EPSON
EXCEED YOUR VISION

Administratorhandbuch

NPD5668-00 DE

Inhalt

Anhang

Erweiterte Sicherheitseinstellungen für Unternehmen

Copyright

Markennachweis

- ❏ EPSON® ist eine eingetragene Marke und EPSON EXCEED YOUR VISION oder EXCEED YOUR VISION ist eine Marke der 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.
- ❏ Allgemeiner Hinweis: Andere hierin genannte Produktnamen dienen lediglich der Identifizierung und können Marken ihrer jeweiligen Eigentümer sein. Epson hat keinerlei Rechte an diesen Marken.

Über dieses Handbuch

Markierungen und Symbole

> ⚠ ***Achtung:***
> *Hinweise, die unbedingt beachtet werden müssen, um Körperverletzungen zu vermeiden.*

> ***Wichtig:***
> *Hinweise, die beachtet werden müssen, um Schäden am Gerät zu vermeiden.*

Hinweis:
Hinweise mit nützlichen Tipps zu Betrieb und Einsatzmöglichkeiten des Scanners.

Zugehörige Informationen

➡ Wenn Sie auf dieses Symbol klicken, werden verwandte Informationen aufgerufen.

In diesem Handbuch verwendete Beschreibungen

❏ Die Bildschirmdarstellungen des Scannertreibers und des Scannertreibers Epson Scan 2 stammen aus Windows 10 oder OS X El Capitan. Der Inhalt der Bildschirmdarstellungen hängt vom Modell und von der Situation ab.

❏ Die in diesem Handbuch verwendeten Abbildungen sind lediglich Beispiele. Auch wenn es von Modell zu Modell leichte Abweichungen geben kann, liegt allen das gleiche Funktionsprinzip zugrunde.

❏ Welche Menüpunkte im LCD-Bildschirm verfügbar sind, hängt vom Modell und den Einstellungen ab.

Betriebssysteme

Windows

In diesem Handbuch beziehen sich Begriffe wie „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“, und „Windows Server 2003“ auf die folgenden Betriebssysteme. Darüber hinaus bezieht sich der Begriff „Windows“ auf alle Windows-Versionen.

❏ Betriebssystem Microsoft® Windows® 10

❏ Betriebssystem Microsoft® Windows® 8.1

❏ Betriebssystem Microsoft® Windows® 8

❏ Betriebssystem Microsoft® Windows® 7

❏ Betriebssystem Microsoft® Windows Vista®

❏ Betriebssystem Microsoft® Windows® XP

❏ Betriebssystem Microsoft® Windows® XP Professional x64 Edition

- ❏ Betriebssystem Microsoft® Windows Server® 2016
- ❏ Betriebssystem Microsoft® Windows Server® 2012 R2
- ❏ Betriebssystem Microsoft® Windows Server® 2012
- ❏ Betriebssystem Microsoft® Windows Server® 2008 R2
- ❏ Betriebssystem Microsoft® Windows Server® 2008
- ❏ Betriebssystem Microsoft® Windows Server® 2003 R2
- ❏ Betriebssystem Microsoft® Windows Server® 2003

Mac OS

In diesem Handbuch bezieht sich „Mac OS“ auf macOS Sierra, OS X El Capitan, OS X Yosemite, OS X Mavericks, OS X Mountain Lion, Mac OS X v10.7.x und Mac OS X v10.6.8.

Einleitung

Manuelle Komponente

Dieses Handbuch dient dem Geräteadministrator, der für das Verbinden des Druckers oder Scanners mit dem Netzwerk zuständig ist, und es enthält Informationen zu den verfügbaren Funktionen und Einstellungen.

Informationen zur Nutzung der Funktionen finden Sie im *Benutzerhandbuch*.

Vorbereitung

Erläutert Aufgaben des Administrators, das Einrichten von Geräten sowie die Verwaltungssoftware.

Verbindung

Erläutert das Anschließen des Geräts ans Netzwerk oder an die Telefonleitung. Erläutert auch die Netzwerkumgebung, beispielsweise die Nutzung eines Ports für das Gerät, das DNS und die Proxyserver-Angabe.

Funktionseinstellungen

Erläutert die Einstellungen der einzelnen Gerätefunktionen.

Einfache Sicherheitseinstellungen

Beschreibt die Einstellungen der einzelnen Funktionen wie Drucken, Scannen und Faxen.

Betriebs- und Verwaltungseinstellungen

Beschreibt die Vorgänge nach Aufnahme der Gerätenutzung, beispielsweise das Überprüfen von Daten, sowie Wartungsaufgaben.

Problemlösung

Erläutert das Initialisieren von Einstellungen, sowie die Fehlerbehebung des Netzwerks.

Erweiterte Sicherheitseinstellungen für Unternehmen

Beschreibt Einstellungsmethoden, mit denen die Gerätesicherheit verbessert werden kann, beispielsweise die Nutzung eines CA-Zertifikats, der SSL/TLS-Kommunikation und der IPsec/IP-Filterung.

Je nach Modell werden einige Funktionen in diesem Kapitel nicht unterstützt.

Definitionen von Begriffen in diesem Handbuch

Die folgenden Begriffe werden in diesem Handbuch verwendet.

Administrator

Die Person, die für die Installation und Einrichtung des Geräts oder des Netzwerks in einem Büro oder einer Organisation zuständig ist. Für kleine Organisationen kann dieselbe Person sowohl für die Geräte- als auch für die Netzwerkverwaltung zuständig sein. In großen Organisationen haben Administratoren Autorität über das Netzwerk oder die Geräte einer Gruppe, der Abteilung oder anderen Geschäftseinheit, und

Einleitung

Netzwerkadministratoren sind zuständig für die Kommunikationseinstellungen außerhalb der Organisation, beispielsweise für das Internet.

Netzwerkadministrator

Die Person, die für die Kontrolle der Netzwerkkommunikation zuständig ist. Die Person, die Router, Proxyserver, DNS-Server und Mailserver einrichtet, um die Kommunikation mit dem Internet oder dem Netzwerk zu ermöglichen.

Benutzer

Die Person, die Geräte wie z. B. Drucker oder Scanner verwendet.

Web Config (Webseite des Geräts)

Der in das Gerät eingebaute Web-Server. Der Server heißt Web Config. Mit dem Browser kann der Gerätezustand geprüft und verändert werden.

Tool

Ein Sammelbegriff für Software zur Einrichtung oder Verwaltung eines Geräts, z. B. Epson Device Admin, EpsonNet Config, EpsonNet SetupManager usw.

Push-Scan

Eine Bezeichnung für das Scannen vom Bedienfeld des Geräts.

ASCII (American Standard Code for Information Interchange)

Einer der Standard-Zeichencodes. Darin sind 128 Zeichen definiert, einschließlich der Buchstaben des Alphabets (a–z, A–Z), arabischer Ziffern (0–9), Symbole, Leerzeichen und Steuerzeichen. When in diesem Handbuch von „ASCII“ die Rede ist, sind die folgenden Zeichen 0x20–0x7E (Hexzahlen) gemeint, ohne die Steuerzeichen.

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	{	|	}	~	

* Leerzeichen.

Unicode (UTF-8)

Ein internationaler Standardcode, der die meisten wichtigen Sprachen weltweit abbildet. Wenn in diesem Handbuch von „UTF-8“ die Rede ist, sind Zeichen gemeint, die im UTF-8-Format kodiert sind.

Vorbereitung

In diesem Kapitel wird die Rolle des Administrators und der Vorbereitung der Einstellungen erläutert.

Pflege und Verwaltung der Scannereinstellungen

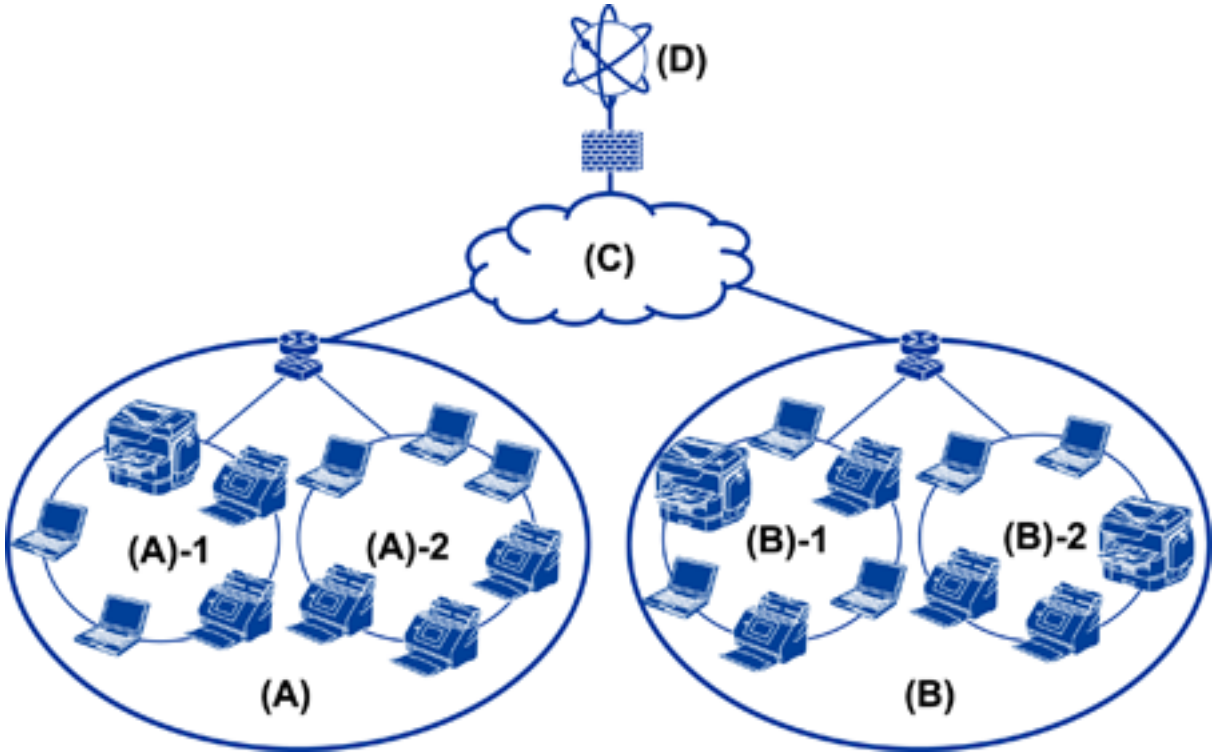
Der Administrator übernimmt das Einrichten der Netzwerkverbindung, die Ersteinrichtung und die Wartung des Scanners, damit diese dem Benutzer zur Verfügung stehen.

1. Vorbereiten
   - ❏ Erfassen der Einstellungen für die Verbindung
   - ❏ Entscheiden für eine Verbindungsmethode
2. Verbinden
   - ❏ Netzwerkverbindung über das Scannerbedienfeld
3. Einrichten der Funktionen
   - ❏ Scannertreibereinstellungen
   - ❏ Sonstige erweiterte Einstellungen
4. Sicherheitseinstellungen
   - ❏ Administratoreinstellungen
   - ❏ SSL/TLS
   - ❏ Protokollsteuerung
   - ❏ Erweiterte Sicherheitseinstellungen (optional)
5. Betrieb und Verwaltung
   - ❏ Prüfen des Gerätezustands
   - ❏ Umgang mit Notfall-Events
   - ❏ Sichern der Geräteeinstellungen

Zugehörige Informationen

➡ „Vorbereitung“ auf Seite 10
➡ „Verbindung“ auf Seite 15
➡ „Funktionseinstellungen“ auf Seite 22
➡ „Einfache Sicherheitseinstellungen“ auf Seite 32
➡ „Betriebs- und Verwaltungseinstellungen“ auf Seite 40

Beispiel einer Netzwerkumgebung



(A) Büro 1

❏ (A) – 1: LAN 1

❏ (A) – 2: LAN 2

(B) Büro 2

❏ (B) – 1: LAN 1

❏ (B) – 2: LAN 2

(C) WAN

(D) Internet

Einstellungsbeispiel für die Scannerverbindung

Je nach Nutzungsweise des Scanners gibt es hauptsächlich zwei Verbindungstypen. Bei beiden wird der Scanner über einen Hub mit dem Netzwerk und dem Computer verbunden.

❏ Client-/Server-Verbindung (Scanner verwendet Windows-Server, Auftragsverwaltung)

❏ Peer-to-peer-Verbindung (direkte Verbindung durch den Client-Computer)

Zugehörige Informationen

➡ „Server/Client-Verbindung“ auf Seite 12

➡ „Peer-to-peer-Verbindung“ auf Seite 12

Server/Client-Verbindung

Durch das auf dem Server installierte Document Capture Pro Server lässt sich die Scanner- und Auftragsverwaltung zentralisieren. Es eignet sich hauptsächlich für Vorgänge, bei denen mehrere Scanner zum Scannen einer großen Anzahl von Dokumenten in einem bestimmten Format verwendet werden.

Zugehörige Informationen

➡ „Definitionen von Begriffen in diesem Handbuch“ auf Seite 8

Peer-to-peer-Verbindung

Zur Verwendung mit einem bestimmten Scanner und einem auf dem Client-Computer installierten Scannertreiber, beispielsweise Epson Scan 2. Durch das Installieren von Document Capture Pro (Document Capture) auf dem Client-Computer lassen sich Aufträge auf bestimmten Client-Computern des Scanners ausführen.

Zugehörige Informationen

➡ „Definitionen von Begriffen in diesem Handbuch“ auf Seite 8

Vorbereiten einer Netzwerkverbindung

Abrufen von Informationen zu Verbindungseinstellungen

Für die Netzwerkverbindung müssen eine IP-Adresse, Gateway-Adresse usw. vorliegen. Prüfen Sie folgende Punkte im Voraus.

Kategorie	Optionen	Hinweis
Art der Geräteverbindung	❏ Ethernet	Verwenden Sie ein STP-Kabel (Shielded Twisted Pair) der Kategorie 5e oder höher für die Ethernet-Verbindung.
LAN-Verbindungsdaten	❏ IP-Adresse ❏ Subnetzmaske ❏ Standard-Gateway	Wenn die IP-Adresse über die DHCP-Funktion des Routers automatisch zugeweisen wird, ist diese Angabe nicht erforderlich.
DNS-Serverangaben	❏ IP-Adresse für primären DNS-Server ❏ IP-Adresse für sekundären DNS-Server	Bei Verwendung einer statischen IP-Adresse sollte die DNS-Servereinstellung konfiguriert werden. Konfigurieren bei automatischer Zuweisung über die DHCP-Funktion und wenn der DNS-Server nicht automatisch zugewiesen wird.
Proxyserverangaben	❏ Proxyservername ❏ Portnummer	Konfigurieren, wenn ein Proxyserver für die Internetverbindung verwendet wird und beim Einsatz des Epson Connect-Dienstes oder der automatischen Aktualisierung der Firmware.

Scanner-Spezifikationen

Die Spezifikation des Scanners für Standard- oder Verbindungsmodus finden Sie im *Benutzerhandbuch*.

Verwenden der Anschlussnummer

Informationen zur Anschlussnummer (Port), die der Scanner verwendet, finden Sie im „Anhang“.

Zugehörige Informationen

➡ „Verwendeter Scannerport“ auf Seite 60

Arten der IP-Adresszuweisung

Es gibt zwei Arten der Adresszuweisung an den Scanner.

Statische IP-Adresse:

Es wird eine im Voraus vergebene eindeutige IP-Adress an den Scanner vergeben.

Die IP-Adresse wird nicht geändert, selbst wenn der Scanner oder der Router ausgeschaltet werden, daher kann das Gerät über die IP-Adresse verwaltet werden.

Diese Methode eignet sich für Netzwerke, in denen viele Scanner verwaltet werden, wie beispielsweise ein großes Büro oder eine Schule.

Automatische Zuweisung über die DHCP-Funktion:

Die korrekte IP-Adresse wird automatisch zugewiesen, wenn die Kommunikation zwischen dem Scanner und dem Router mit der DHCP-Funktion erfolgreich ist.

Wenn es unpraktisch ist, die IP-Adresse eines bestimmten Geräts ändern zu müssen, reservieren Sie die IP-Adresse im Voraus durch direktes Einstellen.

DNS-Server und Proxyserver

Falls Sie einen Internetanbieter verwenden, konfigurieren Sie zunächst den entsprechenden DNS-Server. Sollte dieser nicht konfiguriert sein, muss bei jedem Zugriff die IP-Adresse konfiguriert sein, da die Namensauflösung dann im Allgemeinen fehlschlägt.

Der Proxyserver wird am Gateway zwischen Netzwerk und Internet platziert und kommuniziert als Mittler zwischen Computer, Scanner und Internet (Gegenstelle). Der Server der Gegenstelle kommuniziert nur mit dem Proxyserver. Daher hat er keinen Zugriff auf Scannerinformationen wie IP-Adresse und Portnummer, wodurch die Sicherheit verbessert wird.

Der Zugang zu bestimmten URLs kann mithilfe einer Filterfunktion verhindert werden, da der Proxyserver den Kommunikationsinhalt überprüfen kann.

Methode zum Einrichten einer Netzwerkverbindung

Gehen zum Einrichten von Verbindungseinstellungen wie IP-Adresse des Scanners, Subnetzmaske und Standardgateway wie folgt vor.

Über das Bedienfeld:

So konfigurieren Sie die Einstellungen mithilfe des Scannerbedienfelds für einzelne Scanner. Stellen Sie eine Verbindung mit dem Netzwerk her, nachdem die Verbindungseinstellungen des Scanners konfiguriert wurden.

Über das Installationsprogramm:

Wenn das Installationsprogramm verwendet wird, so werden Scannernetzwerk und Client-Computer automatisch eingestellt. Die Einrichtung ist anhand der Anweisungen des Installationsprogramms auch ohne detailliertes technisches Wissen über das Netzwerk möglich.

Mithilfe eines Tools:

Verwenden Sie hierzu ein Tool des Administratorcomputers. Sie können einen Scanner ausfindig machen und dann einrichten oder eine SYLK-Datei erstellen, um Batch-Einstellungen an mehreren Scannern vorzunehmen. Es lassen sich viele Scanner einrichten, die jedoch über Ethernet-Verkabelung vor der Einrichtung physisch verbunden sein müssen. Diese Methode wird daher empfohlen, wenn ein Ethernet-Netwerk zur Einrichtung hergestellt werden kann.

Zugehörige Informationen

➡ „Verbinden mit dem Netzwerk über das Bedienfeld“ auf Seite 15

➡ „Herstellen einer Netzwerkverbindung mithilfe des Installationsprogramms“ auf Seite 19

➡ „Zuweisen von IP-Adressen mithilfe von EpsonNet Config“ auf Seite 56

Verbindung

In diesem Kapitel wird die Umgebung oder das Verfahren zum Verbinden des Scanners mit einem Netzwerk erläutert.

Verbinden mit einem Netzwerk

Verbinden mit dem Netzwerk über das Bedienfeld

Verbinden Sie den Scanner über das Bedienfeld des Scanners mit dem Netzwerk.

Weitere Informationen über das Bedienfeld des Scanners finden Sie im *Benutzerhandbuch*.

Zuweisen der IP-Adresse

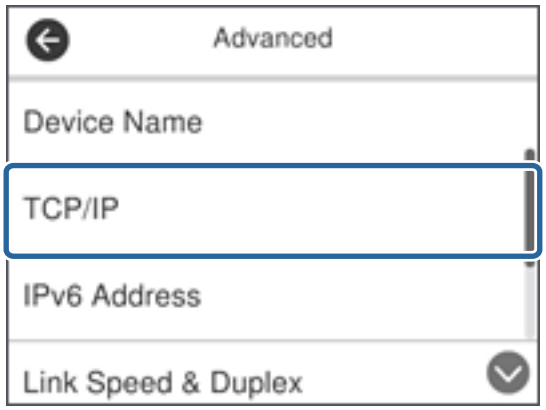
So richten Sie grundlegende Punkte wie IP-Adresse, Subnetzmaske und Standard-Gateway ein.

1. Schalten Sie den Scanner ein.
2. Wischen Sie am Bildschirm des Scannerbedienfelds nach links, und tippen Sie dann auf **Einstellungen**.

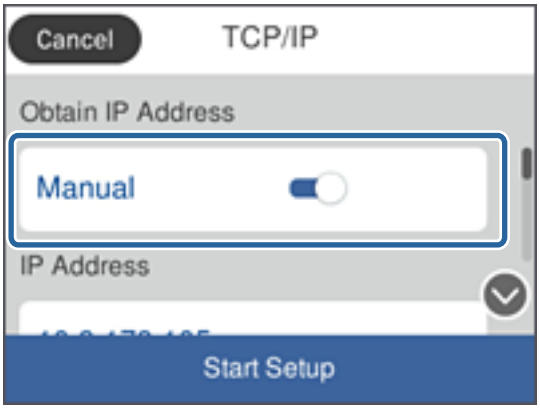
3. Tippen Sie auf **Netzwerkeinstellungen** > **Einstellungen ändern**.

   Falls der Punkt nicht sichtbar ist, wischen Sie am Bildschirm nach oben, damit er angezeigt wird.

4. Tippen Sie auf **TCP/IP**.

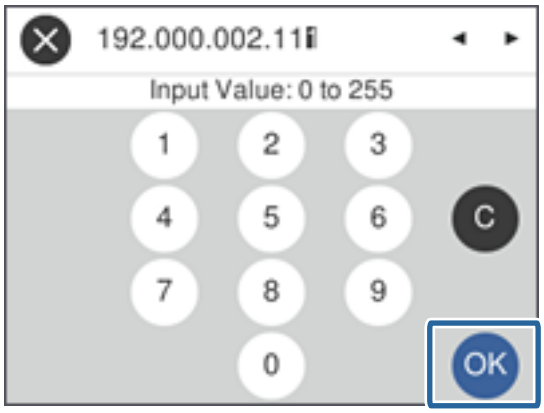


5. Wählen Sie **Manuell** bei **IP-Adresse anfordern**.



Hinweis:
Wenn die IP-Adresse automatisch durch Verwendung der DHCP-Funktion des Routers abgerufen wird, wählen Sie ***Auto*** *aus. In diesem Fall werden* ***IP-Adresse***, ***Subnetzmaske*** *und* ***Standard-Gateway*** *der Schritte 6 bis 7 ebenfalls automatisch eingestellt — fahren Sie daher mit Schritt 8 fort.*

6. Tippen Sie auf das Feld **IP-Adresse**, geben Sie mithilfe der Bildschirmtastatur die IP-Adresse ein, und tippen Sie dann auf **OK**.



Bestätigen Sie den am vorherigen Bildschirm angezeigten Wert.

7. Richten Sie die **Subnetzmaske** und das **Standard-Gateway** ein.

   Bestätigen Sie den am vorherigen Bildschirm angezeigten Wert.

   Hinweis:
   *Falls die Kombination aus IP-Adresse, Subnetzmaske und Standard-Gateway ungültig ist, kann **Einrichtung starten** nicht mit der Einstellung fortfahren. Überprüfen Sie, ob kein Eingabefehler vorliegt.*

8. Tippen Sie auf das Feld **Primäre DNS** für **DNS-Server**, geben Sie mithilfe der Bildschirmtastatur die IP-Adresse des primären DNS-Servers ein, und tippen Sie auf **OK**.

   Bestätigen Sie den am vorherigen Bildschirm angezeigten Wert.

   Hinweis:
   *Wenn **Auto** in den Einstellungen für die IP-Adresszuweisung ausgewählt wird, können die DNS-Server-Einstellungen über **Manuell** oder **Auto** ausgewählt werden. Wenn die Adresse des DNS-Servers nicht automatisch ermittelt werden kann, wählen Sie **Manuell** aus, und geben Sie die DNS-Server-Adresse ein. Geben Sie anschließend die Adresse des sekundären DNS-Servers direkt ein. Falls **Auto** ausgewählt wird, bei Schritt 10 fortfahren.*

9. Tippen Sie auf das Feld **Sekundäre DNS**, geben Sie mithilfe der Bildschirmtastatur die IP-Adresse des sekundären DNS-Servers ein, und tippen Sie auf **OK**.

   Bestätigen Sie den am vorherigen Bildschirm angezeigten Wert.

10. Tippen Sie auf **Einrichtung starten**.

11. Tippen Sie im Bestätigungsbildschirm auf **schließen**.

    Der Bildschirm wird automatisch nach einer bestimmten Zeit geschlossen, solange Sie nicht auf **schließen** tippen.

