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.
- Importación y exportación de los ajustes: 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, conecte 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, conecte 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. Determine 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 Configuración básica:

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

Cómo cambiar la contraseña de administrador en Web Config

Puede configurar una contraseña de administrador utilizando el panel de control del producto o a través de 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, seleccione **Configuración del administrador** y seleccione **Cambiar la Información de autenticación del administrador**.

   Verá una ventana como esta:

2. 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.
3. Haga clic en **Aceptar**.

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

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 los ajustes de 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 configurar protocolos y servicios en Web Config
Cómo utilizar un servidor de correo electrónico
Cómo importar y exportar los ajustes de Web Config

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

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 **Configuración de seguridad de red**.
2. Seleccione **SSL/TLS** y seleccione **Básica**.
3. Seleccione una de las opciones para el ajuste **Intensidad de cifrado**.
4. Seleccione **Habilitar** o **Deshabilitar** para 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 utilizar su producto en una red segura

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.

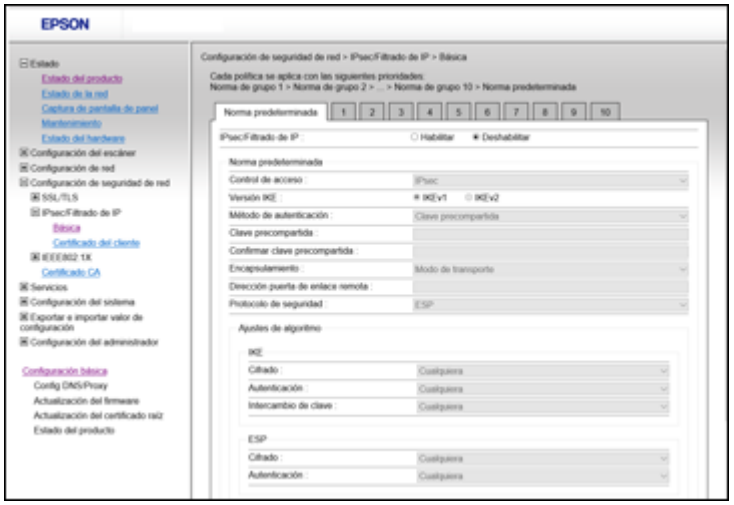
Tema principal: Cómo configurar el protocolo IPsec/Filtrado de IP

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 **Configuración de seguridad de red**.
2. Seleccione **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**.

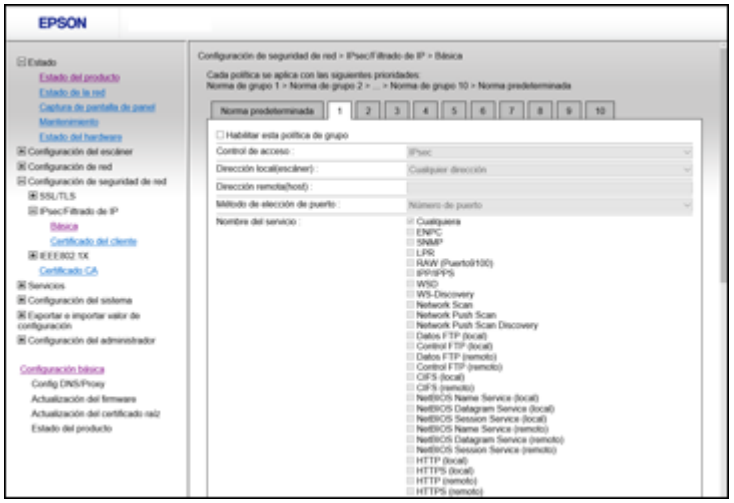
Tema principal: Cómo configurar el protocolo IPsec/Filtrado de IP

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 **Configuración de seguridad de red**.
2. Seleccione **IPsec/Filtrado de IP** y 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	Seleccione **Permitir acceso** para permitir que pasen los paquetes IP configurados. Seleccione **Denegar acceso** para prohibir que pasen los paquetes IP. Seleccione **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.
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.

