde los servicios especificados.

Política predeterminada:

- **IPsec/Filtrado de IP**: **Habilitar**
- **Control de acceso**: **Denegar acceso**

Política de grupo:

- **Control de acceso**: **Permitir acceso**
- **Dirección remota(host)**: Dirección IP del cliente
- **Método de elección de puerto**: **Nombre del servicio**
- **Nombre del servicio**: Seleccione **ENPC**, **SNMP**, **HTTP (local)**, **HTTPS (local)** y **RAW (Puerto9100)**

Para recibir acceso únicamente de una dirección especificada para el acceso del producto

En estos ejemplos, el cliente podrá acceder a y configurar el producto independientemente de las políticas configuradas.

Política predeterminada:

- **IPsec/Filtrado de IP**: **Habilitar**

- **Control de acceso**: **Denegar acceso**

Política de grupo:

- **Control de acceso**: **Permitir acceso**
- **Dirección remota(host)**: Dirección IP del cliente de un administrador

Tema principal: Cómo configurar el protocolo IPsec/Filtrado de IP

Cómo configurar un certificado para IPsec/Filtrado de IP

Puede configurar un certificado para el filtrado de tráfico IPsec/IP a través de Web Config.

1. Acceda a Web Config y seleccione la ficha **Seguridad de red**.
2. Debajo de **IPsec/Filtrado de IP**, seleccione **Certificado del cliente**.

   Verá una ventana como esta:

3. Haga clic en **Importar** para añadir un certificado de cliente nuevo e introduzca los ajustes necesarios.
4. Haga clic en **Aceptar**.

Tema principal: Cómo configurar el protocolo IPsec/Filtrado de IP

Tareas relacionadas

Cómo obtener e importar un certificado firmado por una CA

Cómo configurar los ajustes del protocolo SNMPv3

Si su producto es compatible con el protocolo SNMPv, puede monitorear y control el acceso a su producto a través de ese protocolo.

1. Acceda a Web Config y seleccione la ficha **Seguridad de red**.

   Verá una ventana como esta:

2. Desplácese hacia abajo y seleccione la casilla **Activar SNMPv3** para activar los ajustes de SNMPv3.
3. Seleccione los ajustes que desea en la sección Configuración de SNMPv3.
4. Haga clic en **Siguiente**.

   Verá un mensaje de confirmación.
5. Haga clic en **Aceptar**.

Ajustes de SNMPv3

Tema principal: Cómo utilizar su producto en una red segura

Ajustes de SNMPv3

Puede configurar estos ajustes de SNMPv3 en Web Config.

Ajuste	Opciones/Descripción
Nombre de usuario	Introduzca un nombre de usuario de 1 a 32 caracteres ASCII.

Ajuste	Opciones/Descripción
Configuración de autenticación	
Algoritmo	Seleccione el algoritmo para autenticación.
Contraseña	Introduzca una contraseña de 8 a 32 caracteres ASCII.
Confirmar contraseña	Introduzca la contraseña de autenticación otra vez.
Configuración de cifrado	
Algoritmo	Seleccione el algoritmo para codificación.
Contraseña	Introduzca una contraseña de 8 a 32 caracteres ASCII.
Confirmar contraseña	Introduzca la contraseña de codificación otra vez.
Nombre de contexto	Introduzca un nombre de contexto de 1 a 32 caracteres ASCII.

Tema principal: Cómo configurar los ajustes del protocolo SNMPv3

Cómo conectar el producto a una red IEEE 802.1X

Siga las instrucciones de las siguientes secciones para conectar el producto a una red IEEE 802.1X a través de Web Config.

Cómo configurar una red IEEE 802.1X
Ajustes de red IEEE 802.1X
Cómo configurar un certificado para una red IEEE 802.1X
Estado de red IEEE 802.1X

Tema principal: Cómo utilizar su producto en una red segura

Cómo configurar una red IEEE 802.1X

Si su producto es compatible con IEEE 802.1X, puede usarlo en una red con autenticación proporcionada por un servidor RADIUS con un concentrador como un autenticador a través de Web Config.

1. Acceda a Web Config y seleccione la ficha **Seguridad de red**.
2. Debajo de **IEEE802.1X**, seleccione **Básica**.

Verá una ventana como esta:

3. Seleccione **Habilitar** como el ajuste **IEEE802.1X (LAN cableada)**.
4. Para utilizar el producto en una red Wi-Fi, habilite los ajustes de Wi-Fi de su producto. Consulte el *Manual del usuario* de su producto para obtener instrucciones.

   El estado de la conexión se muestra como el ajuste **IEEE802.1X (Wi-Fi)**.

   Nota: Puede compartir los ajustes de red para conexión de red Ethernet y Wi-Fi.

5. Seleccione los ajustes de IEEE 802.1X que desea utilizar.
6. Haga clic en **Siguiente**.

   Verá un mensaje de confirmación.
7. Haga clic en **Aceptar**.

Tema principal: Cómo conectar el producto a una red IEEE 802.1X

Ajustes de red IEEE 802.1X

Puede configurar estos ajustes de IEEE 802.1X en Web Config.

Ajuste	Opciones/Descripción
Método de Conexión	Muestra el método de conexión de red actual.

Ajuste	Opciones/Descripción
Tipo de EAP	Seleccione uno de estos métodos de autenticación para conexiones entre el producto y un servidor RADIUS: **EAP-TLS** o **PEAP-TLS**: Debe obtener e importar un certificado firmado por una CA. **PEAP/MSCHAPv2**: Debe configurar una contraseña.
ID del usuario	Introduzca un ID entre 1 y 128 caracteres ASCII para la autenticación en un servidor RADIUS.
Contraseña	Introduzca una contraseña entre 1 y 128 caracteres ASCII para la autenticación del producto. Si está utilizando una computadora con Windows como un servidor RADIUS, introduzca hasta 127 caracteres ASCII.
Confirmar contraseña	Introduzca la contraseña de autenticación otra vez.
ID del servidor	Introduzca un ID de servidor entre 1 y 128 caracteres ASCII para la autenticación en un servidor RADIUS específico; el ID de servidor se verifica en el campo subject/subjectAltName de un certificado de servidor enviado desde el servidor RADIUS.
Validación de certificado	Seleccione un certifico válido independientemente del método de autenticación; importe el certificado con la opción **Certificado CA**.
Nombre anónimo	Si seleccionó **PEAP-TLS** o **PEAP/MSCHAPv2** como el **Método de autenticación**, puede configurar un nombre anónimo entre 1 y 128 caracteres ASCII en lugar de un ID de usuario para la fase 1 de una autenticación PEAP.
Intensidad de cifrado	Seleccione una de las siguientes opciones de intensidad de cifrado: **Alto** para AES256/3DES **Medio** para AES256/3DES/AES128/RC4

Tema principal: Cómo conectar el producto a una red IEEE 802.1X

Cómo configurar un certificado para una red IEEE 802.1X

Si su producto es compatible con IEEE 802.1X, puede configurar un certificado para la red a través de Web Config.

1. Acceda a Web Config y seleccione la ficha **Seguridad de red**.
2. Debajo de **IEEE802.1X**, seleccione **Certificado del cliente**.

   Verá una ventana como esta:

3. Haga clic en **Importar** para agregar un certificado de cliente nuevo.
4. Haga clic en **Aceptar**.

Tema principal: Cómo conectar el producto a una red IEEE 802.1X

Estado de red IEEE 802.1X

Puede imprimir una hoja de estado de su producto para revisar el estado de los ajustes de red IEEE 802.1X. Consulte el *Manual del usuario* del producto para obtener instrucciones sobre cómo imprimir una hoja de estado de la red.

La hoja de estado de la red muestra la información en esta tabla para redes IEEE 802.1X.

ID de estado	Descripción del estado
Disable	La red IEEE 802.1X está desactivada.
EAP Success	La autenticación de IEEE 802.1X se ha confirmado y la conexión de red está disponible.
Authenticating	La autenticación de IEEE 802.1X está en progreso.
Config Error	La autenticación falló porque el ID de usuario no se ha configurado.
Client Certificate Error	La autenticación falló porque el certificado del cliente ha caducado.

