EPSON
EXCEED YOUR VISION

DS-790WN

Manual del administrador

NPD6726-00 ES

Copyright

Marcas comerciales

- ❏ EPSON, EPSON EXCEED YOUR VISION, EXCEED YOUR VISION y sus logotipos son marcas comerciales registradas o marcas comerciales de Seiko Epson.
- ❏ Microsoft®, Windows®, and Windows Server® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- ❏ Chrome is a trademark of Google LLC.
- ❏ The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- ❏ Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- ❏ FeliCa y PaSoRi son marcas comerciales registradas de Sony Corporation.
- ❏ MIFARE es una marca registrada de NXP Semiconductor Corporation.
- ❏ Aviso general: otros nombres de otros productos utilizados en esta documentación se citan con el mero fin de su identificación y son marcas comerciales de sus respectivos propietarios. Epson renuncia a cualquier derecho sobre esas marcas.

Índice

Copyright

Marcas comerciales

Introducción

Ajustes necesarios para su objetivo

Configuración de red

Software para configurar el escáner

Ajustes necesarios para el escaneado

Personalización de la pantalla del panel de control

Configuración de seguridad básica

Ajustes de seguridad avanzados

Configuración de autenticación

Mantenimiento

Introducción

Contenido de este documento

Este documento proporciona la siguiente información a los administradores del escáner.

❏ Configuración de red

❏ Preparar la función de escaneado

❏ Habilitar y administrar la configuración de seguridad

❏ Habilitar y administrar Configuración de autenticación

❏ Realizar el mantenimiento diario

Para ver los métodos de uso estándar del escáner, consulte el *Manual de usuario*.

Nota:
Este documento explica la Configuración de autenticación que proporciona una autenticación independiente sin necesidad de usar un servidor de autenticación. Además del Configuración de autenticación que se describe en este manual, también puede crear un sistema de autenticación mediante un servidor de autenticación. Para crear un sistema, use Document Capture Pro Server Authentication Edition (el nombre abreviado es Document Capture Pro Server AE).

Para obtener más información, póngase en contacto con la oficina local de Epson.

Usar este manual

Marcas y símbolos

> ⚠ ***Precaución:***
> *Instrucciones que se deben seguir cuidadosamente para evitar lesiones.*

> ***Importante:***
> *Instrucciones que se deben respetar para evitar daños en el equipo.*

Nota:
Suministra información complementaria y de referencia.

Información relacionada

➡ Enlaces a las secciones relacionadas.

Descripciones utilizadas en este manual

❏ Las capturas de pantalla de las aplicaciones corresponden a Windows 10 o macOS High Sierra. El contenido mostrado en las pantallas varía dependiendo del modelo y situación.

❏ Las ilustraciones usadas en este manual son solo para referencia. Aunque pueden diferir ligeramente del producto real, los métodos de funcionamiento son los mismos.

Referencias del sistema operativo

Windows

En este manual, términos como «Windows 10», «Windows 8.1», «Windows 8», «Windows 7», «Windows Server 2019», «Windows Server 2016», «Windows Server 2012 R2», «Windows Server 2012», y «Windows Server 2008 R2» se refieren a los siguientes sistemas operativos. Además, «Windows» se utiliza para referirse a todas las versiones y «Windows Server» se usa para referirse a «Windows Server 2019», «Windows Server 2016», «Windows Server 2012 R2», «Windows Server 2012» y «Windows Server 2008 R2».

- ❏ Sistema operativo Microsoft® Windows® 10
- ❏ Sistema operativo Microsoft® Windows® 8.1
- ❏ Sistema operativo Microsoft® Windows® 8
- ❏ Sistema operativo Microsoft® Windows® 7
- ❏ Sistema operativo Microsoft® Windows Server® 2019
- ❏ Sistema operativo Microsoft® Windows Server® 2016
- ❏ Sistema operativo Microsoft® Windows Server® 2012 R2
- ❏ Sistema operativo Microsoft® Windows Server® 2012
- ❏ Sistema operativo Microsoft® Windows Server® 2008 R2

Mac OS

En este manual, «Mac OS» se usa para referirse a macOS Big Sur, macOS Catalina, macOS Mojave, macOS High Sierra, macOS Sierra, OS X El Capitan, y OS X Yosemite.

Ajustes necesarios para su objetivo

Ajustes necesarios para su objetivo

Consulte a continuación cómo realizar los ajustes necesarios que se adapten a su objetivo.

Conexión del escáner a la red

Objetivo	Parámetros necesarios
Quiero conectar el escáner a la red.	Configure su escáner para escanear en red. "Conexión del escáner a la red" de la página 14
Quiero conectar el escáner a un nuevo ordenador.	Establece la configuración de red del escáner en el nuevo ordenador. "Añadir o sustituir el ordenador o los dispositivos" de la página 20

Configuración para escanear

Objetivo	Parámetros necesarios
Quiero enviar imágenes escaneadas por correo electrónico. (Dig. a correo electrónico)	1. Configure el servidor de correo electrónico que desea vincular. "Configurar un servidor de correo" de la página 42 2. Registre la dirección de correo electrónico del destinatario en **Contactos** (opcional). Al registrar la dirección de correo electrónico, no es necesario introducirla cada vez que desee enviar algo, solo tiene que seleccionarla en sus Contactos. "Hacer que los contactos estén disponibles" de la página 63
Quiero guardar las imágenes escaneadas en una carpeta de la red. (Digitaliz. a carpeta red/FTP)	1. Cree una carpeta en la red para guardar las imágenes. "Configurar una carpeta de red compartida" de la página 45 2. Registre la ruta a la carpeta en **Contactos** (opcional). Al registrar la ruta de la carpeta, no es necesario introducirla cada vez que desee enviar algo, solo tiene que seleccionarla en sus Contactos. "Hacer que los contactos estén disponibles" de la página 63
Quiero guardar las imágenes escaneadas en un servicio en la nube. (Digitalizar a cloud)	Configuración de Epson Connect. Consulte el sitio web del portal Epson Connect para obtener detalles acerca de la configuración. Necesitará una cuenta de usuario para el servicio de almacenamiento en línea al que crear el vínculo. https://www.epsonconnect.com/ http://www.epsonconnect.eu (sólo para Europa)

Personalización de la pantalla del panel de control

Objetivo	Parámetros necesarios
Quiero cambiar los elementos que se aparecen en el panel de control del escáner.	Seleccione **Ajustes** o **Editar inicio**. Puede registrar su configuración de escaneado favorita en el panel de control y editar los elementos que se muestran. "Personalización de la pantalla del panel de control" de la página 77

Configuración de las funciones de seguridad básicas

Objetivo	Parámetros necesarios
Quiero evitar que nadie que no sea el administrador pueda cambiar la configuración del escáner.	Establezca una contraseña de administrador para el escáner. "Configuración de administrador" de la página 86
Quiero desactivar el uso de escáneres con conexiones USB.	Desactive la interfaz externa. "Deshabilitación de la interfaz externa" de la página 92

Configuración de las funciones de seguridad avanzadas

Objetivo	Parámetros necesarios
Quiero controlar qué protocolos se usan.	Habilite o deshabilite los protocolos. "Control mediante protocolos" de la página 98
Quiero cifrar la ruta de comunicación.	1. Configure su certificado digital. "Modo de uso de un certificado digital" de la página 101 2. Configure la comunicación SSL/TLS. "Comunicación SSL/TLS con la impresora" de la página 106
Quiero usar comunicación cifrada (IPsec). Quiero poder usar el software solo desde un ordenador concreto (filtrado de IP).	Configure las políticas de filtrado del tráfico. "Comunicación cifrada mediante el uso de filtro IPsec/IP" de la página 108
Quiero usar un escáner en una red IEEE802.1X.	Configure IEEE802.1X para el escáner. "Conexión del escáner a una red IEEE802.1X" de la página 120

Configuración de funciones para que sean autenticadas por el escáner

Objetivo	Parámetros necesarios
Quiero habilitar Configuración de autenticación.	Consulte a continuación para obtener más información sobre la Configuración de autenticación y el Método de autenticación disponibles. "Acerca de Configuración de autenticación" de la página 129 "Acerca de Método de autenticación" de la página 130

Uso de un sistema de autenticación de un servidor

Con Document Capture Pro Server Authentication Edition (abreviado como Document Capture Pro Server AE), puede crear un sistema que utilice un servidor para la autenticación.

Para obtener más información, póngase en contacto con la oficina local de Epson.

Configuración de red

Conexión del escáner a la red

En esta sección se explica cómo conectar el escáner a la red utilizando el panel de control del escáner.

Nota:
Si su escáner y su ordenador están en el mismo segmento, también puede conectarlo usando el instalador.

❏ *Instalación desde la página web*

Acceda a la siguiente página web y, a continuación, introduzca el nombre del producto. Vaya a ***Configuración*** *y comience la configuración.*

http://epson.sn

❏ *Instalación a través del disco de software (solo para los modelos que vienen con un disco de software y para los usuarios con ordenadores Windows con lector de discos).*

Inserte el disco de software en el ordenador y, a continuación, siga las instrucciones que aparecen en la pantalla.

Antes de realizar la conexión a la red

Antes de realizar la conexión a la red, compruebe el método de conexión y la información de configuración para la conexión.

Acopio de información sobre la configuración de conexión

Prepare la información de configuración necesaria para la conexión. Compruebe la siguiente información de antemano.

Divisiones	Elementos	Nota
Método de conexión de dispositivos	❏ Ethernet ❏ Wi-Fi	Decida cómo conectar el escáner a la red. Para conexiones por cable LAN, conéctela al interruptor LAN. Para conexiones Wi-Fi, conéctela a la red (SSID) del punto de acceso.
Información de conexión LAN	❏ Dirección IP ❏ Máscara de subred ❏ Puerta enlace predeterminada	Decida la dirección IP que quiere asignar al escáner. Si asigna una dirección IP estática, necesitará todos los valores. Si asigna una dirección IP dinámica utilizando la función DHCP, no necesitará esta información porque se configurará de forma automática.
Información de conexión Wi-Fi	❏ SSID ❏ Contraseña	Por un lado está el SSID (nombre de la red) y por otro la contraseña del punto de acceso al que se conecta el escáner. Si se ha configurado el filtrado de direcciones MAC, registre la dirección MAC del escáner antes de registrar este. Consulte a continuación los estándares admitidos. "Especificaciones de la red" de la página 28
Información de servidor DNS	❏ Dirección IP para DNS primario ❏ Dirección IP para DNS secundario	Estos son necesarios para especificar servidores DNS. El DNS secundario se configura cuando el sistema tiene una configuración redundante y hay un servidor DNS secundario. Si forma parte de una organización pequeña en la que no se configura el servidor DNS, configure la dirección IP del router.

Divisiones	Elementos	Nota
Información de servidor proxy	❏ Nombre de servidor proxy	Configure estas funciones cuando su entorno de red utilice el servidor proxy para acceder a Internet desde la Intranet y esté habilitada la función que permite que el escáner se conecte directamente a Internet. Para las siguientes funciones, el escáner se conecta directamente a Internet. ❏ Servicios de Epson Connect ❏ Servicios en la nube de otras empresas ❏ Actualizaciones de firmware ❏ Envío de imágenes escaneadas a SharePoint (WebDAV)
Información de número de puerto	❏ Liberación de número de puerto	Compruebe el número de puerto que utilizan el escáner y el ordenador y, a continuación, libere el puerto bloqueado por el cortafuegos, si es necesario. Consulte lo siguiente para ver el número de puerto utilizado por el escáner. "Uso del puerto del escáner" de la página 30

Asignación de dirección IP

Estos son los distintos tipos de asignación de dirección IP.

Dirección IP fija:

Asigne la dirección IP predeterminada al escáner (host) de forma manual.

La información de conexión a la red (máscara de subred, puerta de enlace predeterminada, servidor DNS, etc.) debe configurarse manualmente.

La dirección IP no cambia ni aunque se apague el dispositivo, así que esto puede serle útil cuando quiera administrar dispositivos en un entorno en que no sea posible cambiar la dirección IP o cuando quiera administrar dispositivos utilizando la dirección IP. Esta configuración es recomendable para el escáner, el servidor y otros dispositivos a los que puede acceder mucha gente. Además, asigne una dirección IP fija cuando utilice funciones de seguridad como el filtrado IPsec/IP para evitar que cambie la IP.

Asignación automática con la función DHCP (dirección IP dinámica):

Asigne la dirección IP al escáner (host) de forma automática con la función DHCP del servidor DHCP o router.

La información de conexión a la red (máscara de subred, puerta de enlace predeterminada, servidor DNS, etc.) se configura de forma automática, por lo que puede conectar el dispositivo a la red fácilmente.

Puede que la dirección IP cambie si se apagan el dispositivo o el router y se vuelven a conectar, o dependiendo de la configuración del servidor DHCP.

Es recomendable administrar los dispositivos que no sean la dirección IP y comunicarse con protocolos que puedan seguir la dirección IP.

Nota:
Si utiliza la función de reserva de dirección IP del DHCP, puede asignar la misma dirección IP a los dispositivos en cualquier momento.

Servidor DNS y servidor proxy

El servidor DNS tiene un nombre de host, un nombre de dominio de la dirección de correo electrónico, etc. asociados a la información de la dirección IP.

La comunicación es imposible si se ha definido el nombre de host, nombre de dominio, etc. de la otra parte cuando el ordenador o el escáner lleva a cabo la comunicación IP.

Consulte dicha información del servidor DNS y obtenga la dirección IP de la otra parte. Este proceso se denomina resolución de nombres.

De este modo podrán comunicarse los ordenadores y escáneres utilizando la dirección IP.

La resolución de nombres es necesaria para que pueda comunicarse el escáner por medio de la función de correo electrónico o de conexión a Internet.

Si utiliza dichas funciones, efectúe la configuración del servidor DNS.

Si asigna la dirección IP del escáner a través de la función DHCP del router o el servidor DHCP, se configurará automáticamente.

El servidor proxy se ubica en la puerta de enlace entre la red e Internet y se comunica con el ordenador, el escáner e Internet (servidor opuesto) en nombre de cada uno. El servidor opuesto se comunica solo con el servidor proxy. Por lo tanto, la información del escáner tal como la dirección IP y el número de puerto no se pueden leer y se espera mayor seguridad.

Cuando se conecte a Internet a través de un servidor proxy, configure el servidor proxy en el escáner.

Conexión a la red desde el panel de control

Conecte el escáner a la red mediante el panel de control del escáner.

Asignación de la dirección IP

Configure los elementos básicos, como la dirección del host, Máscara de subred, Puerta enlace predet..

En esta sección se explica el procedimiento para configurar una dirección IP estática.

1. Encienda el escáner.
2. Seleccione **Configuración** en la pantalla de inicio del panel de control del escáner.
3. Seleccione **Configuración de red** > **Avanzado** > **TCP/IP**.
4. Seleccione **Manual** para **Obtener dirección IP**.

   Si configure la dirección IP automáticamente mediante la función DHCP del router, seleccione **Automático**. En este caso, **Dirección IP**, **Máscara de subred** y **Puerta enlace predet.** en los pasos 5 a 6 también se configuran automáticamente, así que vaya al paso 7.
5. Introduzca la dirección IP.

   Si seleccionó ◀ y ▶ el foco pasa al segmento delantero o al segmento trasero separados por un punto.

   Confirme el valor reflejado en la pantalla anterior.

6. Configure **Máscara de subred** y **Puerta enlace predet.**.

   Confirme el valor reflejado en la pantalla anterior.

   > ***Importante:***
   > *Si la combinación de Dirección IP, Máscara de subred y Puerta enlace predet. es incorrecta,* ***Iniciar configuración*** *estará inactivo y no podrá continuar con la configuración. Confirme que lo introducido es correcto.*

7. Introduzca la dirección IP para el servidor DNS principal.

   Confirme el valor reflejado en la pantalla anterior.

   Nota:
   Si selecciona ***Automático*** *para los ajustes de asignación de la dirección IP, podrá seleccionar los ajustes del servidor DNS en* ***Manual*** *o* ***Automático****. Si no puede obtener la dirección del servidor DNS automáticamente, seleccione* ***Manual*** *e introduzca la dirección del servidor DNS. A continuación, introduzca directamente la dirección del servidor DNS secundario. Si selecciona* ***Automático****, vaya al paso 9.*

8. Introduzca la dirección IP para el servidor DNS secundario.

   Confirme el valor reflejado en la pantalla anterior.

9. Toque **Iniciar configuración**.

Configuración de servidor proxy

Configure el servidor proxy si se cumplen las dos condiciones siguientes.

❏ El servidor proxy está pensado para la conexión a Internet.

❏ Si se utiliza una función en la que el escáner se conecta directamente a Internet, como el servicio Epson Connect o los servicios en la nube de otra empresa.

1. Seleccione **Configuración** en la pantalla de inicio.

   Si realiza ajustes después configurar la dirección IP, se muestra la pantalla **Avanzado**. Vaya al paso 3.

2. Seleccione **Configuración de red** > **Avanzado**.

3. Seleccione **Servidor proxy**.

4. Seleccione **Uso** para **Config. servidor proxy**.

5. Escriba la dirección del servidor proxy en formato IPv4 o FQDN.

   Confirme el valor reflejado en la pantalla anterior.

6. Escriba el número de puerto del servidor proxy.

   Confirme el valor reflejado en la pantalla anterior.

7. Toque **Iniciar configuración**.

Conexión a Ethernet

Conecte el escáner a la red mediante un cable LAN y luego compruebe la conexión.

1. Conecte el escáner y el concentrador (conmutador LAN) a mediante un cable LAN.
2. Seleccione  en la pantalla de inicio.
3. Seleccione **Enrutador**.
4. Asegúrese de que los ajustes de Conexión y Dirección IP sean correctos.
5. Toque **Cerrar**.

Conexión a la LAN inalámbrica (Wi-Fi)

El escáner se puede conectar a la LAN inalámbrica (Wi-Fi) de diferentes maneras. Elija el modo de conexión que se adecue al entorno y las condiciones que esté utilizando.

Si conoce la información respectiva al router inalámbrico como el SSID y la contraseña, puede realizar los ajustes manualmente.

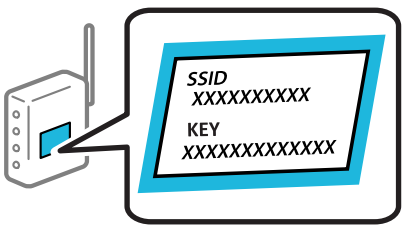
Si el router inalámbrico admite la funcionalidad WPS, puede realizar los ajustes mediante configuración por botón de comando.

Tras conectar el escáner a la red, conéctese al escáner desde el dispositivo que quiera usar (ordenador, dispositivo inteligente, tablet y demás dispositivos).

Configurar la Wi-Fi introduciendo el SSID y la contraseña

Puede configurar una red Wi-Fi introduciendo los datos necesarios para conectarse a un router inalámbrico desde el panel de control del escáner. Para configurar con este método, necesita el SSID y la contraseña del router inalámbrico.

Nota:
Si utiliza el router inalámbrico con su configuración predeterminada, utilice el SSID y la contraseña escritos en la etiqueta. Si no conoce el SSID ni la contraseña, consulte a la persona que configuró el router inalámbrico o la documentación que acompaña a este.



1. En la pantalla de inicio, pulse  .
2. Seleccione **Enrutador**.

3. Toque **Iniciar configuración**.

   Si la conexión de red ya está configurada, se muestran los detalles de la misma. Pulse **Cambie a la conexión Wi-Fi.** o **Cambiar configuración** para cambiar la configuración.

4. Seleccione **Asistente para la instalación de Wi-Fi**.

5. Siga las instrucciones en pantalla para seleccionar el SSID, introduzca la contraseña del router inalámbrico e inicie la configuración.

   Si desea comprobar el estado de la conexión de red del escáner una vez finalizada la configuración, consulte el siguiente enlace de información relacionada para ver los detalles.

   Nota:
   - ❏ *Si no conoce el SSID, compruebe si figura en la etiqueta del router inalámbrico. Si utiliza el router inalámbrico con su configuración predeterminada, escriba el SSID que figura en la etiqueta. Si no puede encontrar ninguna información, consulte la documentación proporcionada con el router inalámbrico.*
   - ❏ *La contraseña distingue entre mayúsculas y minúsculas.*
   - ❏ *Si no conoce la contraseña, compruebe si los datos se encuentran en la etiqueta del router inalámbrico. En la etiqueta, la contraseña puede denominarse «Network Key», «Wireless Password», o algo similar. Si utiliza el router inalámbrico con su configuración predeterminada, escriba la contraseña que figura en la etiqueta.*

Información relacionada

➡ "Comprobación del estado de conexión a la red" de la página 26

Configuración del Wi-Fi mediante configuración por botón de comando (WPS)

Puede configurar automáticamente una red Wi-Fi pulsando un botón del router inalámbrico. Si se dan las condiciones siguientes, puede configurar usando este método.

- ❏ El router inalámbrico es compatible con WPS (Wi-Fi Protected Setup).
- ❏ La conexión Wi-Fi actual se estableció pulsando un botón del router inalámbrico.

Nota:
Si no encuentra el botón o la está configurando con el software, consulte el manual del router inalámbrico.

1. En la pantalla de inicio, pulse  .

2. Seleccione **Enrutador**.

3. Toque **Iniciar configuración**.

   Si la conexión de red ya está configurada, se muestran los detalles de la misma. Pulse **Cambie a la conexión Wi-Fi.** o **Cambiar configuración** para cambiar la configuración.

4. Seleccione **Configuración de pulsador (WPS)**.

5. Siga los pasos indicados en la pantalla.

   Si desea comprobar el estado de la conexión de red del escáner una vez finalizada la configuración, consulte el siguiente enlace de información relacionada para ver los detalles.

   Nota:
   Si no se logra conectar, reinicie el router inalámbrico, acérquelo al escáner y vuelva a intentarlo.

Información relacionada

➡ "Comprobación del estado de conexión a la red" de la página 26

Configuración del Wi-Fi estableciendo un código PIN (WPS)

Puede conectarse automáticamente a un router inalámbrico utilizando un código PIN. Con este método, puede configurar si un router inalámbrico está capacitado para la WPS (configuración protegida de Wi-Fi). Utilice un ordenador para introducir un código PIN en el router inalámbrico.

1. En la pantalla de inicio, pulse  .
2. Seleccione **Enrutador**.
3. Toque **Iniciar configuración**.

   Si la conexión de red ya está configurada, se muestran los detalles de la misma. Pulse **Cambie a la conexión Wi-Fi.** o **Cambiar configuración** para cambiar la configuración.
4. Seleccione **Otros** > **Conf. código PIN (WPS)**
5. Siga los pasos indicados en la pantalla.

   Si desea comprobar el estado de la conexión de red del escáner una vez finalizada la configuración, consulte el siguiente enlace de información relacionada para ver los detalles.

   Nota:
   En el manual que acompaña a su router inalámbrico encontrará las instrucciones para introducir un código PIN.

Información relacionada

➡ "Comprobación del estado de conexión a la red" de la página 26

Añadir o sustituir el ordenador o los dispositivos

Conexión a un escáner conectado a la red

Si el escáner ya se ha conectado a la red, puede conectarle un ordenador o un dispositivo inteligente a través de la red.

Uso de un escáner de red desde un segundo ordenador

Se recomienda el uso del instalador para conectar el escáner a un ordenador. Puede ejecutar el instalador usando uno de los métodos siguientes.

❏ Instalación desde la página web

Acceda a la siguiente página web y, a continuación, introduzca el nombre del producto. Vaya a **Configuración** y comience la configuración.

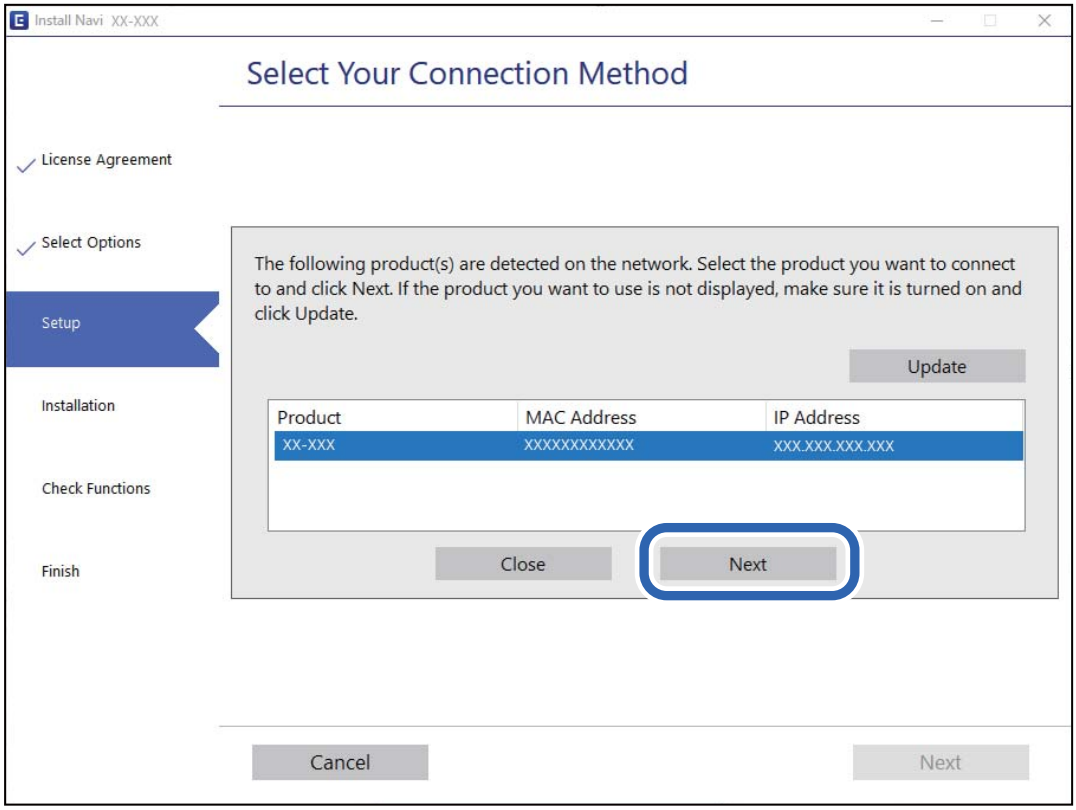
http://epson.sn

❏ Instalación a través del disco de software (solo para los modelos que vienen con un disco de software y para los usuarios con ordenadores Windows con lector de discos).

Inserte el disco de software en el ordenador y, a continuación, siga las instrucciones que aparecen en la pantalla.

Selección del escáner

Siga las instrucciones que aparecen en la pantalla hasta que se muestra la pantalla siguiente, seleccione el nombre del escáner al que desea conectarse y, a continuación, haga clic en **Siguiente**.



Siga los pasos indicados en la pantalla.

Uso de un escáner de red desde un dispositivo inteligente

Puede conectar un dispositivo inteligente al escáner mediante uno de los métodos siguientes.

Conexión a través de un router inalámbrico

Conecte el dispositivo inteligente a la misma red Wi-Fi (SSID) que el escáner.

Para obtener más información, consulte la siguiente sección.

"Configuración de ajustes para la conexión al dispositivo inteligente" de la página 25

Conexión mediante Wi-Fi Direct

Conecte directamente el dispositivo inteligente al escáner sin usar el router inalámbrico.

Para obtener más información, consulte la siguiente sección.

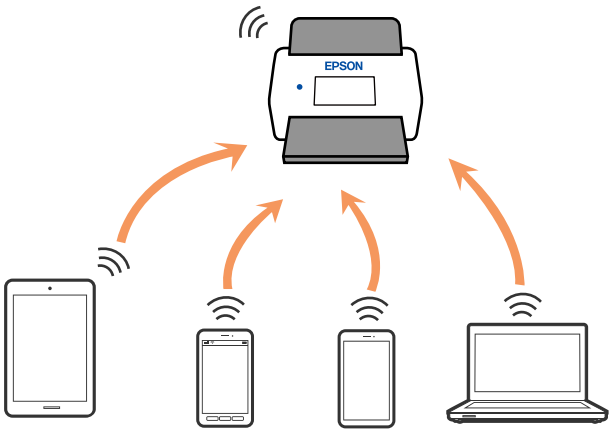
"Conexión directa de un dispositivo inteligente y un escáner (Wi-Fi Direct)" de la página 22

Conexión directa de un dispositivo inteligente y un escáner (Wi-Fi Direct)

Wi-Fi Direct (PA simple) le permite conectar un dispositivo inteligente directamente el escáner sin un router inalámbrico y escanear desde el dispositivo inteligente.

Acerca de Wi-Fi Direct

Siga este método de conexión si no utiliza la red Wi-Fi de casa o de la oficina, o cuando quiera conectar el escáner directamente al ordenador o dispositivo inteligente. Con este modo de conexión, el escáner actúa como router inalámbrico y puede conectar los dispositivos al escáner sin usar un router inalámbrico estándar. Sin embargo, los dispositivos conectados directamente al escáner no pueden comunicarse entre ellos a través del escáner.



El escáner puede conectarse por Wi-Fi o por Ethernet, y por conexión Wi-Fi Direct (PA simple) simultáneamente. No obstante, si inicia una conexión de red mediante Wi-Fi Direct (PA simple) cuando el escáner está conectado por Wi-Fi, la red Wi-Fi se desconectará temporalmente.

Conexión a un dispositivo inteligente con Wi-Fi Direct

Con este método, puede conectar el escáner directamente a dispositivos inteligentes sin usar ningún router inalámbrico.

1. Seleccione  en la pantalla de inicio.
2. Seleccione **Wi-Fi Direct**.
3. Seleccione **Iniciar configuración**.
4. Inicie Epson Smart Panel en su dispositivo inteligente.
5. Siga las instrucciones mostradas en Epson Smart Panel para conectarse al escáner.

   Cuando su dispositivo inteligente se conecte al escáner, vaya al paso siguiente.
6. En el panel de control del escáner, seleccione **Completo**.

Desconexión de la conexión Wi-Fi Direct (PA simple)

Hay dos métodos disponibles para desactivar una conexión Wi-Fi Direct (PA simple); puede desactivar todas las conexiones usando el panel de control del escáner, o desactivar cada una de ellas desde el ordenador o el dispositivo inteligente.

Si desea deshabilitar todas las conexiones, seleccione  > **Wi-Fi Direct** > **Iniciar configuración** > **Cambiar** > **Deshabilitar Wi-Fi Direct**.

Importante:

Al desactivar la conexión Wi-Fi Direct (PA simple), todos los ordenadores y dispositivos inteligentes conectados a la escáner mediante Wi-Fi Direct (PA simple) se desconectan.

Nota:

Si quiere desconectar un dispositivo en concreto, tiene que hacerlo desde el dispositivo y no desde el escáner. Siga uno de estos métodos para desconectar la conexión de Wi-Fi Direct (PA simple) desde el dispositivo.

❏ *Desconecte la conexión Wi-Fi del nombre de red del escáner (SSID).*

❏ *Conéctese a otro nombre de red (SSID).*

Cambio de ajustes de Wi-Fi Direct (PA simple), como el SSID

Si está habilitada la conexión Wi-Fi Direct (PA simple), puede modificar la configuración en  > **Wi-Fi Direct** > **Iniciar configuración** > **Cambiar** y, a continuación, se mostrarán las siguientes opciones de menú.

Cambiar nombre de red

Cambie el nombre de red (SSID) de Wi-Fi Direct (PA simple) utilizado para conectar el escáner a su nombre arbitrario. Puede establecer en nombre de la red (SSID) utilizando los caracteres ASCII que se muestran en el teclado del software del panel de control. Puede introducir hasta 22 caracteres.

Al cambiar el nombre de la red (SSID), todos los dispositivos conectados se desconectan. Emplee el nuevo nombre de red (SSID) si desea volver a conectar el dispositivo.

Cambiar contraseña

Cambie la contraseña de Wi-Fi Direct (PA simple) para la conexión del escáner con los valores que desee. Puede crear la contraseña utilizando los caracteres ASCII que se muestran en el teclado del software del panel de control. Puede introducir de 8 a 22 caracteres.

Cuando cambie la contraseña, se desconectarán todos los dispositivos conectados. Emplee la nueva contraseña si desea volver a conectar el o los dispositivos.

Cambiar rango de frecuencia

Cambie el intervalo de frecuencias de Wi-Fi Direct que se utiliza para conectarse al escáner. Puede seleccionar 2,4 GHz o 5 GHz.

Al cambiar el intervalo de frecuencias, todos los dispositivos conectados se desconectarán. Vuelva a conectar el dispositivo.

Tenga en cuenta que, al cambiar a 5 GHz, no podrá volver a conectarse desde dispositivos que no sean compatibles con el intervalo de frecuencias de 5 GHz.

En algunas regiones puede que este ajuste no se muestre.

Deshabilitar Wi-Fi Direct

Desactive la configuración de Wi-Fi Direct (PA simple) del escáner. Al deshabilitarla, todos los dispositivos conectados al escáner a través de Wi-Fi Direct (PA simple) se desconectarán.

Restaurar configuración pred.

Recupere todos los valores por defecto de los ajustes de Wi-Fi Direct (PA simple).

La información de la conexión Wi-Fi Direct (PA simple) del dispositivo conectado al escáner se elimina.

Nota:
*También puede configurar los siguientes ajustes en la pestaña **Red** > **Wi-Fi Direct** en Web Config.*

- ❏ *Habilitar o deshabilitar Wi-Fi Direct (PA simple)*
- ❏ *Cambio del nombre de la red (SSID)*
- ❏ *Cambiar contraseña*
- ❏ *Modificación del intervalo de frecuencias*

  En algunas regiones puede que este ajuste no se muestre.
- ❏ *Restauración de la configuración de Wi-Fi Direct (PA simple)*

Restablecer la conexión de red

Esta sección explica cómo realizar la configuración de la conexión de red y cambiar el método de conexión cuando se cambian el router inalámbrico o el ordenador.

Al cambiar el router inalámbrico

Cuando cambie de router inalámbrico, configure la conexión entre el ordenador o el dispositivo inteligente y el escáner.

Si cambia de proveedor de servicios de Internet, etc., es necesario realizar estos ajustes.

Configuración de ajustes para la conexión al ordenador

Se recomienda el uso del instalador para conectar el escáner a un ordenador. Puede ejecutar el instalador usando uno de los métodos siguientes.

- ❏ Instalación desde la página web

  Acceda a la siguiente página web y, a continuación, introduzca el nombre del producto. Vaya a **Configuración** y comience la configuración.

  http://epson.sn
- ❏ Instalación a través del disco de software (solo para los modelos que vienen con un disco de software y para los usuarios con ordenadores Windows con lector de discos).

  Inserte el disco de software en el ordenador y, a continuación, siga las instrucciones que aparecen en la pantalla.

Seleccionar el modo de conexión

Siga los pasos indicados en la pantalla. En la pantalla **Seleccione su operación**, seleccione **Vuelva a configurar la conexión de su Impresora (para un nuevo enrutador de red o cambiar USB a la red, etc.)** y, a continuación, haga clic en **Siguiente**.

Siga las instrucciones en pantalla para finalizar la configuración.

Si no puede conectarse, consulte lo siguiente para tratar de resolver el problema.

"No se puede conectar a una red" de la página 31

Configuración de ajustes para la conexión al dispositivo inteligente

Puede usar el escáner desde un dispositivo inteligente cuando conecte el escáner a la misma red Wi-Fi (SSID) que el dispositivo inteligente. Para usar el escáner desde un dispositivo inteligente, vaya al siguiente sitio web e introduzca el nombre del producto. Vaya a **Configuración** y comience la configuración.

http://epson.sn

Acceda a la página web desde el dispositivo inteligente que desee conectar al escáner.

Al cambiar el ordenador

Cuando cambie el ordenador, configure la conexión entre este y el escáner.

Configuración de ajustes para la conexión al ordenador

Se recomienda el uso del instalador para conectar el escáner a un ordenador. Puede ejecutar el instalador utilizando el siguiente método.

❏ Instalación desde la página web

Acceda a la siguiente página web y, a continuación, introduzca el nombre del producto. Vaya a **Configuración** y comience la configuración.

http://epson.sn

❏ Instalación a través del disco de software (solo para los modelos que vienen con un disco de software y para los usuarios con ordenadores Windows con lector de discos).

Inserte el disco de software en el ordenador y, a continuación, siga las instrucciones que aparecen en la pantalla.

Siga los pasos indicados en la pantalla.

Cambiar el método de conexión al ordenador

Esta sección explica cómo cambiar el método de conexión cuando el ordenador y el escáner están conectados.

Cambio de la conexión de red de Ethernet a Wi-Fi

Cambie de la conexión Ethernet a Wi-Fi desde el panel de control del escáner. El método de cambio de conexión es básicamente el mismo que para configurar la conexión Wi-Fi.

Información relacionada

➡ "Conexión a la LAN inalámbrica (Wi-Fi)" de la página 18

Cambio de la conexión de red de Wi-Fi a Ethernet

Siga estos pasos para cambiar de una conexión Wi-Fi a una conexión Ethernet.

1. Seleccione **Configuración** en la pantalla de inicio.

2. Seleccione **Configuración de red** > **Configuración LAN cableada**.

3. Siga los pasos indicados en la pantalla.

Cambio de USB a una conexión de red

Uso del instalador y reconfiguración de un modo diferente de conexión.

❏ Instalación desde la página web

Acceda a la siguiente página web y, a continuación, introduzca el nombre del producto. Vaya a **Configuración** y comience la configuración.

http://epson.sn

❏ Instalación a través del disco de software (solo para los modelos que vienen con un disco de software y para los usuarios con ordenadores Windows con lector de discos).

Inserte el disco de software en el ordenador y, a continuación, siga las instrucciones que aparecen en la pantalla.

Selección de otro modo de conexión

Siga los pasos indicados en la pantalla. En la pantalla **Seleccione su operación**, seleccione **Vuelva a configurar la conexión de su Impresora (para un nuevo enrutador de red o cambiar USB a la red, etc.)** y, a continuación, haga clic en **Siguiente**.

Seleccione la conexión de red que desee utilizar, **Conectar a través de la red inalámbrica (Wi-Fi)** o **Conectar a través de LAN cableada (Ethernet)**, y, a continuación, haga clic en **Siguiente**.

Siga las instrucciones en pantalla para finalizar la configuración.

Comprobación del estado de conexión a la red

Puede comprobar el estado de conexión de red de la siguiente forma.

Comprobación del estado de la conexión de red desde el panel de control

Puede comprobar el estado de la conexión de red utilizando el icono de red o la información de la red del panel de control del escáner.

Comprobación del estado de la conexión de red mediante el icono de red

Para conocer el estado de la conexión a la red y la potencia de la onda de radio, fíjese en el icono de la red que hay en la pantalla de inicio del escáner.

	Muestra el estado de la conexión de red. Seleccione el icono para comprobar la configuración actual y cambiarla. Este es un acceso directo al siguiente menú. **Configuración** > **Configuración de red** > **Config. Wi-Fi**	
		El escáner no está conectado a una red inalámbrica (Wi-Fi).
		El escáner está buscando el SSID, direcciones IP sin establecer o está teniendo problemas con una conexión inalámbrica (Wi-Fi).
		El escáner está conectado a una red inalámbrica (Wi-Fi). El número de barras indica la intensidad de la señal de conexión. Cuantas más barras hay, más intensa es la señal de conexión.
		El escáner no está conectado a una red inalámbrica (Wi-Fi) en el modo Wi-Fi Direct (PA simple).
		El escáner está conectado a una red inalámbrica (Wi-Fi) en el modo Wi-Fi Direct (PA simple).
		La escáner no está conectada a una red cableada (Ethernet) o no está configurada.
		La escáner está conectada a una red cableada (Ethernet).

Ver información detallada de la red en el panel de control

Cuando su escáner esté conectada a la red, también puede ver otros datos relacionados con la red seleccionando los menús de red que quiera consultar.

1. Seleccione **Configuración** en la pantalla de inicio.
2. Seleccione **Configuración de red** > **Estado de la red**.
3. Si quiere consultar la información, seleccione los menús que quiera consultar.
   - ❏ Estado de LAN cabl./Wi-Fi

     Muestra la información de red (nombre del dispositivo, conexión, potencia de la señal, etc.) en conexiones Wi-Fi o Ethernet.
   - ❏ Estado de Wi-Fi Direct

     Muestra la contraseña SSID, si la conexión Wi-Fi Direct está habilitada o deshabilitada, etc. en conexiones Wi-Fi Direct.
   - ❏ Est. serv. correo elec.

     Muestra la información de red de los servidores de correo electrónico.

Especificaciones de la red

Especificaciones Wi-Fi

Consulte en la siguiente tabla las especificaciones Wi-Fi.

Países o regiones, excepto los que se enumeran a continuación	Tabla A
Australia Nueva Zelanda Taiwán Corea del Sur	Tabla B

Tabla A

Estándares	IEEE 802.11b/g/n*1
Intervalo de frecuencia	2,4 GHz
Máxima potencia de radiofrecuencia transmitida	2400–2483,5 MHz: 20 dBm (EIRP)
Canales	1/2/3/4/5/6/7/8/9/10/11/12/13
Modos de conexión	Infraestructura, Wi-Fi Direct (PA simple)*2*3
Protocolos de seguridad*4	WEP (64/128bit), WPA2-PSK (AES)*5, WPA3-SAE (AES), WPA2/WPA3-Enterprise

*1 Solo disponible para HT20.

*2 No es compatible con IEEE 802.11b.

*3 Los modos de Infraestructura y Wi-Fi Direct o una conexión Ethernet se pueden utilizar simultáneamente.

*4 Wi-Fi Direct solo admite WPA2-PSK (AES).

*5 Cumple normas WPA2 y admite WPA/WPA2 Personal.

Tabla B

Estándares	IEEE 802.11a/b/g/n*1/ac
Intervalos de frecuencias	IEEE 802.11b/g/n: 2,4 GHz, IEEE 802.11a/n/ac: 5 GHz

Canales	Wi-Fi	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12*2/13*2
		5 GHz*3	W52 (36/40/44/48), W53 (52/56/60/64), W56 (100/104/108/112/116/120/124/128/132/136/140/144), W58 (149/153/157/161/165)
	Wi-Fi Direct	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12*2/13*2
		5 GHz*3	W52 (36/40/44/48) W58 (149/153/157/161/165)
Modos de conexión	Infraestructura, Wi-Fi Direct (PA simple)*4, *5		
Protocolos de seguridad*6	WEP (64/128bit), WPA2-PSK (AES)*7, WPA3-SAE (AES), WPA2/WPA3-Enterprise		

*1 Solo disponible para HT20.