Herstellen einer Ethernet-Verbindung

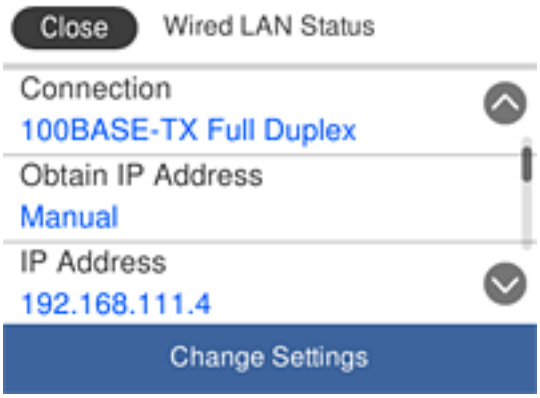
So verbinden Sie den Scanner über ein Ethernetkabel mit dem Netzwerk und prüfen die Verbindung.

1. Verbinden Sie den Scanner mit einem Hub (L2-Switch) über ein Ethernet-Kabel.

   Das Symbol im Startbildschirm ändert sich in  .

2. Drücken Sie auf dem Startbildschirm auf  .

3. Stellen Sie den Bildschirm aufrecht, und achten Sie dann darauf, dass der Verbindungsstatus und die IP-Adresse korrekt sind.



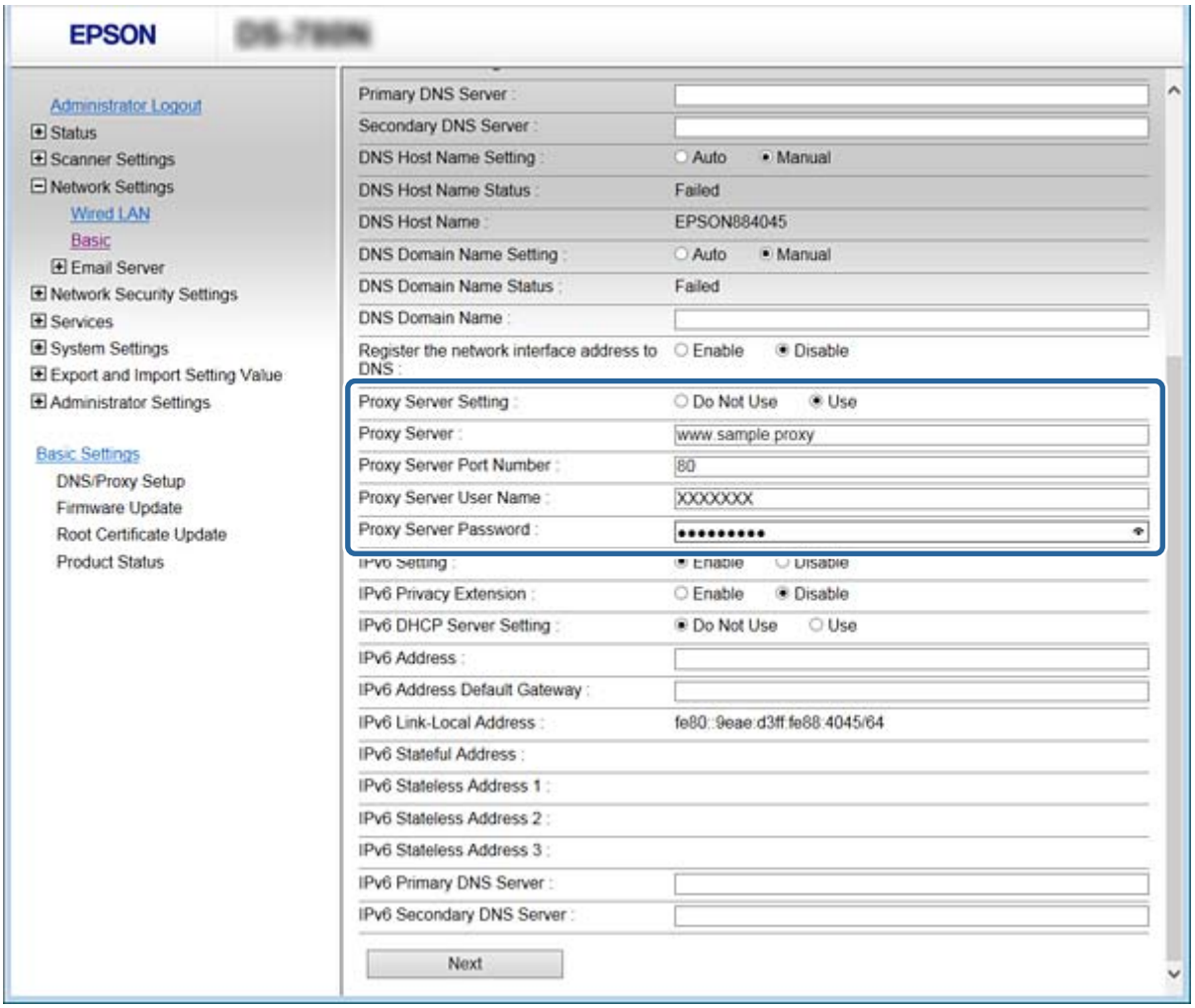
Einrichten des Proxy-Servers

Der Proxy-Server lässt sich nicht am Bedienfeld einstellen. Konfigurieren Sie ihn mithilfe von Web Config.

1. Rufen Sie Web Config auf und wählen Sie **Netzwerkeinstellungen** > **Grundlegend**.
2. Wählen Sie **Verwenden** in **Einstellung Proxyserver**.
3. Geben Sie den Proxy-Server als IPv4-Adresse oder im FQDN-Format unter **Proxy-Server** an, und geben Sie dann die Portnummer unter **Proxy-Server-Portnummer** an.

   Geben Sie für Proxy-Server, die eine Authentifizierung erfordern, den Benutzernamen und das Kennwort für die Proxy-Server-Authentifizierung ein.

4. Klicken Sie auf die Schaltfläche **Weiter**.



5. Überprüfen Sie die Einstellungen, und klicken Sie dann auf **Einstellungen**.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

Herstellen einer Netzwerkverbindung mithilfe des Installationsprogramms

Wir empfehlen, das Installationsprogramm zu verwenden, um den Scanner mit dem Computer zu verbinden. Sie können das Installationsprogramm mit einer der folgenden Methoden ausführen.

❏ Einrichtung über die Website

Rufen Sie die folgende Webseite auf und geben Sie dann den Produktnamen ein. Rufen Sie **Setup** auf, und beginnen Sie dann die Einrichtung.

http://epson.sn

❏ So verläuft die Einrichtung mithilfe des Datenträgers (nur für Modelle, die mit Datenträger geliefert werden, bzw. für Computer mit optischen Laufwerken.)

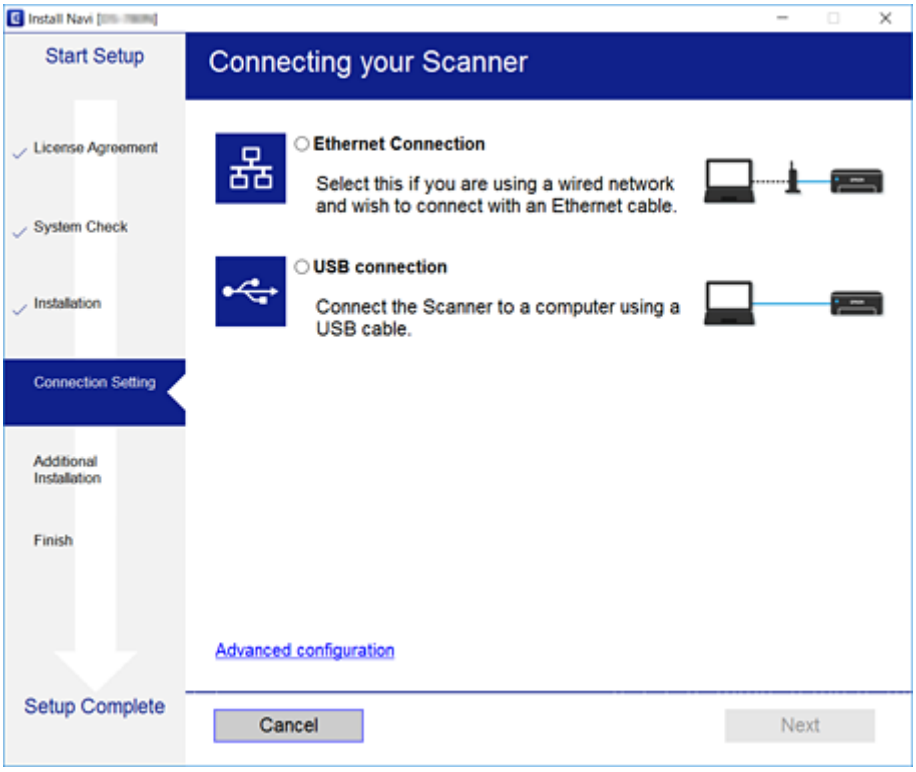
Legen Sie den Datenträger in das Laufwerk ein und folgen Sie der Anleitung auf dem Bildschirm.

Auswählen der Verbindungsmethode

Befolgen Sie die Bildschirmanleitung, bis der folgende Bildschirm angezeigt wird, und wählen Sie dann die Verbindungsmethode zwischen Drucker und Scanner aus.

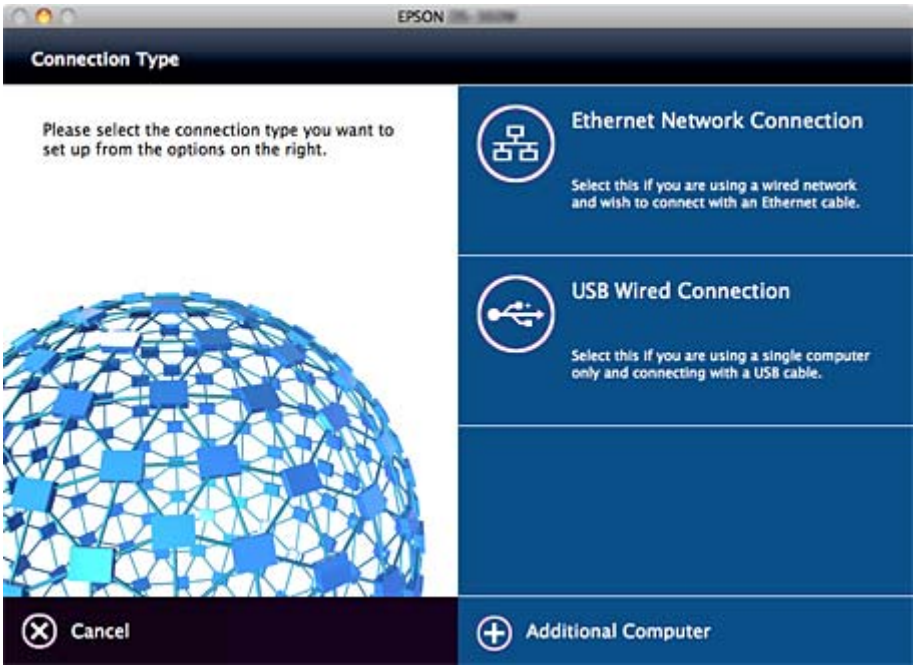
❏ Windows

Wählen Sie den Verbindungstyp aus, und klicken Sie auf **Weiter**.



❏ Mac OS

Wählen Sie den Verbindungstyp aus.



Verbindung

Folgen Sie der Bildschirmanleitung. Die erforderliche Software wird installiert.

Funktionseinstellungen

In diesem Kapitel werden die grundlegenden Einstellungen für die Nutzung der einzelnen Gerätefunktionen erläutert.

Software für Einstellungen

In diesem Thema wird das Vornehmen von Einstellungen vom Computer des Administrators aus mithilfe von Web Config erläutert.

Web Config (Webseite des Geräts)

Über Web Config

Web Config ist eine Browser-basierte Anwendung zum Konfigurieren von Scannereinstellungen.

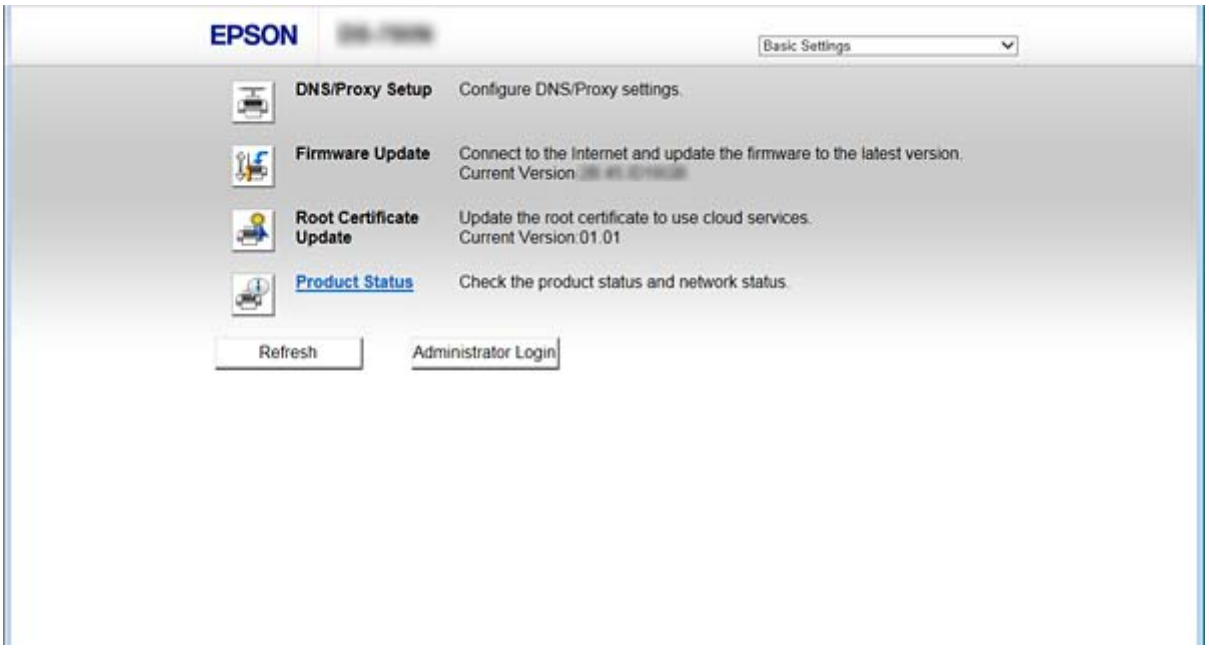
Um Web Config aufrufen zu können, muss dem Scanner zuerst eine IP-Adresse zugewiesen werden.

Hinweis:
Sie können die Einstellungen durch Festlegen eines Administratorkennwortes für den Scanner sperren.

Es gibt zwei Einstellungsseiten (siehe unten).

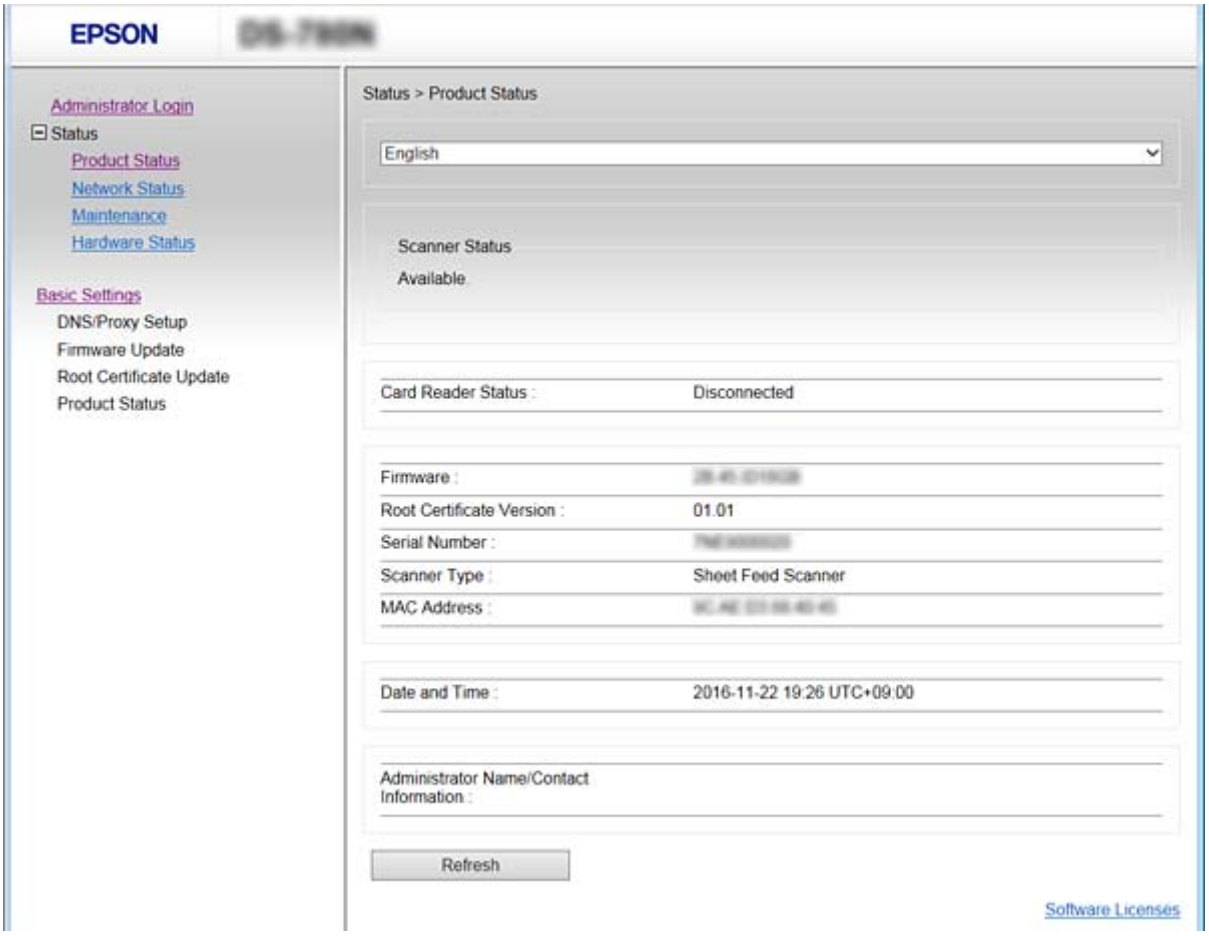
❏ **Grundeinstellungen**

Sie können die Standardeinstellungen des Scanners konfigurieren.



❏ **Erweiterte Einstellungen**

Sie können die erweiterten Einstellungen des Scanners konfigurieren. Diese Seite ist hauptsächlich für den Administrator.



Aufrufen von Web Config

Geben Sie die IP-Adresse des Scanners in einen Webbrowser ein. JavaScript muss aktiviert sein. Beim Zugriff auf Web Config über HTTPS wird im Browser eine Warnmeldung angezeigt, da im Scanner ein selbstsigniertes Zertifikat gespeichert ist.

❏ Aufruf über HTTPS

IPv4: https://<Scanner-IP-Adresse> (ohne < >)

IPv6: https://[Scanner-IP-Adresse] (mit [ ])

❏ Aufruf über HTTP

IPv4: http://<Scanner-IP-Adresse> (ohne < >)

IPv6: http://[Scanner-IP-Adresse] (mit [ ])

Hinweis:

❏ *Beispiele*

IPv4:

https://192.0.2.111/

http://192.0.2.111/

IPv6:

https://[2001:db8::1000:1]/

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

❏ *Wenn der Scannername mit dem DNS-Server registriert ist, können Sie anstelle der Drucker-IP-Adresse den Scannernamen verwenden.*

Zugehörige Informationen

➡ „SSL/TLS-Kommunikation mit dem Scanner“ auf Seite 63

➡ „Über digitale Zertifizierung“ auf Seite 63

Verwenden der Scan-Funktionen

Installieren Sie je nach Nutzung des Scanners die folgende Software, und nehmen Sie mit dieser entsprechende Einstellungen vor.

❏ **Scannen vom Computer**

❏ Überprüfen Sie die Funktion des Netzwerk-Scan-Dienstes mit Web Config (werkseitig eingestellt).

❏ Installieren Sie Epson Scan 2 auf Ihrem Computer und stellen Sie die IP-Adresse ein

❏ Installieren Sie beim Scannen mithilfe von Druckaufträgen Document Capture Pro (Document Capture) und nehmen Sie Auftragseinstellungen vor.

❏ **Scannen vom Bedienfeld**

❏ Bei Verwendung von Document Capture Pro oder Document Capture Pro Server:

Installieren Sie Document Capture Pro oder Document Capture Pro Server

DCP-Einstellung (Servermodus, Clientmodus).

❏ Bei Verwendung des WSD-Protokolls:

Überprüfen Sie die Funktion von WSD mit Web Config oder am Bedienfeld (werkseitig eingestellt)

Zusätzliche Geräteeinstellungen (Windows-Computer).

Scannen von einem Computer

Installieren Sie die Software und prüfen Sie, ob der Netzwerk-Scan-Dienst aktiviert ist, um vom Computer aus über ein Netzwerk zu scannen.

Zugehörige Informationen

➡ „Zu installierende Software“ auf Seite 25

➡ „Aktivieren des Netzwerk-Scannens“ auf Seite 25

Zu installierende Software

❏ Epson Scan 2

Dies ist der Scanner-Treiber. Falls Sie dass Gerät von einem Computer aus nutzen, installieren Sie den Treiber auf jedem Client-Computer. Wenn Document Capture Pro/Document Capture installiert ist, können Sie die den Gerätetasten zugewiesenen Funktionen ausführen.

Mit EpsonNet SetupManager lassen sich Druckertreiber auch gemeinsam in Paketen verteilen.

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

Installation auf dem Client-Computer. Auf einem Computer registrierte Aufträge lassen sich mit dem im Netzwerk installierten Document Capture Pro/Document Capture vom Computer und vom Scanner-Bedienfeld aus abrufen und ausführen.

Über das Netzwerk lässt sich auch vom Computer aus scannen. Epson Scan 2 ist für das Scannen erforderlich.

Zugehörige Informationen

➡ „EpsonNet SetupManager“ auf Seite 56

Einstellen der IP-Adresse des Scanners auf Epson Scan 2

So richten Sie die IP-Adresse des Scanners ein, damit dieser im Netzwerk verwendet werden kann.

1. Starten Sie **Epson Scan 2 Utility** über **Start** > **Alle Programme** > **EPSON** > **Epson Scan 2**.

   Falls ein anderer Scanner bereits registriert ist, mit Schritt 2 fortfahren.

   Falls nicht registriert, mit Schritt 4 fortfahren.

2. Klicken Sie auf ▼ auf dem **Scanner**.
3. Klicken Sie auf **Einstellungen**.
4. Klicken Sie auf **Bearbeiten aktivieren**, und klicken Sie dann auf **Hinzufügen**.
5. Wählen Sie den Namen des Scannermodells unter **Modell**.
6. Wählen Sie die IP-Adresse des zu verwendenden Scanners unter **Adresse** in **Nach Netzwerk suchen** aus.

   Klicken Sie auf  und dann auf  , um die Liste zu bearbeiten. Wenn sich die IP-Adresse des Scanners nicht ermitteln lässt, wählen Sie **Adresse eingeben** aus, und geben Sie die IP-Adresse ein.

7. Klicken Sie auf **Hinzufügen**.
8. Klicken Sie auf **OK**.

Aktivieren des Netzwerk-Scannens

So richten Sie den Netzwerk-Scan-Dienst für das Scannen von einem Client-Computer aus über das Netzwerk ein. Die Standardeinstellung ist aktiviert.

1. Rufen Sie „Web Config“ auf und wählen Sie **Services** > **Netzwerkscan**.

2. Achten Sie darauf, dass **Scannen aktivieren** in **EPSON Scan** ausgewählt ist.

   Falls der Punkt aktiviert wurde, ist der Vorgang damit beendet. Schließen Sie „Web Config“.

   Falls der Punkt deaktiviert ist, aktivieren Sie ihn, und fahren Sie mit dem nächsten Schritt fort.