ID de estado	Descripción del estado
Timeout Error	La autenticación falló porque el servidor RADIUS o el autenticador no responde.
User ID Error	La autenticación falló porque el ID de usuario o el protocolo del certificado del producto es incorrecto.
Server ID Error	La autenticación falló porque el ID del servidor en el certificado del servidor y el ID del servidor no coinciden.
Server Certificate Error	La autenticación falló porque el certificado del servidor ha caducado o la cadena del certificado del servidor es incorrecta.
CA Certificate Error	La autenticación falló porque el certificado de CA es incorrecto, no fue importado o ha caducado.
EAP Failure	La autenticación falló porque el certificado del cliente es incorrecto (EAP-TLS o PEAP-TLS) o el ID del usuario o la contraseña es incorrecto. (PEAP/MSCHAPv2).

Tema principal: Cómo conectar el producto a una red IEEE 802.1X

Cómo usar un certificado digital

Siga las instrucciones de las siguientes sección para configurar y usar certificados digitales a través de Web Config.

Acerca de la certificación digital
Cómo obtener e importar un certificado firmado por una CA
Ajustes de configuración de CSR
Ajustes de importación de CSR
Cómo eliminar un certificado firmado por una CA
Cómo actualizar un certificado autofirmado

Tema principal: Cómo utilizar su producto en una red segura

Acerca de la certificación digital

Puede configurar los siguientes certificados digitales para su red a través de Web Config:

Certificado firmado por una CA
Puede garantizar la seguridad de las comunicaciones con un certificado firmado por una CA para cada función de seguridad. Los certificados deben ser firmados por y obtenidos a través de una CA (Autoridad de certificados).

Certificado autofirmado

Un certificado autofirmado es emitido y firmado por el producto mismo. Solo puede utilizar el certificado para una comunicación SSL/TLS, pero la seguridad no es fiable y puede ver una alerta de seguridad en el navegador cuando lo esté usando.

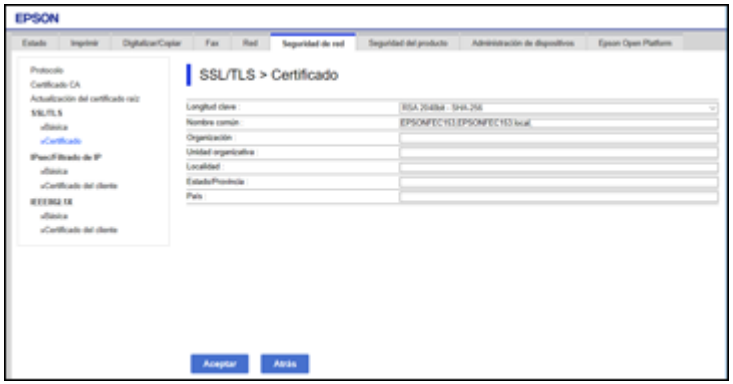
Tema principal: Cómo usar un certificado digital

Cómo obtener e importar un certificado firmado por una CA

Puede obtener un certificado firmado por una CA creando una solicitud de firma de certificado (Certificate Signing Request o CSR, por sus siglas en inglés) a través de Web Config y enviándola a una autoridad de certificados. La CSR creada en Web Config tiene el formato PEM/DER. Puede importar una CSR creada mediante Web Config a la vez.

1. Acceda a Web Config y seleccione la ficha **Seguridad de red**.
2. Debajo de una de las siguientes opciones de seguridad de red, seleccione el certificado correspondiente:
   - **SSL/TLS** y **Certificado**
   - **IPsec/Filtrado de IP** y **Certificado del cliente**
   - **IEEE802.1X** y **Certificado del cliente**
3. En la sección CSR, seleccione **Generar**.

   Verá una ventana como esta:



4. Seleccione los ajustes de CSR que desea utilizar.
5. Haga clic en **Aceptar**.

Verá un mensaje de finalización.

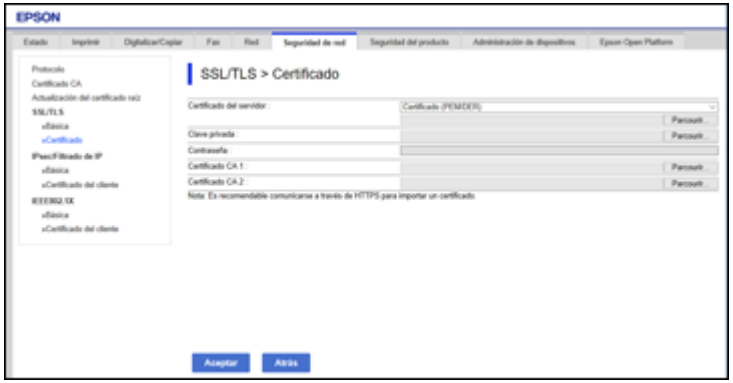
6. Seleccione la ficha **Seguridad de red** otra vez y seleccione su opción de seguridad de red y el certificado correspondiente.
7. En la sección de CSR, haga clic en la opción de **Descargar** que corresponde al formato especificado por la autoridad de certificados para descargar la CSR.

   Precaución: No genere otra CSR o es posible que no pueda importar un certificado firmado por una CA.

8. Envíe la CSR a la autoridad de certificados siguiendo las directrices de formato proporcionadas por dicha autoridad.
9. Guarde el certificado firmado por una CA que fue emitido a una computadora conectada al producto.

   Antes de continuar, asegure que los ajustes de fecha y hora estén correctos en su producto. Consulte el *Manual del usuario* del producto para obtener instrucciones.
10. Seleccione la ficha **Seguridad de red** otra vez y seleccione su opción de seguridad de red y el certificado correspondiente.
11. En la sección Certificado firmado CA, haga clic en **Importar**.

    Verá una ventana como esta:



12. Seleccione el formato del certificado como el ajuste **Certificado del servidor**.
13. Seleccione los ajustes de importación del certificado según sea necesario para el formato y el origen del certificado.

14. Haga clic en **Aceptar**.

    Verá un mensaje de confirmación.

15. Haga clic en **Confirmar** para verificar la información del certificado.

Tema principal: Cómo usar un certificado digital

Ajustes de configuración de CSR

Puede seleccionar estos ajustes cuando configure una CSR en Web Config.

Nota: Lo longitud y abreviaciones disponibles para la clave varían según la autoridad de certificados, por lo tanto, sigas las reglas de la autoridad cuando introduzca información en la CSR.

Ajuste	Opciones/Descripción
Longitud clave	Seleccione una longitud de la clave para la CSR.
Nombre común	Introduzca un nombre o dirección IP estática entre 1 y 125 caracteres; por ejemplo, **Impresora de recepción** o **https://10.152.12.225**.
Organización, **Unidad organizativa**, **Localidad**, **Estado/Provincia**	Introduzca información en cada campo, según sea necesario, entre 0 y 64 caracteres ASCII; separe los nombres con comas.
País	Introduzca el código de dos dígitos del país especificado por la norma ISO-3166.

Tema principal: Cómo usar un certificado digital

Ajustes de importación de CSR

Puede configurar estos ajustes cuando importe una CSR en Web Config.

Nota: Los requisitos de los ajustes de importación varían según el formato del certificado y cómo obtuvo el certificado.

Formato de certificado	Descripciones de ajustes
Formato PEM/DER obtenido a través de Web Config	**Clave privada**: No configure este ajuste porque el producto contiene una clave privada. **Contraseña**: No configure este ajuste. **Certificado CA 1/Certificado CA 2**: Opcional

Formato de certificado	Descripciones de ajustes
Formato PEM/DER obtenido a través de una computadora	**Clave privada**: Configure una clave privada. **Contraseña**: No configure este ajuste. **Certificado CA 1/Certificado CA 2**: Opcional
Formato PKCS#12 obtenido a través de una computadora	**Clave privada**: No configure este ajuste. **Contraseña**: Opcional **Certificado CA 1/Certificado CA 2**: No configure este ajuste.

Tema principal: Cómo usar un certificado digital

Cómo eliminar un certificado firmado por una CA

Puede eliminar un certificado firmado por una CA que fue importado a través de Web Config cuando el certificado se caduque o si ya no necesita una conexión codificada.