*2 No disponible en Taiwán.

*3 La disponibilidad de estos canales y el uso del producto en exteriores en estos canales varía según la ubicación. Para obtener más información, consulte http://support.epson.net/wifi5ghz/.

*4 No es compatible con IEEE 802.11b.

*5 Los modos de Infraestructura y Wi-Fi Direct o una conexión Ethernet se pueden utilizar simultáneamente.

*6 Wi-Fi Direct solo admite WPA2-PSK (AES).

*7 Cumple normas WPA2 y admite WPA/WPA2 Personal.

Especificaciones de Ethernet

Estándares	IEEE802.3i (10BASE-T)*1 IEEE802.3u (100BASE-TX)*1 IEEE802.3ab (1000BASE-T)*1 IEEE802.3az (Energy Efficient Ethernet)*2
Modo de comunicación	Automático, 10 Mbps dúplex, 10 Mbps semidúplex, 100 Mbps dúplex, 100 Mbps semidúplex
Conector	RJ-45

*1 Utilice un cable STP (Shielded twisted pair) de categoría 5e o superior para evitar el riesgo de interferencias de radio.

*2 El dispositivo conectado debe cumplir con los estándares IEEE802.3az.

Funciones de red y tabla de IPv4/IPv6

Funciones	Compatibles
Epson Scan 2	IPv4, IPv6
Document Capture Pro/Document Capture	IPv4

Funciones	Compatibles
Document Capture Pro Server	IPv4, IPv6

Protocolo de seguridad

IEEE802.1X*	
Filtrado IPsec/IP	
SSL/TLS	Servidor/Cliente HTTPS
SMTPS (STARTTLS, SSL/TLS)	
SNMPv3	

* Es necesario utilizar un dispositivo de conexión que cumpla con IEEE802.1X.

Uso del puerto del escáner

El escáner admite los siguientes puertos. Estos puertos deberían estar disponibles mediante el administrador de red según sea necesario.

Si el remitente (cliente) es el escáner

Para usarlo	Destino (servidor)	Protocolo	Número de puerto
Envío de archivos (cuando se escanea a una carpeta de red desde el escáner)	Servidor FTP/FTPS	FTP/FTPS (TCP)	20
			21
	Servidor de archivos	SMB (TCP)	445
		NetBIOS (UDP)	137
			138
		NetBIOS (TCP)	139
	Servidor WebDAV	Protocolo HTTP (TCP)	80
		Protocolo HTTPS (TCP)	443
Envío de correos electrónicos (al escanear al correo desde el escáner)	Servidor SMTP	SMTP (TCP)	25
		SMTP SSL/TLS (TCP)	465
		SMTP STARTTLS (TCP)	587
POP antes de conexión SMTP (cuando escanea al correo desde el escáner)	Servidor POP	POP3 (TCP)	110
Si se utiliza Epson Connect	Servidor de Epson Connect	HTTPS	443
		XMPP	5222

Para usarlo	Destino (servidor)	Protocolo	Número de puerto
Recopilación de la información del usuario (usando los contactos del escáner)	Servidor LDAP	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
Autenticación del usuario al recopilar información del usuario (si se utilizan los contactos del escáner) Autenticación de usuario al escanear a la carpeta de red (SMB) desde el escáner	Servidor KDC	Kerberos	88
Control de WSD	Equipo cliente	WSD (TCP)	5357
Buscar el ordenador al usar el escaneado desatendido desde una aplicación	Equipo cliente	Network Push Scan Discovery	2968

Si el remitente (cliente) es el ordenador

Para usarlo	Destino (servidor)	Protocolo	Número de puerto
Descubre el escáner desde una aplicación como EpsonNet Config y el controlador del escáner.	Escáner	ENPC (UDP)	3289
Recopile y configure la información MIB desde una aplicación tal como EpsonNet Config y el controlador del escáner.	Escáner	SNMP (UDP)	161
Búsqueda de escáner WSD	Escáner	WS-Discovery (UDP)	3702
Reenvío de los datos escaneados desde una aplicación	Escáner	Escaneado por red (TCP)	1865
Obtener la información del trabajo en escaneados desatendidos desde una aplicación	Escáner	Network Push Scan	2968
Web Config	Escáner	HTTP (TCP)	80
		HTTPS (TCP)	443

Resolución de problemas

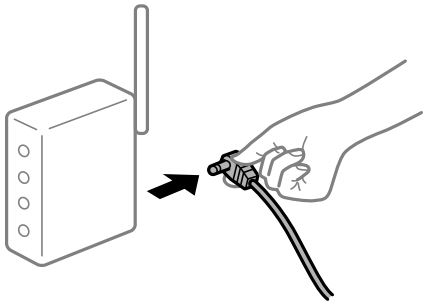
No se puede conectar a una red

El problema podría ser uno de los siguientes.

Hay un error con los dispositivos de la red de la conexión Wi-Fi.

Soluciones

Apague los dispositivos que quiera conectar a la red. Espere unos 10 segundos y luego encienda los dispositivos en el siguiente orden: router inalámbrico, ordenador o dispositivo inteligente y luego el escáner. Acerque el escáner y el ordenador o dispositivo inteligente al router inalámbrico para mejorar la comunicación por ondas de radio y, a continuación, intente configurar los ajustes de red de nuevo.



Los dispositivos no pueden recibir señales del router inalámbrico porque están demasiado alejados.

Soluciones

Después de acercar el ordenador o el dispositivo inteligente y el escáner al router inalámbrico, apáguelo y luego vuelva a encenderlo.

Al cambiar el router inalámbrico, la configuración ya no coincide con el nuevo router inalámbrico.

Soluciones

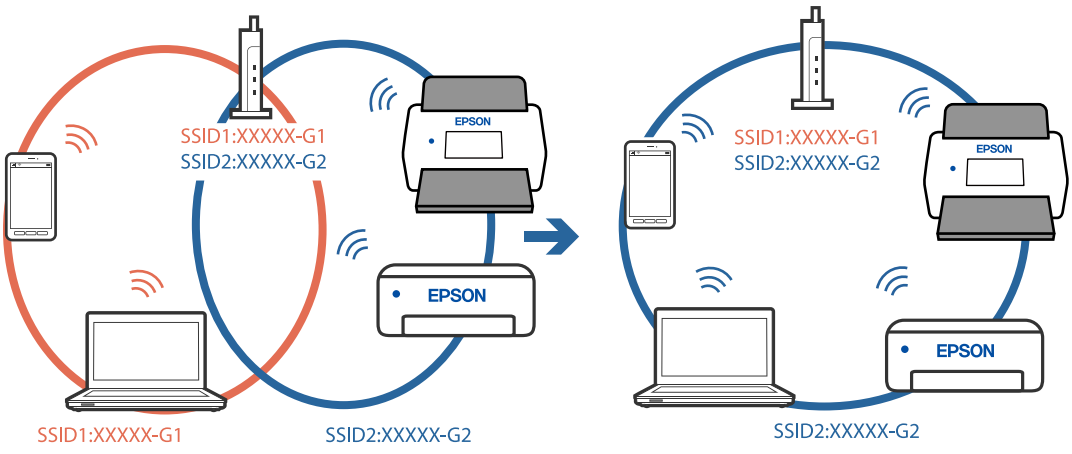
Realice de nuevo los ajustes de la conexión para que coincidan con los del nuevo router inalámbrico.

Los SSID conectados desde el ordenador o el dispositivo inteligente y el ordenador son diferentes.

Soluciones

No podrá conectarse al router inalámbrico si se utilizan varios routers inalámbricos al mismo tiempo, o si el router inalámbrico tiene varios SSID y los dispositivos están conectados a SSID distintas.

Conecte el ordenador o dispositivo inteligente al mismo SSID que el escáner.



El router inalámbrico dispone de un separador de privacidad.

Soluciones

La mayoría de routers inalámbricos cuentan con una función de separador de privacidad que bloquea la comunicación entre dispositivos conectados. Si no puede establecer comunicación entre el escáner y el ordenador o dispositivo inteligente incluso si están conectados a la misma red, desactive el separador de privacidad en el router inalámbrico. Consulte el manual proporcionado con el router para obtener más detalles.

La dirección IP está incorrectamente asignada.

Soluciones

Si la dirección IP asignada al escáner es 169.254.XXX.XXX y la máscara de subred es 255.255.0.0, puede que la dirección IP no está correctamente asignada.

Seleccione **Configuración** > **Configuración de red** > **Avanzado** > **Configuración TCP/IP** en el panel de control del escáner y, a continuación, compruebe la dirección IP y la máscara de subred asignada al escáner.

Reinicie el router inalámbrico o restablezca los ajustes de red del escáner.

Se ha producido un problema con la configuración de red del ordenador.

Soluciones

Intente acceder a una página web desde su ordenador para comprobar que la configuración de red de su ordenador es correcta. Si no puede acceder a ninguna página web, hay un problema con el ordenador.

Compruebe la conexión de red del ordenador. Para más información, consulte el manual del ordenador.

El escáner se ha conectado mediante Ethernet utilizando dispositivos compatibles con IEEE 802.3az (Ethernet con eficiencia energética).

Soluciones

Si conecta el escáner mediante Ethernet utilizando dispositivos compatibles con IEEE 802.3az (Ethernet con eficiencia energética), pueden producirse los siguientes problemas en función del concentrador o de router que esté utilizando.

❏ La conexión se vuelve inestable, el escáner se conecta y desconecta una y otra vez.

❏ No se puede conectar al escáner.

❏ La velocidad de comunicación se reduce.

Siga los pasos que se indican a continuación para deshabilitar IEEE 802.3az para el escáner y luego conéctelo.

1. Retire el cable Ethernet conectado al ordenador y al escáner.
2. Si IEEE 802.3az está habilitado para el ordenador, deshabilítelo.

   Para más información, consulte el manual del ordenador.
3. Conecte directamente el ordenador y el escáner con un cable Ethernet.
4. En el escáner, compruebe la configuración de la red.

   Seleccione **Configuración** > **Configuración de red** > **Estado de la red** > **Estado de LAN cabl./Wi-Fi**.

5. Averigüe la dirección IP del escáner.
6. En el ordenador, acceda a Web Config.

   Inicie un navegador web y, a continuación, introduzca la dirección IP del escáner.

   "Ejecución de Web Config en un navegador web" de la página 36
7. Seleccione la pestaña **Red** > **LAN cableada**.
8. Seleccione **DESACT.** para **IEEE 802.3az**.
9. Haga clic en **Siguiente**.
10. Haga clic en **Aceptar**.
11. Retire el cable Ethernet conectado al ordenador y al escáner.
12. Si deshabilitó IEEE 802.3az para el ordenador del paso 2, habilítelo.
13. Conecte los cables Ethernet que quitó en el paso 1 al ordenador y al escáner.

Si el problema persiste, es posible que otros dispositivos que no sean el escáner estén causando el problema.

El escáner está apagado.

Soluciones

Asegúrese de que el escáner está encendido.

Asimismo, espere a que el indicador luminoso de estado deje de parpadear, lo que indica que el escáner está preparado para escanear.

Software para configurar el escáner

Web Config

Web Config es una aplicación que se ejecuta en un ordenador en navegadores web como Internet Explorer y Safari. Puede confirmar el estado del escáner o cambiar el servicio de red y la configuración del escáner. Dado que a los escáneres se accede y se utilizan directamente desde la red, es adecuado para configurar un escáner cada vez. Para usar Web Config, conecte el ordenador a la misma red que el escáner.

Se admiten los siguientes navegadores.

Microsoft Edge, Windows Internet Explorer 8 o posterior, Firefox*, Chrome*, Safari*

* Utilice la última versión.

Ejecución de Web Config en un navegador web

1. Averigüe la dirección IP del escáner.

   Seleccione **Configuración** > **Configuración de red** > **Estado de la red** en el panel de control del escáner. A continuación, seleccione el estado del método de conexión activo (**Estado de LAN cabl./Wi-Fi** o **Estado de Wi-Fi Direct**) para confirmar la dirección IP del escáner.

2. Inicie un navegador web desde un ordenador o dispositivo inteligente. A continuación, introduzca la dirección IP del escáner.

   Formato:

   IPv4: http://dirección IP del escáner/

   IPv6: http://[dirección IP del escáner]/

   Ejemplos:

   IPv4: http://192.168.100.201/

   IPv6: http://[2001:db8::1000:1]/

   Nota:
   Puesto que el escáner utiliza un certificado autofirmado al acceder a HTTPS, se muestra una advertencia en el navegador al iniciar Web Config; esto no indica ningún problema y se puede ignorar sin más.

3. Inicie sesión como administrador para cambiar la configuración del escáner.

   Haga clic en **Inicio de sesión de administrador** en la parte superior derecha de la pantalla. Introduzca los números **Nombre de usuario** y **Contraseña actual** y, a continuación, haga clic en **Aceptar**.

   Nota:
   - ❏ *A continuación se proporcionan los valores iniciales para la información del administrador Web Config.*

     ·Nombre de usuario: ninguno (en blanco)

     ·Contraseña: número de serie del escáner

     Para encontrar el número de serie, compruebe la etiqueta pegada en la parte posterior del escáner.
   - ❏ *Si se muestra **Cierre de sesión de administrador** en la parte superior derecha de la pantalla, es que ya ha iniciado la sesión como administrador.*

Ejecutar Web Config en Windows

Al conectar un ordenador al escáner a través de WSD, siga los pasos que se detallan a continuación para ejecutar Web Config.

1. Abra la lista de escáneres en el ordenador.
   - ❏ Windows 10

     Haga clic en el botón de inicio y luego seleccione **Sistema de Windows** > **Panel de control** > **Ver dispositivos e impresoras** en **Hardware y sonido**.
   - ❏ Windows 8.1/Windows 8

     Seleccione **Escritorio** > **Configuración** > **Panel de control** > **Ver dispositivos e impresoras** en **Hardware y sonido** (o **Hardware**).
   - ❏ Windows 7

     Haga clic en el botón de inicio y seleccione **Panel de control** > **Ver dispositivos e impresoras** en **Hardware y sonido**.
2. Haga clic con el botón derecho en su escáner y seleccione **Propiedades**.
3. Seleccione la ficha **Servicio web** y haga clic en la dirección.

   Puesto que el escáner utiliza un certificado autofirmado al acceder a HTTPS, se muestra una advertencia en el navegador al iniciar Web Config; esto no indica ningún problema y se puede ignorar sin más.

   Nota:
   - ❏ *A continuación se proporcionan los valores iniciales para la información del administrador Web Config.*

     ·Nombre de usuario: ninguno (en blanco)

     ·Contraseña: número de serie del escáner

     Para encontrar el número de serie, compruebe la etiqueta pegada en la parte posterior del escáner.
   - ❏ *Si se muestra **Cierre de sesión de administrador** en la parte superior derecha de la pantalla, es que ya ha iniciado la sesión como administrador.*

Epson Device Admin

Epson Device Admin es una aplicación que ofrece varias funciones y que le permite administrar los dispositivos de una red.

Puede utilizar plantillas para aplicar configuraciones unificadas a diferentes escáneres de una red, siendo adecuada para instalar y administrar varios escáneres.

Puede descargar Epson Device Admin desde el sitio web de soporte técnico de Epson. Consulte los detalles de uso de esta aplicación en la documentación o en la ayuda de Epson Device Admin.

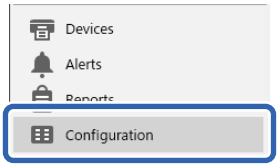
Plantilla de configuración

Crear una plantilla de configuración

Cree una plantilla de configuración desde cero.

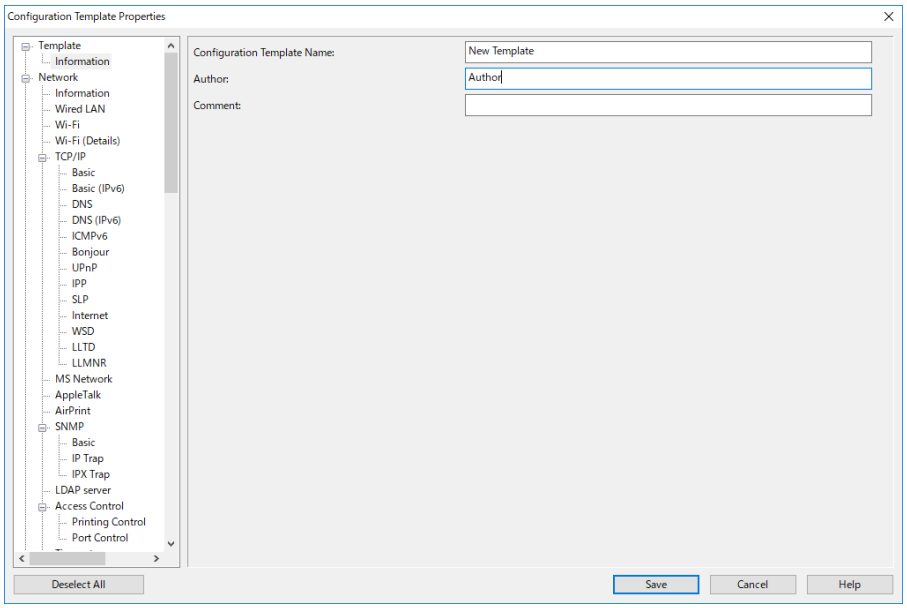
1. Inicie Epson Device Admin.

2. Seleccione **Configuración** en la barra de tareas lateral del menú.



3. Seleccione **Nuevo** en el menú de cinta.

4. Configure cada elemento.



Elemento	Explicación
Nombre de plantilla de configuración	Nombre de la plantilla de configuración. Introduzca hasta 1024 caracteres en Unicode (UTF-8).
Autor	Información sobre el creador de la plantilla. Introduzca hasta 1024 caracteres en Unicode (UTF-8).
Comentario	Introduzca cualquier información. Introduzca hasta 1024 caracteres en Unicode (UTF-8).

5. Seleccione los elementos que desee configurar a la izquierda.

   Nota:
   Haga clic en los elementos del menú de la izquierda para ir a cada pantalla. El valor establecido se conserva al cambiar de pantalla, pero no si cancela la pantalla. Cuando termine de realizar todos los ajustes, clic en ***Guardar****.*

Aplicación de la plantilla de configuración

Aplique la plantilla de configuración guardada al escáner. Se aplican los elementos seleccionados en la plantilla. Si el escáner de destino no tiene la función adecuada, no se aplica.

Nota:
Si la escáner tiene una contraseña de administrador, configure ésta de antemano.

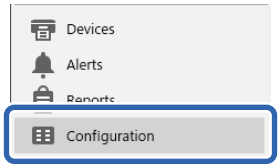
1. En el menú de cinta de la pantalla de la lista de dispositivos, seleccione ***Opciones*** *>* ***Administración de contraseñas****.*

2. Seleccione ***Habilitar administración automática de contraseñas*** *y, a continuación, haga clic en* ***Administración de contraseñas****.*

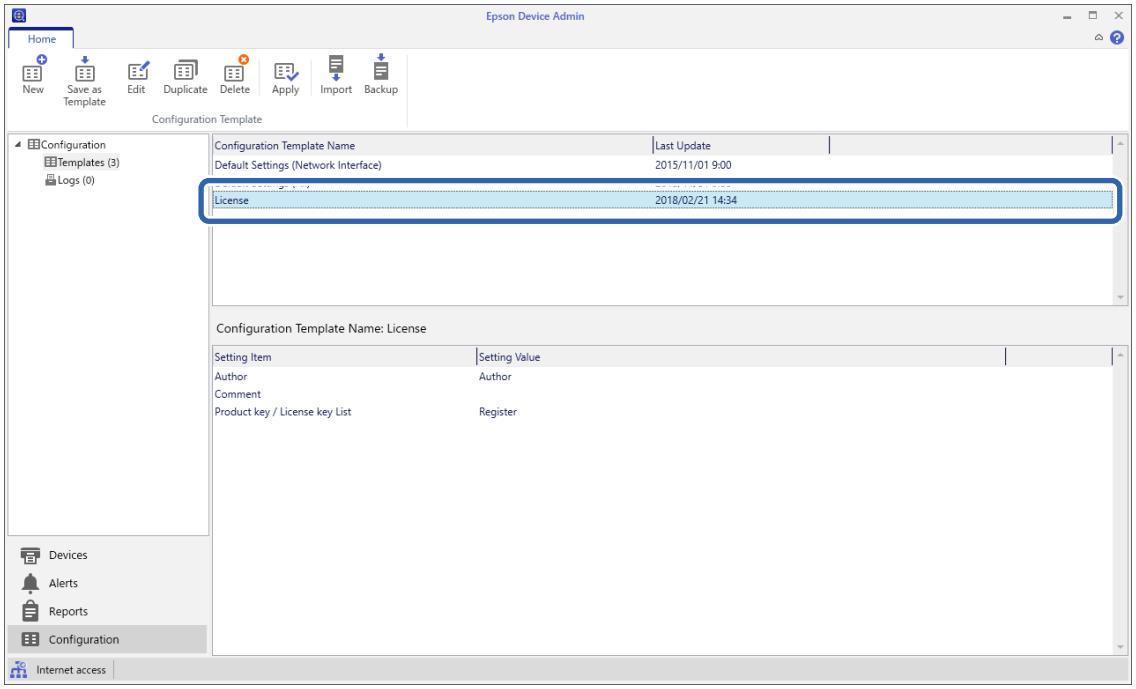
3. Seleccione el escáner adecuado y, a continuación, haga clic en ***Editar****.*

4. Establezca la contraseña y, a continuación, haga clic en ***Aceptar****.*

1. Seleccione **Configuración** en la barra de tareas lateral del menú.



2. Seleccione en **Nombre de plantilla de configuración** la plantilla de configuración que desee aplicar.



3. Haga clic en **Aplicar** en el menú de cinta.

   Se mostrará la pantalla de selección de dispositivos.

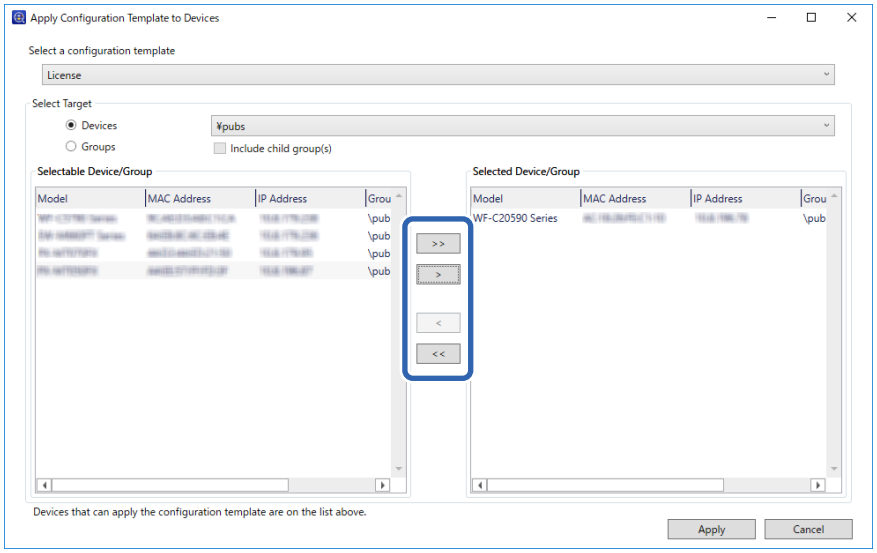
4. Seleccione la plantilla de configuración que desea aplicar.

   Nota:

   ❏ *Cuando seleccione **Dispositivos** y grupos que contengan dispositivos en el menú desplegable, se mostrará cada dispositivo.*

   ❏ *Los grupos se mostrarán cuando seleccione **Grupos**. Elija **Incluir grupos secundarios** para seleccionar grupos secundarios automáticamente con el grupo seleccionado.*

5. Mueva el escáner o los grupos a los que desea aplicar la plantilla a **Dispositivo/grupo seleccionado**.



6. Haga clic en **Aplicar**.

   Se mostrará una pantalla de confirmación para la plantilla de configuración que se va a aplicar.

7. Haga clic en **Aceptar** para aplicar la plantilla de configuración.

8. Cuando se muestre un mensaje comunicándole que el procedimiento ha finalizado, haga clic en **Aceptar**.

9. Haga clic en **Detalles** y verifique la información.

   Si aparece en los elementos que aplique, la aplicación se ha realizado correctamente.

10. Haga clic en **Cerrar**.

Ajustes necesarios para el escaneado

Configurar un servidor de correo

Configure el servidor de correo desde Web Config.

Si el escáner puede enviar el correo electrónico configurando el servidor de correo, es posible hacer lo siguiente.

❏ Transferir los resultados del escaneado mediante correo electrónico

❏ Recibir la notificación por correo electrónico desde el escáner

Compruebe lo siguiente antes de realizar la configuración.

❏ El escáner está conectado a una red que puede acceder al servidor de correo.

❏ La información de la configuración de correo electrónico del ordenador utiliza el mismo servidor de correo que el escáner.

Nota:

❏ *Si utiliza el servidor de correo en Internet, confirme la información de la configuración del proveedor o del sitio web.*

❏ *También puede configurar el servidor de correo desde el panel de control. Acceda de la siguiente manera.*
Configuración > ***Configuración de red*** > ***Avanzado*** > ***Servidor correo elect.*** > ***Configuración del servidor***

1. Acceda a Web Config y seleccione la pestaña **Red** > **Servidor correo electrónico** > **Básica**.
2. Introduzca un valor para cada opción.
3. Seleccione **Aceptar**.
   Se mostrarán los ajustes que ha seleccionado.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Opciones de ajuste del servidor de correo

Elementos	Ajustes y explicación	
Método de autenticación	Especifique el método de autenticación para que el escáner acceda al servidor de correo.	
	Desactivar	La autenticación queda deshabilitada al realizar una comunicación con un servidor de correo.
	AUTENTICACIÓN SMTP	Requiere un servidor de correo compatible con la autenticación SMTP.
	POP antes de SMTP	Si elige este método, tiene que configurar el servidor POP3.
Cuenta autenticada	Si selecciona **AUTENTICACIÓN SMTP** o **POP antes de SMTP** como **Método de autenticación**, escriba el nombre de la cuenta autenticada de manera que tenga entre 0 y 255 caracteres ASCII (0x20–0x7E).	
Contraseña autenticada	Si selecciona **AUTENTICACIÓN SMTP** o **POP antes de SMTP** como **Método de autenticación**, escriba la contraseña autenticada de manera que tenga entre 0 y 20 caracteres ASCII (0x20–0x7E).	

Elementos	Ajustes y explicación	
Dirección correo del remitente	Escriba la dirección del remitente del correo electrónico. Escriba entre 0 y 255 caracteres ASCII (0x20–0x7E). No se admiten los siguientes caracteres: : ( ) < > [ ] ; ¥. El primer carácter no puede ser un punto «.».	
Dirección del servidor SMTP	Escriba entre 0 y 255 caracteres. Caracteres admitidos: A–Z a–z 0–9 . -. Puede utilizar el formato IPv4 o el FQDN.	
Nº de puerto del servidor SMTP	Escriba un número comprendido entre el 1 y el 65535.	
Conexión segura	Especifique el método de conexión segura para el servidor de correo electrónico.	
	Ninguno	Si selecciona **POP antes de SMTP** en **Método de autenticación**, el método de conexión se establece en **Ninguno**.
	SSL/TLS	Esto está disponible cuando **Método de autenticación** se establece en **Desactivar** o **AUTENTICACIÓN SMTP**.
	STARTTLS	Esto está disponible cuando **Método de autenticación** se establece en **Desactivar** o **AUTENTICACIÓN SMTP**.
Validación de certificado	El certificado se valida cuando esta opción está habilitada. Le recomendamos que lo configure como **Activar**.	
Dirección del servidor POP3	Si selecciona **POP antes de SMTP** como **Método de autenticación**, introduzca una dirección del servidor POP3 que contenga entre 0 y 255 caracteres. Caracteres admitidos: A–Z a–z 0–9 . -. Puede utilizar el formato IPv4 o el FQDN.	
Nº de puerto del servidor POP3	Si selecciona **POP antes de SMTP** como **Método de autenticación**, introduzca un número comprendido entre el 1 y el 65535.	

Comprobación de la conexión del servidor de correo

Puede comprobar la conexión al servidor de correo ejecutando la función de prueba de conexión.

1. Acceda a Web Config y seleccione la pestaña **Red** > **Servidor correo electrónico** > **Prueba de conex.**.
2. Seleccione **Iniciar**.

   La prueba de conexión al servidor de correo se inicia. Cuando termine la prueba, se mostrará el informe.

   Nota:
   También puede comprobar la conexión al servidor de correo desde el panel de control. Acceda de la siguiente manera.

   Configuración** > **Configuración de red** > **Avanzado** > **Servidor correo elect.** > **Comprobar conexión

Referencias de la prueba de conexión del servidor de correo

Mensajes	Causa
Prueba de conexión correcta.	Este mensaje aparece si la conexión con el servidor es satisfactoria.

Mensajes	Causa
Error de comunicación del servidor SMTP. Compruebe lo siguiente. - Configuración de red	Este mensaje aparece cuando ❏ El escáner no está conectado a una red ❏ El servidor SMTP está fuera de servicio ❏ La conexión de red se ha interrumpido durante la comunicación ❏ Los datos recibidos están incompletos
Error de comunicación del servidor POP3. Compruebe lo siguiente. - Configuración de red	Este mensaje aparece cuando ❏ El escáner no está conectado a una red ❏ El servidor POP3 está fuera de servicio ❏ La conexión de red se ha interrumpido durante la comunicación ❏ Los datos recibidos están incompletos
Error al conectar con el servidor SMTP. Compruebe lo siguiente. - Dirección del servidor SMTP - Servidor DNS	Este mensaje aparece cuando ❏ Error al conectar con un servidor DNS ❏ Error en la resolución de nombre para un servidor SMTP
Error al conectar con el servidor POP3. Compruebe lo siguiente. - Dirección del servidor POP3 - Servidor DNS	Este mensaje aparece cuando ❏ Error al conectar con un servidor DNS ❏ La resolución de nombres de un servidor POP3 ha fallado
Error de autenticación del servidor SMTP. Compruebe lo siguiente. - Método de autenticación - Cuenta autenticada - Contraseña autenticada	Este mensaje aparece cuando se produce un error en la autenticación del servidor SMTP.
Error de autenticación del servidor POP3. Compruebe lo siguiente. - Método de autenticación - Cuenta autenticada - Contraseña autenticada	Este mensaje aparece cuando se produce un error en la autenticación del servidor POP3.
Método de comunicación no admitido. Compruebe lo siguiente. - Dirección del servidor SMTP - Nº de puerto del servidor SMTP	Este mensaje aparece cuando intenta comunicarse con protocolos no admitidos.
Error de conexión con el servidor SMTP. Cambie Conexión segura a Ninguno.	Este mensaje aparece cuando se produce una discordancia SMTP entre un servidor y un cliente, o cuando el servidor no admite una conexión segura SMTP (conexión SSL).
Error de conexión con el servidor SMTP. Cambie Conexión segura a SSL/TLS.	Este mensaje aparece cuando se produce una discordancia SMTP entre un servidor y un cliente, o cuando el servidor solicita usar una conexión SSL/TLS para una conexión segura SMTP.
Error de conexión con el servidor SMTP. Cambie Conexión segura a STARTTLS.	Este mensaje aparece cuando se produce una discordancia SMTP entre un servidor y un cliente, o cuando el servidor solicita usar una conexión STARTTLS para una conexión segura SMTP.
La conexión no es de confianza. Compruebe lo siguiente. - Fecha y hora	Este mensaje aparece cuando la configuración de la fecha y hora del escáner es incorrecta o el certificado ha expirado.
La conexión no es de confianza. Compruebe lo siguiente. - Certificado CA	Este mensaje aparece cuando el escáner no tiene un certificado raíz correspondiente al servidor o no se ha importado un Certificado CA.
La conexión no es de confianza.	Este mensaje aparece cuando el certificado obtenido está dañado.

Mensajes	Causa
Error de autenticación del servidor SMTP. Cambie Método de autenticación a AUTENTICACIÓN SMTP.	Este mensaje aparece cuando se produce una discordancia en el método de autenticación entre un servidor y un cliente. El servidor admite AUTENTICACIÓN SMTP.
Error de autenticación del servidor SMTP. Cambie Método de autenticación a POP antes de SMTP.	Este mensaje aparece cuando se produce 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.	Este mensaje aparece cuando la dirección de correo electrónico del remitente especificada es errónea.
No se puede acceder al producto hasta que el proceso se haya completado.	Este mensaje aparece cuando el escáner está ocupado.

Configurar una carpeta de red compartida

Configure una carpeta de red compartida para guardar la imagen escaneada.

Al guardar un archivo en la carpeta, el escáner inicia sesión como el usuario de la computadora en la que se creó la carpeta.

Creación de carpetas compartidas

Información relacionada

➡ “Antes de crear la carpeta compartida” de la página 45

➡ “Consulta del perfil de red” de la página 46

➡ “Ubicación en la que se crea la carpeta compartida y ejemplo de la seguridad” de la página 46

➡ “Adición de grupos o usuarios para permiso de acceso” de la página 59

Antes de crear la carpeta compartida

Antes de crear la carpeta compartida, compruebe lo siguiente.

❏ El escáner está conectado a la red, a través de la cual puede acceder al ordenador donde se creará la carpeta compartida.

❏ El nombre del ordenador donde se creará la carpeta compartida no debe contener ningún carácter multibyte.

Importante:

Si el nombre del ordenador contiene algún carácter multibyte, podría fallar la operación de guardado del archivo en la carpeta compartida.

En ese caso, cambie a un ordenador cuyo nombre no contenga caracteres multibyte o bien cambie el nombre del ordenador.

Si cambia el nombre del ordenador, confírmelo con el administrador de antemano ya que podría afectar a ciertos elementos de configuración, como la administración del equipo, el acceso a recursos, etc.

Consulta del perfil de red

Consulte en el ordenador donde se creará la carpeta compartida si está habilitada la función de uso compartido de carpetas.

1. Inicie sesión en el ordenador donde se va a crear la carpeta compartida con la cuenta de usuario con permisos de administrador.
2. Seleccione **Panel de control** > **Redes e Internet** > **Centro de redes y recursos compartidos**.
3. Haga clic en **Cambiar configuración de uso compartido** y, a continuación, haga clic en en el **(perfil actual)** de la lista de perfiles de red que aparece.
4. Compruebe si está seleccionado **Activar el uso compartido de archivos e impresoras** en **Compartir archivos e impresoras**.

   Si ya está seleccionado, haga clic en **Cancelar** y cierre la ventana.

   Si cambia la configuración, haga clic en **Guardar cambios** y cierre la ventana.

Ubicación en la que se crea la carpeta compartida y ejemplo de la seguridad

La seguridad y la comodidad varían dependiendo de la ubicación en la que se cree la carpeta compartida.

Para poder utilizar la carpeta compartida desde los escáneres u otros ordenadores, son necesarios los siguientes permisos de lectura y modificación de la carpeta.

❏ Pestaña **Compartir** > **Uso compartido avanzado** > **Permisos**

Controla el permiso de acceso a la red de la carpeta compartida.

❏ Pestaña Permiso de acceso de **Seguridad**

Controla los permisos de acceso a la red y acceso local de la carpeta compartida.

Si selecciona **Todos** para la carpeta compartida que ha creado en el escritorio como ejemplo, se permitirá el acceso a todos los usuarios que tengan acceso al ordenador.

Sin embargo, los usuarios que no tengan autoridad no podrán acceder a ella porque la carpeta del escritorio está controlada por la carpeta del usuario y cuenta con los mismos ajustes de seguridad. Los usuarios a los que se les permita el acceso desde la pestaña **Seguridad** (usuario con sesión iniciada y administrador, en este caso) podrán utilizar la carpeta.

Más abajo encontrará información relacionada con la creación de carpetas en la ubicación adecuada.

Este ejemplo sirve para la creación de la carpeta «scan_folder».

Información relacionada

➡ "Ejemplo de configuración para servidores de archivos" de la página 46

➡ "Ejemplo de configuración para un ordenador personal" de la página 53

Ejemplo de configuración para servidores de archivos

Esta explicación es un ejemplo de cómo crear la carpeta compartida en el directorio raíz de la unidad del ordenador compartido, como el servidor de archivos en la siguiente situación.

Los usuarios con acceso controlable, como aquellos que tienen el mismo dominio de un ordenador para crear una carpeta compartida, pueden acceder la carpeta compartida.

Realice esta configuración cuando desee otorgar a cualquier usuario permiso de lectura y escritura para la carpeta compartida en el ordenador, como el servidor de archivos y el ordenador compartido.

❏ Lugar de creación de la carpeta compartida: directorio raíz de la unidad

❏ Ruta de la carpeta: C:\scan_folder

❏ Permiso de acceso a través de la red (Permisos de los recursos compartidos): todos

❏ Permiso de acceso en sistema de archivos (Seguridad): usuarios autentificados

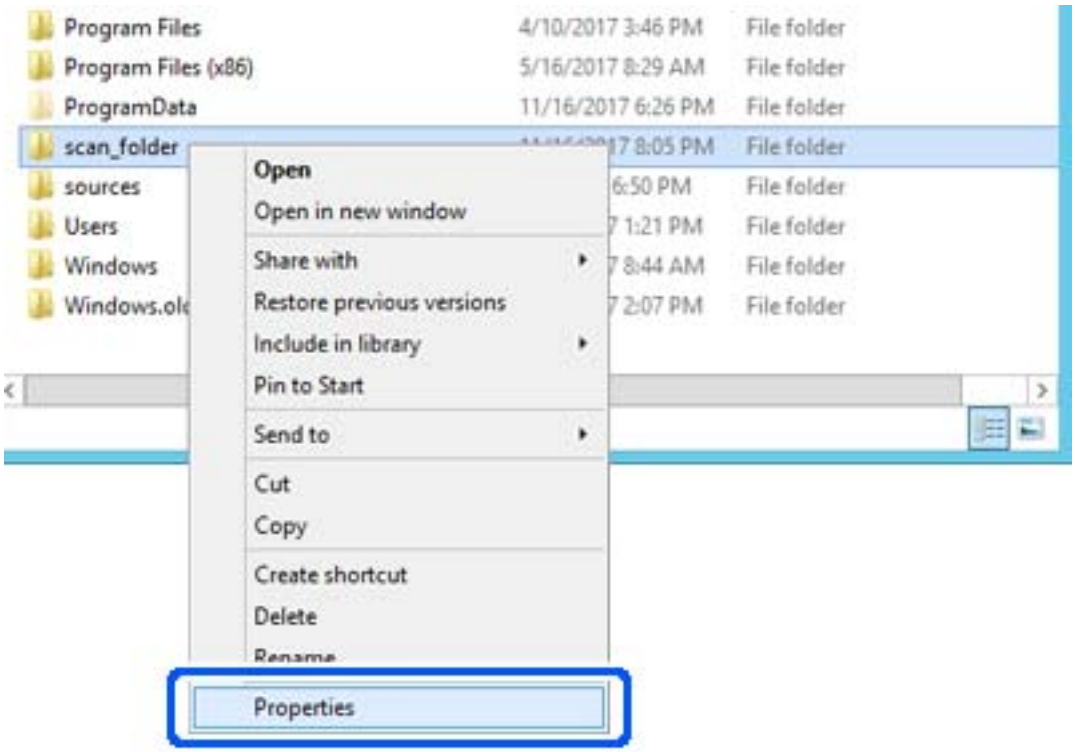
1. Inicie sesión en el ordenador donde se va a crear la carpeta compartida con la cuenta de usuario con permisos de administrador.

2. Inicie el explorador.

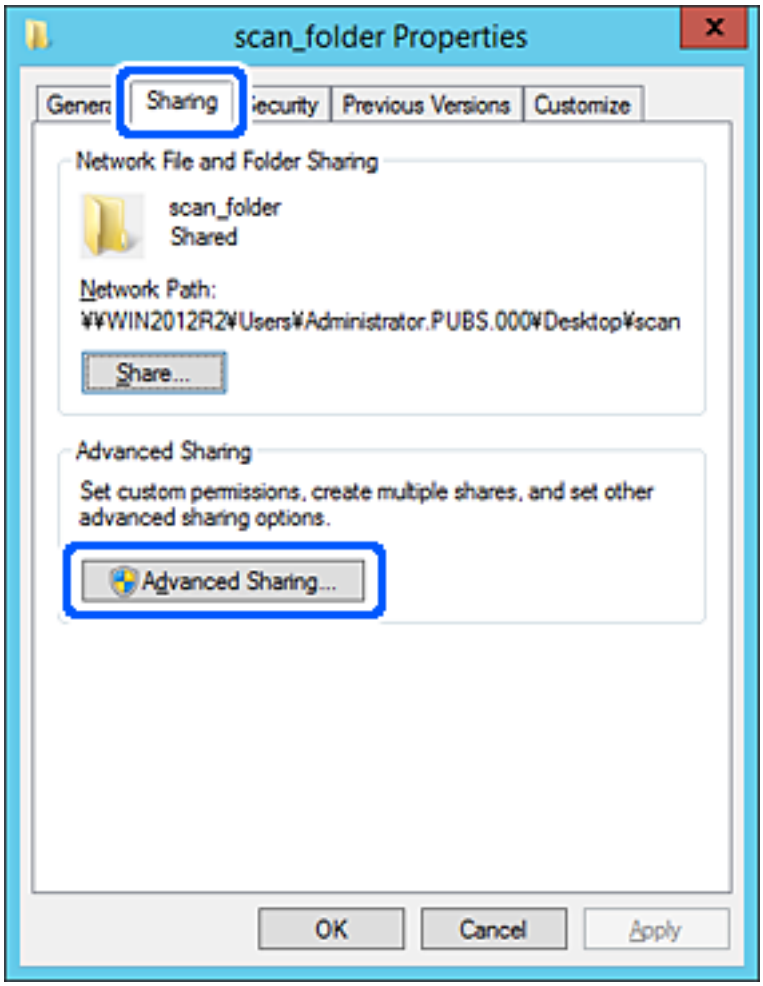
3. Cree la carpeta en el directorio raíz de la unidad y denomínela «scan_folder».

   Para el nombre de la carpeta, introduzca entre 1 y 12 caracteres alfanuméricos. Si se supera el límite, es posible que no pueda acceder a ella de forma normal según el entorno.