Ajuste	Opciones/Descripción
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	Seleccione **Permitir acceso** para permitir que pasen los paquetes IP configurados. Seleccione **Denegar acceso** para prohibir que pasen los paquetes IP. Seleccione **IPsec** para permitir que pasen los paquetes IPsec.
Dirección local(escáner)	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 siguiente tabla 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**.
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	Operaciones controladas
ENPC	UDP	3289/cualquier puerto	Búsqueda de un producto desde aplicaciones, tales como un driver de escáner o EpsonNet Config
SNMP	UDP	161/cualquier puerto	Adquisición y configuración de MIB desde aplicaciones, tales como un driver de escáner o EpsonNet Config
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
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 actualización de firmware y actualización de certificado raíz en un cliente HTTP o HTTPS
HTTPS (remoto)	TCP	Cualquier puerto/443	

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 aceptar datos de escaneo utilizando Epson Scan 2 y ajustes de escaneo

Utilice este ejemplo para permitir la comunicación de datos de escaneo y los ajustes del escáner desde los servicios especificados.

Política predeterminada:

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

Política de grupo:

- **Habilitar esta política de grupo**: Seleccione esta casilla.
- **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**, **Escaneado por red**, **HTTP (local)** y **HTTPS (local)**

Para recibir acceso únicamente de una dirección IP especificada

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:

- **Habilitar esta política de grupo**: Seleccione esta casilla.
- **Control de acceso**: **Permitir acceso**
- **Dirección remota(host)**: Dirección IP del cliente de un administrador

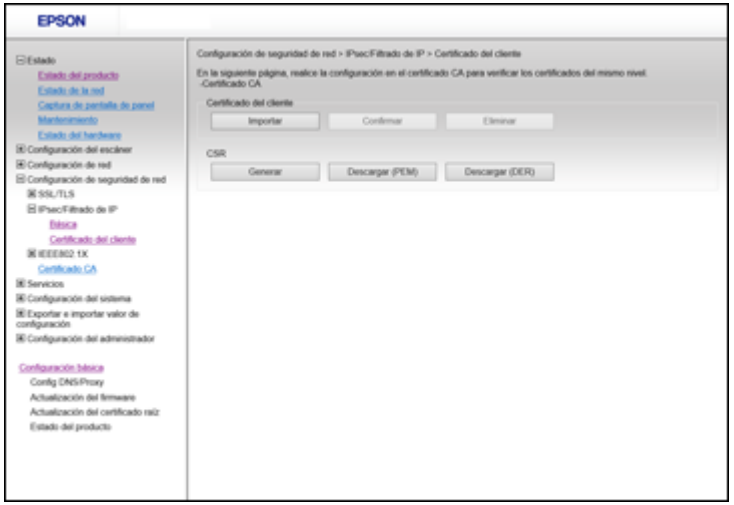
Tema principal: Cómo configurar el protocolo IPsec/Filtrado de IP

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 **Configuración de seguridad de red**.
2. Seleccione **IPsec/Filtrado de IP** y seleccione **Certificado del cliente**.

   Verá una ventana como esta:



3. Realice una de las siguientes acciones:
   - Haga clic en **Importar** para agregar un certificado de cliente nuevo.
   - Seleccione el certificado que desea utilizar como la opción **Copiar desde** y haga clic en **Copiar**.
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 **Servicios**.
2. Seleccione **Protocolo**.

   Verá una ventana como esta:

3. Seleccione la casilla **Activar SNMPv3** para activar los ajustes de SNMPv3.
4. Seleccione los ajustes que desea en la sección Configuración de SNMPv3.
5. Haga clic en **Siguiente**.

   Verá un mensaje de confirmación.
6. 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.
Configuración de autenticación	
Algoritmo	Seleccione el algoritmo para autenticación.

Ajuste	Opciones/Descripción
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

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 **Configuración de seguridad de red**.
2. Seleccione **IEEE802.1X** y seleccione **Básica**.

Verá una ventana como esta:

3. Seleccione **Habilitar** como el ajuste **IEEE802.1X (LAN cableada)**.
4. Seleccione los ajustes de IEEE 802.1X que desea utilizar.
5. Haga clic en **Siguiente**.

   Verá un mensaje de confirmación.
6. 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
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.

Ajuste	Opciones/Descripción
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 **Configuración de seguridad de red**.
2. Seleccione **IEEE802.1X** y seleccione **Certificado del cliente**.

Verá una ventana como esta:

3. Realice una de las siguientes acciones:
   - Haga clic en **Importar** para agregar un certificado de cliente nuevo.
   - Seleccione el certificado que desea utilizar como la opción **Copiar desde** y haga clic en **Copiar**.
4. Haga clic en **Aceptar**.