Nota: Si obtuvo un certificado firmado por una CA a través de Web Config, no puede importar un certificado que ha sido eliminado; debe obtener e importar un certificado nuevo.

1. Acceda a Web Config y seleccione la ficha **Seguridad de red**.
2. Debajo de una de las siguientes opciones de seguridad de red, seleccione el certificado correspondiente:
   - **SSL/TLS** y **Certificado**
   - **IPsec/Filtrado de IP** y **Certificado del cliente**
   - **IEEE802.1X** y **Certificado del cliente**
3. Haga clic en **Eliminar**.

   Verá un mensaje de finalización.
4. Haga clic en **Aceptar**.

Tema principal: Cómo usar un certificado digital

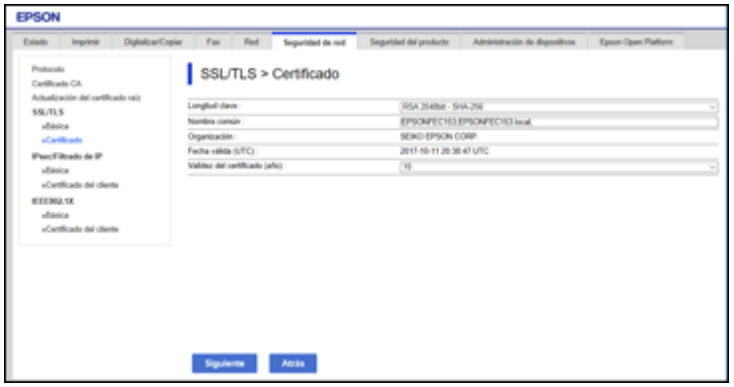
Cómo actualizar un certificado autofirmado

Si su producto es compatible con la función del servidor HTTPS, puede actualizar un certificado autofirmado a través de Web Config.

1. Acceda a Web Config y seleccione la ficha **Seguridad de red**.

2. Debajo de **SSL/TLS**, seleccione **Certificado**.
3. Haga clic en **Actualizar**.

   Verá una ventana como esta:



4. Introduzca un identificador para su producto de 1 a 128 caracteres en el campo **Nombre común**.
5. Seleccione un periodo de validez para el certificado como el ajuste **Validez del certificado (año)**.
6. Haga clic en **Siguiente**.

   Verá un mensaje de finalización.
7. Haga clic en **Aceptar**.
8. Haga clic en **Confirmar** para verificar la información del certificado.

Tema principal: Cómo usar un certificado digital

Cómo utilizar un servidor LDAP

Siga las instrucciones de las siguientes secciones para usar un servidor LDAP para proporcionar los datos del destino de faxes y mensajes de correo electrónico a través de Web Config.

Cómo configurar el servidor LDAP y seleccionar los ajustes de búsqueda
Ajustes del servidor LDAP
Ajustes de búsqueda del servidor LDAP
Cómo revisar la conexión del servidor LDAP
Mensajes del informe de la prueba de conexión del servidor LDAP

Tema principal: Cómo utilizar su producto en una red segura

Cómo configurar el servidor LDAP y seleccionar los ajustes de búsqueda

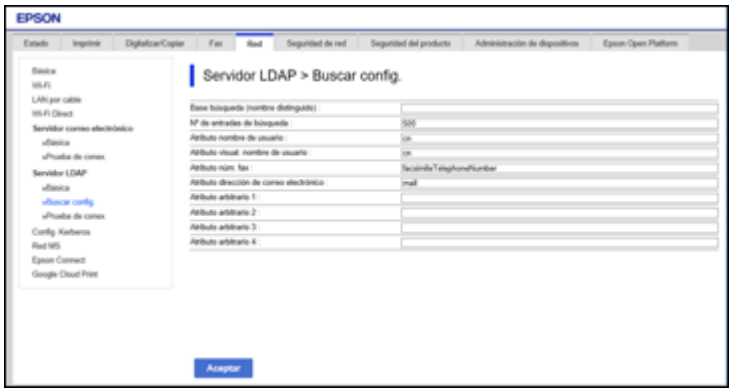
Puede configurar el servidor LDAP y seleccionar los ajustes de búsqueda a través de Web Config.

1. Acceda a Web Config y seleccione la ficha **Red**.
2. Debajo de **Servidor LDAP**, seleccione **Básica**.

   Verá una ventana como esta:

3. Seleccione **Utilizar** como el ajuste **Usar serv. LDAP**.
4. Seleccione los ajustes del servidor LDAP.
5. Haga clic en **Aceptar**.
6. Seleccione la ficha **Red**, según sea necesario.
7. Debajo de **Servidor LDAP**, seleccione **Buscar config**.

Verá una ventana como esta:



8. Seleccione los ajustes de búsqueda del servidor LDAP que desea utilizar.
9. Haga clic en **Aceptar**.

Tema principal: Cómo utilizar un servidor LDAP

Ajustes del servidor LDAP

Puede configurar estos ajustes del servidor LDAP en Web Config.

Ajuste	Opciones/Descripción
Dirección serv. LDAP	Introduzca la dirección del servidor LDAP, según sea necesario, dependiendo del formato del servidor: • Formato IPv4 o IPv6: Introduzca entre 1 y 255 caracteres. • Formato FQDN: Introduzca entre 1 y 255 caracteres alfanuméricos ASCII; puede usar "-", excepto al principio o al final de la dirección.
Nº puerto serv. LDAP	Introduzca un número de puerto del servidor LDAP entre 1 y 65535.
Conexión segura	Seleccione el método de codificación para conectar el producto al servidor LDAP.
Validación de certificado	Seleccione **Habilitar** para validar el certificado cuando conecte el producto al servidor LDAP.

Ajuste	Opciones/Descripción
Tiempo espera búsqueda (seg.)	Introduzca el tiempo máximo permitido para la búsqueda entre 5 y 300 segundos.
Método de autenticación	Seleccione uno de los métodos de autenticación disponibles de esta lista.
Dominio kerberos para utilizar	Si seleccionó **Autenticación Kerberos** como la opción de **Método de autenticación**, seleccione el dominio correcto de la autenticación Kerberos de los dominios definidos debajo del menú **Config. Kerberos**.
Nombre de usuario	Deje este campo en blanco o introduzca un nombre de usuario para el servidor LDAP de 0 a 128 caracteres Unicode (UTF-8); no utilice caracteres de control como 0x00-0x1F o OX7F (no disponible cuando selecciona **Autenticación anónima** como el **Método de autenticación**).
Contraseña	Deje este campo en blanco o introduzca una contraseña de 1 a 128 caracteres Unicode (UTF-8) para la autenticación del servidor LDAP; no utilice caracteres de control como 0x00-0x1F o OX7F (no disponible cuando selecciona **Autenticación anónima** como el **Método de autenticación**).
Config. Kerberos	
Dominio Kerberos	Si seleccionó **Autenticación Kerberos** como la opción de **Método de autenticación**, introduzca el dominio de la autenticación Kerberos de 0 a 255 caracteres ASCII; puede definir hasta 10 dominios con direcciones y números de puerto asociados.
Dirección KDC	Deje este campo en blanco o, si seleccionó **Autenticación Kerberos** como el **Método de autenticación**, introduzca la dirección del servidor Kerberos de 0 a 255 caracteres en formato IPv4, IPv6 o FQDN.
Número de puerto (kerberos)	Deje este campo en blanco o, si seleccionó **Autenticación Kerberos** como el **Método de autenticación**, introduzca el número de puerto del servidor Kerberos entre 1 y 65535.

Tema principal: Cómo utilizar un servidor LDAP

Ajustes de búsqueda del servidor LDAP

Puede configurar estos ajustes de búsqueda del servidor LDAP en Web Config.