3. Klicken Sie auf **Weiter**.

4. Klicken Sie auf **OK**.

   Die Netzwerkverbindung wird erneut hergestellt, und die Einstellungen werden aktiviert.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

Scannen über das Bedienfeld

Die Funktionen „An Ordner scannen“ und „Scannen an E-Mail“ über das Scannerbedienfeld sowie das Übertragen von Scanergebnissen per E-Mail an Ordner usw. werden durch das Ausführen eines Auftrags vom Computer aus durchgeführt.

Richten Sie den Auftrag beim Übertragen von Scanergebnissen mit Document Capture Pro Server oder Document Capture Pro ein.

Einzelheiten zu den Einstellungen bzw. über das Einrichten des Auftrags finden Sie in der Dokumentation oder Hilfe zu Document Capture Pro Server oder Document Capture Pro.

Zugehörige Informationen

➡ „Einstellungen für Document Capture Pro Server/Document Capture Pro“ auf Seite 26

➡ „Benennen von Servern und Ordnern“ auf Seite 27

Software zur Installation auf dem Computer

❏ **Document Capture Pro Server**

Dies ist die Serverversion von Document Capture Pro. Installieren Sie sie auf einem Windows-Server. Mehrere Geräte und Aufträge lassen sich zentral durch den Server verwalten. Die Aufträge können gleichzeitig von mehreren Scannern ausgeführt werden.

Durch die Nutzung der zertifizierten Version von Document Capture Pro Server lässt sich der Verlauf von Aufträgen und Scans verwalten.

Einzelheiten zu Document Capture Pro Server erhalten Sie von Ihrer Epson-Präsenz vor Ort.

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

Wie beim Scannen vom Computer aus können Sie die auf dem Computer registrierten Aufträge vom Bedienfeld aus abrufen und ausführen. Es ist nicht möglich, Computer-Aufträge gleichzeitig von mehreren Scannern ausführen zu lassen.

Einstellungen für Document Capture Pro Server/Document Capture Pro

Vornehmen von Einstellungen zur Nutzung der Scan-Funktion vom Scannerbedienfeld aus.

1. Rufen Sie Web Config auf und wählen Sie **Services** > **Document Capture Pro**.

2. Wählen Sie **Betriebsmodus**.

   ❏ Servermodus:

   Wählen Sie diese Option aus bei der Verwendung von Document Capture Pro Server oder von Document Capture Pro nur für Aufträge aus, die für einen bestimmten Computer eingestellt wurden.

   ❏ Client-Modus:

   Wählen sie diese Option bei der Auswahl von auf den Client-Computern im Netzwerk installierten Auftragseinstellung von Document Capture Pro (Document Capture) aus, ohne einen Computer anzugeben.

3. Nehmen Sie je nach ausgewähltem Modus folgende Einstellungen vor.

   ❏ Servermodus:

   Legen Sie unter **Serveradresse** den Server fest, auf dem Document Capture Pro Server installiert ist. Dieser Eintrag ist zwischen 2 und 252 Zeichen lang, im Format IPv4-, IPv6-, Hostnamen- oder FQDN. Im FQDN-Format können ASCII-Zeichen, Zahlen, Buchstaben und Bindestriche (außer als erstes oder letztes Zeichen) verwendet werden.

   ❏ Client-Modus:

   Mit **Gruppeneinstellungen** wird eine in Document Capture Pro (Document Capture) festgelegte Scannergruppe angegeben.

4. Klicken Sie auf **Einstellungen**.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

Benennen von Servern und Ordnern

Document Capture Pro und Document Capture Pro Server speichern die gescannten Daten einmalig auf dem Server oder Client-Computer und verwenden die Transfer-Funktion, um die Funktionen „An Ordner scannen“ und „Scannen an E-Mail“ auszuführen.

Sie benötigen eine Berechtigung und Anmeldedaten für den Transfer von dem Computer, auf dem Document Capture Pro, Document Capture Pro Server installiert ist, auf den Computer oder Cloud-Dienst.

Bereiten Sie diese Angaben entsprechend der zu nutzenden Funktion anhand folgender Hinweise vor.

Die Einstellungen für diese Funktionen lassen sich mithilfe von Document Capture Pro oder Document Capture Pro Server vornehmen. Einzelheiten zu den Einstellungen finden Sie in der Dokumentation oder Hilfe zu Document Capture Pro Server oder Document Capture Pro.

Name	Einstellung	Anforderung
Scannen an Netzwerkordner (SMB)	Erstellen und Einrichten der Freigabe für den Speicherordner	Admin-Konto für den Computer, der den Speicherordner stellt.
	Ziel für Scannen an Netzwerkordner (SMB)	Benutzername und Kennwort zur Anmeldung an dem Computer mit dem Speicherordner und Berechtigung für das Aktualisieren des Speicherordners.
Scannen an Netzwerkordner (FTP)	Einrichten des FTP-Servers zur Anmeldung	Anmeldedaten für den FTP-Server und Berechtigung für das Aktualisieren des Speicherordners.

Name	Einstellung	Anforderung
Scannen an E-Mail	Einrichten des E-Mail-Servers	Einstellungsdaten für den E-Mail-Server
Scannen an Document Capture Pro (beim Gebrauch von Document Capture Pro Server)	Setup für das Anmelden bei Cloud-Diensten	Arbeitsumgebung mit Internetverbindung Kontoregistrierung für Cloud-Dienste

Verwenden von WSD-Scan (nur Windows)

Wenn der Computer Windows Vista oder höher verwendet, lässt sich die Funktion WSD-Scan nutzen.

Bei Verwendung des WSD-Protokolls wird das Menü **Computer (WSD)** am Bedienfeld des Scanners angezeigt.

1. Rufen Sie Web Config auf und wählen Sie **Services** > **Protokoll**.
2. Überprüfen Sie, dass **WSD aktivieren** in den **WSD-Einstellungen** aktiviert ist.
   Falls der Punkt aktiviert ist, ist der Auftrag vollständig und Web Config kann geschlossen werden.
   Falls der Punkt nicht aktiviert ist, aktivieren Sie ihn und fahren dann mit dem nächsten Schritt fort.
3. Klicken Sie auf die Schaltfläche **Weiter**.
4. Bestätigen Sie die Einstellungen und klicken Sie auf **Einstellungen**.

Vornehmen von Systemeinstellungen

Vornehmen von Systemeinstellungen am Bedienfeld

Einstellen der Bildschirmhelligkeit

So stellen Sie die Helligkeit des LCD-Bildschirms ein.

1. Tippen Sie auf dem Startbildschirm auf **Einstellungen**.
2. Tippen Sie auf **Allgemeine Einstellungen** > **LCD-Helligkeit**.
3. Tippen Sie zum Anpassen der Helligkeit auf  oder  .
   Die möglichen Werte zur Anpassung sind 1 bis 9.
4. Tippen Sie auf **OK**.

Sound einrichten

So richten Sie die Betriebs- und Fehlertonsignale des Bedienfelds ein.

1. Tippen Sie auf dem Startbildschirm auf **Einstellungen**.
2. Tippen Sie auf **Allgemeine Einstellungen** > **Ton**.
3. Stellen Sie die folgenden Punkte nach Bedarf ein.
   - ❏ Tonsignale bei Betrieb
     Stellen Sie die Lautstärke der Betriebstonsignale am Bedienfeld ein.
   - ❏ Tonsignale bei Fehlern
     Stellen Sie die Lautstärke der Fehlertonsignale ein.
4. Tippen Sie auf **OK**.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

Doppeleinzug von Vorlagen erkennen

Beschreibt die Funktion zur Erkennung eines Doppeleinzugs gescannter Dokumente und zum Stoppen des Scanvorgangs beim Einzug mehrerer Vorlagen.

Deaktivieren Sie diese Einstellung beim Scannen von Vorlagen, die häufig doppelt eingezogen werden, beispielsweise Umschläge oder Papier mit Etiketten.

Hinweis:
Die Einstellung lässt sich in Web Config oder in Epson Scan 2 vornehmen.

1. Tippen Sie auf dem Startbildschirm auf **Einstellungen**.
2. Tippen Sie auf **Externe Scaneinstellungen** > **Ultraschall-Doppeleinzugerk.**.
3. Tippen Sie zum Einschalten auf **Ultraschall-Doppeleinzugerk.**.
4. Tippen Sie auf **schließen**.

Einstellen des Modus mit niedriger Geschwindigkeit

So richten Sie das Scannen mit niedriger Geschwindigkeit ein, damit beim Scannen dünner Dokumente wie Durchschriften kein Papierstau entsteht.

1. Tippen Sie auf dem Startbildschirm auf **Einstellungen**.
2. Tippen Sie auf **Externe Scaneinstellungen** > **Langsam**.
3. Tippen Sie zum Einschalten auf **Langsam**.
4. Tippen Sie auf **schließen**.

Vornehmen von Systemeinstellungen mit „Web Config“

Einstellen der Energiesparfunktion bei Inaktivität

So stellen Sie die Energiesparfunktion bei Inaktivität des Scanners ein. Passen Sie die Zeitspanne an Ihr Nutzungsverhalten an.

Hinweis:
Die Energiesparfunktionen lassen sich auch am Bedienfeld des Scanners einstellen.

1. Rufen Sie Web Config auf und wählen Sie **Systemeinstellungen** > **Energiesparen**.
2. Geben Sie eine Zeitspanne für den **Schlaf-Timer** ein, nach der bei Inaktivität in den Energiesparmodus gewechselt wird.

   Die Zeitspanne kann in Minutenabstufung bis zu 240 Minuten betragen.
3. Wählen Sie die Abschaltzeit für den **Abschalttimer** aus.
4. Klicken Sie auf **OK**.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

Einrichten des Bedienfelds

So richten Sie das Scannerbedienfeld ein. Die Einrichtung umfasst folgende Schritte.

1. Rufen Sie Web Config auf und wählen Sie **Systemeinstellungen** > **Bedienfeld**.
2. Stellen Sie die folgenden Punkte nach Bedarf ein.
   - ❏ Sprache

     Wählen Sie die am Bedienfeld eingestellte Sprache ein.
   - ❏ Bedienfeldsperre

     Bei der Einstellung **Ein** ist das Administratorkennwort erforderlich, wenn ein Vorgang ausgeführt wird, der Administratorbefugnis erfordert. Falls kein Administratorkennwort eingerichtet ist, wird die Bedienfeldsperre deaktiviert.
   - ❏ Betriebszeitüberschr.

     Wenn **Ein** bei der Anmeldung als Administrator ausgewählt wird, erfolgt nach einer gewissen Zeitspanne ohne Aktivität eine automatische Abmeldung und Rückkehr zum Startbildschirm.

     Die Zeitspanne kann in Sekundenabstufung von 10 Sekunden bis zu 240 Minuten betragen.
3. Klicken Sie auf **OK**.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

Einschränken der Benutzung externer Schnittstellen

Die USB-Verbindung vom Computer lässt sich einschränken. Mit dieser Einstellung können Sie das Scannen auf die Netzwerkverbindung beschränken.

1. Rufen Sie Web Config auf und wählen Sie **Systemeinstellungen** > **Externe Schnittstelle**.
2. Wählen Sie **Aktivieren** oder **Deaktivieren**.

   Wählen Sie zum Beschränken **Deaktivieren** aus.
3. Tippen Sie auf **OK**.

Synchronisieren von Datum und Uhrzeit mit einem Zeitserver

Durch Nutzung eines CA-Zertifikats lassen sich Probleme mit der Zeiteinstellung vermeiden.

1. Rufen Sie hierzu Web Config auf und wählen Sie **Systemeinstellungen** > **Datum und Zeit** > **Zeitserver**.
2. Wählen Sie **Verwenden** bei **Zeitserver verwenden**.
3. Geben Sie die Adresse des Zeitservers in das Feld **Zeitserveradresse** ein.

   Sie können das IPv4-, IPv6 oder FQDN-Format verwenden. Geben Sie nicht mehr als 252 Zeichen ein. Falls keine Angabe gewünscht ist, das Feld leer lassen.
4. Geben Sie **Aktualisierungsintervall (Min.)** ein.

   Die Zeitspanne kann in Minutenabstufung bis zu 10.800 Minuten betragen.
5. Klicken Sie auf **OK**.

   Hinweis:
   *Sie können den Status der Verbindung mit dem Zeitserver mit **Zeitserverstatus** prüfen.*

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

Einfache Sicherheitseinstellungen

In diesem Kapitel werden einfache Sicherheitseinstellungen erläutert, die keine besondere Umgebung erfordern.

Einführung grundlegender Sicherheitsfunktionen

In diesem Abschnitt werden die grundlegenden Sicherheitsfunktionen von Epson-Geräten vorgestellt.

Funktion	Funktionstyp	Einstellungen	Zu vermeiden
Einrichten des Administratorkennworts	Sperren Sie die Einstellungen mit Systembezug, beispielsweise für Netzwerk und USB-Verbindung, damit sie außer dem Administrator von niemandem geändert werden können.	Ein Administrator richtet für das Gerät ein Kennwort ein. Konfiguration oder Aktualisierung sind von überall aus über Web Config, das Bedienfeld, Epson Device Admin und EpsonNet Config verfügbar.	Schützt vor unbefugten Lesen und Verändern der im Gerät gespeicherten Angaben wie ID, Kennwort, Netzwerkeinstellungen und Kontakten. Verringert auch eine Vielzahl von Sicherheitsrisiken wie Datenlecks der Netzwerkumgebung oder Aushebeln der Sicherheitsrichtlinie.
SSL/TLS-Kommunikation	Die Kommunikationsinhalte beim Zugriff auf einen Epson-Server im Internet von einem Gerät aus, beispielsweise während der Kommunikation zwischen Computer und Browser oder während eines Firmware-Updates, sind durch SSL/TLS verschlüsselt.	Stellen Sie ein CA-signiertes Zertifikat bereit, und importieren Sie es in den Scanner.	Durch die Identitätsbestätigung des Geräts aufgrund der CA-Signatur wird ein Identitätswechsel und unbefugter Zugriff verhindert. Zudem ist die Kommunikation von Inhalten mit SSL/TLS geschützt und ein Datenleck von Drucker- und Einstellungsdaten wird verhindert.
Steuerprotokolle	Steuerprotokolle dienen zur Kommunikation zwischen Geräten und Computern und aktivieren/deaktivieren Funktionen.	Ein Protokoll oder Dienst, der auf separat erlaubte oder untersagte Funktionen angewendet wird.	Verringert Sicherheitsrisiken, die durch die unbeabsichtigte Benutzung entstehen könnten, durch Einschränkung der benutzerzugänglichen Funktionen.

Zugehörige Informationen

➡ „Über Web Config“ auf Seite 22
➡ „EpsonNet Config“ auf Seite 55
➡ „Epson Device Admin“ auf Seite 55
➡ „Konfiguration des Administratorkennwortes“ auf Seite 33
➡ „Protokolle kontrollieren“ auf Seite 35

Konfiguration des Administratorkennwortes

Sobald ein Administratorkennwort eingerichtet ist, können außer dem Administrator keine anderen Benutzer die Einstellungen zur Systemverwaltung ändern. Das Administratorkennwort lässt sich entweder mit Web Config, am Scannerbedienfeld oder mit der Software (Epson Device Admin oder EpsonNet Config) einstellen oder ändern. Lesen Sie zum Gebrauch der Software zunächst die jeweilige Dokumentation.

Zugehörige Informationen

➡ „Konfigurieren des Administratorkennworts über das Bedienfeld“ auf Seite 33

➡ „Konfiguration des Administratorkennworts mit Web Config“ auf Seite 33

➡ „EpsonNet Config“ auf Seite 55

➡ „Epson Device Admin“ auf Seite 55

Konfigurieren des Administratorkennworts über das Bedienfeld

So richten Sie ein Administratorkennwort über das Scannerbedienfeld ein.

1. Tippen Sie auf dem Startbildschirm auf **Einstellungen**.
2. Tippen Sie auf **Systemadministration** > **Admin-Einstellungen**.

   Falls der Punkt nicht angezeigt wird, wischen Sie am Bildschirm nach oben, damit die entsprechende Seite angezeigt wird.
3. Tippen Sie auf **Admin-Kennwort** > **Registrieren**.
4. Geben Sie das neue Kennwort ein und tippen Sie dann auf **OK**.
5. Geben Sie das Kennwort ein und tippen Sie dann auf **OK**.
6. Tippen Sie im Bestätigungsbildschirm auf **OK**.

   Der Bildschirm mit Administratoreinstellungen wird angezeigt.
7. Tippen Sie auf **Sperreinstellung**, und tippen Sie dann auf dem Bestätigungsbildschirm auf **OK**.

   Sperreinstellung ist auf **Ein** eingestellt, und das Administratorkennwort wird abgefragt, wenn ein gesperrter Menüeintrag ausgewählt wird.

Hinweis:

❏ *Bei der Einstellung **Einstellungen** > **Allgemeine Einstellungen** > **Betriebszeitüberschr.** auf **Ein** meldet der Drucker Sie nach einer bestimmen Zeitspanne ohne Aktivität am Bedienfeld ab.*

❏ *Das Administratorkennwort lässt sich ändern oder löschen, indem Sie **Ändern** oder **Rücksetzen** auf dem **Admin-Kennwort**-Bildschirm auswählen und das Administratorkennwort eingeben.*

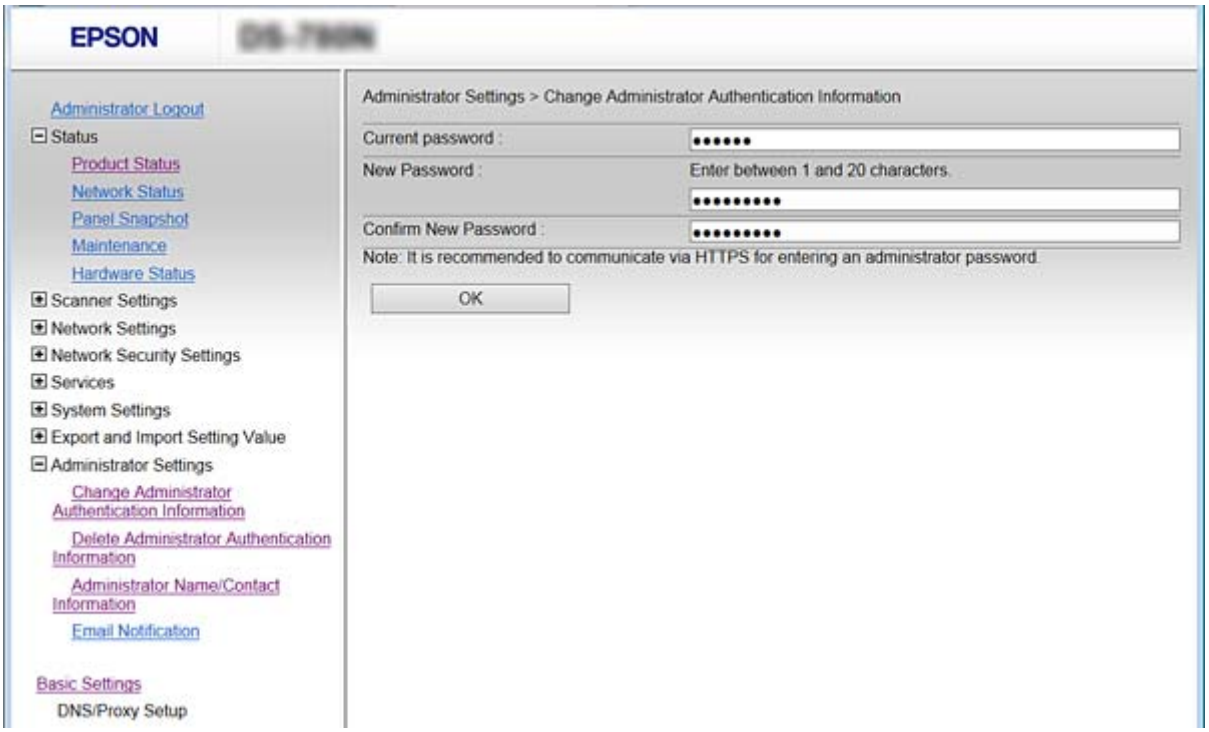
Konfiguration des Administratorkennworts mit Web Config

Das Administratorkennwort lässt sich mit Web Config einrichten.

1. Rufen Sie Web Config auf und wählen Sie **Administratoreinstellungen** > **Administratorauthentifizierungsinformationen ändern**.

2. Geben Sie in **Neues Kennwort** ein Kennwort ein und bestätigen Sie es in **Neues Kennwort bestätigen**. Geben Sie falls erforderlich einen Benutzernamen ein.

   Falls Sie das Passwort ändern möchten, geben Sie zunächst das aktuelle Passwort ein.



3. Wählen Sie **OK**.

Hinweis:

- *Um die gesperrten Menüpunkte einzustellen oder zu ändern, klicken Sie auf* ***Administratoranmeldung****, und geben Sie dann das Administratorkennwort ein.*
- *Um das Administratorkennwort zu löschen, klicken Sie auf* ***Administratoreinstellungen*** *>* ***Administratorauthentifizierungsinformationen löschen****, und geben Sie dann das Administratorkennwort ein.*

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

Per Administratorkennwort gesperrte Punkte

Administratoren sind berechtigt, alle Einstellungen und Funktionen des Geräts zu ändern.

Zudem lässt sich nach dem Einrichten des Administratorkennworts auf dem Gerät dieses sperren, sodass Einstellungspunkte in Bezug auf die Geräteverwaltung nicht geändert werden können.

Folgende Punkte können nur vom Administrator geändert werden.

Option	Beschreibung
Scannereinstellung	Einstellungen für Doppeleinzug-Erkennung und Modus mit niedriger Geschwindigkeit.

Einfache Sicherheitseinstellungen

Option	Beschreibung
Ethernet-Verbindungseinstellungen	Ändern des Gerätenamens und der IP-Adresse, Einrichtung des DNS-Servers oder Proxys, sowie Einstellungsänderungen für Netzwerkverbindungen.
Einstellung für Benutzerdienste	Einstellung zur Steuerung von Kommunikationsprotokollen, Netzwerkscan und Document Capture Pro-Diensten.
E-Mail-Server-Einstellung	Einrichten eines E-Mail-Servers, mit dem Geräte direkt kommunizieren können.
Sicherheitseinstellungen	Einstellungen für Netzwerksicherheit, z. B. SSL/TLS-Kommunikation, IPsec/IP-Filterung und IEEE802.1X.
Aktualisierung von Stammzertifikaten	Eine Aktualisierung von Stammzertifikaten für Document Capture Pro Server erfordert eine Authentifizierung und Firmware-Update über Web Config.
Firmware-Update	Prüfen und Aktualisieren der Firmware von Geräten.
Zeit und Timer-Einstellungen	Übergangszeit für Schlafmodus, automatische Abschaltung, Datum/Uhrzeit, Timer für Nichtbetrieb, andere Einstellungen in Bezug auf Timer.
Zurücksetzen auf Standardeinstellungen	Einstellung für das Zurücksetzen des Scanners auf Werkseinstellungen.
Administratoreinstellung	Einstellung für Administratorsperre oder -kennwort.
Zertifizierte Geräteeinstellung	ID-Einstellung des Authentifizierungsgeräts. Wird verwendet, wenn der Scanner mit einem Authentifizierungssystem betrieben wird, dass Authentifizierungsgeräte unterstützt.

Protokolle kontrollieren

Sie können mit einer Vielzahl von Pfaden und Protokollen scannen. Sie können auch das Netzwerk-Scannen von beliebig vielen Netzwerk-Computern verwenden. Beispielsweise wird auch die Beschränkung der Scanvorgänge auf bestimmte Pfade und Protokolle unterstützt. Sie können unbeabsichtigte Sicherheitsrisiken verringern, indem Sie das Scannen von spezifischen Pfaden beschränken oder die verfügbaren Funktionen kontrollieren.

Konfigurieren Sie die Protokolleinstellungen.

1. Rufen Sie Web Config auf und wählen Sie **Services** > **Protokoll**.
2. Konfigurieren Sie die entsprechenden Elemente.
3. Klicken Sie auf **Weiter**.
4. Klicken Sie auf **OK**.

