

Manual del administrador

Índice

Copyright

Marcas comerciales

Acerca de este manual

Marcas y símbolos.	6
Descripciones utilizadas en este manual.	6
Referencias a sistemas operativos.	6

Introducción

Componente manual.	8
Definiciones de los términos empleados en esta guía.	8

Preparación

Flujo de la configuración y la administración del escáner.	10
Ejemplo de entorno de red.	11
Ejemplo de introducción del ajuste de conexión del escáner.	11
Preparación de conexión a una red.	12
Acopio de información sobre la configuración de conexión.	12
Especificaciones del escáner.	13
Uso del número de puerto.	13
Tipo de asignación de dirección IP.	13
Servidor DNS y servidor proxy.	13
Método para configurar la conexión de red.	13

Conexión

Conexión a la red.	15
Conexión a la red desde el panel de control.	15
Conexión a la red mediante el uso del instalador.	19

Configuración de las funciones

Software para ajustes.	22
Web Config (página web del dispositivo).	22
Uso de funciones de escaneado.	24
Escaneado desde un ordenador.	24
Escaneado desde el panel de control.	26
Configuración del sistema.	28

Configuración de los ajustes avanzados de red desde el panel de control.	28
Configuración de ajustes del sistema con Web Config.	30

Configuración de seguridad básica

Introducción a las funciones de seguridad básicas.	32
Configuración de la contraseña de administrador.	33
Configuración de la contraseña de administrador desde el panel de control.	33
Configuración de la contraseña de administrador mediante Web Config.	33
Elementos para bloqueo mediante contraseña de administrador.	34
Protocolos de control.	35
Protocolos que puede habilitar o inhabilitar.	36
Elementos de ajuste del protocolo.	37

Configuración de funcionamiento y administración

Confirmación de la información de un dispositivo.	40
Administración de dispositivos (Epson Device Admin).	40
Cómo recibir notificaciones por correo electrónico cuando se produzcan determinadas situaciones.	41
Acerca de las notificaciones por correo electrónico.	41
Configuración de las notificaciones por correo electrónico.	41
Configuración de un servidor de correo.	42
Comprobación de la conexión del servidor de correo.	44
Actualización del firmware.	46
Actualización del firmware con Web Config.	46
Actualización del firmware mediante el uso de Epson Firmware Updater.	46
Copia de seguridad de la configuración.	47
Cómo exportar los ajustes.	47
Cómo importar la configuración.	47

Solución de problemas

Consejos para solucionar problemas.	49
Comprobación del registro de dispositivo de red y servidor.	49

Índice

Inicialización de configuración de red.	49	Modo de uso del protocolo SNMPv3.	83
Restablecimiento de la configuración de red desde el panel de control.	49	Acerca de SNMPv3.	83
Configuración de SNMPv3.	83	Configuración de SNMPv3.	83
Comprobación de comunicación entre dispositivos y ordenadores.	49	Conexión del escáner a una red IEEE802.1X.	85
Comprobación de la conexión con un comando Ping — Windows.	49	Configuración de una red IEEE802.1X.	85
Comprobación de la conexión con un comando Ping — Mac OS.	51	Configuración de un certificado para IEEE802.1X.	86
Problemas de uso del software de red.	52	Solución de problemas de seguridad avanzada.	87
No se puede acceder a Web Config.	52	Restauración de la configuración de seguridad.	87
En EpsonNet Config no se muestra el nombre del modelo ni la dirección IP.	53	Problemas en el uso de funciones de seguridad de red.	88
		Problemas de uso de un certificado digital.	90
Apéndice			
Introducción al software de red.	55		
Epson Device Admin.	55		
EpsonNet Config.	55		
EpsonNet SetupManager.	56		
Asignación de una dirección IP mediante EpsonNet Config.	56		
Asignación de dirección IP mediante ajustes en lote.	56		
Asignación de una dirección IP distinta a cada dispositivo.	59		
Uso del puerto del escáner.	60		
Configuración de seguridad avanzada para Enterprise			
Configuración de seguridad y prevención de peligros.	62		
Configuración de las funciones de seguridad.	63		
Comunicación SSL/TLS con la impresora.	63		
Acerca de la certificación digital.	63		
Cómo obtener e importar un certificado firmado CA.	64		
Cómo eliminar un certificado firmado por entidad certificadora.	67		
Actualización de un certificado autofirmado.	68		
Configurar un Certificado CA.	69		
Comunicación cifrada mediante el uso de filtro IPsec/IP.	71		
Acerca de IPsec/Filtrado de IP.	71		
Configuración de la Norma predeterminada.	72		
Configuración de la Norma de grupo.	75		
Ejemplos de configuración de IPsec/Filtrado de IP.	81		
Configuración de un certificado para IPsec/Filtrado de IP.	82		

Copyright

Ninguna parte de esta publicación puede ser reproducida, almacenada en un sistema de recuperación o transmitida de ninguna forma ni por ningún medio, electrónico, mecánico, fotocopiado, grabación o de otra manera, sin el permiso previo por escrito de Seiko Epson Corporation. No se asume ninguna responsabilidad de patente con respecto al uso de la información contenida en este documento. Tampoco se asume ninguna responsabilidad por los daños resultantes del uso de la información aquí contenida. La información contenida en este manual está diseñada únicamente para su uso con este producto Epson. Epson no es responsable del uso de esta información si se aplica a otros productos.

Ni Seiko Epson Corporation ni sus afiliados serán responsables ante el comprador de este producto o de terceros por daños, pérdidas, costes o gastos incurridos por el comprador o terceros como resultado de un accidente, mal uso o abuso de este producto o de un uso no autorizado, modificaciones, reparaciones o alteraciones de este producto, o (excluyendo los EE.UU.) el incumplimiento estricto de las instrucciones de operación y mantenimiento de Seiko Epson Corporation.

Seiko Epson Corporation y sus afiliados no serán responsables de los daños o problemas derivados del uso de opciones o productos consumibles distintos de los designados como productos originales Epson o productos aprobados por Seiko Epson Corporation.

Seiko Epson Corporation no se hace responsable de los daños resultantes de las interferencias electromagnéticas que se producen por el uso de cualquier cable de interfaz distinto de los designados como productos aprobados por Seiko Epson Corporation.

©Seiko Epson Corporation 2016.

El contenido de este manual y las especificaciones de este producto están sujetos a cambios sin previo aviso.

Marcas comerciales

- ❑ EPSON® es una marca comercial registrada y EPSON EXCEED YOUR VISION o EXCEED YOUR VISION es una marca comercial de Seiko Epson Corporation.
- ❑ Epson Scan 2 software is based in part on the work of the Independent JPEG Group.
- ❑ Google Cloud Print™, Chrome™, Chrome OS™, and Android™ are trademarks of Google Inc.
- ❑ Microsoft®, Windows®, Windows Server®, and Windows Vista® are registered trademarks of Microsoft Corporation.
- ❑ Apple, Macintosh, Mac OS, OS X, AirMac, Bonjour, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc.
- ❑ Aviso general: Los nombres de otros productos utilizados en esta documentación se citan con el mero fin de su identificación y son marcas comerciales de sus propietarios respectivos. Epson renuncia a cualquier derecho sobre esas marcas.

Acerca de este manual

Marcas y símbolos



Precaución:

Instrucciones que deben seguirse estrictamente para evitar daños físicos.



Importante:

Instrucciones que deben seguirse para evitar daños materiales en el equipo.

Nota:

Instrucciones que contienen consejos y limitaciones en el manejo del escáner.

Información relacionada

➔ Si hace clic en este icono accederá a la información relacionada.

Descripciones utilizadas en este manual

- Las capturas de pantalla del controlador del escáner y de Epson Scan 2 (controlador del escáner) son de Windows 10 o OS X El Capitan. El contenido que aparece en las pantallas varía según el modelo y la situación.
- Las ilustraciones utilizadas en este manual son sólo ilustrativas. Aunque puede haber ligeras diferencias según el modelo, el método de funcionamiento es el mismo.
- Algunos de los elementos de menú en la pantalla LCD varían según el modelo y la configuración.

Referencias a sistemas operativos

Windows

En este manual, términos como “Windows 10”, “Windows 8.1”, “Windows 8”, “Windows 7”, “Windows Vista”, “Windows XP”, “Windows Server 2016”, “Windows Server 2012 R2”, “Windows Server 2012”, “Windows Server 2008 R2”, “Windows Server 2008”, “Windows Server 2003 R2” y “Windows Server 2003” se refieren a los siguientes sistemas operativos. Además, “Windows” se usa para hacer referencia a todas las versiones.

- 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 Vista®
- Sistema operativo Microsoft® Windows® XP
- Sistema operativo Microsoft® Windows® XP Professional x64 Edition

Acerca de este manual

- 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
- Sistema operativo Microsoft® Windows Server® 2008
- Sistema operativo Microsoft® Windows Server® 2003 R2
- Sistema operativo Microsoft® Windows Server® 2003

Mac OS

En este manual, “Mac OS” se utiliza para referirse a macOS Sierra, OS X El Capitan, OS X Yosemite, OS X Mavericks, OS X Mountain Lion, Mac OS X v10.7.x y Mac OS X v10.6.8.

Introducción

Componente manual

Este manual está dirigido al administrador del dispositivo que está a cargo de conectar la impresora o el escáner a la red y contiene información sobre cómo realizar las configuraciones para utilizar las funciones.

Consulte en la *Manual de usuario* la información sobre el uso de la función.

Preparación

Explica las tareas del administrador, cómo configurar los dispositivos y el software de administración.

Conexión

Explica cómo conectar un dispositivo a una red o línea telefónica. También explica el entorno de red, como el uso de un puerto para el dispositivo e información de servidor proxy y DNS.

Configuración de las funciones

Explica la configuración de cada función del dispositivo.

Configuración de seguridad básica

Explica la configuración de cada función: impresión, escaneado y envío y recepción de faxes.

Configuración de funcionamiento y administración

Explica las operaciones después de comenzar a usar los dispositivos: mantenimiento y comprobación de información.

Solución de problemas

Explica la inicialización de la configuración y la solución de problemas de la red.

Configuración de seguridad avanzada para Enterprise

Explica el método de configuración para mejorar la seguridad del dispositivo: uso del certificado CA, la comunicación SSL/TLS y el filtro IPsec/IP.

Según el modelo, algunas funciones de este capítulo no se admiten.

Definiciones de los términos empleados en esta guía

En esta guía se utilizan los siguientes términos.

Administrador

La persona a cargo de la instalación y la configuración del dispositivo o de la red en una oficina u organización. En el caso de organizaciones pequeñas, es posible que esta persona esté a cargo tanto de la administración del dispositivo como de la red. En el caso de las organizaciones grandes, los administradores tienen autoridad sobre la

Introducción

red o los dispositivos en la unidad de grupo de un departamento o división y los administradores de red están a cargo de la configuración de comunicación más allá de la organización, tal como Internet.

Administrador de red

La persona a cargo de controlar la comunicación de la red. La persona que configura el router, el servidor proxy, el servidor DNS y el servidor de correo para controlar la comunicación a través de Internet o de la red.

Usuario

La persona que utiliza dispositivos tales como impresoras y escáneres.

Web Config (página web del dispositivo)

El servidor web que está integrado en el dispositivo. Se llama Web Config. Puede utilizar el navegador para comprobar y cambiar el estado del dispositivo.

Herramienta

Un término genérico para el software para configurar o administrar un dispositivo, como Epson Device Admin, EpsonNet Config, EpsonNet SetupManager, etc.

Escaneado por botón de comando

Un término genérico para el escaneado desde el panel de control del dispositivo.

ASCII (American Standard Code for Information Interchange)

Uno de los códigos de caracteres estándar. Se definen 128 caracteres, incluidos caracteres tales como el alfabeto (a–z, A–Z), números arábigos (0–9), símbolos, caracteres en blanco y caracteres de control. Cuando se describe “ASCII” en esta guía, indica el 0x20–0x7E (número hexadecimal) que se menciona a continuación y no involucra caracteres de control.

SP*	!	"	#	\$	%	&	'	()	*	+	,	-	.	/
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
p	q	r	s	t	u	v	w	x	y	z	{		}	~	

* Carácter de espacio.

Unicode (UTF-8)

Un código estándar internacional, que cubre los principales idiomas mundiales. Cuando se describe “UTF-8” en esta guía, indica los caracteres de codificación en formato UTF-8.

Preparación

Este capítulo explica el rol del administrador y la preparación previa a la configuración.

Flujo de la configuración y la administración del escáner

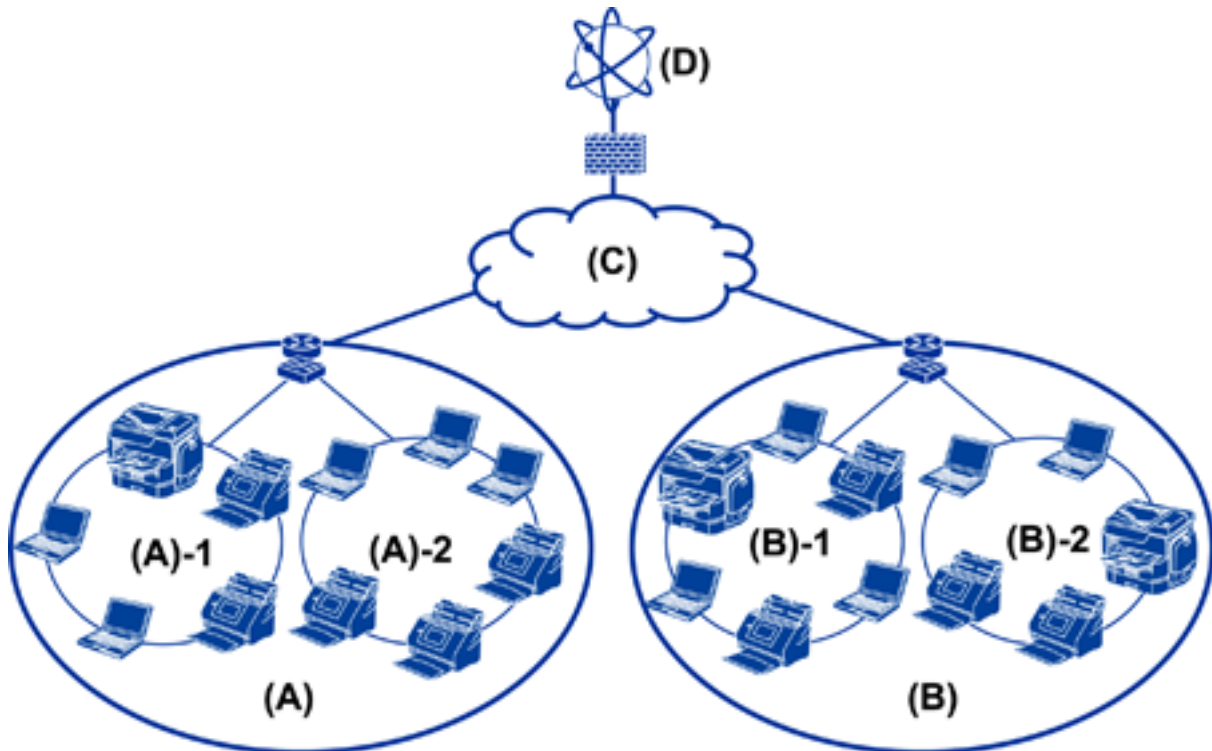
El administrador realiza configuración de la conexión de red, la configuración inicial y el mantenimiento del escáner para que puedan estar disponibles para los usuarios.

1. Preparación
 - Recopilación de información de configuración de conexión
 - Decisión sobre el método de conexión
2. Conexión
 - Conexión de red desde el panel de control del escáner
3. Configuración de las funciones
 - Configuración del controlador de escáner
 - Otras configuraciones avanzadas
4. Configuración de seguridad
 - Configuración de administrador
 - SSL/TLS
 - Control de protocolo
 - Configuración de seguridad avanzada (opción)
5. Funcionamiento y administración
 - Comprobación del estado del dispositivo
 - Manejo de la aparición de eventos
 - Copia de seguridad de la configuración del dispositivo

Información relacionada

- ➔ [“Preparación” de la página 10](#)
- ➔ [“Conexión” de la página 15](#)
- ➔ [“Configuración de las funciones” de la página 22](#)
- ➔ [“Configuración de seguridad básica” de la página 32](#)
- ➔ [“Configuración de funcionamiento y administración” de la página 40](#)

Ejemplo de entorno de red



(A): Office 1

(A) – 1: LAN 1

(A) – 2: LAN 2

(B): Office 2

(B) – 1: LAN 1

(B) – 2: LAN 2

(C): WAN

(D): Internet

Ejemplo de introducción del ajuste de conexión del escáner

Principalmente hay dos tipos de conexión en función de cómo se use el escáner. Ambos conectan el escáner a la red con el ordenador mediante el concentrador.

- Conexión servidor/cliente (escáner usando el servidor de Windows, gestión de trabajos)
- Conexión puerto a puerto (conexión directa mediante el ordenador cliente)

Información relacionada

- ➔ [“Ajuste de la conexión servidor/cliente” de la página 12](#)
- ➔ [“Ajustes de la conexión puerto a puerto” de la página 12](#)

Preparación

Ajuste de la conexión servidor/cliente

Centralice la gestión del escáner y de los trabajos la con Document Capture Pro Server instalado en el servidor. Es más adecuado para trabajos que requieren varios escáneres para escanear un gran número de documentos en un formato determinado.

Información relacionada

➔ [“Definiciones de los términos empleados en esta guía” de la página 8](#)

Ajustes de la conexión puerto a puerto

Utilice un escáner individual con un controlador de escáner como Epson Scan 2 instalado en el ordenador cliente. La instalación de Document Capture Pro (Document Capture) en el ordenador cliente le permite ejecutar trabajos en los ordenadores cliente del escáner individual.

Información relacionada

➔ [“Definiciones de los términos empleados en esta guía” de la página 8](#)

Preparación de conexión a una red

Acopio de información sobre la configuración de conexión

Para conexión de red debe contar con una dirección IP, dirección de puerta de enlace, etc. Compruebe lo siguiente de forma anticipada.

Divisiones	Elementos	Nota
Método de conexión de dispositivos	<input type="checkbox"/> Ethernet	Use un cable blindado y de pares trenzados de la categoría 5e o superior para la conexión Ethernet.
Información de conexión LAN	<input type="checkbox"/> Dirección IP <input type="checkbox"/> Máscara de subred <input type="checkbox"/> Puerta de enlace predeterminada	Si configura automáticamente la dirección IP mediante el uso de la función DHCP del router, no se requiere.
Información de servidor DNS	<input type="checkbox"/> Dirección IP para DNS primario <input type="checkbox"/> Dirección IP para DNS secundario	Si utiliza una dirección IP fija como dirección IP, configure el servidor DNS. Configure cuándo asignar automáticamente mediante la función DHCP y cuándo el servidor DNS no se puede asignar automáticamente.
Información de servidor proxy	<input type="checkbox"/> Nombre de servidor proxy <input type="checkbox"/> Número de puerto	Configúrela cuándo utilice un servidor proxy para una conexión de Internet y cuándo utilice el servicio Epson Connect o la función de actualización automática del firmware.

Preparación

Especificaciones del escáner

Para ver la especificación de que el escáner admite el modo estándar o de conexión, consulte la *Manual de usuario*.

Uso del número de puerto

Consulte el “Apéndice” para conocer el número de puerto que utiliza el escáner.

Información relacionada

➔ [“Uso del puerto del escáner” de la página 60](#)

Tipo de asignación de dirección IP

Hay dos tipos de asignación de dirección IP al escáner.

Dirección IP fija:

Asigne la dirección IP única predeterminada al escáner.

La dirección IP no se cambia aún cuando se apaga el escáner o el router, para que pueda administrar el dispositivo mediante la dirección IP.

Este tipo es adecuado para una red donde se administren varios escáneres, como es el caso de una escuela o una oficina grande.

Asignación automática mediante la función DHCP:

La dirección IP correcta se asigna automáticamente cuando la comunicación entre el escáner y el router que admite una función DHCP es satisfactoria.

Resulta conveniente cambiar la dirección IP para un dispositivo particular, reserve de antemano la dirección IP y luego asígnela.

Servidor DNS y servidor proxy

Si puede utilizar un servicio de conexión de Internet, configure el servidor DNS. Si no lo configura, debe especificar la dirección IP para acceder porque podría fallar la resolución de nombre.

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.

Puede prohibir acceso a un URL específico mediante el uso de la función de filtro, ya que el servidor proxy es capaz de comprobar el contenido de la comunicación.

Método para configurar la conexión de red

Para configurar la conexión de la dirección IP, máscara de subred y puerta de enlace predeterminada del escáner, proceda de la siguiente manera.