Ajuste	Opciones/Descripción
Base búsqueda (nombre distinguido)	Deje este campo en blanco o busque un nombre de dominio arbitrario en el servidor LDAP utilizando 1 a 128 caracteres Unicode (UTF-8).
Nº de entradas de búsqueda	Especifique el máximo número de resultados de búsqueda que se debe mostrar antes de que aparezca un mensaje de error, de 1 a 500.
Atributo nombre de usuario	Introduzca el nombre de atributo para mostrar cuando busque nombres de usuario; el nombre puede tener de 1 y 255 caracteres Unicode (UTF-8); el primer carácter debe ser una letra de a-z o A-Z.
Atributo visual. nombre de usuario	Deje este campo en blanco o introduzca el nombre de atributo para mostrar como el nombre de usuario; el nombre puede tener de 1 y 255 caracteres Unicode (UTF-8); el primer carácter debe ser una letra de a-z o A-Z.
Atributo núm. fax	Introduzca el nombre de atributo para mostrar cuando busque números de fax; el nombre puede tener de 1 y 255 caracteres utilizando A-Z, a-z, 0-9 y "-" en Unicode (UTF-8); el primer carácter debe ser una letra de a-z o A-Z.
Atributo dirección de correo electrónico	Deje este campo en blanco o introduzca el nombre de atributo para mostrar cuando busque direcciones de correo electrónico; el nombre puede tener de 1 y 255 caracteres Unicode (UTF-8); el primer carácter debe ser una letra de a-z o A-Z.
Atributo arbitrario 1 - **Atributo arbitrario 4**	Deje este campo en blanco o especifique otros atributo arbitrarios para buscar de 1 y 255 caracteres Unicode (UTF-8); el primer carácter debe ser una letra de a-z o A-Z.

Tema principal: Cómo utilizar un servidor LDAP

Cómo revisar la conexión del servidor LDAP

Puede revisar la conexión del servidor LDAP y ver un informe de la conexión a través de Web Config.

1. Acceda a Web Config y seleccione la ficha **Red**.

2. Debajo de **Servidor LDAP**, seleccione **Prueba de conex**.
3. Haga clic en **Iniciar**.

   Web Config realiza la prueba de conexión y muestra un informe de la conexión al terminar.

Tema principal: Cómo utilizar un servidor LDAP

Mensajes del informe de la prueba de conexión del servidor LDAP

Puede revisar los mensajes del informe de la prueba de conexión para diagnosticar problemas de conexión con el servidor LDAP en Web Config.

Mensaje	Descripción
Prueba de conexión correcta.	La conexión con el servidor es correcta.
Error en prueba de conex. Comprobar config.	Una de las siguientes condiciones ha ocurrido: • El número del puerto o la dirección del servidor LDAP es incorrecto. • Se ha agotado el tiempo de espera. • Seleccionó **No utilizar** como el ajuste **Usar serv. LDAP**. • Si seleccionó **Autenticación Kerberos** como el **Método de autenticación**, los ajustes del servidor Kerberos son incorrectos.
Error en prueba de conex. Compruebe la fecha y la hora en la impresora o el servidor.	La conexión falló porque la configuración de hora del producto y del servidor LDAP no coinciden.
Error de autenticación. Comprobar config.	La autenticación falló porque los ajustes Nombre de usuario y Contraseña son incorrectos o, si seleccionó **Autenticación Kerberos** como el **Método de autenticación**, la hora y la fecha no están configuradas correctamente.
No se puede acceder a la impresora hasta que termine el procesamiento.	El producto está ocupado.

Tema principal: Cómo utilizar un servidor LDAP

Cómo configurar protocolos en Web Config

Puede activar o desactivar protocolos a través de Web Config.

1. Acceda a Web Config y seleccione la ficha **Seguridad de red**.

2. Seleccione o anule la selección de la casilla junto al nombre del servicio para activar o desactivar un protocolo.
3. Configure los otros ajustes de protocolo disponibles.
4. Haga clic en **Siguiente**.
5. Haga clic en **Aceptar**.

Los cambios se aplicarán después de que se reinicien los protocolos.

Ajustes de protocolo

Tema principal: Cómo utilizar su producto en una red segura

Ajustes de protocolo

Protocolos

Nombre	Descripción
Bonjour	Bonjour se utiliza para buscar dispositivos y AirPrint.
SLP	SLP se utiliza para realizar el escaneo directo y búsquedas de red en EpsonNet Config
WSD	Agregue dispositivos WSD o imprima y escanee desde el puerto WSD.
LLTD	Muestra el producto en el mapa de red de Windows.
LLMNR	Utilice la resolución de nombres sin NetBIOS aunque no pueda utilizar DNS.
LPR	Imprima desde el puerto LPR.
RAW (Puerto 9100)	Imprima desde el puerto RAW (Puerto 9100)
IPP	Imprima a través de Internet, incluso AirPrint.
FTP	Imprima a través de un servidor FTP.
SNMPv1/v2c	Configure y supervise su producto de forma remota.
SNMPv3	Configure y supervise su producto de forma remota con el protocolo SNMPv3.

Configuración Bonjour

Ajuste	Opciones/Descripción
Usar Bonjour	Busque o utilice dispositivos a través de Bonjour (no puede usar AirPrint si está desactivado).
Nombre Bonjour	Muestra el nombre Bonjour.
Nombre de servicio Bonjour	Muestra el nombre de servicio Bonjour.
Ubicación	Muestra el nombre de ubicación de Bonjour.
Protocolo de prioridad principal	Selecciona el protocolo que es la prioridad principal para la impresión Bonjour.
Wide-Area Bonjour	Habilita el protocolo Wide-Area Bonjour; registre todos los productos en un servidor DNS para localizarlos a través del segmento.

Conifg. SLP

Ajuste	Opciones/Descripción
Habilitar SLP	Active la función SLP para usar la función de escaneo directo y para realizar búsquedas de red en EpsonNet Config.

Configuración WSD

Ajuste	Opciones/Descripción
Habilitar WSD	Active este ajuste para añadir dispositivos usando WSD y para imprimir y escanear desde el puerto WSD.
Tiempo espera Impr. (seg.)	Introduzca el valor del tiempo de espera de comunicación para la impresión WSD entre 3 y 3.600 segundos.
Tiempo de espera dig. (seg.)	Introduzca el valor del tiempo de espera de comunicación para el escaneo WSD entre 3 y 3.600 segundos.
Nombre disp.	Muestra el nombre de dispositivo de WSD.
Ubicación	Muestra el nombre de ubicación de WSD.

Config. LLTD

Ajuste	Opciones/Descripción
Habilitar LLTD	Active LLTD para mostrar el producto en el mapa de red de Windows.
Nombre disp.	Muestra el nombre de dispositivo de LLTD.

Config. LLMNR

Ajuste	Opciones/Descripción
Habilitar LLMNR	Active LLMNR para usar la resolución de nombres sin NetBIOS aunque no pueda utilizar DNS.

Config. LPR

Ajuste	Opciones/Descripción
Permitir impr. puerto LPR	Permite la impresión desde el puerto LPR.
Tiempo espera Impr. (seg.)	Introduzca el valor del tiempo de espera para la impresión LPR entre 0 y 3.600 segundos.

Config. RAW (Puerto 9100)

Ajuste	Opciones/Descripción
Permitir impr. RAW (Puerto 9100)	Seleccione esta opción para permite la impresión desde el puerto RAW (Puerto 9100).
Tiempo espera Impr. (seg.)	Introduzca el valor del tiempo de espera para la impresión RAW (Puerto 9100) entre 0 y 3.600 segundos.

Config. IPP

Ajuste	Opciones/Descripción
Habilitar IPP	Active la comunicación IPP para productos que se muestran que admiten IPP (no puede usar AirPrint si está desactivado).

Ajuste	Opciones/Descripción
Permitir comunicación no segura	Deje que la impresora se comunique sin medidas de seguridad (IPP).
Tiempo de espera de comunicación (seg.)	Introduzca el valor del tiempo de espera para la impresión IPP entre 0 y 3.600 segundos.
URL(red)	Muestra las direcciones URL IPP (http y https) cuando el producto está conectado mediante una red alámbrica o inalámbrica (la dirección es un valor combinado de la dirección IP, el número de puerto y el nombre de impresora IPP del producto).
URL(Wi-Fi Direct)	Muestra las direcciones URL IPP (http y https) cuando el producto está conectado mediante Wi-Fi Direct (la dirección es un valor combinado de la dirección IP, el número de puerto y el nombre de impresora IPP del producto).
Nombre de la impresora	Muestra el nombre de la impresora IPP.
Ubicación	Muestra la ubicación de IPP.