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
Cómo importar un certificado CA
Cómo eliminar un certificado CA

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 CA
Un certificado CA indica que un tercero ha verificado la identidad de un servidor. Necesita obtener un certificado CA para la autenticación de servidor desde una CA distribuidora.

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.

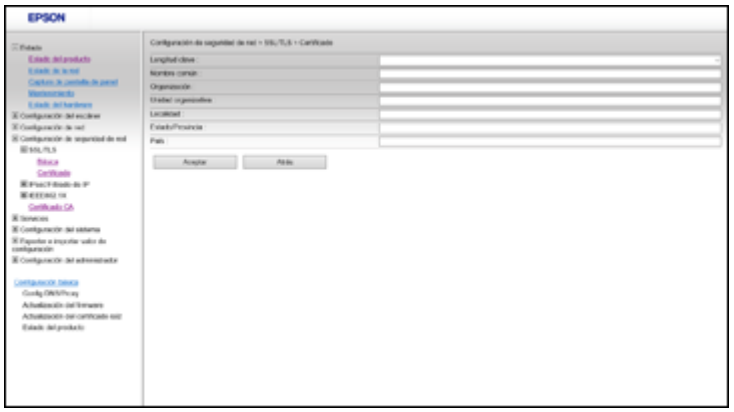
Tema principal: Cómo usar un certificado digital

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 **Configuración de seguridad de red**.
2. Seleccione una de las siguientes opciones de seguridad de red y los certificados correspondientes:
   - **SSL/TLS** y seleccione **Certificado**
   - **IPsec/Filtrado de IP** y seleccione **Certificado del cliente**
   - **IEEE802.1X** y seleccione **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 **Configuración de seguridad de red** y seleccione una de las siguientes opciones de seguridad de red y los certificados correspondientes:
   - **SSL/TLS** y seleccione **Certificado**
   - **IPsec/Filtrado de IP** y seleccione **Certificado del cliente**
   - **IEEE802.1X** y seleccione **Certificado del cliente**
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 **Configuración de seguridad de red** y seleccione una de las siguientes opciones de seguridad de red y los certificados correspondientes:
    - **SSL/TLS** y seleccione **Certificado**
    - **IPsec/Filtrado de IP** y seleccione **Certificado del cliente**
    - **IEEE802.1X** y seleccione **Certificado del cliente**
11. En la sección Certificado 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 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 **Configuración de seguridad de red**.
2. Seleccione una de las siguientes opciones de seguridad de red y el certificado correspondiente:
   - **SSL/TLS** y seleccione **Certificado**
   - **IPsec/Filtrado de IP** y seleccione **Certificado del cliente**
   - **IEEE802.1X** y seleccione **Certificado del cliente**
3. Haga clic en **Eliminar**.

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

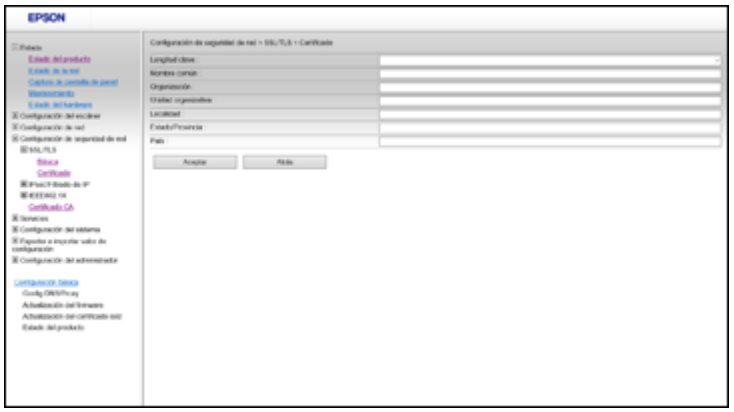
Tema principal: Cómo usar un certificado digital

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 **Configuración de seguridad de red**, seleccione **SSL/TLS** y seleccione **Certificado**.
2. Haga clic en **Actualizar**.