Preparación

Uso del panel de control:

Configure la configuración mediante el uso del panel de control del escáner de cada escáner. Conecte a la red después de configurar la configuración de conexión del escáner.

Uso del instalador:

Si se utiliza el instalador, la red del escáner y el ordenador cliente se establecen automáticamente. La configuración está disponible mediante el seguimiento de las instrucciones del instalador, aún si no tiene un conocimiento profundo de la red.

Uso de una herramienta:

Utilice una herramienta desde el ordenador del administrador. Puede descubrir un escáner y luego configurar el escáner o crear un archivo SYLK para configuración de ajustes en lote en escáneres. Puede configurar varios escáneres, pero es necesario que se conecten físicamente con un cable Ethernet antes de la configuración. Por lo tanto, esto se recomienda si puede realizar una conexión Ethernet para la configuración.

Información relacionada

- ➔ [“Conexión a la red desde el panel de control” de la página 15](#)
- ➔ [“Conexión a la red mediante el uso del instalador” de la página 19](#)
- ➔ [“Asignación de una dirección IP mediante EpsonNet Config” de la página 56](#)

Conexión

Este capítulo explica el entorno o procedimiento para conectar el escáner a la red.

Conexión a la red

Conexión a la red desde el panel de control

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

En el panel de control del escáner, consulte la *Manual de usuario* para obtener más detalles.

Asignación de dirección IP

Configure los elementos básicos, como Dirección IP, Máscara de subred y Puerta enlace predet..

1. Encienda el escáner.
2. Desplace la pantalla a la izquierda en el panel de control del escáner y luego pulse **Configuración**.

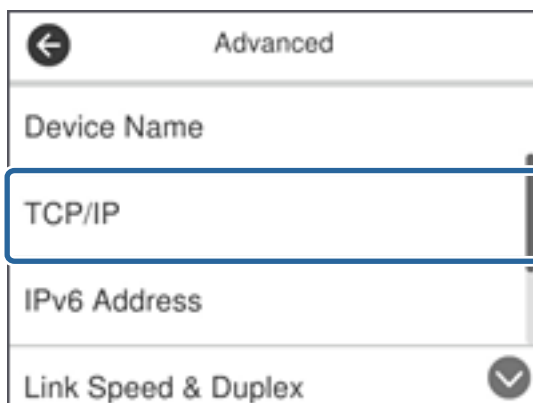


3. Pulse **Configuración de red > Cambiar configuración**.

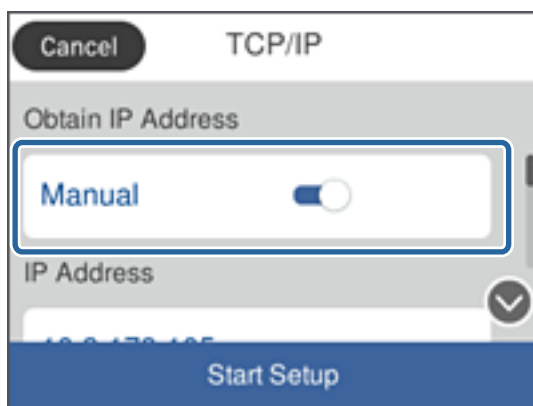
Si no se muestra el elemento, realice un movimiento ascendente en la pantalla para que se muestre.

Conexión

- Pulse **TCP/IP**.



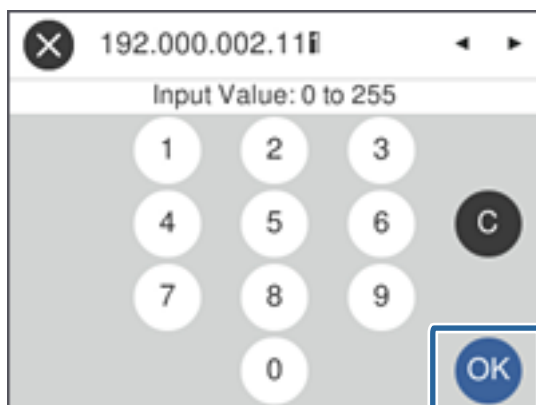
- Seleccione **Manual** para **Obtener dirección IP**.



Nota:

Cuando establezca automáticamente una dirección IP mediante el uso de la función DHCP de router, seleccione **Automático**. En ese caso, el **Dirección IP**, **Máscara de subred** y el **Puerta enlace predet.** en el paso 6 al 7 también se establecen automáticamente, así que vaya al paso 8.

- Pulse el campo **Dirección IP**, escriba la dirección IP con el teclado que se muestra en la pantalla y luego pulse **Aceptar**.



Confirme el valor reflejado en la pantalla anterior.

Conexión

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

Confirme el valor reflejado en la pantalla anterior.

Nota:

Si la combinación de Dirección IP, Máscara de subred y Puerta enlace predet. es incorrecta, **Iniciar configuración** no se activa y no se puede continuar con la configuración. Confirme que no haya un error de entrada.

8. Pulse el campo **DNS primario** en **Servidor DNS**, escriba la dirección IP del servidor DNS primario con el teclado que se muestra en pantalla y luego pulse **Aceptar.**

Confirme el valor reflejado en la pantalla anterior.

Nota:

Cuando selecciona **Automático** en la configuración de asignación de dirección IP, puede seleccionar la configuración del servidor DNS desde **Manual** o **Automático**. Si no puede obtener la dirección del servidor DNS de forma automática, seleccione **Manual** para introducir la dirección del servidor DNS. A continuación, escriba la dirección del servidor DNS secundario en forma directa. Si selecciona **Automático**, vaya al paso 10.

9. Pulse el campo **DNS secundario**, escriba la dirección IP del servidor DNS secundario con el teclado que se muestra en pantalla y luego pulse **Aceptar.**

Confirme el valor reflejado en la pantalla anterior.

10. Pulse **Iniciar configuración.**


11. Pulse **Cerrar** en la pantalla de confirmación.


La pantalla se cerrará automáticamente al cabo de un tiempo determinado si no pulsa **Cerrar**.

Conexión a Ethernet

Conecte el escáner a la red mediante el uso del cable Ethernet y compruebe la conexión.

1. Conecte el escáner y el concentrador (interruptor L2) a través de un cable Ethernet.

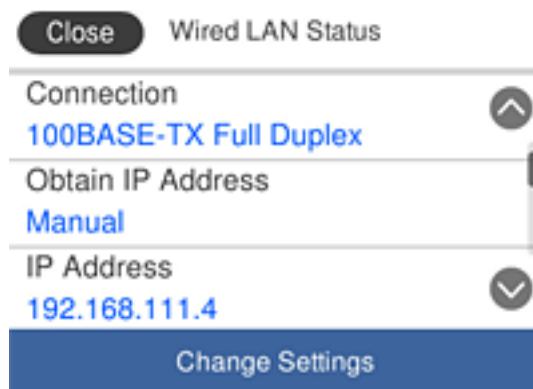
El icono de la pantalla de inicio cambia a  .

2. Pulse  en la pantalla de inicio.



Conexión

3. Desplace la pantalla hacia arriba y, a continuación, asegúrese de que el estado de la conexión y la dirección IP sean correctas.



Configuración de servidor proxy

El servidor proxy no se puede configurar en el panel. Configúrelo con Web Config.

1. Acceda a Web Config y seleccione **Configuración de red > Básica**.
2. Seleccione **Uso** en **Ajuste de Servidor proxy**.
3. Especifique el servidor proxy en la dirección IPv4 o en formato FQDN en **Servidor proxy**, y luego introduzca el número de puerto en **Nº puerto serv. proxy**.

Para servidores proxy que requieren autenticación, introduzca el nombre de usuario de autenticación del servidor proxy y la contraseña de autenticación del servidor proxy.

Conexión

4. Haga clic en el botón **Siguiente**.

The screenshot shows the EPSON Web Config interface for the DS-7600 model. The interface is divided into a left sidebar and a main content area. The sidebar contains navigation options like Administrator Logout, Status, Scanner Settings, Network Settings, Wired LAN, Basic, Email Server, Network Security Settings, Services, System Settings, Export and Import Setting Value, and Administrator Settings. Under Basic Settings, there are links for DNS/Proxy Setup, Firmware Update, Root Certificate Update, and Product Status. The main content area displays various network settings. A blue box highlights the Proxy Server Setting section, which includes the following fields and options:

- Proxy Server Setting: Do Not Use Use
- Proxy Server:
- Proxy Server Port Number:
- Proxy Server User Name:
- Proxy Server Password:

Other settings visible include DNS (Primary/Secondary DNS Server, Host Name Setting, Host Name Status, Host Name, Domain Name Setting, Domain Name Status, Domain Name, Register the network interface address to DNS), IPv6 (Setting, Privacy Extension, DHCP Server Setting, Address, Default Gateway, Link-Local Address, Stateless Address 1-3, Primary/Secondary DNS Server), and a 'Next' button at the bottom.

5. Confirme la configuración y, a continuación, haga clic en **Configuración**.

Información relacionada

- ➔ “Acceso a Web Config” de la página 23

Conexión a la red mediante el uso del instalador

Se recomienda el uso del instalador para conectar el escáner al ordenador. Siga uno de estos métodos para ejecutar el instalador.

- Configuración desde el sitio web

Acceda al siguiente sitio web y, a continuación, introduzca el nombre del producto. Vaya a **Configuración** y, a continuación, inicie la configuración.

<http://epson.sn>

- Configuración del uso del disco de software (solo para modelos que viene con un disco de software y para usuarios con ordenadores con controladores de disco.)

Inserte en el ordenador el disco del software y luego siga las instrucciones que aparezcan en pantalla.

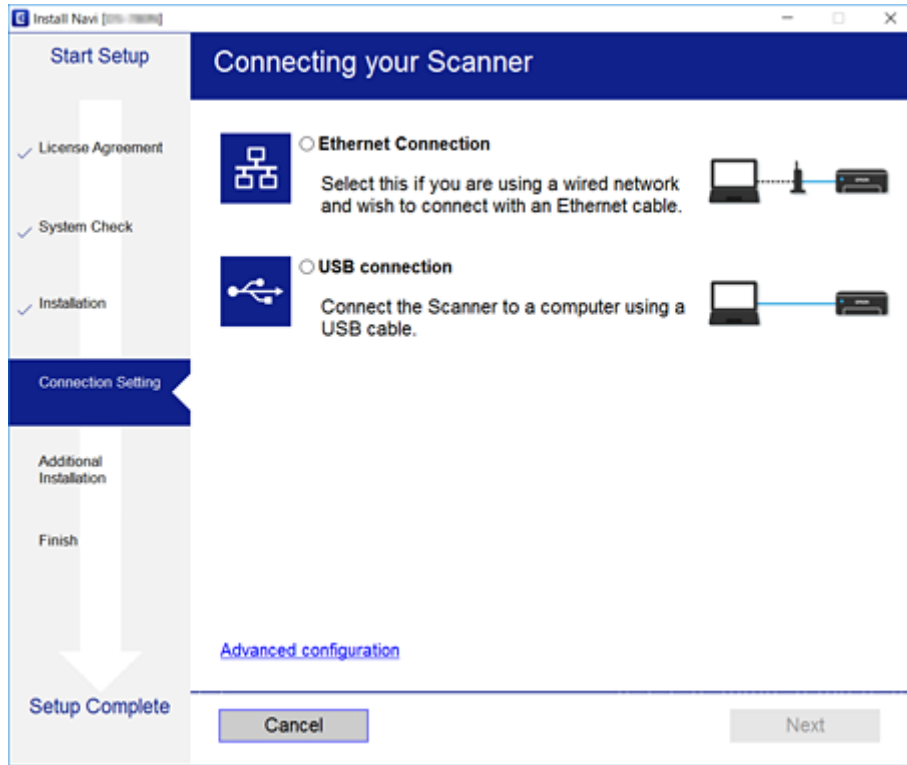
Conexión

Selección de los métodos de conexión

Siga las instrucciones en la pantalla hasta que se muestre la siguiente pantalla y luego seleccione el método de conexión del escáner al ordenador.

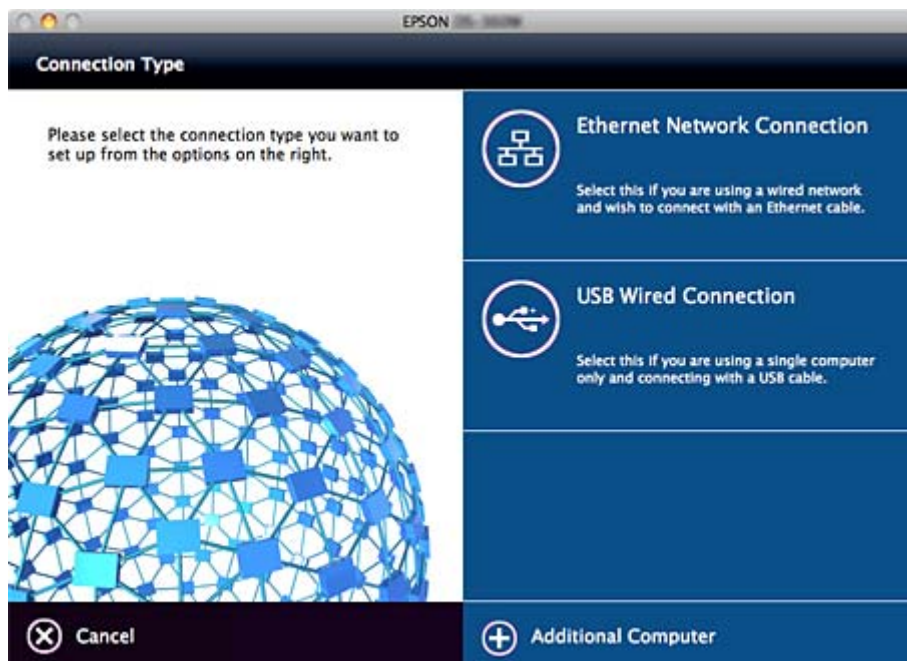
Windows

Seleccione el tipo de conexión y luego haga clic en **Siguiente**.



Mac OS

Seleccione el tipo de conexión.



Conexión

Siga las instrucciones de la pantalla. Se instalará el software necesario.

Configuración de las funciones

Este capítulo explica las primeras configuraciones que se deben realizar para usar cada función del dispositivo.

Software para ajustes

En este tema se explica el procedimiento para realizar los ajustes desde el ordenador del administrador mediante el uso de Web Config.

Web Config (página web del dispositivo)

Acerca de Web Config

Web Config es una aplicación basada en explorador que sirve para configurar el escáner.

Para acceder a Web Config, antes tiene que asignar una dirección IP al escáner.

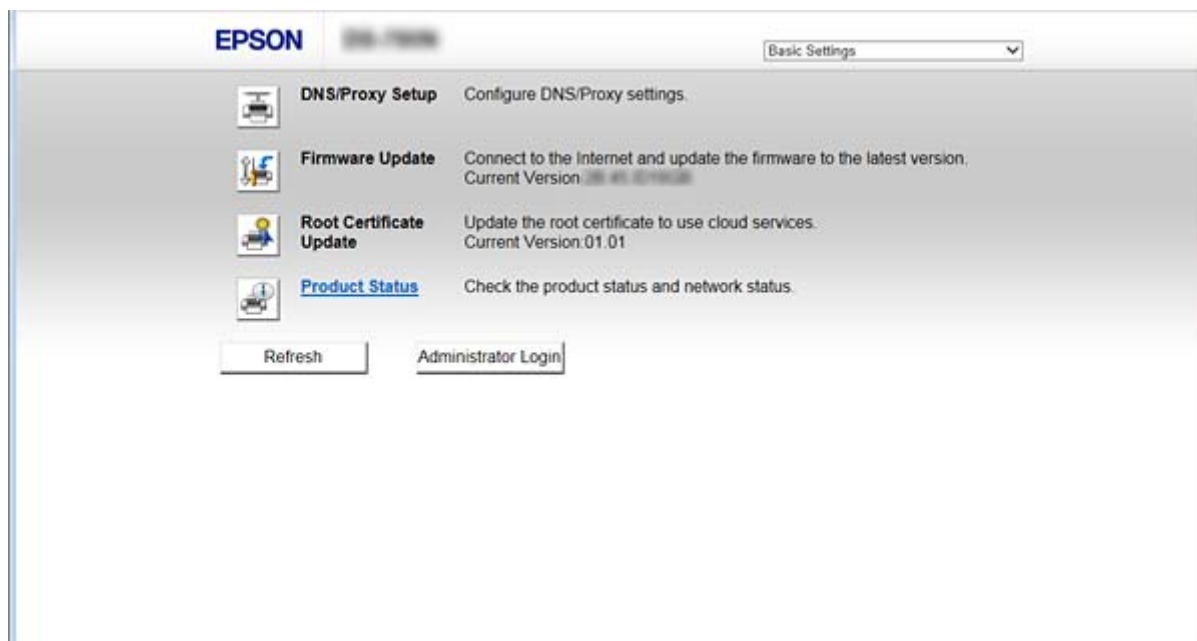
Nota:

Si desea bloquear los ajustes, configure una contraseña de administrador para el escáner.

A continuación se explican las dos páginas de ajustes.

Configuración básica

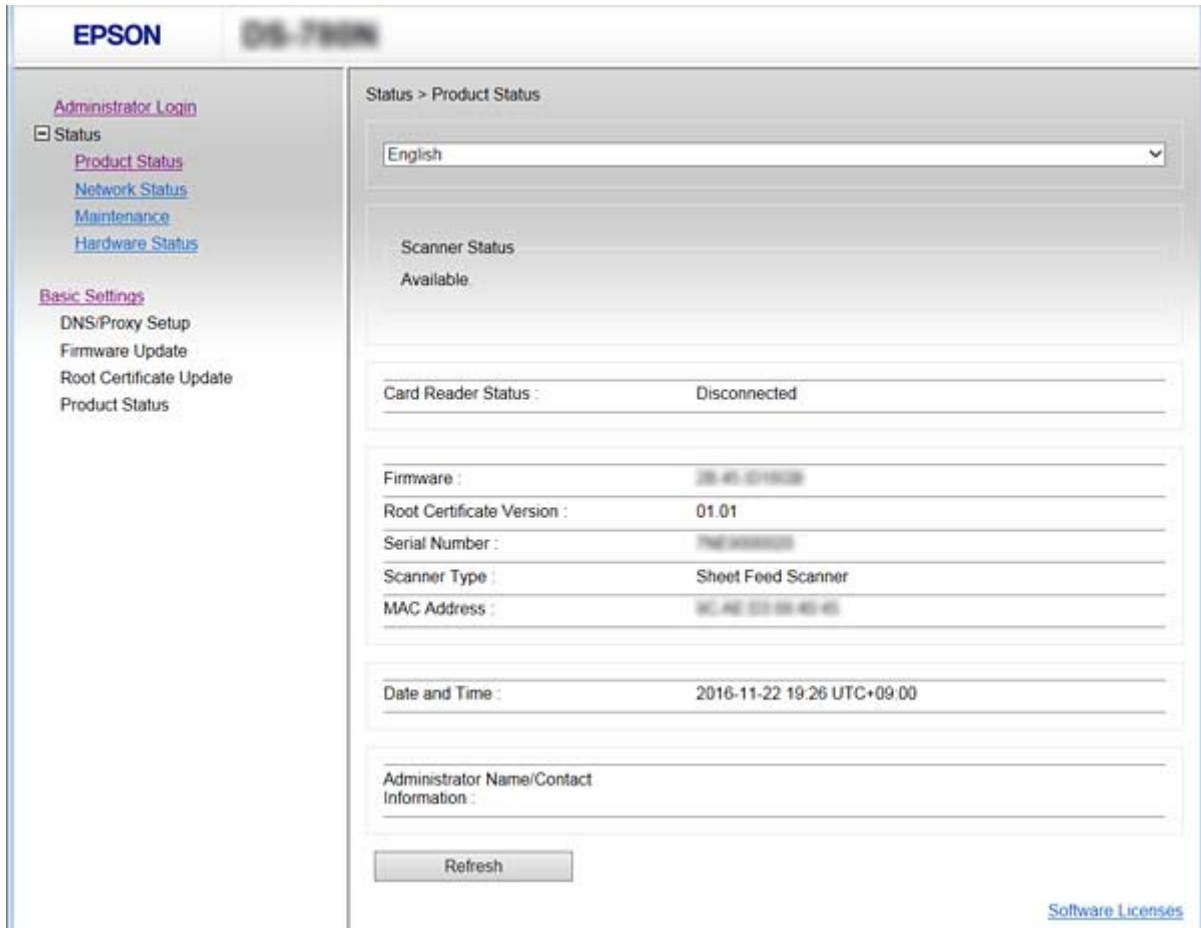
Puede realizar ajustes básicos del escáner.