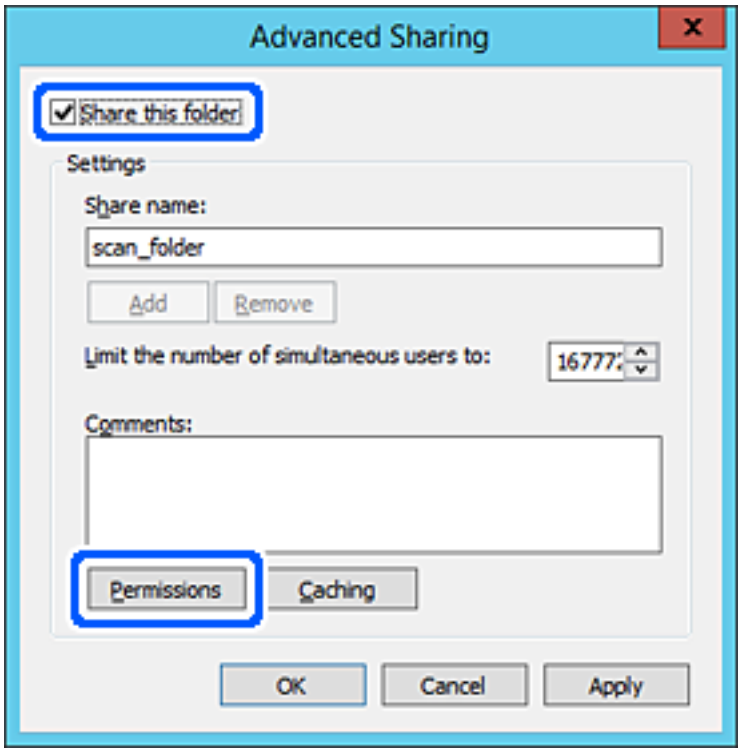
4. Haga clic con el botón derecho en la carpeta y seleccione **Propiedades**.



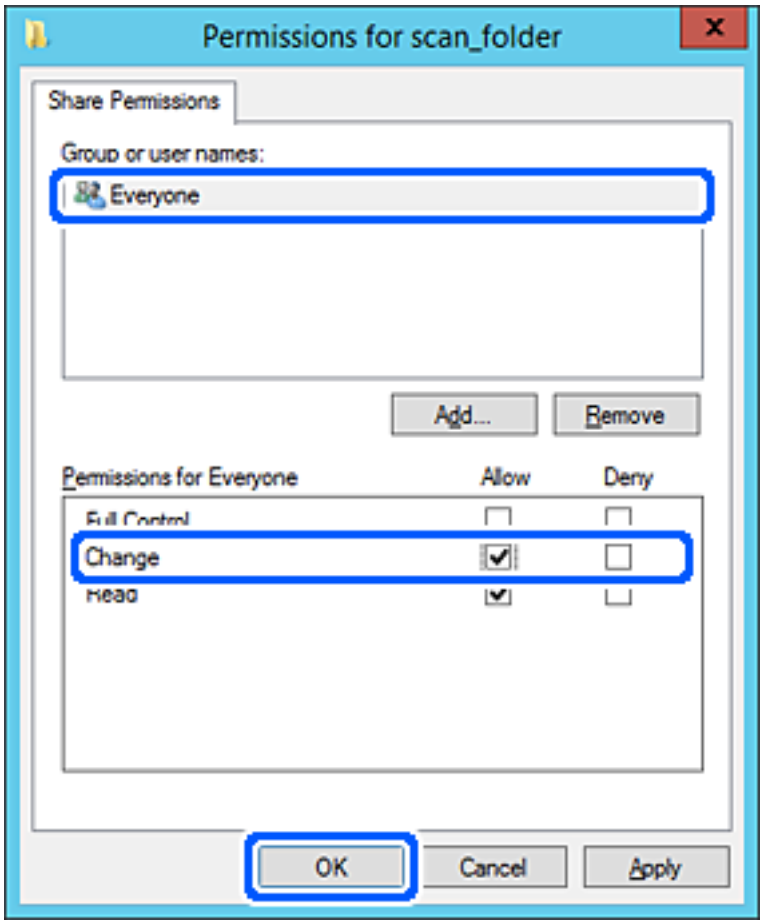
5. Haga clic en **Uso compartido avanzado** en la pestaña **Compartir**.



6. Seleccione **Compartir esta carpeta** y, a continuación, haga clic en **Permisos**.

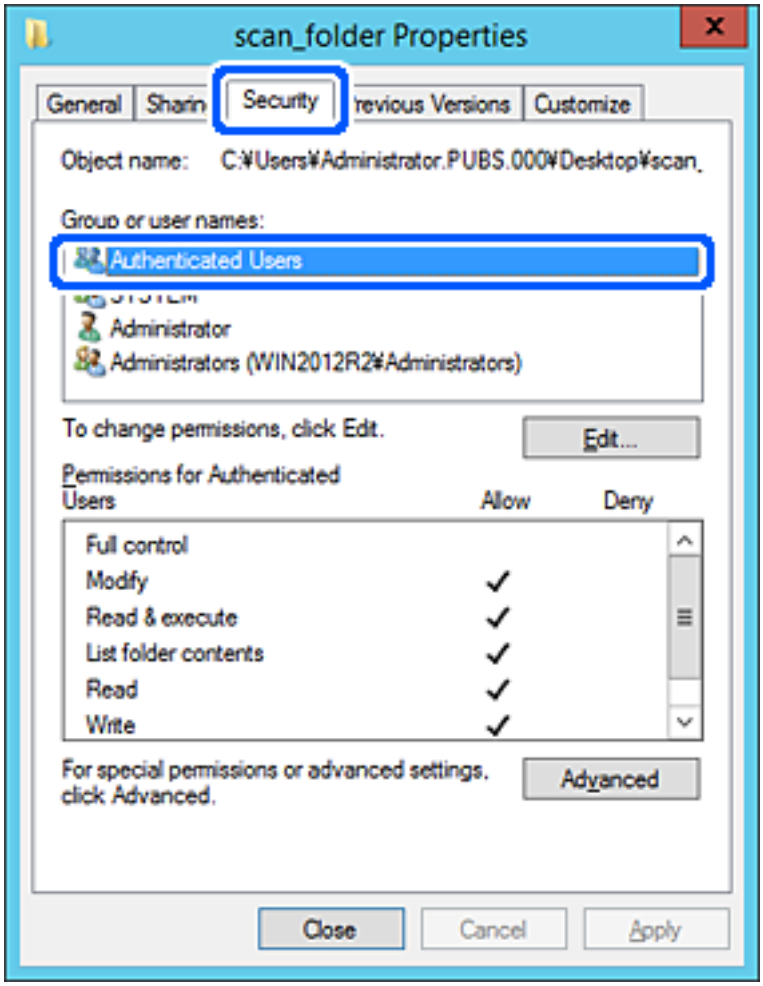


7. Seleccione el grupo **Todos** en **Nombres de grupos o usuarios**, seleccione **Permitir** en **Cambiar** y, a continuación, haga clic en **OK**.



8. Haga clic en **OK**.

9. Seleccione la pestaña **Seguridad** y, a continuación, seleccione **Usuarios autentificados** en **Nombres de grupos o usuarios**.

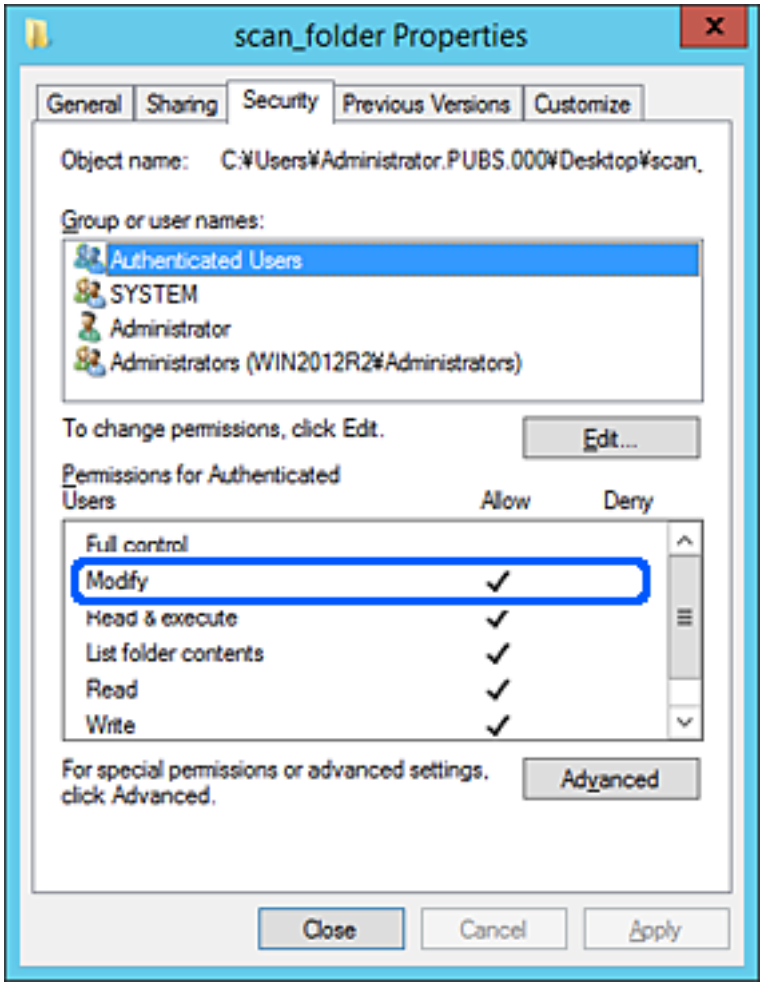


«Usuarios autentificados» es el grupo especial que incluye a todos los usuarios que pueden iniciar sesión en el dominio o el ordenador. Este grupo se muestra solo cuando se crea la carpeta justo un nivel por debajo de la carpeta raíz.

Si no se muestra, puede añadirlo haciendo clic en **Editar**. Consulte la Información relacionada para obtener más información.

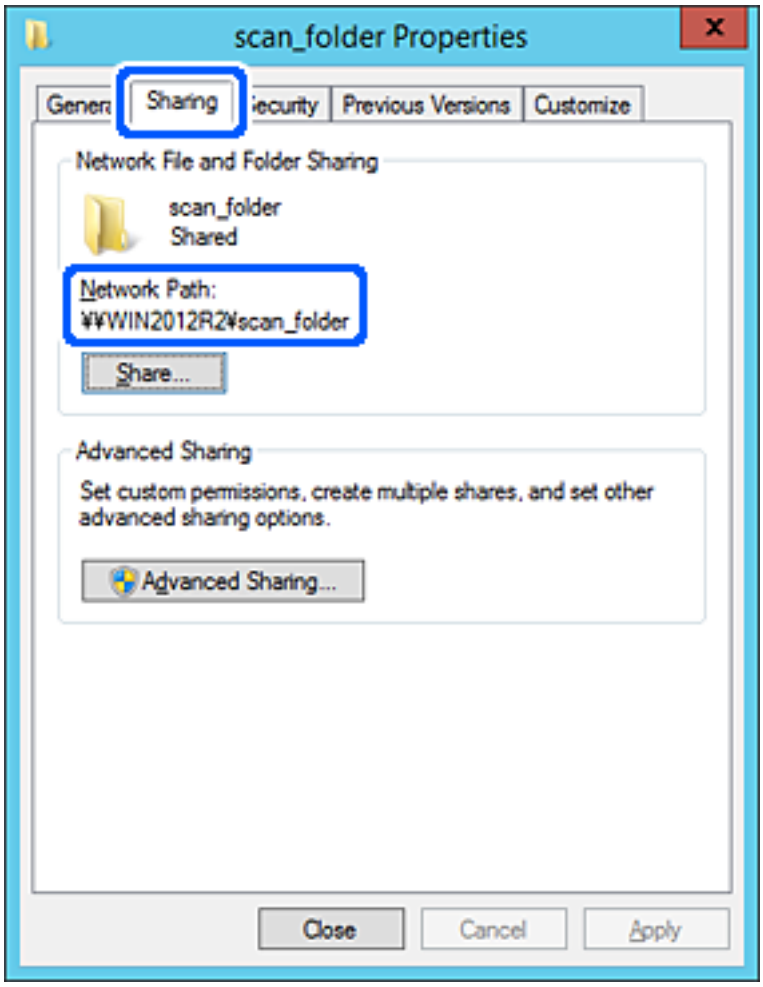
10. Compruebe que está seleccionado **Permitir** en **Cambiar** en el cuadro de **Permisos para Usuarios autentificados**.

    Si no está seleccionado, seleccione **Usuarios autentificados**, haga clic en **Editar**, seleccione **Permitir** en **Cambiar** en el cuadro de **Permisos para Usuarios autentificados** y, a continuación, haga clic en **OK**.



11. Seleccione la pestaña **Compartir**.

    Aparecerá la ruta de red de la carpeta compartida. Esto se utiliza cuando se registran los contactos del escáner. Anótela.



12. Haga clic en **OK** o **Cerrar** para cerrar la pantalla.

    Compruebe si el archivo es de lectura o escritura en la carpeta compartida de los ordenadores del mismo dominio.

Información relacionada

➡ "Adición de grupos o usuarios para permiso de acceso" de la página 59

➡ "Registro de un destino para contactos mediante Web Config" de la página 64

Ejemplo de configuración para un ordenador personal

Esta explicación es un ejemplo de cómo crear la carpeta compartida en el escritorio del usuario que ha iniciado sesión actualmente en el ordenador.

El usuario que inicie sesión en el ordenador y que cuente con permisos de administrador podrá acceder a la carpeta del escritorio y la carpeta de documentos que se encuentran en la carpeta del Usuario.

Realice esta configuración cuando NO desee permitir la lectura y escritura de la carpeta compartida de un ordenador a otro usuario.

- ❏ Lugar de creación de la carpeta compartida: escritorio
- ❏ Ruta de la carpeta: C:\Users\xxxx\Desktop\scan_folder
- ❏ Permiso de acceso a través de la red (Permisos de los recursos compartidos): todos
- ❏ Permiso de acceso en sistema de archivos (Seguridad): no añadir o añadir nombres de usuario/grupos para permitir el acceso

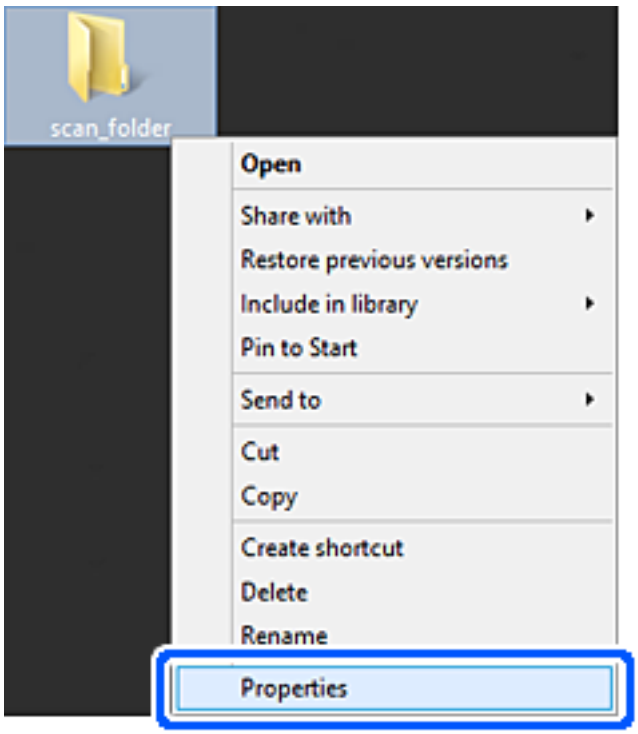
1. Inicie sesión en el ordenador donde se va a crear la carpeta compartida con la cuenta de usuario con permisos de administrador.

2. Inicie el explorador.

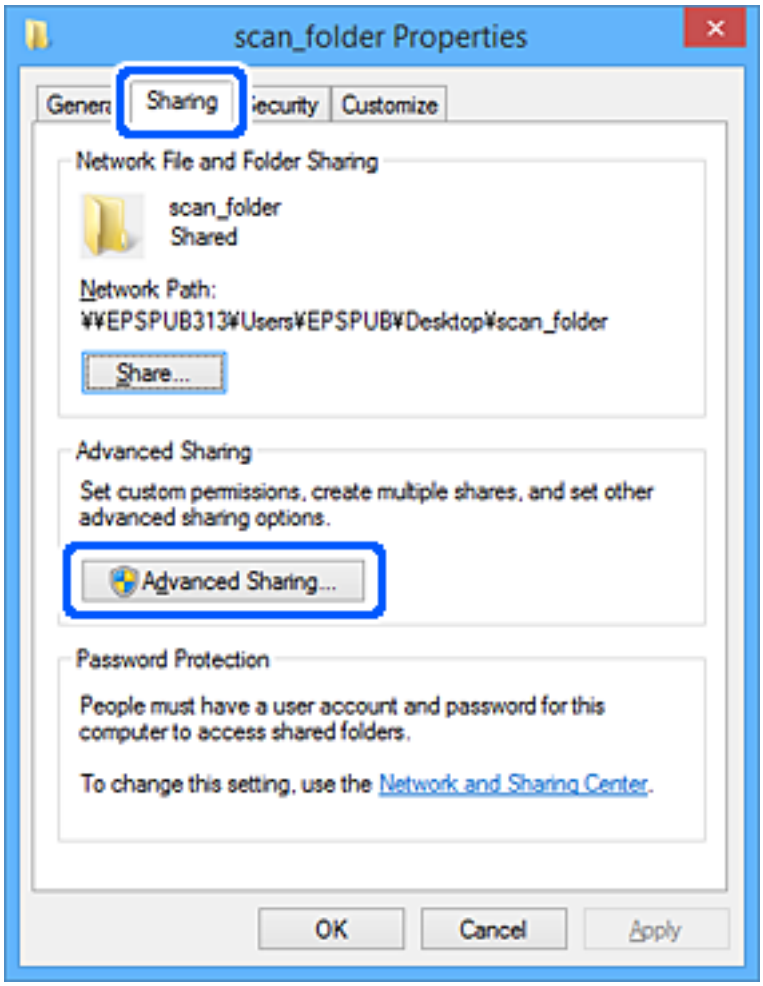
3. Cree la carpeta en el escritorio y denomínela «scan_folder».

   Para el nombre de la carpeta, introduzca entre 1 y 12 caracteres alfanuméricos. Si se supera el límite, es posible que no pueda acceder a ella de forma normal según el entorno.

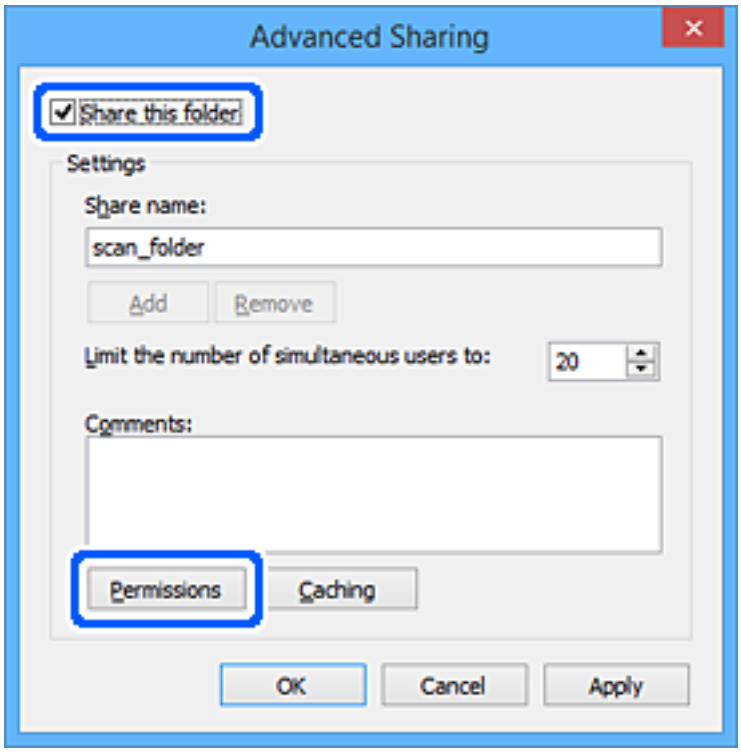
4. Haga clic con el botón derecho en la carpeta y seleccione **Propiedades**.



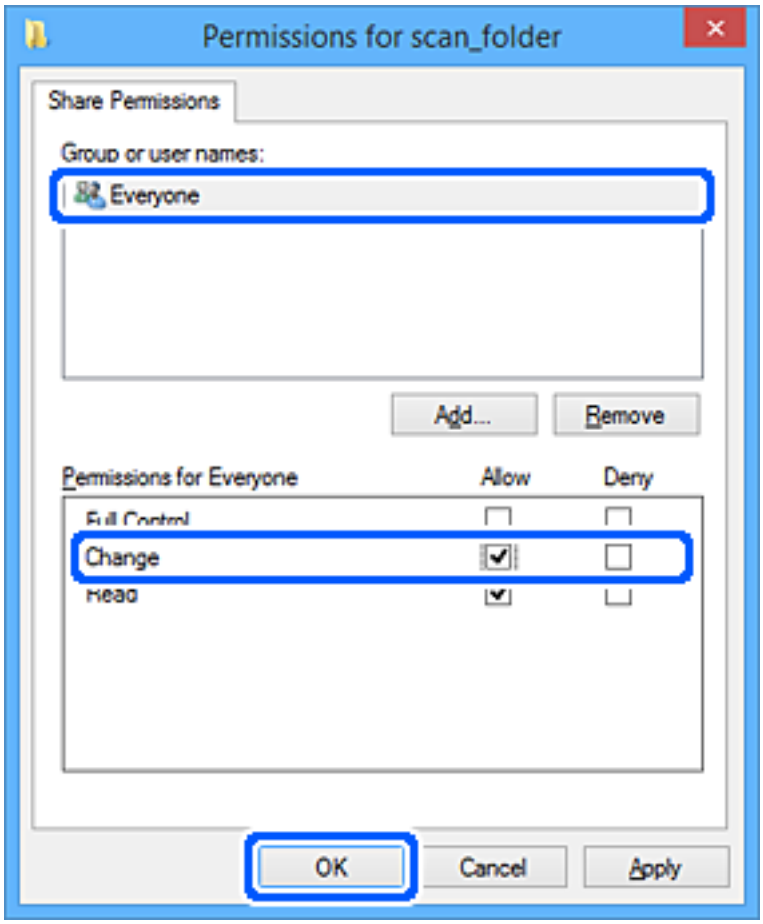
5. Haga clic en **Uso compartido avanzado** en la pestaña **Compartir**.



6. Seleccione **Compartir esta carpeta** y, a continuación, haga clic en **Permisos**.



7. Seleccione el grupo **Todos** en **Nombres de grupos o usuarios**, seleccione **Permitir** en **Cambiar** y, a continuación, haga clic en **OK**.



8. Haga clic en **OK**.

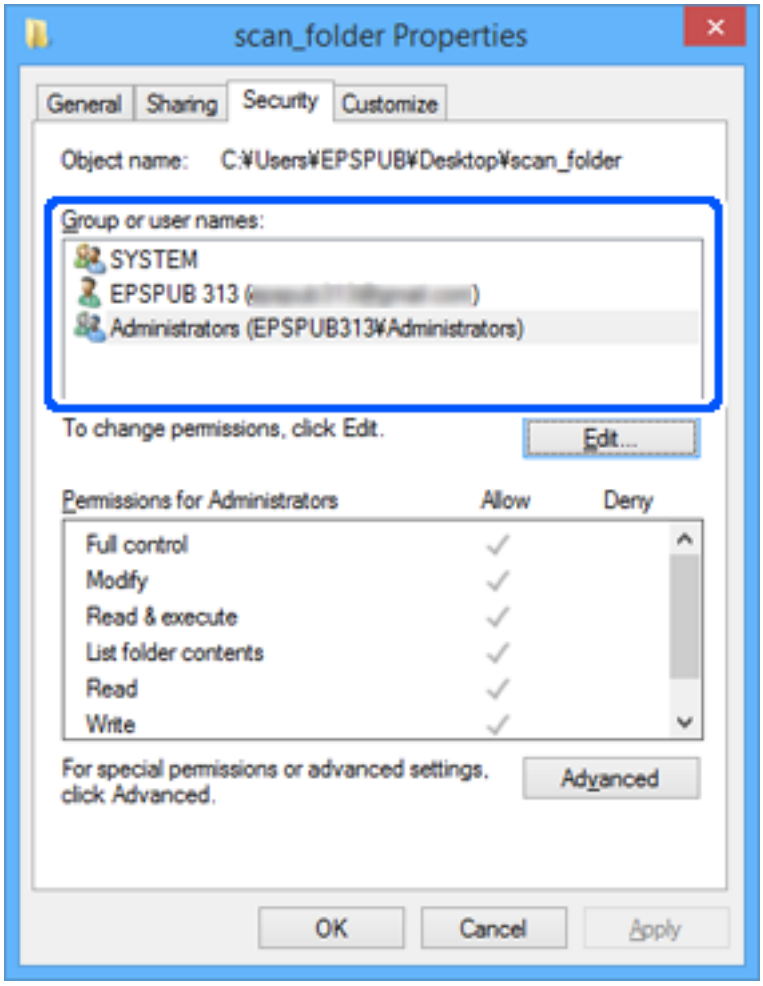
9. Seleccione la pestaña **Seguridad**.

10. Compruebe el grupo o el usuario en **Nombres de grupos o usuarios**.

    El grupo o usuario que aparezca aquí tendrá acceso a la carpeta compartida.

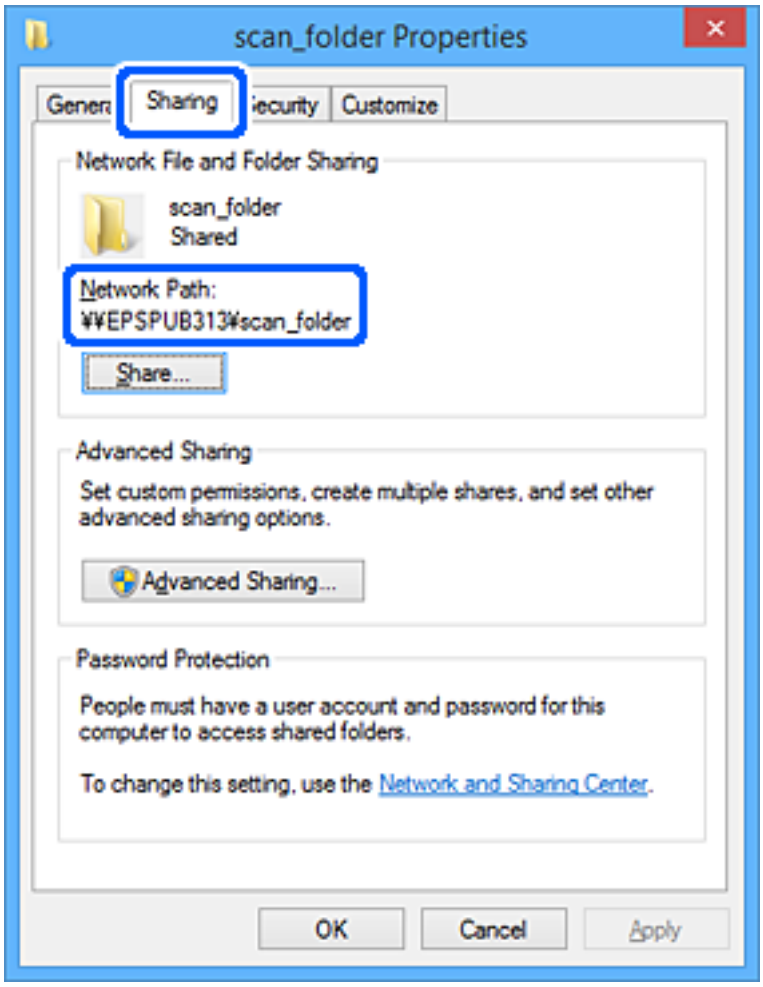
    En este caso, el usuario que inicie sesión en el ordenador y el administrador podrán acceder a la carpeta compartida.

Añada permisos de acceso, si fuera necesario. Puede añadirlos haciendo clic en **Editar**. Consulte la Información relacionada para obtener más información.



11. Seleccione la pestaña **Compartir**.

    Aparecerá la ruta de red de la carpeta compartida. Esto se utiliza cuando se registran los contactos del escáner. Anótela.



12. Haga clic en **OK** o **Cerrar** para cerrar la pantalla.

    Compruebe si el archivo es de lectura o escritura en la carpeta compartida de los ordenadores de los usuarios o grupos con permiso de acceso.

Información relacionada

➡ "Adición de grupos o usuarios para permiso de acceso" de la página 59
➡ "Registro de un destino para contactos mediante Web Config" de la página 64

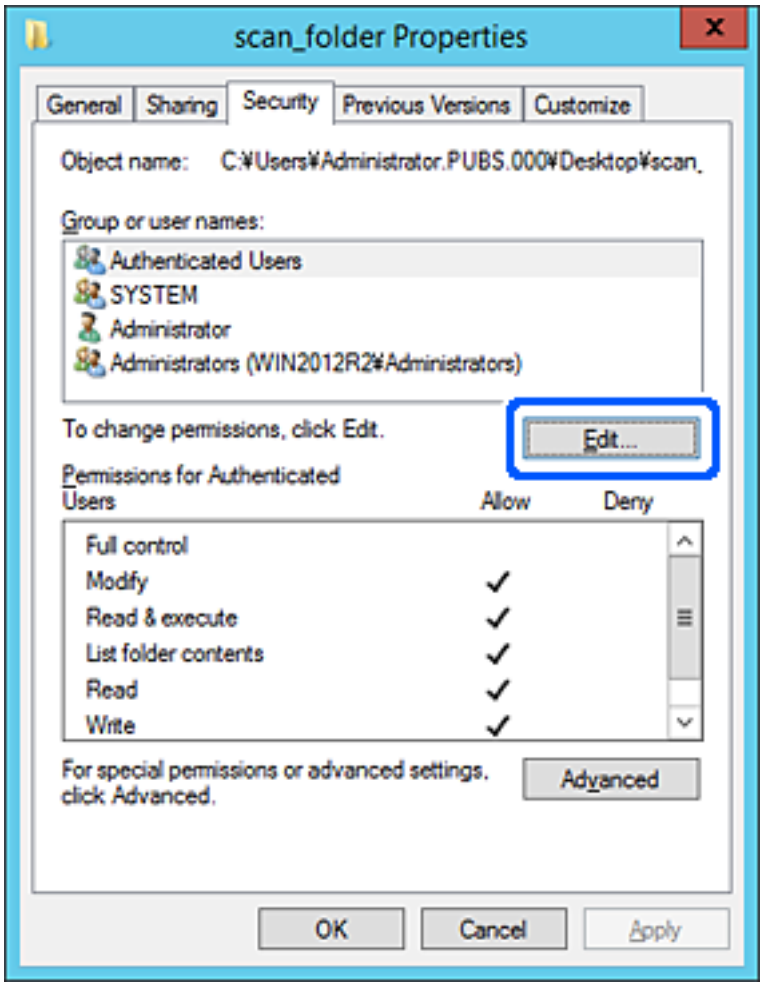
Adición de grupos o usuarios para permiso de acceso

Puede añadir grupos o usuarios a los que dar permiso de acceso.

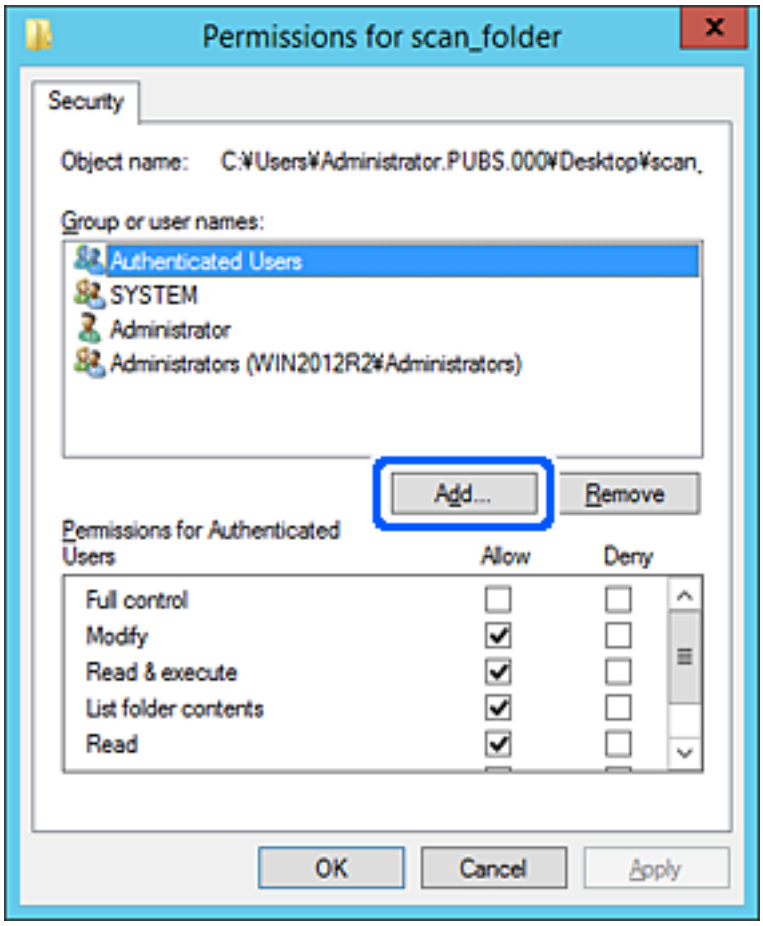
1. Haga clic con el botón derecho en la carpeta y seleccione **Propiedades**.

2. Seleccione la pestaña **Seguridad**.

3. Haga clic en **Editar**.



4. Haga clic en **Agregar** debajo de **Nombres de grupos o usuarios**.

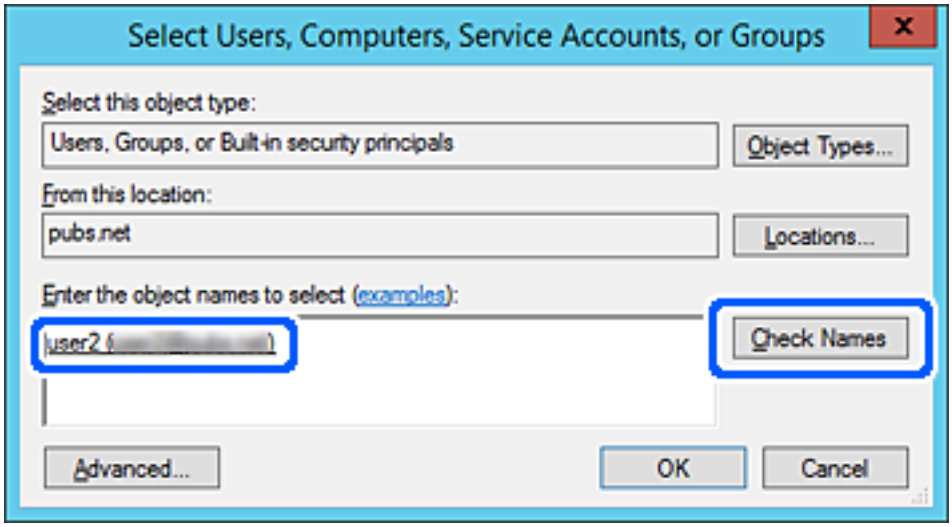


5. Introduzca el nombre del grupo o usuario para el que desee permitir el acceso y, a continuación, haga clic en **Comprobar nombres**.

   Aparecerá el nombre subrayado.

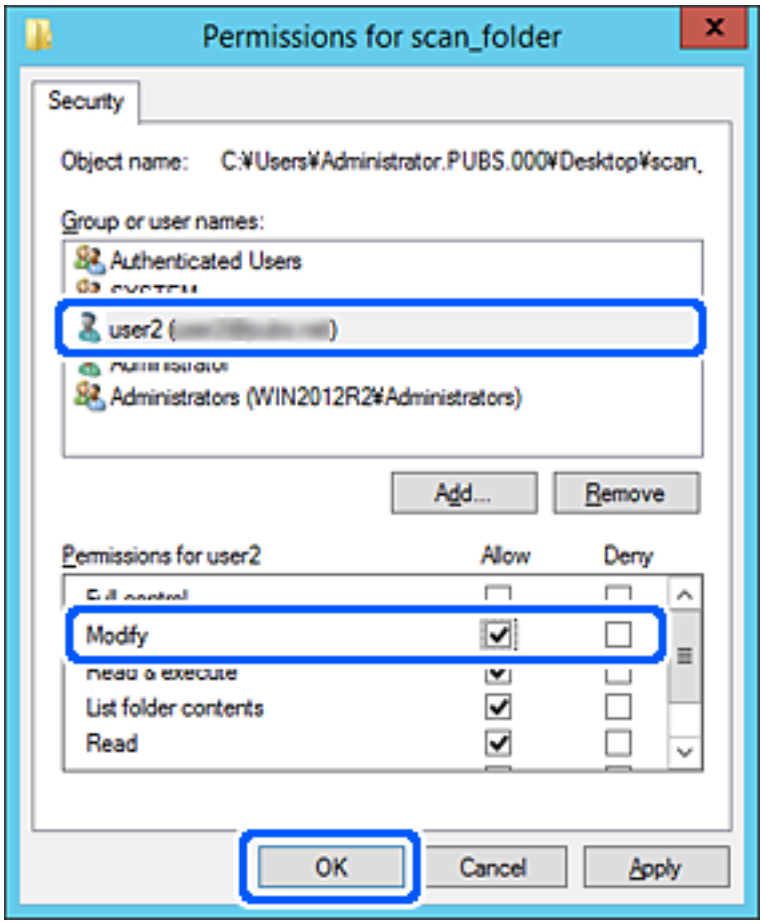
Nota:
Si no conoce el nombre completo del grupo o usuario, introduzca parte del nombre y, a continuación, haga clic en ***Comprobar nombres****. Aparecerá una lista con los nombres de grupo o usuario que coincidan con la parte del nombre introducida, y podrá entonces seleccionar el nombre completo en la lista.*

Si solo coincide un nombre, el nombre completo subrayado aparecerá en ***Escriba el nombre del objeto que desea seleccionar****.*



6. Haga clic en **Aceptar**.

7. En la pantalla Permiso, seleccione el nombre de usuario introducido en **Nombres de grupos o usuarios**, seleccione el permiso de acceso en **Cambiar** y haga clic en **Aceptar**.



8. Haga clic en **Aceptar** o **Cerrar** para cerrar la pantalla.

   Compruebe si el archivo es de lectura o escritura en la carpeta compartida de los ordenadores de los usuarios o grupos con permiso de acceso.

Hacer que los contactos estén disponibles

El registro de destinos de la lista de contactos del escáner le permite introducir fácilmente el destino cuando escanee.

En la lista de contactos puede registrar los siguientes tipos de destinos. Puede registrar hasta 300 entradas en total.

Nota:
También puede utilizar el servidor LDAP (búsqueda LDAP) para introducir el destino.

Correo electrónico	Destino del correo electrónico. Necesita configurar los ajustes del servidor de correo electrónico con antelación.
Carpeta de red	Destino de los datos del escaneado. La carpeta de red se debe preparar de antemano.

Información relacionada

➡ "Cooperación entre el servidor LDAP y los usuarios" de la página 70

Comparación de las configuraciones de los contactos

Hay tres herramientas para configurar los contactos del escáner: Web Config, Epson Device Admin y el panel de control del escáner. En la tabla siguiente se muestran las diferencias entre las tres herramientas.

Funciones	Web Config*	Epson Device Admin	Panel de control del escáner
Registrar un destino	✓	✓	✓
Modificar un destino	✓	✓	✓
Añadir un grupo	✓	✓	✓
Modificar un grupo	✓	✓	✓
Borrar destinos o grupos	✓	✓	✓
Borrar todos los destinos	✓	✓	–
Importar un archivo	✓	✓	–
Exportar a un archivo	✓	✓	–

* Inicie sesión como administrador para realizar ajustes.

Registro de un destino para contactos mediante Web Config

Nota:
También puede registrar contactos en el panel de control del escáner.

1. Acceda a Web Config y seleccione la pestaña **Digitalizar** > **Contactos**.
2. Seleccione el número que desea registrar y haga clic en **Editar**.
3. Introduzca un **Nombre** y una **Palabra índice**.
4. Seleccione el tipo de destino como valor de ajuste de **Tipo**.

   Nota:
   *Una vez completado el registro, no puede cambiarse la opción **Tipo**. Si quiere cambiar el tipo, borre el destino y regístrelo de nuevo.*
5. Introduzca un valor para cada elemento y, a continuación, haga clic en **Aplicar**.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Opciones de configuración de destino

Elementos	Ajustes y explicación
Ajustes comunes	
Nombre	Escriba el nombre mostrado en los contactos en 30 caracteres Unicode (UTF-8) o menos. Si no quiere especificarlo, déjelo en blanco.
Palabra índice	Introduzca un nombre con 30 caracteres o menos en Unicode (UTF-8) para buscar los contactos en el panel de control del escáner. Si no quiere especificarlo, déjelo en blanco.
Tipo	Seleccione el tipo de dirección que desea registrar.
Asignar a uso frecuente	Establezca la dirección registrada como una dirección de uso frecuente. Cuando establezca la dirección de uso frecuente, esta se mostrará en la parte superior de la pantalla y escaneado, de forma que podrá especificar el destino sin tener que mostrar todos los contactos.
Correo electrónico	
Dirección de correo	Escriba de 1 a 255 caracteres. Caracteres admitidos: A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.
Carpeta de redes (SMB)	
Guardar en	\\«Ruta de acceso a la carpeta» Introduzca la ubicación de la carpeta de destino empleando entre 1 y 253 caracteres Unicode (UTF-8), omitiendo «\\». Introduzca la ruta de red que se muestra en la pantalla de propiedades de la carpeta. Consulte lo que sigue para obtener detalles sobre cómo configurar la ruta de red. "Ejemplo de configuración para un ordenador personal" de la página 53
Nombre de usuario	Introduzca un nombre de usuario para acceder a la carpeta de red empleando 30 caracteres Unicode (UTF-8) o menos. No obstante, evite utilizar caracteres de control (0x00 a 0x1F, 0x7F).
Contraseña	Introduzca una contraseña para acceder a la carpeta de red de 20 caracteres Unicode (UTF-8) o menos. No obstante, evite utilizar caracteres de control (0x00 a 0x1F, 0x7F).
FTP	
Conexión segura	Seleccione FTP o FTPS en función del protocolo de transferencia de archivos del servidor FTP. Seleccione **FTPS** para que el escáner se pueda comunicar con las medidas de seguridad.
Guardar en	Introduzca el nombre del servidor, entre 1 y 253 caracteres en ASCII (0x20–0x7E), omitiendo «ftp://» o «ftps://».
Nombre de usuario	Introduzca un nombre de usuario para acceder al servidor FTP empleando 30 caracteres Unicode (UTF-8) o menos. No obstante, evite utilizar caracteres de control (0x00 a 0x1F, 0x7F). Si el servidor permite conexiones anónimas, introduzca un nombre de usuario (por ejemplo: Anónimo y FTP). Si no quiere especificarlo, déjelo en blanco.
Contraseña	Introduzca una contraseña para acceder al servidor FTP de 20 caracteres Unicode (UTF-8) o menos. No obstante, evite utilizar caracteres de control (0x00 a 0x1F, 0x7F). Si no quiere especificarlo, déjelo en blanco.