Verá una ventana como esta:



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

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

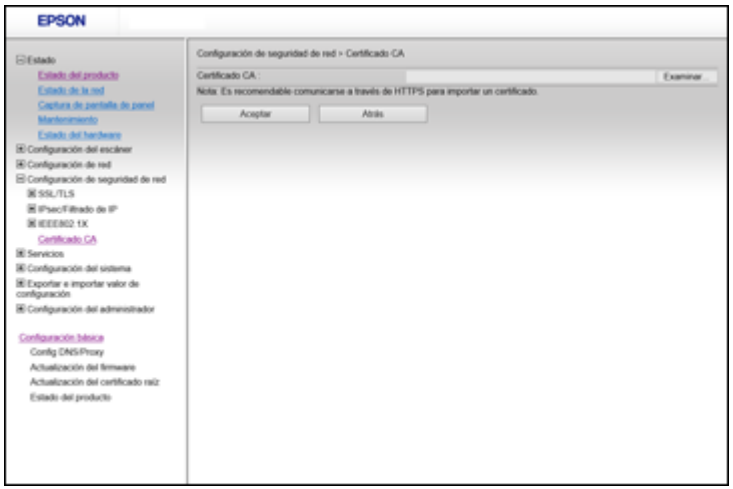
Tema principal: Cómo usar un certificado digital

Cómo importar un certificado CA

Puede importar un certificado CA a través de Web Config.

1. Acceda a Web Config y seleccione **Configuración de seguridad de red**.
2. Seleccione **Certificado CA**.
3. Seleccione **Importar**.

4. Seleccione el certificado CA que desea importar.



5. Haga clic en **Aceptar**.

Cuando ve la página **Certificado CA** y aparece el certificado importado, ha terminado la importación.

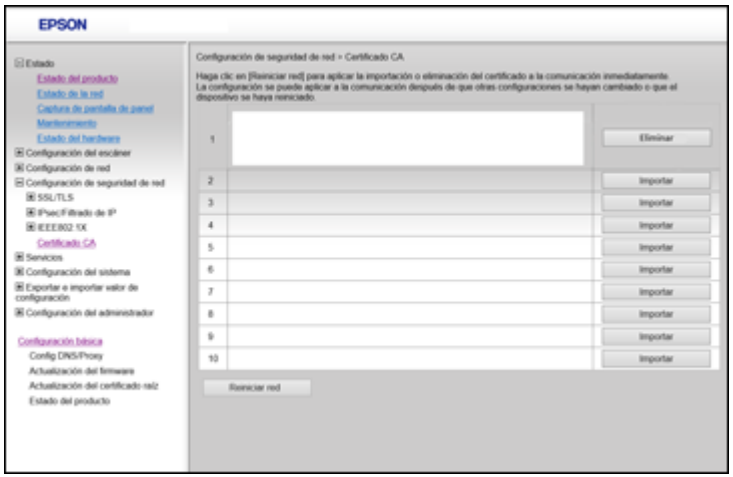
Tema principal: Cómo usar un certificado digital

Cómo eliminar un certificado CA

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

1. Acceda a Web Config y seleccione **Configuración de seguridad de red**.

2. Seleccione **Certificado CA**.



3. Localice el certificado que desea eliminar y haga clic en botón **Eliminar** a un lado.
4. Haga clic en **Aceptar** para confirmar la eliminación.

Tema principal: Cómo usar un certificado digital

Cómo configurar protocolos y servicios en Web Config

Puede activar o desactivar protocolos a través de Web Config.

1. Acceda a Web Config, seleccione **Servicios** y seleccione **Protocolo**.
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**.
6. Seleccione y configure los ajustes de servicios y protocolos, según sea necesario.

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

Puede configurar estos ajustes de protocolo en Web Config.

Protocolos

Nombre	Descripción
Bonjour	Utilice Bonjour para buscar dispositivos y AirPrint.
SLP	Utilice SLP 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.
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.

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 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.

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 y servicios 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

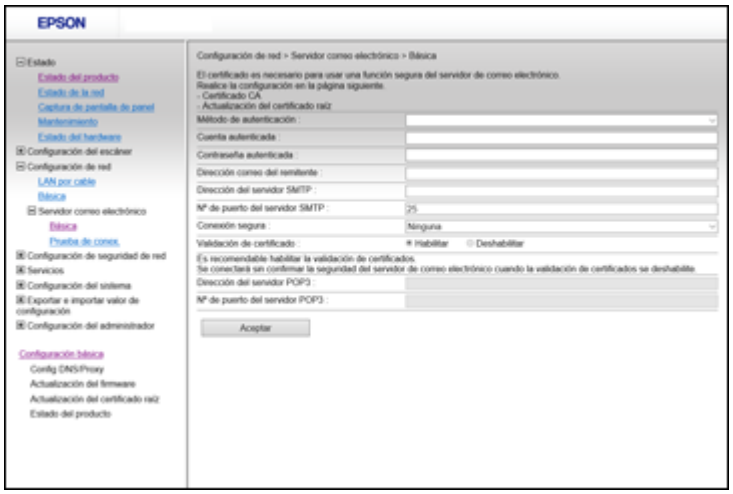
Tema principal: Cómo utilizar su producto en una red segura