   Die Einstellungen werden auf den Scanner angewandt.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23
➡ „Protokolle, die Sie aktivieren oder deaktivieren können“ auf Seite 36
➡ „Protokolleinstellungselemente“ auf Seite 37

Protokolle, die Sie aktivieren oder deaktivieren können

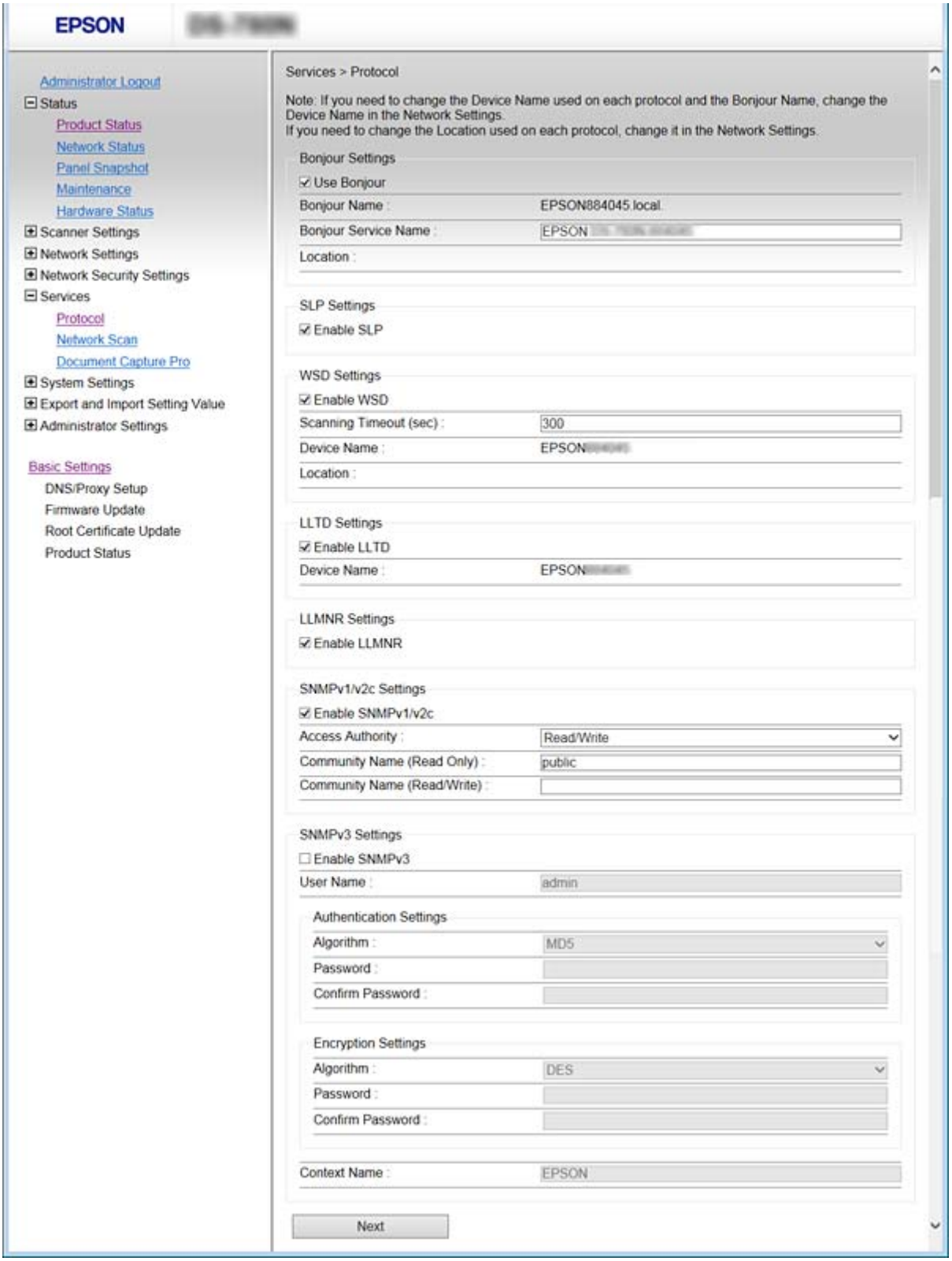
Protokoll	Beschreibung
Bonjour-Einstellungen	Sie können festlegen, ob Bonjour genutzt werden soll. Bonjour dient zur Suche nach Geräten, zum Scannen und so weiter.
SLP-Einstellungen	Sie können die SLP-Funktion aktivieren oder deaktivieren. SLP wird benötigt für Epson Scan 2 und die Netzwerksuche in EpsonNet Config.
WSD-Einstellungen	Sie können die WSD-Funktion aktivieren oder deaktivieren. Wenn diese Option aktiviert ist, können Sie WSD-Geräte hinzufügen oder über den WSD-Port scannen.
LLTD-Einstellungen	Sie können die LLTD-Funktion aktivieren oder deaktivieren. Wenn diese Option aktiviert ist, wird sie in der Windows-Netzwerkübersicht angezeigt.
LLMNR-Einstellungen	Sie können die LLMNR-Funktion aktivieren oder deaktivieren. Wenn diese Option aktiviert ist, können Sie eine Namensauflösung ohne NetBIOS nutzen, selbst wenn Sie DNS nicht nutzen können.
SNMPv1/v2c-Einstellungen	Sie können festlegen, ob SNMPv1/v2c aktiviert werden soll. Damit lassen sich Geräte einrichten, überwachen und so weiter.
SNMPv3-Einstellungen	Sie können festlegen, ob SNMPv3 aktiviert werden soll. Damit lassen sich verschlüsselte Geräte einrichten, überwachen usw.

Zugehörige Informationen

➡ „Protokolle kontrollieren“ auf Seite 35

➡ „Protokolleinstellungselemente“ auf Seite 37

Protokolleinstellungselemente



Optionen	Einstellungswert und Beschreibung
Bonjour-Einstellungen	

Einfache Sicherheitseinstellungen

Optionen	Einstellungswert und Beschreibung
Bonjour nutzen	Wählen Sie diese Option zur Suche nach oder Benutzung von Geräten über Bonjour.
Bonjour-Name	Zeigt den Bonjour-Namen.
Bonjour-Dienstname	Der Bonjour-Dienstname kann angezeigt und eingestellt werden.
Ort	Zeigt den Bonjour-Standortnamen.
SLP-Einstellungen	
SLP aktivieren	Wählen Sie diese Option zur Aktivierung der SLP-Funktion. Sie wird zur Netzwerkerkennung in Epson Scan 2 und EpsonNet Config verwendet.
WSD-Einstellungen	
WSD aktivieren	Wählen Sie diese Option zum Aktivieren der Hinzufügung von Geräten per WSD und zum Drucken und Scannen vom WSD-Port.
Scanzeitüberschreitung (Sek.)	Stellen Sie den Wert der Kommunikationszeitüberschreitung für den WSD-Scan auf 3 bis 3600 Sekunden ein.
Gerätename	Zeigt den WSD-Gerätenamen.
Ort	Zeigt den WSD-Standortnamen.
LLTD-Einstellungen	
LLTD aktivieren	Wählen Sie diese Option zur Aktivierung von LLTD. Der Scanner wird in der Windows-Netzwerkübersicht angezeigt.
Gerätename	Zeigt den LLTD-Gerätenamen.
LLMNR-Einstellungen	
LLMNR aktivieren	Wählen Sie diese Option zur Aktivierung von LLMNR. Sie können eine Namensauflösung ohne NetBIOS nutzen, selbst wenn Sie DNS nicht nutzen können.
SNMPv1/v2c-Einstellungen	
SNMPv1/v2c aktivieren	Wählen Sie diese Option zum Aktivieren von SNMPv1/v2c. Nur Scanner mit SNMPv3-Unterstützung werden angezeigt.
Zugangsautorität	Stellen Sie die Zugangsautorität ein, wenn SNMPv1/v2c aktiviert ist. Wählen Sie **Nur Lesen** oder **Lesen/Schreiben**.
Community-Name (nur Lesen)	Geben Sie 0 bis 32 ASCII-Zeichen (0x20 bis 0x7E) ein.
Community-Name (Lesen/Schreiben)	Geben Sie 0 bis 32 ASCII-Zeichen (0x20 bis 0x7E) ein.
SNMPv3-Einstellungen	
SNMPv3 aktivieren	SNMPv3 ist aktiviert, wenn das Kontrollkästchen aktiviert ist.
Benutzername	Geben Sie 1 bis 32 1-Byte-Zeichen ein.
Authentifizierungseinstellungen	

Einfache Sicherheitseinstellungen

Optionen	Einstellungswert und Beschreibung
Algorithmus	Wählen Sie einen Algorithmus zur Authentifizierung für SNMPv3 aus.
Kennwort	Geben Sie das Kennwort zur Authentifizierung für SNMPv3 ein. Geben Sie zwischen 8 und 32 ASCII-Zeichen (0x20–0x7E) ein. Falls keine Angabe gewünscht ist, das Feld leer lassen.
Kennwort bestätigen	Geben Sie das zur Bestätigung konfigurierte Kennwort ein.
Verschlüsselungseinstellungen	
Algorithmus	Wählen Sie einen Algorithmus zur Verschlüsselung aus für SNMPv3.
Kennwort	Geben Sie das Kennwort zur Verschlüsselung für SNMPv3 ein. Geben Sie zwischen 8 und 32 ASCII-Zeichen (0x20–0x7E) ein. Falls keine Angabe gewünscht ist, das Feld leer lassen.
Kennwort bestätigen	Geben Sie das zur Bestätigung konfigurierte Kennwort ein.
Kontextname	Geben Sie bis zu 32 Unicode-Zeichen (UTF-8) ein. Falls keine Angabe gewünscht ist, das Feld leer lassen. Die Anzahl der Zeichen, die eingegeben werden können, sind von der Sprache abhängig.

Zugehörige Informationen

➡ „Protokolle kontrollieren“ auf Seite 35

➡ „Protokolle, die Sie aktivieren oder deaktivieren können“ auf Seite 36

Betriebs- und Verwaltungseinstellungen

In diesem Kapitel werden die für den täglichen Einsatz und die Verwaltung des Geräts relevanten Punkte erläutert.

Bestätigen von Gerätedaten

Die folgenden Daten des Gerätebetriebs aus dem **Status** lassen sich mit Web Config überprüfen.

❏ Produktstatus

Sprache, Status, Produktnummer, MAC-Adresse usw.

❏ Netzwerkstatus

Angaben zum Netzwerkstatus, IP-Adresse, DNS-Server usw.

❏ Panel-Schnappschuss

Anzeigen eines Screenshots des Gerätebedienfelds.

❏ Wartung

Überprüfen Sie das Startdatum, die Scan-Angaben usw.

❏ Hardwarestatus

Prüfen Sie den Status des Scanners.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

Verwalten von Geräten (Epson Device Admin)

Sie können mithilfe von Epson Device Admin mehrere Geräte verwalten und bedienen. Epson Device Admin ermöglicht die Verwaltung von Geräten in unterschiedlichen Netzwerken. Im Folgenden werden die wichtigsten Verwaltungsfunktionen erläutert.

Weitere Informationen über Funktionen und zur Verwendung der Software finden Sie in der Dokumentation oder Hilfe von Epson Device Admin.

❏ Auffinden von Geräten

Nach dem Auffinden von Geräten im Netzwerk können diese in einer Liste registriert werden. Wenn Epson-Geräte wie Drucker und Scanner in demselben Netzwerksegment wie der Administratorcomputer verbunden sind, lassen Sie sich auch dann auffinden, wenn keine IP-Adresse zugewiesen wurde.

Es lassen sich auch Geräte auffinden, die über USB-Kabel an Netzwerkcomputer angeschlossen sind. Auf dem Computer muss hierzu der Epson Device USB Agent installiert sein.

❏ Einrichten von Geräten

Sie können eine Vorlage mit Einstellungspunkten wie Netzwerkschnittstelle und Papierquelle erstellen und diese dann auf andere Geräte als freigegebene Einstellungen anwenden. Sobald ein Gerät ans Netzwerk angeschlossen ist, können Sie ihm eine IP-Adresse zuweisen, falls noch nicht geschehen.

❏ Überwachen von Geräten

Der Status und weitere Detailangaben für die Geräte im Netzwerk lassen sich regelmäßig abrufen. Auch Geräte, die über USB-Kabel an Netzwerkcomputer angeschlossen sind, sowie Geräte anderer Hersteller, die in der Geräteliste erfasst wurden, können überwacht werden. Zur Überwachung von Geräten, die über USB-Kabel verbunden sind, muss der Epson Device USB Agent installiert sein.

❏ Verwaltung von Warnhinweisen

Der Status von Geräten und Verbrauchsmaterial lässt sich überwachen. Das System versendet automatisch anhand vordefinierter Bedingungen Benachrichtigungen an den Administrator.

❏ Verwalten von Berichten

Es lassen sich regelmäßige Berichte anhand der vom System erfassten Daten zur Gerätenutzung und zum Verbrauchsmaterial erstellen. Diese erstellten Berichte lassen sich dann speichern und per E-Mail versenden.

Zugehörige Informationen

➡ „Epson Device Admin“ auf Seite 55

Empfang von E-Mail-Benachrichtigungen bei Ereignissen

Infos zur E-Mail-Benachrichtigung

Diese Funktion steht zur Verfügung, um bei bestimmten Ereignissen eine E-Mail-Benachrichtigung zu erhalten. Es lassen sich bis zu 5 E-Mail-Adressen hinterlegen, sowie die Ereignisse, für die Sie Benachrichtigungen erhalten möchten.

Der Mailserver muss zunächst für die Benutzung dieser Funktion konfiguriert sein.

Zugehörige Informationen

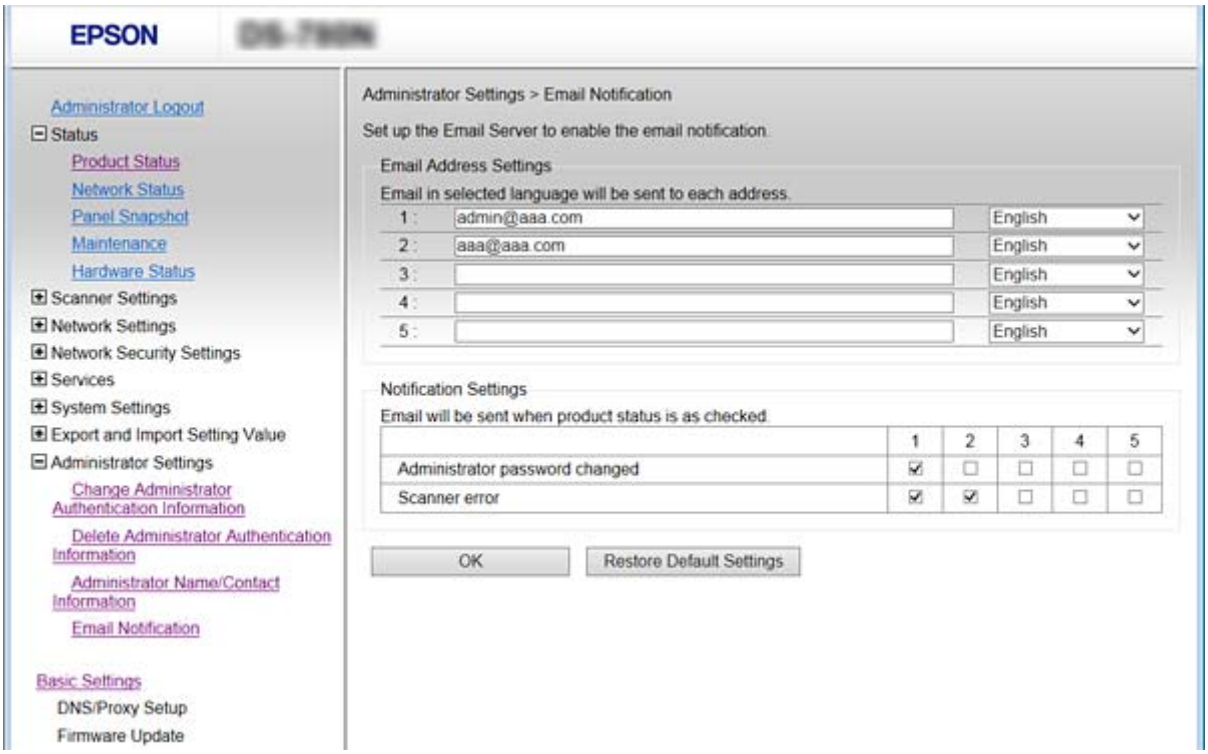
➡ „Konfiguration eines Mail-Servers“ auf Seite 42

Konfiguration der E-Mail-Benachrichtigung

Um diese Funktion nutzen zu können, muss ein E-Mail-Server konfiguriert werden.

1. Rufen Sie Web Config auf, und wählen Sie dann **Administratoreinstellungen** > **eMail-Benachrichtigung** aus.
2. Geben Sie eine E-Mail-Adresse ein, unter der Sie E-Mail-Benachrichtigungen erhalten möchten.
3. Wählen Sie die Sprache für die E-Mail-Benachrichtigungen aus.

4. Markieren Sie die Kontrollkästchen für die Benachrichtigungen, die Sie erhalten möchten.



5. Klicken Sie auf **OK**.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23
➡ „Konfiguration eines Mail-Servers“ auf Seite 42

Konfiguration eines Mail-Servers

Prüfen Sie Folgendes vor der Konfiguration.

❏ Der Scanner ist mit einem Netzwerk verbunden.

❏ Die E-Mail-Serverinformationen des Computers.

1. Rufen Sie Web Config auf, und wählen Sie dann **Netzwerkeinstellungen** > **eMail-Server** > **Grundlegend** aus.

2. Geben Sie für jedes Element einen Wert ein.

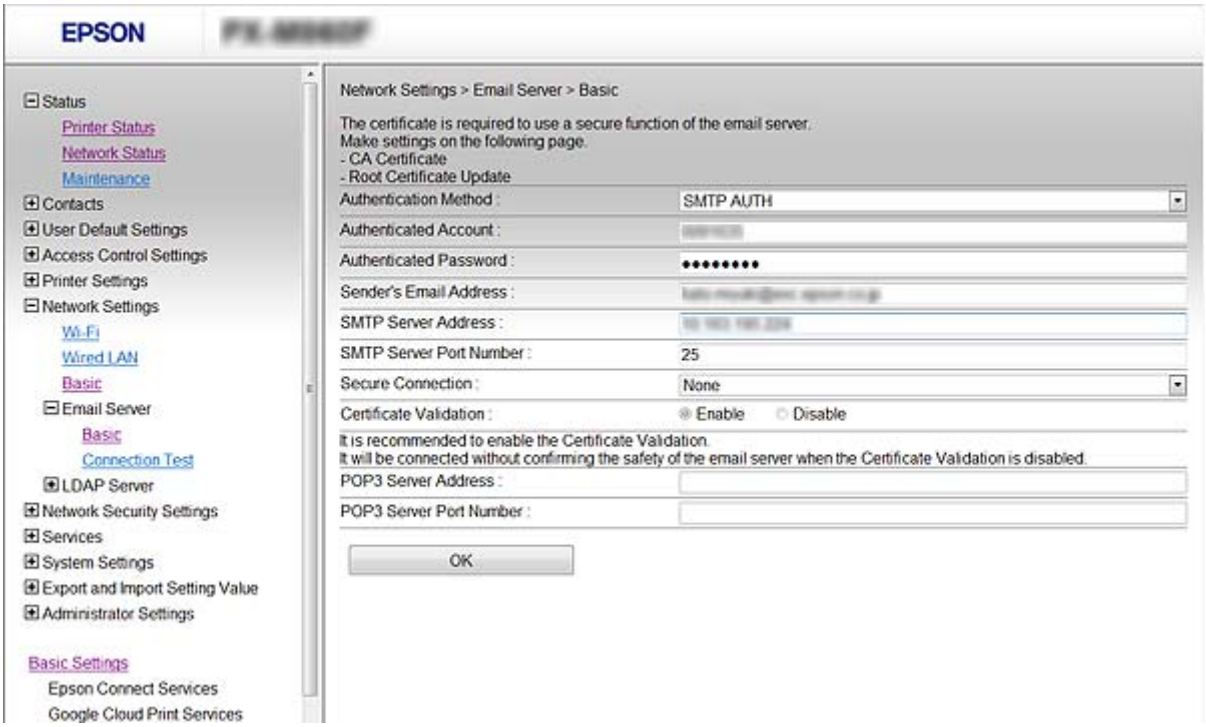
3. Wählen Sie **OK**.

   Die gewählten Einstellungen werden angezeigt.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23
➡ „Einstellungselemente des Mail-Servers“ auf Seite 43

Einstellungselemente des Mail-Servers



Bezeichnung	Einstellungen und Erläuterung	
Authentisierungsmethode	Geben Sie die Authentifizierungsmethode für den Zugriff des Scanners auf den Mail-Server ein.	
	Aus	Die Authentifizierung ist bei der Kommunikation mit dem Mailserver deaktiviert.
	SMTP-Authentisierung	Erfordert, dass der Mailserver die SMTP-Authentifizierung unterstützt.
	POP vor SMTP	Konfigurieren Sie den POP3-Server, wenn Sie diese Methode wählen.
Authentisierungskonto	Wenn Sie **SMTP-Authentisierung** oder **POP vor SMTP** als **Authentisierungsmethode** wählen, geben Sie den authentifizierten Kontonamen bestehend aus 0 bis 255 ASCII-Zeichen (0x20–0x7E) ein.	
Authentisiertes Kennwort	Wenn Sie **SMTP-Authentisierung** oder **POP vor SMTP** als **Authentisierungsmethode** wählen, geben Sie das authentifizierte Passwort aus 0 bis 20 Zeichen A–Z a–z 0–9 ein ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.	
Absender-eMail-Adresse	Geben Sie die E-Mail-Adresse des Absenders ein. Sie können zwischen 0 und 255 ASCII-Zeichen (0x20–0x7E) eingeben, außer : ( ) < > [ ] ; ¥. Das erste Zeichen darf kein Punkt „.“ sein.	
SMTP-Serveradresse	Geben Sie 0 bis 255 Zeichen ein: A–Z a–z 0–9 . - . Sie können IPv4- oder FQDN-Format verwenden.	
SMTP-Serverportnummer	Geben Sie eine Nummer zwischen 1 und 65535 ein.	

Bezeichnung	Einstellungen und Erläuterung	
Sichere Verbindung	Geben Sie die sichere Verbindungsmethode für den E-Mail-Server an.	
	Keine	Wenn Sie **POP vor SMTP** bei **Authentisierungsmethode** wählen, wird die Verbindungsmethode auf **Keine** eingestellt.
	SSL/TLS	Dies ist verfügbar, wenn **Authentisierungsmethode** auf **Aus** oder **SMTP-Authentisierung** eingestellt ist.
	STARTTLS	Dies ist verfügbar, wenn **Authentisierungsmethode** auf **Aus** oder **SMTP-Authentisierung** eingestellt ist.
Zertifikatsvalidierung	Das Zertifikat wird validiert, wenn diese Option aktiviert ist. Wir empfehlen, diese Option auf **Aktivieren** zu setzen.	
POP3-Serveradresse	Falls **POP vor SMTP** als **Authentisierungsmethode** eingegeben wird, geben Sie die POP3-Serveradresse mit zwischen 0 und 255 Zeichen als A–Z a–z 0–9 ein. - . Sie können IPv4- oder FQDN-Format verwenden.	
POP3-Serverportnummer	Falls **POP vor SMTP** für **Authentisierungsmethode** ausgewählt wird, geben Sie eine Zahl zwischen 1 und 65535 Zeichen ein.	

Zugehörige Informationen

➡ „Konfiguration eines Mail-Servers“ auf Seite 42

Prüfen einer Mail-Server-Verbindung

1. Rufen Sie Web Config auf, und wählen Sie dann **Netzwerkeinstellungen** > **eMail-Server** > **Verbindungstest** aus.
2. Wählen Sie **Start**.

   Der Verbindungstest mit dem Mail-Server wird gestartet. Nach dem Test wird der Prüfbericht angezeigt.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23
➡ „Ergebnisse der Mail-Server-Verbindungsprüfung“ auf Seite 44

Ergebnisse der Mail-Server-Verbindungsprüfung

Meldungen	Erläuterung
Verbindungstest war erfolgreich.	Diese Meldung wird bei einer erfolgreichen Verbindung mit dem Server angezeigt.