Elementos	Ajustes y explicación
Modo de conexión	Seleccione el modo de conexión desde el menú. Si se ha establecido un firewall entre el escáner y el servidor FTP, seleccione **Modo pasivo**.
Número de puerto	Introduzca el número de puerto del servidor FTP (entre 1 y 65535).
Validación de certificado	El certificado del servidor FTP se valida al habilitar esta opción. Esta opción está disponible si se selecciona **FTPS** para **Conexión segura**. Para configurarlo, debe importar el Certificado CA al escáner.
SharePoint(WebDAV)	
Conexión segura	Seleccione HTTP o HTTPS en función del protocolo de transferencia de archivos que admita el servidor. Seleccione **HTTPS** para que el escáner se pueda comunicar con las medidas de seguridad.
Guardar en	Introduzca el nombre del servidor, entre 1 y 253 caracteres en ASCII (0x20–0x7E), omitiendo «http://» o «https://».
Nombre de usuario	Introduzca un nombre de usuario para acceder al servidor empleando 30 caracteres Unicode (UTF-8) o menos. No obstante, evite utilizar caracteres de control (0x00 a 0x1F, 0x7F). Si no quiere especificarlo, déjelo en blanco.
Contraseña	Introduzca una contraseña para acceder al servidor de 20 caracteres Unicode (UTF-8) o menos. No obstante, evite utilizar caracteres de control (0x00 a 0x1F, 0x7F). Si no quiere especificarlo, déjelo en blanco.
Validación de certificado	El certificado del servidor se valida al habilitar esta opción. Esta opción está disponible si se selecciona **HTTPS** para **Conexión segura**. Para configurarlo, debe importar el Certificado CA al escáner.
Servidor proxy	Elija si quiere usar o no un servidor proxy.

Registro de destinos como un grupo mediante Web Config

Si el tipo de destino se establece en **Correo electrónico**, puede registrar los destinos como un grupo.

1. Acceda a Web Config y seleccione la pestaña **Digitalizar** > **Contactos**.
2. Seleccione el número que desea registrar y haga clic en **Editar**.
3. Seleccione un grupo desde **Tipo**.
4. Haga clic en **Seleccionar** para acceder a **Contact. para Grupo**.
   Se mostrarán los destinos disponibles.
5. Seleccione el destino que quiere registrar en el grupo y después haga clic en **Seleccionar**.
6. Introduzca un **Nombre** y una **Palabra índice**.
7. Seleccione si quiere o no quiere asignar el grupo registrado a los grupos de uso frecuente.

   Nota:
   Los destinos se pueden registrar en varios grupos.

8. Haga clic en **Aplicar**.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Copia de seguridad e importación de contactos

Mediante Web Config u otras herramientas, puede hacer copias de seguridad e importar contactos.

Para Web Config, puede hacer una copia de seguridad de los contactos exportando los ajustes del escáner que incluyen los contactos. El archivo exportado no se puede editar porque se exporta como archivo binario.

Al importar los ajustes del escáner al escáner, los contactos se sobrescriben.

En el caso de Epson Device Admin, solo pueden exportarse los contactos desde la pantalla de propiedades del dispositivo. Además, si no exporta los elementos relacionados con la seguridad, puede editar los contactos exportados y volver a importarlos porque puede guardarse como archivo SYLK o CSV.

Importar contactos mediante Web Config

Si tiene un escáner que le permite realizar una copia de seguridad de los contactos y es compatible con este escáner, puede registrar fácilmente los contactos importando el archivo de la copia de seguridad.

Nota:
Para obtener instrucciones sobre cómo hacer una copia de seguridad de los contactos del escáner, consulte el manual que se proporciona con este.

Siga los pasos a continuación para importar los contactos a este escáner.

1. Acceda a Web Config y seleccione la pestaña **Gestión del dispositivo** > **Exportar e importar valor de configuración** > **Importar**.

2. Seleccione el archivo de copia de seguridad que creó en **Archivo**, introduzca la contraseña y haga clic en **Siguiente**.

3. Active la casilla de verificación **Contactos** y, a continuación, haga clic en **Siguiente**.

Realizar copias de seguridad de contactos mediante Web Config

Los datos de los contactos pueden perderse debido a un mal funcionamiento del escáner. Es aconsejable hacer una copia de seguridad de los datos siempre que se modifiquen. Epson no se responsabilizará de la pérdida de ningún dato, de la copia de seguridad ni de la recuperación de datos y/o ajustes durante el periodo de garantía.

Usando Web Config, puede hacer copias de seguridad en el ordenador de los datos de contacto almacenados en el escáner.

1. Acceda a Web Config y luego seleccione la pestaña **Gestión del dispositivo** > **Exportar e importar valor de configuración** > **Exportar**.

2. Active la casilla de verificación **Contactos** de la categoría **Digitalizar**.

3. Escriba una contraseña para cifrar el archivo exportado.

   Necesita la contraseña para importar el archivo. Deje esto en blanco si no desea cifrar el archivo.

4. Haga clic en **Exportar**.

Cómo exportar y registrar en bloque contactos mediante herramientas

Si utiliza Epson Device Admin, puede hacer una copia de seguridad únicamente de los contactos y editar los archivos exportados para luego registrarlos todos a la vez.

Puede resultarle útil si desea hacer una copia de seguridad únicamente de los contactos o quiere sustituir el escáner pero desea transferir los contactos del antiguo al nuevo.

Exportación de contactos

Guarde la información de los contactos en el archivo.

Puede editar los archivos guardados en formato SYLK o csv mediante una aplicación de hojas de cálculo o un procesador de textos. Puede registrar todos los contactos a la vez después de borrar o añadir la información.

La información que incluya datos de seguridad como contraseñas o información personal puede guardarse en formato binario con una contraseña. No puede editar el archivo. Puede usarse como archivo de copia de seguridad de la información, incluyendo los datos de seguridad.

1. Inicie Epson Device Admin.

2. Seleccione **Dispositivos** en la barra de tareas lateral del menú.

3. Seleccione en la lista de dispositivos el que desea configurar.

4. Haga clic en **Configuración del dispositivo** en la pestaña **Inicio** de la barra de menú.

   Cuando se haya configurado la contraseña del administrador, escríbala y haga clic en **Aceptar**.

5. Haga clic en **Comunes** > **Contactos**.

6. Seleccione el formato de exportación en **Exportar** > **Exportar elementos**.

   ❏ Todos los elementos

   Exporte el archivo binario cifrado. Seleccione esta opción cuando quiera incluir datos de seguridad como contraseñas o información personal. No puede editar el archivo. Si la selecciona, tendrá que configurar la contraseña. Haga clic en **Configuración** y configure una contraseña de entre 8 y 63 caracteres ASCII. Necesitará esta contraseña para importar el archivo binario.

   ❏ Elementos, excepto información de seguridad

   Exporte los archivos en formato SYLK o en formato csv. Seleccione esta opción cuando quiera editar la información del archivo exportado.

7. Haga clic en **Exportar**.

8. Especifique la ubicación en la que quiere guardar el archivo, seleccione el tipo de archivo y, a continuación, haga clic en **Guardar**.

   Aparecerá un mensaje para confirmar que se ha completado la operación.

9. Haga clic en **Aceptar**.

   Compruebe que el archivo se ha guardado en la ubicación especificada.

Cómo importar contactos

Importe la información de los contactos desde el archivo.

Puede importar los archivos guardados en formato SYLK o csv, o el archivo binario de la copia de seguridad que incluye los datos de seguridad.

1. Inicie Epson Device Admin.

2. Seleccione **Dispositivos** en la barra de tareas lateral del menú.

3. Seleccione en la lista de dispositivos el que desea configurar.

4. Haga clic en **Configuración del dispositivo** en la pestaña **Inicio** de la barra de menú.

   Cuando se haya configurado la contraseña del administrador, escríbala y haga clic en **Aceptar**.

5. Haga clic en **Comunes** > **Contactos**.

6. Haga clic en **Examinar** en **Importar**.

7. Seleccione el archivo que desee importar y haga clic en **Abrir**.

   Si selecciona el archivo binario, escriba en **Contraseña** la contraseña que haya configurado al exportar el archivo.

8. Haga clic en **Importar**.

   Se muestra la pantalla de confirmación.

9. Haga clic en **Aceptar**.

   Se mostrará el resultado de la validación.

   ❏ Editar la información cargada

   Haga clic cuando desee editar la información de manera individual.

   ❏ Cargar más archivos

   Haga clic cuando desee importar varios archivos.

10. Haga clic en **Importar** y, a continuación, haga clic en **Aceptar** en la pantalla de finalización de la importación.

    Vuelva a la pantalla de propiedades del dispositivo.

11. Haga clic en **Transmitir**.

12. Haga clic en **Aceptar** en el mensaje de confirmación.

    Los ajustes se envían al escáner.

13. Cuando aparezca la pantalla de finalización del envío, haga clic en **Aceptar**.

    La información del escáner se actualiza.

    Abra los contactos desde Web Config o desde el panel de control del escáner y luego compruebe que el contacto se ha actualizado.

Cooperación entre el servidor LDAP y los usuarios

Durante la cooperación con el servidor LDAP, puede utilizar la dirección registrada en el servidor LDAP como destinataria de los correos electrónicos.

Configuración del servidor LDAP

Para utilizar la información del servidor LDAP, regístrelo en el escáner.

1. Acceda a Web Config y seleccione la pestaña **Red** > **Servidor LDAP** > **Básica**.

2. Introduzca un valor para cada opción.

3. Seleccione **Aceptar**.

   Se mostrarán los ajustes que ha seleccionado.

Opciones de configuración del servidor LDAP

Elementos	Ajustes y explicación
Usar serv. LDAP	Seleccione **Uso** o **No usar**.
Dirección serv. LDAP	Introduzca la dirección del servidor LDAP. Escriba entre 1 y 255 caracteres en formato IPv4, IPv6 o FQDN. Para el formato FQDN puede utilizar caracteres alfanuméricos ASCII (0x20–0x7E) y «-» excepto al principio y al final de la dirección.
Nº puerto serv. LDAP	Introduzca el número de puerto del servidor LDAP entre 1 y 65535.
Conexión segura	Especifique el método de autenticación cuando el escáner accede al servidor LDAP.
Validación de certificado	Si habilita esta opción, se valida el certificado del servidor LDAP. Le recomendamos que lo configure como **Activar**. Para configurarlo, los **Certificado CA** deben ser importados al escáner.
Tiempo espera búsqueda (seg.)	Establezca el tiempo (entre 5 y 300) que debe pasar antes de que exceda el límite de tiempo al realizar una búsqueda.

Elementos	Ajustes y explicación
Método de autenticación	Seleccione uno de los métodos. Si selecciona **Autenticación Kerberos**, seleccione **Config. Kerberos** configurar Kerberos. Para realizar la Autenticación Kerberos es necesario el siguiente entorno. ❏ El escáner y el servidor DNS pueden comunicarse entre sí. ❏ La hora del escáner, el servidor KDC y el servidor necesario para la autenticación (servidor LDAP, servidor SMTP, servidor de archivos) están sincronizados. ❏ Si el servidor de servicio se asigna como la dirección IP, el FQDN del servidor de servicio se registra en la zona de búsqueda inversa del servidor DNS.
Dominio kerberos para utilizar	Si selecciona **Autenticación Kerberos** como **Método de autenticación**, seleccione el dominio Kerberos que quiera utilizar.
DN de administrador / Nombre de usuario	Escriba el nombre de usuario para el servidor LDAP en 128 caracteres Unicode (UTF-8) o menos. No pueden utilizarse caracteres de control tales como 0x00–0x1F y 0x7F. Este ajuste no se puede utilizar cuando se ha seleccionado **Autenticación anónima** como **Método de autenticación**. Si no quiere especificarlo, déjelo en blanco.
Contraseña	Introduzca la contraseña de autenticación del servidor LDAP en 128 caracteres Unicode (UTF-8) o menos. No pueden utilizarse caracteres de control tales como 0x00–0x1F y 0x7F. Este ajuste no se puede utilizar cuando se ha seleccionado **Autenticación anónima** como **Método de autenticación**. Si no quiere especificarlo, déjelo en blanco.

Configuración del protocolo Kerberos

Si selecciona **Autenticación Kerberos** para **Método de autenticación** de **Servidor LDAP** > **Básica**, configure Kerberos de la siguiente manera desde la pestaña **Red** > **Config. Kerberos**. Puede registrar hasta 10 ajustes de configuración del protocolo Kerberos.

Elementos	Ajustes y explicación
Dominio Kerberos	Introduzca el dominio de la autenticación Kerberos en 255 caracteres ASCII (0x20–0x7E) o menos. Si no quiere registrarlo, déjelo en blanco.
Dirección KDC	Introduzca la dirección del servidor de autenticación Kerberos. Escriba 255 caracteres o menos en formato IPv4, IPv6 o FQDN. Si no quiere registrarlo, déjelo en blanco.
Número de puerto (kerberos)	Introduzca el número de puerto del servidor Kerberos entre 1 y 65535.

Configuración de los ajustes de búsqueda del servidor LDAP

Cuando configure los ajustes de búsqueda, puede utilizar la dirección de correo electrónico registrada en el servidor LDAP.

1. Acceda a Web Config y seleccione la pestaña **Red** > **Servidor LDAP** > **Buscar config.**.

2. Introduzca un valor para cada opción.

3. Haga clic en **Aceptar** para mostrar la configuración resultante.

   Se mostrarán los ajustes que ha seleccionado.

Elementos de configuración de búsqueda del servidor LDAP

Elementos	Ajustes y explicación
Base búsqueda (nombre distinguido)	Si quiere buscar un dominio arbitrario, especifique el nombre de dominio del servidor LDAP. Introduzca entre 0 y 128 caracteres Unicode (UTF-8). Si no quiere realizar una búsqueda de un atributo arbitrario, deje este espacio en blanco. Ejemplo para el directorio del servidor local: dc=server,dc=local
Nº de entradas de búsqueda	Especifique el número de entradas de búsqueda, entre 5 y 500. El número de entradas establecido se guarda y muestra temporalmente. La búsqueda se podrá realizar aunque aparezca un error indicando que el número de entradas de búsqueda supera el número especificado.
Atributo nombre de usuario	Especifique el nombre del atributo a mostrar cuando realice una búsqueda de nombres de usuario. Introduzca entre 1 y 255 caracteres Unicode (UTF-8). El primer carácter debería ser a–z o A–Z. Ejemplo: cn, uid
Atributo visual. nombre de usuario	Especifique el nombre del atributo a mostrar como nombre de usuario. Introduzca entre 0 y 255 caracteres Unicode (UTF-8). El primer carácter debería ser a–z o A–Z. Ejemplo: cn, sn
Atributo dirección de correo electrónico	Especifique el nombre del atributo a mostrar cuando realice una búsqueda de direcciones de correo electrónico. Escriba una combinación entre 1 y 255 caracteres. Caracteres admitidos: A–Z, a–z, 0–9 y -. El primer carácter debería ser a–z o A–Z. Ejemplo: mail
Atributo arbitrario 1 - Atributo arbitrario 4	Puede especificar otros atributos arbitrarios para realizar la búsqueda. Introduzca entre 0 y 255 caracteres Unicode (UTF-8). El primer carácter debería ser a–z o A–Z. Si no quiere realizar una búsqueda de un atributo arbitrario, deje este espacio en blanco. Ejemplo: o, ou

Comprobación de la conexión del servidor LDAP

Ejecuta una prueba de conexión del servidor LDAP según los parámetros establecidos en **Servidor LDAP** > **Buscar config.**.

1. Acceda a Web Config y seleccione la pestaña **Red** > **Servidor LDAP** > **Prueba de conex.**.

2. Seleccione **Iniciar**.

   La prueba de conexión comenzará. Cuando termine la prueba, se mostrará el informe.

Referencias de la prueba de conexión del servidor LDAP

Mensajes	Explicación
Prueba de conexión correcta.	Este mensaje aparece si la conexión con el servidor es satisfactoria.
Error en prueba de conex. Comprobar config.	Este mensaje aparece por las siguientes razones: ❏ La dirección del servidor LDAP o el número de puerto son incorrectos. ❏ Se ha excedido el límite de tiempo. ❏ La opción **No usar** está seleccionada como **Usar serv. LDAP**. ❏ Si se ha seleccionado la **Autenticación Kerberos** como el **Método de autenticación**, ajustes como **Dominio Kerberos**, **Dirección KDC** y **Número de puerto (kerberos)** serán incorrectos.
Error en prueba de conex. Compruebe la fecha y hora en su producto o en el servidor.	Este mensaje aparece cuando la conexión falla porque los ajustes de tiempo del escáner y del servidor LDAP no coinciden.
Error de autenticación. Comprobar config.	Este mensaje aparece por las siguientes razones: ❏ El **Nombre de usuario** y/o la **Contraseña** son incorrectos. ❏ Si se selecciona **Autenticación Kerberos** como **Método de autenticación**, es posible que la hora/fecha no estén configuradas.
No se puede acceder al producto hasta que el proceso se haya completado.	Este mensaje aparece cuando el escáner está ocupado.

Uso de Document Capture Pro Server

Mediante el uso de Document Capture Pro Server, puede administrar el método de clasificación, el formato de guardado y el destino de reenvío de un resultado de escaneado ejecutado desde el panel de control del escáner. Puede llamar y ejecutar un trabajo previamente registrado en el servidor desde el panel de control del escáner.

Instálelo en el ordenador del servidor.

Para obtener más información sobre Document Capture Pro Server, póngase en contacto con la oficina local de Epson.

Configuración del modo de servidor

Para usar Document Capture Pro Server, configure de la siguiente manera.

1. Acceda a Web Config y seleccione la pestaña **Digitalizar** > **Document Capture Pro**.

2. Seleccione **Modo Servidor** para **Modo**.

3. Introduzca la dirección del servidor con Document Capture Pro Server instalado en el mismo para **Dirección del servidor**.

   Escriba entre 2 y 255 caracteres de uno de estos formatos: IPv4, IPv6, nombre de host o FQDN. Para el formato FQDN se admiten los caracteres alfanuméricos ASCII (0x20–0x7E) y el «-» excepto al principio y al final de la dirección.

4. Haga clic en **Aceptar**.

   La red se vuelve a conectar y entonces se activan los ajustes.

Configuración de AirPrint

Acceda a Web Config, seleccione la pestaña **Red** y seleccione **Configuración de AirPrint**.

Elementos	Explicación
Nombre servic. Bonjour	Introduzca el nombre del servicio Bonjour usando texto ASCII (0x20–0x7E), máximo de 41 caracteres.
Ubicación de Bonjour	Introduzca una descripción de la ubicación del escáner, usando texto Unicode (UTF-8), máximo de 127 bytes.
Wide-Area Bonjour	Establece si se va a utilizar o no Bonjour de área extensa. Si lo utiliza, el escáner debe estar registrado en el servidor DNS para poder buscar el escáner en el segmento.
Activar AirPrint	Bonjour y AirPrint (servicio de escaneado) están habilitados.

Problemas al preparar el escaneado a través de la red

Consejos para resolución de problemas

❏ Comprobación de mensajes de error

Si hay algún problema, primero compruebe si hay algún mensaje en el panel de control del escáner o en la pantalla del controlador. Si tiene configurada la opción de recibir notificaciones por correo electrónico cuando se producen errores, podrá conocer enseguida el estado.

❏ Comprobación del estado de la comunicación

Compruebe el estado de la comunicación del ordenador servidor o del equipo cliente con un comando Ping o ipconfig.

❏ Prueba de conexión

Para comprobar la conexión entre el escáner y el servidor de correo, realice la prueba de conexión desde el escáner. Compruebe también la conexión entre el equipo cliente y el servidor para conocer el estado de la comunicación.

❏ Inicialización de la configuración

Si no encuentra ningún problema ni en la configuración ni en el estado de la comunicación, es posible que pueda solucionar los problemas deshabilitando o inicializando los ajustes de red del escáner y, después, configurándolos de nuevo.

No se puede acceder a Web Config

No se ha asignado una dirección IP al escáner.

Soluciones

Puede que no se haya asignado una dirección IP válida al escáner. Configure la dirección IP con el papel de control del escáner. Puede confirmar la información de la configuración actual desde el panel de control del escáner.

El navegador web no admite la potencia de cifrado para SSL/TLS.

Soluciones

SSL/TLS tiene Intensidad de cifrado. Puede abrir Web Config mediante un navegador web que admita cifrados masivos, como se indica a continuación. Compruebe que está utilizando un navegador que sea compatible.

- ❏ 80 bits: AES256/AES128/3DES
- ❏ 112 bits: AES256/AES128/3DES
- ❏ 128 bits: AES256/AES128
- ❏ 192 bits: AES256
- ❏ 256 bits: AES256

Certificado firmado CA ha expirado.

Soluciones

Si hay un problema con la fecha de expiración del certificado, se mostrará «El certificado ha expirado» al conectarse Web Config con comunicación SSL/TLS (https). Si el mensaje aparece antes de la fecha de e, asegúrese de que la fecha del escáner esté bien configurada.

El nombre común del certificado y el del escáner no coinciden.

Soluciones

Si el nombre común del certificado y el del escáner no coinciden, aparecerá el mensaje «El nombre del certificado de seguridad no coincide···» cuando acceda a Web Config mediante una comunicación SSL/TLS (https). Esto sucede porque las siguientes direcciones IP no coinciden.

- ❏ La dirección IP del escáner introducida como nombre común para crear un Certificado auto-firmado o un CSR
- ❏ La dirección IP introducida en el navegador web al ejecutar Web Config

Para Certificado auto-firmado, actualice el certificado.

En el caso del Certificado firmado CA, obtenga de nuevo el certificado para el escáner.

La configuración del servidor proxy de la dirección local no se ha establecida en el navegador web.

Soluciones

Si el escáner está configurado para usar un servidor proxy, configure el navegador web para que no se conecte a la dirección local a través del servidor proxy.

❏ Windows:

Seleccione **Panel de control** > **Redes e Internet** > **Opciones de Internet** > **Conexiones** > **Configuración LAN** > **Servidor proxy** y, a continuación, realice la configuración de forma que no se use el servidor para la LAN (direcciones locales).

❏ Mac OS:

Seleccione **Preferencias del sistema** > **Red** > **Avanzado** > **Proxies** y, a continuación, registre la dirección local para **Omitir ajustes de proxy para estos hosts y dominios**.

Ejemplo:

192.168.1.*: Dirección local 192.168.1.XXX, máscara de subred 255.255.255.0

192.168.*.*: Dirección local 192.168.XXX.XXX, máscara de subred 255.255.0.0

DHCP está desactivado en la configuración del ordenador.

Soluciones

Si el DHCP para obtener una dirección IP automáticamente está deshabilitado en el ordenador, no podrá acceder a Web Config. Habilite DHCP.

Ejemplo para Windows 10:

Abra el Panel de control y, a continuación, haga clic en **Red e Internet** > **Centro de redes y recursos compartidos** > **Cambiar configuración del adaptador**. Abra la pantalla Propiedades de la conexión que está utilizando y, a continuación, la pantalla de propiedades para **Protocolo de Internet versión 4 (TCP/IPv4)** o **Protocolo de Internet versión 6 (TCP/IPv6)**. Compruebe que esté seleccionado **Obtener una dirección IP automáticamente** en la pantalla que se muestra.

Personalización de la pantalla del panel de control

Registro de Ajustes

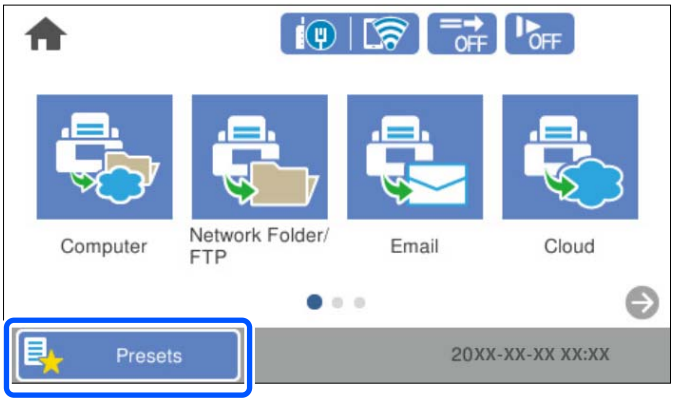
Puede registrar la configuración de escaneado más frecuente como **Ajustes**. Puede registrar hasta 48 predeterminados.

Nota:

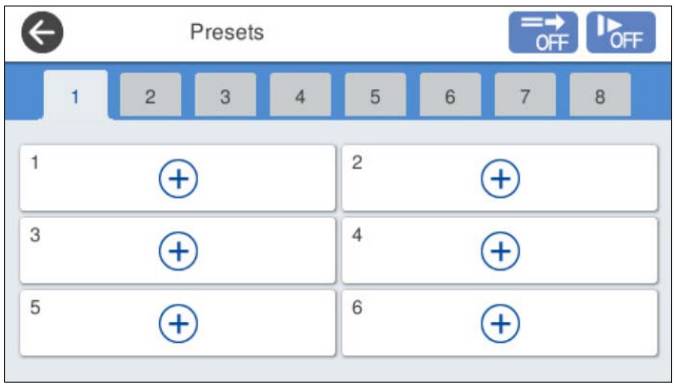
- *Puede registrar los ajustes actuales seleccionando* ☆ *en la pantalla de configuración de escaneado.*
- *También puede registrar* ***Ajustes*** *en Web Config.*

  Seleccione la pestaña ***Digitalizar*** *>* ***Ajustes****.*
- *Si selecciona* ***Digitalizar a PC*** *al registrarse, puede registrar el trabajo creado en Document Capture Pro como* ***Ajustes****. Esta opción está disponible solo para ordenadores conectados a través de una red. Registre de antemano el trabajo en Document Capture Pro.*
- *Si la función de autenticación está habilitada, solo el administrador puede registrar* ***Ajustes****.*

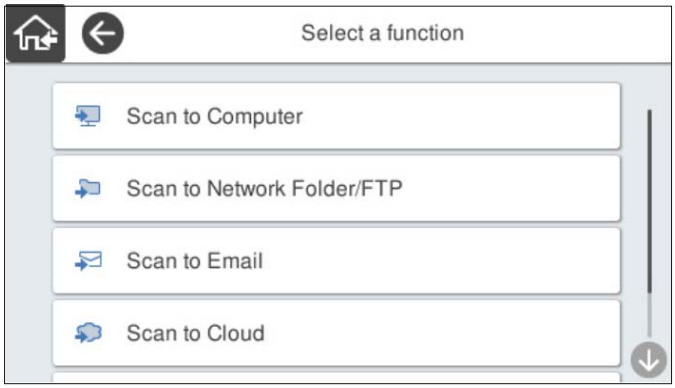
1. Seleccione **Ajustes** en la pantalla de inicio del panel de control del escáner.



2. Seleccione ⊕.



3. Seleccione el menú que desee utilizar para registrar un preajuste.



4. Configure cada elemento y seleccione ☆+.

Nota:
*Si selecciona **Digitalizar a PC**, seleccione el ordenador en el que está instalado Document Capture Pro y, a continuación, seleccione un trabajo registrado. Esta opción está disponible solo para ordenadores conectados a través de una red.*

5. Configure el preajuste.

- ❏ **Nombre**: indique el nombre.
- ❏ **Establecer Icono**: configure la imagen y el color del icono mostrar.
- ❏ **Configuración de Envío rápido**: inicia inmediatamente el escaneado sin necesidad de confirmarlo al seleccionar el preajuste.

  Si utiliza Document Capture Pro Server, incluso si configura el software para que confirme el contenido de un trabajo antes de escanear, **Configuración de Envío rápido**, en la configuración predeterminada del escáner, tiene prioridad sobre el software.
- ❏ **Contenido**: compruebe la configuración de escaneado.

6. Seleccione **OK**.

Opciones del menú de Ajustes

Puede cambiar la configuración de los preajustes seleccionando › en cada uno de ellos.

Cambiar nombre:

cambia el nombre del preajuste.

Cambiar Icono:

cambia la imagen del icono y el color del preajuste.

Configuración de Envío rápido:

inicia inmediatamente el escaneado sin necesidad de confirmarlo al seleccionar el preajuste.

Cambiar posición:

cambia el orden de visualización de los preajustes.

Eliminar:

elimina el preajuste.

Agregar o quitar Icono en Inicio:

añade o elimina el icono del preajuste de la pantalla de inicio.

Confirme los detalles:

ver la configuración de un preajuste. Puede cargar el preajuste seleccionando **Usar esta configuración**.

Edición de la pantalla de inicio del panel de control

Puede personalizar la pantalla de inicio seleccionando **Configuración** > **Editar inicio** en el panel de control del escáner.

- ❏ Diseño: cambia el método de visualización de los iconos del menú.
  "Modificación de Diseño de la pantalla de inicio" de la página 80
- ❏ Agregar icono: añade iconos a los ajustes de **Ajustes** que ha realizado o restaura los iconos que se han eliminado de la pantalla.
  "Agregar icono" de la página 81
- ❏ Quitar icono: quita los iconos de la pantalla de inicio.
  "Quitar icono" de la página 82
- ❏ Mover icono: cambia el orden de visualización de los iconos.
  "Mover icono" de la página 83
- ❏ Restaurar visualización de icono pred.: restaura la configuración de visualización predeterminada de la pantalla de inicio.
- ❏ Fondo de pantalla: cambia el color del fondo de la pantalla.

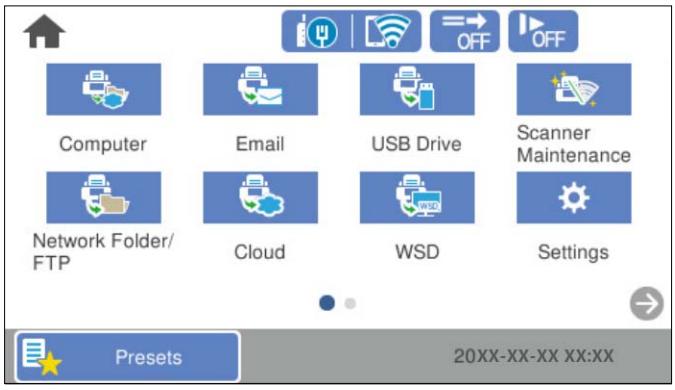
Modificación de Diseño de la pantalla de inicio

1. Seleccione **Configuración** > **Editar inicio** > **Diseño** en el panel de control del escáner.

2. Seleccione **Línea** o **Matriz**.

   Línea:

   Matriz:



3. Seleccione  para volver y comprobar la pantalla de inicio.

Agregar icono

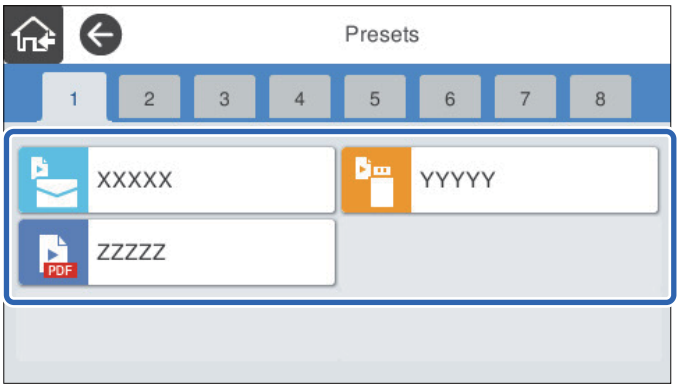
1. Seleccione **Configuración** > **Editar inicio** > **Agregar icono** en el panel de control del escáner.

2. Seleccione **Función** o **Ajustes**.

   ❏ Función: muestra las funciones predeterminadas que aparecen en la pantalla de inicio.

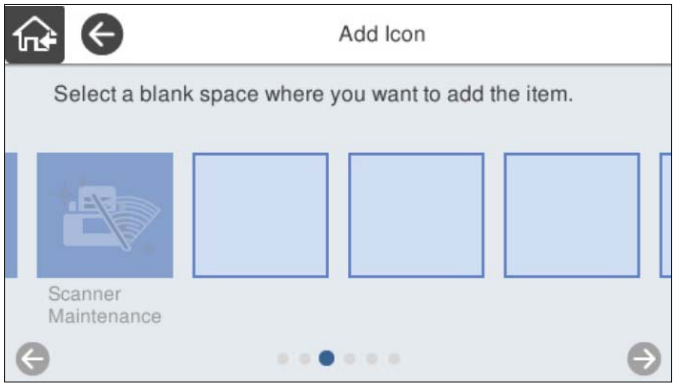
❏ Ajustes: muestra los preajustes registrados.

3. Seleccione el elemento que desea añadir a la pantalla de inicio.



4. Seleccione el espacio en blanco donde desea añadir el elemento.

   Si desea añadir varios iconos, repita los pasos 3 y 4.

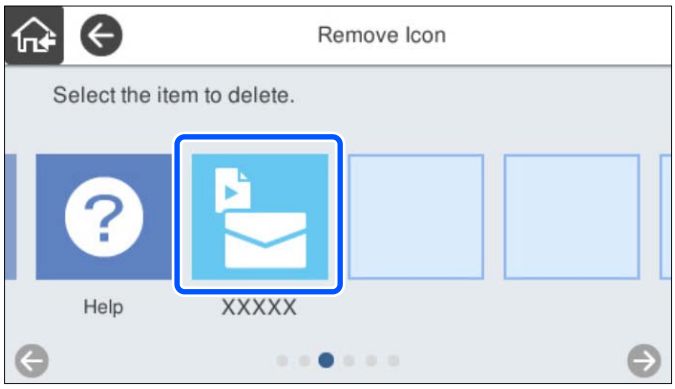


5. Seleccione  para volver y comprobar la pantalla de inicio.

Quitar icono

1. Seleccione **Configuración** > **Editar inicio** > **Quitar icono** en el panel de control del escáner.

2. Seleccione el icono que desea eliminar.



3. Seleccione **Sí** para finalizar.

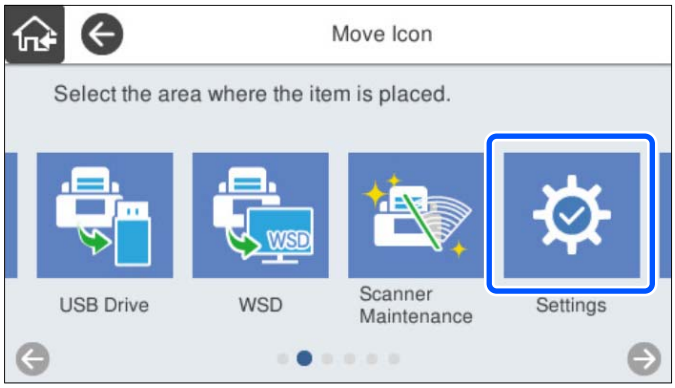
   Si desea eliminar varios iconos, repita los pasos 2 y 3.

4. Seleccione  para volver y comprobar la pantalla de inicio.

Mover icono

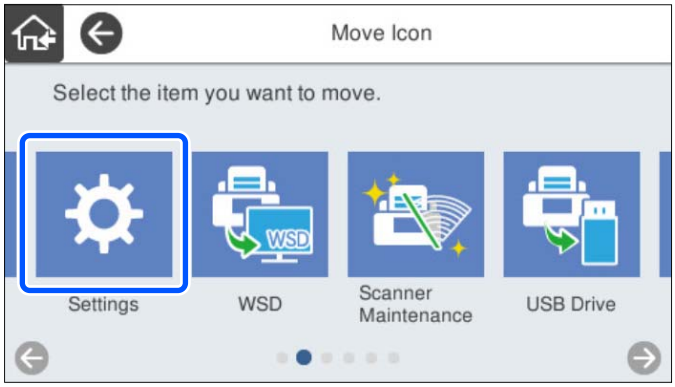
1. Seleccione **Configuración** > **Editar inicio** > **Mover icono** en el panel de control del escáner.

2. Seleccione el icono que desea mover.



3. Seleccione el marco de destino.

   Si ya hay otro icono en el marco de destino, el icono se sustituye.



4. Seleccione  para volver y comprobar la pantalla de inicio.

Configuración de seguridad básica

Introducción a las funciones de seguridad del producto

Esta sección presenta la función de seguridad de los dispositivos Epson.

Nombre de función	Tipo de función	Qué configurar	Qué evitar
Configuración de la contraseña de administrador	Bloquea la configuración del sistema, como la configuración de conexión de red o USB.	Un administrador establece una contraseña para el dispositivo. Puede establecerla o modificarla tanto desde Web Config como desde el panel de control del escáner.	Evita la lectura y alteración ilegal de la información almacenada en el dispositivo, como identificadores, contraseñas, la configuración de red, etc. Además, reduce una amplia variedad de riesgos de seguridad, tales como la fuga de información del entorno de red o la política de seguridad.
Configuración de la interfaz externa	Controla la interfaz que conecta con el dispositivo.	Habilite o deshabilite la conexión USB con el ordenador.	Conexión USB del ordenador: evita el uso no autorizado del dispositivo prohibiendo escanear a no ser que sea a través de la red.

Información relacionada

➡ "Configurar la contraseña del administrador" de la página 86
➡ "Deshabilitación de la interfaz externa" de la página 92

Configuración de administrador

Configurar la contraseña del administrador

Si configura la contraseña de administrador puede evitar que los usuarios cambien la configuración de la administración del sistema. Los valores predeterminados se establecen en el momento de la compra. Puede cambiarlos en caso necesario.

Nota:
A continuación se proporcionan los valores predeterminados para la información del administrador.

❏ *Nombre de usuario (se utiliza solo para Web Config): ninguno (en blanco)*

❏ *Contraseña: número de serie del escáner*

Para encontrar el número de serie, compruebe la etiqueta pegada en la parte posterior del escáner.

Puede cambiar la contraseña de administrador mediante Web Config, el panel de control del escáner o Epson Device Admin. Si utiliza Epson Device Admin, consulte el manual o la ayuda Epson Device Admin.

Cambio de la contraseña de administrador mediante Web Config

Cambie la contraseña de administrador en Web Config.

1. Acceda a Web Config y seleccione la pestaña **Seguridad del producto** > **Cambiar contraseña administrador**.

2. Introduzca la información necesaria en **Contraseña actual**, **Nombre de usuario**, **Contraseña nueva** y **Confirme la contraseña nueva**.

   Introduzca al menos un carácter para la nueva contraseña.

   Nota:
   A continuación se proporcionan los valores predeterminados para la información del administrador.

   ❏ *Nombre de usuario: ninguno (en blanco)*

   ❏ *Contraseña: número de serie del escáner*

   Para encontrar el número de serie, compruebe la etiqueta pegada en la parte posterior del escáner.

   > ***Importante:***
   > *Asegúrese de recordar la contraseña del administrador configurada. Si la olvida, no podrá restablecerla y deberá solicitar ayuda al personal del servicio técnico.*

3. Seleccione **Aceptar**.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Cambio de la contraseña del administrador desde el panel de control

Desde el panel de control del escáner se puede cambiar la contraseña del administrador.

1. Seleccione **Configuración** en el panel de control del escáner.

2. Seleccione **Admin. del sistema** > **Configuración admin.**.

3. Seleccione **Contraseña admin** > **Cambiar**.

4. Introduzca su contraseña actual.

   Nota:
   El ajuste en el momento de la compra (valor predeterminado) de la contraseña del administrador es el número de serie del escáner.

   Para encontrar el número de serie, compruebe la etiqueta pegada en la parte posterior del escáner.

5. Introduzca la nueva contraseña.

   Introduzca al menos un carácter.

> ***Importante:***
> *Asegúrese de recordar la contraseña del administrador configurada. Si la olvida, no podrá restablecerla y deberá solicitar ayuda al personal del servicio técnico.*

6. Introduzca otra vez la nueva contraseña para confirmarla.

Se muestra un mensaje de finalización.

Uso de Configuración bloqueo para el panel de control

Puede usar Configuración bloqueo para bloquear el panel de control y evitar que los usuarios cambien aspectos relacionados con la configuración del sistema.

Nota:
Si habilita Configuración de autenticación en el escáner, Configuración bloqueo también estará habilitado para el panel de control. El panel de control no se puede desbloquear si Configuración de autenticación está habilitado.

Aunque deshabilite Configuración de autenticación, Configuración bloqueo permanece habilitado. Si desea deshabilitarlo, puede realizar los ajustes desde el panel de control o Web Config.

Ajuste de Configuración bloqueo desde el panel de control

1. Si desea cancelar **Configuración bloqueo** después de haberse habilitado, toque en la esquina superior derecha de la pantalla de inicio para iniciar sesión como administrador.

   no se muestra si **Configuración bloqueo** está deshabilitado. Si desea habilitar este ajuste, vaya al paso siguiente.

2. Seleccione **Configuración**.

3. Seleccione **Admin. del sistema** > **Configuración admin.**.

4. Seleccione **Activ.** o **Desa** como **Configuración bloqueo**.

Configuración de Configuración bloqueo desde Web Config

1. Seleccione la pestaña **Gestión del dispositivo** > **Panel de control**.

2. Seleccione **ACT.** o **DESACT.** para **Bloqueo del panel**.

3. Haga clic en **Aceptar**.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Elementos de Configuración bloqueo en el menú Configuración

Esta es una lista de los elementos bloqueados en el menú **Configuración** del el panel de control por Configuración bloqueo.

✓: para bloquear.

- : para no bloquear.