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 **Configuración de red**.
2. Seleccione **Servidor correo electrónico** y 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: ( ) < > [ ] ;

Ajuste	Opciones/Descripción
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.
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 ajuste **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 **Configuración de red**.
2. Seleccione **Servidor correo electrónico** y 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 SMTP 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.

Mensaje	Descripción
Método de comunicación no admitido. Compruebe lo siguiente - Dirección del servidor SMTP - Nº de puerto del servidor SMTP. La conexión segura (SSL) no se admite.	El protocolo de comunicación no es admitido.
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 al producto hasta que termine el procesamiento.	El producto está ocupado.

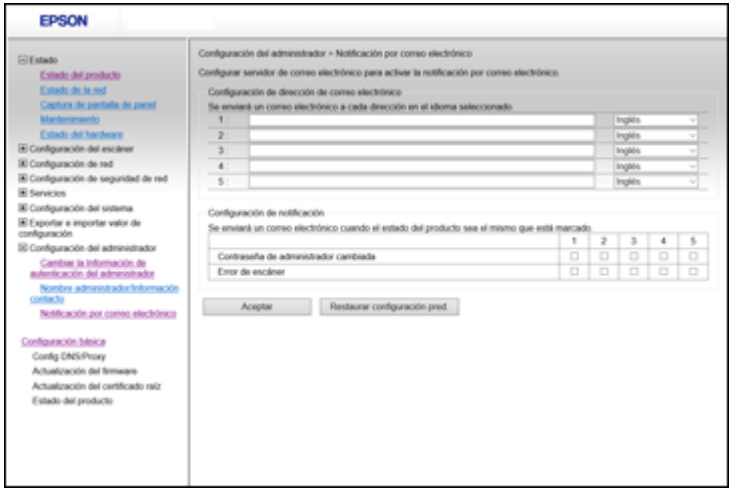
Tema principal: Cómo utilizar un servidor de correo electrónico

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. 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 **Configuración del administrador**.
2. Seleccione **Notificación por correo electrónico**.

   Verá una ventana como esta:



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

Tema principal: Cómo utilizar un servidor de correo electrónico

Cómo importar y exportar los ajustes de Web Config

Siga las instrucciones de las siguientes secciones para importar y exportar los ajustes de su producto utilizando el software Web Config.

Cómo exportar los ajustes utilizando Web Config
Cómo importar los ajustes utilizando Web Config

Tema principal: Cómo utilizar su producto en una red segura

Cómo exportar los ajustes utilizando Web Config

Puede exportar los ajustes de su producto y, si desea, codificar el archivo de los ajustes con una contraseña.

1. Acceda a Web Config y seleccione **Exportar e importar valor de configuración**.
2. Seleccione **Exportar**.
3. Seleccione los ajustes que desea exportar.

   Nota: Si selecciona una categoría principal, también se seleccionan las subcategoriás. Por defecto, no se pueden seleccionar los elementos que son exclusivos a la red, tal como la dirección IP. Si desea exportar estos elementos, seleccione **Habilitar para seleccionar la configuración individual del dispositivo**. Se recomienda solo exportar elementos exclusivos cuando vaya a reemplazar un producto en la red, de lo contrario, podría tener conflictos en la red.

4. Introduzca una contraseña para codificar el archivo, si desea.
5. Haga clic en **Exportar** y guarde el archivo.

Tema principal: Cómo importar y exportar los ajustes de Web Config

Cómo importar los ajustes utilizando Web Config

Puede importar ajustes a su producto que había exportado previamente. Si el archivo de ajustes fue codificado cuando se exportó, obtenga la contraseña necesaria antes de importarlo.