Betriebs- und Verwaltungseinstellungen

Meldungen	Erläuterung
SMTP-Server-Kommunikationsfehler. Folgendes prüfen. - Netzwerkeinstellungen	Diese Meldung erscheint, wenn ❏ Der Scanner nicht mit einem Netzwerk verbunden ist ❏ Der SMTP-Server abgeschaltet ist ❏ Die Netzwerkverbindung während der Kommunikation getrennt wird ❏ Unvollständige Daten empfangen werden
POP3-Server-Kommunikationsfehler. Folgendes prüfen. - Netzwerkeinstellungen	Diese Meldung erscheint, wenn ❏ Der Scanner nicht mit einem Netzwerk verbunden ist ❏ Der POP3-Server abgeschaltet ist ❏ Die Netzwerkverbindung während der Kommunikation getrennt wird ❏ Unvollständige Daten empfangen werden
Beim Verbinden mit dem SMTP-Server ist ein Fehler aufgetreten. Folgendes prüfen. - SMTP-Serveradresse - DNS-Server	Diese Meldung erscheint, wenn ❏ Die Verbindung zu einem DNS-Server fehlschlägt ❏ Die Namensauflösung für einen SMTP-Server fehlschlägt
Beim Verbinden mit dem POP3-Server ist ein Fehler aufgetreten. Folgendes prüfen. - POP3-Serveradresse - DNS-Server	Diese Meldung erscheint, wenn ❏ Die Verbindung zu einem DNS-Server fehlschlägt ❏ Die Namensauflösung für einen POP3-Server fehlschlägt
SMTP-Server-Authentifizierungs-fehler. Folgendes prüfen. - Authentisierungsmethode - Authentisierungskonto - Authentisiertes Kennwort	Diese Meldung erscheint, wenn die SMTP-Serverauthentifizierung fehlschlägt.
POP3-Server-Authentifizierungs-fehler. Folgendes prüfen. - Authentisierungsmethode - Authentisierungskonto - Authentisiertes Kennwort	Diese Meldung erscheint, wenn die POP3-Serverauthentifizierung fehlschlägt.
Nicht unterstützte Kommunikationsmethode. Folgendes prüfen. - SMTP-Serveradresse - SMTP-Serverportnummer	Diese Meldung erscheint, wenn Sie versuchen, mit nicht unterstützten Protokollen zu kommunizieren.
Verbindung zum SMTP-Server fehlgeschlagen. Sichere Verbindung in Keine ändern.	Diese Meldung erscheint, wenn eine SMTP-Nichtübereinstimmung zwischen einem Server und einem Client auftritt oder wenn der Server keine sichere SMTP-Verbindung (SSL-Verbindung) unterstützt.
Verbindung zum SMTP-Server fehlgeschlagen. Sichere Verbindung in SSL/TLS ändern.	Diese Meldung erscheint, wenn eine SMTP-Nichtübereinstimmung zwischen einem Server und einem Client auftritt oder wenn der Server die Nutzung einer SSL/TLS-Verbindung für eine sichere SMTP-Verbindung anfragt.
Verbindung zum SMTP-Server fehlgeschlagen. Sichere Verbindung in STARTTLS ändern.	Diese Meldung erscheint, wenn eine SMTP-Nichtübereinstimmung zwischen einem Server und einem Client auftritt oder wenn der Server die Nutzung einer STARTTLS-Verbindung für eine sichere SMTP-Verbindung anfragt.
Die Verbindung ist nicht vertrauenswürdig. Folgendes prüfen. - Datum und Zeit	Diese Meldung erscheint, wenn Datums- und Zeiteinstellung des Scanners falsch sind oder das Zertifikat abgelaufen ist.

Meldungen	Erläuterung
Die Verbindung ist nicht vertrauenswürdig. Folgendes prüfen. - CA-Zertifikat	Diese Meldung erscheint, wenn der Scanner kein Stammzertifikat entsprechend dem Server hat oder kein CA-Zertifikat importiert wurde.
Die Verbindung ist nicht vertrauenswürdig.	Diese Meldung erscheint, wenn das bezogene Zertifikat beschädigt ist.
SMTP-Serverauthentifizierung fehlgeschlagen. Authentisierungsmethode in SMTP-Authentisierung ändern.	Diese Meldung erscheint, wenn eine Nichtübereinstimmung der Authentifizierungsmethode zwischen einem Server und einem Client auftritt. Der Server unterstützt SMTP-Authentisierung.
SMTP-Serverauthentifizierung fehlgeschlagen. Authentisierungsmethode in POP vor SMTP ändern.	Diese Meldung erscheint, wenn eine Nichtübereinstimmung der Authentifizierungsmethode zwischen einem Server und einem Client auftritt. Der Server unterstützt SMTP-Authentisierung nicht.
Absender-eMail-Adresse ist falsch. Zur eMail-Adresse für Ihren eMail-Dienst wechseln.	Diese Meldung erscheint, wenn die angegebene E-Mail-Adresse des Absenders falsch ist.
Zugriff auf das Produkt bis zum Abschluss des Vorgangs nicht möglich.	Diese Meldung erscheint, wenn der Scanner ausgelastet ist.

Zugehörige Informationen

➡ „Prüfen einer Mail-Server-Verbindung“ auf Seite 44

Aktualisieren der Firmware

Aktualisieren der Firmware mit Web Config

So aktualisieren Sie die Firmware mit Web Config. Das Gerät muss mit dem Internet verbunden sein.

1. Rufen Sie Web Config auf und wählen Sie **Grundeinstellungen** > **Firmware-Update**.
2. Klicken Sie auf **Start**.

   Die Firmware-Überprüfung beginnt, und die Firmware-Angaben werden angezeigt, falls eine aktualisierte Firmware vorhanden ist.
3. Klicken Sie auf **Start**, und befolgen Sie die Anweisungen am Bildschirm.

Hinweis:
Sie können die Firmware auch mithilfe von Epson Device Admin aktualisieren. In der Geräteliste lassen sich die Firmware-Angaben ablesen. Dies ist nützlich, wenn die Firmware mehrerer Geräte aktualisiert werden soll. Weitere Informationen finden Sie im Epson Device Admin-Handbuch oder in der Hilfe.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

➡ „Epson Device Admin“ auf Seite 55

Aktualisieren der Firmware mit Epson Firmware Updater

Die Firmware für das Gerät lässt sich von der Epson-Website auf den Computer herunterladen, und über eine USB-Verbindung zwischen dem Computer und dem Gerät lässt sich dann dessen Firmware aktualisieren. Falls eine Aktualisierung über das Netzwerk nicht möglich ist, versuchen Sie folgende Methode.

1. Rufen Sie die Epson-Website auf, und laden Sie die Firmware herunter.
2. Verbinden Sie den Computer, auf dem die Firmware gespeichert ist, über ein USB-Kabel mit dem Gerät.
3. Doppelklicken Sie auf die heruntergeladene EXE-Datei.

   Epson Firmware Updater wird gestartet.
4. Folgen Sie der Bildschirmanleitung.

Sichern der Einstellungen

Über die Funktion Exportieren der Einstellungspunkte in Web Config können die Punkte auf andere Scanner übertragen werden.

Einstellungen exportieren

Exportieren Sie einzelne Einstellungen für den Scanner.

1. Rufen Sie Web Config auf, und wählen Sie dann **Einstellungswert exportieren und importieren** > **Exportieren** aus.
2. Wählen Sie die Einstellungen, die Sie exportieren möchten.

   Wählen Sie die Einstellungen, die Sie exportieren möchten. Wenn Sie die übergeordnete Kategorie wählen, werden auch die Unterkategorien ausgewählt. Unterkategorien, die durch Duplikation innerhalb desselben Netzwerks Fehler verursachen (wie IP-Adressen usw.), können jedoch nicht ausgewählt werden.
3. Geben Sie ein Kennwort zur Verschlüsselung der exportierten Datei ein.

   Sie benötigen das Kennwort zum Importieren der Datei. Lassen Sie dieses Feld leer, wenn Sie die Datei nicht verschlüsseln möchten.
4. Klicken Sie auf **Exportieren**.

> ***Wichtig:***
>
> *Wenn Sie die Netzwerkeinstellungen des Scanners wie den Scannernamen und die IP-Adresse exportieren möchten, wählen Sie **Zur Auswahl der individuellen Geräteeinstellungen aktivieren** und dann weitere Elemente. Verwenden Sie nur die ausgewählten Werte für den Scanner.*

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

Einstellungen importieren

Importieren Sie die exportierte Web Config-Datei auf den Scanner.

> ***Wichtig:***
> *Beim Importieren von Werten, die individuelle Informationen, wie einen Scannernamen oder eine IP-Adresse enthalten, achten Sie darauf, dass die IP-Adresse nicht bereits im Netzwerk existiert. Falls die IP-Adresse bereits vorhanden ist, reflektiert der Scanner den Wert nicht.*

1. Rufen Sie Web Config auf, und wählen Sie dann **Einstellungswert exportieren und importieren** > **Importieren** aus.
2. Wählen Sie die exportierte Datei, geben Sie dann das Verschlüsselungskennwort ein.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie das Laufwerk, das Sie einbinden möchten, klicken Sie dann auf **Weiter**.
5. Klicken Sie auf **OK**.

Die Einstellungen werden auf den Scanner angewandt.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

Problemlösung

Tipps zur Problemlösung

In folgendem Handbuch finden Sie weitere Informationen.

❏ Benutzerhandbuch

Bietet Anleitungen zur Scannerverwendung, Wartung und Problemlösung.

Auswerten des Protokolls für Server und Netzwerkgerät

Bei Problemen mit der Netzwerkverbindung besteht die Möglichkeit, die Ursache anhand des Protokolls des Mailservers, LDAP-Servers usw. zu ermitteln oder den Status anhand des Netzwerkprotokolls und von Befehlen der Systemgeräte wie z. B. Router zu ermitteln.

Initialisieren der Netzwerkeinstellungen

Wiederherstellen der Netzwerkeinstellungen im Bedienfeld

Sie können alle Netzwerkeinstellungen auf die Standardeinstellungen zurücksetzen.

1. Tippen Sie auf dem Startbildschirm auf **Einstellungen**.
2. Tippen Sie auf **Systemadministration** > **Werkseinstlg. wiederh.** > **Netzwerkeinstellungen**.
3. Prüfen Sie die Meldung und tippen Sie dann auf **Ja**.
4. Wenn eine Abschlussmeldung angezeigt wird, tippen Sie auf **schließen**.

   Der Bildschirm wird automatisch nach einer bestimmten Zeit geschlossen, solange Sie nicht auf **schließen** tippen.

Prüfen der Kommunikation zwischen Geräten und Computer

Prüfen der Verbindung mit dem Ping-Befehl — Windows

Mit dem Ping-Befehl kann geprüft werden, ob der Computer mit dem Scanner verbunden ist. Befolgen Sie die nachfolgenden Schritte, um die Verbindung mit dem Ping-Befehl zu prüfen.

1. Prüfen Sie die Scanner-IP-Adresse für die Verbindung, die Sie prüfen möchten.

   Sie können diese Überprüfung mit Epson Scan 2 durchführen.

2. Öffnen Sie den Eingabeaufforderungs-Bildschirm des Computers.

   ❏ Windows 10

   Klicken Sie mit der rechten Maustaste auf die Startschaltfläche, halten Sie sie gedrückt und wählen Sie dann **Befehlszeile** aus.

   ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012

   Öffnen Sie den Anwendungsbildschirm und wählen Sie dann **Eingabeaufforderung**.

   ❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 oder früher

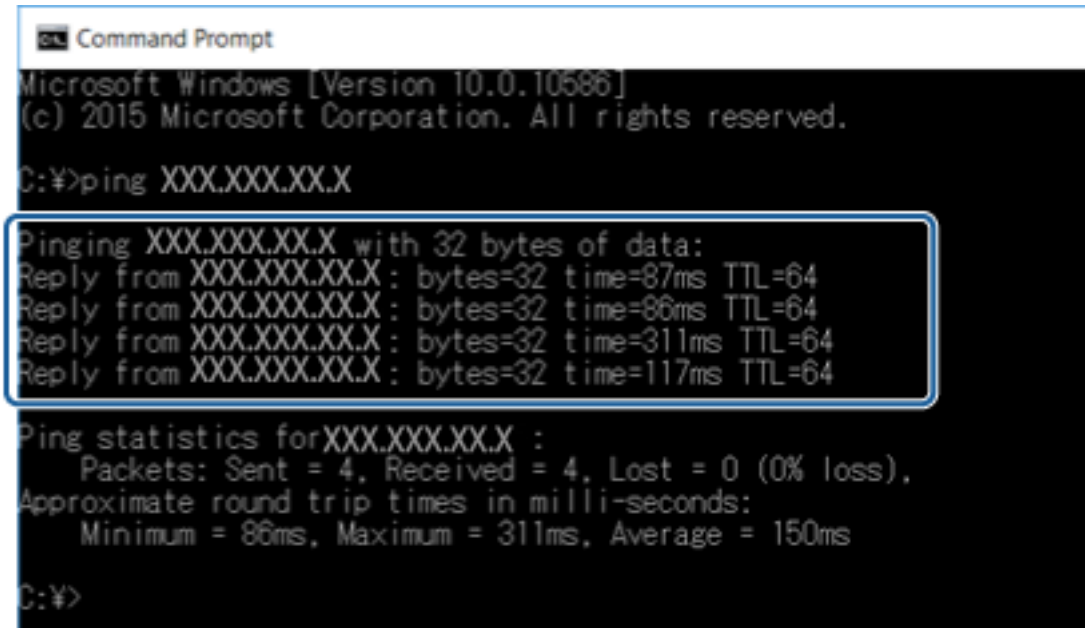
   Klicken Sie auf die Schaltfläche Start und wählen Sie dann **Alle Programme** oder **Programme** > **Zubehör** > **Eingabeaufforderung**.

3. Geben Sie „Ping xxx.xxx.xxx.xxx“ ein und drücken Sie dann die Eingabetaste.

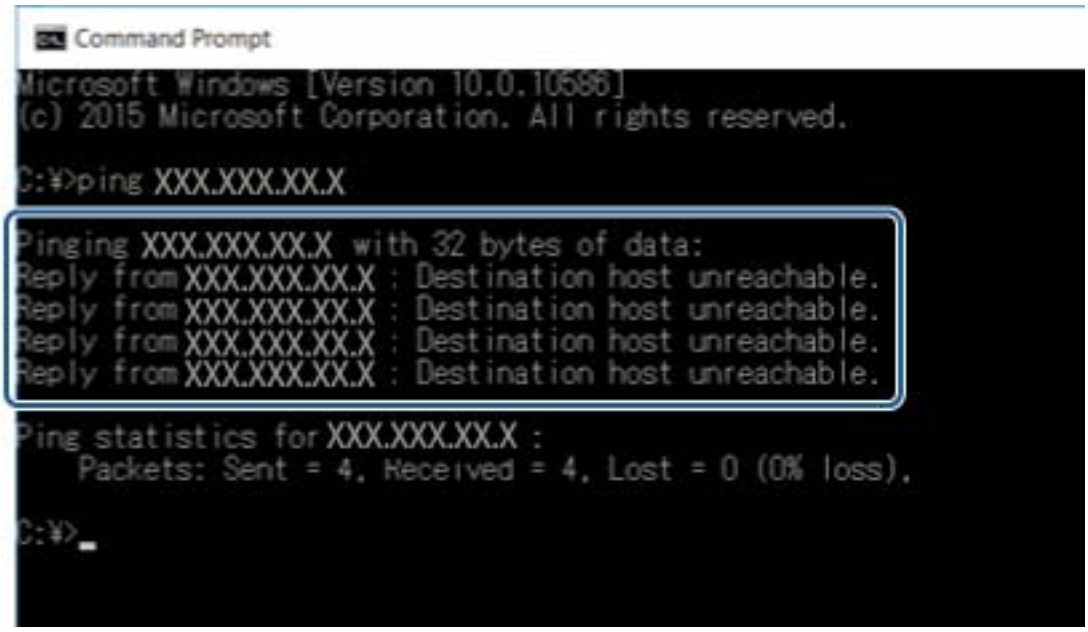
   Geben Sie die Scanner-IP-Adresse für xxx.xxx.xxx.xxx ein.

4. Prüfen Sie den Kommunikationsstatus.

   Wenn Scanner und Computer kommunizieren, wird die folgende Meldung angezeigt.



Wenn Scanner und Computer nicht kommunizieren, wird die folgende Meldung angezeigt.



Prüfen der Verbindung mit dem Ping-Befehl — Mac OS

Mit dem Ping-Befehl kann geprüft werden, ob der Computer mit dem Scanner verbunden ist. Befolgen Sie die nachfolgenden Schritte, um die Verbindung mit dem Ping-Befehl zu prüfen.

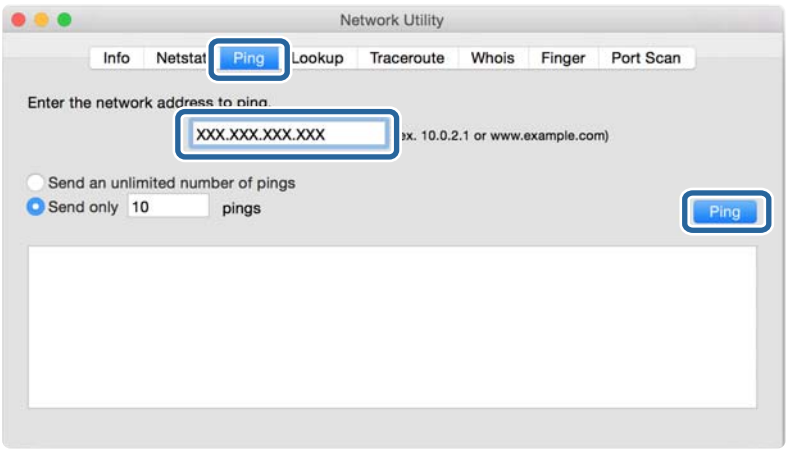
1. Prüfen Sie die Scanner-IP-Adresse für die Verbindung, die Sie prüfen möchten.

   Sie können diese Überprüfung mit Epson Scan 2 durchführen.

2. Starten Sie Network Utility.

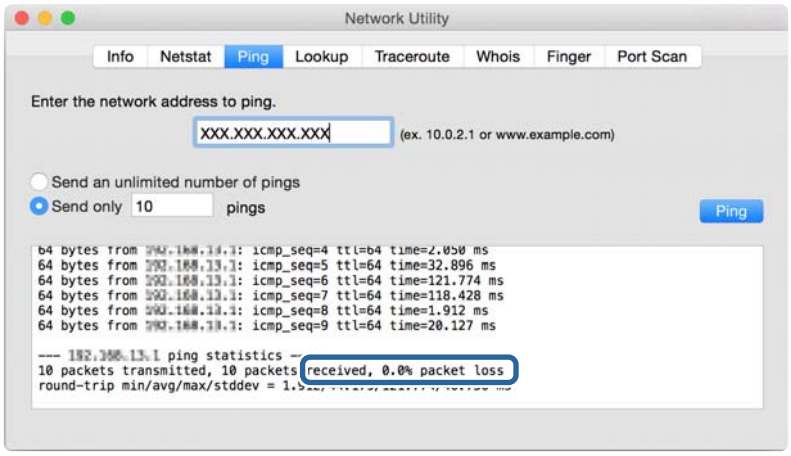
   Geben Sie „Network Utility“ in **Spotlight** ein.

3. Klicken Sie auf die Registerkarte **Ping**, geben Sie die in Schritt 1 geprüfte IP-Adresse ein und klicken Sie dann auf **Ping**.

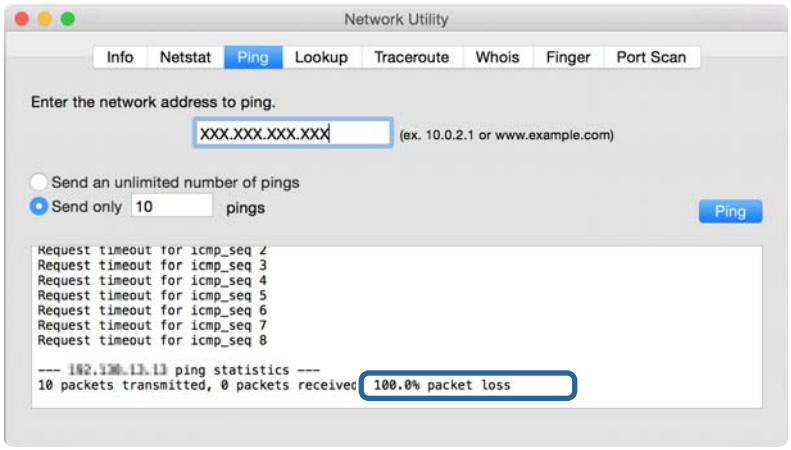


4. Prüfen Sie den Kommunikationsstatus.

   Wenn Scanner und Computer kommunizieren, wird die folgende Meldung angezeigt.



   Wenn Scanner und Computer nicht kommunizieren, wird die folgende Meldung angezeigt.



Probleme bei der Verwendung von Netzwerksoftware

„Web Config“ kann nicht aufgerufen werden

Ist die IP-Adresse des Scanners richtig konfiguriert?

Konfigurieren Sie die IP-Adresse mit Epson Device Admin oder EpsonNet Config.

Unterstützt Ihr Browser die Batchverschlüsselungen als Verschlüsselungsstärke für SSL/TLS?

Die Batchverschlüsselungen als Verschlüsselungsstärke für SSL/TLS sind wie folgt. Web Config kann nur in einem Browser aufgerufen werden, der die folgenden Batchverschlüsselungen unterstützt. Prüfen Sie die Verschlüsselungsunterstützung des Browsers.

- ❏ 80-Bit: AES256/AES128/3DES
- ❏ 112-Bit: AES256/AES128/3DES
- ❏ 128-Bit: AES256/AES128

❏ 192-Bit: AES256

❏ 256-Bit: AES256

Beim Aufrufen von Web Config mit SSL-Kommunikation (https) erscheint die Meldung „Abgelaufen“.

Wenn das Zertifikat abgelaufen ist, beziehen Sie das Zertifikat erneut. Wenn die Meldung vor dem Ablaufdatum angezeigt wird, achten Sie darauf, dass das Scannerdatum richtig eingestellt ist.

Beim Aufrufen von Web Config mit SSL-Kommunikation (https) erscheint die Meldung „Der Name des Sicherheitszertifikats stimmt nicht…“.

Die für **Allgemeiner Name** eingegebene Scanner-IP-Adresse zur Erstellung eines selbstsignierten Zertifikats oder eines CSR stimmt nicht mit der in den Browser eingegebenen Adresse überein. Beziehen und importieren Sie erneut ein Zertifikat oder ändern Sie den Scannernamen.

Auf den Scanner wird über einen Proxyserver zugegriffen.

Wenn Sie mit dem Scanner einen Proxyserver verwenden, müssen die Proxyeinstellungen des Browsers konfiguriert werden.

❏ Windows:

Wählen Sie **Systemsteuerung** > **Netzwerk und Freigabecenter** > **Internetoptionen** > **Verbindungen** > **LAN-Einstellungen** > **Proxyserver** und legen Sie dann fest, dass der Proxyserver für lokale Adressen nicht verwendet werden soll.

❏ Mac OS:

Wählen Sie **Systemeinstellungen** > **Netzwerk** > **Weitere Optionen** > **Proxies** und registrieren Sie dann die lokale Adresse für **Proxy-Einstellungen für diese Hosts und Domains nicht verwenden**.

Beispiel:

192.168.1.*: Lokale Adresse 192.168.1.XXX, Teilnetzmaske 255.255.255.0

192.168.*.*: Lokale Adresse 192.168.XXX.XXX, Teilnetzmaske 255.255.0.0

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

➡ „Zuweisen der IP-Adresse“ auf Seite 15

➡ „Zuweisen von IP-Adressen mithilfe von EpsonNet Config“ auf Seite 56

Modellname und/oder IP-Adresse werden in EpsonNet Config nicht angezeigt

Haben Sie bei Anzeige des Windows-Sicherheits- oder Firewall-Bildschirms Blockieren, Abbrechen oder Herunterfahren gewählt?

Wenn Sie **Blockieren**, **Abbrechen** oder **Herunterfahren** wählen, werden IP-Adresse und Modellname in EpsonNet Config oder EpsonNet Setup nicht angezeigt.

Um dies zu korrigieren, registrieren Sie EpsonNet Config in der Windows-Firewall und in handelsüblicher Sicherheitssoftware als Ausnahme. Wenn Sie ein Antivirus- oder Sicherheitsprogramm verwenden, schließen Sie es und versuchen Sie dann, EpsonNet Config zu verwenden.