Menú Configuración		**Configuración bloqueo**
Config. básica		-
	Brillo LCD	-
	Sonidos	-
	Tempor apagado	✓
	Temp. apagado autom.	✓
	Conf. de fecha y hora	✓
	Idioma/Language	✓/-*
	Teclado (Es posible que esta función no esté disponible en su región.)	-
	Agotado tiempo func.	✓
	Conex. PC a través USB	✓
	Encendido directo	✓
Configuración del escáner		-
	Len	-
	Tiempo de parada de doble aliment.	✓
	Función DFDS	-
	Prot. del papel	✓
	Detección de suciedad en el cristal	✓
	Detec. ultrasónica doble inserción	✓
	Tiempo de espera de Modo Alimentación automática	✓
	Confirmar destinatario	✓
Editar inicio		✓

Menú Configuración		**Configuración bloqueo**
	Diseño	✓
	Agregar icono	✓
	Quitar icono	✓
	Mover icono	✓
	Restaurar visualización de icono pred.	✓
	Fondo de pantalla	✓
Configuración del usuario		✓
	Carpeta de red/FTP	✓
	Correo electr.	✓
	Nube	✓
	Unidad USB	✓
Configuración de red		✓
	Config. Wi-Fi	✓
	Configuración LAN cableada	✓
	Estado de la red	✓
	Avanzado	✓
Configuración del servicio web		✓
	Servicios Epson Connect	✓
Document Capture Pro		-
	Cambiar configuración	✓
Administrador de Contactos		-
	Registrar/Eliminar	✓/-*
	Frecuente	-
	Ver opciones	-
	Opciones de búsqueda	-
Admin. del sistema		✓

Menú Configuración			Configuración bloqueo
	Administrador de Contactos		✓
	Configuración admin.		✓
	Restricciones		✓
	Cifrado con contraseña		✓
	Investigación del cliente		✓
	Configuración WSD		✓
	Restaurar configuración pred.		✓
	Actualización de firmware		✓
Información del dispositivo			-
	Número de serie		-
	Versión actual		-
	Número total de digitalizaciones		-
	Nº digitaliz. a una sola cara		-
	Nº digitaliz. a doble cara		-
	Nº digitaliz. hoja portadora		-
	Digitalizac. tras sustituir el rodillo		-
	Digit. tras limpieza convencional		-
	Restablecer el número de digitalizaciones		✓
Mantenimiento del escáner			-
	Limpieza de rodillos		-
	Sustitución del rodillo		-
		Restablecer el número de digitalizaciones	✓
		Cómo llevar a cabo la sustitución	-
	Limpieza convencional		-
		Restablecer el número de digitalizaciones	✓
		Cómo limpiar	-
	Limpieza del cristal		-
Configuración de alerta de sustitución del rodillo			✓
	Conf. recuento alertas		✓
Ajustes de alerta de limpieza periódica			✓

Menú Configuración		Configuración bloqueo
	Ajustes de alerta de advertencia	✓
	Conf. recuento alertas	✓

* Puede establecer si desea permitir que se realcen cambios en **Admin. del sistema** > **Restricciones**.

Iniciar sesión como administrador desde el panel de control

Puede utilizar cualquiera de los siguientes métodos para iniciar sesión como administrador desde el panel de control del escáner.

1. Toque  en la parte superior derecha de la pantalla.
   - ❏ Si Configuración de autenticación está habilitado, el icono se muestra en la pantalla **Bienvenido** (pantalla de espera de autenticación).
   - ❏ Si Configuración de autenticación está deshabilitado, el icono se muestra en la pantalla de inicio.
2. Toque **Sí** cuando aparezca la pantalla de confirmación.
3. Escriba la contraseña de administrador.

   Se muestra un mensaje que indica que el inicio de sesión se ha realizado y, a continuación, la pantalla de inicio del panel de control.

Para cerrar sesión, toque  en la parte superior derecha de la pantalla de inicio.

Deshabilitación de la interfaz externa

Puede deshabilitar la interfaz utilizada para conectar el dispositivo al escáner. Configure la restricción para limitar el escaneado para que no realice a través de la red.

Nota:
También puede configurar la restricción en el panel de control del escáner.

Conex. PC a través USB: ***Configuración*** > ***Config. básica*** > ***Conex. PC a través USB***

1. Acceda a Web Config y seleccione la pestaña **Seguridad del producto** > **Interfaz externa**.
2. Seleccione **Desactivar** en las funciones que desee establecer.

   Seleccione **Activar** si desea cancelar el control.

   Conex. PC a través USB

   Puede restringir el uso de la conexión USB desde el equipo. Si desea restringirlo, seleccione **Desactivar**.
3. Haga clic en **Aceptar**.

4. Compruebe que el puerto deshabilitado no puede usarse.

   Conex. PC a través USB

   Si el controlador se instaló en el ordenador

   Conecte el escáner al ordenador con un cable USB y luego confirme que el escáner no escanea.

   Si el controlador no se instaló en el ordenador

   Windows:

   Abra el administrador de dispositivos y déjelo abierto; conecte el escáner al ordenador con un cable USB y verifique que no aparecen nuevos contenidos en el administrador de dispositivos.

   Mac OS:

   Conecte el escáner al ordenador mediante un cable USB y, a continuación, confirme que no puede añadir el escáner desde **Impresoras y escáneres**.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Monitorización de un escáner remoto

Comprobación de la información de un escáner remoto

La siguiente información del escáner en funcionamiento se puede comprobar desde **Estado** mediante Web Config.

❏ Estado del producto

Compruebe el estado, el servicio en la nube, el número de producto, la dirección MAC, etc.

❏ Estado de la red

Compruebe la información del estado de conexión de red, la dirección IP, el servidor DNS, etc.

❏ Estado de usos

Compruebe el primer día de escaneados, recuento de escaneados, etc.

❏ Estado del hardware

Compruebe el estado de cada función del escáner.

❏ Instantánea del panel

Muestra una instantánea de la pantalla en el panel de control del escáner.

Cómo recibir notificaciones por correo electrónico cuando se produzcan determinadas situaciones

Acerca de las notificaciones por correo electrónico

Se trata de una función de notificación que, cuando tienen lugar incidentes como interrumpirse el escaneo y errores del escáner, se envía un correo electrónico a la dirección especificada.

Puede registrar hasta cinco destinatarios y configurar los ajustes de notificación para cada destinatario.

Para utilizar esta función, debe configurar el servidor de correo antes de configurar las notificaciones.

Información relacionada

➡ "Configurar un servidor de correo" de la página 42

Configurar las notificaciones por correo electrónico

Configure la notificación por correo electrónico mediante Web Config.

1. Acceda a Web Config y seleccione la pestaña **Gestión del dispositivo** > **Notificación por correo electrónico**.
2. Indique el asunto de la notificación por correo electrónico.

   Seleccione el contenido que se muestra sobre el tema en los dos menús desplegables.

   ❏ Los contenidos seleccionados se muestran junto a **Asunto**.

   ❏ No se puede establecer el mismo contenido a izquierda y derecha.

   ❏ Si el número de caracteres de **Ubicación** supera los 32 bytes, se omiten los caracteres que exceden los 32 bytes.
3. Introduzca la dirección de correo electrónico para enviar el correo electrónico de notificación.

   Utilice A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @, e introduzca entre 1 y 255 caracteres.
4. Seleccione el idioma de las notificaciones de correo electrónico.
5. Seleccione la casilla de verificación del evento para el que desea recibir una notificación.

   El número de **Configuración de notificación** está vinculado al número de destino de **Configuración de dirección de correo electrónico**.

   Ejemplo:

   Si desea enviar una notificación a la dirección de correo electrónico configurada para el número 1 en **Configuración de dirección de correo electrónico** cada vez que se cambie la contraseña del administrador, seleccione la casilla de verificación de la columna **1** en la línea **Contraseña de administrador cambiada**.
6. Haga clic en **Aceptar**.

   Confirme que se enviará una notificación por correo electrónico en respuesta a un evento.

   Ejemplo: la contraseña del administrador se ha cambiado.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Opciones de notificación por correo electrónico

Elementos	Ajustes y explicación
Contraseña de administrador cambiada	Notificación cuando se cambia la contraseña de administrador.

Elementos	Ajustes y explicación
Error de escáner	Notificación cuando se produce un error del escáner.
Fallo de Wi-Fi	Notificación cuando se produce un error de la interfaz de red LAN inalámbrica.

Resolución de problemas

Ha olvidado la contraseña de administrador

Necesita la ayuda del personal de servicio. Póngase en contacto con su distribuidor local.

Nota:
A continuación, se proporcionan los valores iniciales para el administrador de Web Config.

❏ *Nombre de usuario: ninguno (en blanco)*

❏ *Contraseña: número de serie del escáner*

Para encontrar el número de serie, compruebe la etiqueta pegada en la parte posterior del escáner. Si restaura la configuración predeterminada de la contraseña de administrador, se restablece a los valores iniciales.

Ajustes de seguridad avanzados

Configuración de seguridad y prevención de peligros

Si el escáner está conectado a una red, se puede acceder a él desde una ubicación remota. Además, muchas personas pueden compartir el escáner, lo cual resulta útil para mejorar la conveniencia y la eficacia operativa. Sin embargo, los riesgos tales como el acceso ilegal, el uso ilegal y la alteración de datos han aumentado. Si utiliza el escáner en un entorno en el cual se puede acceder a Internet, los riesgos son aún mayores.

En el caso de los escáneres que no tienen protección de acceso externo, es posible ver los contactos almacenados en el escáner desde Internet.

A fines de evitar este riesgo, los escáneres Epson cuentan con una variedad de tecnologías de seguridad.

Configure el escáner según sea necesario, de acuerdo con las condiciones del entorno que se han construido con la información de entorno del cliente.

Nombre	Tipo de función	Qué configurar	Qué evitar
Control del protocolo	Controla los protocolos y servicios que se usarán para comunicarse entre escáneres y ordenadores, y activa y desactiva funciones.	Un protocolo o servicio que se aplica a funciones permitidas o prohibidas por separado.	Se pueden reducir los riesgos de seguridad a través del uso no deliberado si se evita que los usuarios utilicen funciones innecesarias.
Comunicaciones SSL/TLS	Al momento de acceder en Internet al servidor de Epson desde el escáner, el contenido de la comunicación se cifra con comunicaciones SSL/TLS, por ejemplo cuando se comunica con el ordenador desde un explorador web mediante Epson Connect y cuando se actualiza el firmware.	Obtenga un certificado firmado por entidad certificadora y luego impórtelo al escáner.	Eliminar una identificación del escáner mediante un certificado firmado por entidad certificadora evita la falsificación de identidad y el acceso no autorizado. Además, el contenido de comunicación de SSL/TLS está protegido y evita la fuga de contenido de datos de escaneados e información de configuración.
Filtro IPsec/IP	Puede establecer permitir el seccionamiento o corte de datos que provengan de cierto cliente o que sean de un tipo en particular. Como IPsec protege los datos por unidad de paquete IP (cifrado y autenticación), puede comunicar de manera segura el protocolo no garantizado.	Crear una política básica y una política individual para establecer el cliente o el tipo de datos que pueden acceder al escáner.	Proteja el acceso no autorizado y la alteración e intercepción de datos de comunicación con el escáner.
IEEE 802.1X	Solo permite que se conecten a la red usuarios autenticados. Permite usar el escáner solo a un usuario con permiso.	Configuración de autenticación para el servidor RADIUS (servidor de autenticación).	Proteja contra el acceso y el uso no autorizado del escáner.

Información relacionada

- ➡ "Control mediante protocolos" de la página 98
- ➡ "Comunicación SSL/TLS con la impresora" de la página 106
- ➡ "Comunicación cifrada mediante el uso de filtro IPsec/IP" de la página 108
- ➡ "Conexión del escáner a una red IEEE802.1X" de la página 120

Configuración de las funciones de seguridad

Al configurar el filtro IPsec/IP o IEEE 802.1X, es recomendable acceder a Web Config mediante SSL/TLS para comunicar la información de la configuración y reducir los riesgos de seguridad, como la manipulación o la intercepción.

Asegúrese de configurar la contraseña de administrador antes de hacer lo propio con el filtro IPsec/IP o IEEE 802.1X.

Control mediante protocolos

Puede escanear utilizando las siguientes vías y protocolos. Asimismo, puede utilizar la exploración de redes desde un número no especificado de equipos de red.

Puede reducir los riesgos de seguridad no deliberados restringiendo el escaneado desde ciertas vías o controlando las funciones disponibles.

Protocolos de control

Configure los ajustes del protocolo admitido por el escáner.

1. Acceda Web Config y luego seleccione la pestaña **Seguridad de red** tab > **Protocolo**.
2. Configure cada elemento.
3. Haga clic en **Siguiente**.
4. Haga clic en **Aceptar**.

   La configuración se aplica al escáner.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Protocolos que puede habilitar o inhabilitar

Protocolo	Descripción
Configuración Bonjour	Si lo desea, puede especificar si utilizar Bonjour. Bonjour se utiliza para buscar dispositivos, escanear, etc.
Config. SLP	La función SLP se puede habilitar o deshabilitar. SLP se utiliza para llevar a cabo el escaneado y la búsqueda de red en EpsonNet Config.
Configuración WSD	La función WSD se puede habilitar o deshabilitar. Si se habilita, puede agregar dispositivos WSD y escanear desde el puerto WSD.
Config. LLTD	La función LLTD se puede habilitar o deshabilitar. Si se habilita, se muestra en el mapa de red de Windows.

Protocolo	Descripción
Config. LLMNR	La función LLMNR se puede habilitar o deshabilitar. Si se habilita, puede usar la resolución de nombres sin NetBIOS aunque no pueda usar DNS.
Configuración de SNMPv1/v2c	Puede especificar si desea habilitar o no SNMPv1/v2c. Esto se utiliza para configurar dispositivos, supervisar, etc.
Configuración de SNMPv3	Puede especificar si desea habilitar o no SNMPv3. Esto se utiliza para configurar dispositivos cifrados, supervisar, etc.

Elementos de ajuste del protocolo

Configuración Bonjour

Elementos	Valor y descripción del ajuste
Usar Bonjour	Seleccione esta opción para buscar o usar dispositivos a través de Bonjour.
Nombre Bonjour	Muestra el nombre de Bonjour.
Nombre servic. Bonjour	Muestra el nombre del servicio de Bonjour.
Ubicación	Muestra el nombre de la ubicación de Bonjour.
Wide-Area Bonjour	Indique si desea utilizar Wide-Area Bonjour.

Config. SLP

Elementos	Valor y descripción del ajuste
Habilitar SLP	Seleccione esta opción para habilitar la función SLP. Esto se usa como en la búsqueda de red en EpsonNet Config.

Configuración WSD

Elementos	Valor y descripción del ajuste
Habilitar WSD	Seleccione esta opción para poder añadir dispositivos mediante WSD y escanear desde el puerto WSD.
Tiempo de espera dig. (seg.)	Escriba el valor del tiempo de espera de comunicación para el escaneado WSD entre 3 y 3.600 segundos.
Nombre disp.	Muestra el nombre del dispositivo WSD.
Ubicación	Muestra el nombre de la ubicación de WSD.

Config. LLTD

Elementos	Valor y descripción del ajuste
Habilitar LLTD	Seleccione esta opción para habilitar LLTD. El escáner se muestra en el mapa de red de Windows.

Elementos	Valor y descripción del ajuste
Nombre disp.	Muestra el nombre del dispositivo LLTD.

Config. LLMNR

Elementos	Valor y descripción del ajuste
Habilitar LLMNR	Seleccione esta opción para habilitar LLMNR. Puede usar la resolución de nombres sin NetBIOS aunque no pueda usar DNS.

Configuración de SNMPv1/v2c

Elementos	Valor y descripción del ajuste
Activar SNMPv1/v2c	Seleccione esta opción para habilitar SNMPv1/v2c.
Autoridad de acceso	Establezca la autoridad de acceso cuando SNMPv1/v2c esté habilitada. Seleccione **Sólo lectura** o **Lectura/Escritura**.
Nombre de comunidad (solo lectura)	Escriba entre 0 y 32 caracteres ASCII (0x20 a 0x7E).
Nombre de comunidad (lectura/escritura)	Escriba entre 0 y 32 caracteres ASCII (0x20 a 0x7E).

Configuración de SNMPv3

Elementos		Valor y descripción del ajuste
Activar SNMPv3		Cuando la casilla está marcada, SNMPv3 está habilitado.
Nombre de usuario		Escriba entre 1 y 32 caracteres. Caracteres admitidos: caracteres de 1 byte.
Configuración de autenticación		
	Algoritmo	Seleccione un algoritmo para una autenticación de SNMPv3.
	Contraseña	Escriba la contraseña para una autenticación de SNMPv3. Escriba entre 8 y 32 caracteres ASCII (0x20–0x7E). Si no quiere especificarlo, déjelo en blanco.
	Confirmar contraseña	Introduzca la contraseña establecida para confirmarla.
Configuración de cifrado		
	Algoritmo	Seleccione un algoritmo para un cifrado de SNMPv3.
	Contraseña	Escriba la contraseña para un cifrado de SNMPv3. Escriba entre 8 y 32 caracteres ASCII (0x20–0x7E). Si no quiere especificarlo, déjelo en blanco.
	Confirmar contraseña	Introduzca la contraseña establecida para confirmarla.
Nombre de contexto		Escriba un máximo de 32 caracteres en Unicode (UTF-8). Si no quiere especificarlo, déjelo en blanco. La cantidad de caracteres que se pueden escribir varían según el idioma.

Modo de uso de un certificado digital

Acerca de la certificación digital

❏ Certificado firmado CA

Este es un certificado firmado por la autoridad de certificación. Puede obtenerlo para aplicarlo. Mediante certificado se certifica la existencia del escáner y se utiliza para la comunicación SSL/TLS, de forma que pueda garantizar la seguridad de la comunicación de los datos.

Cuando se usa en una comunicación SSL/TLS, se hace como certificado del servidor.

Cuando se configura para el filtrado IPsec/IP o la comunicación IEEE 802.1X, se emplea como certificado de cliente.

❏ Certificado de la autoridad de certificación

Este es un certificado que está en la cadena del Certificado firmado CA, también denominado certificado de la autoridad de certificación intermedio. El navegador web lo utiliza para validar la ruta del certificado del escáner al acceder al servidor de la otra parte o Web Config.

Para el certificado de la autoridad de certificación, configure cuándo validar la ruta de acceso del certificado del servidor desde el escáner. Para el escáner, configure para certificar la ruta del Certificado firmado CA para la conexión SSL/TLS.

Puede obtener el certificado de la autoridad de certificación del escáner de la autoridad de certificación que emitió el certificado.

Además, puede obtener el certificado de la autoridad de certificación utilizado para validar el servidor de la otra parte de la autoridad de certificación que emitió el Certificado firmado CA del otro servidor.

❏ Certificado auto-firmado

Este es un certificado que firma y emite el propio escáner. También se denomina certificado raíz. Debido a que el emisor se certifica a sí mismo, no es fiable y no puede evitar la suplantación.

Úselo cuando configure la seguridad y establezca una comunicación SSL/TLS sencilla sin el Certificado firmado CA.

Si utiliza este certificado para una comunicación SSL/TLS, es posible que se muestre una alerta de seguridad en el navegador web, ya que el certificado no está registrado en un navegador web. Solamente puede usar el Certificado auto-firmado para una comunicación SSL/TLS.

Información relacionada

➡ "Configuración de un Certificado firmado CA" de la página 101

➡ "Actualización de un certificado autofirmado" de la página 105

➡ "Configuración de un Certificado CA" de la página 106

Configuración de un Certificado firmado CA

Cómo obtener un certificado firmado por entidad certificadora

Para obtener un certificado firmado por entidad certificadora, cree una CSR (Solicitud de firma de certificado) y envíela a una entidad certificadora (CA). Puede crear una CSR mediante Web Config y un ordenador.

Siga estos pasos para crear una CSR y obtener un certificado firmado CA con Web Config. Cuando se crea una CSR con Web Config, el certificado tiene el formato PEM/DER.

1. Acceda a Web Config y, a continuación, seleccione la pestaña **Seguridad de red**. A continuación, seleccione **SSL/TLS** > **Certificado** o **IPsec/Filtrado de IP** > **Certificado del cliente** o **IEEE802.1X** > **Certificado del cliente**.

   Sea cual sea su elección, puede obtener el mismo certificado y utilizarlo en común.

2. Haga clic en **Generar** en **CSR**.

   Se abrirá la página de creación de CSR.

3. Introduzca un valor para cada opción.

   Nota:
   La longitud de la clave y las abreviaturas disponibles varían según la entidad certificadora. Cree una solicitud conforme a las normas de cada entidad certificadora.

4. Haga clic en **Aceptar**.

   Aparecerá un mensaje para confirmar que ha terminado.

5. Seleccione la pestaña **Seguridad de red**. A continuación, seleccione **SSL/TLS** > **Certificado**, o **IPsec/Filtrado de IP** > **Certificado del cliente** o **IEEE802.1X** > **Certificado del cliente**.

6. Haga clic en el botón de descarga de **CSR** correspondiente al formato especificado por la entidad certificadora para descargarse una CSR en un ordenador.

   Importante:
   No genere una CSR de nuevo. Si lo hace, quizá no pueda importar un Certificado firmado CA expedido.

7. Envíe la CSR a una entidad certificadora y obtenga un Certificado firmado CA.

   Siga las normas de cada entidad certificadora sobre el método y la forma de envío.

8. Guarde el Certificado firmado CA en un ordenador conectado al escáner.

   El Certificado firmado CA se considera obtenido cuando se guarda en un destino.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Elementos de configuración del CSR

Elementos	Ajustes y explicación
Longitud clave	Seleccione una longitud de la cadena del CSR.

Elementos	Ajustes y explicación
Nombre común	Puede introducir entre 1 y 128 caracteres. Si se trata de una dirección IP, debería ser una dirección IP estática. Puede introducir de 1 a 5 direcciones IPv4, direcciones IPv6, nombres de host y FQDN separándolos con comas. El primer elemento se guarda con el nombre común y el resto en el campo de alias del sujeto del certificado. Ejemplo: Dirección IP del escáner: 192.0.2.123, Nombre del escáner: EPSONA1B2C3 Nombre común: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
Organización/ Unidad organizativa/ Localidad/ Estado/Provincia	Puede introducir entre 0 y 64 caracteres ASCII (0x20–0x7E). Puede dividir los nombres distinguidos con comas.
País	Introduzca un código de país con un número de dos dígitos según ISO-3166.
Dirección correo del remitente	Puede introducir la dirección del remitente del correo electrónico para la configuración del servidor de correo. Introduzca la misma dirección de correo electrónico que en **Dirección correo del remitente** en la pestaña **Red** > **Servidor correo electrónico** > **Básica**.

Importar un certificado firmado por la autoridad de certificación

Importe el Certificado firmado CA obtenido al escáner.

Importante:

- ❏ *Confirme que la fecha y la hora del escáner estén bien configuradas. El certificado puede no ser válido.*
- ❏ *Si obtiene un certificado utilizando un CSR creado desde Web Config, puede volver a importar un certificado una vez.*

1. Acceda a Web Config y luego seleccione la pestaña **Seguridad de red**. A continuación, seleccione **SSL/TLS** > **Certificado**, o **IPsec/Filtrado de IP** > **Certificado del cliente** o **IEEE802.1X** > **Certificado del cliente**.

2. Haga clic en **Importar**

   Se abrirá la página de importación del certificado.

3. Introduzca un valor para cada opción. Configure **Certificado CA 1** y **Certificado CA 2** si verifica la ruta de acceso de certificado en el navegador web que accede al escáner.

   En función de dónde cree el CSR y del formato de archivo del certificado, los ajustes necesarios pueden ser diferentes. Introduzca los valores de los elementos requeridos de acuerdo a lo siguiente.

   - ❏ Un certificado de formato PEM/DER obtenido de Web Config
     - ❏ **Clave privada**: no configure nada, pues el escáner ya contiene una clave privada.
     - ❏ **Contraseña**: no configurar.
     - ❏ **Certificado CA 1/Certificado CA 2**: opcional

❏ Un certificado de formato PEM/DER obtenido de un ordenador

❏ **Clave privada**: es necesario configurarla.

❏ **Contraseña**: no configurar.

❏ **Certificado CA 1/Certificado CA 2**: opcional

❏ Un certificado de formato PKCS#12 obtenido de un ordenador

❏ **Clave privada**: no configurar.

❏ **Contraseña**: opcional

❏ **Certificado CA 1/Certificado CA 2**: no configurar.

4. Haga clic en **Aceptar**.

   Se muestra un mensaje de finalización.

Nota:
*Haga clic en **Confirmar** para comprobar la información del certificado.*

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Elementos de configuración de importación de certificados firmados por entidades certificadoras

Elementos	Ajustes y explicación
Certificado del servidor o Certificado del cliente	Seleccione el formato del certificado. Para conexiones SSL/TLS, se muestra Certificado del servidor. Para IPsec/Filtrado de IP o IEEE 802.1x, se muestra Certificado del cliente.
Clave privada	Si obtiene un certificado de formato PEM/DER utilizando un CSR creado desde una computadora, especifique un archivo de clave privada que coincida con un certificado.
Contraseña	Si el formato del archivo es **Certificado con clave privada (PKCS#12)**, introduzca la contraseña para cifrar la clave privada que se establece al obtener el certificado.
Certificado CA 1	Si el formato de su certificado es **Certificado (PEM/DER)**, importe un certificado de una autoridad de certificación que emita un Certificado firmado CA utilizado como certificado de servidor. Especifique un archivo en caso necesario.
Certificado CA 2	Si el formato de su certificado es **Certificado (PEM/DER)**, importe un certificado de una autoridad de certificación que emita un Certificado CA 1. Especifique un archivo en caso necesario.

Cómo eliminar un certificado firmado por entidad certificadora

Puede eliminar un certificado importado cuando haya caducado o cuando ya no necesite una conexión cifrada.

Importante:
Si ha obtenido el certificado mediante una CSR creada con Web Config, no puede volver a importar un certificado borrado. En ese caso, cree una CSR y vuelva a obtener un certificado.

1. Acceda a Web Config y, a continuación, seleccione la pestaña **Seguridad de red**. A continuación, seleccione **SSL/TLS** > **Certificado** o **IPsec/Filtrado de IP** > **Certificado del cliente** o **IEEE802.1X** > **Certificado del cliente**.
2. Haga clic en **Eliminar**.
3. Confirme que desea eliminar el certificado en el mensaje mostrado.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Actualización de un certificado autofirmado

Como el Certificado auto-firmado lo expide el escáner, puede actualizarlo cuando caduque o cuando el contenido cambie.

1. Acceda Web Config y seleccione la pestaña **Seguridad de red** tab > **SSL/TLS** > **Certificado**.
2. Haga clic en **Actualizar**.
3. Introduzca **Nombre común**.

   Puede introducir hasta 5 direcciones IPv4 e IPv6, nombres de hosts y FQDNs de entre 1 y 128 caracteres y separadas por comas. El primer parámetro se guardará como nombre común, y el resto se guardará en el campo de alias del asunto del certificado.

   Ejemplo:

   Dirección IP del escáner: 192.0.2.123, Nombre del escáner: EPSONA1B2C3

   Nombre común: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
4. Especifique el periodo de validez del certificado.
5. Haga clic en **Siguiente**.

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

   Se actualizará el escáner.

Nota:
*Puede consultar la información del certificado en la pestaña **Seguridad de red** > **SSL/TLS** > **Certificado** > **Certificado auto-firmado** y hacer clic en **Confirmar**.*

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Configuración de un Certificado CA

Al configurar el Certificado CA, puede validar la ruta al certificado de CA del servidor al que accede el escáner. Esto puede evitar la suplantación de personalidad.

Puede obtener el Certificado CA de la autoridad de certificación donde se emite el Certificado firmado CA.

Importar un Certificado CA

Importe el Certificado CA al escáner.

1. Acceda a Web Config y, a continuación, seleccione la pestaña **Seguridad de red** > **Certificado CA**.
2. Haga clic en **Importar**.
3. Especifique el Certificado CA que desea importar.
4. Haga clic en **Aceptar**.

Cuando finalice la importación, volverá a la pantalla **Certificado CA** y se mostrará el Certificado CA importado.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Eliminar una Certificado CA

La Certificado CA importada se puede eliminar.

1. Acceda a Web Config y, a continuación, seleccione la pestaña **Seguridad de red** > **Certificado CA**.
2. Haga clic en **Eliminar** junto al Certificado CA que desee eliminar.
3. Confirme que desea eliminar el certificado en el mensaje que se muestra.
4. Haga clic en **Reiniciar red** y, a continuación, compruebe que el certificado de la autoridad de certificación no aparece en la pantalla actualizada.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Comunicación SSL/TLS con la impresora

Cuando se establece el certificado de servidor mediante el uso de la comunicación SSL/TLS (capa de puertos seguros/seguridad de la capa de transporte) con el escáner, puede cifrar la ruta de comunicación entre ordenadores. Haga esto si desea evitar el acceso remoto y sin autorización.

Configuración de ajustes básicos de SSL/TLS

Si el escáner admite la función de servidor HTTPS, puede usar una comunicación SSL/TLS para cifrar las comunicaciones. Puede configurar y administrar el escáner utilizando Web Config mientras garantiza la seguridad.

Configure la potencia de cifrado y la función de redireccionamiento.

1. Acceda a Web Config y seleccione la pestaña **Seguridad de red** > **SSL/TLS** > **Básica**.
2. Seleccione un valor para cada elemento.
   - ❏ Intensidad de cifrado
     Seleccione el nivel de potencia del cifrado.
   - ❏ Redirigir HTTP a HTTPS
     Redirecciona a HTTPS cuando se accede a HTTP.
3. Haga clic en **Siguiente**.
   Aparecerá un mensaje de confirmación.
4. Haga clic en **Aceptar**.
   Se actualizará el escáner.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Configuración de un certificado de servidor para el escáner

1. Acceda a Web Config y seleccione la pestaña **Seguridad de red** > **SSL/TLS** > **Certificado**.
2. Especifique un certificado a usar en **Certificado del servidor**.
   - ❏ Certificado auto-firmado
     El escáner generará un certificado autofirmado. Si no obtiene el certificado firmado por la autoridad de certificación, seleccione esto.
   - ❏ Certificado firmado CA
     Si obtiene e importa el certificado firmado por la autoridad de certificación con antelación, puede especificar esto.
3. Haga clic en **Siguiente**.
   Aparecerá un mensaje de confirmación.
4. Haga clic en **Aceptar**.
   Se actualizará el escáner.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36
➡ "Configuración de un Certificado firmado CA" de la página 101

➡ "Configuración de un Certificado CA" de la página 106

Comunicación cifrada mediante el uso de filtro IPsec/IP

Acerca de IPsec/Filtrado de IP

Puede filtrar el tráfico en base a las direcciones IP, los servicios y el puerto mediante la función de Filtrado IPsec/IP. Si combina los filtros, puede configurar el escáner para que acepte o bloquee determinados clientes y datos. Además, el nivel de seguridad aumenta si utiliza una IPsec.

Nota:
Los ordenadores con Windows Vista o posterior o Windows Server 2008 o posterior admiten IPsec.

Configuración de la directiva predeterminada

Para filtrar el tráfico, tiene que configurar la directiva predeterminada. Se trata de las normas que se aplican a todo usuario o grupo que se conecta al escáner. Si quiere controlar con más precisión a usuarios y grupos de usuarios, configure directivas de grupo.

1. Acceda a Web Config y luego seleccione la pestaña **Seguridad de red** > **IPsec/Filtrado de IP** > **Básica**.
2. Introduzca un valor para cada opción.
3. Haga clic en **Siguiente**.
   Aparecerá un mensaje de confirmación.
4. Haga clic en **Aceptar**.
   Se actualizará el escáner.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Elementos de configuración de Norma predeterminada

Norma predeterminada

Elementos	Ajustes y explicación
IPsec/Filtrado de IP	Puede habilitar o inhabilitar la función del filtro de IPsec/IP.

❏ **Control de acceso**

Configure un método para controlar el tráfico de paquetes IP.

Elementos	Ajustes y explicación
Permitir acceso	Seleccione esta opción si quiere permitir que pasen los paquetes IP configurados.
Denegar acceso	Seleccione esta opción si quiere prohibir que pasen los paquetes IP configurados.
IPsec	Seleccione esta opción si quiere permitir que pasen los paquetes IPsec configurados.

❏ **Versión IKE**

Seleccione **IKEv1** o **IKEv2** para **Versión IKE**. Seleccione uno de ellos de acuerdo al dispositivo al que esté conectado el escáner.

❏ IKEv1

Los siguientes elementos se muestran cuando selecciona **IKEv1** en **Versión IKE**.

Elementos	Ajustes y explicación
Método de autenticación	Para poder seleccionar **Certificado**, antes tiene que haber obtenido e importado un certificado firmado por la entidad certificadora.
Clave precompartida	Si selecciona **Clave precompartida** para **Método de autenticación**, introduzca una clave previamente compartida que tenga entre 1 y 127 caracteres.
Confirmar clave precompartida	Introduzca la clave establecida para confirmarla.

❏ IKEv2

Los siguientes elementos se muestran cuando selecciona **IKEv2** en **Versión IKE**.

Elementos		Ajustes y explicación
Local	Método de autenticación	Para poder seleccionar **Certificado**, antes tiene que haber obtenido e importado un certificado firmado por la entidad certificadora.
	Tipo de Identificación (ID)	Si selecciona **Clave precompartida** para **Método de autenticación**, seleccione el tipo de identificación del escáner.
	Identificación (ID)	Escriba el ID del escáner que coincida con el tipo de ID. No se puede utilizar «@», «#» ni «=» como primer carácter. **Nombre distinguido**: escriba entre 1 y 255 caracteres ASCII de 1 byte (0x20 a 0x7E). Debe incluir «=». **Dirección IP**: introduzca el formato IPv4 o IPv6. **FQDN**: introduzca una combinación entre 1 y 255 caracteres. Los caracteres admitidos son A–Z, a–z, 0–9, «-» y punto (.). **Dirección de correo**: escriba entre 1 y 255 caracteres ASCII de 1 byte (0x20 a 0x7E). Debe incluir «@». **ID clave**: escriba entre 1 y 255 caracteres ASCII de 1 byte (0x20 a 0x7E).
	Clave precompartida	Si selecciona **Clave precompartida** para **Método de autenticación**, introduzca una clave previamente compartida que tenga entre 1 y 127 caracteres.
	Confirmar clave precompartida	Introduzca la clave establecida para confirmarla.

Elementos		Ajustes y explicación
Remota	Método de autenticación	Para poder seleccionar **Certificado**, antes tiene que haber obtenido e importado un certificado firmado por la entidad certificadora.
	Tipo de Identificación (ID)	Si selecciona **Clave precompartida** para **Método de autenticación**, seleccione el tipo de ID del dispositivo que desea autenticar.
	Identificación (ID)	Escriba el ID del escáner que coincida con el tipo de ID. No se puede utilizar «@», «#» ni «=» como primer carácter. **Nombre distinguido**: escriba entre 1 y 255 caracteres ASCII de 1 byte (0x20 a 0x7E). Debe incluir «=». **Dirección IP**: introduzca el formato IPv4 o IPv6. **FQDN**: introduzca una combinación entre 1 y 255 caracteres. Los caracteres admitidos son A–Z, a–z, 0–9, «-» y punto (.). **Dirección de correo**: escriba entre 1 y 255 caracteres ASCII de 1 byte (0x20 a 0x7E). Debe incluir «@». **ID clave**: escriba entre 1 y 255 caracteres ASCII de 1 byte (0x20 a 0x7E).
	Clave precompartida	Si selecciona **Clave precompartida** para **Método de autenticación**, introduzca una clave previamente compartida que tenga entre 1 y 127 caracteres.
	Confirmar clave precompartida	Introduzca la clave establecida para confirmarla.

❏ Encapsulamiento

Si selecciona **IPsec** como **Control de acceso**, tiene que configurar un modo de encapsulación.

Elementos	Ajustes y explicación
Modo de transporte	Seleccione esta opción si solamente utiliza el escáner en una red LAN. Se cifrarán los paquetes IP de capa 4 o posteriores.
Modo túnel	Seleccione esta opción para utilizar el escáner en una red con conexión a Internet (IPsec-VPN, por ejemplo). Se codificarán los encabezados y los datos de los paquetes IP. **Dirección puerta de enlace remota**: si selecciona **Modo túnel** para **Encapsulamiento**, introduzca una dirección de puerta de enlace que contenga entre 1 y 39 caracteres.

❏ Protocolo de seguridad

Si selecciona **IPsec** para **Control de acceso**, seleccione una opción.

Elementos	Ajustes y explicación
ESP	Seleccione esta opción si quiere garantizar la integridad de una autenticación y de los datos, además de cifrar los datos.
AH	Seleccione esta opción si quiere garantizar la integridad de una autenticación y de los datos. Puede utilizar IPsec aunque esté prohibido el cifrado de datos.

❏ **Ajustes de algoritmo**

Se recomienda que seleccione **Cualquiera** para todos los ajustes o que seleccione un elemento distinto de **Cualquiera** para cada ajuste. Si selecciona **Cualquiera** para algunos de los ajustes y selecciona un elemento distinto de **Cualquiera** para los otros ajustes, es posible que el dispositivo no se comunique, en función del otro dispositivo que desee autenticar.

Elementos		Ajustes y explicación
IKE	Cifrado	Seleccione el algoritmo de cifrado de IKE. El elemento varía según la versión de IKE.
	Autenticación	Seleccione el algoritmo de autenticación de IKE.
	Intercambio de clave	Seleccione el algoritmo de intercambio de claves de IKE. El elemento varía según la versión de IKE.
ESP	Cifrado	Seleccione el algoritmo de cifrado de ESP. Esta opción está disponible si se selecciona **ESP** para **Protocolo de seguridad**.
	Autenticación	Seleccione el algoritmo de autenticación de ESP. Esta opción está disponible si se selecciona **ESP** para **Protocolo de seguridad**.
AH	Autenticación	Seleccione el algoritmo de cifrado de AH. Esta opción está disponible si se selecciona **AH** para **Protocolo de seguridad**.

Configuración de la directiva de grupo

Una directiva de grupo consta de una o varias reglas que se aplican a un usuario o a un grupo de usuarios. El escáner controla los paquetes IP que coinciden con las directivas configuradas. Los paquetes IP se autentifican por orden: primero las directivas de grupo 1–10 y luego las directivas predeterminadas.

1. Acceda a Web Config y luego seleccione la pestaña **Seguridad de red** > **IPsec/Filtrado de IP** > **Básica**.
2. Haga clic en la pestaña numerada que desee configurar.
3. Introduzca un valor para cada opción.
4. Haga clic en **Siguiente**.

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

   Se actualizará el escáner.

Elementos de configuración de Norma de grupo

Elementos	Ajustes y explicación
Habilitar esta política de grupo	Puede habilitar o inhabilitar una directiva de grupo.

Control de acceso

Configure un método para controlar el tráfico de paquetes IP.

Elementos	Ajustes y explicación
Permitir acceso	Seleccione esta opción si quiere permitir que pasen los paquetes IP configurados.
Denegar acceso	Seleccione esta opción si quiere prohibir que pasen los paquetes IP configurados.
IPsec	Seleccione esta opción si quiere permitir que pasen los paquetes IPsec configurados.

Dirección local(escáner)

Seleccione una dirección IPv4 o IPv6 adecuada para su entorno de red. Si se asigna una dirección IP automáticamente, puede seleccionar **Usar dirección IPv4 obtenida automáticamente**.

Nota:
Si se asigna automáticamente una dirección IPv6, es posible que la conexión no esté disponible. Configure una dirección IPv6 fija.

Dirección remota(host)

Introduzca la dirección IP de un dispositivo para controlar el acceso. La dirección IP debe contener 43 caracteres o menos. Si no introduce ninguna dirección IP, se controlarán todas las direcciones.

Nota:
Si se asigna una dirección IP automáticamente (si la asigna DHCP, por ejemplo), quizá la conexión no esté disponible. Configure una dirección IP fija.

Método de elección de puerto

Seleccione un método para especificar los puertos.

❏ Nombre del servicio

Si selecciona **Nombre del servicio** para **Método de elección de puerto**, seleccione una opción.

❏ Protocolo de transporte

Si selecciona **Número de puerto** como **Método de elección de puerto**, tiene que configurar un modo de encapsulación.

Elementos	Ajustes y explicación
Cualquier protocolo	Seleccione esta opción si desea controlar todo tipo de protocolos.
TCP	Seleccione esta opción si desea controlar los datos transmitidos por unidifusión.
UDP	Seleccione esta opción si desea controlar los datos transmitidos por difusión o multidifusión.
ICMPv4	Seleccione esta opción si desea controlar el comando «ping».

❏ Puerto local

Si selecciona **Número de puerto** para **Método de elección de puerto** y selecciona **TCP** o **UDP** para **Protocolo de transporte**, introduzca los números de puerto para controlar los paquetes de recepción, separándolos con comas. Puede escribir 10 números de puerto como máximo.

Por ejemplo: 20,80,119,5220

Si no escribe ningún número de puerto, se controlarán todos los puertos.

❏ Puerto remoto

Si selecciona **Número de puerto** para **Método de elección de puerto** y selecciona **TCP** o **UDP** para **Protocolo de transporte**, introduzca los números de puerto para controlar los paquetes de envío, separándolos con comas. Puede escribir 10 números de puerto como máximo.

Por ejemplo: 25,80,143,5220

Si no escribe ningún número de puerto, se controlarán todos los puertos.

Versión IKE

Seleccione **IKEv1** o **IKEv2** para **Versión IKE**. Seleccione uno de ellos de acuerdo al dispositivo al que esté conectado el escáner.

❏ IKEv1

Los siguientes elementos se muestran cuando selecciona **IKEv1** en **Versión IKE**.

Elementos	Ajustes y explicación
Método de autenticación	Si selecciona **IPsec** para **Control de acceso**, seleccione una opción. El certificado utilizado es común con una política por defecto.
Clave precompartida	Si selecciona **Clave precompartida** para **Método de autenticación**, introduzca una clave previamente compartida que tenga entre 1 y 127 caracteres.
Confirmar clave precompartida	Introduzca la clave establecida para confirmarla.

❏ IKEv2

Los siguientes elementos se muestran cuando selecciona **IKEv2** en **Versión IKE**.