1. Acceda a Web Config y seleccione **Exportar e importar valor de configuración**.
2. Seleccione **Importar**.
3. Haga clic en **Examinar** y seleccione el archivo de ajustes exportado.
4. Si es necesario, introduzca la contraseña de descifrado.
5. Haga clic en **Siguiente**.
6. Seleccione los ajustes que desea importar y haga clic en **Siguiente**.

7. Haga clic en **Aceptar**.

Los ajustes seleccionados se importan al producto.

Tema principal: Cómo importar y exportar los ajustes de Web Config

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 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 y seleccione **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**.

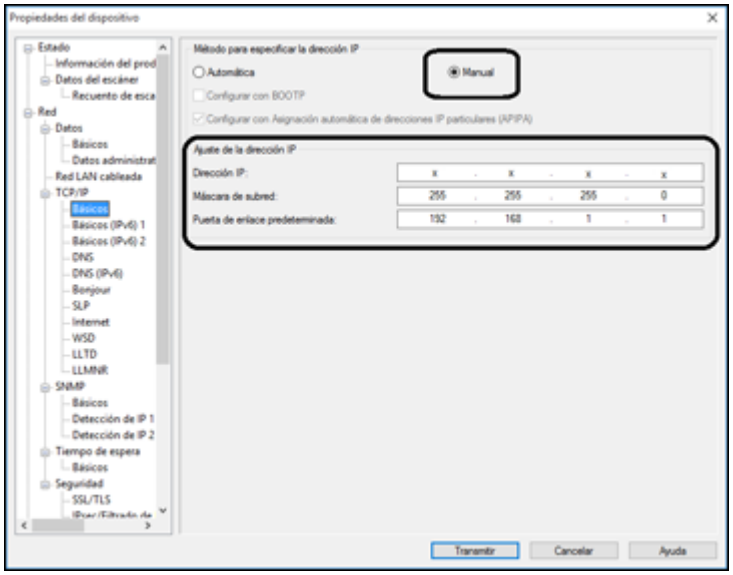
   Después de unos momentos, el programa muestra los productos conectados.

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, seleccione **TCP/IP** y seleccione **Básica**.

   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 **Transmitir**.

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.

Solución de problemas de uso del software de red
Solución de problemas de seguridad de red
Solución de problemas con certificados digitales
Dónde obtener ayuda

Solución de problemas de uso del software de red

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

No puede acceder a Web Config
Aparece el mensaje "Sin actualizar"
Aparece el mensaje "El nombre del certificado de seguridad no coincide"
El nombre del modelo o la dirección IP no aparece en EpsonNet Config

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. 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 y seleccione **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 **On**. 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.

Ha olvidado la clave precompartida
No se puede comunicar con el producto utilizando la comunicación IPsec
La comunicación se interrumpió de repente
No puede establecer una conexión después de configurar el protocolo IPsec/Filtrado de IP
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

Método de seguridad	Algoritmos compatibles
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 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 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	
Chile	(56 2) 2484-3400
Colombia	Bogotá: (57 1) 523-5000 Resto del país: 018000-915235
Costa Rica	800-377-6627
Ecuador*	1-800-000-044
El Salvador*	800-6570
Guatemala*	1-800-835-0358
Honduras**	800-0122 Código NIP: 8320
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.

** Marque los primeros 7 dígitos, espere el mensaje de respuesta y luego ingrese el código NIP.

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.

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

Quedan reservados todos los derechos. Ninguna parte de esta publicación podrá ser reproducida, almacenada en un sistema de recuperación, transmitida bajo ninguna forma por ningún medio, ya sea electrónico, mecánico, de fotocopiado, grabación o cualquier otro, sin el previo consentimiento por escrito de Seiko Epson Corporation. La información contenida en el presente aplica solamente a este producto Epson. Epson no se hace responsable si esta información es utilizada en otros productos.

Ni Seiko Epson Corporation ni sus filiales asumirán responsabilidad ante el comprador de este producto o ante terceros por daños, pérdidas, costos o gastos en que incurrieren los usuarios como consecuencia de: accidente, uso inadecuado o abuso de este producto o modificaciones, reparaciones o alteraciones no autorizadas al mismo, o (excluidos los EE. UU.) por no seguir rigurosamente las instrucciones de operación y mantenimiento de Seiko Epson Corporation.

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

7/17

CPD-54164

Tema principal: Aviso de derechos reservados