Configuración de FTP

Ajuste	Opciones/Descripción
Activar servidor FTP	Activa la impresión FTP para productos que admiten la impresión a través de un servidor FTP.
Tiempo de espera de comunicación (seg.)	Introduzca el valor del tiempo de espera para comunicación FTP entre 3 y 3.600 segundos.

Configuración de SNMPv1/v2c

Ajuste	Opciones/Descripción
Activar SNMPv1/v2c	Active SNMPv1/v2c para productos que admiten SNMPv3.
Autoridad de acceso	Configure la autoridad de acceso cuando SNMPv1/v2c está activada en **Sólo lectura o Lectura/Escritura**.
Nombre de comunidad (solo lectura)	Introduzca entre 0 y 32 caracteres ASCII.
Nombre de comunidad (lectura/escritura)	Introduzca entre 0 y 32 caracteres ASCII.

Ajustes de SNMPv3

Ajuste	Opciones/Descripción
Activar SNMPv3	Active SNMPv3 para productos que admiten SNMPv3.
Nombre de usuario	Introduzca entre 1 y 32 caracteres.
Configuración de autenticación	Seleccione un algoritmo y configure una contraseña para una autenticación.
Configuración de cifrado	Seleccione un algoritmo y configure una contraseña para una codificación.
Nombre de contexto	Introduzca entre 1 y 32 caracteres.

Tema principal: Cómo configurar protocolos en Web Config

Referencias relacionadas

Ajustes de SNMPv3

Cómo utilizar un servidor de correo electrónico

Siga las instrucciones de las siguientes secciones para usar un servidor de correo electrónico para enviar datos de escaneo y de fax por correo electrónico, o para usar la función de notificaciones por correo electrónico a través de Web Config.

Cómo configurar un servidor de correo electrónico

Ajustes del servidor de correo electrónico

Cómo revisar la conexión del servidor de correo electrónico

Mensajes del informe de la prueba de conexión del servidor de correo electrónico

Cómo configurar notificaciones por correo electrónico

Tema principal: Cómo utilizar su producto en una red segura

Cómo configurar un servidor de correo electrónico

Puede configurar un servidor de correo electrónico a través de Web Config.

1. Acceda a Web Config y seleccione la ficha **Red**.
2. Debajo de **Servidor correo electrónico**, seleccione **Básica**.

Verá una ventana como esta:

3. Seleccione los ajustes del servidor de correo electrónico.
4. Haga clic en **Aceptar**.

Tema principal: Cómo utilizar un servidor de correo electrónico

Ajustes del servidor de correo electrónico

Puede configurar estos ajustes del servidor de correo electrónico en Web Config.

Ajuste	Opciones/Descripción
Método de autenticación	Seleccione el método de autenticación que corresponde a su servidor de correo electrónico.
Cuenta autenticada	Introduzca el nombre de cuenta autenticada de 1 a 255 caracteres ASCII.
Contraseña autenticada	Introduzca la contraseña autenticada de 1 a 20 caracteres ASCII, utilizando A-Z, a-z, 0-9 y estos caracteres: ! # $ % ' * + - . / = ? ^ _ { ! } ~ @
Dirección correo del remitente	Introduzca la dirección de correo electrónico del remitente de 1 a 255 caracteres ASCII; no use un punto (.) como el primer carácter y tampoco utilice estos caracteres: ( ) < > [ ] ;
Dirección del servidor SMTP	Introduzca la dirección del servidor SMTP de 1 a 255 caracteres, utilizando A-Z, a-z, 0-9 y "-" en formato IPv4 o FQDN.

Ajuste	Opciones/Descripción
Nº de puerto del servidor SMTP	Introduzca el número de puerto del servidor SMTP entre 1 y 65535.
Conexión segura	Seleccione el método de seguridad para el servidor de correo electrónico; las opciones disponibles dependen del **Método de autenticación**.
Validación de certificado	Active la verificación de un certificado válido; el valor recomendado es **Habilitar**.
Dirección del servidor POP3	Introduzca la dirección del servidor POP de 1 a 255 caracteres, utilizando A-Z, a-z, 0-9 y "-" en formato IPv4 o FQDN.
Nº de puerto del servidor POP3	Introduzca el número de puerto del servidor POP entre 1 y 65535.

Tema principal: Cómo utilizar un servidor de correo electrónico

Cómo revisar la conexión del servidor de correo electrónico

Puede revisar la conexión del servidor de correo electrónico y ver un informe de la conexión a través de Web Config.

1. Acceda a Web Config y seleccione la ficha **Red**.
2. Debajo de **Servidor correo electrónico**, seleccione **Prueba de conex**.
3. Haga clic en **Iniciar**.

   Web Config realiza la prueba de conexión y muestra un informe de la conexión al terminar.

Tema principal: Cómo utilizar un servidor de correo electrónico

Mensajes del informe de la prueba de conexión del servidor de correo electrónico

Puede revisar los mensajes del informe de la prueba de conexión para diagnosticar problemas de conexión con el servidor de correo electrónico en Web Config.

Mensaje	Descripción
Prueba de conexión correcta.	La conexión con el servidor es correcta.

Mensaje	Descripción
Error de comunicación del servidor SMTP. Compruebe lo siguiente - Configuración de red	Una de las siguientes condiciones ha ocurrido: • El producto no está conectado a una red. • El servidor SMTP está fuera de servicio. • La conexión de red se desconecta durante la comunicación. • Se recibieron datos incompletos.
Error de comunicación del servidor POP3. Compruebe lo siguiente - Configuración de red	Una de las siguientes condiciones ha ocurrido: • El producto no está conectado a una red. • El servidor POP3 está fuera de servicio. • La conexión de red se desconecta durante la comunicación. • Se recibieron datos incompletos.
Error al conectar con el servidor SMTP. Compruebe lo siguiente - Dirección del servidor SMTP - Servidor DNS	Una de las siguientes condiciones ha ocurrido: • La resolución DNS falló. • La resolución de nombre para un servidor SMTP falló.
Error al conectar con el servidor POP3. Compruebe lo siguiente - Dirección del servidor POP3 - Servidor DNS	Una de las siguientes condiciones ha ocurrido: • La resolución DNS falló. • La resolución de nombre para un servidor POP3 falló.
Error de autenticación del servidor SMTP. Compruebe lo siguiente - Método de autenticación - Cuenta autenticada - Contraseña autenticada	La autenticación del servidor EAP falló.
Error de autenticación del servidor POP3. Compruebe lo siguiente - Método de autenticación - Cuenta autenticada - Contraseña autenticada	La autenticación del servidor POP3 falló.
Método de comunicación no admitido. Compruebe lo siguiente - Dirección del servidor SMTP - Nº de puerto del servidor SMTP	El protocolo de comunicación no es admitido.

Mensaje	Descripción
Error de conexión con el servidor SMTP. Cambie Conexión segura a Ninguno.	Hay una discordancia SMTP entre un servidor y un cliente o el servidor no admite una conexión segura SMTP.
Error de conexión con el servidor SMTP. Cambie Conexión segura a SSL/TLS.	Hay una discordancia SMTP entre un servidor y un cliente o el servidor está solicitando una conexión SSL/TLS para SMTP.
Error de conexión con el servidor SMTP. Cambie Conexión segura a STARTTLS.	Hay una discordancia SMTP entre un servidor y un cliente o el servidor está solicitando una conexión STARTTLS para SMTP.
La conexión no es de confianza. Compruebe lo siguiente - Fecha y hora	La configuración de la fecha y la hora del producto es incorrecta o el certificado ha caducado.
La conexión no es de confianza. Compruebe lo siguiente - Certificado CA	El producto tiene un certificado raíz que no corresponde o no se ha importado un certificado firmado por una CA.
La conexión no es de confianza.	El certificado está dañado.
Error de autenticación del servidor SMTP. Cambie Método de autenticación a AUTENTICACIÓN SMTP.	Hay una discordancia en el método de autenticación entre un servidor y un cliente. El servidor no admite AUTENTICACIÓN SMTP.
Error de autenticación del servidor SMTP. Cambie Método de autenticación a POP antes de SMTP.	Hay una discordancia en el método de autenticación entre un servidor y un cliente. El servidor no admite AUTENTICACIÓN SMTP.
Dirección correo del remitente es incorrecto. Cambie a la dirección de correo electrónico para el servicio de correo electrónico.	La dirección de correo electrónico del remitente especificada es incorrecta.
No se puede acceder a la impresora hasta que termine el procesamiento.	El producto está ocupado.