Elementos		Ajustes y explicación
Local	Método de autenticación	Si selecciona **IPsec** para **Control de acceso**, seleccione una opción. El certificado utilizado es común con una política por defecto.
	Tipo de Identificación (ID)	Si selecciona **Clave precompartida** para **Método de autenticación**, seleccione el tipo de identificación del escáner.
	Identificación (ID)	Escriba el ID del escáner que coincida con el tipo de ID. No se puede utilizar «@», «#» ni «=» como primer carácter. **Nombre distinguido**: escriba entre 1 y 255 caracteres ASCII de 1 byte (0x20 a 0x7E). Debe incluir «=». **Dirección IP**: introduzca el formato IPv4 o IPv6. **FQDN**: introduzca una combinación entre 1 y 255 caracteres. Los caracteres admitidos son A–Z, a–z, 0–9, «-» y punto (.). **Dirección de correo**: escriba entre 1 y 255 caracteres ASCII de 1 byte (0x20 a 0x7E). Debe incluir «@». **ID clave**: escriba entre 1 y 255 caracteres ASCII de 1 byte (0x20 a 0x7E).
	Clave precompartida	Si selecciona **Clave precompartida** para **Método de autenticación**, introduzca una clave previamente compartida que tenga entre 1 y 127 caracteres.
	Confirmar clave precompartida	Introduzca la clave establecida para confirmarla.
Remota	Método de autenticación	Si selecciona **IPsec** para **Control de acceso**, seleccione una opción. El certificado utilizado es común con una política por defecto.
	Tipo de Identificación (ID)	Si selecciona **Clave precompartida** para **Método de autenticación**, seleccione el tipo de ID del dispositivo que desea autenticar.
	Identificación (ID)	Escriba el ID del escáner que coincida con el tipo de ID. No se puede utilizar «@», «#» ni «=» como primer carácter. **Nombre distinguido**: escriba entre 1 y 255 caracteres ASCII de 1 byte (0x20 a 0x7E). Debe incluir «=». **Dirección IP**: introduzca el formato IPv4 o IPv6. **FQDN**: introduzca una combinación entre 1 y 255 caracteres. Los caracteres admitidos son A–Z, a–z, 0–9, «-» y punto (.). **Dirección de correo**: escriba entre 1 y 255 caracteres ASCII de 1 byte (0x20 a 0x7E). Debe incluir «@». **ID clave**: escriba entre 1 y 255 caracteres ASCII de 1 byte (0x20 a 0x7E).
	Clave precompartida	Si selecciona **Clave precompartida** para **Método de autenticación**, introduzca una clave previamente compartida que tenga entre 1 y 127 caracteres.
	Confirmar clave precompartida	Introduzca la clave establecida para confirmarla.

Encapsulamiento

Si selecciona **IPsec** como **Control de acceso**, tiene que configurar un modo de encapsulación.

Elementos	Ajustes y explicación
Modo de transporte	Seleccione esta opción si solamente utiliza el escáner en una red LAN. Se cifrarán los paquetes IP de capa 4 o posteriores.
Modo túnel	Seleccione esta opción para utilizar el escáner en una red con conexión a Internet (IPsec-VPN, por ejemplo). Se codificarán los encabezados y los datos de los paquetes IP. **Dirección puerta de enlace remota**: si selecciona **Modo túnel** para **Encapsulamiento**, introduzca una dirección de puerta de enlace que contenga entre 1 y 39 caracteres.

Protocolo de seguridad

Si selecciona **IPsec** para **Control de acceso**, seleccione una opción.

Elementos	Ajustes y explicación
ESP	Seleccione esta opción si quiere garantizar la integridad de una autenticación y de los datos, además de cifrar los datos.
AH	Seleccione esta opción si quiere garantizar la integridad de una autenticación y de los datos. Puede utilizar IPsec aunque esté prohibido el cifrado de datos.

Ajustes de algoritmo

Se recomienda que seleccione **Cualquiera** para todos los ajustes o que seleccione un elemento distinto de **Cualquiera** para cada ajuste. Si selecciona **Cualquiera** para algunos de los ajustes y selecciona un elemento distinto de **Cualquiera** para los otros ajustes, es posible que el dispositivo no se comunique, en función del otro dispositivo que desee autenticar.

Elementos		Ajustes y explicación
IKE	Cifrado	Seleccione el algoritmo de cifrado de IKE. El elemento varía según la versión de IKE.
	Autenticación	Seleccione el algoritmo de autenticación de IKE.
	Intercambio de clave	Seleccione el algoritmo de intercambio de claves de IKE. El elemento varía según la versión de IKE.
ESP	Cifrado	Seleccione el algoritmo de cifrado de ESP. Esta opción está disponible si se selecciona **ESP** para **Protocolo de seguridad**.
	Autenticación	Seleccione el algoritmo de autenticación de ESP. Esta opción está disponible si se selecciona **ESP** para **Protocolo de seguridad**.
AH	Autenticación	Seleccione el algoritmo de cifrado de AH. Esta opción está disponible si se selecciona **AH** para **Protocolo de seguridad**.

Combinación de Dirección local(escáner) y Dirección remota(host) en Norma de grupo

		Configuración de Dirección local(escáner)		
		IPv4	IPv6*2	Cualquier dirección*3
Configuración de Dirección remota(host)	IPv4*1	✓	–	✓
	IPv6*1, *2	–	✓	✓
	En blanco	✓	✓	✓

*1 Si selecciona **IPsec** como valor de ajuste de **Control de acceso**, no podrá especificar la longitud de prefijo.

*2 Si selecciona **IPsec** como valor de ajuste de **Control de acceso**, podrá seleccionar una dirección local de vínculo (fe80::) pero la directiva de grupo quedará deshabilitada.

*3 Excepto las direcciones locales de vínculo IPv6.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Referencias del nombre del servicio en la directiva de grupo

Nota:
Se muestran los servicios no disponibles pero no se pueden seleccionar.

Nombre del servicio	Tipo de protocolo	Número de puerto local	Número de puerto remoto	Funciones controladas
Cualquiera	–	–	–	Todos los servicios
ENPC	UDP	3289	Cualquier puerto	Búsqueda de un escáner desde aplicaciones como Epson Device Admin y el controlador del escáner
SNMP	UDP	161	Cualquier puerto	Adquisición y configuración de MIB desde aplicaciones como Epson Device Admin y el controlador del escáner de Epson
WSD	TCP	Cualquier puerto	5357	Control de WSD
WS-Discovery	UDP	3702	Cualquier puerto	Búsqueda de escáneres WSD
Network Scan	TCP	1865	Cualquier puerto	Reenvío de los datos escaneados desde Document Capture Pro
Network Push Scan	TCP	Cualquier puerto	2968	Adquisición de información del trabajo de escaneado desatendido desde Document Capture Pro
Network Push Scan Discovery	UDP	2968	Cualquier puerto	Búsqueda de un ordenador desde el escáner

Nombre del servicio	Tipo de protocolo	Número de puerto local	Número de puerto remoto	Funciones controladas
Datos FTP (remoto)	TCP	Cualquier puerto	20	Cliente FTP (reenvío de datos de escaneado) Sin embargo esto puede controlar solo un servidor FTP que utilice el puerto remoto número 20.
Control FTP (remoto)	TCP	Cualquier puerto	21	Cliente FTP (control de los datos escaneados reenviados)
CIFS (remoto)	TCP	Cualquier puerto	445	Cliente CIFS (reenvío de datos escaneados a una carpeta)
NetBIOS Name Service (remoto)	UDP	Cualquier puerto	137	Cliente CIFS (reenvío de datos escaneados a una carpeta)
NetBIOS Datagram Service (remoto)	UDP	Cualquier puerto	138	
NetBIOS Session Service (remoto)	TCP	Cualquier puerto	139	
HTTP (local)	TCP	80	Cualquier puerto	Servidor HTTP(S) (envío de datos de Web Config y WSD)
HTTPS (local)	TCP	443	Cualquier puerto	
HTTP (remoto)	TCP	Cualquier puerto	80	Cliente HTTP(S) (actualización del firmware y el certificado raíz)
HTTPS (remoto)	TCP	Cualquier puerto	443	

Ejemplos de configuración de IPsec/Filtrado de IP

Recepción de paquetes IPsec solamente

Este ejemplo solo para configurar una política predeterminada.

Norma predeterminada:

❏ **IPsec/Filtrado de IP**: **Activar**

❏ **Control de acceso**: **IPsec**

❏ **Método de autenticación**: **Clave precompartida**

❏ **Clave precompartida**: escriba 127 caracteres como máximo.

Norma de grupo: no configurar.

Recepción de datos de escaneado y configuraciones del escáner

Este ejemplo permite la comunicación de datos de escaneado y la configuración del escáner desde servicios especificados.

Norma predeterminada:

❏ **IPsec/Filtrado de IP**: **Activar**

❏ **Control de acceso**: **Denegar acceso**

Norma de grupo:

❏ **Habilitar esta política de grupo**: seleccione la casilla.

❏ **Control de acceso**: **Permitir acceso**

❏ **Dirección remota(host)**: dirección IP de un cliente

❏ **Método de elección de puerto**: **Nombre del servicio**

❏ **Nombre del servicio**: seleccione la casilla de **ENPC**, **SNMP**, **HTTP (local)**, **HTTPS (local)** y de **Network Scan**.

Recibir acceso solo desde una dirección IP especificada

Este ejemplo permite que una dirección IP especificada acceda al escáner.

Norma predeterminada:

❏ **IPsec/Filtrado de IP**: **Activar**

❏ **Control de acceso**:**Denegar acceso**

Norma de grupo:

❏ **Habilitar esta política de grupo**: seleccione la casilla.

❏ **Control de acceso**: **Permitir acceso**

❏ **Dirección remota(host)**: dirección IP de un cliente del administrador

Nota:
Independientemente de la configuración de la política, el cliente podrá acceder y configurar el escáner.

Configuración de un certificado para filtro IPsec/IP

Configure el certificado del cliente para el filtro IPsec/IP. Al configurarlo, puede usar el certificado como método de autenticación del filtro IPsec/IP. Si desea configurar la autoridad de certificación, acceda a **Certificado CA**.

1. Acceda a Web Config y seleccione la pestaña **Seguridad de red** > **IPsec/Filtrado de IP** > **Certificado del cliente**.

2. Importe el certificado en **Certificado del cliente**.

   Si ya ha importado un certificado publicado por una autoridad de certificación, puede copiarlo y usarlo en el filtro IPsec/IP. Para copiarlo, seleccione el certificado en **Copiar desde** y, a continuación, haga clic en **Copiar**.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

➡ "Configuración de un Certificado firmado CA" de la página 101

➡ "Configuración de un Certificado CA" de la página 106

Conexión del escáner a una red IEEE802.1X

Configuración de una red IEEE 802.1X

Si habilita IEEE 802.1X en el escáner, puede utilizarlo en una red que esté conectada a un servidor RADIUS, a un interruptor LAN con función de autenticación o a un punto de acceso.

1. Acceda a Web Config y luego seleccione la pestaña **Seguridad de red** > **IEEE802.1X** > **Básica**.

2. Introduzca un valor para cada opción.

   Para utilizar el escáner a través de una red Wi-Fi, haga clic en **Instalación de Wi-Fi** y seleccione o introduzca un SSID.

   Nota:
   Puede compartir la configuración entre las redes Ethernet y Wi-Fi.

3. Haga clic en **Siguiente**.

   Aparecerá un mensaje de confirmación.

4. Haga clic en **Aceptar**.

   Se actualizará el escáner.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Opciones de ajuste de las redes IEEE 802.1X

Elementos	Ajustes y explicación	
IEEE802.1X (LAN cableada)	Puede habilitar o deshabilitar la configuración de la página (**IEEE802.1X** > **Básica**) para IEEE802.1X (LAN cableada).	
IEEE802.1X (Wi-Fi)	Se muestra el estado de la conexión de IEEE802.1X (Wi-Fi).	
Método de Conexión	Se mostrará el método de conexión de una red actual.	
Tipo de EAP	Seleccione una opción para el método de autenticación entre el escáner y un servidor RADIUS.	
	EAP-TLS	Tiene que obtener e importar un certificado firmado por entidad certificadora.
	PEAP-TLS	
	PEAP/MSCHAPv2	Tiene que configurar una contraseña.
	EAP-TTLS	
ID del usuario	Configure un ID para utilizar en la autenticación de un servidor RADIUS. Escriba entre 1 y 128 caracteres ASCII de 1 byte (0x20 a 0x7E).	

Elementos	Ajustes y explicación	
Contraseña	Configure una contraseña para autenticar el escáner. Escriba entre 1 y 128 caracteres ASCII de 1 byte (0x20 a 0x7E). Si utiliza un servidor de Windows como servidor RADIUS, puede escribir hasta 127 caracteres.	
Confirmar contraseña	Introduzca la contraseña establecida para confirmarla.	
ID del servidor	Puede configurar un ID de servidor para la autenticación con un servidor RADIUS determinado. El autenticador comprueba si hay o no un ID de servidor en el campo subject/subjectAltName del certificado de un servidor enviado desde un servidor RADIUS. Escriba entre 0 y 128 caracteres ASCII de 1 byte (0x20 a 0x7E).	
Validación de certificado	Puede establecer la validación de certificados independientemente del método de autenticación. Importe el certificado en **Certificado CA**.	
Nombre anónimo	Si selecciona **PEAP-TLS** o **PEAP/MSCHAPv2** como **Tipo de EAP**, puede configurar un nombre anónimo en vez de un ID de usuario para la fase 1 de una autenticación PEAP. Escriba entre 0 y 128 caracteres ASCII de 1 byte (0x20 a 0x7E).	
Intensidad de cifrado	Puede elegir uno de los siguientes.	
	Alto	AES256/3DES
	Medio	AES256/3DES/AES128/RC4

Configurar un certificado para IEEE 802.1X

Configure el Certificado de cliente de IEEE802.1X. Al configurarlo, puede usar **EAP-TLS** y **PEAP-TLS** como método de autenticación de IEEE 802.1x. Si desea configurar el certificado de la autoridad de certificación, vaya a **Certificado CA**.

1. Acceda a Web Config y seleccione la pestaña **Seguridad de red** > **IEEE802.1X** > **Certificado del cliente**.
2. Introduzca un certificado en el **Certificado del cliente**.

   Si ya ha importado un certificado publicado por una autoridad de certificación, puede copiarlo y usarlo en IEEE802.1X. Para copiarlo, seleccione el certificado en **Copiar desde** y, a continuación, haga clic en **Copiar**.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Solución de problemas de seguridad avanzada

Restauración de la configuración de seguridad

Cuando establece entorno de alta seguridad tal como un filtro IPsec/IP, es posible que no sea capaz de comunicarse con los dispositivos debido a una configuración incorrecta o por problemas con el dispositivo o el servidor. En este caso, restaure la configuración de seguridad para poder configurar nuevamente el dispositivo o para que le permita un uso temporal.

Deshabilitar la función de seguridad mediante Web Config

Puede desactivar IPsec/Filtrado de IP con Web Config.

1. Acceda a Web Config y seleccione la pestaña **Seguridad de red** > **IPsec/Filtrado de IP** > **Básica**.
2. Deshabilite el **IPsec/Filtrado de IP**.

Problemas en el uso de funciones de seguridad de red

He olvidado una clave previamente compartida

Reconfiguración de una clave previamente compartida.

Para cambiar la clave, acceda a Web Config y seleccione la pestaña **Seguridad de red** > **IPsec/Filtrado de IP** > **Básica** > **Norma predeterminada** o **Norma de grupo**.

Cuando cambie la clave previamente compartida, configúrela para los ordenadores.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36
➡ "Comunicación cifrada mediante el uso de filtro IPsec/IP" de la página 108

La comunicación mediante IPsec no funciona

Especifique el algoritmo que el escáner o el ordenador no admite.

El escáner admite los siguientes algoritmos. Compruebe la configuración del ordenador.

Métodos de seguridad	Algoritmos
Algoritmo de cifrado de IKE	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
Algoritmo de autenticación de IKE	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Algoritmo de intercambio de claves de 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 cifrado 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	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* disponible únicamente para IKEv2

Información relacionada

➡ "Comunicación cifrada mediante el uso de filtro IPsec/IP" de la página 108

He perdido la comunicación de repente

La dirección IP del escáner se ha modificado o no puede utilizarse.

Si se ha modificado o no puede utilizarse la dirección IP registrada como dirección local en Norma de grupo, no podrá llevarse a cabo la comunicación IPsec. Desactive IPsec con el panel de control del escáner.

Si DHCP está desfasado, se reinicia, o la dirección IPv6 está obsoleta o no se ha obtenido, es posible que no se encuentre la dirección IP registrada en Web Config para el escáner (pestaña **Seguridad de red** > **IPsec/Filtrado de IP** > **Básica** > **Norma de grupo** > **Dirección local(escáner)**) no se encuentra.

Utilice una dirección IP fija.

La dirección IP del ordenador se ha modificado o no puede utilizarse.

Si se ha modificado o no puede utilizarse la dirección IP registrada como dirección remota en Norma de grupo, no podrá llevarse a cabo la comunicación IPsec.

Desactive IPsec con el panel de control del escáner.

Si DHCP está desfasado, se reinicia, o la dirección IPv6 está obsoleta o no se ha obtenido, es posible que no se encuentre la dirección IP registrada en Web Config para el escáner (pestaña **Seguridad de red** > **IPsec/Filtrado de IP** > **Básica** > **Norma de grupo** > **Dirección remota(host)**) no se encuentra.

Utilice una dirección IP fija.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

➡ "Comunicación cifrada mediante el uso de filtro IPsec/IP" de la página 108

No se puede conectar después de configurar el filtro de IPsec/IP

La configuración de Filtrado IPsec/IP no es correcta.

Deshabilite el filtro IPsec/IP desde el panel de control del escáner. Conecte el escáner y el ordenador y realice de nuevo los ajustes del filtro de IPsec/IP.

Información relacionada

➡ "Comunicación cifrada mediante el uso de filtro IPsec/IP" de la página 108

No se puede acceder al escáner tras configurar IEEE 802.1X

La configuración de IEEE 802.1X no es correcta.

Desactive IEEE 802.1X y la conexión Wi-Fi desde el panel de control del escáner. Conecte el escáner y un ordenador y, a continuación, vuelva a configurar IEEE 802.1X.

Conecte el escáner y un ordenador y, a continuación, vuelva a configurar IEEE 802.1X.

Información relacionada

➡ "Configuración de una red IEEE 802.1X" de la página 120

Problemas de uso de un certificado digital

No puedo importar un Certificado firmado CA

El Certificado firmado CA y la información de la CSR no coinciden.

Si el Certificado firmado CA y la CSR no tienen los mismos datos, no se podrá importar la CSR. Revise los siguientes puntos:

❏ ¿Intenta importar el certificado a un dispositivo que tiene otros datos?
Revise los datos de la CSR y luego importe el certificado a un dispositivo que tenga los mismos datos.

❏ ¿Después de enviar la CSR a una entidad certificadora usted sobrescribió la CSR guardada en el escáner?
Vuelva a obtener el certificado firmado por entidad certificadora con la CSR.

El Certificado firmado CA pesa más de 5 KB.

No se puede importar un Certificado firmado CA de más de 5 KB.

La contraseña para importar el certificado es incorrecta.

Escriba la contraseña correcta. Si ha olvidado la contraseña, no podrá importar el certificado. Obtenga de nuevo el Certificado firmado CA.

Información relacionada

➡ "Importar un certificado firmado por la autoridad de certificación" de la página 103

No puedo actualizar un certificado de firma digital

No se ha introducido el Nombre común.

Tiene que escribir el **Nombre común**.

Se han introducido caracteres no válidos en el Nombre común.

Escriba entre 1 y 128 caracteres de uno de estos formatos: IPv4, IPv6, nombre de host o FQDN en ASCII (0x20–0x7E).

Se ha incluido una coma o un espacio en el nombre común.

Si tiene una coma, el **Nombre común** se divide en ese punto. Si solamente ha escrito un espacio antes o después de una coma, se producirá un error.

Información relacionada

➡ "Actualización de un certificado autofirmado" de la página 105

No puedo crear una CSR (Solicitud de firma de certificado)

No se ha introducido el Nombre común.

Debe introducir el **Nombre común**.

Se han introducido caracteres no válidos en Nombre común, Organización, Unidad organizativa, Localidad y Estado/Provincia.

Escriba caracteres de uno de estos formatos: IPv4, IPv6, nombre de host o FQDN en ASCII (0x20–0x7E).

Se ha incluido una coma o un espacio en el Nombre común.

Si tiene una coma, el **Nombre común** se divide en ese punto. Si solamente ha escrito un espacio antes o después de una coma, se producirá un error.

Información relacionada

➡ "Cómo obtener un certificado firmado por entidad certificadora" de la página 101

Aparece una advertencia relativa a un certificado digital

Mensajes	Causa/Qué hacer
Introduzca un certificado de servidor.	**Causa:** No ha seleccionado ningún archivo para importarlo. **Qué hacer:** Seleccione un archivo y haga clic en **Importar**.
No se ha introducido el Certificado CA 1.	**Causa:** No ha introducido el certificado de entidad certificadora 1, solamente el certificado de entidad certificadora 2. **Qué hacer:** Importe primero el certificado de entidad certificadora 1.
Valor no válido a continuación.	**Causa:** La ruta o la contraseña del archivo contienen caracteres no admitidos. **Qué hacer:** Compruebe que haya escrito los caracteres correctos para ese elemento.
Fecha y hora no válidas.	**Causa:** El escáner no tiene configurada la hora ni la fecha. **Qué hacer:** Configure la fecha y la hora con Web Config o con EpsonNet Config.
Contraseña no válida.	**Causa:** La contraseña configurada para el certificado de entidad certificadora no coincide con la contraseña que ha escrito. **Qué hacer:** Escriba la contraseña correcta.

Mensajes	Causa/Qué hacer
Archivo no válido.	**Causa:** El archivo del certificado que quiere importar no tiene el formato X509. **Qué hacer:** Seleccione el certificado correcto enviado por una entidad certificadora de confianza.
	Causa: El archivo que ha importado es demasiado grande. Se admiten archivos de 5 KB como máximo. **Qué hacer:** Si ha seleccionado el archivo correcto, es posible que el certificado esté dañado o que sea falso.
	Causa: La cadena que contiene el certificado no es válida. **Qué hacer:** Encontrará más información sobre el certificado en el sitio web de la entidad certificadora.
No se pueden usar los certificados de servidor que incluyen más de tres certificados CA.	**Causa:** El archivo del certificado de formato PKCS#12 contiene más de 3 certificados de entidad certificadora. **Qué hacer:** Importe los certificados de uno en uno, convirtiéndolos del formato PKCS#12 al formato PEM, o bien importe un archivo de certificados en formato PKCS#12 que contenga 2 certificados de entidad certificadora como máximo.
El certificado ha expirado. Compruebe si el certificado es válido, o bien, la Fecha y hora del producto.	**Causa:** El certificado ha caducado. **Qué hacer:** ❏ Si el certificado ha caducado, obtenga uno nuevo e impórtelo. ❏ Si el certificado no ha caducado, compruebe que la fecha y la hora configuradas en el escáner sean las correctas.
Se necesita una clave privada.	**Causa:** No hay ninguna clave privada emparejada con el certificado. **Qué hacer:** ❏ Si el certificado tiene el formato PEM/DER y se ha obtenido a partir de una CSR con un ordenador, especifique el archivo de la clave privada. ❏ Si el certificado tiene el formato PKCS#12 y se ha obtenido a partir de una CSR con un ordenador, guarde la clave privada en un archivo nuevo.
	Causa: Ha reimportado el certificado PEM/DER obtenido a partir de una CSR con Web Config. **Qué hacer:** Si el certificado tiene el formato PEM/DER y se ha obtenido a partir de una CSR con Web Config, solamente puede importarlo una vez.

Mensajes	Causa/Qué hacer
La configuración ha fallado.	**Causa:** No se puede finalizar la configuración porque existe un fallo de comunicación entre el escáner y el ordenador o algunos errores impiden la lectura del archivo. **Qué hacer:** Después de revisar el archivo especificado y la comunicación, vuelva a importar el archivo.

Información relacionada

➡ "Acerca de la certificación digital" de la página 101

He borrado un certificado firmado por entidad certificadora sin querer

No hay archivo de copia de seguridad del certificado firmado por entidad certificadora.

Si tiene el archivo de copia de seguridad, vuelva a importar el certificado.

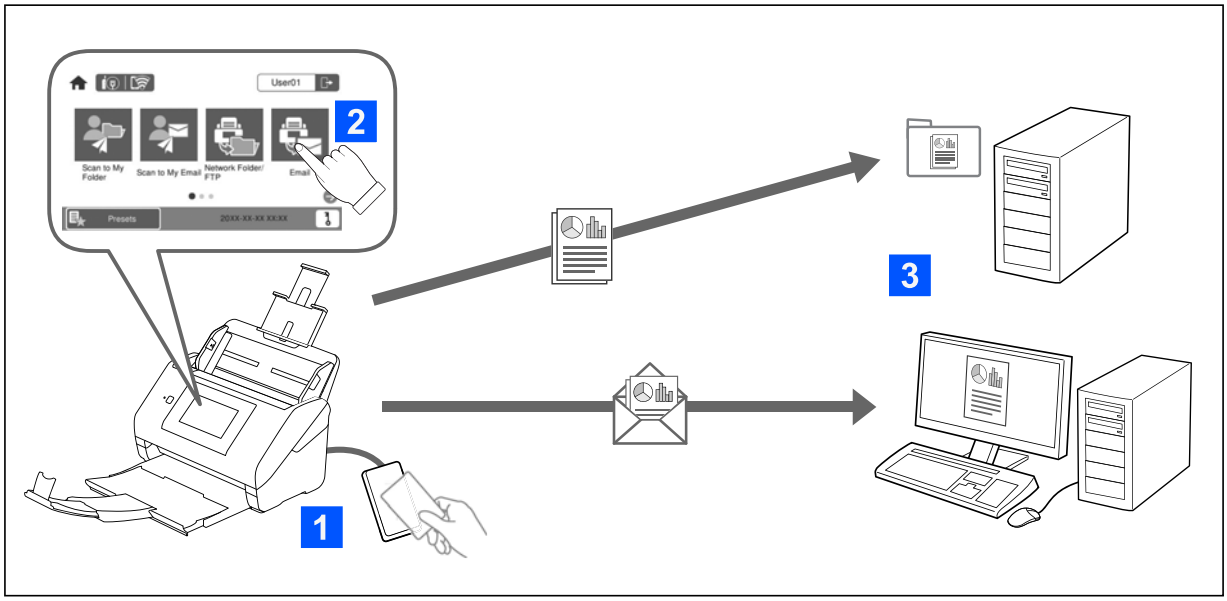
Si ha obtenido el certificado mediante una CSR creada con Web Config, no puede volver a importar un certificado borrado. Cree una CSR y obtenga un certificado nuevo.

Información relacionada

➡ "Importar un certificado firmado por la autoridad de certificación" de la página 103
➡ "Cómo eliminar un certificado firmado por entidad certificadora" de la página 104

Configuración de autenticación

Acerca de Configuración de autenticación



Si Configuración de autenticación está habilitado, se requiere la autenticación de usuario para escanear. Puede configurar los métodos de escaneado que puede utilizar cada usuario y evitar operaciones accidentales.

Puede especificar la dirección de correo electrónico del usuario autenticado como el destino del escaneado (Digital. a mi correo) o guardar los datos de cada usuario en una carpeta personal (Digital. a mi carpeta). También puede especificar otros métodos de escaneado.

Nota:

❏ *No es posible escanear desde un ordenador o un dispositivo inteligente si se ha habilitado Configuración de autenticación.*

❏ *Además del Configuración de autenticación que se describe en este manual, también puede crear un sistema de autenticación mediante un servidor de autenticación. Para crear un sistema, use Document Capture Pro Server Authentication Edition (el nombre abreviado es Document Capture Pro Server AE). Para obtener más información, póngase en contacto con la oficina local de Epson.*

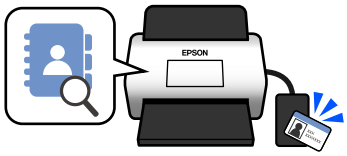
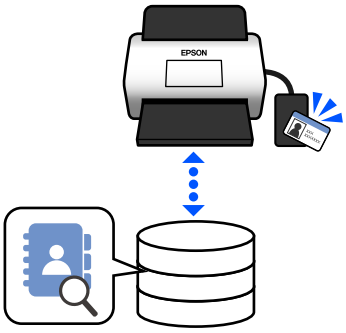
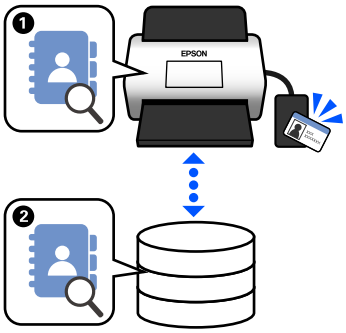
Funciones disponibles para Configuración de autenticación

Función de escaneado en el panel de control	Configuración de autenticación	
	Si está habilitado	Si está deshabilitado
Digitalizar a mi carpeta Guarda las imágenes en la carpeta asignada al usuario autenticado.	✓	-
Digitalizar a mi correo Envía las imágenes a la dirección de correo electrónico del usuario autenticado.	✓	-
Digitaliz. a car. red/FTP Guarda las imágenes en una carpeta de la red.	✓	✓

Función de escaneado en el panel de control	Configuración de autenticación	
	Si está habilitado	**Si está deshabilitado**
Digitalizar a PC Guarda las imágenes en un ordenador conectado utilizando trabajos creados en Document Capture Pro (Windows)/Document Capture (Mac OS). * Si Configuración de autenticación está habilitado, solo puede usar trabajos registrados en **Ajustes**.	✓*	✓
Dig. correo electrónico Envía las imágenes a la dirección de correo electrónico configurada.	✓	✓
Digitalizar a nube Envía las imágenes al servicio en la nube configurado.	✓	✓
Digitalizar a la unidad USB Guarda las imágenes en una unidad USB conectada al escáner. Esto solo está disponible si no hay ningún dispositivo de autenticación conectado al escáner.	✓	✓
Digitalizar a WSD Guarda las imágenes en un ordenador conectado mediante la función WSD.	-	✓
Ajustes Puede registrar hasta 48 funciones de escaneado predefinidas. Puede asignar hasta cinco Ajustes a los usuarios registrados en DB local. Los Ajustes asignados están disponibles solo para ese usuario. Los Ajustes que no se han asignado a ningún usuario pueden ser utilizados por todos los usuarios.	✓	✓

Acerca de Método de autenticación

Este escáner puede proporcionar la autenticación mediante los siguientes métodos, sin necesidad de tener que crear un servidor de autenticación.

	DB local	LDAP	DB local y LDAP
Ubicación de la información del usuario	**Memoria del escáner** Este método de autenticación comprueba la información del usuario registrada en el escáner y la compara con la del usuario que va a escanear.	**Servidor LDAP*** Este método de autenticación verifica comprueba información del usuario del servidor LDAP sincronizado con el escáner. Puesto que se pueden almacenar temporalmente hasta 300 elementos de información de usuario del servidor LDAP en la memoria intermedia del escáner, la autenticación se puede realizar utilizando dicha memoria en caso de que el servidor LDAP deje de funcionar. * Un servidor que proporciona un servicio de directorio que puede comunicarse con LDAP.	**Memoria del escáner y servidor LDAP** Compruebe primero la información del usuario registrada en el escáner (❶) y, si no hay ninguna coincide, verifique la información del usuario con el servidor LDAP (❷).
			
Número de usuarios registrados	50 (memoria del escáner)	Ilimitado (servidor LDAP)	50 (memoria del escáner) Ilimitado (servidor LDAP)
Caché de memoria del escáner	-	300	Máximo 300 (50 de las posiciones en la memoria caché se comparten con Ajustes usuario en DB local)
Métodos de inicio de sesión	Puede utilizar cualquiera de los siguientes métodos. ❏ Con una tarjeta de autenticación o introduciendo un **ID del usuario** y una **Contraseña** ❏ Con una tarjeta de autenticación o introduciendo un **Número de identidad** ❏ Introduciendo un **ID del usuario** y una **Contraseña** ❏ Introduciendo un **ID del usuario** ❏ Introduciendo un **Número de identidad**		
Límites de la función «Escanear a»	Se establece individualmente para cada usuario	Misma configuración para todos los usuarios de LDAP	Usuarios de DB local: se establece individualmente Usuarios de LDAP: misma configuración para todos los usuarios
Asignación de Ajustes a usuarios	Hasta 5 por usuario	- (No se puede configurar individualmente)	Usuarios de DB local: hasta 5 por usuario Usuarios de LDAP: -

Software de configuración

Configure con Web Config o Epson Device Admin.

❏ Si utiliza Web Config, puede configurar el escáner utilizando solamente un explorador web.
"Web Config" de la página 36

❏ Si utiliza Epson Device Admin, puede configurar varios escáneres a la vez con una plantilla de configuración.
"Epson Device Admin" de la página 37

Actualización del firmware del escáner

Antes de habilitar Configuración de autenticación, actualice el firmware del escáner a la última versión. Conecte antes el escáner a Internet.

Importante:
No apague el ordenador ni el escáner durante la actualización.

Si configura desde Web Config:

Seleccione la pestaña **Gestión del dispositivo** > **Actualización del firmware** y siga las instrucciones que aparecen en pantalla para actualizar el firmware.

Si configura desde Epson Device Admin:

Seleccione la pestaña **Inicio** > **Firmware** > **Actualizar** en la pantalla de la lista de dispositivos y siga las instrucciones que aparecen en pantalla para actualizar el firmware.

Nota:
Si el firmware más reciente ya está instalado, no es necesario que lo actualice.

Conexión y configuración de un dispositivo de autenticación

Si desea conectarse a un dispositivo de autenticación para utilizarlo, como un lector de tarjetas IC, antes debe configurar el dispositivo. Esto no es necesario si no utiliza un dispositivo de autenticación.

Información relacionada

➡ "Conexión del dispositivo de autenticación" de la página 135
➡ "Configuración del dispositivo de autenticación" de la página 136

Lista de lectores de tarjetas compatibles

Esta lista no garantiza el funcionamiento de los lectores de tarjetas enumerados.

Sí: compatible (la información de identificación se puede leer con la configuración estándar del lector de tarjetas).

No: no compatible

Fabricante	Modelo	Número de modelo	Tarjeta de autenticación							Modo
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (Type B) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
RF IDEAS	pcProx Plus	RDR-80081AKU	Sí	Sí*1	Sí*1	Sí*1	No	No	No	Teclado
RF IDEAS	pcProx	RDR-7081BKU	Sí*1	No	Sí	Sí	No	No	No	Teclado
RF IDEAS	pcProx	RDR-7581AKU	Sí	No	Sí*1	Sí*1	No	No	No	Teclado
ELATEC	TWN3 MIFARE	T3DT--MB2BEL T3DT--MB2WEL	No	No	Sí	Sí	No	No	No	Teclado
ELATEC	TWN3 MIFARE NFC	T3DT--FB2BEL T3DT--FB2WEL	Sí	No	Sí	Sí	Sí	Sí	Sí	Teclado
ELATEC	TWN4 MULTI-TECH	T4DT--FB2BEL-PI T4DT--FB2WEL-PI	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Teclado
ELATEC	TWN4 Multi-Tech 2 BLE-PI	T4LK--FB4BLZ-PI	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Teclado
ELATEC	TWN4 Slim	T4QC--FC3B7	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Teclado

Fabricante	Modelo	Número de modelo	Tarjeta de autenticación							Modo
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (Type B) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
HID Global	OMNIKEY 5427	OMNIKEY5427CK OMNIKEY5427CK gen2	Sí	Sí	Sí	Sí	Sí	No	Sí	Teclado[*1]
ACS	ACR122U	ACR122U	No	No	Sí[*2]	Sí[*2]	Sí	No	Sí[*2]	PC/SC
ACS	ACR1252	ACR1252	No	No	Sí[*2]	Sí[*2]	Sí	Sí	Sí[*2]	PC/SC
Sony	PaSoRi	RC-S330/S	No	No	Sí[*2]	Sí[*2]	Sí[*2]	Sí[*2]	Sí[*2]	PaSoRi
Sony	PaSoRi	RC-S380/P RC-S380/S	No	No	Sí[*2]	Sí[*2]	Sí[*2]	Sí[*2]	Sí[*2]	PaSoRi
DMZ	Leitor RFID Universal	DMZ008	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Teclado
DMZ	Leitor RFID Multi-125	DMZ087	No	Sí	No	No	No	No	No	Teclado
DMZ	Leitor RFID Mifare	DMZ088	No	No	Sí	Sí	No	No	No	Teclado
DMZ	Biometric & RFID Reader	DMZ073	No	Sí	No	No	No	No	No	Teclado
inepro	SCR708	SCR708	Sí[*1]	Sí[*1]	Sí[*1]	Sí[*1]	Sí[*1]	Sí[*1]	Sí[*1]	Teclado
Y Soft	YU03088 001	MU0388	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Teclado

Fabricante	Modelo	Número de modelo	Tarjeta de autenticación							Modo
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (Type B) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
Cartadis	TCM3 Cartadis MiFare Card Reader	ZTCM3--MIFARE	No	No	Sí	Sí	No	No	Sí	Teclado
MICI Network Co., Ltd.	EM & Mifare Card Reader	mCR-600	No	No	Sí	Sí	No	No	Sí	Teclado
NT-ware	MiCard Multi-Tech4--PI	T4DT--FB4WUF-PI	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Teclado
NT-ware	MiCard Plus-2--V2	RDR-80081AGU--NT2-20	Sí*1	Sí*1	Sí*1	Sí*1	No	No	No	Teclado
NT-ware	MiCard V3 Multi	MiCard V3 Multi	Sí	Sí	Sí	Sí	Sí	Sí	No	Teclado

*1 Necesita cambiar la configuración del lector de tarjetas mediante el software proporcionado por el fabricante del lector.

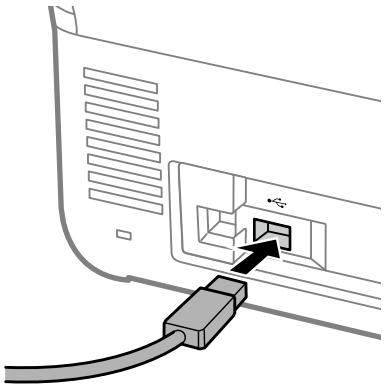
*2 Si necesita utilizar datos de un área en concreto de la tarjeta que no sea el ID estándar de la tarjeta como ID de autenticación para configurar el producto, póngase en contacto con su asociado o representante local de Epson para obtener más información sobre la forma de configurar el producto.

Conexión del dispositivo de autenticación

Importante:

Si conecta el dispositivo de autenticación a varios escáneres, utilice un producto con el mismo número de modelo.

Conecte el cable USB del lector de tarjetas al puerto USB de la interfaz externa del escáner.



Comprobación del funcionamiento del dispositivo de autenticación

El estado de la conexión y el reconocimiento de la tarjeta de autenticación del dispositivo de autenticación se puede comprobar desde el panel de control del escáner.

La información se muestra si selecciona **Configuración** > **Información del dispositivo** > **Estado del dispositivo de autenticación**.

Configuración del dispositivo de autenticación

Establezca el formato de lectura de la información de autenticación recibida de una tarjeta de autenticación.

Puede establecer el siguiente método de lectura para el dispositivo de autenticación.

❏ Lea el área específica de la tarjeta de autenticación, como el número de empleado o el ID personal.

❏ Utilice la información de la tarjeta de autenticación, excepto el UID (información de la tarjeta de autenticación, como el número de serie).

Puede utilizar una herramienta para generar los parámetros de funcionamiento. Pregunte los detalles a su proveedor.

Nota:
Uso de tarjetas de autenticación de diferentes fabricantes:

Cuando use la información de la tarjeta UID (información de identificación de la tarjeta, como el número de serie), puede usar una combinación de diferentes tipos de tarjetas de autenticación. Esto no se puede mezclar cuando se usa otra información de tarjeta.

Si configura desde Web Config:

Seleccione la pestaña **Gestión del dispositivo** > **Lector de tarjetas**.

Si configura desde Epson Device Admin:

Seleccione **Ajustes del administrador** > **Configuración de autenticación** > **Lector de tarjetas** en la plantilla de configuración.

Elemento	Explicación
Vendor ID	Establezca la ID del vendedor del dispositivo de autenticación, que limita el uso de 0000 a FFFF utilizando 4 caracteres alfanuméricos. Si no desea limitarlo, ajústelo en 0000.

Elemento	Explicación
Product ID	Establezca el ID del producto del dispositivo de autenticación que limita el uso de 0000 a FFFF utilizando 4 caracteres alfanuméricos. Si no desea limitarlo, ajústelo en 0000.
Parámetro operacional	Establezca el parámetro de funcionamiento del dispositivo de autenticación entre 0 y 8192 caracteres. A–Z, a–z, 0–9, +, /, =, espacio y avance de línea están disponibles.
Lector de tarjetas	Seleccione el formato de conversión del dispositivo de autenticación. Puede comprobar los detalles del formato. Consulte el enlace proporcionado en la descripción del elemento.
Formato de almacenamiento de ID de tarjeta de autenticación	Seleccione el formato de conversión de la información de autenticación de una tarjeta de ID. Puede comprobar los detalles del formato. Consulte el enlace proporcionado en la descripción del elemento.
Establecer intervalo del identificador de tarjeta	Habilite la especificación de la posición de lectura.
Posición de inicio del texto	Especifique la posición de inicio del texto para leer la información de identificación. Puede especificarla entre 1 y 4096.
Número de caracteres	Especifique el número de caracteres a leer desde la posición inicial de la información de identificación. Puede especificarla entre 1 y 4096.

Registro y configuración de la información

Configuración

Realice los ajustes necesarios en función del Método de autenticación y del método de escaneado que utilice.

Importante:

Antes de iniciar la configuración, compruebe que el escáner tiene la hora correcta.

Si la hora no está bien ajustada, se muestra un mensaje de error indicando que «La licencia ha caducado», que puede hacer que no se pueda configurar escáner. Además, para usar una función de seguridad como la comunicación SSL/TLS o IPsec, es necesario ajustar la hora correcta. Puede ajustar la hora de la siguiente manera.