Ist die Einstellung für die Kommunikationszeitüberschreitung zu kurz?

Rufen Sie EpsonNet Config auf, wählen Sie **Tools** > **Options** > **Timeout** und verlängern Sie die Zeitspanne für die Einstellung **Communication Error**. Beachten Sie, dass EpsonNet Config daraufhin ggf. langsamer ausgeführt wird.

Zugehörige Informationen

➡ „Ausführen von EpsonNet Config — Windows“ auf Seite 56

➡ „Ausführen von EpsonNet Config — Mac OS“ auf Seite 56

Anhang

Einleitung zur Netzwerksoftware

Im Folgenden wird die Software für das Konfigurieren und Verwalten von Geräten beschrieben.

Epson Device Admin

Epson Device Admin ist eine Anwendung, die es Ihnen ermöglicht, Geräte im Netzwerk zu installieren und die Geräte anschließend zu konfigurieren und zu verwalten. Sie können Einzelheiten für Geräte abrufen, beispielsweise den Status und den Stand des Verbrauchsmaterials, Benachrichtigungen über Warnungen versenden, und Berichte über die Gerätenutzung erstellen. Sie können auch eine Vorlage mit Einstellungspunkten erstellen und diese dann auf andere Geräte als freigegebene Einstellungen anwenden. Sie können Epson Device Admin von der Epson-Supportwebsite herunterladen. Weitere Informationen finden Sie in der Dokumentation oder Hilfe von Epson Device Admin.

Ausführen von Epson Device Admin (nur Windows)

Wählen Sie **Alle Programme** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

Hinweis:
Wenn die Firewall-Warnung angezeigt wird, erlauben Sie den Zugriff für Epson Device Admin.

EpsonNet Config

EpsonNet Config ermöglicht dem Administrator die Konfiguration der Scanner-Netzwerkeinstellungen, wie z. B. Zuweisen einer IP-Adresse und Ändern des Verbindungsmodus. Die Funktion zur Batch-Einstellung ist unter Windows verfügbar. Weitere Informationen finden Sie in der Dokumentation oder Hilfe von EpsonNet Config.

Ausführen von EpsonNet Config — Windows

Wählen Sie **Alle Programme** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

Hinweis:
Wenn die Firewall-Warnung angezeigt wird, erlauben Sie den Zugriff für EpsonNet Config.

Ausführen von EpsonNet Config — Mac OS

Wählen Sie **Gehe zu** > **Programme** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config** aus.

EpsonNet SetupManager

EpsonNet SetupManager ist ein Programm zum Erstellen eines Pakets für die einfache Scannerinstallation, wie z. B. Installieren des Scannertreibers und Installieren von Document Capture Pro. Dieses Programm ermöglicht es dem Administrator, einmalige Softwarepakete zu erstellen und unter den Gruppen zu verteilen.

Besuchen Sie zu weiteren Informationen Ihre regionale Epson-Website.

Zuweisen von IP-Adressen mithilfe von EpsonNet Config

So weisen Sie mit EpsonNet Config dem Scanner eine IP-Adresse zu. EpsonNet Config ermöglicht es, Scannern eine IP-Adresse zuzuweisen, denen nach dem Anschluss über ein Ethernet-Kabel noch keine Adresse zugewiesen wurde.

Zuweisen von IP-Adressen mithilfe von Batch-Einstellungen

Erstellen der Datei für Batcheinstellungen

Mithilfe der MAC-Adresse und dem Modellnamen als Schlüssel lässt sich eine neue SYLK-Datei zum Einstellen der IP-Adresse erstellen.

1. Öffnen Sie eine Spreadsheet-Anwendung (z. B. Microsoft Excel) oder einen Texteditor.

2. Geben Sie in der ersten Zeile „Info_MACAddress“, „Info_ModelName“ und „TCPIP_IPAddress“ als Spaltentitel für die Einstellungspunkte ein.

   Geben Sie für folgende Zeichenfolgen Einstellungswerte ein. Dabei wird zwischen Groß/Kleinschreibung und Doppelbyte/Singlebyte-Zeichen unterschieden. Wenn nur ein Zeichen unterschiedlich ist, wird der Punkt nicht erkannt.

   Geben Sie den Namen des Einstellungspunkts wie unten beschrieben ein; andernfalls kann EpsonNet Config den Einstellungspunkt nicht erkennen.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. Geben Sie MAC-Adresse, Modellnamen und IP-Adresse für jede Netzwerkschnittstelle ein.

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. Geben Sie einen Namen ein, und speichern Sie die SYLK-Datei (*.slk).

Vornehmen von Batcheinstellungen mithilfe einer Konfigurationsdatei

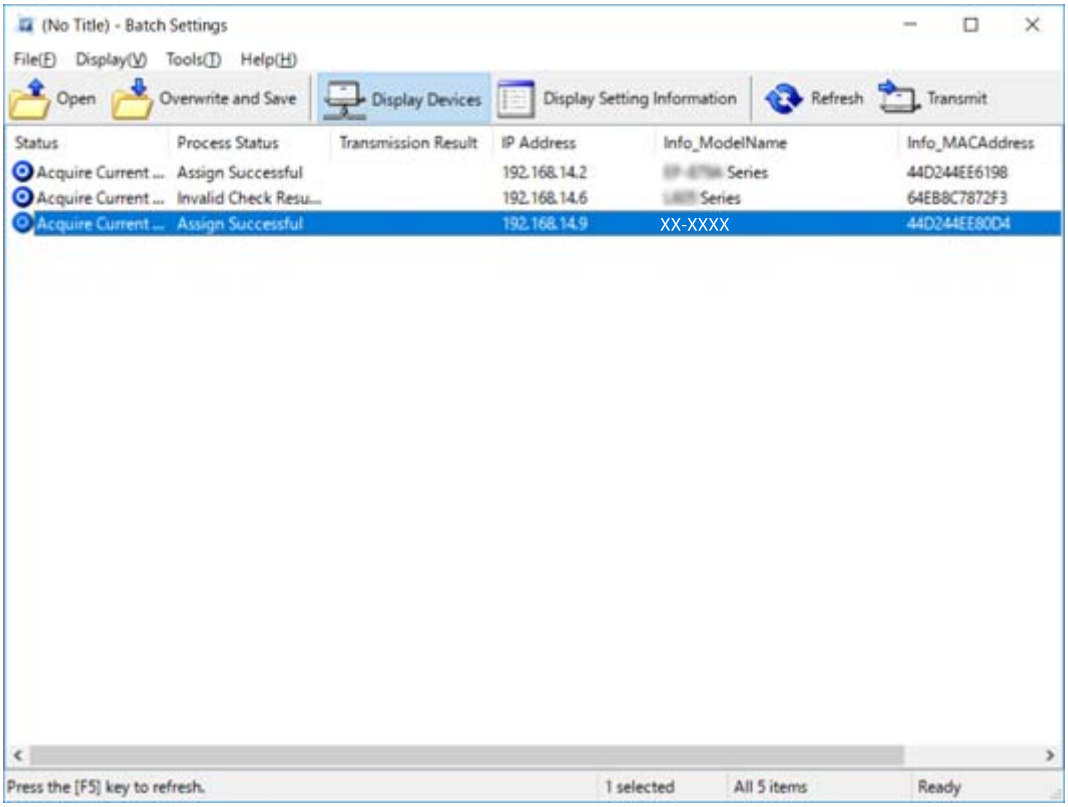
So nehmen Sie mehrere IP-Adresszuweisungen auf einmal über eine Konfigurationsdatei (SYLK-Datei) vor. Die Konfigurationsdatei muss vor der Zuweisung erstellt werden.

1. Verbinden Sie alle Geräte über Ethernetkabel mit dem Netzwerk.
2. Schalten Sie den Scanner ein.
3. Starten Sie EpsonNet Config.

   Eine Liste der Scanner im Netzwerk wird angezeigt. Es kann einige Zeit dauern, bis die Liste angezeigt wird.
4. Klicken Sie auf **Tools** > **Batch Settings**.
5. Klicken Sie auf **Open**.
6. Wählen Sie im Dateiauswahlbildschirm die SYLK file (*.slk) mit den Einstellungen aus, und klicken Sie dann auf **Open**.

7. Wählen Sie die Geräte aus, die über die Batcheinstellungen konfiguriert werden und bei denen die Spalte **Status** auf **Unassigned** steht und der **Process Status** auf **Assign Successful**.

   Um eine Mehrfachauswahl vorzunehmen, drücken Sie die Strg- oder Umschalttaste, und klicken bzw. ziehen Sie mit der Maus.



8. Klicken Sie auf **Transmit**.

9. Wenn der Kennworteingabebildschirm angezeigt wird, geben Sie das Kennwort ein, und klicken Sie auf **OK**.

   Übertragen Sie die Einstellungen.

   Hinweis:
   Die Daten werden über die Netzwerkkarte übertragen, bis der Verlaufsbalken durchgelaufen ist. Schalten Sie das Gerät oder den WLAN-Adapter nicht ab, und senden Sie keine Daten an das Gerät.

10. Klicken Sie auf dem Bildschirm **Transmitting Settings** auf **OK**.

11. Prüfen Sie den Status der eingestellten Geräte.

    Überprüfen Sie bei Geräten, die als  oder  angezeigt werden, den Inhalt der Einstellungsdatei oder auch, ob das Gerät einen normalen Neustart durchlaufen hat.

Symbol	Status	Process Status	Erläuterung
	Setup Complete	Setup Successful	Die Einrichtung wurde normal abgeschlossen.
	Setup Complete	Rebooting	Nachdem die Daten übertragen wurden, müssen die einzelnen Geräte neu starten, damit die Einstellungen angewendet werden. Es wird geprüft, ob eine Verbindung zu dem Gerät nach dem Neustart durchgeführt werden kann.
	Setup Complete	Reboot Failed	Gerät konnte nach der Übertragung der Einstellungen nicht überprüft werden. Überprüfen Sie, ob das Gerät eingeschaltet ist bzw. den Neustart normal abgeschlossen hat.
	Setup Complete	Searching	Das in der Einstellungsdatei angegebene Gerät wird gesucht.*
	Setup Complete	Search Failed	Eine Überprüfung von bereits eingerichteten Geräten ist nicht möglich. Überprüfen Sie, ob das Gerät eingeschaltet ist bzw. den Neustart normal abgeschlossen hat.*

    * Nur, wenn Einstellungsdaten angezeigt werden.

Zugehörige Informationen

➡ „Ausführen von EpsonNet Config — Windows“ auf Seite 56

➡ „Ausführen von EpsonNet Config — Mac OS“ auf Seite 56

Zuweisen einer IP-Adresse an jedes Gerät

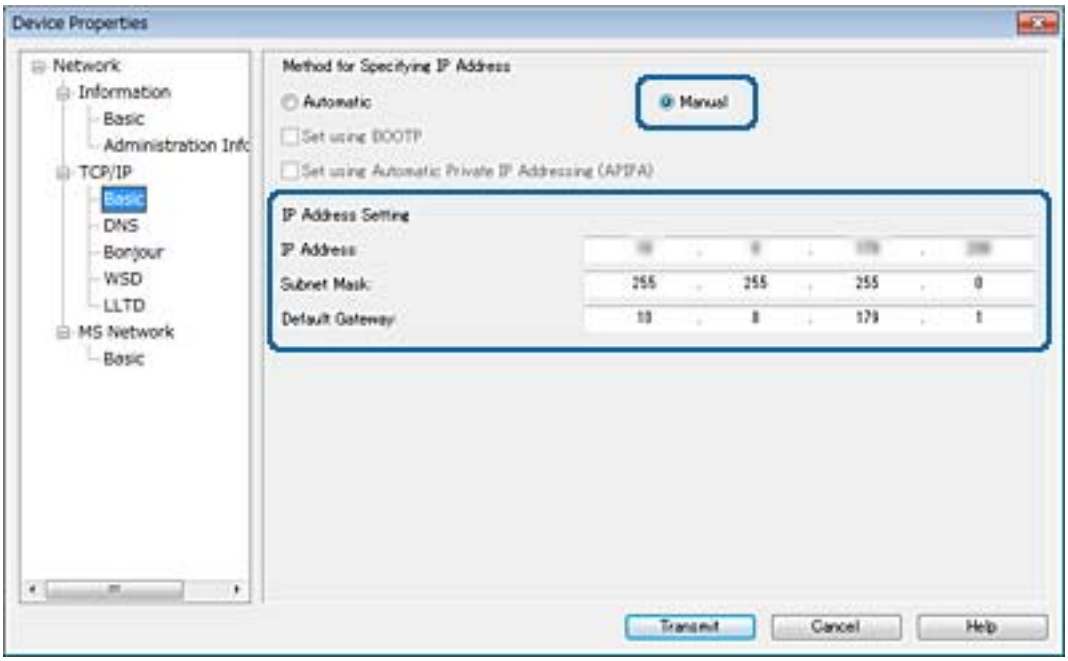
So weisen Sie dem Scanner mit EpsonNet Config eine IP-Adresse zu.

1. Schalten Sie den Scanner ein.
2. Verbinden Sie den Scanner mit einem Ethernetkabel mit dem Netzwerk.
3. Starten Sie EpsonNet Config.

   Eine Liste der Scanner im Netzwerk wird angezeigt. Es kann einige Zeit dauern, bis die Liste angezeigt wird.
4. Doppelklicken Sie auf den Scanner, für den die Zuweisung gelten soll.

   Hinweis:
   Falls mehrere Scanner des gleichen Modells angeschlossen wurden, können einzelne Scanner über ihre MAC-Adresse unterschieden werden.
5. Wählen Sie **Network** > **TCP/IP** > **Basic**.

6. Geben Sie die Adressen für **IP Address**, **Subnet Mask**, und **Default Gateway** ein.



Hinweis:
Geben Sie eine statische Adresse ein, wenn der Scanner an ein sicheres Netzwerk angeschlossen wird.

7. Klicken Sie auf **Transmit**.

   Der Bildschirm mit der Übertragungsbestätigung der Daten wird angezeigt.

8. Klicken Sie auf **OK**.

   Der Bildschirm mit dem Übertragungsabschluss wird angezeigt.

   Hinweis:
   Die Daten werden an das Gerät übermittelt, und dann wird die Meldung „Konfiguration erfolgreich abgeschlossen“ angezeigt. Schalten Sie das Gerät nicht aus, und senden Sie keine Daten an den Dienst.

9. Klicken Sie auf **OK**.

Zugehörige Informationen

➡ „Ausführen von EpsonNet Config — Windows“ auf Seite 56
➡ „Ausführen von EpsonNet Config — Mac OS“ auf Seite 56

Verwendeter Scannerport

Der Scanner verwendet folgenden Port. Diese Ports sollten vom Netzwerkadministrator falls erforderlich freigeschaltet werden.

Anhang

Absender (Client)	Aktivieren	Ziel (Server)	Protokoll	Portnummer
Scanner	E-Mail senden (E-Mail-Benachrichtigung)	SMTP-Server	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	POP-before-SMTP-Verbindung (E-Mail-Benachrichtigung)	POP-Server	POP3 (TCP)	110
	Control WSD	Client-Computer	WSD (TCP)	5357
	Suche nach dem Computer, wenn Push-Scan über Document Capture Pro ausgeführt wird	Client-Computer	Netzwerk-Ermittlung über Push-Scan	2968
	Erfassen von Auftragsdaten, wenn Push-Scan über Document Capture Pro ausgeführt wird	Client-Computer	Push-Scan über Netzwerk	2968
Client-Computer	Ermitteln des Scanners von einer Anwendung wie EpsonNet Config oder dem Scannertreiber.	Scanner	ENPC (UDP)	3289
	Ermitteln und Einrichten der MIB-Daten von einer Anwendung wie EpsonNet Config oder dem Scannertreiber.	Scanner	SNMP (UDP)	161
	Suche nach WSD-Scanner	Scanner	WS-Ermittlung (UDP)	3702
	Weiterleitung von Scandaten über Document Capture Pro	Scanner	Network Scan (TCP)	1865

Erweiterte Sicherheitseinstellungen für Unternehmen

In diesem Kapitel werden erweiterte Sicherheitsfunktionen erläutert.

Sicherheitseinstellungen und Gefahrenvermeidung

Wenn ein Gerät mit dem Netzwerk verbunden ist, können Sie von einem entfernten Ort aus darauf zugreifen. Zudem können mehrere Personen gemeinsam das Gerät nutzen, was der Effizienz der Abläufe und dem Komfort zuträglich ist. Dennoch entstehen auf diese Weise auch Risiken durch unbefugten Zugriff, Missbrauch und Datenfälschung. Falls Sie das Gerät in einer Umgebung nutzen, in der Zugang zum Internet besteht, sind die Risiken noch höher.

Um dieses Risiko zu vermeiden, sind Epson-Geräte mit einer Reihe von Sicherheitstechniken ausgestattet.

Richten Sie das Gerät gemäß der Erfordernisse der Betriebsumgebung ein.

Name	Funktionstyp	Einstellungen	Zu vermeiden
SSL/TLS-Kommunikation	Der Kommunikationspfad zwischen Computer und Gerät wird mithilfe der SSL/TLS-Kommunikation verschlüsselt. Der Kommunikationsinhalt über den Browser ist geschützt.	Richten Sie ein CA-Zertifikat auf dem Server ein, das von einer CA (Zertifizierungsstelle) für das Geräte ausgestellt wurde.	Vermeiden Sie das Offenlegen von Einstellungsdaten und übertragenen Daten vom Computer zum Scanner. Der Zugriff auf den Epson-Server im Internet vom Gerät aus kann durch die Verwendung eines Firmware-Updates usw. ebenfalls geschützt werden.
IPsec-/IP-Filter	Es ist möglich, für Daten von einem bestimmten Client oder eines bestimmten Typs die Verbindung zu trennen. Da IPsec die Daten auf Ebene von IP-Paketen (Verschlüsselung und Authentifizierung) schützt, können Sie sicher über ungesicherte Scanprotokolle kommunizieren.	Erstellen Sie eine Basisrichtlinie und individuelle Richtlinien, um den Client oder die Art von Daten festzulegen, die das Gerät verwenden dürfen.	Schützen Sie das Gerät vor unbefugtem Zugriff sowie vor Fälschung und Ausleitung von Kommunikationsdaten.
SNMPv3	Es wurden Funktionen hinzugefügt wie beispielsweise das Überwachen verbundener Geräte im Netzwerk, die Integrität der Daten für das SNMP-Protokoll, Verschlüsselung, Benutzerauthentifizierung usw.	Aktivieren Sie SNMPv3 und stellen Sie dann die Authentifizierungs- und Verschlüsselungsmethode ein.	Achten Sie beim Ändern von Einstellungen über das Netzwerk auf Vertraulichkeit und Zustandsüberwachung.

Name	Funktionstyp	Einstellungen	Zu vermeiden
IEEE802.1X	Erlaubt nur authentifizierten Benutzern die Verwendung des Ethernet. Erlaubt nur berechtigten Nutzern die Verwendung des Geräts.	Authentifizierungseinstellungen für den RADIUS-Server (Authentifizierungsserver).	Schützen Sie das Gerät vor unbefugtem Zugriff.
Einlesen der ID-Karte	Sie können das Gerät benutzen, indem Sie eine ID-Karte an das verbundene Authentifizierungsgerät halten. Die Protokollerfassung für einzelne Benutzer und Geräte sowie die für einzelne Benutzer und Gruppen verfügbaren Geräte und Funktionen können eingeschränkt werden.	Verbinden Sie ein Authentifizierungsgerät mit dem Gerät, und legen Sie im Authentifizierungssystem die entsprechenden Benutzer an.	Unbefugte Nutzung und Spoofing des Geräts verhindern.

Zugehörige Informationen

➡ „SSL/TLS-Kommunikation mit dem Scanner“ auf Seite 63

➡ „Verschlüsselte Kommunikation mit IPsec/IP-Filterung“ auf Seite 71

➡ „Verwenden des SNMPv3-Protokolls“ auf Seite 83

➡ „Verbinden des Scanners mit einem IEEE802.1X-Netzwerk“ auf Seite 85

Einstellungen für Sicherheitsfunktionen

Beim Einrichten von IPsec/IP-Filtern oder IEEE802.1X wird empfohlen, die Einstellungsdaten über SSL/TLS an Web Config zu übermitteln, um Sicherheitsrisiken wie ein Ausspähen oder Fälschen zu vermeiden.

SSL/TLS-Kommunikation mit dem Scanner

Wenn das Server-Zertifikat für die Kommunikation mit dem Scanner mit SSL/TLS (Secure Sockets Layer/ Transport Layer Security) verwendet wird, lässt sich der Kommunikationsweg zwischen Computern verschlüsseln. Verwenden Sie diese Funktion, um einen insbesondere unbefugten Fernzugriff zu verhinden.

Über digitale Zertifizierung

❏ Von einer CA signiertes Zertifikat

Ein von einer CA (Certificate Authority, Zertifizierungsbehörde) signiertes Zertifikat muss von einer Zertifizierungsbehörde bezogen werden. Die Verwendung eines CA-signierten Zertifikats gewährleistet eine sichere Kommunikation. Sie können ein CA-signiertes Zertifikat für jede Sicherheitsfunktion verwenden.

❏ CA-Zertifikat

Ein CA-Zertifikat bedeutet, dass die Identität eines Servers von einem Drittanbieter geprüft worden ist. Dies ist ein wichtiger Bestandteil des Sicherheitsmodells „Web of Trust“ (Vertrauenswürdiges Netz). Ein CA-Zertifikat zur Serverauthentifizierung muss von einer CA bezogen werden, die es ausstellt.

❏ Selbstsigniertes Zertifikat

Ein selbstsigniertes Zertifikat wird vom Scanner ausgestellt und gleich signiert. Ein solches Zertifikat ist unzuverlässig und kann Spoofing nicht verhindern. Wenn Sie dieses Zertifikat für ein SSL/TLS-Zertifikat verwenden, wird in einem Browser ggf. eine Sicherheitswarnung angezeigt. Sie können dieses Zertifikat nur für eine SSL/TLS-Kommunikation einsetzen.

Zugehörige Informationen

➡ „Erhalten und Importieren eines CA-signierten Zertifikats“ auf Seite 64

➡ „Löschen eines CA-signierten Zertifikats“ auf Seite 68

➡ „Aktualisieren eines selbstsignierten Zertifikats“ auf Seite 68

Erhalten und Importieren eines CA-signierten Zertifikats

Erhalten eines CA-signierten Zertifikats

Um ein CA-signiertes Zertifikat zu erhalten, erstellen Sie einen Zertifikatsantrag (CSR, Certificate Signing Request) und senden ihn an die Zertifizierungsbehörde. Sie können einen CSR mit Web Config und einem Computer erstellen.

Führen Sie zur Erstellung eines CSR und zum Erhalten eines CA-signierten Zertifikats mit Web Config die folgenden Schritte aus. Wenn Sie einen CSR mit Web Config erstellen, erhält das Zertifikat das PEM/DER-Format.

1. Rufen Sie Web Config auf, und wählen Sie dann **Netzwerksicherheitseinstellungen** aus. Wählen Sie als nächstes **SSL/TLS** > **Zertifikat** oder **IPsec/IP-Filterung** > **Client-Zertifikat** oder **IEEE802.1X** > **Client-Zertifikat** aus.

2. Klicken Sie auf **Generieren** von **CSR**.

   Eine Seite zur CSR-Erstellung wird angezeigt.

3. Geben Sie für jedes Element einen Wert ein.

   Hinweis:
   Verfügbare Schlüssellänge und Abkürzungen variieren je nach Zertifizierungsbehörde. Erstellen Sie einen Antrag entsprechend den Regeln der jeweiligen Zertifizierungsbehörde.

4. Klicken Sie auf **OK**.

   Eine Abschlussmeldung wird angezeigt.

5. Wählen Sie **Netzwerksicherheitseinstellungen**. Wählen Sie als nächstes **SSL/TLS** > **Zertifikat** oder **IPsec/IP-Filterung** > **Client-Zertifikat** oder **IEEE802.1X** > **Client-Zertifikat** aus.

6. Klicken Sie entsprechend dem Ausstellungsformat der jeweiligen Zertifizierungsbehörde auf eine der **CSR**-Download-Schaltflächen, um einen CSR auf einen Computer herunterzuladen.