Configuración de las funciones

❑ Configuración avanzada

Puede configurar los ajustes avanzados del escáner. Esta página está dirigida principalmente a los administradores.



Acceso a Web Config

Escriba la dirección IP del escáner en un explorador web. Debe tener habilitado JavaScript. Cuando acceda a Web Config mediante HTTPS, un mensaje de alerta aparecerá en el explorador dado que se usa un certificado autofirmado, almacenado en el escáner.

❑ Acceso a través de HTTPS

IPv4: <https://<dirección IP del escáner>> (no escriba las < >)

IPv6: [https://\[dirección IP del escáner\]/](https://[dirección IP del escáner]/) (escriba los [])

❑ Acceso a través de HTTP

IPv4: <http://<dirección IP del escáner>> (no escriba las < >)

IPv6: [http://\[dirección IP del escáner\]/](http://[dirección IP del escáner]/) (escriba los [])

Configuración de las funciones

Nota:

Ejemplos

IPv4:

<https://192.0.2.111/>

<http://192.0.2.111/>

IPv6:

[https://\[2001:db8::1000:1\]/](https://[2001:db8::1000:1]/)

[http://\[2001:db8::1000:1\]/](http://[2001:db8::1000:1]/)

- Si el nombre del escáner está registrado en el servidor DNS, puede utilizar el nombre del escáner en vez de su dirección IP.

Información relacionada

- ➔ [“Comunicación SSL/TLS con la impresora” de la página 63](#)
- ➔ [“Acerca de la certificación digital” de la página 63](#)

Uso de funciones de escaneado

En función de cómo utilice el escáner, instale el siguiente software y realice la configuración con él.

Escanear desde el ordenador

- Confirme la validez del servicio de exploración de red con Web Config (válido en el envío de fábrica).
- Instale Epson Scan 2 en su ordenador y configure la dirección IP
- Cuando escanee utilizando trabajos, instale Document Capture Pro (Document Capture) y establezca los ajustes del trabajo.

Escanear desde el panel de control

- Cuando se utiliza Document Capture Pro o Document Capture Pro Server:
Instale Document Capture Pro o Document Capture Pro Server
Configuración de DCP (modo de servidor, modo de cliente).
- Cuando se utiliza el protocolo WSD:
Confirme la validez de WSD en Web Config o en el panel de control (válido en el envío de fábrica)
Configuración adicional del dispositivo (ordenador con Windows).

Escaneado desde un ordenador

Instale el software y compruebe que el servicio de escaneado de red para escanear a través de una red desde el ordenador está activado.

Información relacionada

- ➔ [“Software a instalarse” de la página 25](#)
- ➔ [“Habilitación de escáner de red” de la página 25](#)

Configuración de las funciones

Software a instalarse

Epson Scan 2

Este es un controlador de escáner. Si utiliza el dispositivo desde un ordenador, instale el controlador en cada ordenador cliente. Si se instala Document Capture Pro/Document Capture, puede realizar las operaciones asignadas a los botones del dispositivo.

Con EpsonNet SetupManager, los controladores de impresora también se pueden distribuir conjuntamente en paquetes.

Document Capture Pro (Windows)/Document Capture (Mac OS)

Se instala en el ordenador cliente. Puede recuperar y ejecutar trabajos registrados en un ordenador con Document Capture Pro/Document Capture instalado en la red desde el ordenador y el panel de control del escáner.

También puede escanear desde el ordenador a través de la red. Epson Scan 2 es necesario para escanear.

Información relacionada

➔ [“EpsonNet SetupManager” de la página 56](#)

Ajuste la dirección IP del escáner en Epson Scan 2



Especifique la dirección IP del escáner para que el escáner se pueda utilizar en la red.

1. Inicie **Epson Scan 2 Utility** desde **Inicio > Todos los programas > EPSON > Epson Scan 2**.

Si ya hay otro escáner registrado, vaya al paso 2.

Si no está registrado, vaya al paso 4.

2. Haga clic en ▼ en **Escáner**.
3. Haga clic en **Ajustes**.
4. Haga clic en **Habilitar edición** y, a continuación, haga clic en **Añadir**.
5. Seleccione el nombre del modelo del escáner en **Modelo**.
6. Seleccione la dirección IP del escáner a utilizar en **Dirección** en **Buscar red**.

Haga clic en  y a continuación en  para actualizar la lista. Si no puede encontrar la dirección IP del escáner, seleccione **Entrar dirección** e introduzca la dirección IP.

7. Haga clic en **Añadir**.
8. Haga clic en **Aceptar**.

Habilitación de escáner de red

Puede configurar el servicio de escáner de red cuando escanee desde un ordenador cliente a través de la red. Se habilita la configuración predeterminada.

1. Acceda a Web Config y seleccione **Servicios > Digitalización red**.

Configuración de las funciones

2. Asegúrese de haber seleccionado **Activar escaneado de EPSON Scan**.
Si se ha seleccionado, esta tarea ha finalizado. Cierre Web Config.
Si no está seleccionado, selecciónelo y vaya al paso siguiente.
3. Haga clic en **Siguiente**.
4. Haga clic en **Aceptar**.
La red se vuelve a conectar y entonces se activan los ajustes.

Información relacionada

➔ [“Acceso a Web Config” de la página 23](#)

Escaneado desde el panel de control

La función de escaneado a carpeta y la función de escaneado a correo electrónico mediante el panel de control del escáner, así como la transferencia de los resultados del escaneado al correo, carpetas, etc. se realizan ejecutando un trabajo desde el ordenador.

Al transferir los resultados del escaneado, configure el trabajo con Document Capture Pro Server o Document Capture Pro.

Para obtener más información sobre la configuración y los ajustes de los trabajos, consulte la documentación o la ayuda de Document Capture Pro Server o de Document Capture Pro.

Información relacionada

- ➔ [“Configuración de Document Capture Pro Server/Document Capture Pro” de la página 26](#)
- ➔ [“Configuración de servidores y carpetas” de la página 27](#)

Software para instalar en el ordenador

Document Capture Pro Server

Ésta es la versión de servidor de Document Capture Pro. Instálale en un servidor Windows. El servidor puede gestionar de forma centralizada varios dispositivos y trabajos. Los trabajos se pueden ejecutar simultáneamente desde varios escáneres.

Si utiliza la versión certificada de Document Capture Pro Server, puede administrar trabajos y escanear el historial vinculado a usuarios y grupos.

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

Document Capture Pro (Windows)/Document Capture (Mac OS)

Al igual que en el escaneado desde un ordenador, puede recuperar los trabajos registrados en el ordenador desde el panel de control y ejecutarlos. No es posible ejecutar simultáneamente trabajos del ordenador desde varios escáneres.

Configuración de Document Capture Pro Server/Document Capture Pro

Realice los ajustes para utilizar la función de escaneado desde el panel de control del escáner.

Configuración de las funciones

1. Acceda a Web Config y seleccione **Servicios > Document Capture Pro**.
2. Seleccione **Modo funcionam..**
 - Modo Servidor:**
 Seleccione esta opción cuando utilice Document Capture Pro Server o cuando utilice Document Capture Pro sólo para los trabajos que se hayan configurado para un ordenador específico.
 - Modo Cliente:**
 Configure esta opción cuando seleccione la configuración de trabajo de Document Capture Pro (Document Capture) instalada en cada ordenador cliente de la red sin especificar el ordenador.
3. Ajuste lo siguiente en función del modo seleccionado.
 - Modo Servidor:**
 En **Dirección del servidor**, especifique el servidor en el que se instala Document Capture Pro Server. Puede tener de 2 a 252 caracteres en IPv4, IPv6, nombre de host, formato FQDN. En el formato FQDN, pueden usarse letras, números, alfabetos y guiones US-ASCII (excepto al principio y al final).
 - Modo Cliente:**
 Especifique **Configuración de grupo** para utilizar un grupo de escáneres especificado desde Document Capture Pro (Document Capture).
4. Haga clic en **Configuración**.

Información relacionada

➔ [“Acceso a Web Config” de la página 23](#)

Configuración de servidores y carpetas

Document Capture Pro y Document Capture Pro Server guardan los datos escaneados en el servidor o en el ordenador cliente una vez y usan la función de transferencia para ejecutar la función de escaneo a carpeta y a correo.

Necesita la autoridad y la información para transferir desde el ordenador en el que Document Capture Pro, Document Capture Pro Server está instalado al ordenador o al servicio en la nube.

Prepare la información sobre la función que utilizará consultando lo siguiente.

Puede configurar estas funciones con Document Capture Pro o Document Capture Pro Server. Para obtener más información acerca de la configuración, consulte la documentación o ayuda de Document Capture Pro Server o Document Capture Pro.

Nombre	Ajustes	Requisito
Escanear a carpeta de red (SMB)	Cree y configure la función para compartir la carpeta para guardar	La cuenta de usuario administrativo en el ordenador que crea carpetas para guardar.
	Destino para escanear a carpeta de red (SMB)	Nombre de usuario y contraseña para iniciar sesión en el ordenador que cuenta con la carpeta para guardar y el privilegio para actualizar la carpeta para guardar.

Configuración de las funciones

Nombre	Ajustes	Requisito
Escanear a carpeta de red (FTP)	Configure el inicio de sesión del servidor FTP	Información de inicio de sesión del servidor FTP y privilegio para actualizar la carpeta para guardar.
Escanear a correo electrónico	Configuración del servidor de correo electrónico	Información de configuración del servidor de correo electrónico
Escanear a Documento Capture Pro (al usar Document Capture Pro Server)	Configuración para iniciar sesión en servicios en la nube	Entorno de conexión a Internet Registro de la cuenta para servicios en la nube

Usar escaneado WSD (Windows solamente)

Si el ordenador utiliza Windows Vista o una versión posterior, puede utilizar el escaneado WSD.

Cuando se pueda utilizar el protocolo WSD, aparecerá el menú **PC (WSD)** en el panel de control del escáner.



1. Acceda a Web Config y seleccione **Servicios > Protocolo**.
2. Confirme que **Habilitar WSD** está marcado en **Configuración WSD**.
Si está marcada, la tarea está finalizada y puede cerrar Web Config.
Si no está marcada, compruébelo y continúe con el siguiente paso.
3. Haga clic en el botón **Siguiente**.
4. Confirme la configuración y haga clic en **Configuración**.

Configuración del sistema

Configuración de los ajustes avanzados de red desde el panel de control

Configurar el brillo de la pantalla

Configurar el brillo de la pantalla LCD.

1. Pulse **Configuración** en la pantalla de inicio.
2. Pulse **Config. común > Brillo LCD**.
3. Pulse  o  para ajustar el brillo.
Puede ajustarlo de 1 a 9.
4. Pulse **Aceptar**.

Configuración de las funciones

Configurar el sonido

Configure el sonido de funcionamiento del panel de control y el sonido de error.

1. Pulse **Configuración** en la pantalla de inicio.
2. Pulse **Config. común > Sonido**.
3. Configure los siguientes elementos según sea necesario.
 - Sonido de funcionamiento
Ajuste el volumen del sonido de funcionamiento del panel.
 - Sonido de error
Configure el volumen del sonido de error.
4. Pulse **Aceptar**.

Información relacionada

➔ [“Acceso a Web Config” de la página 23](#)

Detectar la alimentación doble de originales

Determine la función para detectar la alimentación doble del documento que se va a escanear y para detener el escaneado cuando se produce una alimentación múltiple.

Desactive esta opción si va escanear originales que requieren alimentación, como sobres o papel con pegatinas.

Nota:

También se puede establecer desde Web Config o Epson Scan 2.

1. Pulse **Configuración** en la pantalla de inicio.
2. Pulse **Configuración de digitalización externa > Detec. ultrasónica doble inserción**.
3. Pulse **Detec. ultrasónica doble inserción** para activarlo o desactivarlo.
4. Pulse **Cerrar**.

Establecer el modo de baja velocidad

Establezca el escaneado a baja velocidad para que no se produzcan atascos de papel al escanear documentos delgados.

1. Pulse **Configuración** en la pantalla de inicio.
2. Pulse **Configuración de digitalización externa > Len**.
3. Pulse **Len** para activarlo o desactivarlo.
4. Pulse **Cerrar**.

Configuración de ajustes del sistema con Web Config

Configuración de ahorro de energía durante inactividad

Configure el ahorro de energía para el período de inactividad del escáner. Establezca el tiempo de acuerdo con su entorno de uso.

Nota:

También puede realizar los ajustes de ahorro de energía en el panel de control del escáner.

1. Acceda a Web Config y seleccione **Configuración del sistema > Ahorro de energía**.
2. Introduzca el tiempo en **Temporizador de apagado** para cambiar al modo de ahorro de energía cuando haya inactividad.
Puede configurar hasta 240 minutos en un minuto.
3. Seleccione el tiempo de apagado para **Temporiz. de apagado aut.**
4. Haga clic en **Aceptar**.

Información relacionada

➔ [“Acceso a Web Config” de la página 23](#)

Configuración del panel de control

Configuración del panel de control del escáner. Puede configurar de la siguiente manera.

1. Acceda a Web Config y seleccione **Configuración del sistema > Panel de control**.
2. Configure los siguientes elementos según sea necesario.
 - Idioma
Seleccione el idioma que se muestra en el panel de control.
 - Bloqueo del panel
Si selecciona **ACT.**, es necesaria la contraseña de administrador cuando realice una operación que requiera la autoridad de administrador. Si la contraseña de administrador no está configurada, se desactiva el bloqueo del panel.
 - Agotado tiempo func.
Si selecciona **ACT.**, cuando inicie sesión como administrador, después de un tiempo determinado sin actividad, la sesión se cierra automáticamente y lo dirige a la página de inicio.
Puede establecer entre 10 segundos y 240 minutos en el segundo.
3. Haga clic en **Aceptar**.

Información relacionada

➔ [“Acceso a Web Config” de la página 23](#)

Configuración de las funciones

Configuración de la restricción de la interfaz externa

Puede restringir la conexión USB desde el ordenador. Configúrelo para limitar los escaneados a los realizados a través de la red.

1. Acceda a Web Config y seleccione **Configuración del sistema > Interfaz externa**.
2. Seleccione **Activar** o **Desactivar**.
Para restringirlo, seleccione **Desactivar**.
3. Pulse **Aceptar**.

Sincronización de fecha y hora con servidor de tiempo

Si utiliza un certificado CA, puede evitar problemas con el tiempo.

1. Acceda a Web Config y seleccione **Configuración del sistema > Fecha y hora > Servidor tiempo**.
2. Seleccione **Uso** para **Usar serv. tiempo**.
3. Introduzca la dirección del servidor de hora para **Dirección serv. tiempo**.
Puede utilizar el formato IPv4, IPv6 o FQDN. Escriba un máximo de 252 caracteres. Si no especifica esto, déjelo en blanco.
4. Introduzca **Intervalo de actualiz. (min.)**.
Puede configurar hasta 10.800 minutos por minuto.
5. Haga clic en **Aceptar**.

Nota:

*Puede confirmar el estado de conexión con el servidor de hora en **Estado ser. tiempo**.*

Información relacionada

➔ [“Acceso a Web Config” de la página 23](#)

Configuración de seguridad básica

Este capítulo explica la configuración de seguridad básica que no requiere un entorno especial.

Introducción a las funciones de seguridad básicas

Presentamos las funciones de seguridad básicas de dispositivos Epson.

Nombre de función	Tipo de función	Qué configurar	Qué evitar
Configuración de la contraseña de administrador	Bloquee los ajustes relacionados con el sistema, como la configuración de conexión de red y USB, de forma que sólo el administrador pueda modificarlos.	Un administrador establece una contraseña para el dispositivo. La configuración o la actualización pueden realizarse desde Web Config, el panel de control, Epson Device Admin y EpsonNet Config.	Evita las lecturas ilegales y el cambio de la información almacenada en el dispositivo, tales como ID, contraseña, configuración de red y contactos. Además, reduce una amplia variedad de riesgos de seguridad, tales como la fuga de información del entorno de red o la política de seguridad.
Comunicaciones SSL/TLS	Al acceder a un servidor Epson en Internet desde un dispositivo, como la comunicación con un ordenador mediante una actualización del navegador o del firmware, el contenido de la comunicación se cifra mediante SSL/TLS.	Obtenga un certificado firmado por entidad certificadora y luego impórtelo al escáner.	Eliminar una identificación del dispositivo 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 impresión e información de configuración.
Protocolos de controles	Los protocolos de controles se utilizan para la comunicación entre dispositivos y ordenadores y activa/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.

Información relacionada

- ➔ [“Acerca de Web Config” de la página 22](#)
- ➔ [“EpsonNet Config” de la página 55](#)
- ➔ [“Epson Device Admin” de la página 55](#)
- ➔ [“Configuración de la contraseña de administrador” de la página 33](#)
- ➔ [“Protocolos de control” de la página 35](#)

Configuración de la contraseña de administrador

Cuando configure la contraseña de administrador, los usuarios que no sean administradores no podrán cambiar los ajustes de administración del sistema. Puede establecer y cambiar la contraseña de administrador a través de Web Config, el panel de control del escáner o el software (Epson Device Admin o EpsonNet Config). Cuando utilice el software, consulte la documentación para cada software.

Información relacionada

- ➔ [“Configuración de la contraseña de administrador desde el panel de control” de la página 33](#)
- ➔ [“Configuración de la contraseña de administrador mediante Web Config” de la página 33](#)
- ➔ [“EpsonNet Config” de la página 55](#)
- ➔ [“Epson Device Admin” de la página 55](#)

Configuración de la contraseña de administrador desde el panel de control

Puede configurar la contraseña de administrador desde el panel de control del escáner.

1. Pulse **Configuración** en la pantalla de inicio.
2. Pulse **Admin. del sistema > Configuración admin.**
Si no se muestra el elemento, realice un movimiento ascendente en la pantalla para que se muestre el elemento.
3. Pulse **Contraseña admin > Registrar.**
4. Escriba la nueva contraseña y, a continuación, pulse **Aceptar.**
5. Escriba la contraseña una vez más y, a continuación, pulse **Aceptar.**
6. Pulse **Aceptar.** en la pantalla de confirmación.
Se muestra la pantalla de configuración del administrador.
7. Pulse **Configuración bloqueo** y, a continuación, **Aceptar.** en la pantalla de confirmación.
Configuración bloqueo está establecido en **Act.**, cuando opere el elemento de menú bloqueado, se le solicitará la contraseña de administrador.

Nota:

- Si configura **Configuración > Config. común > Agotado tiempo func.** en **Act.**, el escáner cerrará su sesión después de un período de inactividad del panel de control.
- Puede cambiar o eliminar la contraseña de administrador seleccionando **Cambiar** o **Restablecer** en la pantalla **Contraseña admin** y escribiendo la contraseña de administrador.

Configuración de la contraseña de administrador mediante Web Config

Puede configurar la contraseña de administrador mediante el uso de Web Config.

Configuración de seguridad básica

1. Acceda a Web Config y seleccione **Configuración del administrador > Cambiar la Información de autenticación del administrador**.
2. Introduzca una contraseña en **Contraseña nueva** y en **Confirme la contraseña nueva**. Si fuera necesario, escriba el nombre del usuario.

Para crear una contraseña nueva, introduzca la contraseña actual.

The screenshot shows the EPSON Web Config interface. On the left is a navigation menu with categories like Status, Scanner Settings, Network Settings, and Administrator Settings. The 'Administrator Settings' category is expanded, showing options like 'Change Administrator Authentication Information', 'Delete Administrator Authentication Information', 'Administrator Name/Contact Information', and 'Email Notification'. The main content area is titled 'Administrator Settings > Change Administrator Authentication Information'. It contains three password input fields: 'Current password', 'New Password' (with a note 'Enter between 1 and 20 characters'), and 'Confirm New Password'. Below the fields is an 'OK' button and a note: 'Note: It is recommended to communicate via HTTPS for entering an administrator password.'

3. Seleccione **Aceptar**.

Nota:

- Para establecer o cambiar los elementos bloqueados del menú, haga clic en **Inicio de sesión de administrador** y luego escriba la contraseña de administrador.
- Para eliminar la contraseña de administrador, haga clic en **Configuración del administrador > Borrar la Información de autenticación del administrador** y, a continuación, introduzca la contraseña de administrador.

Información relacionada

➔ [“Acceso a Web Config” de la página 23](#)

Elementos para bloqueo mediante contraseña de administrador

Los administradores cuentan con privilegios de cambios y configuración para todas las funciones de los dispositivos.

Además, si establece la contraseña de administrador en el dispositivo, puede bloquearlo para que no se puedan modificar los elementos relacionados con la administración del dispositivo.