❏ *Web Config: pestaña* ***Gestión del dispositivo*** > ***Fecha y hora*** > ***Fecha y hora****.*

❏ *Panel de control del escáner:* ***Configuración*** > ***Config. básica*** > ***Conf. de fecha y hora****.*

Ajustes	DB local	LDAP	DB local y LDAP
Habilitar la autenticación Antes de configurar la autenticación, es necesario habilitarla. "Habilitar la autenticación" de la página 138	✓	✓	✓
Configuración de autenticación Configuración de Método de autenticación y cómo autenticar usuarios. "Configuración de autenticación" de la página 139	✓	✓	✓

Ajustes	DB local	LDAP	DB local y LDAP
Registro de Ajustes usuario Registra la configuración de cada usuario. También puede registrar a muchos usuarios a la vez mediante un archivo CSV. "Registro de Ajustes usuario" de la página 140	✓	–	✓
Sincronización con el Servidor LDAP Configura la sincronización del servidor LDAP. "Sincronización con el Servidor LDAP" de la página 146	–	✓	✓
Configuración de Servidor correo electrónico Establece la configuración del servidor de correo electrónico. Configúrelo cuando utilice funciones que requieran la configuración del servidor de correo electrónico, como Digital. a mi correo. "Configuración del servidor de correo electrónico" de la página 150	✓	✓	✓
Configuración de Digital. a mi carpeta Configura las carpetas de destino. Realice este ajuste cuando utilice la función Digital. a mi carpeta. "Configuración de Digital. a mi carpeta" de la página 151	✓	✓	✓
Personalizar funciones de un toque Realice este ajuste para cambiar los elementos que se muestran en el panel de control del escáner. Puede mostrar en el panel de control solo los iconos que necesite o cambiar su orden. "Personalizar funciones de un toque" de la página 153	✓	✓	✓

Habilitar la autenticación

Antes de configurar la autenticación, es necesario habilitarla.

Si configura desde Web Config:

Seleccione **Activado (dispositivo/Servidor LDAP)** en la pestaña **Seguridad del producto** > **Básica** > **Autenticación**.

Si configura desde Epson Device Admin:

En la plantilla de configuración, seleccione **Activado (dispositivo/Servidor LDAP)** en **Ajustes del administrador** > **Configuración de autenticación** > **Básicos** > **Autenticación**.

Nota:
Si habilita Configuración de autenticación en el escáner, Configuración bloqueo también estará habilitado para el panel de control. El panel de control no se puede desbloquear si Configuración de autenticación está habilitado.

Aunque deshabilite Configuración de autenticación, Configuración bloqueo permanece habilitado. Si desea deshabilitarlo, puede realizar los ajustes desde el panel de control o Web Config.

Información relacionada

➡ "Ajuste de Configuración bloqueo desde el panel de control" de la página 88

➡ "Configuración de Configuración bloqueo desde Web Config" de la página 88

Configuración de autenticación

Configuración de Método de autenticación y cómo autenticar usuarios.

Si configura desde Web Config:

Seleccione la pestaña **Seguridad del producto** > **Configuración de autenticación**.

Si configura desde Epson Device Admin:

Seleccione **Ajustes del administrador** > **Configuración de autenticación** > **Configuración de autenticación** en la plantilla de configuración.

Elemento	Explicación
Método de autenticación	Seleccione Método de autenticación. ❏ DB local Realiza la autenticación utilizando el Ajustes usuario registrado en el escáner. Es necesario registrar al usuario en el escáner. ❏ LDAP Realice la autenticación usando la información del usuario del servidor LDAP sincronizado con el escáner. Necesita configurar los ajustes del servidor de LDAP con antelación. ❏ DB local y LDAP Realice la autenticación utilizando la información del usuario registrada en el escáner o en el servidor LDAP sincronizado con el escáner. Necesita registrar al usuario en el escáner y configurar el servidor LDAP.
Cómo autenticar al usuario	Seleccione cómo autentificar a un usuario. ❏ Tarjeta o Id. de usuario y contraseña Utilice una tarjeta para autentificar a los usuarios. También puede usar una ID y una contraseña de usuario para autentificarse. ❏ Id. de usuario y contraseña Utilice una ID y una contraseña de usuario para autentificar usuarios. Si selecciona esta función, no puede utilizar una tarjeta para autentificarse. ❏ ID del usuario Utilice solo una ID de usuario para autentificar usuarios. No es necesario establecer una contraseña. ❏ Tarjeta o Número de identidad Utilice una tarjeta para autentificar a los usuarios. También puede usar un Número de identidad. ❏ Número de identidad Utilice solo un número de ID para autentificar usuarios.
Permitir al usuario registrar tarjetas de autenticación	Habilítelo si desea permitir que los usuarios registren la tarjeta de autenticación en el sistema. Si selecciona **LDAP** para **Método de autenticación**, no puede configurarlo. Para obtener más información sobre la forma en la que los usuarios pueden registrar sus tarjetas de autenticación, consulte «Registro de una tarjeta de autenticación» en *Manual de usuario*.

Elemento	Explicación
Número mínimo de dígitos de Número de identidad	Seleccione el número mínimo de dígitos del número de ID.
Almacenamiento en caché para usuarios autenticados LDAP	Cuando usa la autenticación del servidor LDAP, puede establecer si se usa o no el almacenamiento en caché para la información del usuario.
Usar información del usuario en la autenticación SMTP	Cuando usa una identificación del usuario y una contraseña para la autenticación, puede establecer si se usa o no la información del usuario para la autenticación SMTP. El sistema usa la última identificación del usuario y contraseña que se registraron.
Restricciones para usuarios autenticados LDAP	Si utiliza LDAP, puede configurar qué funciones están disponibles para el usuario.

Registro de Ajustes usuario

Registre la Ajustes usuario utilizada para la autenticación del usuario. Puede registrarla utilizando cualquiera de los siguientes métodos.

❏ Registro Ajustes usuario uno por uno (Web Config)

❏ Registro de varias Ajustes usuario en lote mediante un archivo CSV (Web Config)

❏ Registro de la Ajustes del usuario en varios escáneres en lote mediante una plantilla de configuración (Epson Device Admin)

Información relacionada

➡ "Registro individual de Ajustes usuario (Web Config)" de la página 140

➡ "Registro de varias Ajustes usuario mediante un archivo CSV (Web Config)" de la página 141

➡ "Registro de Ajustes del usuario en varios escáneres en lote (Epson Device Admin)" de la página 144

Registro individual de Ajustes usuario (Web Config)

Acceda a Web Config y seleccione la pestaña **Seguridad del producto** > **Ajustes usuario** > **Añadir** y, a continuación, introduzca la Ajustes usuario.

Elemento	Explicación
ID del usuario	Introduzca el ID de usuario que desee utilizar para la autenticación dentro de un intervalo de 1 a 83 bytes, que se puede expresar en Unicode (UTF-8). Dado que el nombre de identificación de usuario no distingue entre mayúsculas y, puede iniciar sesión utilizando letras mayúsculas o minúsculas.
Visualización del nombre del usuario	Introduzca el nombre de usuario que se muestra en el panel de control del escáner con el máximo de 32 caracteres de Unicode (UTF-16). Puede dejarlo en blanco.
Contraseña	Introduzca la contraseña que desea usar para la autenticación con un máximo de 32 caracteres en ASCII. La contraseña distingue entre mayúsculas y minúsculas. Déjelo en blanco si selecciona **ID del usuario** para **Cómo autenticar al usuario**.

Elemento	Explicación
ID de tarjeta de autenticación	Introduzca el ID de la tarjeta de autenticación con un máximo de 116 caracteres en ASCII. Puede dejarlo en blanco. Si permite **Permitir al usuario registrar tarjetas de autenticación** para **Configuración de autenticación**, se refleja el resultado registrado por los usuarios.
Número de identidad	Este elemento se muestra si se selecciona **Tarjeta o Número de identidad** o **Número de identidad** en **Configuración de autenticación** > **Cómo autenticar al usuario**. Introduzca un número entre el indicado en **Configuración de autenticación** > **Número mínimo de dígitos de Número de identidad**, un máximo de 8 dígitos.
Generar automáticamente	Este elemento se muestra si se selecciona **Tarjeta o Número de identidad** o **Número de identidad** en **Configuración de autenticación** > **Cómo autenticar al usuario**. Haga clic para generar automáticamente un número de identificación con el mismo número de dígitos seleccionado en **Número mínimo de dígitos de Número de identidad**.
Departamento	Introduzca, por ejemplo, el nombre del departamento y que identifique al usuario con un máximo de 40 caracteres para Unicode (UTF-16). Puede dejarlo en blanco.
Dirección de correo	Introduzca la dirección de correo electrónico del usuario con un máximo de 200 caracteres ASCII. Esta se utiliza como destino para **Digital. a mi correo**. Puede dejarlo en blanco.
Digital. a mi carpeta	Configure indivisamente los destinos de guardado cuando seleccione **Individual** en **Digital. a mi carpeta** > **Tipo de ajustes**. Consulte lo siguiente para obtener más información sobre los elementos de ajuste. "Configuración de Digital. a mi carpeta" de la página 151
Restricciones	Puede restringir las funciones para cada usuario. Seleccione la función que desea permitir utilizar.
Ajustes	Puede configurar hasta cinco valores predefinidos, que solamente están disponibles para el usuario seleccionado en la Ajustes registrada en la impresora. ❏ Los Ajustes asignados a un usuario solo pueden ser utilizados por ese usuario. Los Ajustes que no se han asignado a ningún usuario pueden ser utilizados por todos los usuarios. ❏ Si un usuario solo tiene un Ajustes disponible, se carga automáticamente después de la autenticación. Si hay varios Ajustes disponibles, se muestra una lista de Ajustes después de la autenticación. ❏ No es posible crear ni mostrar Ajustes que usen funciones que han sido restringidas en **Restricciones**.

Registro de varias Ajustes usuario mediante un archivo CSV (Web Config)

Introduzca la configuración de cada usuario en un archivo CSV y regístrelos en lote.

Crear un archivo CSV

Cree un archivo CSV para importar Ajustes usuario.

Nota:
Si registra uno o más Ajustes usuario de antemano y luego exporta un archivo formateado (archivo CSV), puede usar la configuración registrada como referencia para ingresar elementos de configuración.

1. Acceda a Web Config y seleccione la pestaña **Seguridad del producto** > **Ajustes usuario**.
2. Haga clic en **Exportar**.
3. Seleccione el formato de archivo de **Formato de archivo**.

   Selecciónelo según se indica describe a continuación.

Elemento	Explicación
CSV UTF-16 (delimitado por tabulaciones)	Seleccione esta opción para editar el archivo usando Microsoft Excel. Cada parámetro va entre «[ ]» (corchetes). Introduzca los parámetros entre «[ ]». Cuando actualice el archivo, le recomendamos que lo sobrescriba. Si guarda un el archivo por primera vez, seleccione el formato de texto Unicode (*.txt).
CSV UTF-8 (delimitado por comas)	Seleccione esta opción para editar el archivo mediante un editor de texto o una macro sin Microsoft Excel.
CSV UTF-8 (delimitado por puntos y coma)	

4. Haga clic en **Exportar**.
5. Edite y guarde este archivo CSV en una aplicación de hoja de cálculo como Microsoft Excel o en un editor de texto.

> ***Importante:***
> *Cuando edite el archivo, no modifique la información de codificación y del encabezado.*

Elementos de configuración de archivos CSV

Elemento	Ajustes y explicación
UserID	Introduzca el ID de usuario para usar la autentificación de entre 1 y 83 bytes en Unicode.
UserName	Introduzca el nombre de usuario que se muestra en el panel de control de la escáner con un máximo de 32 caracteres en Unicode. Puede dejarlo en blanco.
Password	Introduzca la contraseña para usar la autenticación con 32 caracteres ASCII. Cuando realiza la importación, esto se establece como la contraseña en lugar de **EncPassword**. Déjelo en blanco si selecciona **ID del usuario** para **Cómo autenticar al usuario**. Cuando realiza la exportación, esto siempre se deja en blanco.

Elemento	Ajustes y explicación
AuthenticationCardID	Establece el resultado de la lectura de la tarjeta de autenticación. Si permite **Permitir al usuario registrar tarjetas de autenticación** en **Configuración de autenticación**, se refleja el resultado registrado por los usuarios. Introduzca hasta 116 caracteres ASCII. Puede dejarlo en blanco.
IDNumber	Este elemento se muestra si se selecciona **Tarjeta o Número de identidad** o **Número de identidad** en **Configuración de autenticación** > **Cómo autenticar al usuario**. Introduzca un número entre el indicado en **Configuración de autenticación** > **Número mínimo de dígitos de Número de identidad**, un máximo de 8 dígitos. El número de ID no puede estar duplicado. Si está duplicado, se le alertará del error al importar el archivo. Cuando se deja en blanco, se asigna un número automáticamente.
Department	Introduzca un nombre cualquiera para el departamento para distinguir a los usuarios. Introduzca un máximo de 40 caracteres en Unicode. Puede dejarlo en blanco.
MailAddress	Establezca la dirección de correo electrónico de los usuarios. Esta se utiliza como destino para **Digital. a mi correo**. Puede utilizar A-Z, a-z, 0-9, !#'%&'*+-./=?^_{|}~@. Escriba un máximo de 200 caracteres. Para el primer carácter no se puede utilizar «,» (coma). Puede dejarlo en blanco.
FolderProtocol	Establezca el tipo de la función Digital. a mi carpeta. Carpeta de red/FTP (SMB): 0, FTP: 1
FolderPath	Establezca el destino de almacenamiento para la función Digital. a mi carpeta.
FolderUserName	Establezca el nombre de usuario para la función Digital. a mi carpeta.
FolderPassword	Establezca la contraseña para autenticar la carpeta de destino para la función Digital. a mi carpeta (no puede tener más de 32 caracteres ASCII). Cuando realiza la importación, esto se establece como la contraseña en lugar de **EncPassword**. Cuando realiza la exportación, esto siempre se deja en blanco.
FtpPassive	Establezca el modo de conexión para el servidor FTP cuando **FTP** se selecciona para **Tipo** para la función Digital. a mi carpeta. Modo activo: 0, Modo pasivo: 1
FtpPort	Establezca el número de puerto para enviar datos digitalizados al servidor FTP de 0 a 65535 cuando **FTP** se selecciona como **Tipo** para la función Digital. a mi carpeta.
ScanToMemory	Establezca las restricciones para Digitalizar a la unidad USB. No permitido: 0, Permitido: 1
ScanToMail	Establezca las restricciones para Dig. a correo electrónico. Solamente puede configurar **Digitalizar a mi correo** si se ha habilitado **Dig. a correo electrónico**. No permitido: 0, Permitido: 1
ScanToFolder	Establezca las restricciones para Digitaliz. a carpeta red/FTP. Solamente puede configurar **Digitalizar a mi carpeta** si se ha habilitado **Digitaliz. a carpeta red/FTP**. No permitido: 0, Permitido: 1

Elemento	Ajustes y explicación
ScanToCloud	Establezca las restricciones para Digitalizar a cloud. No permitido: 0, Permitido: 1
ScanToComputer	Establezca las restricciones para Digitalizar a PC. No permitido: 0, Permitido: 1
PresetIndex	Establezca los Ajustes que desee asociar al usuario. Puede configurar hasta cinco números de registro de Ajustes separados por comas.
EncPassword	Si al exportar la configuración del usuario el parámetro ajustado para **Password** está cifrado, el valor se codifica con BASE64 y se le da salida. Al importar con la nueva contraseña de **Password**, este valor se ignora. Si **Password** está en blanco, se utiliza este valor y la contraseña permanece como estaba antes de la exportación.
EncFolderPassword	Al exportar, el conjunto de parámetros de **FolderPassword** está encriptado, el valor se codifica con BASE64 y se le da salida. Al importar con la nueva contraseña de **FolderPassword**, este valor se ignora. Si **FolderPassword** está en blanco, se utiliza este valor y la contraseña permanece como estaba antes de la exportación.

Importación de un archivo CSV

1. Acceda a Web Config y seleccione la pestaña **Seguridad del producto** > **Ajustes usuario**.
2. Haga clic en **Importar**.
3. Seleccione el archivo que desee importar.
4. Haga clic en **Importar**.
5. Una vez verificada la información mostrada, haga clic en **Aceptar**.

Registro de Ajustes del usuario en varios escáneres en lote (Epson Device Admin)

Puede registrar en lote el Ajustes del usuario usado en DB local con un servidor LDAP o un archivo CSV/ENE.

Nota:
*Un archivo ENE es un archivo binario que proporciona Epson y que cifra y guarda la información de los **Contactos** como información personal y la Ajustes usuario. Se puede exportar desde Epson Device Admin y definir una contraseña. Resulta útil si se desea importar la Ajustes usuario desde el archivo de copia de seguridad.*

Importación desde un archivo CSV/ENE

1. Seleccione **Ajustes del administrador** > **Configuración de autenticación** > **Ajustes del usuario** en la plantilla de configuración.

2. Haga clic en **Importar**.

3. Seleccione **Archivo CSV o ENE** en el **Origen de importación**.

4. Haga clic en **Examinar**.

   Se muestra la pantalla de selección de archivos.

5. Seleccione el archivo que desee importar para abrirlo.

6. Seleccione un método de importación.

   ❏ Sobrescribir y agregar: si existe el mismo ID de usuario, se sobrescribe; si no existe se añade una nueva ID.

   ❏ Reemplazar todo: sustituye todo con la configuración de usuario que desea importar.

7. Haga clic en **Importar**.

   Se mostrará la pantalla de confirmación del ajuste.

8. Haga clic en **Aceptar**.

   Se mostrará el resultado de la validación.

   Nota:

   ❏ *Si el número de configuraciones de usuario importadas supera el número máximo permitido, aparecerá un mensaje indicándole que debe eliminar algunas configuraciones de usuario. Elimine las configuraciones de usuario que no necesite antes de importar.*

   ❏ *Seleccione la configuración de usuario que desea eliminar antes de importar y, a continuación, haga clic en **Borrar**.*

9. Haga clic en **Importar**.

   La configuración del usuario se importa a la plantilla de configuración.

Importación desde el servidor LDAP

1. Seleccione **Ajustes del administrador** > **Configuración de autenticación** > **Ajustes del usuario** en la plantilla de configuración.

2. Haga clic en **Importar**.

3. Seleccione **LDAP** en el **Origen de importación**.

4. Haga clic en **Ajustes**.

   Se muestra la configuración de **Servidor LDAP**.

   Nota:

   Esta configuración es para importar la configuración del usuario desde el servidor LDAP. La configuración de usuario importada (copiada) se utiliza para la autenticación de los usuarios mediante el escáner.

   *Por otro lado, si selecciona **LDAP** o **DB local y LDAP** como método de autenticación, los usuarios se autentican comunicándose con el servidor LDAP.*

5. Configure cada elemento.

   Al importar configuraciones de usuario desde un servidor LDAP, también puede realizar los siguientes ajustes.

Para otros elementos, consulte Información relacionada.

Elemento			Explicación
Configuración del servidor LDAP	Tipo de servidor LDAP		Le permite seleccionar el tipo de servidor LDAP.
Configuración de búsqueda	Filtro de búsqueda		Puede configurar el texto utilizado para el filtro de búsqueda de LDAP. Seleccione **Personaliz** para editar el texto de búsqueda.
	Opciones	Tipo	Indica el tipo de destino de guardado para **Digitalizar y enviar a mi carpeta**.
		Modo de conexión	Si **Tipo** está configurado en **FTP**, se puede configurar el modo de conexión FTP.
		Número de puerto	Si **Tipo** está configurado en **FTP**, puede configurar el número de puerto que desea usar.

6. Realice la prueba de conexión si es necesario haciendo clic en **Prueba de conexión**.

   Adquiere y muestra 10 configuraciones de usuario del servidor LDAP.

7. Haga clic en **Aceptar**.

8. Seleccione un método de importación.

   ❏ Sobrescribir y agregar: si existe el mismo ID de usuario, se sobrescribe; si no existe se añade una nueva ID.

   ❏ Reemplazar todo: sustituye todo con la configuración de usuario que desea importar.

9. Haga clic en **Importar**.

   Se mostrará la pantalla de confirmación del ajuste.

10. Haga clic en **Aceptar**.

    Se mostrará el resultado de la validación.

11. Haga clic en **Importar**.

    La configuración del usuario se importa a la plantilla de configuración.

Información relacionada

➡ "Configurar un servidor LDAP" de la página 147

➡ "Configuración de los ajustes de búsqueda del servidor LDAP" de la página 148

Sincronización con el Servidor LDAP

Realice los ajustes de Servidor LDAP para el escáner.

Realice los ajustes necesarios tanto para el servidor principal como para el secundario.

Nota:
*La configuración de **Servidor LDAP** es compartida con **Contactos**.*

Servicios disponibles

Se admiten los siguientes servicios de directorio.

Nombre del Servicio	Versión
Active Directory	Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
OpenLDAP	Ver.2.3, Ver.2.4

Configurar un servidor LDAP

Para utilizar un servidor LDAP, antes debe configurarlo.

Si configura desde Web Config:

Seleccione la pestaña **Red** > **Servidor LDAP** > **Básica (Servidor principal)** o **Básica (Servidor secundario)**.

Si selecciona **Autenticación Kerberos** como **Método de autenticación**, seleccione **Red** > **Config. Kerberos** para configurar Kerberos.

Si configura desde Epson Device Admin:

Seleccione **Red** > **Servidor LDAP** > **Ajustes del servidor (Servidor principal)** o **Ajustes del servidor (Servidor secundario)** en la plantilla de configuración.

Si selecciona **Autenticación Kerberos** como **Método de autenticación**, seleccione **Red — Seguridad** > **Config. Kerberos** para configurar Kerberos.

Elemento	Ajustes y explicación
Usar serv. LDAP	Seleccione **Uso** o **No usar**.
Dirección serv. LDAP	Introduzca la dirección del servidor LDAP. Escriba entre 1 y 255 caracteres en formato IPv4, IPv6 o FQDN. Para el formato FQDN, puede utilizar caracteres alfanuméricos en ASCII (0x20–0x7E) y guiones, salvo al principio y al final de la dirección.
Nº puerto serv. LDAP (Número de puerto)	Introduzca el número de puerto del servidor LDAP entre 1 y 65535.
Conexión segura	Especifique el método de autenticación para que el escáner acceda al servidor LDAP.
Validación de certificado	El certificado del servidor LDAP se autenticará si se habilita esta opción. Es recomendable configurarlo como **Activar**. Para configurarlo, el **Certificado CA** debe ser importado al escáner.
Tiempo espera búsqueda (seg.)	Establezca el tiempo (entre 5 y 300) límite para realizar una búsqueda.

Elemento	Ajustes y explicación
Método de autenticación	Seleccione el método de autenticación. Si selecciona **Autenticación Kerberos**, configure Kerberos de antemano. Para realizar la Autenticación Kerberos es necesario el siguiente entorno. ❏ El escáner y el servidor DNS pueden comunicarse entre sí. ❏ La hora del escáner, el servidor KDC y el servidor necesario para la autenticación (servidor LDAP, servidor SMTP, servidor de archivos) está sincronizada. ❏ Si el servidor de servicio se asigna como la dirección IP, el FQDN del servidor de servicio se registra en la zona de búsqueda inversa del servidor DNS.
Dominio kerberos para utilizar	Si selecciona **Autenticación Kerberos** como **Método de autenticación**, seleccione el dominio Kerberos que quiera utilizar.
DN de administrador / Nombre de usuario	Escriba el nombre de usuario para el servidor LDAP en 128 caracteres Unicode (UTF-8) o menos. No pueden utilizarse caracteres de control, como 0x00 a 0x1F y 0x7F. Este ajuste no se puede utilizar cuando se ha seleccionado **Autenticación anónima** como **Método de autenticación**. Si no quiere especificarlo, déjelo en blanco.
Contraseña	Introduzca la contraseña de autenticación del servidor LDAP en 128 caracteres Unicode (UTF-8) o menos. No pueden utilizarse caracteres de control, como 0x00 a 0x1F y 0x7F. Este ajuste no se puede utilizar cuando se ha seleccionado **Autenticación anónima** como **Método de autenticación**. Si no quiere especificarlo, déjelo en blanco.

Configuración del protocolo Kerberos

Si selecciona **Autenticación Kerberos** como **Método de autenticación**, debe configurar Kerberos. Puede registrar hasta 10 configuraciones de Kerberos.

Si configura desde Web Config:

Seleccione la pestaña **Red** > **Config. Kerberos**.

Si configura desde Epson Device Admin:

Seleccione **Red** > **Seguridad** > **Config. Kerberos** en la plantilla de configuración.

Elemento	Ajustes y explicación
Dominio Kerberos	Introduzca el dominio de la autenticación Kerberos en 255 caracteres ASCII (0x20–0x7E) o menos. Si no quiere registrarlo, déjelo en blanco.
Dirección KDC	Introduzca la dirección del servidor de autenticación Kerberos. Escriba 255 caracteres o menos en formato IPv4, IPv6 o FQDN. Si no quiere registrarlo, déjelo en blanco.
Número de puerto (kerberos)	Introduzca el número de puerto del servidor Kerberos entre 1 y 65535.

Configuración de los ajustes de búsqueda del servidor LDAP

Establece los atributos de búsqueda de la configuración del usuario.

Si configura desde Web Config:

Seleccione la pestaña **Red** > **Servidor LDAP** > **Buscar configuración (autenticación)**.

Si configura desde Epson Device Admin:

Seleccione **Ajustes del administrador** > **Configuración de autenticación** > **Servidor LDAP** > **Configuración de búsqueda (Autenticación)** en la plantilla de configuración.

Elemento	Ajustes y explicación
Base búsqueda (nombre distinguido)	Especifique la posición de inicio para buscar información del usuario en el servidor LDAP. Introduzca entre 0 y 128 caracteres Unicode (UTF-8). Si no quiere realizar una búsqueda de un atributo arbitrario, deje este espacio en blanco. Ejemplo del directorio del servidor local: dc=server,dc=local
Atributo de identificador de usuario	Especifique el nombre del atributo a mostrar cuando realice una búsqueda del número de ID. Introduzca entre 1 y 255 caracteres ASCII. El primer carácter debería ser a–z o A–Z. Ejemplo: cn, uid
Atributo visual. nombre de usuario	Especifique el nombre del atributo a mostrar como nombre de usuario. Introduzca entre 0 y 255 caracteres ASCII. El primer carácter debería ser a–z o A–Z. Puede dejarlo en blanco. Ejemplo: cn, name
Atributo de identificador de tarjeta de autenticación	Especifique el nombre del atributo que se debe mostrar como ID de la tarjeta de autenticación. Introduzca entre 0 y 255 caracteres ASCII. El primer carácter debería ser a–z o A–Z. Puede dejarlo en blanco. Ejemplo: cn, sn
Atributo de número de identificación	Especifique el nombre del atributo a mostrar cuando realice una búsqueda del número de ID. Introduzca entre 1 y 255 caracteres ASCII. El primer carácter debería ser a–z o A–Z. Ejemplo: cn, id
Atributo de departamento	Especifique el nombre del atributo a mostrar como nombre del d. Introduzca entre 0 y 255 caracteres ASCII. El primer carácter debería ser a–z o A–Z. Puede dejarlo en blanco. Ejemplo: ou, ou-cl
Atributo dirección de correo electrónico	Especifique el nombre del atributo a mostrar cuando realice una búsqueda de direcciones de correo electrónico. Introduzca entre 1 y 255 caracteres ASCII. El primer carácter debería ser a–z o A–Z. Ejemplo: mail
Guardar en atributo	Especifique el nombre del atributo que indica el destino de Digitalizar y enviar a mi carpeta. Introduzca entre 0 y 255 caracteres ASCII. Ejemplo: homeDirectory

Comprobación de la conexión del servidor LDAP

Ejecuta una prueba de conexión del servidor LDAP según los parámetros establecidos en **Servidor LDAP** > **Buscar config.**.

1. Acceda a Web Config y seleccione la pestaña **Red** > **Servidor LDAP** > **Prueba de conex.**.

2. Seleccione **Iniciar**.

   La prueba de conexión comenzará. Cuando termine la prueba, se mostrará el informe.

Referencias de la prueba de conexión del servidor LDAP

Mensajes	Explicación
Prueba de conexión correcta.	Este mensaje aparece si la conexión con el servidor es satisfactoria.
Error en prueba de conex. Comprobar config.	Este mensaje aparece por las siguientes razones: ❏ La dirección del servidor LDAP o el número de puerto son incorrectos. ❏ Se ha excedido el límite de tiempo. ❏ La opción **No usar** está seleccionada como **Usar serv. LDAP**. ❏ Si se ha seleccionado la **Autenticación Kerberos** como el **Método de autenticación**, ajustes como **Dominio Kerberos**, **Dirección KDC** y **Número de puerto (kerberos)** serán incorrectos.
Error en prueba de conex. Compruebe la fecha y hora en su producto o en el servidor.	Este mensaje aparece cuando la conexión falla porque los ajustes de tiempo del escáner y del servidor LDAP no coinciden.
Error de autenticación. Comprobar config.	Este mensaje aparece por las siguientes razones: ❏ El **Nombre de usuario** y/o la **Contraseña** son incorrectos. ❏ Si se selecciona **Autenticación Kerberos** como **Método de autenticación**, es posible que la hora/fecha no estén configuradas.
No se puede acceder al producto hasta que el proceso se haya completado.	Este mensaje aparece cuando el escáner está ocupado.

Configuración del servidor de correo electrónico

Si utiliza **Digital. a mi correo**, configure el servidor de correo electrónico.

Nota:
*Solamente puede configurar **Digital. a mi correo** si se ha habilitado **Dig. a correo electrónico**.*

Si configura desde Web Config:

Seleccione la pestaña **Red** > **Servidor correo electrónico** > **Básica**.

Si configura desde Epson Device Admin:

Seleccione **Comunes** > **Servidor de correo electrónico** > **Ajustes del servidor de correo** en la plantilla de configuración.

Elemento	Ajustes y explicación	
Método de autenticación	Especifique el método de autenticación para que el escáner acceda al servidor de correo.	
	Desactivar	La autenticación queda deshabilitada al realizar una comunicación con un servidor de correo.
	AUTENTICACIÓN SMTP	El servidor de correo electrónico debe admitir la autenticación SMTP.
	POP antes de SMTP	Si selecciona este elemento, configure un servidor POP3.
Cuenta autenticada	Si selecciona **AUTENTICACIÓN SMTP** o **POP antes de SMTP** como **Método de autenticación**, introduzca el nombre de la cuenta autenticada. Introduzca entre 0 y 255 caracteres en ASCII (0x20–0x7E).	
Contraseña autenticada	Si selecciona **AUTENTICACIÓN SMTP** o **POP antes de SMTP** como **Método de autenticación**, introduzca la contraseña autenticada. Introduzca entre 0 y 20 caracteres en ASCII (0x20–0x7E).	
Dirección correo del remitente	Escriba la dirección del remitente del correo electrónico. Introduzca entre 0 y 255 caracteres en ASCII (0x20–0x7E) excepto para: ( ) < > [ ] ; ¥. Un punto «.» no puede ser el primer carácter.	
Dirección del servidor SMTP	Escriba entre 0 y 255 caracteres. Caracteres admitidos: A–Z a–z 0–9 . -. Puede utilizar el formato IPv4 o el FQDN.	
Nº de puerto del servidor SMTP	Escriba un número comprendido entre el 1 y el 65535.	
Conexión segura	Especifique el método de conexión segura para el servidor de correo electrónico.	
	Ninguno	Si selecciona **POP antes de SMTP** en **Método de autenticación**, el método de conexión se establece en **Ninguno**.
	SSL/TLS	Esto está disponible cuando **Método de autenticación** se establece en **Desactivar** o **AUTENTICACIÓN SMTP**.
	STARTTLS	Esto está disponible cuando **Método de autenticación** se establece en **Desactivar** o **AUTENTICACIÓN SMTP**.
Validación de certificado	El certificado se autentica si esta opción está habilitada. Es recomendable configurarlo como **Activar**.	
Dirección del servidor POP3	Si selecciona **POP antes de SMTP** como **Método de autenticación**, introduzca la dirección del servidor POP3. Puede introducir entre 0 y 255 caracteres usando los caracteres A–Z a–z 0–9. Puede utilizar el formato IPv4 o el FQDN.	
Nº de puerto del servidor POP3	Si selecciona **POP antes de SMTP** como **Método de autenticación**, indique el número de puerto. Escriba un número comprendido entre el 1 y el 65535.	

Configuración de Digital. a mi carpeta

Guarda las imágenes escaneadas en la carpeta asignada a cada usuario. Puede establecer lo siguiente como carpeta dedicada.

Nota:
*Solamente puede configurar **Digitalizar y enviar a mi carpeta** si se ha habilitado **Digitaliz. a carpeta red/FTP**.*

Configuración de Guardar en	Método de autenticación	Ubicación de configuración de la ruta de la carpeta
Especifique una carpeta de red para toda la Configuración de autenticación de forma que se cree automáticamente una carpeta personal debajo de la carpeta especificada con el nombre de la ID del usuario.	❏ DB local ❏ LDAP ❏ DB local y LDAP	Escáner (configuración de Digital. a mi carpeta)
Asignar diferentes carpetas de red individualmente a cada usuario.	DB local	Escáner (Ajustes usuario)
	LDAP	Atributos de LDAP
	DB local y LDAP	Atributos del escáner (Ajustes usuario) o LDAP

Si configura desde Web Config:

Seleccione la pestaña **Seguridad del producto** > **Digitaliz. a carpeta red/FTP**.

Si configura desde Epson Device Admin:

Seleccione **Ajustes del administrador** > **Configuración de autenticación** > **Digitaliz. a carpeta red/FTP** > **Digital. a mi carpeta** en la plantilla de configuración.

Elemento		Explicación
Guardar en ajustes	Tipo de ajustes	❏ **Compartido**: Crea automáticamente una carpeta con el nombre del ID del usuario debajo de la ruta de la carpeta o URL especificada en **Guardar en** y guarda las imágenes escaneadas en esta carpeta. ❏ **Individual**: Establezca el destino de almacenamiento para los resultados del análisis para cada usuario. Se pueden configurar los usuarios de DB local en la configuración de usuario. Los usuarios de LDAP utilizan la ubicación de almacenamiento obtenida a partir de los atributos de búsqueda del servidor LDAP.
	Tipo	Seleccione el protocolo de transmisión en función del destino de salida del escaneado. Para una carpeta de red: **Carpeta de redes (SMB)** Para un servidor FTP: **FTP**
	Guardar en	Especifique la ruta o URL de la ruta de salida. Introduzca un máximo de 160 caracteres en Unicode (UTF-16).
	Modo de conexión	Se establece al seleccionar **FTP** en **Tipo**. Seleccione un modo de conexión para el servidor FTP.
	Número de puerto	Se establece al seleccionar **FTP** en **Tipo**. Escriba el número de puerto (entre 0 y 65535) para enviar los datos digitalizados a un servidor FTP.

Elemento		Explicación
Configuración de autenticación	Tipo de ajustes	Se establece al seleccionar **Individual** como **Tipo de ajustes** en **Guardar en ajustes**. Establece «Nombre de usuario» y «Contraseña» para acceder a la carpeta. ❏ **Compartido**: Se utiliza el mismo **Nombre de usuario** y la misma **Contraseña** para todos los usuarios. ❏ **Individual**: Para los usuarios de DB local, establezca **Nombre de usuario** y **Contraseña** individualmente en **Configuración del usuario**. Los usuarios de LDAP no se pueden configurar individualmente. El **Nombre de usuario** y la **Contraseña** establecidos por este elemento se utilizan en lote.
	Nombre de usuario	Escriba el nombre de usuario para acceder a la carpeta de destino de salida de digitalización. Introduzca un máximo de 30 caracteres en Unicode (UTF-16). Seleccione esta opción si utiliza **Compartido** o un servidor LDAP.
	Contraseña	Introduzca la contraseña correspondiente a **Nombre de usuario**. Introduzca un máximo de 20 caracteres en Unicode (UTF-16). Seleccione esta opción si utiliza **Compartido** o un servidor LDAP.

Prohibir el cambio de destino de Digitaliz. a carpeta red/FTP

Elemento	Explicación
Prohibido especificar el destino manualmente	Si está habilitado, el usuario no puede cambiar el destino predeterminado.

Personalizar funciones de un toque

Puede mostrar solamente los iconos necesarios editando la distribución de iconos mostrada en la pantalla de inicio para el panel de control.

Si configura desde Web Config:

Seleccione la pestaña **Seguridad del producto** > **Personalizar funciones de un toque**.

Si configura desde Epson Device Admin:

Seleccione **Ajustes del administrador** > **Configuración de autenticación** > **Personalizar funciones de un toque** en la plantilla de configuración.

Nota:
En los casos siguientes, los iconos de las funciones especificadas no se muestran en la pantalla de inicio.

❏ *Cuando seleccione funciones que no están permitidas debido a **Restricciones**.*

❏ *Cuando la dirección de correo electrónico de un usuario que ha iniciado sesión no está registrada. (Digital. a mi correo)*

❏ *Cuando la carpeta de destino no está establecida. (Digital. a mi carpeta)*

Elemento	Explicación
Número máximo de funciones por pantalla	Selecciona la disposición de los iconos que se muestran en el panel de control. La imagen cambia en función de la distribución seleccionada.
Pantalla(s)	Selecciona el número de páginas.
Número	Selecciona las funciones que se desea mostrar para cada posición numerada.

Informes de Historial de trabajos con Epson Device Admin

Se puede crear un informe de Historial de trabajos para cada grupo y para cada usuario mediante Epson Device Admin. En el escáner se pueden guardar hasta 3000 historiales de uso. Puede crear el informe especificando un período o estableciendo una programación periódica.

Para generar el Historial de trabajos modo de informe, seleccione **Opciones** > **Configuración de Epson Print Admin Serverless/Autenticación** > **Administrar los dispositivos compatibles Epson Print Admin Serverless/Autenticación** en el menú de cinta de la pantalla de la lista de dispositivos.

Para ver los detalles acerca de cómo crear un informe de usuario, consulte la documentación de Epson Device Admin.

Elementos que pueden incluirse en el informe

El informe de usuario puede incluir los siguientes elementos.

Fecha/Identificador del trabajo/Operación/Identificador de usuario/Departamento/Resultado/Detalles del resultado/Escanear: Tipo de destino/Escanear: Destino/Escanear: Tamano de Papel/Escanear: 2 caras/Escanear: Color/Escanear: Páginas/Dispositivos: Modelo/Dispositivos: Dirección IP/Dispositivos: Número de serie/Dispositivos: Departamento/Dispositivos: Ubicación/Dispositivos: Comentarios/Dispositivos: Nota

Iniciar sesión como administrador desde el panel de control

Puede utilizar cualquiera de los siguientes métodos para iniciar sesión como administrador desde el panel de control del escáner.

1. Toque  en la parte superior derecha de la pantalla.
   - ❏ Si Configuración de autenticación está habilitado, el icono se muestra en la pantalla **Bienvenido** (pantalla de espera de autenticación).
   - ❏ Si Configuración de autenticación está deshabilitado, el icono se muestra en la pantalla de inicio.
2. Toque **Sí** cuando aparezca la pantalla de confirmación.

3. Escriba la contraseña de administrador.

   Se muestra un mensaje que indica que el inicio de sesión se ha realizado y, a continuación, la pantalla de inicio del panel de control.

Para cerrar sesión, toque  en la parte superior derecha de la pantalla de inicio.

Deshabilitar Configuración de autenticación

Puede desactivar Configuración de autenticación con Web Config.

Nota:
Los Ajustes usuario registrados en el escáner se guardan aunque Configuración de autenticación esté desactivado. Puede eliminarlos restaurando la configuración predeterminada del escáner.

1. Acceda a «Web Config».
2. Seleccione la pestaña **Seguridad del producto** > **Básica** > **Autenticación**.
3. Seleccione **DESACT.**.
4. Haga clic en **Siguiente**.
5. Haga clic en **Aceptar**.

Nota:
Aunque deshabilite Configuración de autenticación, Configuración bloqueo permanece habilitado. Si desea deshabilitarlo, puede realizar los ajustes desde el panel de control o Web Config.

Información relacionada

➡ "Ajuste de Configuración bloqueo desde el panel de control" de la página 88
➡ "Configuración de Configuración bloqueo desde Web Config" de la página 88

Eliminar la información de Configuración de autenticación (Restaurar configuración pred.)

Para eliminar toda la información de Configuración de autenticación (Lector de tarjetas, Método de autenticación, Ajustes usuario, etc.), restaure la configuración predeterminada del escáner que tenía en el momento de la compra.

Seleccione **Configuración** > **Admin. del sistema** > **Restaurar configuración pred.** > **Todas las configuraciones** en el panel de control.

Importante:
También se eliminarán todos los contactos y el resto de ajustes de la red. Los ajustes eliminados no se pueden restaurar.

Resolución de problemas

No se puede leer la tarjeta de autenticación

Compruebe lo siguiente.

❏ Compruebe si el dispositivo de autenticación está correctamente conectado al escáner.
Conecte el dispositivo de autenticación al puerto USB de la interfaz externa en la parte posterior del escáner.

❏ Compruebe que el dispositivo de autenticación y la tarjeta de autenticación son compatibles.

Mantenimiento

Limpieza del exterior del escáner

Limpie las manchas de la carcasa exterior con un paño seco o un paño humedecido con detergente neutro y agua.

Importante:

- ❏ *Nunca utilice alcohol, disolventes ni ningún producto corrosivo para limpiar el escáner. Esto puede causar decoloración o deformaciones.*
- ❏ *No permita que le entre agua al producto. Esto podría provocar un mal funcionamiento.*
- ❏ *Nunca abra la carcasa del escáner.*

1. Pulse el botón ⏻ para apagar el escáner.
2. Desconecte el adaptador de CA del escáner.
3. Limpie la carcasa exterior con un paño humedecido con detergente neutro y agua.

   Nota:
   Limpie la pantalla táctil con un paño suave y seco.

Limpieza del interior del escáner

Tras haber utilizado el escáner durante un tiempo, puede que el polvo proveniente de la habitación y el papel se acumule en los rodillos o en la parte de cristal del interior del escáner. Esto puede causar problemas en la bandeja de alimentación de papel o en la calidad de las imágenes escaneadas. Limpie el interior del escáner cada 5,000 escaneados.

Puede consultar el número actualizado de escaneados en el panel de control o en Epson Scan 2 Utility.