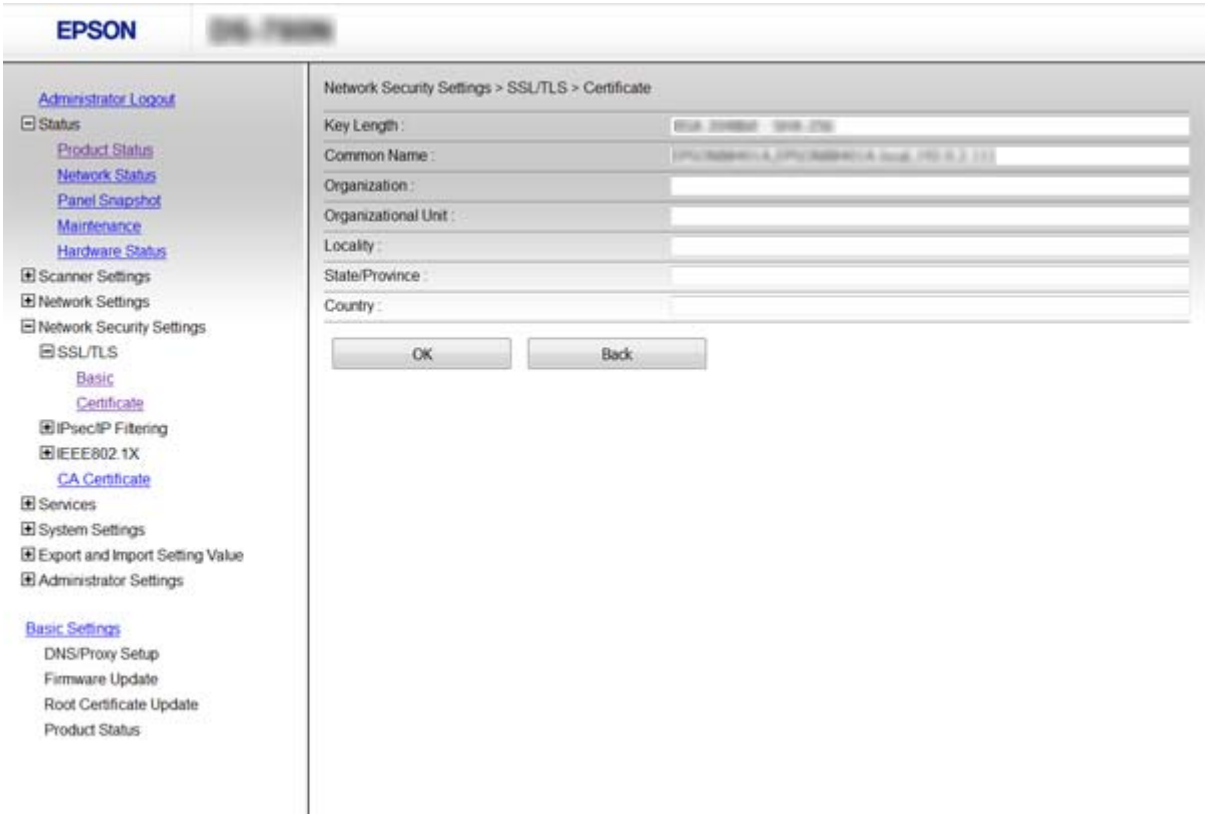
   > ***Wichtig:***
   > *Generieren einen CSR nicht erneut. Andernfalls können Sie ein ausgestelltes CA-signiertes Zertifikat möglicherweise nicht importieren.*

7. Senden Sie den CSR an eine Zertifizierungsbehörde und beziehen Sie ein CA-signiertes Zertifikat.
   Folgen Sie für Sendemethode und -form den Regeln der jeweiligen Zertifizierungsbehörde.
8. Speichern Sie das ausgestellte CA-signiertes Zertifikat auf einem mit dem Scanner verbundenen Computer.
   Der Bezug eines CA-signiertes Zertifikat ist abgeschlossen, wenn Sie das Zertifikat auf einem Ziel speichern.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23
➡ „CSR-Einstellungselemente“ auf Seite 65
➡ „Importieren eines CA-signierten Zertifikats“ auf Seite 66

CSR-Einstellungselemente



Optionen	Einstellungen und Erläuterung
Schlüssellänge	Wählen Sie eine Schlüssellänge für einen CSR.
Allgemeiner Name	Es können zwischen 1 und 128 Zeichen eingegeben werden. Bei einer IP-Adresse sollte dies eine statische IP-Adresse sein. Beispiel: URL für den Aufruf von Web Config: https://10.152.12.225 Common-Name: 10.152.12.225
Organisation/ Organisationseinheit/ Ort/ Staat/Bundesland	Es können zwischen 0 und 64 ASCII-Zeichen (0x20–0x7E) eingegeben werden. Mehrere Namen können durch Kommas getrennt werden.

Optionen	Einstellungen und Erläuterung
Land	Geben Sie einen zweistelligen Ländercode nach ISO-3166 ein.

Zugehörige Informationen

➡ „Erhalten eines CA-signierten Zertifikats“ auf Seite 64

Importieren eines CA-signierten Zertifikats

Wichtig:

❏ *Achten Sie darauf, dass Datum und Uhrzeit des Scanners richtig eingestellt sind.*

❏ *Wenn Sie ein Zertifikat beziehen, das mit einem in Web Config erstellten CSR beantragt worden ist, können Sie ein Zertifikat einmal importieren.*

1. Rufen Sie Web Config auf, und wählen Sie dann **Netzwerksicherheitseinstellungen** aus. Wählen Sie als nächstes **SSL/TLS** > **Zertifikat** oder **IPsec/IP-Filterung** > **Client-Zertifikat** oder **IEEE802.1X** > **Client-Zertifikat** aus.

2. Klicken Sie auf **Importieren**.

   Eine Seite zum Importieren eines Zertifikats wird angezeigt.

3. Geben Sie für jedes Element einen Wert ein.

   Die erforderlichen Einstellungen variieren je nach Ort der CSR-Erstellung und Dateiformat des Zertifikats. Geben Sie die Werte für die erforderlichen Elemente den folgenden Punkten entsprechend ein.

   ❏ Ein Zertifikat im PEM/DER-Format erhalten von Web Config

      ❏ **Privater Schlüssel**: Nicht konfigurieren, da der Scanner einen privaten Schlüssel enthält.

      ❏ **Kennwort**: Nicht konfigurieren.

      ❏ **CA-Zertifikat 1**/**CA-Zertifikat 2**: Optional

   ❏ Ein Zertifikat im PEM/DER-Format erhalten von einem Computer

      ❏ **Privater Schlüssel**: Muss eingestellt werden.

      ❏ **Kennwort**: Nicht konfigurieren.

      ❏ **CA-Zertifikat 1**/**CA-Zertifikat 2**: Optional

   ❏ Ein Zertifikat im Format PKCS#12 erhalten von einem Computer

      ❏ **Privater Schlüssel**: Nicht konfigurieren.

      ❏ **Kennwort**: Optional

      ❏ **CA-Zertifikat 1**/**CA-Zertifikat 2**: Nicht konfigurieren.

4. Klicken Sie auf **OK**.

   Eine Abschlussmeldung wird angezeigt.

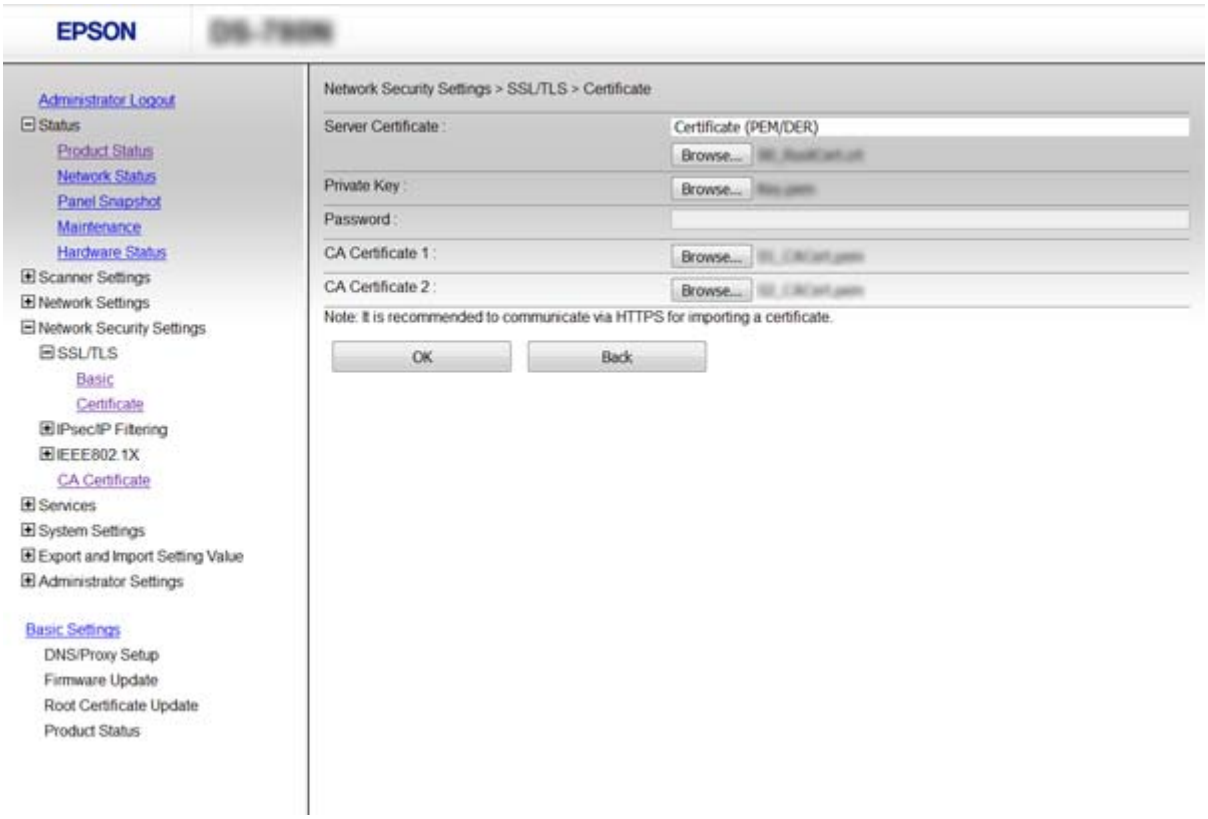
Hinweis:
*Klicken Sie auf **Bestätigen**, um die Zertifikatsdaten zu prüfen.*

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

➡ „Importeinstellungselemente für CA-signiertes Zertifikat“ auf Seite 67

Importeinstellungselemente für CA-signiertes Zertifikat



Bezeichnung	Einstellungen und Erläuterung
Serverzertifikat oder Client-Zertifikat	Wählen Sie ein Zertifikatsformat.
Privater Schlüssel	Wenn Sie ein mit einem computererstellten CSR beantragtes Zertifikat im PEM/DER-Format beziehen, geben Sie eine zu dem Zertifikat passende Privatschlüsseldatei ein.
Kennwort	Geben Sie ein Kennwort zur Verschlüsselung des privaten Schlüssels ein.
CA-Zertifikat 1	Hat Ihr Zertifikat das Format **Zertifikat (PEM/DER)**, importieren Sie ein Zertifikat von einer Zertifizierungsbehörde, die ein Serverzertifikat ausstellt. Geben Sie bei Bedarf eine Datei an.
CA-Zertifikat 2	Hat Ihr Zertifikat das Format **Zertifikat (PEM/DER)**, importieren Sie ein Zertifikat von einer Zertifizierungsbehörde, die ein **CA-Zertifikat 1** ausstellt. Geben Sie bei Bedarf eine Datei an.

Zugehörige Informationen

➡ „Importieren eines CA-signierten Zertifikats“ auf Seite 66

Löschen eines CA-signierten Zertifikats

Sie können ein importiertes Zertifikat löschen, wenn es abgelaufen ist oder eine verschlüsselte Verbindung nicht mehr erforderlich ist.

> ***Wichtig:***
> *Wenn Sie ein Zertifikat beziehen, das mit einem in Web Config erstellten CSR beantragt worden ist, können Sie ein gelöschtes Zertifikat nicht noch einmal importieren. Erstellen Sie in diesem Fall einen CSR und beziehen Sie das Zertifikat erneut.*

1. Rufen Sie Web Config auf, und wählen Sie dann **Netzwerksicherheitseinstellungen** aus. Wählen Sie als nächstes **SSL/TLS** > **Zertifikat** oder **IPsec/IP-Filterung** > **Client-Zertifikat** oder **IEEE802.1X** > **Client-Zertifikat** aus.
2. Klicken Sie auf **Löschen**.
3. Bestätigen Sie, dass Sie das in der Meldung angezeigte Zertifikat löschen möchten.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

Aktualisieren eines selbstsignierten Zertifikats

Wenn der Scanner die HTTPS-Serverfunktion unterstützt, können Sie ein selbstsigniertes Zertifikat aktualisieren. Wenn Sie Web Config mit einem selbstsignierten Zertifikat aufrufen, wird eine Warnmeldung angezeigt.

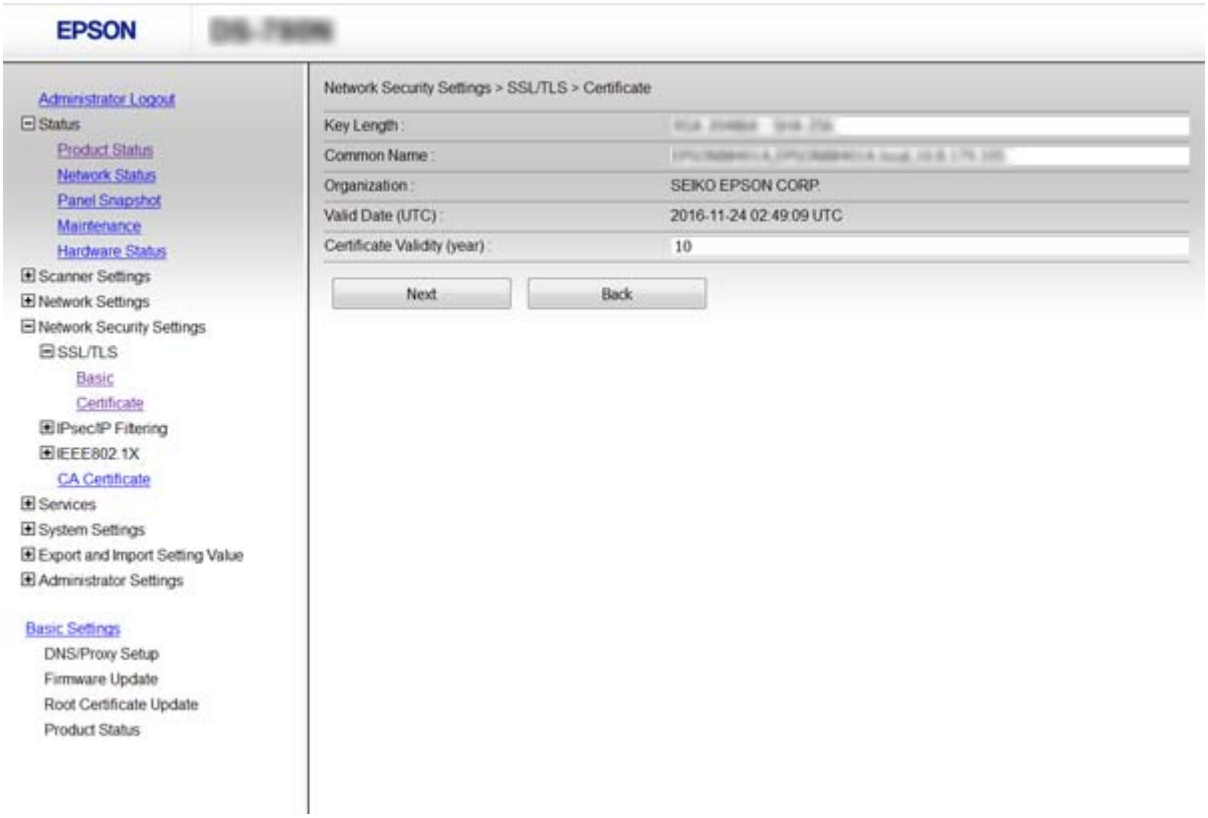
Verwenden Sie ein selbstsigniertes Zertifikat nur vorübergehend, bis Sie ein CA-signiertes Zertifikat erhalten und importiert haben.

1. Rufen Sie Web Config auf, und wählen Sie dann **Netzwerksicherheitseinstellungen** > **SSL/TLS** > **Zertifikat** aus.
2. Klicken Sie auf **Aktualisieren**.
3. Geben Sie **Allgemeiner Name** ein.

   Geben Sie eine IP-Adresse oder einen Indikator wie z. B. einen FQDN-Namen für den Scanner ein. Es können zwischen 1 und 128 Zeichen eingegeben werden.

   Hinweis:
   Verschiedene Namen (CN) können Sie durch Kommas trennen.

4. Geben Sie eine Gültigkeitsdauer für das Zertifikat ein.



5. Klicken Sie auf **Weiter**.

   Eine Bestätigungsmeldung wird angezeigt.

6. Klicken Sie auf **OK**.

   Der Scanner ist aktualisiert.

Hinweis:
*Klicken Sie auf **Bestätigen**, um die Zertifikatsdaten zu prüfen.*

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

CA-Zertifikat konfigurieren

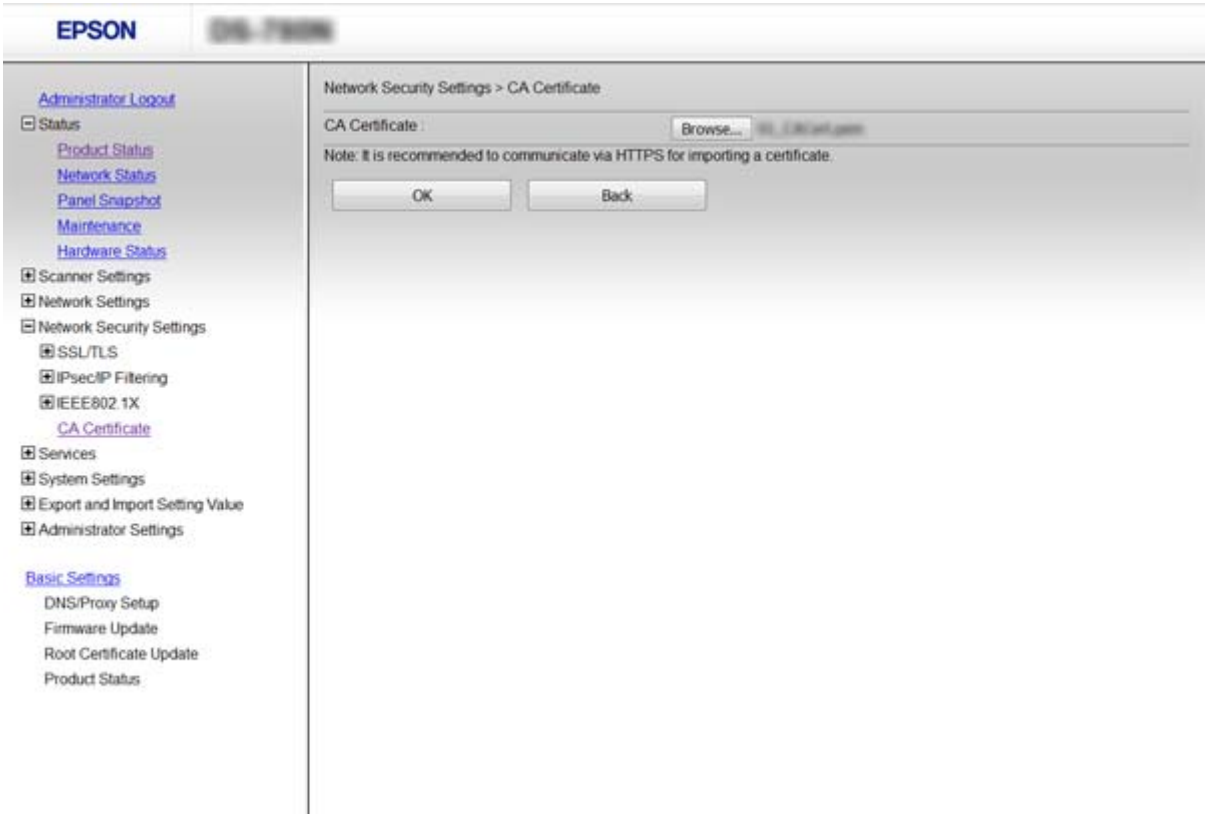
Sie können ein CA-Zertifikat importieren, anzeigen und löschen.

Ein CA-Zertifikat importieren

1. Rufen Sie Web Config auf, und wählen Sie dann **Netzwerksicherheitseinstellungen** > **CA-Zertifikat** aus.

2. Klicken Sie auf **Importieren**.

3. Geben Sie das CA-Zertifikat an, das Sie importieren möchten.



4. Klicken Sie auf **OK**.

Wenn der Import abgeschlossen ist, gelangen Sie zum **CA-Zertifikat**-Bildschirm zurück und das importierte CA-Zertifikat wird angezeigt.

Zugehörige Informationen

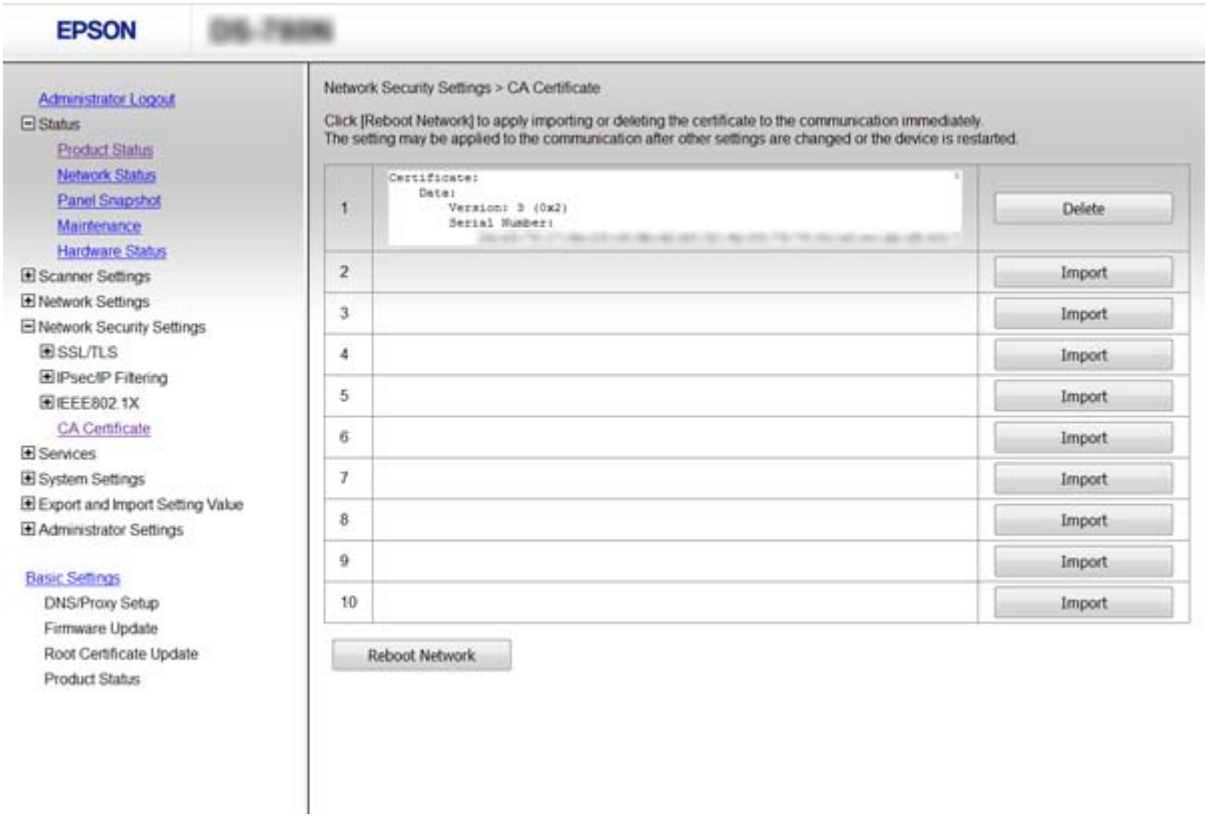
➡ „Aufrufen von Web Config“ auf Seite 23

Ein CA-Zertifikat löschen

Sie können das importierte CA-Zertifikat löschen.