A continuación se mencionan los elementos que puede controlar un administrador.

Configuración de seguridad básica

Elemento	Descripción
Configuración de escáner	Configuración de detección de alimentación doble y del modo de baja velocidad.
Configuración de la conexión Ethernet	Cambie el nombre de los dispositivos y la dirección IP, configure el servidor DNS o el servidor proxy y configure los cambios asociados a las conexiones de red.
Configuración de servicios del usuario	Configuración para controlar los protocolos de comunicación, el escaneado por red y los servicios Document Capture Pro.
Configuración del servidor de correo electrónico	Configuración de un servidor de correo electrónico que se comunique directamente con los dispositivos.
Configuración de seguridad	Ajuste de seguridad de red, tales como comunicación SSL/TLS, filtro IPsec/IP y IEEE802.1X.
Actualización del certificado raíz	Actualización de los certificados raíz necesarios para la autenticación de Document Capture Pro Server y la actualización del firmware desde Web Config.
Actualización de firmware	Comprobación y actualización del firmware de los dispositivos.
Configuración de hora y temporizador	Tiempo de transición a suspensión, apagado automático, fecha/hora, temporizador sin funcionamiento, otras configuraciones relacionadas al temporizador.
Restaura a la configuración predeterminada	Configuración del escáner para restablecer la configuración de fábrica.
Configuración de administrador	Configuración del bloqueo de administrador o la contraseña de administrador.
Configuración de dispositivo certificado	Configuración de ID del dispositivo de autenticación. Se usa cuando se utiliza el escáner en un sistema de autenticación compatible con dispositivos de autenticación.

Protocolos de control

Puede escanear utilizando las siguientes vías y protocolos. También puede utilizar la exploración de redes desde un número no especificado de equipos de red. Por ejemplo, se permite el escaneo utilizando sólo vías y protocolos especificados. Puede reducir los riesgos de seguridad no deliberados restringiendo el escaneado desde ciertas vías o controlando las funciones disponibles.

Configure las opciones de ajuste del protocolo.

1. Acceda a Web Config y seleccione **Servicios > Protocolo**.
2. Configure cada elemento.
3. Haga clic en **Siguiente**.
4. Haga clic en **Aceptar**.

Se aplicará la configuración al escáner.

Configuración de seguridad básica

Información relacionada

- ➔ [“Acceso a Web Config” de la página 23](#)
- ➔ [“Protocolos que puede habilitar o inhabilitar” de la página 36](#)
- ➔ [“Elementos de ajuste del protocolo” de la página 37](#)

Protocolos que puede habilitar o inhabilitar

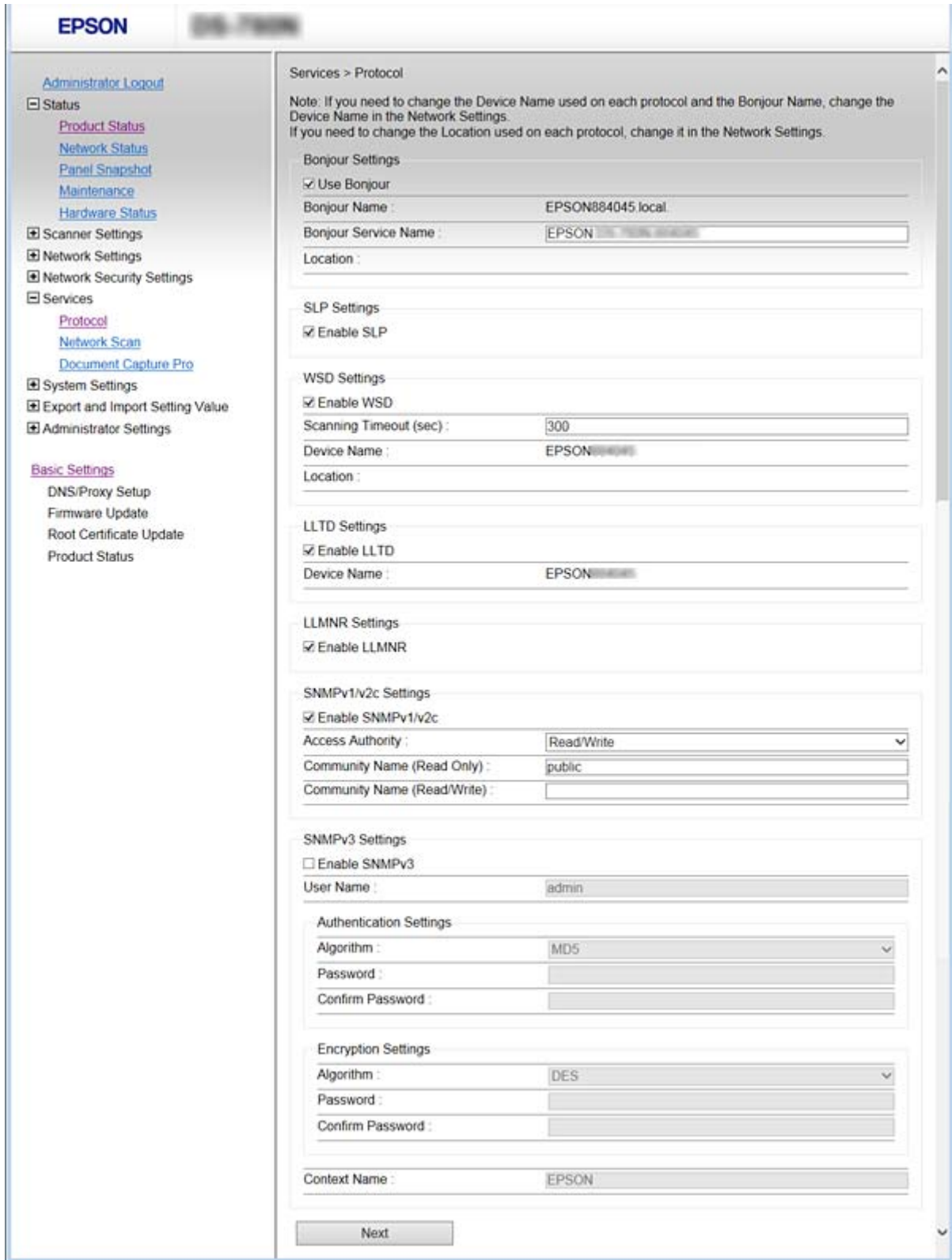
Protocolo	Descripción
Configuración Bonjour	Puede especificar si desea usar Bonjour o no. Bonjour se utiliza para buscar dispositivos, escanear, etc.
Config. SLP	Puede activar o desactivar la función SLP. SLP se utiliza para Epson Scan 2 y la búsqueda de red en EpsonNet Config.
Configuración WSD	Puede activar o desactivar la función WSD. Cuando se activa, puede agregar dispositivos WSD o escanear desde el puerto WSD.
Config. LLTD	Puede activar o desactivar la función LLTD. Cuando se habilita, se muestra en el mapa de red de Windows.
Config. LLMNR	Puede activar o desactivar la función LLMNR. Cuando se habilita, puede utilizar la resolución de nombres sin NetBIOS aunque no pueda utilizar DNS.
Configuración de SNMPv1/v2c	Puede especificar si desea habilitar SNMPv1/v2c o no. Esto se utiliza para configurar dispositivos, supervisar, etc.
Configuración de SNMPv3	Puede especificar si desea habilitar SNMPv3 o no. Esto se utiliza para configurar dispositivos cifrados, supervisar, etc.

Información relacionada

- ➔ [“Protocolos de control” de la página 35](#)
- ➔ [“Elementos de ajuste del protocolo” de la página 37](#)

Configuración de seguridad básica

Elementos de ajuste del protocolo



Elementos	Valor y descripción del ajuste
Configuración Bonjour	

Configuración de seguridad básica

Elementos	Valor y descripción del ajuste
Usar Bonjour	Seleccionar esto para buscar o usar dispositivos a través de Bonjour.
Nombre Bonjour	Muestra el nombre de Bonjour.
Nombre servic. Bonjour	Puede mostrar y configurar el nombre del servicio Bonjour.
Ubicación	Muestra el nombre de ubicación de Bonjour.
Config. SLP	
Habilitar SLP	Seleccione esta opción para habilitar la función SLP. Se utiliza para el descubrimiento de redes en Epson Scan 2 y EpsonNet Config.
Configuración WSD	
Habilitar WSD	Seleccione esta opción para habilitar la adición de dispositivos mediante WSD.
Tiempo de espera dig. (seg.)	Escriba el valor del tiempo de espera de comunicación para escaneado WSD entre 3 y 3.600 segundos.
Nombre disp.	Muestra el nombre de dispositivo de WSD.
Ubicación	Muestra el nombre de ubicación de WSD.
Config. LLTD	
Habilitar LLTD	Seleccione esta opción para habilitar LLTD. El escáner se muestra en el mapa de red de Windows.
Nombre disp.	Muestra el nombre de dispositivo de LLTD.
Config. LLMNR	
Habilitar LLMNR	Seleccione esta opción para habilitar LLMNR. Puede utilizar la resolución de nombres sin NetBIOS aunque no pueda utilizar DNS.
Configuración de SNMPv1/v2c	
Activar SNMPv1/v2c	Seleccione para habilitar SNMPv1/v2c. Solamente se muestran los escáneres que admiten SNMPv3.
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	
Activar SNMPv3	SNMPv3 está activado si la casilla está marcada.
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.

Configuración de seguridad básica

Elementos	Valor y descripción del ajuste
Contraseña	Escriba la contraseña para una autenticación de SNMPv3. Escriba entre 8 y 32 caracteres en ASCII (0x20–0x7E). Si no especifica esto, déjelo en blanco.
Confirmar contraseña	Escriba otra vez 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 en ASCII (0x20–0x7E). Si no especifica esto, déjelo en blanco.
Confirmar contraseña	Escriba otra vez la contraseña establecida para confirmarla.
Nombre de contexto	Escriba un máximo de 32 caracteres en Unicode (UTF-8). Si no especifica esto, déjelo en blanco. La cantidad de caracteres que se pueden escribir varían según el idioma.

Información relacionada

- ➔ [“Protocolos de control” de la página 35](#)
- ➔ [“Protocolos que puede habilitar o inhabilitar” de la página 36](#)

Configuración de funcionamiento y administración

Este capítulo explica los elementos relacionados con la administración y el funcionamiento diario del dispositivo.

Confirmación de la información de un dispositivo

Puede comprobar la siguiente información del dispositivo de funcionamiento desde **Estado** mediante el uso de Web Web Config.

- Estado del producto
Compruebe el idioma, el estado, el número del 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.
- Instantánea del panel
Muestre una instantánea de imagen de pantalla que se muestra en el panel de control del dispositivo.
- Mantenimiento
Compruebe la fecha de inicio, la información del escaneo, etc.
- Estado del hardware
Compruebe el estado del escáner.

Información relacionada

➔ [“Acceso a Web Config” de la página 23](#)

Administración de dispositivos (Epson Device Admin)

Mediante Epson Device Admin puede administrar y usar varios dispositivos. Epson Device Admin le permite administrar dispositivos ubicados en otra red. A continuación se describen las principales funciones de administración.

Para obtener más información acerca de las funciones y del uso del software, consulte la documentación o la Ayuda de Epson Device Admin.

- Descubrimiento de dispositivos
Puede descubrir dispositivos en la red y luego registrarlos en una lista. Si los dispositivos Epson tales como impresoras y escáneres están conectados al mismo segmento de red que el ordenador de administrador, puede encontrarlos aún si no se les ha asignado una dirección IP.
También puede descubrir dispositivos que están conectados a ordenadores en la red con cables USB. Es necesario instalar Epson Device USB Agent en el ordenador.
- Configuración de dispositivos
Puede hacer una plantilla que contenga elementos de configuración, tales como la interfaz de red y la fuente de papel, y aplicarla a otros dispositivos a modo de configuración compartida. Cuando se conecta a la red, puede asignar una dirección IP a un dispositivo que no tenga una dirección IP asignada.

Configuración de funcionamiento y administración

Supervisión de dispositivos

Puede adquirir regularmente el estado e información detallada para dispositivos en la red. También puede controlar dispositivos que estén conectados a ordenadores en la red con cables USB y dispositivos de otras compañías que hayan sido registradas a la lista de dispositivo. Para controlar dispositivos conectados mediante cables USB, necesita instalar el Epson Device USB Agent.

Administración de alertas

Puede controlar alertas acerca del estado de dispositivos y consumibles. El sistema envía automáticamente notificaciones por correo electrónico al administrador de acuerdo con las condiciones establecidas.

Administración de informes

Puede crear informes regulares a medida que el sistema acumula datos sobre el uso del dispositivo y los consumibles. Luego puede guardar los informes crearos y enviarlos por correo electrónico.

Información relacionada

➔ [“Epson Device Admin” de la página 55](#)

Cómo recibir notificaciones por correo electrónico cuando se produzcan determinadas situaciones

Acerca de las notificaciones por correo electrónico

Puede utilizar esta función para recibir alertas por correo electrónico cuando se produzca un error. Puede registrar un máximo de 5 direcciones de correo electrónico y elegir las alertas de errores que desea recibir.

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

Información relacionada

➔ [“Configuración de un servidor de correo” de la página 42](#)

Configuración de las notificaciones por correo electrónico

Para poder utilizar esta función, tiene que configurar un servidor de correo.

1. Acceda a Web Config y seleccione **Configuración del administrador > Notificación por correo electrónico**.
2. Introduzca una dirección de correo electrónico en la que desee recibir las notificaciones.
3. Seleccione el idioma de las notificaciones de correo electrónico.

Configuración de funcionamiento y administración

4. Marque las casillas de las notificaciones que desea recibir.

Administrator Settings > Email Notification

Set up the Email Server to enable the email notification.

Email Address Settings

Email in selected language will be sent to each address.

1 :	admin@aaa.com	English
2 :	aaa@aaa.com	English
3 :		English
4 :		English
5 :		English

Notification Settings

Email will be sent when product status is as checked.

	1	2	3	4	5
Administrator password changed	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Scanner error	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK Restore Default Settings

5. Haga clic en **Aceptar**.

Información relacionada

- ➔ “Acceso a Web Config” de la página 23
- ➔ “Configuración de un servidor de correo” de la página 42

Configuración de un servidor de correo

Compruebe lo siguiente antes de realizar la configuración.

- El escáner está conectado a una red.
- La información del servidor de correo electrónico del ordenador.

1. Acceda a Web Config y seleccione **Configuración de red > Servidor correo electrónico > Básica**.
2. Introduzca un valor para cada opción.
3. Seleccione **Aceptar**.

Se mostrarán los ajustes que ha seleccionado.

Información relacionada

- ➔ “Acceso a Web Config” de la página 23
- ➔ “Opciones de ajuste del servidor de correo” de la página 43

Configuración de funcionamiento y administración

Opciones de ajuste del servidor de correo

EPSON F8-888888

Network Settings > Email Server > Basic

The certificate is required to use a secure function of the email server. Make settings on the following page.

- CA Certificate
- Root Certificate Update

Authentication Method : SMTP AUTH

Authenticated Account : [text]

Authenticated Password : [masked]

Sender's Email Address : [text]

SMTP Server Address : [text]

SMTP Server Port Number : 25

Secure Connection : None

Certificate Validation : Enable Disable

It is recommended to enable the Certificate Validation. It will be connected without confirming the safety of the email server when the Certificate Validation is disabled.

POP3 Server Address : [text]

POP3 Server Port Number : [text]

OK

Opciones	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 , introduzca el nombre de la cuenta autenticada de manera que tenga entre 0 y 20 caracteres. Caracteres admitidos: A–Z a–z 0–9 ! # \$ % & ' * + - . / = ? ^ _ { } ~ @.	
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.	

Configuración de funcionamiento y administración

Opciones	Ajustes y explicación	
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. Recomendamos establecer esta opción en 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.	

Información relacionada

➔ [“Configuración de un servidor de correo” de la página 42](#)

Comprobación de la conexión del servidor de correo

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

Información relacionada

➔ [“Acceso a Web Config” de la página 23](#)

➔ [“Referencias de la prueba de conexión del servidor de correo” de la página 44](#)

Referencias de la prueba de conexión del servidor de correo

Mensajes	Explicación
Prueba de conexión correcta.	Este mensaje aparece si la conexión con el servidor es satisfactoria.
Error de comunicación del servidor SMTP. Compruebe lo siguiente. - Configuración de red	<p>Aparece este mensaje cuando</p> <ul style="list-style-type: none"> <input type="checkbox"/> El escáner no está conectado a una red <input type="checkbox"/> El servidor SMTP está fuera de servicio <input type="checkbox"/> La conexión de red se ha interrumpido durante la comunicación <input type="checkbox"/> Datos incompletos recibidos

Configuración de funcionamiento y administración

Mensajes	Explicación
Error de comunicación del servidor POP3. Compruebe lo siguiente. - Configuración de red	Aparece este mensaje cuando <ul style="list-style-type: none"> <input type="checkbox"/> El escáner no está conectado a una red <input type="checkbox"/> El servidor POP3 está fuera de servicio <input type="checkbox"/> La conexión de red se ha interrumpido durante la comunicación <input type="checkbox"/> Datos incompletos recibidos
Error al conectar con el servidor SMTP. Compruebe lo siguiente. - Dirección del servidor SMTP - Servidor DNS	Aparece este mensaje cuando <ul style="list-style-type: none"> <input type="checkbox"/> Error al conectar con un servidor DNS <input type="checkbox"/> 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	Aparece este mensaje cuando <ul style="list-style-type: none"> <input type="checkbox"/> Error al conectar con un servidor DNS <input type="checkbox"/> Error en la resolución de nombre para un servidor POP3
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.
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.

Configuración de funcionamiento y administración

Mensajes	Explicación
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.

Información relacionada

➔ [“Comprobación de la conexión del servidor de correo” de la página 44](#)

Actualización del firmware

Actualización del firmware con Web Config

Actualiza el firmware usando Web Config. El dispositivo se debe conectar a Internet.

1. Acceda a Web Config y seleccione **Configuración básica > Actualización del firmware**.
2. Haga clic en **Iniciar**.
Se inicia la confirmación del firmware y, si hay un firmware actualizado, se muestra la información del mismo.
3. Haga clic en **Iniciar** y siga las instrucciones de la pantalla.

Nota:

También puede actualizar el firmware utilizando Epson Device Admin. Puede confirmar visualmente la información del firmware en la lista de dispositivos. Resulta útil cuando desea actualizar el firmware de varios dispositivos. Consulte la ayuda de Epson Device Admin para obtener más información.

Información relacionada

➔ [“Acceso a Web Config” de la página 23](#)

➔ [“Epson Device Admin” de la página 55](#)

Actualización del firmware mediante el uso de Epson Firmware Updater

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.

1. Acceda al sitio web de Epson y descargue el firmware.
2. Conecte el ordenador que contenga el firmware descargado en el dispositivo con un cable USB.

Configuración de funcionamiento y administración

3. Haga doble clic sobre el archivo .exe descargado.
Epson Firmware Updater se iniciará.
4. Siga las instrucciones de la pantalla.

Copia de seguridad de la configuración

Puede copiar los elementos a los otros escáneres mediante la exportación de elementos de ajuste en Web Config.

Cómo exportar los ajustes

Exporte ajustes específicos del escáner.

1. Acceda a Web Config y seleccione **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 y la dirección IP del escáner, pulse **Habilitar para seleccionar la configuración individual del dispositivo** y seleccione más elementos. Utilice solamente los valores seleccionados para el escáner de reemplazo.*

Información relacionada

➔ [“Acceso a Web Config” de la página 23](#)

Cómo importar la configuración

Importe el archivo de Web Config exportado al escáner.

 **Importante:**

Cuando importe valores que incluyan información individual como el nombre o la dirección IP del escáner, asegúrese de que la misma dirección IP no existe en la misma red. Si la dirección IP se solapa, el escáner no reflejará el valor.

1. Acceda a Web Config y seleccione **Exportar e importar valor de configuración > Importar**.
2. Seleccione el archivo exportado y, a continuación, escriba la contraseña cifrada.

Configuración de funcionamiento y administración

3. Haga clic en **Siguiente**.
4. Seleccione los ajustes que desea importar y haga clic en **Siguiente**.
5. Haga clic en **Aceptar**.

Se aplicará la configuración al escáner.

Información relacionada

➔ [“Acceso a Web Config” de la página 23](#)

Solución de problemas

Consejos para solucionar problemas

Encontrará más información en el siguientes manual.

- Manual de usuario

Instrucciones sobre el uso del escáner, el mantenimiento y la resolución de problemas.