Tema principal: Cómo utilizar un servidor de correo electrónico

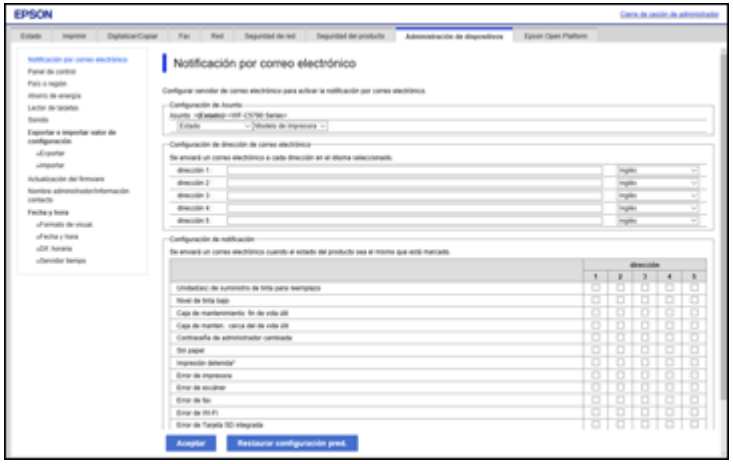
Cómo configurar notificaciones por correo electrónico

Puede configurar notificaciones por correo electrónico utilizando Web Config para que pueda recibir alertas por correo electrónico cuando ocurra algo en el producto, como cuando se termine el papel.

Puede registrar hasta 5 direcciones de correo electrónico y seleccionar los eventos para los cuales desea recibir una notificación.

1. Acceda a Web Config y seleccione la ficha **Administración de dispositivos**.

   Verá una ventana como esta:



2. Introduzca una dirección de correo electrónico en el campo **Dirección 1**.
3. Seleccione el idioma en el que desea recibir las notificaciones por correo electrónico del menú desplegable para la primera dirección.
4. Introduzca direcciones de correo electrónico adicionales en los campos **Dirección 2** a **Dirección 5**, según sea necesario, y seleccione un idioma para cada una.
5. Seleccione las casillas para indicar los eventos para los cuales desea recibir notificaciones por correo electrónico.
6. Haga clic en **Aceptar**.

Tema principal: Cómo utilizar un servidor de correo electrónico

Cómo usar el software de configuración de red EpsonNet Config

Siga las instrucciones de las siguientes secciones para configurar los ajustes de red de administrador de su producto utilizando el software EpsonNet Config.

En Windows, puede configurar los ajustes de red en una operación de lote. Consulte la utilidad de ayuda de EpsonNet Config para obtener instrucciones.

Nota: Antes de que pueda configurar los ajustes de administración de sistema, conecte el producto a una red. Consulte la *Guía de instalación* y el *Manual del usuario* del producto para obtener instrucciones.

Cómo instalar EpsonNet Config
Cómo configurar una dirección IP del producto con EpsonNet Config

Cómo instalar EpsonNet Config

Para instalar EpsonNet Config, descargue el software de la página de soporte del producto en latin.epson.com/soporte y siga las instrucciones que aparecen en pantalla.

Tema principal: Cómo usar el software de configuración de red EpsonNet Config

Cómo configurar una dirección IP del producto con EpsonNet Config

Puede configurar la dirección IP del producto utilizando EpsonNet Config.

1. Encienda el producto.
2. Conecte el producto a una red con un cable Ethernet.
3. Realice una de las siguientes acciones para iniciar EpsonNet Config:
   - **Windows 10**: Haga clic en > **Todas las aplicaciones** > **EpsonNet** > **EpsonNet Config**.
   - **Windows 8.x**: Navegue a la pantalla **Aplicaciones** y seleccione **EpsonNet** > **EpsonNet Config**.
   - **Windows (otras versiones)**: Haga clic en o en **Inicio**, luego seleccione **Todos los programas** o **Programas**. Seleccione **EpsonNet** > **EpsonNet Config**.
   - **Mac**: Abra la carpeta **Aplicaciones**, abra la carpeta **Epson Software** y seleccione **EpsonNet** > **EpsonNet Config** > **EpsonNet Config**.

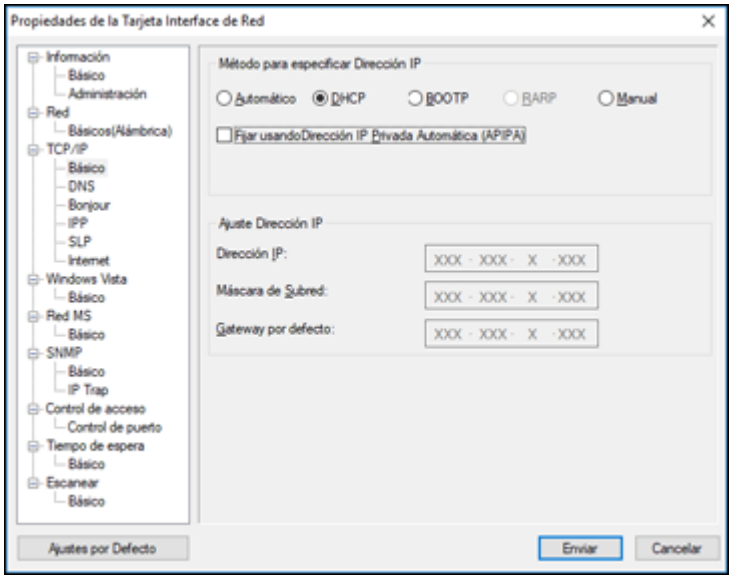
Después de unos momentos, el programa muestra los productos conectados.

4. Haga doble clic en el producto que va a configurar.

   Nota: Si hay varios productos del mismo modelo conectados, puede identificarlos por su dirección MAC.

5. En el menú a la izquierda, debajo de **TCP/IP**, seleccione **Básico**.

   Verá una ventana como esta:



6. Seleccione **Manual**.
7. Introduzca los ajustes de **Dirección IP**, **Máscara subred** y **Puerta de enlace predeterminada** en los campos proporcionados.

   Nota: Para conectar el producto a una red segura, introduzca una dirección IP estática. También puede configurar los ajustes DNS seleccionando **DNS** e introducir los ajustes de proxy seleccionando **Internet** del menú **TCP/IP**.

8. Seleccione **Enviar**.

9. Introduzca la contraseña de administrador actual, si es necesario, y haga clic en **Aceptar**.

Tema principal: Cómo usar el software de configuración de red EpsonNet Config

Cómo usar el software de configuración Epson Device Admin

En Windows, puede detectar y monitorear dispositivos remotos y configurar los ajustes de red en una operación de lote. Consulte la utilidad de ayuda de Epson Device Admin para obtener instrucciones.

Para instalar Epson Device Admin, descargue el software de la página de soporte en latin.epson.com/soporte y siga las instrucciones que aparecen en pantalla.

Solución de problemas

Consulte las siguientes secciones para obtener soluciones a problemas que pueda tener con el software de configuración de red.

Mensajes de error de escaneo

Si ve un mensaje de error cuando escanea imágenes a una carpeta compartida, busque las soluciones en esta tabla.

Mensaje	Solución
Error de DNS. Compruebe la configuración de DNS.	Haga lo siguiente: • Asegure que la dirección en la lista de contactos de la impresora y la dirección de la carpeta compartida sean iguales. • Si la dirección IP de la computadora es estática o se configura manualmente, cambie el nombre de la computadora en la ruta de red a la dirección IP. Por ejemplo, cambie \\EPSON02\SCAN a \\192.168.xxx.xxx\SCAN. • Compruebe que la computadora esté encendida y que no esté en modo de ahorro de energía, como en reposo o en espera. Si la computadora está en modo de reposo, no puede guardar las imágenes escaneadas en la carpeta compartida. • Desactive temporalmente el firewall o el software de seguridad de la computadora. Si esto no elimina el error, revise los ajustes en el software de seguridad. • Si está utilizando una computadora portátil y la dirección IP está configurada en DHCP, es posible que la dirección IP cambie cuando vuelva a conectarse a la red. Obtenga la dirección IP nuevamente. • Revise los ajustes DNS de la impresora utilizando el panel de control del producto. • Revise los ajustes DNS de su servidor, computadora o punto de acceso. • El nombre de la computadora y la dirección IP pueden ser diferentes cuando la tabla de gestión del servidor DNS no se actualiza. Revise el nombre de la computadora y la dirección IP.