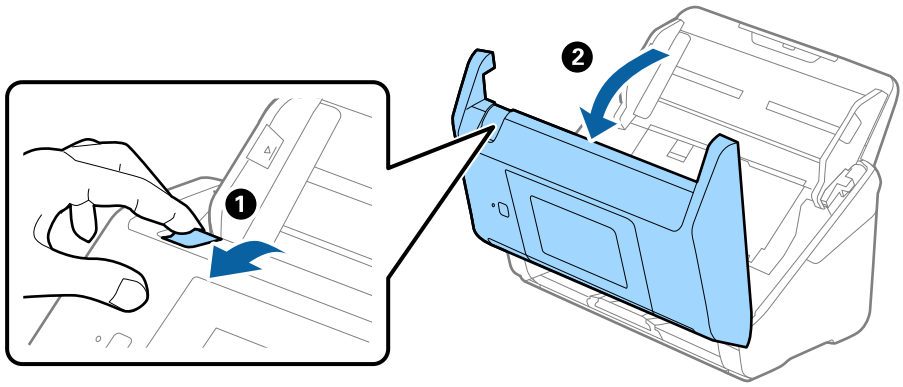
Si la superficie se ha manchado con un material difícil de quitar, utilice un kit de limpieza original de Epson para quitar las manchas. Use una pequeña cantidad del producto en la gamuza para eliminar las manchas.

Importante:

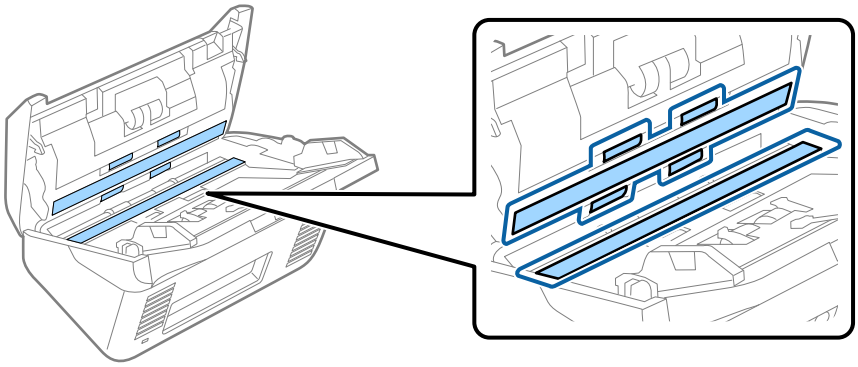
- ❏ *Nunca utilice alcohol, disolventes ni ningún producto corrosivo para limpiar el escáner. Esto puede causar decoloración o deformaciones.*
- ❏ *Nunca pulverice o aplique ningún líquido o espray sobre el escáner. Los daños al equipo o circuitos pueden causar un comportamiento anómalo.*
- ❏ *Nunca abra la carcasa del escáner.*

1. Pulse el botón ⏻ para apagar el escáner.
2. Desconecte el adaptador de CA del escáner.

3. Tire de la palanca y abra la cubierta del escáner.

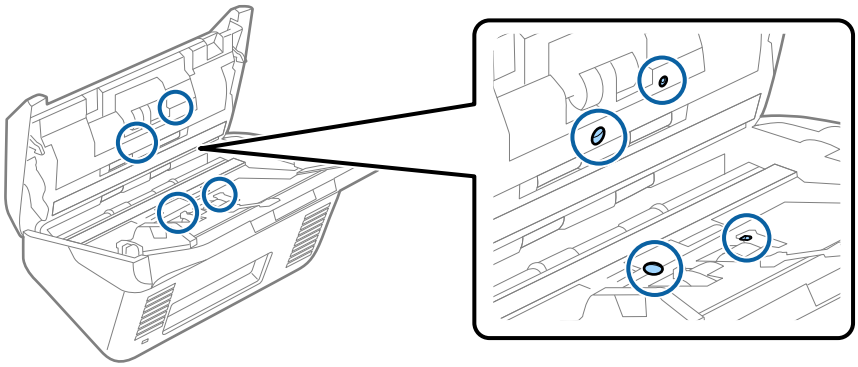


4. Limpie las manchas que pudiera haber en los rodillos y en la superficie de cristal que se encuentra en el fondo dentro de la cubierta usando un paño suave o un kit de limpieza original de Epson.



> ***Importante:***
>
> - ❏ *No presione con demasiada fuerza la superficie de cristal.*
> - ❏ *No use ningún cepillo ni herramienta dura. Cualquier rasguño en el cristal puede afectar a la calidad del escaneado.*
> - ❏ *No pulverice el producto directamente sobre la superficie de cristal.*

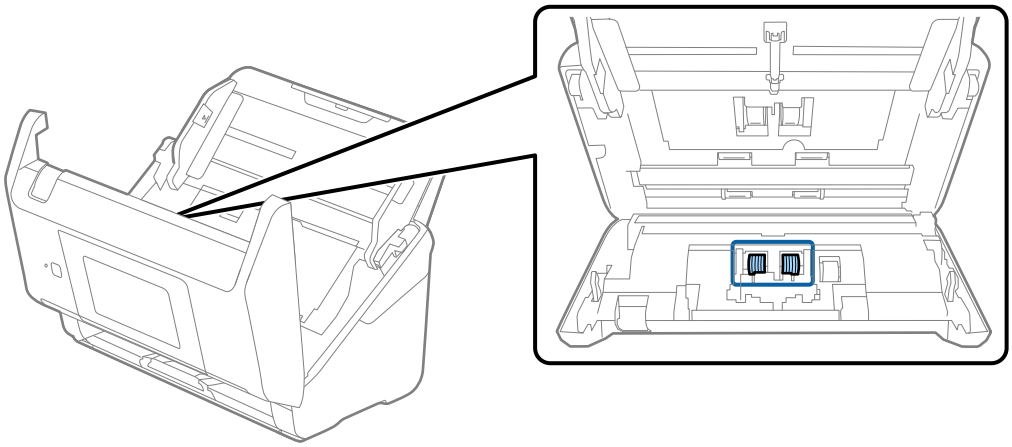
5. Limpie las manchas en los sensores con un bastoncillo de algodón.



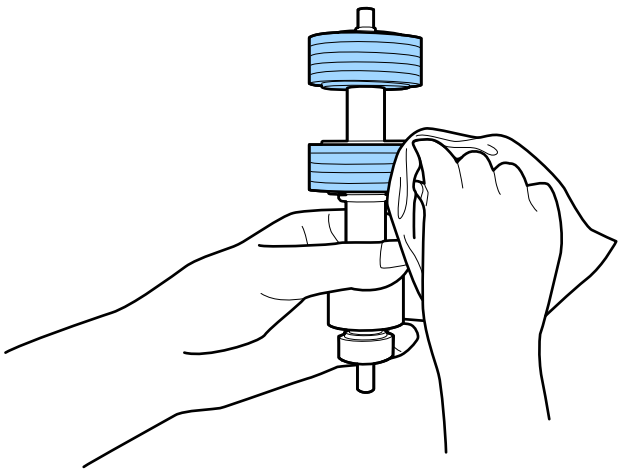
> ***Importante:***
> *No use ningún líquido, como el producto, en el bastoncillo de algodón.*

6. Abra la cubierta y, a continuación, retire el rodillo de separación.

   Consulte «Remplazar el kit de montaje de rodillos» para más información.



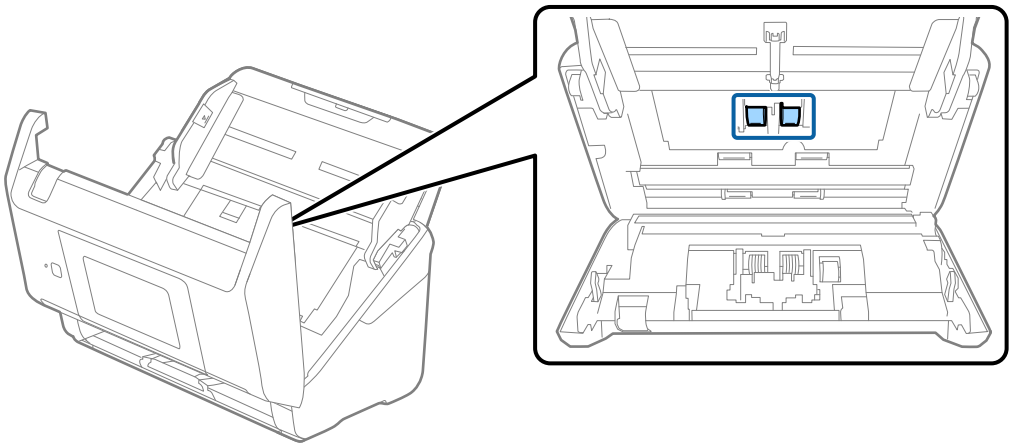
7. Limpie el polvo o suciedad del rodillo de separación con un kit de limpieza original de Epson o un paño suave y húmedo.



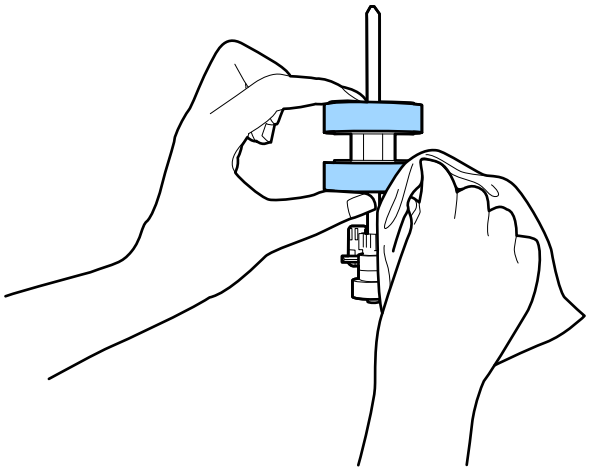
> ***Importante:***
> *Utilice únicamente un kit de limpieza original de Epson o un paño suave y húmedo para limpiar el rodillo. El uso de un paño seco puede dañar la superficie del rodillo.*

8. Abra la cubierta y, a continuación, retire el rodillo de recogida.

   Consulte «Remplazar el kit de montaje de rodillos» para más información.



9. Limpie el polvo o suciedad del rodillo de recogida con un kit de limpieza original de Epson o un paño suave y húmedo.



> ***Importante:***
>
> *Utilice únicamente un kit de limpieza original de Epson o un paño suave y húmedo para limpiar el rodillo. El uso de un paño seco puede dañar la superficie del rodillo.*

10. Cierre la cubierta del escáner.

11. Conecte el adaptador de CA y, a continuación, encienda el escáner.

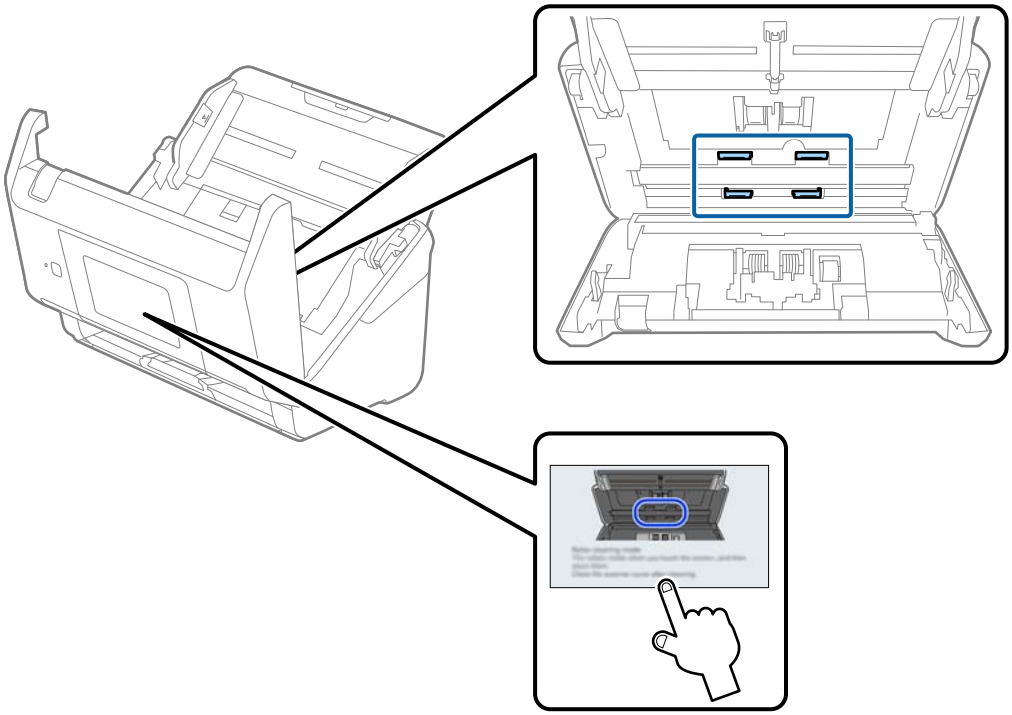
12. Seleccione **Mantenimiento del escáner** en la pantalla de inicio.

13. En la pantalla **Mantenimiento del escáner**, seleccione **Limpieza de rodillos**.

14. Tire de la palanca para abrir la cubierta del escáner.

    El escáner inicia el modo limpieza del rodillo.

15. Gire despacio los rodillos de la parte inferior tocando en cualquier lugar del LCD. Limpie la superficie de los rodillos con un kit de limpieza original de Epson o un paño suave y humedecido con agua. Repita hasta que los rodillos estén limpios.



> ***Precaución:***
>
> *Tenga especial cuidado con las manos y el pelo con el fin de que no acaben atascados en el mecanismo mientras esté manipulando el rodillo. Esto podría causar lesiones.*

16. Cierre la cubierta del escáner.

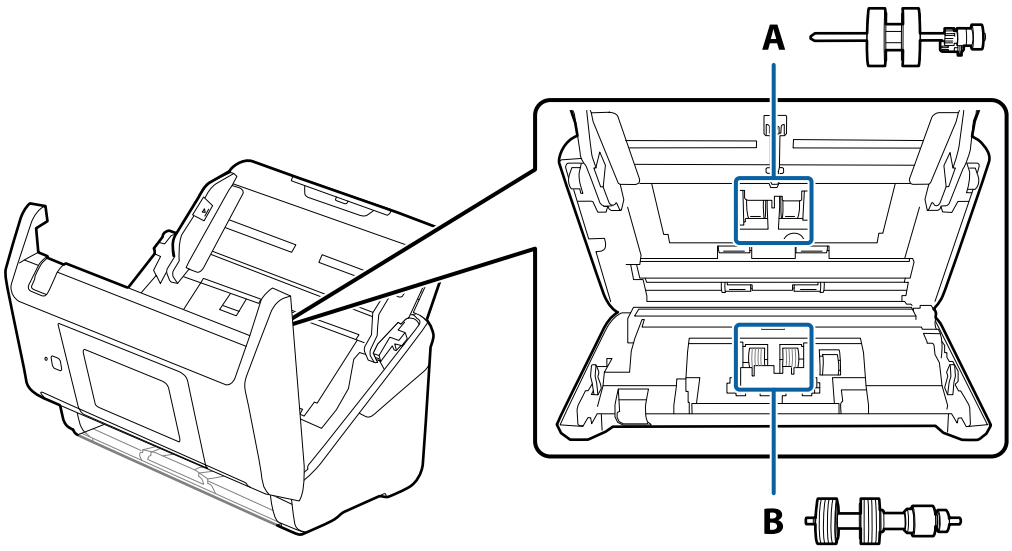
    El escáner sale del modo limpieza del rodillo.

Información relacionada

➡ "Sustitución del kit de montaje de rodillos" de la página 163

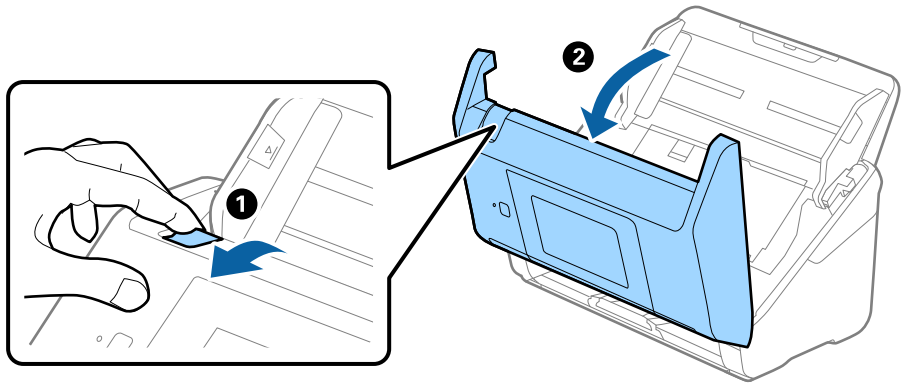
Sustitución del kit de montaje de rodillos

El kit de montaje de rodillos (el rodillo de alimentación y el de separación) necesita ser sustituido cuando el número de escaneados exceda el ciclo vital de los rodillos. Cuando se muestre un mensaje de sustitución en el panel de control o en la pantalla su ordenador, siga los pasos siguientes para sustituirlo.

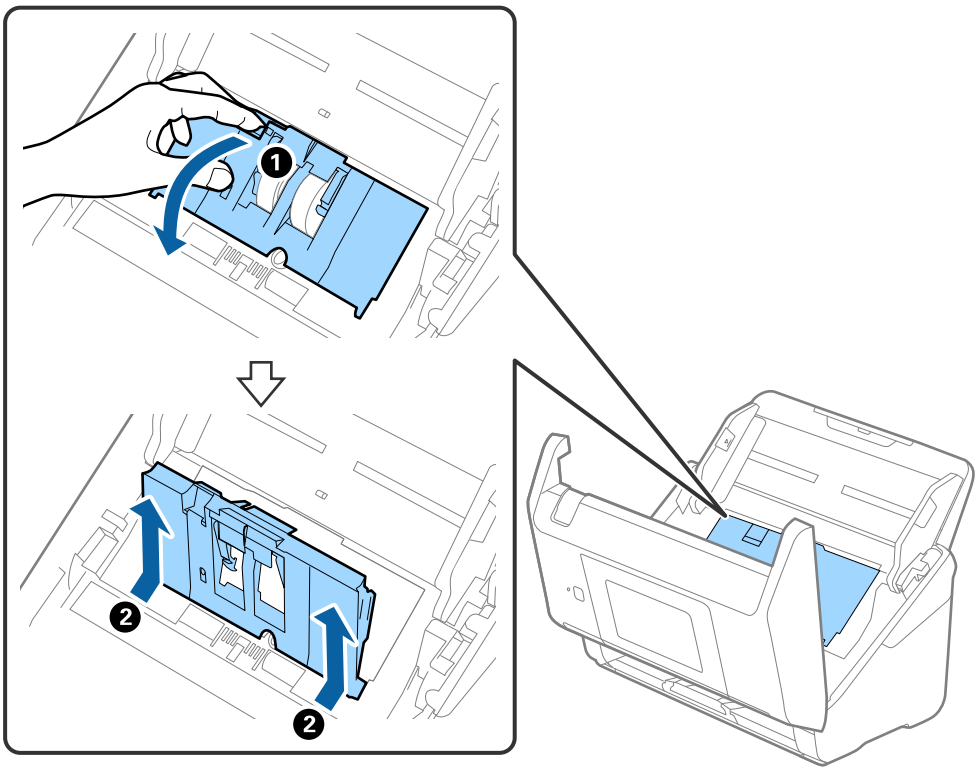


A: rodillo de alimentación, B: rodillo de separación

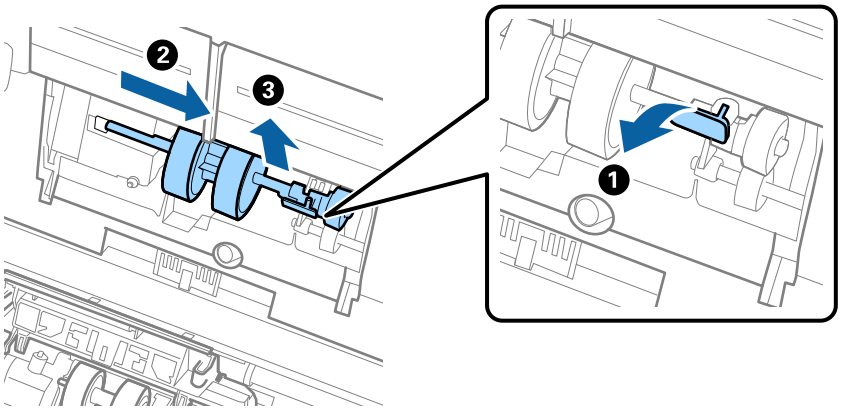
1. Pulse el botón ⏻ para apagar el escáner.
2. Desconecte el adaptador de CA del escáner.
3. Tire de la palanca y abra la cubierta del escáner.



4. Abra la cubierta del rodillo de recogida y, a continuación, deslícelo y retírelo.



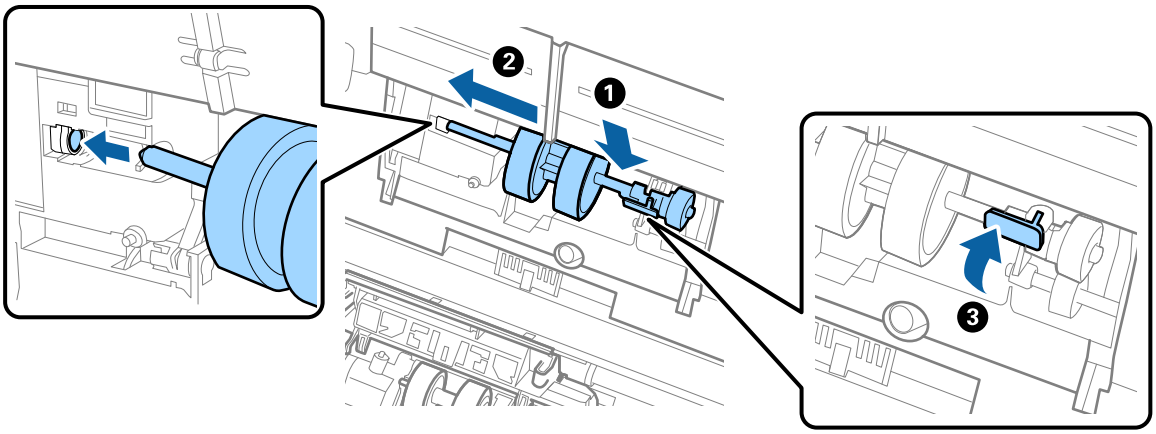
5. Tire hacia abajo de la pestaña del eje del rodillo y, a continuación, deslice y retire los rodillos de recogida instalados.



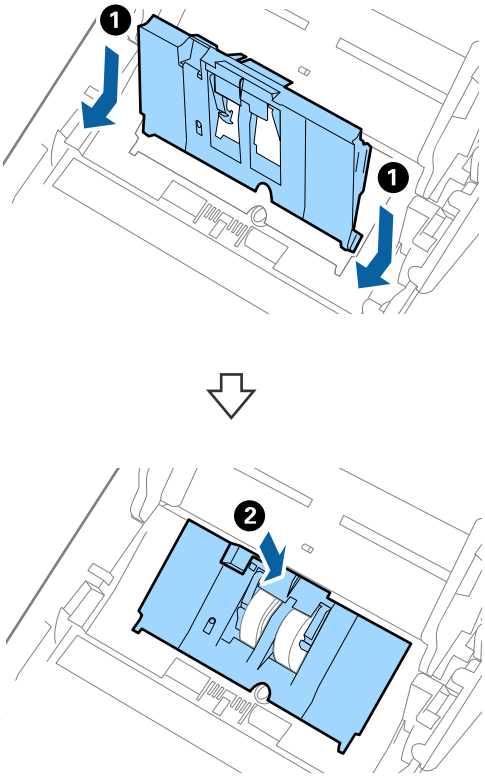
Importante:

No fuerce el rodillo de recogida al intentar sacarlo. Esto podría dañar el interior del escáner.

6. Mientras mantiene la pestaña abajo, deslice el nuevo rodillo de recogida hacia la izquierda e insértelo en el hueco del escáner. Presione la pestaña para asegurarla.

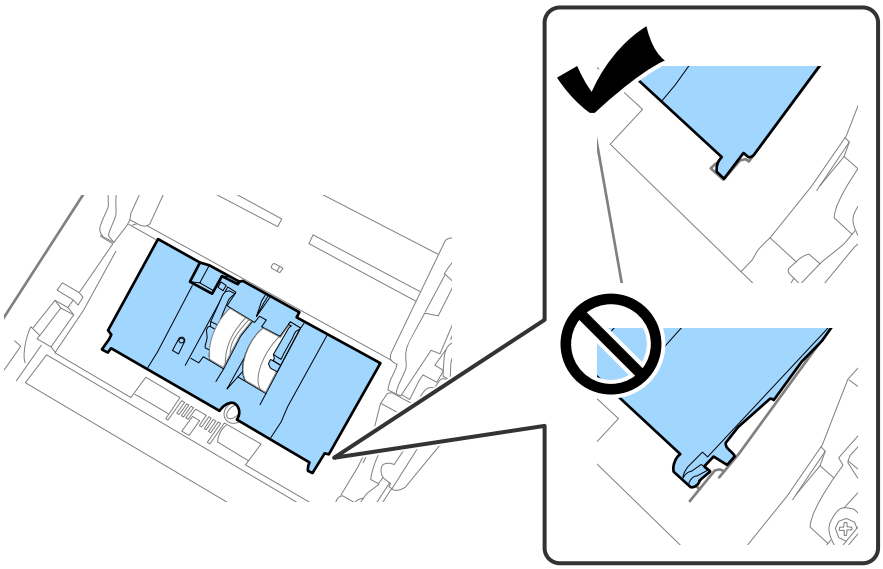


7. Ponga el borde de la cubierta del rodillo de recogida en la muesca y deslícelo. Cierre la cubierta firmemente.

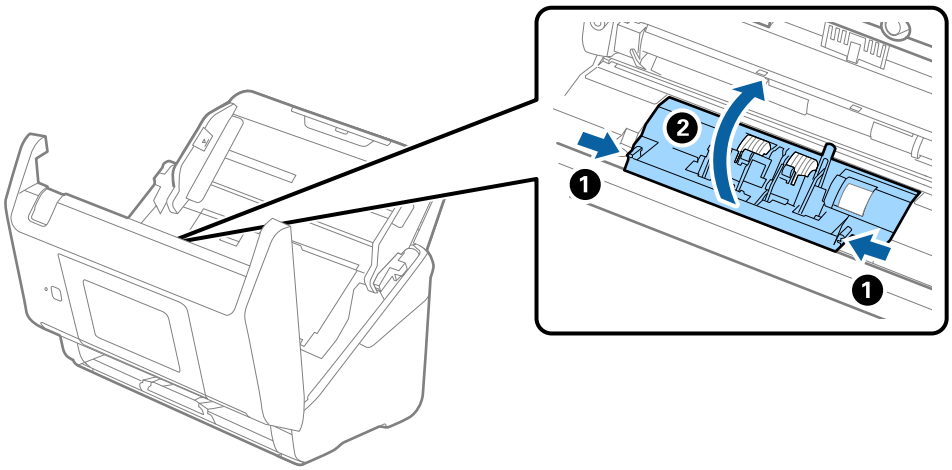


Importante:

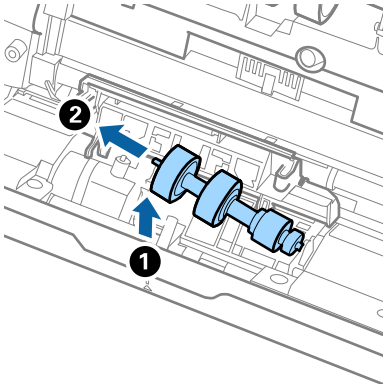
- ❏ *Asegúrese de que la cubierta de recogida está cerrada correctamente.*
- ❏ *Asegúrese de que los rodillos de recogida están instalados correctamente si tiene dificultades para cerrar la cubierta.*
- ❏ *No instale la cubierta mientras esté levantada.*



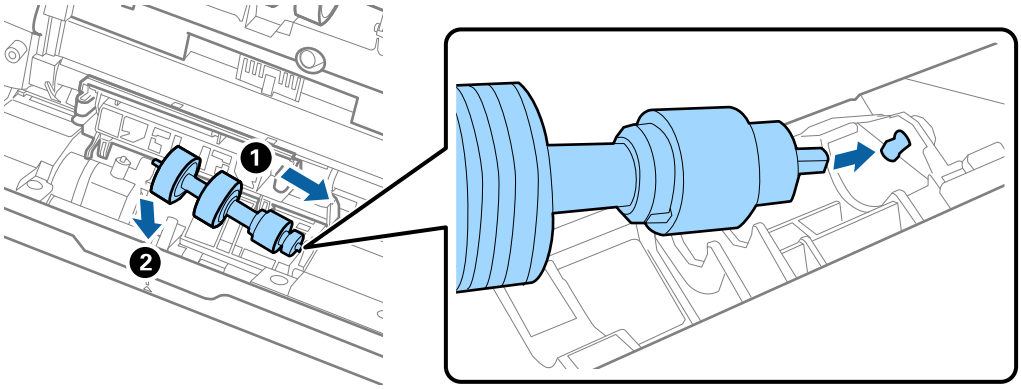
8. Empuje los ganchos en ambas puntas de la cubierta del rodillo de separación para abrir la cubierta.



9. Levante el lado izquierdo del rodillo de separación y, a continuación, deslice y retire los rodillos de separación instalados.



10. Inserte el eje del nuevo rodillo de separación en el hueco del lado derecho y, a continuación, baje el rodillo.



11. Cierre la cubierta del rodillo de separación.

> ***Importante:***
> *Si cuesta cerrar la cubierta, asegúrese de que los rodillos de separación estén correctamente instalados.*

12. Cierre la cubierta del escáner.

13. Conecte el adaptador de CA y, a continuación, encienda el escáner.

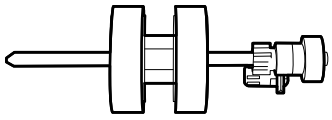
14. Restablezca el número de escaneados en el panel de control.

Nota:
Deseche el rodillo de recogida y el rodillo de separación siguiendo las reglas y normativa de las autoridades de su país. No los desmonte.

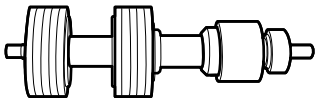
Códigos del kit de montaje de rodillos

Las piezas (el rodillo de alimentación y el rodillo de separación) deberían ser sustituidos cuando el número de escaneados exceda el número de servicio. Puede consultar el número actualizado de escaneados en el panel de control o en Epson Scan 2 Utility.

A



B



A: rodillo de alimentación, B: rodillo de separación

Nombre de pieza	Códigos	Ciclo de vida
Kit de montaje de rodillos	B12B819671 B12B819681 (solo India)	200,000*

* Este número se alcanzó escaneando consecutivamente usando papeles de prueba originales de Epson y sirve de guía para el ciclo de sustitución. El ciclo de sustitución puede variar dependiendo de los diferentes tipos de papel, como el papel que genera mucho polvo o el papel con una superficie áspera que pueden acortar el ciclo de vida.

Restablecimiento del número de escaneados

Restablezca el número de escaneados después de sustituir el kit de montaje de rodillos.

1. Seleccione **Configuración** > **Información del dispositivo** > **Restablecer el número de digitalizaciones** > **Digitalizac. tras sustituir el rodillo** en la pantalla de inicio.

2. Toque **Sí**.

Información relacionada

➡ "Sustitución del kit de montaje de rodillos" de la página 163

Ahorro de energía

Puede ahorrar energía usando el modo de suspensión o el autoapagado cuando el escáner no esté realizando ninguna acción. Puede seleccionar el periodo de tiempo transcurrido antes de que el escáner entre en modo de suspensión y se apague automáticamente. Cualquier aumento afectará a la eficiencia energética del producto. Tenga en cuenta el medio ambiente antes de realizar cualquier cambio.

1. Seleccione **Configuración** en la pantalla de inicio.

2. Seleccione **Config. básica**.

3. Seleccione **Ajustes de apagado** y realice los ajustes que desee.

   Nota:
   Las funciones disponibles pueden variar en función de dónde se haya realizado la compra.

Transporte del escáner

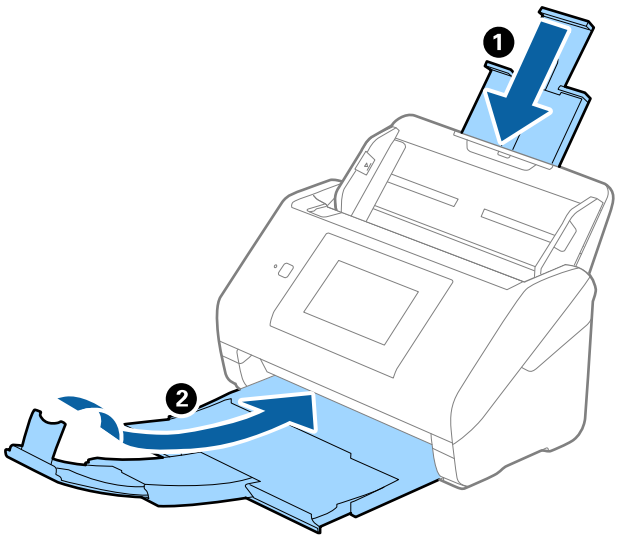
Si necesita transportar el escáner para cambiarlo de sitio o para repararlo, siga los pasos que se indican a continuación para empaquetarlo.

1. Pulse el botón ⏻ para apagar el escáner.

2. Desconecte el adaptador de CA.

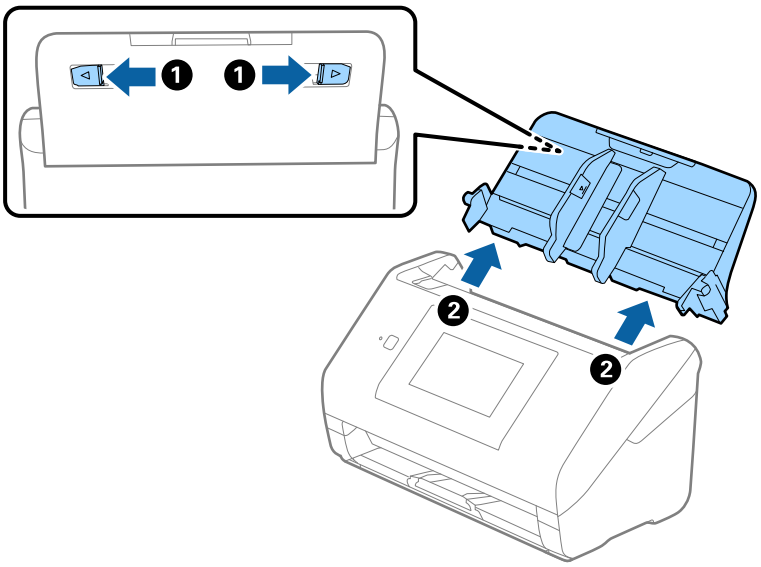
3. Retire los cables y los dispositivos.

4. Cierre la extensión de la bandeja de entrada y la bandeja de salida.



Importante:
Cerciórese de cerrar la bandeja de salida de forma segura; de lo contrario podría sufrir daños durante el transporte.

5. Retire la bandeja de entrada.



6. Adjunte el material de embalaje suministrado con el escáner y vuelva a guardarlo en la caja original o en una caja robusta.

Copia de seguridad de la configuración

Puede exportar los valores de ajuste establecidos desde Web Config a un archivo. Puede utilizarlo para hacer copias de seguridad de los contactos y los valores de ajuste, cambiar el escáner, etc.

El archivo exportado no se puede editar porque se exporta como archivo binario.

Cómo exportar la configuración

Exporte la configuración del escáner.

1. Acceda a Web Config y luego seleccione la pestaña **Gestión del dispositivo** > **Exportar e importar valor de configuración** > **Exportar**.

2. Seleccione los ajustes que desea exportar.

   Seleccione los ajustes que desea exportar. Si selecciona la categoría principal, también se seleccionarán las subcategorías. Sin embargo, la subcategorías que provocan errores por estar duplicadas dentro de la misma red (como direcciones IP, etc.) no se pueden seleccionar.

3. Escriba una contraseña para cifrar el archivo exportado.

   Necesita la contraseña para importar el archivo. Deje esto en blanco si no desea cifrar el archivo.

4. Haga clic en **Exportar**.

> ***Importante:***
> *Si desea exportar la configuración de red del escáner, como el nombre del dispositivo y la dirección IPv6, seleccione **Habilitar para seleccionar la configuración individual del dispositivo** y seleccione más elementos. Utilice solamente los valores seleccionados para el escáner de reemplazo.*

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Importar la configuración

Importe el archivo de Web Config al escáner.

> ***Importante:***
> *Al importar valores que incluyen información individual, como el nombre de un escáner o la dirección IP, asegúrese de que la misma dirección IP no exista en la misma red.*

1. Acceda a Web Config y luego seleccione la pestaña **Gestión del dispositivo** > **Exportar e importar valor de configuración** > **Importar**.
2. Seleccione el archivo exportado y, a continuación, escriba la contraseña cifrada.
3. Haga clic en **Siguiente**.
4. Seleccione la configuración que desee importar y haga clic en **Siguiente**.
5. Haga clic en **Aceptar**.

La configuración se aplica al escáner.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Restaurar configuración pred.

En el panel de control, seleccione **Configuración** > **Admin. del sistema** > **Restaurar configuración pred.** y, a continuación, seleccione los elementos cuyos valores predeterminados desee restaurar.

- ❏ Configuración de red: restaura la configuración relacionada con la red a su estado inicial.
- ❏ Todo excepto la configuración de red: restaura otros ajustes a su estado inicial, excepto para los ajustes relacionados con la red.
- ❏ Todas las configuraciones: restaura todos los ajustes al estado inicial de cuando se adquirió el producto.

Importante:

*Si selecciona y ejecuta **Todas las configuraciones**, se eliminarán todos los datos de configuración registrados en el escáner, incluidos los contactos y la configuración de autenticación del usuario. Los ajustes eliminados no se pueden restaurar.*

Actualización de aplicaciones y firmware

Puede eliminar ciertos problemas y mejorar o agregar funciones actualizando las aplicaciones y el firmware. Asegúrese de que utiliza la versión más reciente de las aplicaciones y del firmware.

Importante:

❏ *No apague el equipo o el escáner durante la actualización.*

Nota:
*Si el escáner puede conectarse a Internet, puede actualizar el firmware desde Web Config. Seleccione la pestaña **Gestión del dispositivo** > **Actualización del firmware**, compruebe el mensaje y, a continuación, haga clic en **Iniciar**.*

1. Asegúrese de que el escáner y el equipo están conectados y que este está conectado a Internet.

2. Inicie EPSON Software Updater y actualice todas las aplicaciones o el firmware.

   Nota:
   Los sistemas operativos Windows Server no son compatibles.

   ❏ Windows 10

   Haga clic en el botón Inicio y, a continuación, seleccione **Epson Software** > **EPSON Software Updater**.

   ❏ Windows 8.1/Windows 8

   Introduzca el nombre de la aplicación en el acceso a Buscar y luego seleccione el icono que aparezca.

   ❏ Windows 7

   Haga clic en el botón de inicio y seleccione **Todos los programas** o **Programas** > **Epson Software** > **EPSON Software Updater**.

   ❏ Mac OS

   Seleccione **Finder** > **Ir** > **Aplicaciones** > **Epson Software** > **EPSON Software Updater**.

Nota:
Si no puede encontrar la aplicación que desea actualizar en la lista, no podrá actualizarla mediante el EPSON Software Updater. Busque las versiones más recientes de las aplicaciones en el sitio web local de Epson.

http://www.epson.com

Actualización del firmware del escáner mediante el panel de control

Si el escáner se puede conectar a Internet, puede actualizar su firmware a través del panel de control. También puede configurar el escáner para que compruebe regularmente si hay actualizaciones de firmware y que lo avise si hay alguna disponible.

1. Seleccione **Configuración** en la pantalla de inicio.

2. Seleccione **Admin. del sistema** > **Actualización de firmware** > **Actualizar**.

   Nota:
   Si quiere que el escáner compruebe regularmente si hay actualizaciones de firmware disponibles, seleccione ***Notificación*** *>* ***Activ.****.*

3. Lea el mensaje que aparece en pantalla y busque las actualizaciones disponibles.

4. Si en la pantalla LCD aparece un mensaje indicándole que hay una actualización de firmware disponible, siga las instrucciones de la pantalla para instalarla.

   Importante:
   - ❏ *No apague ni desenchufe el escáner hasta que finalice la actualización; de lo contrario, el escáner podría funcionar mal.*
   - ❏ *Si la actualización no se ha completado o no se ha instalado bien, la próxima vez que encienda el escáner no se iniciará correctamente y en la pantalla LCD aparecerá el mensaje «Recovery Mode». En ese caso, tendrá que volver a actualizar el firmware con un ordenador. Conecte el escáner al ordenador con un cable USB. Mientras en la pantalla del escáner aparezca el mensaje «Recovery Mode», no podrá actualizar el firmware por red. En el ordenador, acceda a su web de Epson local y descárguese el firmware más reciente del escáner. En el sitio web encontrará todas las instrucciones.*

Actualización del firmware mediante Web Config

Si el escáner puede conectarse a Internet, puede actualizar el firmware desde Web Config.

1. Acceda a Web Config y seleccione la pestaña **Gestión del dispositivo** > **Actualización del firmware**.

2. Haga clic en **Iniciar** y, a continuación, siga las instrucciones en pantalla.

   Se inicia la confirmación del firmware y se muestra la información de este si se ha actualizado.

Nota:
También puede actualizar el firmware mediante Epson Device Admin. Puede confirmar visualmente la información del firmware en la lista de dispositivos. Esto resulta útil cuando desea actualizar el firmware en varios dispositivos. Consulte la guía o la ayuda de Epson Device Admin para obtener más detalles.

Información relacionada

➡ "Ejecución de Web Config en un navegador web" de la página 36

Actualización del firmware sin conexión a Internet

Puede descargar el firmware del dispositivo desde el sitio web de Epson en el ordenador y luego conectar el dispositivo y el ordenador con un cable USB para actualizar el firmware. Si no puede realizar la actualización a través de la red, intente este método.

Nota:
Antes de actualizar, asegúrese de que el controlador del escáner Epson Scan 2 esté instalado en el ordenador. Si Epson Scan 2 no está instalada, instálela de nuevo.

1. Visite el sitio web de Epson para obtener las últimas versiones del firmware.

   http://www.epson.com

❏ Si hay un firmware más reciente para su escáner, descárguelo y vaya al siguiente paso.

❏ Si en el sitio web no consta ningún firmware nuevo, ya está utilizando el más reciente.

2. Conecte el ordenador que tiene el firmware descargado en al escáner con un cable USB.

3. Haga doble clic sobre el archivo .exe descargado.
   Se inicia Epson Firmware Updater.

4. Siga las instrucciones de la pantalla.