Comprobación del registro de dispositivo de red y servidor

En caso de problemas con la conexión de red, es posible que se pueda identificar la causa confirmando el registro del servidor de correo, del servidor LDAP, etc., comprobando el estado mediante el registro de la red de los registros y comandos del equipo del sistema, como los enrutadores.

Inicialización de configuración de red

Restablecimiento de la configuración de red desde el panel de control

Puede recuperar todos los ajustes predeterminados de la red.

1. Pulse **Configuración** en la pantalla de inicio.
2. Pulse **Admin. del sistema** > **Restaurar configuración pred.** > **Configuración de red**.
3. Revise el mensaje y luego pulse **Sí**.
4. Cuando se muestre un mensaje de finalización, pulse **Cerrar**.

La pantalla se cerrará automáticamente al cabo de un tiempo determinado si no pulsa **Cerrar**.

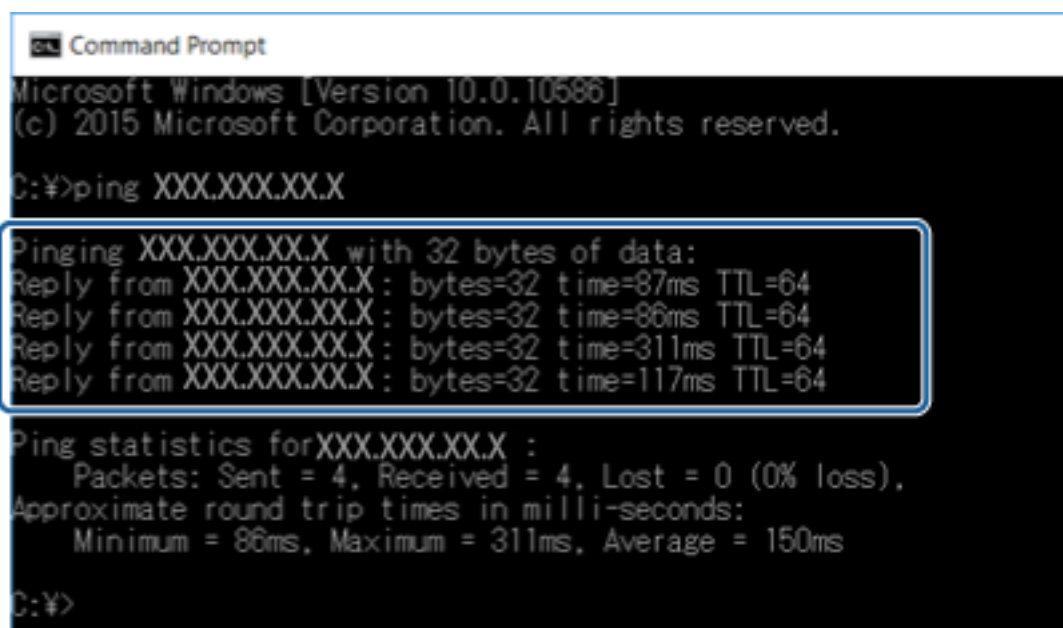
Comprobación de comunicación entre dispositivos y ordenadores

Comprobación de la conexión con un comando Ping — Windows

Puede usar un comando Ping para comprobar que el ordenador esté conectado al escáner. Siga los siguientes pasos para comprobar la conexión mediante un comando Ping.

Solución de problemas

1. Averigüe la dirección IP del escáner para la conexión que quiera comprobar.
Puede comprobarlo usando Epson Scan 2.
2. En el ordenador, abra la pantalla del símbolo del sistema.
 - ❑ Windows 10
Haga clic con el botón derecho en el botón de Inicio o manténgalo pulsado y, a continuación, seleccione **Símbolo del sistema**.
 - ❑ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
Abra la pantalla de la aplicación y seleccione **Símbolo del sistema**.
 - ❑ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 o anteriores
Haga clic en el botón de Inicio, seleccione **Todos los programas** o **Programas > Accesorios > Símbolo del sistema**.
3. Escriba "ping xxx.xxx.xxx.xxx" y pulse la tecla Intro.
Escriba la dirección IP del escáner para xxx.xxx.xxx.xxx.
4. Compruebe el estado de la comunicación.
Si hay comunicación entre el escáner y el ordenador, aparecerá el siguiente mensaje.



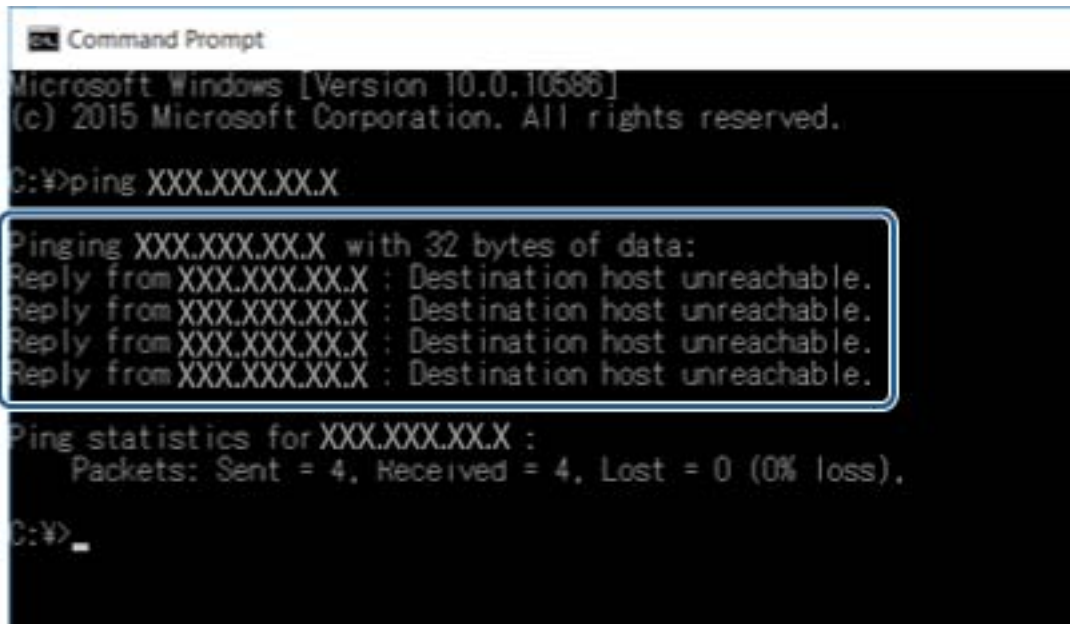
```
Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.
C:\>ping XXX.XXX.XX.X

Pinging XXX.XXX.XX.X with 32 bytes of data:
Reply from XXX.XXX.XX.X : bytes=32 time=87ms TTL=64
Reply from XXX.XXX.XX.X : bytes=32 time=86ms TTL=64
Reply from XXX.XXX.XX.X : bytes=32 time=311ms TTL=64
Reply from XXX.XXX.XX.X : bytes=32 time=117ms TTL=64

Ping statistics for XXX.XXX.XX.X :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 86ms, Maximum = 311ms, Average = 150ms
C:\>
```

Solución de problemas

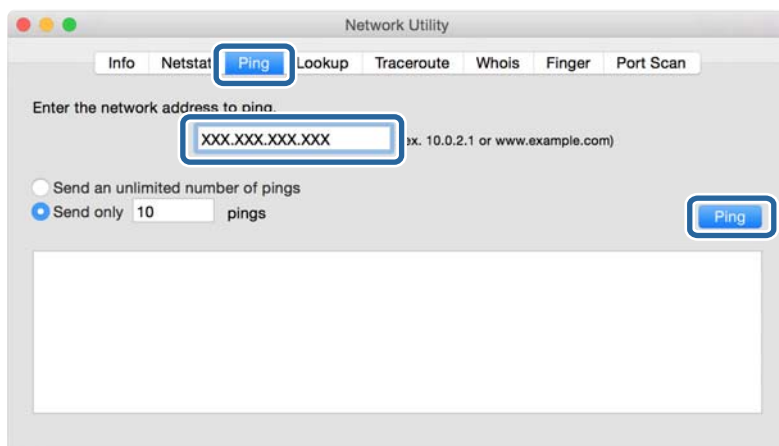
Si no hay comunicación entre el escáner y el ordenador, aparecerá el siguiente mensaje.



Comprobación de la conexión con un comando Ping — Mac OS

Puede usar un comando Ping para comprobar que el ordenador esté conectado al escáner. Siga los siguientes pasos para comprobar la conexión mediante un comando Ping.

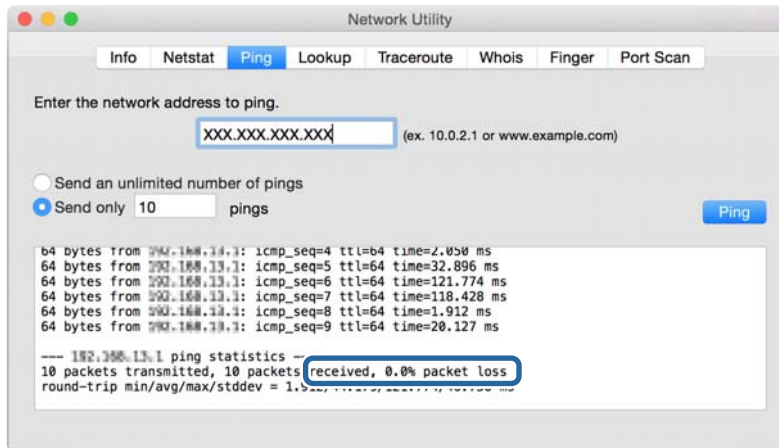
1. Averigüe la dirección IP del escáner para la conexión que quiera comprobar.
Puede comprobarlo con Epson Scan 2.
2. Ejecute Network Utility.
Escriba "Network Utility" en **Spotlight**.
3. Haga clic en la ficha **Ping**, escriba la dirección IP que averiguó en el paso 1 y haga clic en **Ping**.



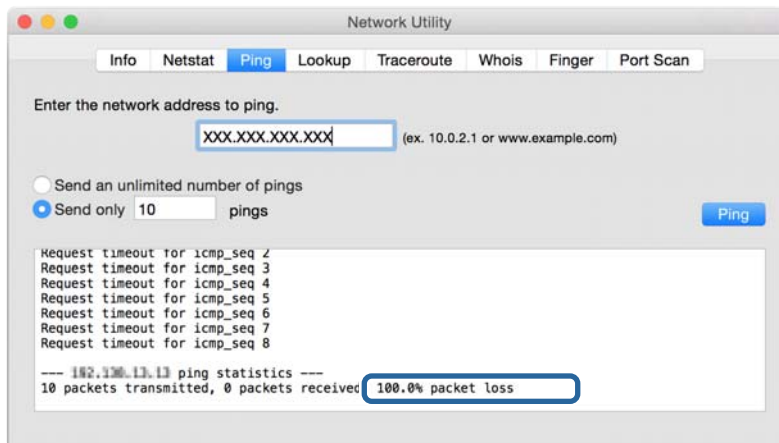
Solución de problemas

4. Compruebe el estado de la comunicación.

Si hay comunicación entre el escáner y el ordenador, aparecerá el siguiente mensaje.



Si no hay comunicación entre el escáner y el ordenador, aparecerá el siguiente mensaje.



Problemas de uso del software de red

No se puede acceder a Web Config

¿Está bien configurada la dirección IP del escáner?

Configure la dirección IP utilizando Epson Device Admin o EpsonNet Config.

¿Admite su navegador cifrado masivo para Intensidad de cifrado para SSL/TLS?

Los cifrados masivos para Intensidad de cifrado para SSL/TLS son los siguientes. Solamente se puede acceder a Web Config con un navegador que admita los siguientes cifrados masivos. Averigüe qué cifrados admite su navegador.

- 80 bits: AES256/AES128/3DES
- 112 bits: AES256/AES128/3DES
- 128 bits: AES256/AES128

Solución de problemas

- 192 bits: AES256
- 256 bits: AES256

Cuando accedo a Web Config con una comunicación SSL (https), aparece el mensaje “Sin actualizar”.

Si el certificado ha caducado, vuelva a obtenerlo. Si el mensaje aparece antes de su fecha de caducidad, compruebe que la fecha del escáner esté correctamente configurada.

Cuando accedo a Web Config con una comunicación SSL (https), aparece el mensaje “El nombre del certificado de seguridad no coincide con...”.

La dirección IP del escáner indicada en **Nombre común** para crear el certificado autofirmado o la CSR no coincide con la dirección escrita en el navegador. Obtenga un certificado e impórtelo otra vez o cambie el nombre del escáner.

Se accede al escáner a través de un servidor proxy.

Si utiliza un servidor proxy con su escáner, tiene que configurar los ajustes de proxy de su navegador.

Windows:

Seleccione **Panel de control > Redes e Internet > Opciones de Internet > Conexiones > Configuración de LAN > Servidor proxy** y establezca en la configuración que no se utilice el servidor proxy para las direcciones locales.

Mac OS:

Seleccione **Preferencias del Sistema > Red > Avanzado > Proxies** y registre la dirección local para **Omitir ajustes proxy para estos servidores y dominios**.

Por ejemplo:

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

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

Información relacionada

- ➔ [“Acceso a Web Config” de la página 23](#)
- ➔ [“Asignación de dirección IP” de la página 15](#)
- ➔ [“Asignación de una dirección IP mediante EpsonNet Config” de la página 56](#)

En EpsonNet Config no se muestra el nombre del modelo ni la dirección IP

¿Cuándo apareció un recordatorio importante de Seguridad de Windows o la pantalla de Firewall usted seleccionó Bloquear, Cancelar o Apagar?

Si seleccionó **Bloquear, Cancelar** o **Apagar**, la dirección IP y el nombre del modelo no se mostrarán ni en EpsonNet Config ni en EpsonNet Setup.

Para evitar esto, registre EpsonNet Config como una excepción con el Firewall de Windows y un software de seguridad. Si utiliza un antivirus o un programa de seguridad, ciérrelo y luego intente usar EpsonNet Config.

Solución de problemas

¿El tiempo de espera del error de comunicación es demasiado breve?

Ejecute EpsonNet Config y seleccione **Tools > Options > Timeout**. Aumente el tiempo en el ajuste de **Communication Error**. Tenga presente que al aumentar ese tiempo, EpsonNet Config funcionará con más lentitud.

Información relacionada

- ➔ [“Cómo ejecutar EpsonNet Config en Windows” de la página 56](#)
- ➔ [“Cómo ejecutar EpsonNet Config en Mac OS” de la página 56](#)

Apéndice

Introducción al software de red

A continuación se describe el software que configura y administra dispositivos.

Epson Device Admin

Epson Device Admin es una aplicación que le permite instalar dispositivos en la red para luego configurar y administrar los dispositivos. Puede adquirir información detallada sobre los dispositivos, como el estado y los consumibles, enviar notificaciones de alerta y crear informes para el uso de dispositivo. También puede hacer una plantilla que contenga elementos de configuración y aplicarla a otros dispositivos a modo de configuración compartida. Puede descargar Epson Device Admin desde el sitio web de soporte de Epson. Para obtener más información, consulte el manual o la ayuda de Epson Device Admin.

Ejecución de Epson Device Admin (solo para Windows)

Seleccione **Todos los programas > EPSON > Epson Device Admin > Epson Device Admin**.

Nota:

Si aparece la alerta del Firewall, permita el acceso a Epson Device Admin.

EpsonNet Config

Con EpsonNet Config, el administrador puede configurar los ajustes de red del escáner (asignarle una dirección IP y cambiar el modo de conexión, por ejemplo). La función de configuración en lote está disponible para Windows. Para obtener más información, consulte el manual o la ayuda de EpsonNet Config.



Cómo ejecutar EpsonNet Config en Windows

Seleccione **Todos los programas > EpsonNet > EpsonNet Config SE > EpsonNet Config**.

Nota:

Si aparece la alerta del Firewall de Windows, permita el acceso a EpsonNet Config.

Cómo ejecutar EpsonNet Config en Mac OS

Seleccione **Ir a > Aplicaciones > Epson Software > EpsonNet > EpsonNet Config SE > EpsonNet Config**.

EpsonNet SetupManager

Con EpsonNet SetupManager puede crear un paquete básico de instalación de escáneres (que instale y configure el controlador del escáner y que instale Document Capture Pro, por ejemplo). Este software permite al administrador crear paquetes de software únicos y repartirlos entre grupos.

Para obtener más información, consulte el sitio web Epson de su zona.

Asignación de una dirección IP mediante EpsonNet Config

Puede asignar una dirección IP al escáner mediante EpsonNet Config. EpsonNet Config le permite asignar una dirección IP al escáner al que no se ha asignado ninguna tras la conexión a través de un cable Ethernet.

Asignación de dirección IP mediante ajustes en lote

Creación de archivo para ajustes en lote

Mediante el uso de la dirección MAC y el nombre de modelo como claves, puede crear un nuevo archivo SYLK para configurar la dirección IP.

1. Abra una aplicación de hoja de cálculo (como Microsoft Excel) o un editor de texto.
2. Escriba “Info_MACAddress”, “Info_ModelName” y “TCPIP_IPAddress” en la primera fila como los nombre de elemento de configuración.

Escriba elementos de configuración para la siguientes cadenas de texto. Para que distinga entre mayúsculas y minúsculas y entre caracteres de uno y dos bytes, si tan solo un carácter es diferente, no se reconocerá el elemento.

Escriba el nombre del elemento de configuración tal como se describe a continuación; de otra manera, EpsonNet Config no puede reconocer los elementos de configuración.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

Apéndice

3. Escriba la dirección MAC, el nombre del modelo y la dirección IP para cada interfaz de red.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress
0000XXXX0001	ALC-XXXXX	192.168.100.102
0000XXXX0002	ALC-XXXXX	192.168.100.103
0000XXXX0003	ALC-XXXXX	192.168.100.104

4. Escriba un nombre y guarde como archivo SYLK (*.slk).

Configuración de ajustes en lote mediante el uso de archivo de configuración

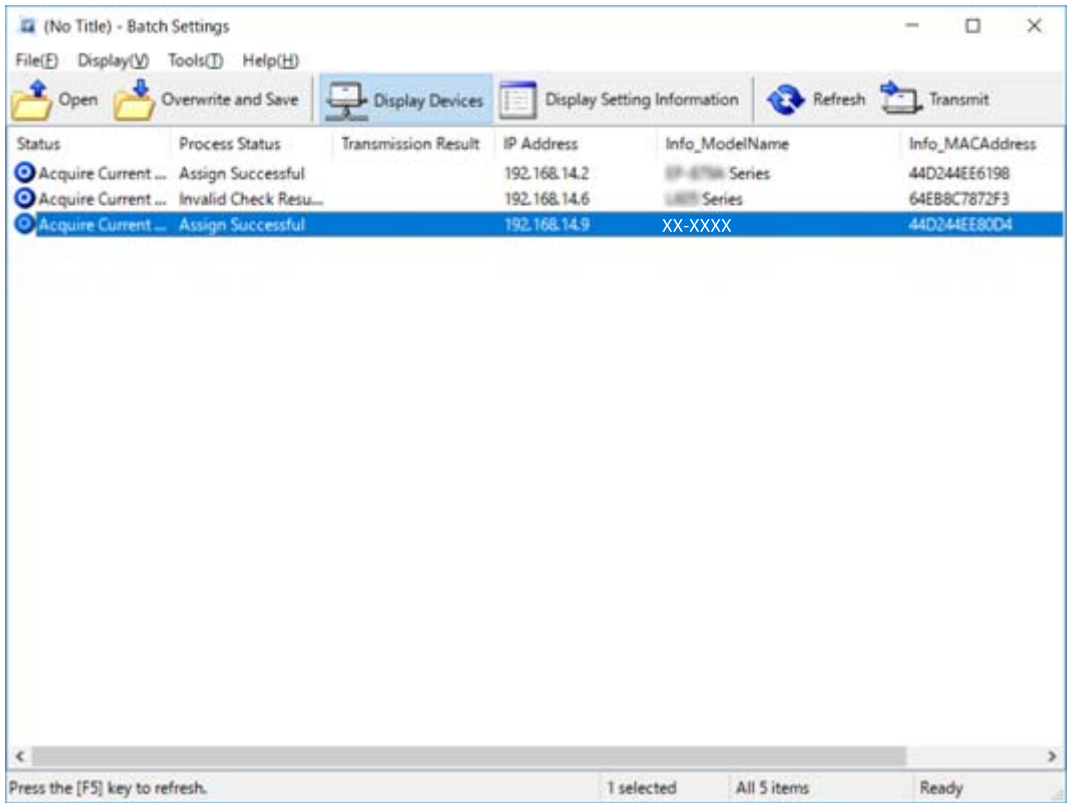
Asignación de direcciones IP en el archivo de configuración (archivo SYLK) a la vez. Debe crear el archivo de configuración antes de realizar la asignación.