Mensaje	Solución
Error de autenticación. Compruebe el método de autent., la cuenta autenticada y la contraseña autenticada.	Haga lo siguiente: • Si se han habilitado las restricciones de usuario, asegúrese de introducir correctamente el nombre de usuario y la contraseña. También compruebe que la contraseña no ha expirado. • Revise los ajustes **Ubicación**.
Error de comunicación. Compruebe la conexión Wi-Fi/red.	Haga lo siguiente: • Compruebe que la Red MS esté habilitada. • Asegure que la dirección en la lista de contactos de la impresora y la dirección de la carpeta compartida sean iguales. • Debe agregar los derechos de acceso para el usuario en la lista de contactos a las fichas Compartir y Seguridad de las propiedades de la carpeta compartida. Los permisos de acceso también se deben habilitar para el usuario. • Revise los ajustes **Ubicación**. • Imprima un informe de la conexión de red para verificar que la impresora está conectada a la red.
El nombre de archivo ya está en uso. Cambie el nombre del archivo y vuelva a escanear.	Revise si hay un archivo con el mismo nombre que el archivo que desea guardar en la carpeta compartida. Elimine el archivo guardado o seleccione un nombre de archivo diferente.
Archivo(s) escaneado(s) demasiado grande(s). Solo se enviaron XX página(s). Compruebe si la carpeta de destino tiene espacio suficiente.	Haga lo siguiente: • Aumente el espacio de almacenamiento en la carpeta especificada. • Reduzca el número de documentos. • Reduzca la resolución de escaneo o aumente la relación de compresión para reducir el tamaño de la imagen escaneada.

Tema principal: Solución de problemas

Solución de problemas de uso del software de red

Consulte las siguientes secciones si tiene problemas con el software de red.

Tema principal: Solución de problemas

No puede acceder a Web Config

Si no puede acceder a Web Config en su producto, pruebe estas soluciones:

- Compruebe que el producto esté encendido y conectado a la red utilizando la dirección IP correcta. Verifique la conexión utilizando el panel de control del producto o imprima una hoja de estado de la red. Consulte el *Manual del usuario* de su producto para obtener instrucciones.
- Si seleccionó **Alto** como el ajuste **Intensidad de cifrado** en Web Config, su navegador debe ser compatible con la codificación AES (de 256 bits) o 3DES (de 168 bits). Averigüe con cuáles codificaciones es compatible su navegador o seleccione una opción de **Intensidad de cifrado** diferente.
- Si está utilizando un servidor proxy con su producto, configure los ajustes de proxy del navegador de la siguiente manera:
  - **Windows 10**: Haga clic en > **Configuración** > **Red e Internet** > **Proxy**. Desplácese hacia abajo y configure **Usar un servidor proxy** en **Activado**. Seleccione **No usar servidor proxy para direcciones locales (intranet)**.
  - **Windows 8.x**: Navegue a la pantalla **Aplicaciones** y seleccione **Configuración de PC** > **Red** > **Proxy**. Desplácese hacia abajo y configure **Usar un servidor proxy** en **Activado**. Seleccione **No usar servidor proxy para direcciones locales (intranet)**.
  - **Windows (otras versiones)**: Haga clic en o en **Inicio** y seleccione **Panel de control** > **Red e Internet** > **Opciones de Internet** > **Conexiones** > **Configuración de LAN** > **Servidor proxy** > **No usar servidor proxy para direcciones locales**.
  - **Mac**: Seleccione **Preferencias del Sistema** > **Red** > **Avanzado** > **Proxies**. Registre la dirección local bajo **Omitir ajustes proxy para estos servidores y dominios**. Por ejemplo, 192.168.1.*: Dirección local 192.168.1.XXX, máscara de subred 255.255.255.0.

Tema principal: Solución de problemas de uso del software de red

Aparece el mensaje "Sin actualizar"

Si aparece el mensaje "Sin actualizar" cuando accede a Web Config utilizando la comunicación SSL (HTTPS), el certificado ha caducado. Compruebe que la fecha y la hora del producto estén configuradas correctamente y obtenga un certificado nuevo.

Tema principal: Solución de problemas de uso del software de red

Aparece el mensaje "El nombre del certificado de seguridad no coincide"

Si aparece un mensaje que empieza con "El nombre del certificado de seguridad no coincide..." cuando accede a Web Config utilizando la comunicación SSL (HTTPS), la dirección IP del producto en la CSR o en el certificado autofirmado no coincide con la dirección que introdujo en el navegador. Cambie la dirección IP que introdujo como el ajuste **Nombre común** y obtenga e importe un certificado otra vez, o cambie el nombre del producto.

Tema principal: Solución de problemas de uso del software de red

El nombre del modelo o la dirección IP no aparece en EpsonNet Config

Si el nombre del modelo del producto o la dirección IP no aparece en EpsonNet Config, pruebe estas soluciones:

- Si seleccionó la opción de bloquear, cancelar o apagar en un mensaje de seguridad de Windows o en la pantalla de firewwall, no se pueden mostrar la dirección IP y el nombre del modelo en EpsonNet Config. Registre EpsonNet Config como una excepción en el firewall o software de seguridad, o bien, cierre el software de seguridad e intente ejecutar EpsonNet Config una vez más.
- Es posible que se haya agotado el tiempo de espera. Seleccione **Herramientas**, seleccione **Opciones**, seleccione **Tiempo de espera** y aumente la opción de tiempo para el ajuste **Error de comunicación**. Tenga presente que al aumentar ese tiempo, EpsonNet puede funcionar con más lentitud.

Tema principal: Solución de problemas de uso del software de red

Solución de problemas de seguridad de red

Consulte las siguientes secciones si tiene problemas con las funciones de seguridad de red.

No puede acceder al producto después de configurar la red IEEE 802.1X

Tema principal: Solución de problemas

Ha olvidado la clave precompartida

Si olvida una clave precompartida, cambie la clave utilizando Web Config para la política predeterminada o la política de grupo.

Tema principal: Solución de problemas de seguridad de red

No se puede comunicar con el producto utilizando la comunicación IPsec

Compruebe que su computadora esté usando uno de estos algoritmos compatibles para comunicarse con el producto:

Método de seguridad	Algoritmos compatibles
Algoritmo de codificación IKE	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
Algoritmo de autenticación IKE	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Algoritmo de intercambio de la clave IKE	DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30*
Algoritmo de codificación ESP	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
Algoritmo de autenticación ESP	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Algoritmo de autenticación AH	

* Disponible solo para IKEv2.

Tema principal: Solución de problemas de seguridad de red

La comunicación se interrumpió de repente

Si la comunicación de red estaba funcionando, pero se interrumpió de repente, es posible que la dirección IP del producto o de la computadora se haya cambiado o es inválida. Pruebe las siguientes soluciones:

- Desactive IPsec utilizando el panel de control del producto.
- Si el DHCP ha caducado, o si la dirección IPv6 ha caducado o no se obtuvo, es posible que no pueda encontrar la dirección IP registrada en Web Config.
- Si esto no resuelve el problema, introduzca una dirección IP estática a través de Web Config.

Tema principal: Solución de problemas de seguridad de red

No puede crear el puerto de impresión IPP segura

Si no puede crear el puerto de impresión IPP segura, pruebe estas soluciones:

- Asegure que haya especificado el certificado del servidor correcto para la comunicación SSL/TLS a través de Web Config.
- Si está utilizando un certificado CA, confirme que se haya importado a la computadora que está accediendo al producto.

Tema principal: Solución de problemas de seguridad de red

No puede establecer una conexión después de configurar el protocolo IPsec/Filtrado de IP

Es posible que el valor configurado es incorrecto. Desactive IPsec/Filtrado de IP desde el panel de control del producto. Conecte la computadora y configure los ajustes de IPsec/Filtrado de IP otra vez.