1. Conecte todos los dispositivos a la red con un cable Ethernet.
2. Encienda el escáner.
3. Inicie EpsonNet Config.
Se muestra una lista de escáneres en la red. Es posible que demore un tiempo antes de que se muestre.
4. Haga clic en **Tools > Batch Settings**.
5. Haga clic en **Open**.
6. En la pantalla de selección de archivos, seleccione el archivo SYLK (*.slk) que contiene la configuración y luego haga clic en **Open**.

Apéndice

- 7. Seleccione los dispositivos para los que desea realizar ajustes en lote con la columna **Status** ajustada en **Unassigned**, y **Process Status** en **Assign Successful**.

Para realizar varias selecciones, pulse Ctrl o flecha hacia arriba y haga clic o arrastre su mouse.



- 8. Haga clic en **Transmit**.
- 9. Cuando se muestra la pantalla de introducción de contraseña, escriba la contraseña y luego haga clic en **OK**.
Transmita la configuración.

Nota:

La información se transmite a la interfaz de red hasta que finaliza la barra de progreso. No apague el dispositivo ni el adaptador inalámbrico y no envíe ningún dato al dispositivo.






- 10. En la pantalla **Transmitting Settings**, haga clic en **OK**.



Apéndice

11. Compruebe el estado del dispositivo que configuró.

En el caso de los dispositivos que muestran  o , compruebe el contenido del archivo de configuración o asegúrese de que el dispositivo se haya reiniciado normalmente.

Icono	Status	Process Status	Explicación
	Setup Complete	Setup Successful	La configuración se completó normalmente.
	Setup Complete	Rebooting	Cuando la información haya sido transmitida, deberá reiniciar cada dispositivo para habilitar la configuración. Se realiza una comprobación para determinar si el dispositivo se puede o no conectar después del reinicio.
	Setup Complete	Reboot Failed	No se puede confirmar el dispositivo después de transmitir la configuración. Compruebe que el dispositivo esté encendido o que se haya reiniciado normalmente.
	Setup Complete	Searching	Búsqueda del dispositivo indicado en el archivo de configuración.*
	Setup Complete	Search Failed	No se pueden comprobar los dispositivos que ya hayan sido configurados. Compruebe que el dispositivo esté encendido o que se haya reiniciado normalmente.*

* Solo cuando se muestre la información de configuración.

Información relacionada

- ➔ [“Cómo ejecutar EpsonNet Config en Windows” de la página 56](#)
- ➔ [“Cómo ejecutar EpsonNet Config en Mac OS” de la página 56](#)

Asignación de una dirección IP distinta a cada dispositivo

Asigne una dirección IP al escáner mediante EpsonNet Config.

1. Encienda el escáner.
2. Conecte el escáner a la red con un cable Ethernet.
3. Inicie EpsonNet Config.

Se muestra una lista de escáneres en la red. Es posible que demore un tiempo antes de que se muestre.

4. Haga doble clic en el escáner al que desea asignar.

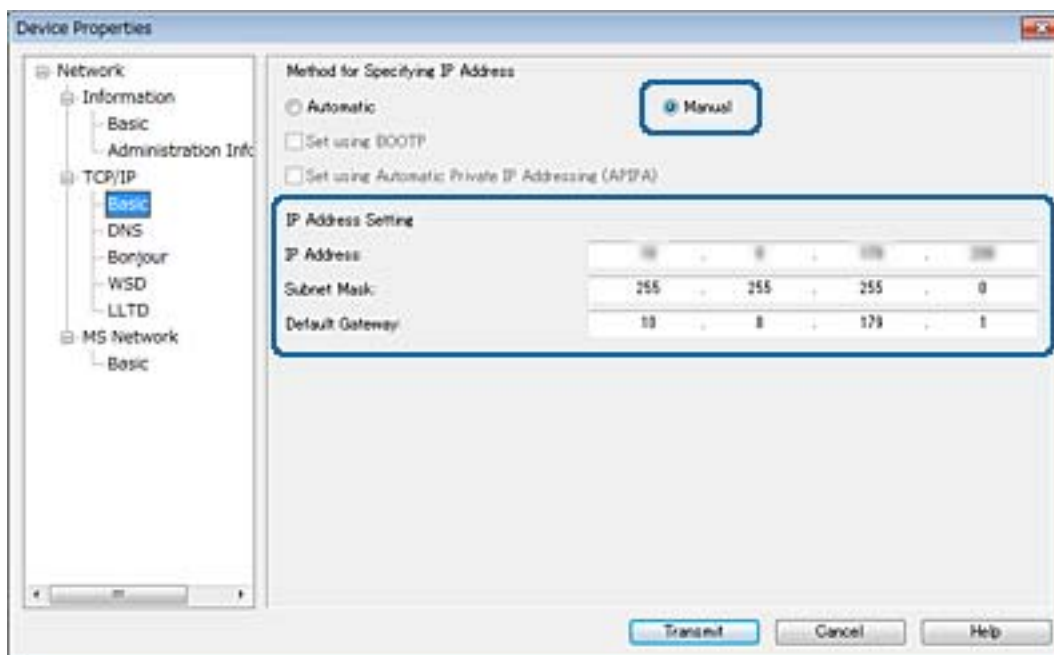
Nota:

Si ha conectado diversos escáneres del mismo modelo, puede identificar el escáner mediante el uso de la dirección MAC.

5. Seleccione **Network > TCP/IP > Basic**.

Apéndice

6. Introduzca las direcciones para **IP Address**, **Subnet Mask**, y **Default Gateway**.



Nota:

Escriba una dirección fija cuando conecte el escáner a una red segura.

7. Haga clic en **Transmit**.

Aparece una pantalla que confirma la transmisión de la información.

8. Haga clic en **OK**.

Aparecerá la pantalla de finalización de la transmisión.

Nota:

La información se transmite al dispositivo y, a continuación, se muestra un mensaje indicando que la configuración ha finalizado correctamente. No apague el dispositivo y no envíe ningún dato al servicio.

9. Haga clic en **OK**.

Información relacionada

- ➔ [“Cómo ejecutar EpsonNet Config en Windows” de la página 56](#)
- ➔ [“Cómo ejecutar EpsonNet Config en Mac OS” de la página 56](#)

Uso del puerto del escáner

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

Apéndice

Remitente (cliente)	Para usarlo	Destino (servidor)	Protocolo	Número de puerto
Escáner	Envío de correo electrónico (notificación por correo electrónico)	Servidor SMTP	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	POP antes de la conexión SMTP (notificación por correo electrónico)	Servidor POP	POP3 (TCP)	110
	Control de WSD	Ordenador cliente	WSD (TCP)	5357
	Para buscar el ordenador cuando escanea por botón de comando desde Document Capture Pro	Ordenador cliente	Exploración de escaneado por botón de comando de red	2968
Recopilación de la información del trabajo cuando escanea por botón de comando desde Document Capture Pro	Ordenador cliente	Escaneado por botón de comando de red	2968	
Ordenador cliente	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 datos de escaneado desde Document Capture Pro	Escáner	Escáner de red (TCP)	1865

Configuración de seguridad avanzada para Enterprise

En este capítulo, se describen las funciones de seguridad avanzada.

Configuración de seguridad y prevención de peligros

Cuando un dispositivo se conecta a una red, se puede acceder a él desde una ubicación remota. Además, muchas personas pueden compartir el dispositivo, 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 dispositivo en un entorno en el cual se puede acceder a Internet, los riesgos son aún mayores.

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

Configure el dispositivo 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
Comunicación SSL/TLS	La ruta de comunicación de un ordenador y un dispositivo se cifran mediante la comunicación SSL/TLS. El contenido de la comunicación enviada a través de un navegador está protegido.	Establezca en el dispositivo un certificado CA que esté firmado por una entidad certificadora.	Evite la fuga de información de configuración y de los contenidos de los datos transferidos al escáner desde el ordenador. El acceso al servidor de Epson en Internet desde el dispositivo también se puede proteger mediante el uso de una actualización de firmware, etc.
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 de escaneado no garantizado.	Cree una directiva básica y una directiva individual para establecer el cliente o el tipo de datos que pueden acceder al dispositivo.	Proteja el acceso no autorizado y la alteración e interceptación de datos de comunicación con el dispositivo.
SNMPv3	Se agregan funciones, tales como monitorización de dispositivos conectados en la red, integridad de los datos para el control del protocolo SNMP, cifrado, autenticación de usuario, etc.	Habilite SNMPv3, luego configure el método de cifrado y autenticación.	Asegure el cambio de configuración mediante la red, confidencialidad en monitorización de estado.
IEEE802.1X	Le permite conectarse solo a un usuario autenticado para Ethernet. Le permite usar el dispositivo solo a un usuario con permiso.	Configuración de autenticación para el servidor RADIUS (servidor de autenticación).	Proteja contra acceso y uso no autorizado del dispositivo.

Configuración de seguridad avanzada para Enterprise

Nombre	Tipo de función	Qué configurar	Qué evitar
Leer tarjeta de identificación	Puede usar el dispositivo si apunta una tarjeta de ID por encima del dispositivo autenticado que está conectado. Puede limitar la adquisición de registros para cada usuario y dispositivo y limitar el uso disponible de dispositivos y las funciones disponibles de cada usuario y grupo.	Conecte un dispositivo de autenticación en el dispositivo y luego configure la información de un usuario en el sistema de autenticación.	Evite el uso no autorizado y la suplantación del dispositivo.

Información relacionada

- ➔ [“Comunicación SSL/TLS con la impresora” de la página 63](#)
- ➔ [“Comunicación cifrada mediante el uso de filtro IPsec/IP” de la página 71](#)
- ➔ [“Modo de uso del protocolo SNMPv3” de la página 83](#)
- ➔ [“Conexión del escáner a una red IEEE802.1X” de la página 85](#)

Configuración de las funciones de seguridad

Cuando se configura el filtro IPsec/IP o IEEE802.1X, se recomienda acceder a Web Config mediante el uso de SSL/TLS para comunicar la información de configuración y reducir los riesgos de seguridad tales como alteración o interceptación.

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.

Acerca de la certificación digital

- Certificado firmado por una entidad certificadora (CA)

Debe solicitar a una CA (entidad certificadora) un certificado CA (firmado por entidad certificadora). Si utiliza un certificado firmado por entidad certificadora, puede garantizar la seguridad de las comunicaciones. Puede utilizar un certificado firmado por entidad certificadora para cada función de seguridad.

- Certificado CA (de entidad certificadora)

Un certificado CA (de entidad certificadora) indica que un tercero ha verificado la identidad de un servidor. Es un componente clave en la seguridad de toda red fiable. Debe obtener un certificado CA (de entidad certificadora) para la autenticación de servidores a una entidad certificadora que los expenda.

- Certificado autofirmado

Un certificado autofirmado es aquel que emite el escáner con su propia firma. Es un certificado no fiable y no puede evitar la suplantación de identidad. Si utiliza un certificado así para la certificación SSL/TLS, los navegadores a veces muestran una alerta de seguridad. Solamente puede usar este certificado para una comunicación SSL/TLS.

Configuración de seguridad avanzada para Enterprise

Información relacionada

- ➔ “Cómo obtener e importar un certificado firmado CA” de la página 64
- ➔ “Cómo eliminar un certificado firmado por entidad certificadora” de la página 67
- ➔ “Actualización de un certificado autofirmado” de la página 68

Cómo obtener e importar 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 por entidad certificadora a través de Web Config. Cuando se crea una CSR a través de Web Config, el certificado tiene el formato PEM/DER.

1. Acceda a Web Config y seleccione **Configuración de 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 **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 **Configuración de seguridad de red**. A continuación, seleccione **SSL/TLS > Certificado**, o bien **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

- ➔ “Acceso a Web Config” de la página 23
- ➔ “Ajustes de una CSR” de la página 65

Configuración de seguridad avanzada para Enterprise

➔ “Cómo importar un certificado firmado por entidad certificadora” de la página 66

Ajustes de una CSR

The screenshot shows the EPSON Web Config interface. On the left is a sidebar with navigation options: Administrator Logout, Status (Product Status, Network Status, Panel Snapshot, Maintenance, Hardware Status), Scanner Settings, Network Settings, Network Security Settings (SSL/TLS, Basic, Certificate, IPsec/IP Filtering, IEEE802.1X, CA Certificate), Services, System Settings, Export and Import Setting Value, and Administrator Settings. Under 'Basic Settings' are DNS/Proxy Setup, Firmware Update, Root Certificate Update, and Product Status. The main content area is titled 'Network Security Settings > SSL/TLS > Certificate' and contains the following fields:

- Key Length: [Input field]
- Common Name: [Input field]
- Organization: [Input field]
- Organizational Unit: [Input field]
- Locality: [Input field]
- State/Province: [Input field]
- Country: [Input field]

At the bottom of the form are 'OK' and 'Back' buttons.

Elementos	Ajustes y explicación
Longitud clave	Seleccione la longitud de la clave de la CSR.
Nombre común	Puede introducir entre 1 y 128 caracteres. Si es una dirección IP, tiene que ser estática. Por ejemplo: URL para acceder a Web Config: https://10.152.12.225 Nombre común: 10.152.12.225
Organización/ Unidad organizativa/ Localidad/ Estado/Provincia	Escriba entre 0 y 64 caracteres en ASCII (0x20–0x7E). Puede separar las palabras con comas.
País	Escriba el código numérico del país de dos cifras especificado por la ISO-3166.

Información relacionada

➔ “Cómo obtener un certificado firmado por entidad certificadora” de la página 64

Configuración de seguridad avanzada para Enterprise

Cómo importar un certificado firmado por entidad certificadora

! *Importante:*

- Confirme que la fecha y la hora del escáner estén bien configuradas.
- Si ha obtenido el certificado mediante una CSR (solicitud de firma de certificado) creada con Web Config, puede importarlo una vez.

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

2. Haga clic en **Importar**.

Se abrirá la página de importación de certificados.

3. Introduzca un valor para cada opción.

Las opciones de configuración varían según dónde haya creado la CSR y el formato de archivo del certificado. Tenga en cuenta lo siguiente cuando configure las opciones.

- Un certificado de formato PEM/DER obtenido a través de Web Config
 - Clave privada:** no hay que configurarlo porque el escáner cuenta con una clave privada.
 - Contraseña:** no configure esta opción.
 - Certificado CA 1/Certificado CA 2:** opcional
- Un certificado de formato PEM/DER obtenido a través de un ordenador
 - Clave privada:** es necesario configurarla.
 - Contraseña:** no configure esta opción.
 - Certificado CA 1/Certificado CA 2:** opcional
- Un certificado de formato PKCS#12 obtenido a través de un ordenador
 - Clave privada:** no configure esta opción.
 - Contraseña:** opcional
 - Certificado CA 1/Certificado CA 2:** no configure esta opción.

4. Haga clic en **Aceptar**.

Aparecerá un mensaje para confirmar que ha terminado.

Nota:

Haga clic en **Confirmar** para confirmar los datos del certificado.

Información relacionada

➔ [“Acceso a Web Config” de la página 23](#)

➔ [“Ajustes de la importación de certificados firmados CA” de la página 67](#)

Configuración de seguridad avanzada para Enterprise

Ajustes de la importación de certificados firmados CA

The screenshot shows the 'Certificate' configuration page under 'Network Security Settings > SSL/TLS'. The interface includes a left-hand navigation menu and a main configuration area. The main area contains fields for 'Server Certificate', 'Private Key', 'Password', 'CA Certificate 1', and 'CA Certificate 2', each with a 'Browse...' button. A note at the bottom states: 'Note: It is recommended to communicate via HTTPS for importing a certificate.' Below the note are 'OK' and 'Back' buttons.

Opciones	Ajustes y explicación
Certificado del servidor o Certificado del cliente	Seleccione un formato de certificado.
Clave privada	Si ha obtenido un certificado del formato PEM/DER mediante una CSR creada en un ordenador, especifique un archivo de clave privada que corresponda a un certificado.
Contraseña	Escriba una contraseña para codificar una clave privada.
Certificado CA 1	Si su certificado tiene el formato Certificado (PEM/DER) , importe un certificado de una autoridad que expenda certificados de servidor. Especifique un archivo si es necesario.
Certificado CA 2	Si su certificado tiene el formato Certificado (PEM/DER) , importe un certificado de una autoridad que expenda Certificado CA 1 . Especifique un archivo si es necesario.

Información relacionada

➔ [“Cómo importar un certificado firmado por entidad certificadora”](#) de la página 66

Cómo eliminar un certificado firmado por entidad certificadora

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

Configuración de seguridad avanzada para Enterprise



Importante:

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

1. Acceda a Web Config y, a continuación, seleccione **Configuración de 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

➔ [“Acceso a Web Config” de la página 23](#)

Actualización de un certificado autofirmado

Si el escáner es compatible con la función de servidor HTTPS, puede actualizar un certificado autofirmado. Si accede a Web Config con un certificado de firma propia, se mostrará un mensaje de advertencia.

Utilice un certificado autofirmado temporalmente hasta que obtenga e importe un certificado firmado por entidad certificadora.

1. Acceda a Web Config y seleccione **Configuración de seguridad de red > SSL/TLS > Certificado**.
2. Haga clic en **Actualizar**.
3. Introduzca **Nombre común**.

Introduzca una dirección IP o un identificador (un nombre FQDN, por ejemplo) para el escáner. Puede introducir entre 1 y 128 caracteres.

Nota:

Separe las palabras del nombre (CN) con comas.

Configuración de seguridad avanzada para Enterprise

4. Especifique el periodo de validez del certificado.

EPSON

Administrator Logout

- Status
 - Product Status
 - Network Status
 - Panel Snapshot
 - Maintenance
 - Hardware Status
- Scanner Settings
- Network Settings
- Network Security Settings
 - SSL/TLS
 - Basic
 - Certificate
 - IPsec/IP Filtering
 - IEEE802.1X
 - CA Certificate
- Services
- System Settings
- Export and Import Setting Value
- Administrator Settings

Basic Settings

- DNS/Proxy Setup
- Firmware Update
- Root Certificate Update
- Product Status

Network Security Settings > SSL/TLS > Certificate

Key Length :	2048
Common Name :	192.168.0.1
Organization :	SEIKO EPSON CORP.
Valid Date (UTC) :	2016-11-24 02:49:09 UTC
Certificate Validity (year) :	10

Next Back

5. Haga clic en **Siguiente**.
Aparecerá un mensaje de confirmación.
6. Haga clic en **Aceptar**.
Se actualizará el escáner.

Nota:

Haga clic en **Confirmar** para confirmar los datos del certificado.

Información relacionada

➔ [“Acceso a Web Config” de la página 23](#)

Configurar un Certificado CA

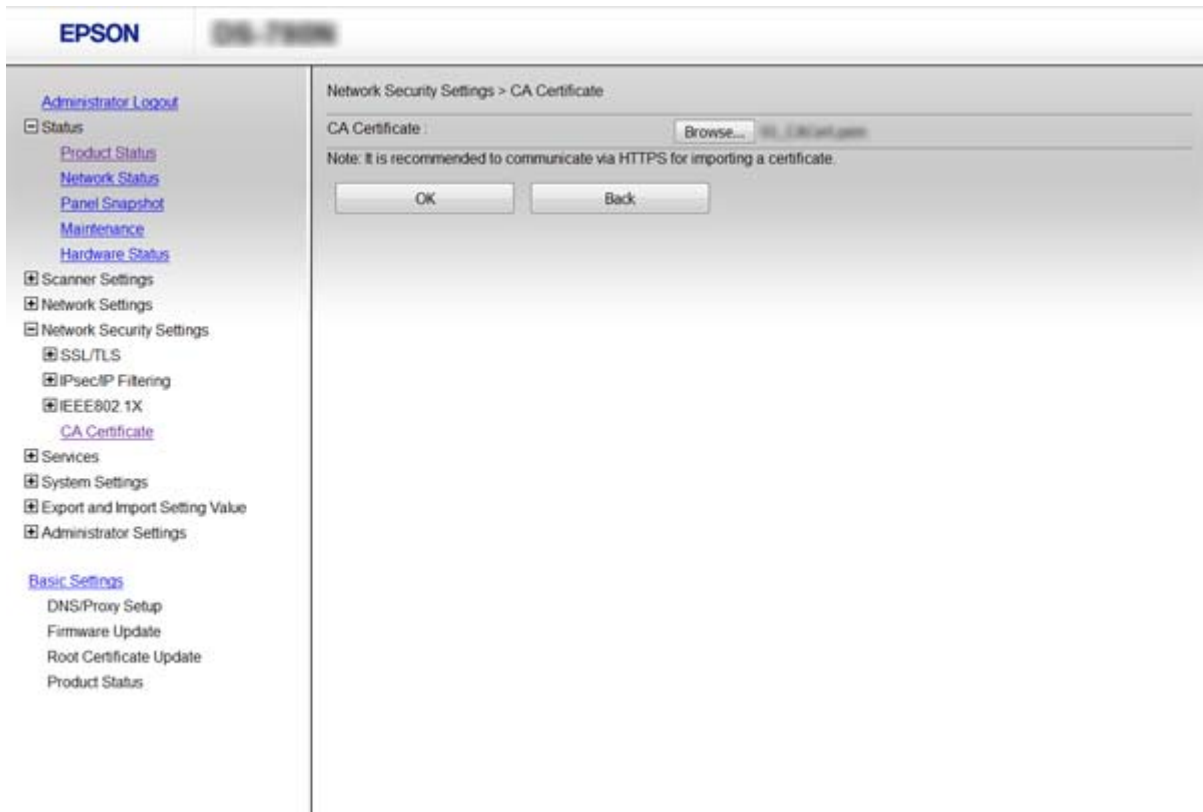
Puede importar, mostrar y eliminar un Certificado CA.

Cómo importar un Certificado CA

1. Acceda a Web Config y seleccione **Configuración de seguridad de red > Certificado CA**.
2. Haga clic en **Importar**.

Configuración de seguridad avanzada para Enterprise

3. Especifique el Certificado CA que desee importar.



4. Haga clic en **Aceptar**.

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

Información relacionada

➔ [“Acceso a Web Config” de la página 23](#)

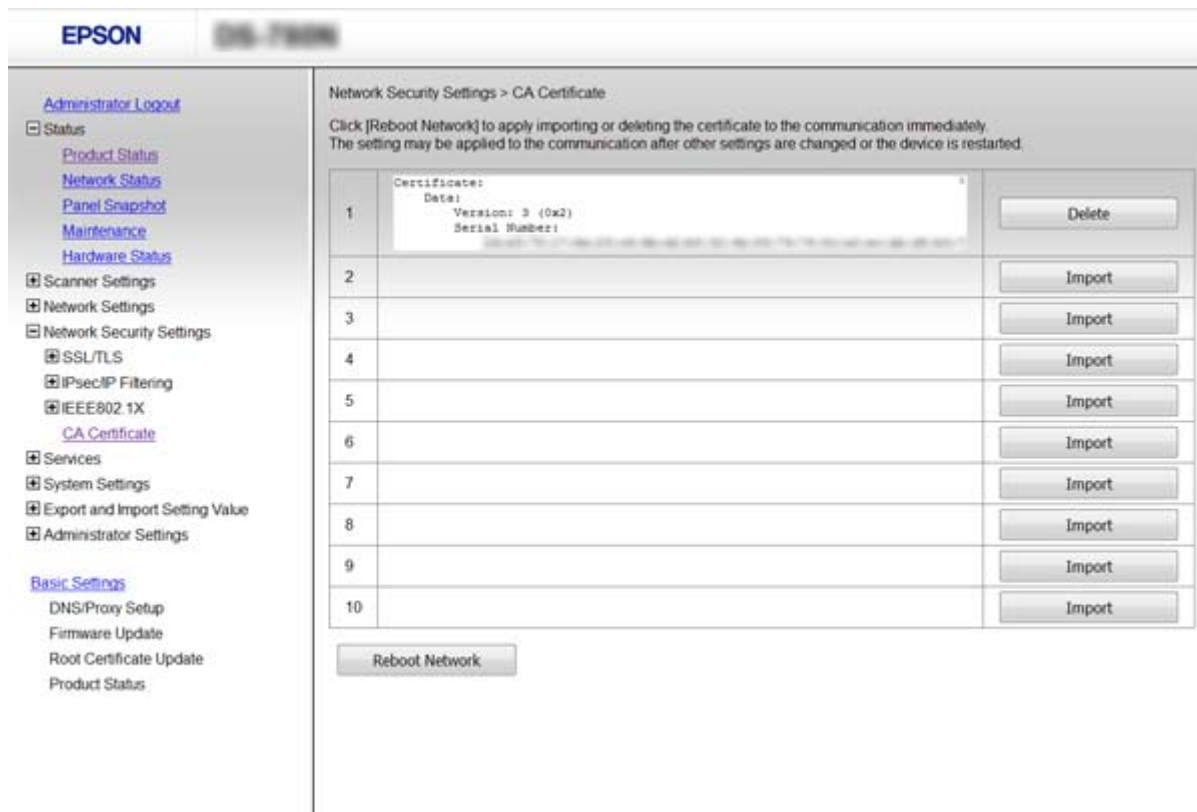
Cómo eliminar un Certificado CA

Puede eliminar el Certificado CA importado.

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

Configuración de seguridad avanzada para Enterprise

- Haga clic en **Eliminar** junto al Certificado CA que desee eliminar.



- Confirme que desea eliminar el certificado en el mensaje mostrado.

Información relacionada

➔ [“Acceso a Web Config” de la página 23](#)

Comunicación cifrada mediante el uso de filtro IPsec/IP

Acerca de IPsec/Filtrado de IP

Si el escáner cuenta con filtro de IPsec/IP, puede filtrar el tráfico en función de las direcciones IP, los servicios y el puerto. 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.

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. 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.

Nota:

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

Configuración de seguridad avanzada para Enterprise

Configuración de la Norma predeterminada

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

- ➔ “Acceso a Web Config” de la página 23
- ➔ “Configurar elementos de Norma predeterminada” de la página 72

Configurar elementos de Norma predeterminada

The screenshot shows the 'Basic' configuration page for IPsec Filtering. The interface includes a left-hand navigation menu with options like 'Administrator Logout', 'Status', 'Scanner Settings', 'Network Settings', 'Network Security Settings', 'SSL/TLS', 'IPsecIP Filtering', 'IEEE802.1X', 'Services', 'System Settings', 'Export and Import Setting Value', and 'Administrator Settings'. The main configuration area is titled 'Network Security Settings > IPsecIP Filtering > Basic' and contains the following settings:

- IPsecIP Filtering:** Enable Disable
- Default Policy:**
 - Access Control: IPsec
 - IKE Version: IKEv1 IKEv2
 - Authentication Method: Pre-Shared Key
 - Pre-Shared Key: [Text Field]
 - Confirm Pre-Shared Key: [Text Field]
 - Encapsulation: Transport Mode
 - Remote Gateway(Tunnel Mode): [Text Field]
 - Security Protocol: ESP
- Algorithm Settings:**
 - IKE:**
 - Encryption: Any
 - Authentication: Any
 - Key Exchange: Any
 - ESP:**
 - Encryption: Any
 - Authentication: Any

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

Configuración de seguridad avanzada para Enterprise

Elementos	Ajustes y explicación	
Control de acceso	Configure un método para controlar el tráfico de paquetes IP.	
	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	<p>Seleccione IKEv1 o IKEv2 para la versión IKE.</p> <p>Seleccione uno de ellos de acuerdo al dispositivo al que esté conectado el escáner.</p>	
IKEv1	Los siguientes elementos se muestran cuando selecciona IKEv1 en Versión IKE .	
	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 de entre 1 y 127 caracteres.
	Confirmar clave precompartida	Escriba otra vez la contraseña establecida para confirmarla.
IKEv2	Los siguientes elementos se muestran cuando selecciona IKEv2 en Versión IKE .	
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)	Seleccione el tipo de ID del escáner.
	Identificación (ID)	<p>Escriba el ID del escáner que coincida con el tipo de ID.</p> <p>No se puede utilizar "@", "#" ni "=" como primer carácter.</p> <p>Nombre distinguido: Escriba entre 1 y 128 caracteres ASCII de 1 byte (0x20 a 0x7E). Debe incluir "=".</p> <p>Dirección IP: Ingrese el formato IPv4 o IPv6.</p> <p>FQDN: Escriba una combinación de entre 1 y 255 caracteres. Los caracteres admitidos son A-Z, a-z, 0-9, "-" y punto (.).</p> <p>Dirección de correo: Escriba entre 1 y 128 caracteres ASCII de 1 byte (0x20 a 0x7E). Debe incluir "@".</p> <p>ID clave: Escriba entre 1 y 128 caracteres ASCII de 1 byte (0x20 a 0x7E).</p>
	Clave precompartida	Si selecciona Clave precompartida para Método de autenticación , introduzca una clave previamente compartida de entre 1 y 127 caracteres.
	Confirmar clave precompartida	Escriba otra vez la contraseña establecida para confirmarla.

Configuración de seguridad avanzada para Enterprise

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)	Seleccione el tipo de ID para el dispositivo que desea autenticar.
	Identificación (ID)	<p>Escriba el ID del escáner que coincida con el tipo de ID.</p> <p>No se puede utilizar “@”, “#” ni “=” como primer carácter.</p> <p>Nombre distinguido: Escriba entre 1 y 128 caracteres ASCII de 1 byte (0x20 a 0x7E). Debe incluir “=”.</p> <p>Dirección IP: Ingrese el formato IPv4 o IPv6.</p> <p>FQDN: Escriba una combinación de entre 1 y 255 caracteres. Los caracteres admitidos son A–Z, a–z, 0–9, “-” y punto (.).</p> <p>Dirección de correo: Escriba entre 1 y 128 caracteres ASCII de 1 byte (0x20 a 0x7E). Debe incluir “@”.</p> <p>ID clave: Escriba entre 1 y 128 caracteres ASCII de 1 byte (0x20 a 0x7E).</p>
	Clave precompartida	Si selecciona Clave precompartida para Método de autenticación , introduzca una clave previamente compartida de entre 1 y 127 caracteres.
	Confirmar clave precompartida	Escriba otra vez la contraseña establecida para confirmarla.
Encapsulamiento	Si selecciona IPsec como Control de acceso , tiene que configurar un modo de encapsulación.	
	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 como valor de ajuste de Encapsulamiento , introduzca una dirección de puerta de enlace que contenga entre 1 y 39 caracteres.	
Protocolo de seguridad	IPsec para Control de acceso , seleccione una opción.	
	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		
IKE	Cifrado	<p>Seleccione el algoritmo de cifrado de IKE.</p> <p>El elemento varía según la versión de IKE.</p>
	Autenticación	Seleccione el algoritmo de autenticación de IKE.
	Intercambio de clave	<p>Seleccione el algoritmo de intercambio de claves de IKE.</p> <p>El elemento varía según la versión de IKE.</p>

Configuración de seguridad avanzada para Enterprise

Elementos	Ajustes y explicación	
ESP	Cifrado	Seleccione el algoritmo de cifrado de ESP. Está disponible cuando se selecciona ESP para Protocolo de seguridad .
	Autenticación	Seleccione el algoritmo de autenticación de ESP. Está disponible cuando se selecciona ESP para Protocolo de seguridad .
AH	Autenticación	Seleccione el algoritmo de cifrado de AH. Está disponible cuando se selecciona AH para Protocolo de seguridad .

Información relacionada

➔ [“Configuración de la Norma predeterminada” de la página 72](#)

Configuración de la Norma de grupo

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

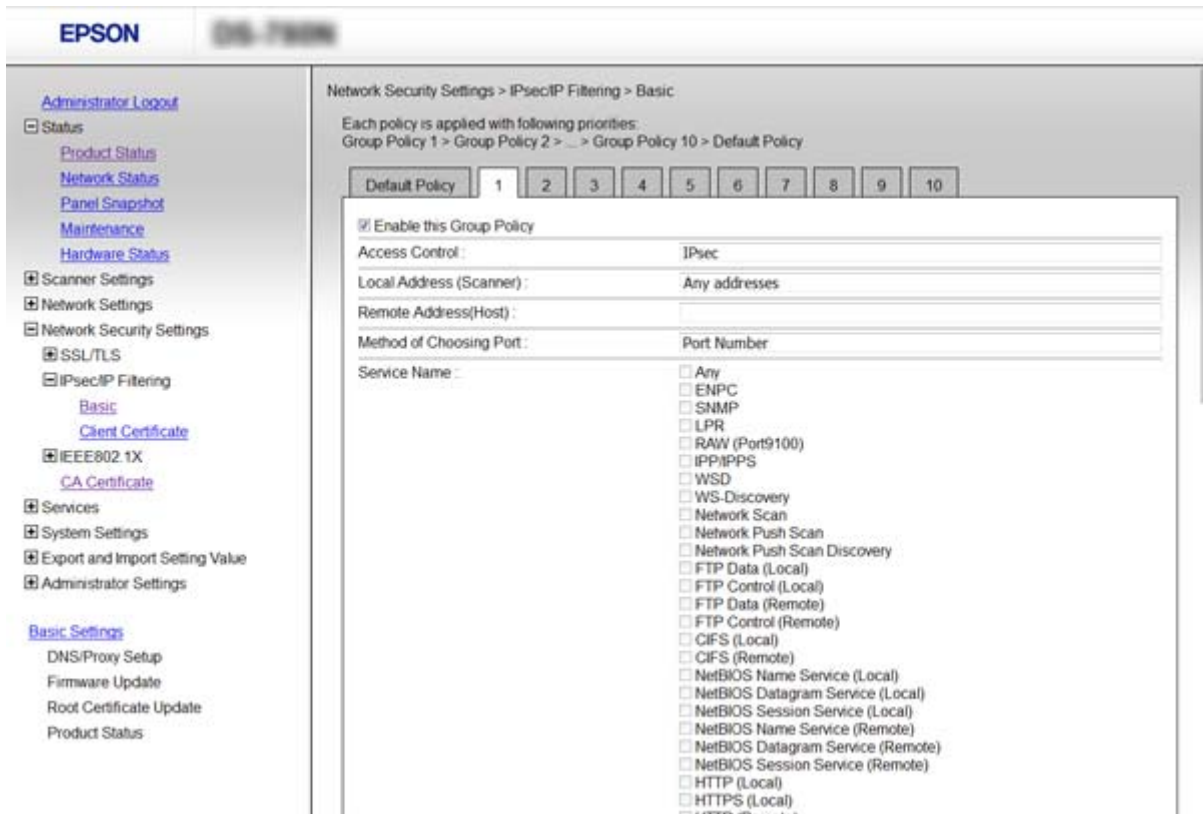
Información relacionada

➔ [“Acceso a Web Config” de la página 23](#)

➔ [“Configurar elementos de Norma de grupo” de la página 76](#)

Configuración de seguridad avanzada para Enterprise

Configurar elementos de Norma de grupo



Elementos	Ajustes y explicación	
Habilitar esta política de grupo	Puede habilitar o inhabilitar una directiva de grupo.	
Control de acceso	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 automáticamente una dirección IP, puede seleccionar Usar dirección IPv4 obtenida automáticamente .	
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.	

Configuración de seguridad avanzada para Enterprise

Elementos	Ajustes y explicación	
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.	
	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 TCP o UDP para Protocolo de transporte , introduzca 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 TCP o UDP para Protocolo de transporte , introduzca 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 la 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 .	
	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 de entre 1 y 127 caracteres.
	Confirmar clave precompartida	Escriba otra vez la contraseña establecida para confirmarla.
IKEv2	Los siguientes elementos se muestran cuando selecciona IKEv2 en Versión IKE .	

Configuración de seguridad avanzada para Enterprise

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)	Seleccione el tipo de ID del escáner.
	Identificación (ID)	<p>Escriba el ID del escáner que coincida con el tipo de ID.</p> <p>No se puede utilizar "@", "#" ni "=" como primer carácter.</p> <p>Nombre distinguido: Escriba entre 1 y 128 caracteres ASCII de 1 byte (0x20 a 0x7E). Debe incluir "=".</p> <p>Dirección IP: Ingrese el formato IPv4 o IPv6.</p> <p>FQDN: Escriba una combinación de entre 1 y 255 caracteres. Los caracteres admitidos son A-Z, a-z, 0-9, "-" y punto (.).</p> <p>Dirección de correo: Escriba entre 1 y 128 caracteres ASCII de 1 byte (0x20 a 0x7E). Debe incluir "@".</p> <p>ID clave: Escriba entre 1 y 128 caracteres ASCII de 1 byte (0x20 a 0x7E).</p>
	Clave precompartida	Si selecciona Clave precompartida para Método de autenticación , introduzca una clave previamente compartida de entre 1 y 127 caracteres.
	Confirmar clave precompartida	Escriba otra vez la contraseña 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)	Seleccione el tipo de ID para el dispositivo que desea autenticar.
	Identificación (ID)	<p>Escriba el ID del escáner que coincida con el tipo de ID.</p> <p>No se puede utilizar "@", "#" ni "=" como primer carácter.</p> <p>Nombre distinguido: Escriba entre 1 y 128 caracteres ASCII de 1 byte (0x20 a 0x7E). Debe incluir "=".</p> <p>Dirección IP: Ingrese el formato IPv4 o IPv6.</p> <p>FQDN: Escriba una combinación de entre 1 y 255 caracteres. Los caracteres admitidos son A-Z, a-z, 0-9, "-" y punto (.).</p> <p>Dirección de correo: Escriba entre 1 y 128 caracteres ASCII de 1 byte (0x20 a 0x7E). Debe incluir "@".</p> <p>ID clave: Escriba entre 1 y 128 caracteres ASCII de 1 byte (0x20 a 0x7E).</p>
	Clave precompartida	Si selecciona Clave precompartida para Método de autenticación , introduzca una clave previamente compartida de entre 1 y 127 caracteres.
	Confirmar clave precompartida	Escriba otra vez la contraseña establecida para confirmarla.

Configuración de seguridad avanzada para Enterprise

Elementos	Ajustes y explicación	
Encapsulamiento	Si selecciona IPsec como Control de acceso , tiene que configurar un modo de encapsulación.	
	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 como valor de ajuste de 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.	
	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		
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. Está disponible cuando se selecciona ESP para Protocolo de seguridad .
	Autenticación	Seleccione el algoritmo de autenticación de ESP. Está disponible cuando se selecciona ESP para Protocolo de seguridad .
AH	Autenticación	Seleccione el algoritmo de autenticación de AH. Está disponible cuando se selecciona AH para Protocolo de seguridad .

Información relacionada

- ➔ [“Configuración de la Norma de grupo” de la página 75](#)
- ➔ [“Combinación de Dirección local\(escáner\) y Dirección remota\(host\) en Norma de grupo” de la página 80](#)
- ➔ [“Referencias del nombre del servicio en la directiva de grupo” de la página 80](#)

Configuración de seguridad avanzada para Enterprise

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.

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 EpsonNet Config y el controlador del escáner
SNMP	UDP	161	Cualquier puerto	Adquisición y configuración de MIB desde aplicaciones como EpsonNet Config y el controlador del escáner Epson
WSD	TCP	Cualquier puerto	5357	Control de WSD
WS-Discovery	UDP	3702	Cualquier puerto	Búsqueda de un escáner desde WSD
Network Scan	TCP	1865	Cualquier puerto	Reenvío de datos de escaneado desde Document Capture Pro
Network Push Scan Discovery	UDP	2968	Cualquier puerto	Búsqueda de un ordenador desde el escáner.
Network Push Scan	TCP	Cualquier puerto	2968	Adquisición de la información de trabajos de escaneado por botón de comando desde Document Capture Pro o Document Capture
HTTP (local)	TCP	80	Cualquier puerto	Servidor HTTP(S) (reenvío de datos de Web Config y WSD)
HTTPS (local)	TCP	443	Cualquier puerto	

Configuración de seguridad avanzada para Enterprise

Nombre del servicio	Tipo de protocolo	Número de puerto local	Número de puerto remoto	Funciones controladas
HTTP (remoto)	TCP	Cualquier puerto	80	Cliente HTTP(S) (comunicación entre actualización del firmware y actualización de certificado raíz)
HTTPS (remoto)	TCP	Cualquier puerto	443	

Ejemplos de configuración de IPsec/Filtrado de IP

Recepción de paquetes IPsec solamente

En este ejemplo solo se configura una directiva 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 configure esta opción.

Aceptar el escaneo mediante Epson Scan 2 y la configuración del escáner

Este ejemplo permite la comunicación de datos de escaneo y ajustes del escáner desde determinados servicios.

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, Network Scan, HTTP (local) y de HTTPS (local).

Recepción de acceso únicamente desde una dirección IP determinada

En este ejemplo se muestra cómo permitir el acceso al escáner a una dirección IP determinada.