Tema principal: Solución de problemas de seguridad de red

No puede acceder al producto después de configurar la red IEEE 802.1X

Si no puede acceder al producto después de configurar la red IEEE 802.1X, desactive la red IEEE 802.1X y la conexión Wi-Fi utilizando el panel de control del producto. Luego, conecte el producto a una computadora y configure la red IEEE 802.1X a través de Web Config otra vez.

Tema principal: Solución de problemas de seguridad de red

Solución de problemas con certificados digitales

Consulte las siguientes secciones si tiene problemas usando un certificado digital.

Mensajes de advertencias de un certificado digital
No puede importar un certificado digital
No puede actualizar un certificado o crear una CSR
Eliminó un certificado firmado por una CA

Tema principal: Solución de problemas

Mensajes de advertencias de un certificado digital

Si ve un mensaje de advertencia cuando está utilizando un certificado digital, consulte las soluciones en esta tabla.

Mensaje	Solución
Introduzca un certificado de servidor.	Seleccione un archivo de certificado y haga clic en **Importar**.
No se ha introducido el Certificado CA 1.	Importe el certificado CA 1 antes de importar más certificados.
Valor no válido a continuación.	Elimine los caracteres no admitidos de la ruta del archivo o la contraseña.
Fecha y hora no válidas.	Configure la fecha y la hora en el producto utilizando Web Config, EpsonNet Config o el panel de control del producto.
Contraseña no válida.	Introduzca la contraseña que coincida con la contraseña configurada para el certificado CA.
Archivo no válido.	Haga lo siguiente: • Importe solo archivos de certificados en formato X509 enviados por una autoridad de certificados de confianza. • Compruebe que el tamaño del archivo sea de 5 KB o menos y que no esté dañado o sea falso. • Confirme que la cadena que contiene el certificado es válida; revise el sitio Web de la autoridad de certificados.

Mensaje	Solución
No se pueden usar los certificados de servidor que incluyen más de tres certificados CA.	Importe archivos de certificados en formato PKCS#12 que contienen dos certificados como máximo o convierta cada certificado en formato PRM y vuelva a importarlos.
El certificado ha caducado. Compruebe que el certificado es válido, o compruebe la fecha y la hora en la impresora.	Asegure que la hora y la fecha del producto estén configuradas correctamente y, si el certificado ha caducado, obtenga e importe un certificado nuevo.
Se necesita una clave privada.	Realice una de las siguientes acciones para emparejar una clave privada con el certificado: • Para certificados en formato PEM/DER obtenidos a partir de una CSR con una computadora, especifique el archivo de la clave privada. • Para certificados en formato PKCS#12 obtenidos a partir de una CSR con una computadora, cree un archivo que contiene la clave privada. Si reimportó un certificado en formato PEM/DER obtenido a partir de una CSR con Web Config, solamente lo puede importar una vez. Debe obtener e importar un certificado nuevo.
La configuración ha fallado.	Asegure que la computadora y el producto estén conectados y que el archivo del certificado no esté dañado, luego importe el archivo del certificado otra vez.

Tema principal: Solución de problemas con certificados digitales

No puede importar un certificado digital

Si no puede importar un certificado digital, pruebe estas soluciones:

- Compruebe que el certificado firmando por una CA y la CSR tienen la misma información. Si no coinciden, importe el certificado a un dispositivo que sí tiene la misma información o use la CSR para obtener el certificado firmado por una CA otra vez.
- Verifique que el tamaño del archivo del certificado firmado por una CA es de 5 KB o menos.

- Asegure que esté introduciendo la contraseña correcta.

Tema principal: Solución de problemas con certificados digitales

No puede actualizar un certificado o crear una CSR

Si no puede actualizar un certificado autofirmado o crear una CSR para un certificado firmado por una CA, pruebe estas soluciones:

- Compruebe que haya introducido un ajuste de **Nombre común** en Web Config.
- Compruebe que el ajuste de **Nombre común** no contiene caracteres no compatibles o está dividido por una coma. Corrija el ajuste y actualice el certificado otra vez.

Tema principal: Solución de problemas con certificados digitales

Eliminó un certificado firmado por una CA

Si eliminó un certificado firmado por una CA sin querer, pruebe estas soluciones:

- Si guardó un archivo de copia de seguridad, importe el certificado firmado por una CA otra vez.
- Si obtuvo el certificado usando una CSR creada en Web Config, no puede importar un certificado que ha sido eliminado. Cree una CSR nueva y obtenga un certificado nuevo.

Tema principal: Solución de problemas con certificados digitales

Dónde obtener ayuda

Si necesita ayuda adicional con su producto Epson, póngase en contacto con Epson.

Epson ofrece estos servicios de soporte técnico:

Soporte por Internet

Visite la página de soporte de Epson en latin.epson.com/soporte para obtener soluciones a los problemas más comunes. Puede descargar drivers y los manuales, obtener respuestas a preguntas frecuentes y soluciones de problemas, o enviar un correo electrónico a Epson con sus preguntas.

Hable con un representante de soporte técnico

Antes de llamar a Epson para obtener asistencia, tenga a la mano la siguiente información:

- Nombre del producto
- Número de serie del producto (ubicado en una etiqueta en el producto)
- Prueba de compra (como el recibo de la tienda) y fecha de adquisición

- Configuración de la computadora
- Descripción del problema

Luego, marque uno de los siguientes números de teléfono:

País	Teléfono
Argentina	(54 11) 5167-0300 0800-288-37766
Bolivia*	800-100-116
Brasil	Para obtener el número de teléfono de soporte para su producto, visite la página epson.com.br/suporte, seleccione su produco y haga clic en la ficha **Entre em contato conosco**.
Chile	(56 2) 2484-3400
Colombia	Bogotá: (57 1) 592-2200 Resto del país: 018000-915235
Costa Rica	800-377-6627
Ecuador*	1-800-000-044
El Salvador*	800-6570
Guatemala*	1-800-835-0358
México	México, D.F.: (52 55) 1323-2052 Resto del país: 01-800-087-1080
Nicaragua*	00-1-800-226-0368
Panamá*	00-800-052-1376
Paraguay	009-800-521-0019
Perú	Lima: (51 1) 418-0210 Resto del país: 0800-10126
República Dominicana*	1-888-760-0068
Uruguay	00040-5210067
Venezuela	(58 212) 240-1111

* Para llamar desde teléfonos móviles a estos números gratuitos, póngase en contacto con su operador telefónico local.

Si su país no figura en la lista, comuníquese con la oficina de ventas de Epson del país más cercano. Puede incurrir en costos de llamada interurbana o de larga distancia.

Compra de suministros y accesorios

Puede adquirir papel y tinta Epson originales de un distribuidor de productos Epson autorizado. Para encontrar el más cercano, visite la página latin.epson.com o llame a la oficina de ventas de Epson más cercana.

Tema principal: Solución de problemas

Avisos

Consulte las siguientes secciones para conocer avisos importantes.

Marcas comerciales

EPSON® es una marca registrada y EPSON Exceed Your Vision es un logotipo registrado de Seiko Epson Corporation.

Mac es una marca comercial de Apple Inc., registrada en EE. UU. y en otros países.

Google Cloud Print™ es una marca comercial de Google LLC.

Aviso general: El resto de los productos que se mencionan en esta publicación aparecen únicamente con fines de identificación y pueden ser marcas comerciales de sus respectivos propietarios. Epson renuncia a todos los derechos sobre dichas marcas.

Tema principal: Avisos

Aviso de derechos reservados

Seiko Epson Corporation no se hace responsable por ningún daño o problemas causados por el uso de diferentes accesorios o productos consumibles que no sean Productos originales Epson o Productos aprobados Epson ratificados por Seiko Epson Corporation.

Seiko Epson Corporation no se hace responsable de cualquier daño provocado por interferencias electromagnéticas producidas al utilizar cables de interfaz que no sean designados como Productos aprobados Epson ratificados por Seiko Epson Corporation.

La información que se incluye en el presente está sujeta a cambios sin previo aviso.

Atribución de derechos reservados

Tema principal: Avisos

Atribución de derechos reservados

11/18

CPD-55306R1

Tema principal: Aviso de derechos reservados