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 del cliente de un administrador

Configuración de seguridad avanzada para Enterprise

Nota:

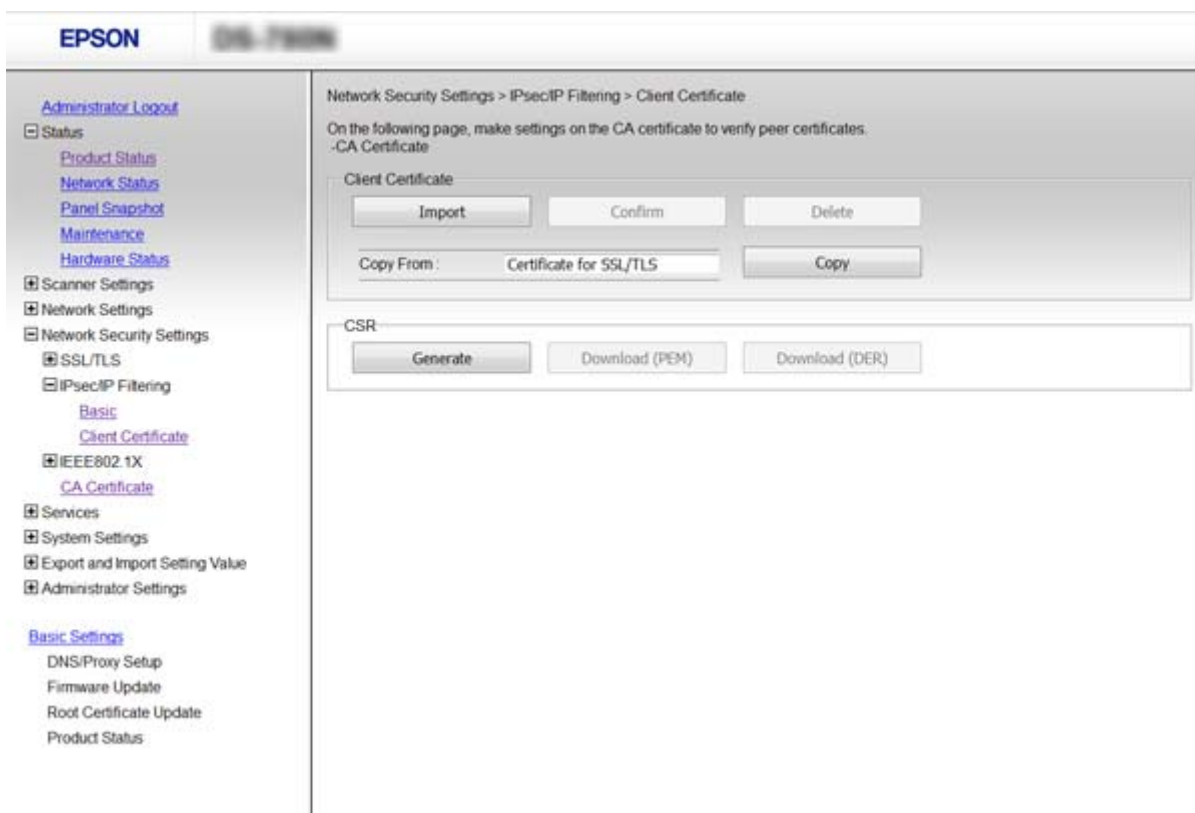
Independientemente de la configuración de las directivas, el cliente siempre podrá acceder y configurar el escáner.

Configuración de un certificado para IPsec/Filtrado de IP

Configure el certificado de cliente para el filtro de IPsec/IP. Si desea configurar la entidad certificadora, vaya a **Certificado CA**.

1. Acceda a Web Config y seleccione **Configuración de seguridad de red > IPsec/Filtrado de IP > Certificado del cliente**.
2. Importe el certificado en **Certificado del cliente**.

Si ya tiene importado un certificado publicado por una entidad certificadora en IEEE802.1X o SSL/TLS, puede copiar dicho certificado y utilizarlo en el filtro de IPsec/IP. Para copiar, seleccione el certificado desde **Copiar desde** y, a continuación, haga clic en **Copiar**.



Información relacionada

- ➔ “Acceso a Web Config” de la página 23
- ➔ “Cómo obtener e importar un certificado firmado CA” de la página 64

Modo de uso del protocolo SNMPv3

Acerca de SNMPv3

SNMP es un protocolo que se encarga de la monitorización y el control para recopilar información de los dispositivos que se encuentran conectados a la red. SNMPv3 es la versión de la función de seguridad de gestión que ha sido mejorada.

Cuando se utiliza SNMPv3, se pueden autenticar y cifrar la monitorización de estado y los cambios de configuración de la comunicación SNMP (paquete) para proteger la comunicación SNMP (paquete) de los riesgos de la red, tales como las escuchas telefónicas, la falsificación de identidad y la alteración.

Configuración de SNMPv3

Puede supervisar y controlar los accesos al escáner si éste admite el protocolo SNMPv3.

1. Acceda a Web Config y seleccione **Servicios > Protocolo**.
2. Escriba un valor para cada opción de los **Configuración de SNMPv3**.
3. Haga clic en **Siguiente**.
Aparecerá un mensaje de confirmación.
4. Haga clic en **Aceptar**.
Se actualizará el escáner.

Información relacionada

- ➔ [“Acceso a Web Config” de la página 23](#)
- ➔ [“Opciones de ajuste de SNMPv3” de la página 84](#)

Configuración de seguridad avanzada para Enterprise

Opciones de ajuste de SNMPv3

Opciones	Ajustes y explicación
Activar SNMPv3	Si la casilla está marcada, SNMPv3 está activado.
Nombre de usuario	Escriba de 1 a 32 caracteres de 1 byte.
Configuración de autenticación	
Algoritmo	Seleccione un algoritmo para una autenticación.
Contraseña	Escriba de 8 a 32 caracteres ASCII (0x20-0x7E).
Confirmar contraseña	Escriba la contraseña que ha configurado para confirmarla.
Configuración de cifrado	
Algoritmo	Seleccione un algoritmo para una codificación.
Contraseña	Escriba de 8 a 32 caracteres ASCII (0x20-0x7E).
Confirmar contraseña	Escriba la contraseña que ha configurado para confirmarla.
Nombre de contexto	Escriba de 1 a 32 caracteres de 1 byte.

Información relacionada

➔ [“Configuración de SNMPv3” de la página 83](#)

Conexión del escáner a una red IEEE802.1X

Configuración de una red IEEE802.1X

Si el escáner es compatible con IEEE802.1X, puede utilizarlo en una red con autenticación que esté conectada a un servidor RADIUS y a un concentrador que actúe como autenticador.

1. Acceda a Web Config y seleccione **Configuración de seguridad de red > IEEE802.1X > 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

- ➔ [“Acceso a Web Config” de la página 23](#)
- ➔ [“Opciones de ajuste de las redes IEEE802.1X” de la página 85](#)
- ➔ [“No se puede acceder a la impresora o al escáner tras configurar IEEE802.1X” de la página 90](#)

Opciones de ajuste de las redes IEEE802.1X

The screenshot shows the Epson Web Config interface for configuring IEEE802.1X settings. The left sidebar contains a navigation menu with options like Administrator Logout, Status, Product Status, Network Status, Panel Snapshot, Maintenance, Hardware Status, Scanner Settings, Network Settings, Network Security Settings, SSL/TLS, IPsec/IP Filtering, IEEE802.1X (selected), Basic, Client Certificate, CA Certificate, Services, System Settings, Export and Import Setting Value, and Administrator Settings. Under IEEE802.1X, the 'Basic' option is selected.

The main content area is titled 'Network Security Settings > IEEE802.1X > Basic'. It contains the following configuration options:

- IEEE802.1X (Wired LAN): Enable Disable
- EAP Type: EAP-TLS
- User ID: [Text Input Field]
- Password: [Text Input Field]
- Confirm Password: [Text Input Field]
- Server ID: [Text Input Field]
- Certificate Validation: Enable Disable
- Anonymous Name: [Text Input Field]
- Encryption Strength: Middle

A 'Next' button is located at the bottom of the configuration area.

Configuración de seguridad avanzada para Enterprise

Elementos	Ajustes y explicación	
IEEE802.1X (LAN cableada)	Puede activar o desactivar la configuración de la página (IEEE802.1X > Básica) para IEEE802.1X (LAN cableada).	
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.	
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).	
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 de RADIUS, puede escribir hasta 127 caracteres.	
Confirmar contraseña	Escriba otra vez la contraseña establecida para confirmarla.	
ID del servidor	Puede configurar un ID de servidor para autenticar con un servidor de determinado RADIUS. 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 Método de autenticación , 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

Información relacionada

➔ [“Configuración de una red IEEE802.1X” de la página 85](#)

Configuración de un certificado para IEEE802.1X

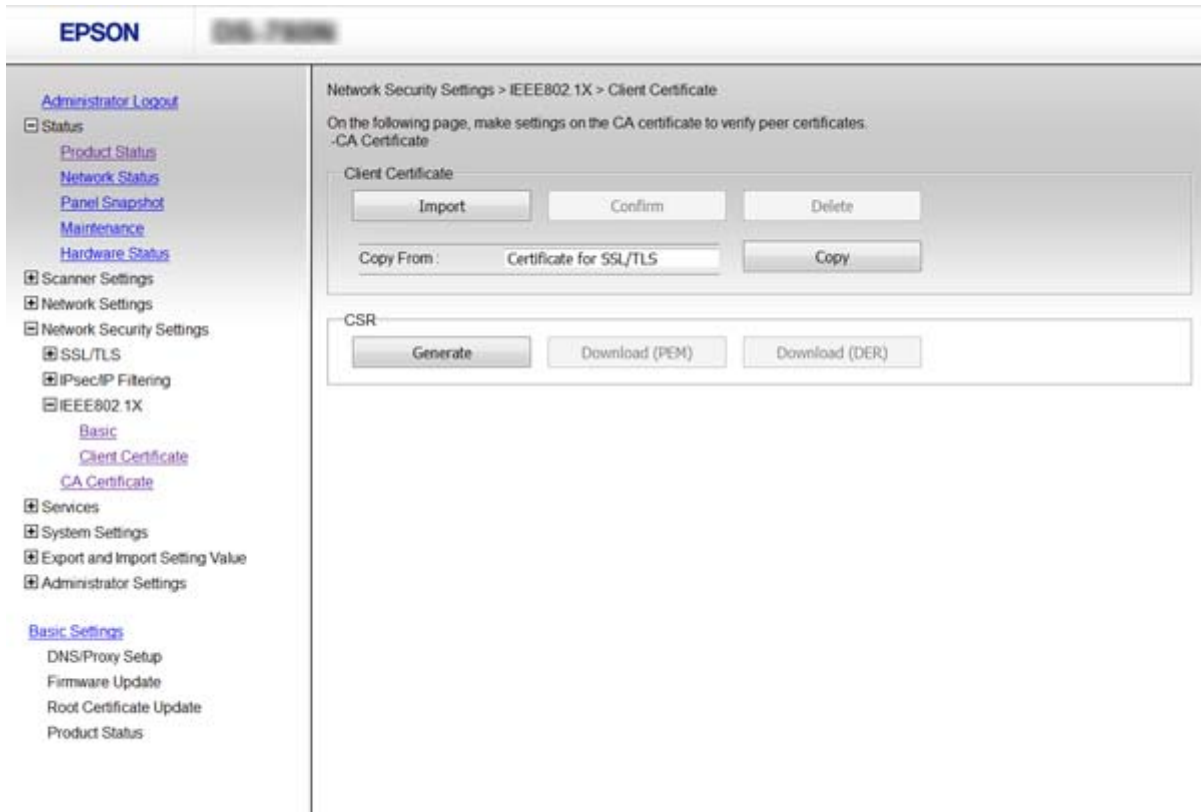
Configure el certificado de cliente para IEEE802.1X. Si desea configurar el certificado de entidad certificadora, vaya a **Certificado CA**.

1. Acceda a Web Config y seleccione **Configuración de seguridad de red > IEEE802.1X > Certificado del cliente**.

Configuración de seguridad avanzada para Enterprise

2. Introduzca un certificado en **Certificado del cliente**.

Puede copiar el certificado si lo ha publicado una entidad certificadora. Para copiar, seleccione el certificado desde **Copiar desde** y, a continuación, haga clic en **Copiar**.



Información relacionada

- ➔ [“Acceso a Web Config” de la página 23](#)
- ➔ [“Cómo obtener e importar un certificado firmado CA” de la página 64](#)

Solución de problemas de seguridad avanzada

Restauración de la configuración de seguridad

Cuando establece entorno de alta seguridad tal como un filtro IPsec/IP o IEEE802.1X, 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.

Desactivación de la función de seguridad mediante el uso del panel de control

Puede desactivar el filtro IPsec/IP o IEEE802.1X mediante el uso del panel de control del escáner.

1. Pulse **Configuración > Configuración de red**.

Configuración de seguridad avanzada para Enterprise

2. Pulse **Cambiar configuración**.
3. Pulse los elementos que desee desactivar.
 - IPsec/Filtrado de IP**
 - IEEE802.1X**
4. Cuando se muestre un mensaje de finalización, pulse **Proceder**.

Restauración de la función de seguridad mediante el uso de Web Config

Con IEEE802.1X, es posible que no se reconozcan los dispositivos en la red. En ese caso, desactive la función desde el panel de control del escáner.

Con filtro IPsec/IP, puede desactivar la función si puede acceder el dispositivo desde el ordenador.

Desactivación del filtro IPsec/IP mediante Web Config

1. Acceda a Web Config y seleccione **Configuración de seguridad de red > IPsec/Filtrado de IP > Básica**.
2. Seleccione **Desactivar** para **IPsec/Filtrado de IP** en **Norma predeterminada**.
3. Haga clic en **Siguiente** y a continuación anule la selección de **Habilitar esta política de grupo** para todas las directivas de grupo.
4. Haga clic en **Aceptar**.

Información relacionada

➔ [“Acceso a Web Config” de la página 23](#)

Problemas en el uso de funciones de seguridad de red

He olvidado una clave previamente compartida

Configure la clave nuevamente con Web Config.

Para cambiar la clave, acceda a Web Config y seleccione **Configuración de 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

➔ [“Acceso a Web Config” de la página 23](#)

Configuración de seguridad avanzada para Enterprise

La comunicación mediante IPsec no funciona

¿Utiliza un algoritmo incompatible en la configuración del ordenador?

El escáner admite los siguientes algoritmos.

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	Grupo DH 1, Grupo DH 2, Grupo DH 5, Grupo DH 14, Grupo DH 15, Grupo DH 16, Grupo DH 17, Grupo DH 18, Grupo DH 19, Grupo DH 20, Grupo DH 21, Grupo DH 22, Grupo DH 23, Grupo DH 24, Grupo DH 25, Grupo DH 26, Grupo DH 27*, Grupo DH 28*, Grupo DH 29*, Grupo DH 30*
Algoritmo de cifrado de ESP	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
Algoritmo de autenticación de ESP	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Algoritmo de autenticación de 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 71](#)

He perdido la comunicación de repente

¿Ha cambiado la dirección IP del escáner o no es válida?

Desactive IPsec con el panel de control del escáner.

Si el DHCP no está actualizado, al reiniciar, o si la dirección IPv6 está obsoleta o no se ha obtenido, es posible que no se encuentre la dirección IP registrada para el Web Config del escáner (**Configuración de seguridad de red > IPsec/Filtrado de IP > Básica > Norma de grupo > Dirección local(escáner)**).

Utilice una dirección IP fija.

¿Ha cambiado o no es válida la dirección IP del ordenador?

Desactive IPsec con el panel de control del escáner.

Si el DHCP no está actualizado, al reiniciar, o si la dirección IPv6 está obsoleta o no se ha obtenido, es posible que no se encuentre la dirección IP registrada para el Web Config del escáner (**Configuración de seguridad de red > IPsec/Filtrado de IP > Básica > Norma de grupo > Dirección remota(host)**).

Utilice una dirección IP fija.

Información relacionada

➔ [“Acceso a Web Config” de la página 23](#)

➔ [“Comunicación cifrada mediante el uso de filtro IPsec/IP” de la página 71](#)

Configuración de seguridad avanzada para Enterprise

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

El valor establecido puede ser incorrecto.

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 71](#)

No se puede acceder a la impresora o al escáner tras configurar IEEE802.1X

Es posible que la configuración sea incorrecta.

Deshabilite IEEE802.1X desde el panel de control del escáner. Conecte el escáner y un ordenador y, a continuación, vuelva a configurar IEEE802.1X.

Información relacionada

➔ [“Configuración de una red IEEE802.1X” de la página 85](#)

Problemas de uso de un certificado digital

No puedo importar un certificado firmado por entidad certificadora

¿El certificado firmado por entidad certificadora coincide con los datos de la CSR?

Si el certificado firmado por entidad certificadora 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 por entidad certificadora pesa más de 5 KB?

No se pueden importar certificados firmados por entidad certificadora de más de 5 KB.

¿La contraseña para importar el certificado es la correcta?

Si ha olvidado la contraseña, no podrá importar el certificado.

Información relacionada

➔ [“Cómo importar un certificado firmado por entidad certificadora” de la página 66](#)

No puedo actualizar un certificado de firma digital

¿Ha escrito el Nombre común?

Tiene que escribir el **Nombre común**.

¿Ha escrito caracteres no admitidos en el Nombre común? Los caracteres japoneses, por ejemplo, no se admiten.

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

¿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 68](#)

No puedo crear una CSR

¿Ha escrito el Nombre común?

Tiene que escribir el **Nombre común**.

¿Ha escrito caracteres no admitidos en Nombre común, Organización, Unidad organizativa, Localidad, Estado/Provincia? Los caracteres japoneses, por ejemplo, no se admiten.

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

¿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 64](#)

Aparece una advertencia relativa a un certificado digital

Mensajes	Causa/Qué hacer
Introduzca un certificado de servidor.	<p>Causa: No ha seleccionado ningún archivo para importarlo.</p> <p>Qué hacer: Seleccione un archivo y haga clic en Importar.</p>

Configuración de seguridad avanzada para Enterprise

Mensajes	Causa/Qué hacer
No se ha introducido el Certificado CA 1.	<p>Causa: No ha introducido el certificado de entidad certificadora 1, solamente el certificado de entidad certificadora 2.</p> <p>Qué hacer: Importe primero el certificado de entidad certificadora 1.</p>
Valor no válido a continuación.	<p>Causa: La ruta o la contraseña del archivo contienen caracteres no admitidos.</p> <p>Qué hacer: Compruebe que haya escrito los caracteres correctos para ese elemento.</p>
Fecha y hora no válidas.	<p>Causa: El escáner no tiene configurada la hora ni la fecha.</p> <p>Qué hacer: Configure la fecha y la hora con Web Config o con EpsonNet Config.</p>
Contraseña no válida.	<p>Causa: La contraseña configurada para el certificado de entidad certificadora no coincide con la contraseña que ha escrito.</p> <p>Qué hacer: Escriba la contraseña correcta.</p>
Archivo no válido.	<p>Causa: El archivo del certificado que quiere importar no tiene el formato X509.</p> <p>Qué hacer: Seleccione el certificado correcto enviado por una entidad certificadora de confianza.</p>
	<p>Causa: El archivo que ha importado es demasiado grande. Se admiten archivos de 5 KB como máximo.</p> <p>Qué hacer: Si ha seleccionado el archivo correcto, es posible que el certificado esté dañado o que sea falso.</p>
	<p>Causa: La cadena que contiene el certificado no es válida.</p> <p>Qué hacer: Encontrará más información sobre el certificado en el sitio web de la entidad certificadora.</p>
No se pueden usar los certificados de servidor que incluyen más de tres certificados CA.	<p>Causa: El archivo del certificado de formato PKCS#12 contiene más de 3 certificados de entidad certificadora.</p> <p>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.</p>

Configuración de seguridad avanzada para Enterprise

Mensajes	Causa/Qué hacer
El certificado ha expirado. Compruebe si el certificado es válido, o bien, la Fecha y hora del producto.	<p>Causa: El certificado ha caducado.</p> <p>Qué hacer:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Si el certificado ha caducado, obtenga uno nuevo e impórtelo. <input type="checkbox"/> 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.	<p>Causa: No hay ninguna clave privada emparejada con el certificado.</p> <p>Qué hacer:</p> <ul style="list-style-type: none"> <input type="checkbox"/> 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. <input type="checkbox"/> 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.
	<p>Causa: Ha reimportado el certificado PEM/DER obtenido a partir de una CSR con Web Config.</p> <p>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.</p>
La configuración ha fallado.	<p>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.</p> <p>Qué hacer: Después de revisar el archivo especificado y la comunicación, vuelva a importar el archivo.</p>

Información relacionada

➔ [“Acerca de la certificación digital” de la página 63](#)

He borrado un certificado firmado CA sin querer**¿Hay alguna copia de seguridad del certificado?**

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

➔ [“Cómo eliminar un certificado firmado por entidad certificadora” de la página 67](#)

➔ [“Cómo importar un certificado firmado por entidad certificadora” de la página 66](#)