1. Rufen Sie Web Config auf, und wählen Sie dann **Netzwerksicherheitseinstellungen** > **CA-Zertifikat** aus.

2. Klicken Sie auf **Löschen** neben dem CA-Zertifikat, das Sie löschen möchten.



3. Bestätigen Sie, dass Sie das in der Meldung angezeigte Zertifikat löschen möchten.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

Verschlüsselte Kommunikation mit IPsec/IP-Filterung

Über IPsec/IP-Filterung

Wenn der Scanner IPsec/IP-Filterung unterstützt, können Sie den Datenverkehr nach IP-Adressen, Diensten und Anschlüssen filtern. Durch Filterkombinationen können Sie den Scanner so konfigurieren, dass bestimmte Clients oder Daten blockiert oder zugelassen werden. Darüber hinaus können Sie die Sicherheitsstufe durch Verwenden einer IPsec noch weiter erhöhen.

Konfigurieren Sie die Standardrichtlinie, um Datenverkehr zu filtern. Die Standardrichtlinie gilt für jeden Benutzer oder jede Gruppe, die eine Verbindung mit dem Scanner herstellt. Für eine detaillierte Kontrolle von Benutzern oder Benutzergruppen konfigurieren Sie Gruppenrichtlinien. Eine Gruppenrichtlinie vereint eine oder mehrere Regeln, die auf einen Benutzer oder eine Benutzergruppe angewendet werden. Der Scanner kontrolliert IP-Pakete, die auf konfigurierte Richtlinien passen. IP-Pakete werden in der Reihenfolge nach entsprechend der Gruppenrichtlinie 1 bis 10 und dann der Standardrichtlinie authentifiziert.

Hinweis:
Computer mit Windows Vista oder späteren Versionen oder Windows Server 2008 oder späteren Versionen unterstützen IPsec.

Konfigurieren von Standardrichtlinie

1. Rufen Sie Web Config auf, und wählen Sie dann **Netzwerksicherheitseinstellungen** > **IPsec/IP-Filterung** > **Grundlegend** aus.
2. Geben Sie für jedes Element einen Wert ein.
3. Klicken Sie auf **Weiter**.

   Eine Bestätigungsmeldung wird angezeigt.
4. Klicken Sie auf **OK**.

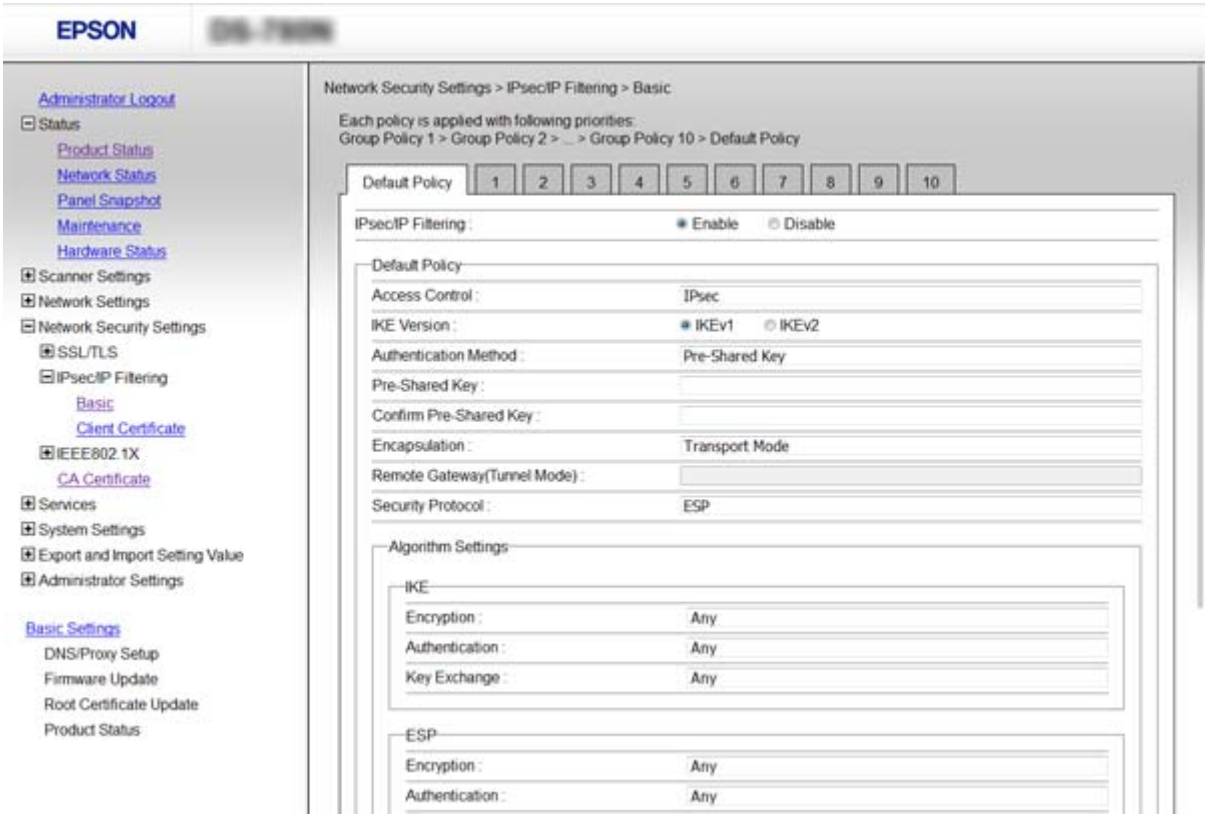
   Der Scanner ist aktualisiert.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

➡ „Einstellungselemente für Standardrichtlinie“ auf Seite 72

Einstellungselemente für Standardrichtlinie



Optionen	Einstellungen und Erläuterung
IPsec/IP-Filterung	Sie können eine IPsec/IP-Filterfunktion aktivieren oder deaktivieren.

Erweiterte Sicherheitseinstellungen für Unternehmen

Optionen	Einstellungen und Erläuterung	
Zugangssteuerung	Konfigurieren Sie eine Kontrollmethode für den Verkehr von IP-Paketen.	
	Zugang erlauben	Wählen Sie diesen Punkt, um konfigurierte IP-Pakete zuzulassen.
	Zugang verweigern	Wählen Sie diesen Punkt, um konfigurierte IP-Pakete zu sperren.
	IPsec	Wählen Sie diesen Punkt, um konfigurierte IPsec-Pakete zuzulassen.
IKE-Version	Wählen Sie IKEv1 oder IKEv2 als IKE-Version an. Wählen Sie eine der beiden Optionen anhand des Geräts aus, an das der Scanner angeschlossen ist.	
IKEv1	Die folgenden Elemente werden angezeigt, wenn Sie **IKEv1** als **IKE-Version** auswählen.	
	Authentisierungsmethode	Um **Zertifikat** wählen zu können, müssen Sie vorher ein CA-signiertes Zertifikat erhalten und importieren.
	Vorinstallierter Schlüssel	Falls **Vorinstallierter Schlüssel** für **Authentisierungsmethode** ausgewählt wird, geben Sie einen PSA-Schlüssel zwischen 1 und 127 Zeichen ein.
	Vorinstallierter Schlüssel bestätigen	Geben Sie zur Bestätigung den konfigurierten Schlüssel ein.
IKEv2	Die folgenden Elemente werden angezeigt, wenn Sie **IKEv2** als **IKE-Version** auswählen.	
Lokal	Authentisierungsmethode	Um **Zertifikat** wählen zu können, müssen Sie vorher ein CA-signiertes Zertifikat erhalten und importieren.
	ID-Typ	Wählen Sie den ID-Typ für den Scanner aus.
	ID	Geben Sie die ID des Scanners ein, die dem ID-Typ entspricht. Die Zeichen „@“, „#“ und „=“ dürfen nicht als erstes Zeichen vorkommen. **Eindeutiger Name**: Geben Sie 1 bis 128 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein. Das Zeichen „=“ muss enthalten sein. **IP-Adresse**: Geben Sie diese im IPv4 oder IPv6-Format ein. **FQDN**: Geben Sie eine Kombination aus 1 bis 255 Zeichen ein: A–Z, a–z, 0–9, „-“ und Punkt „.“. **eMail-Adresse**: Geben Sie 1 bis 128 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein. Das Zeichen „@“ muss enthalten sein. **Schlüssel-ID**: Geben Sie 1 bis 128 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein.
	Vorinstallierter Schlüssel	Falls **Vorinstallierter Schlüssel** für **Authentisierungsmethode** ausgewählt wird, geben Sie einen PSA-Schlüssel zwischen 1 und 127 Zeichen ein.
	Vorinstallierter Schlüssel bestätigen	Geben Sie zur Bestätigung den konfigurierten Schlüssel ein.

Erweiterte Sicherheitseinstellungen für Unternehmen

Optionen	Einstellungen und Erläuterung	
Extern	Authentisierungsmethode	Um **Zertifikat** wählen zu können, müssen Sie vorher ein CA-signiertes Zertifikat erhalten und importieren.
	ID-Typ	Wählen Sie den ID-Typ des Geräts aus, das Sie authentifizieren möchten.
	ID	Geben Sie die ID des Scanners ein, die dem ID-Typ entspricht. Die Zeichen „@“, „#“ und „=“ dürfen nicht als erstes Zeichen vorkommen. **Eindeutiger Name**: Geben Sie 1 bis 128 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein. Das Zeichen „=“ muss enthalten sein. **IP-Adresse**: Geben Sie diese im IPv4 oder IPv6-Format ein. **FQDN**: Geben Sie eine Kombination aus 1 bis 255 Zeichen ein: A–Z, a–z, 0–9, „-“ und Punkt „.“. **eMail-Adresse**: Geben Sie 1 bis 128 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein. Das Zeichen „@“ muss enthalten sein. **Schlüssel-ID**: Geben Sie 1 bis 128 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein.
	Vorinstallierter Schlüssel	Falls **Vorinstallierter Schlüssel** für **Authentisierungsmethode** ausgewählt wird, geben Sie einen PSA-Schlüssel zwischen 1 und 127 Zeichen ein.
	Vorinstallierter Schlüssel bestätigen	Geben Sie zur Bestätigung den konfigurierten Schlüssel ein.
Kapselung	Wenn Sie **IPsec** für **Zugangssteuerung** wählen, müssen Sie einen Encapsulation-Modus konfigurieren.	
	Transportmodus	Falls Sie den Scanner nur im selben LAN verwenden, wählen Sie diese Option. IP-Pakete der Schicht 4 oder höher werden verschlüsselt.
	Tunnelmodus	Falls Sie den Scanner über ein internetfähiges Netzwerk wie IPsec-VPN verwenden, wählen Sie diese Option aus. Header und Daten der IP-Pakete werden verschlüsselt.
Remote-Gateway-Adresse	Falls **Tunnelmodus** für **Kapselung** ausgewählt wird, geben Sie eine Gateway-Adresse zwischen 1 und 39 Zeichen ein.	
Sicherheitsprotokoll	**IPsec** für **Zugangssteuerung**, wählen Sie eine Option.	
	ESP	Wählen Sie diese Option, um die Integrität einer Authentifizierung und der Daten sicherzustellen und die Daten zu verschlüsseln.
	AH	Wählen Sie diese Option, um die Integrität einer Authentifizierung und der Daten sicherzustellen. Selbst wenn die Verschlüsselung von Daten nicht erlaubt ist, können Sie IPsec verwenden.
Algorithmuseinstellungen		

Optionen	Einstellungen und Erläuterung	
IKE	Verschlüsselung	Wählen Sie den Verschlüsselungsalgorithmus für IKE aus. Die Punkte hängen von der verwendeten IKE-Version ab.
	Authentifizierung	Wählen Sie den Authentifizierungsalgorithmus für IKE aus.
	Schlüsselaustausch	Wählen Sie den Algorithmus zum Schlüsseltausch für IKE aus. Die Punkte hängen von der verwendeten IKE-Version ab.
ESP	Verschlüsselung	Wählen Sie den Verschlüsselungsalgorithmus für ESP aus. Dies ist verfügbar, wenn **ESP** als **Sicherheitsprotokoll** ausgewählt ist.
	Authentifizierung	Wählen Sie den Authentifizierungsalgorithmus für ESP aus. Dies ist verfügbar, wenn **ESP** als **Sicherheitsprotokoll** ausgewählt ist.
AH	Authentifizierung	Wählen Sie den Verschlüsselungsalgorithmus für AH aus. Dies ist verfügbar, wenn **AH** als **Sicherheitsprotokoll** ausgewählt ist.

Zugehörige Informationen

➡ „Konfigurieren von Standardrichtlinie“ auf Seite 72

Konfigurieren von Gruppenrichtlinie

1. Rufen Sie Web Config auf, und wählen Sie dann **Netzwerksicherheitseinstellungen** > **IPsec/IP-Filterung** > **Grundlegend** aus.
2. Klicken Sie auf ein nummeriertes Register, um es zu konfigurieren.
3. Geben Sie für jedes Element einen Wert ein.
4. Klicken Sie auf **Weiter**.

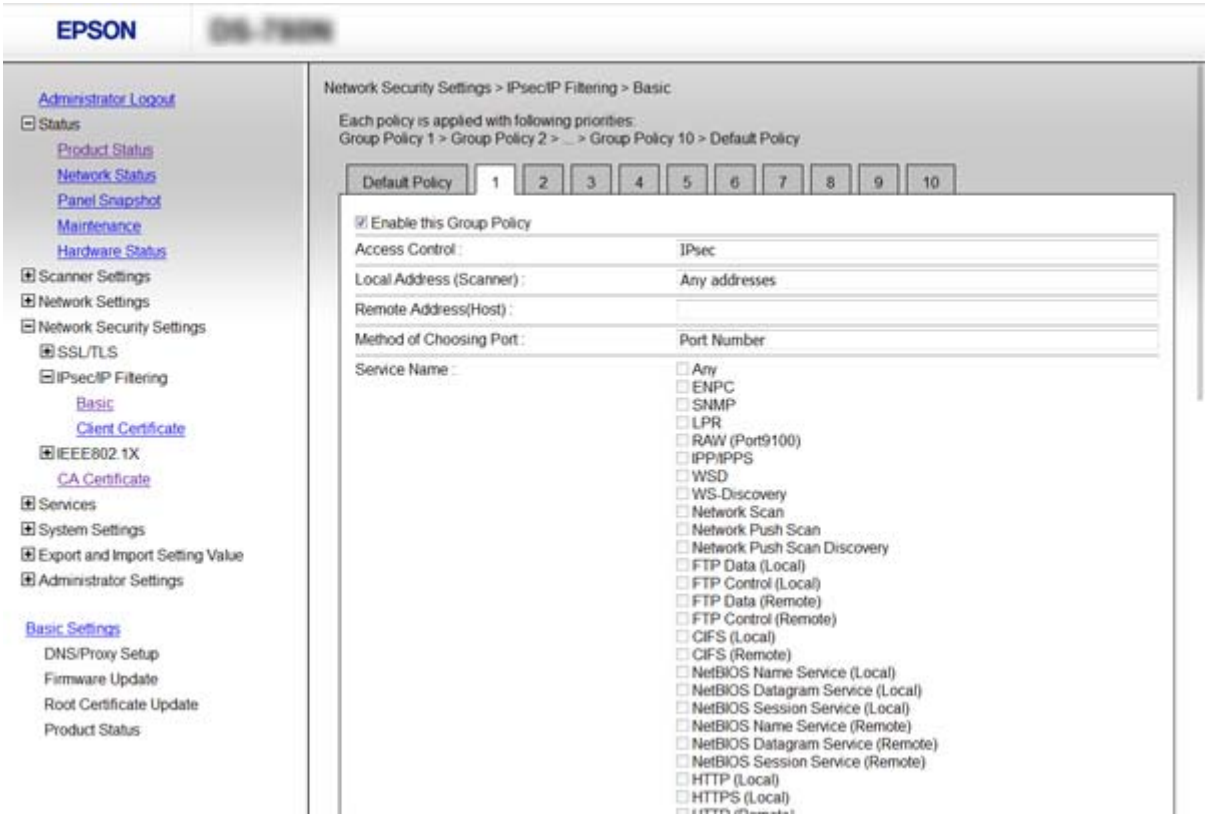
   Eine Bestätigungsmeldung wird angezeigt.
5. Klicken Sie auf **OK**.

   Der Scanner ist aktualisiert.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23
➡ „Einstellungselemente für Gruppenrichtlinie“ auf Seite 76

Einstellungselemente für Gruppenrichtlinie



Optionen	Einstellungen und Erläuterung	
Diese Gruppenrichtlinie aktivieren	Sie können eine Gruppenrichtlinie aktivieren oder deaktivieren.	
Zugangssteuerung	Konfigurieren Sie eine Kontrollmethode für den Verkehr von IP-Paketen.	
	Zugang erlauben	Wählen Sie diesen Punkt, um konfigurierte IP-Pakete zuzulassen.
	Zugang verweigern	Wählen Sie diesen Punkt, um konfigurierte IP-Pakete zu sperren.
	IPsec	Wählen Sie diesen Punkt, um konfigurierte IPsec-Pakete zuzulassen.
Lokale Adresse (Scanner)	Wählen Sie eine IPv4- oder IPv6-Adresse aus, die Ihrer Netzwerkumgebung entspricht. Falls automatisch eine IP-Adresse zugewiesen ist, können Sie **Automatisch bezogene IPv4-Adresse verwenden** auswählen.	
Remote-Adresse(Host)	Geben Sie zur Zugriffskontrolle die IP-Adresse eines Gerätes ein. Die IP-Adresse darf höchstens 43 Zeichen lang sein. Falls keine IP-Adresse eingeben wird, werden alle Adressen kontrolliert. ***Hinweis:*** *Wenn eine IP-Adresse automatisch zugewiesen wird (z. B. durch DHCP), ist die Verbindung ggf. nicht verfügbar. Konfigurieren Sie eine statische IP-Adresse.*	
Methode zur Anschlussauswahl	Wählen Sie eine Methode zur Festlegung von Anschlüssen.	

Erweiterte Sicherheitseinstellungen für Unternehmen

Optionen	Einstellungen und Erläuterung	
Servicename	Wenn Sie **Servicename** für **Methode zur Anschlussauswahl** wählen, wählen Sie eine Option.	
Transportprotokoll	Wenn Sie **Anschlussnummer** für **Methode zur Anschlussauswahl** wählen, müssen Sie einen Encapsulation-Modus konfigurieren.	
	Beliebiges Protokoll	Wählen Sie diese Option zur Datenkontrolle aller Protokolltypen.
	TCP	Wählen Sie diese Option zur Datenkontrolle bei Unicast-Verbindungen.
	UDP	Wählen Sie diese Option zur Datenkontrolle bei Broadcast- und Multicast-Verbindungen.
	ICMPv4	Wählen Sie diese Option zur Kontrolle des Ping-Befehls.
Lokaler Anschluss	Falls **Anschlussnummer** für **Methode zur Anschlussauswahl** ausgewählt wird, sowie **TCP** oder **UDP** für **Transportprotokoll** geben Sie durch Kommas getrennte Anschlussnummern ein, um empfangene Pakete zu kontrollieren. Sie können maximal 10 Anschlussnummern eingeben. Beispiel: 20,80,119,5220 Wenn Sie keine Anschlussnummer eingeben, werden alle Anschlüsse kontrolliert.	
Remote-Anschluss	Falls **Anschlussnummer** für **Methode zur Anschlussauswahl** ausgewählt wird, sowie **TCP** oder **UDP** für **Transportprotokoll** geben Sie durch Kommas getrennte Anschlussnummern ein, um gesendete Pakete zu kontrollieren. Sie können maximal 10 Anschlussnummern eingeben. Beispiel: 25,80,143,5220 Wenn Sie keine Anschlussnummer eingeben, werden alle Anschlüsse kontrolliert.	
IKE-Version	Wählen Sie IKEv1 oder IKEv2 als IKE-Version an. Wählen Sie eine der beiden Optionen anhand des Geräts aus, an das der Scanner angeschlossen ist.	
IKEv1	Die folgenden Elemente werden angezeigt, wenn Sie **IKEv1** als **IKE-Version** auswählen.	
	Authentisierungsmethode	Wenn Sie **IPsec** für **Zugangssteuerung** wählen, wählen Sie eine Option. Verwendetes Zertifikat gemeinsam mit einer Standardrichtlinie.
	Vorinstallierter Schlüssel	Falls **Vorinstallierter Schlüssel** für **Authentisierungsmethode** ausgewählt wird, geben Sie einen PSA-Schlüssel zwischen 1 und 127 Zeichen ein.
	Vorinstallierter Schlüssel bestätigen	Geben Sie zur Bestätigung den konfigurierten Schlüssel ein.
IKEv2	Die folgenden Elemente werden angezeigt, wenn Sie **IKEv2** als **IKE-Version** auswählen.	

Erweiterte Sicherheitseinstellungen für Unternehmen

Optionen	Einstellungen und Erläuterung	
Lokal	Authentisierungsmethode	Wenn Sie **IPsec** für **Zugangssteuerung** wählen, wählen Sie eine Option. Verwendetes Zertifikat gemeinsam mit einer Standardrichtlinie.
	ID-Typ	Wählen Sie den ID-Typ für den Scanner aus.
	ID	Geben Sie die ID des Scanners ein, die dem ID-Typ entspricht. Die Zeichen „@“, „#“ und „=“ dürfen nicht als erstes Zeichen vorkommen. **Eindeutiger Name**: Geben Sie 1 bis 128 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein. Das Zeichen „=“ muss enthalten sein. **IP-Adresse**: Geben Sie diese im IPv4 oder IPv6-Format ein. **FQDN**: Geben Sie eine Kombination aus 1 bis 255 Zeichen ein: A–Z, a–z, 0–9, „-“ und Punkt „.“. **eMail-Adresse**: Geben Sie 1 bis 128 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein. Das Zeichen „@“ muss enthalten sein. **Schlüssel-ID**: Geben Sie 1 bis 128 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein.
	Vorinstallierter Schlüssel	Falls **Vorinstallierter Schlüssel** für **Authentisierungsmethode** ausgewählt wird, geben Sie einen PSA-Schlüssel zwischen 1 und 127 Zeichen ein.
	Vorinstallierter Schlüssel bestätigen	Geben Sie zur Bestätigung den konfigurierten Schlüssel ein.

Erweiterte Sicherheitseinstellungen für Unternehmen

Optionen	Einstellungen und Erläuterung	
Extern	Authentisierungsmethode	Wenn Sie **IPsec** für **Zugangssteuerung** wählen, wählen Sie eine Option. Verwendetes Zertifikat gemeinsam mit einer Standardrichtlinie.
	ID-Typ	Wählen Sie den ID-Typ des Geräts aus, das Sie authentifizieren möchten.
	ID	Geben Sie die ID des Scanners ein, die dem ID-Typ entspricht. Die Zeichen „@“, „#“ und „=“ dürfen nicht als erstes Zeichen vorkommen. **Eindeutiger Name**: Geben Sie 1 bis 128 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein. Das Zeichen „=“ muss enthalten sein. **IP-Adresse**: Geben Sie diese im IPv4 oder IPv6-Format ein. **FQDN**: Geben Sie eine Kombination aus 1 bis 255 Zeichen ein: A–Z, a–z, 0–9, „-“ und Punkt „.“. **eMail-Adresse**: Geben Sie 1 bis 128 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein. Das Zeichen „@“ muss enthalten sein. **Schlüssel-ID**: Geben Sie 1 bis 128 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein.
	Vorinstallierter Schlüssel	Falls **Vorinstallierter Schlüssel** für **Authentisierungsmethode** ausgewählt wird, geben Sie einen PSA-Schlüssel zwischen 1 und 127 Zeichen ein.
	Vorinstallierter Schlüssel bestätigen	Geben Sie zur Bestätigung den konfigurierten Schlüssel ein.
Kapselung	Wenn Sie **IPsec** für **Zugangssteuerung** wählen, müssen Sie einen Encapsulation-Modus konfigurieren.	
	Transportmodus	Falls Sie den Scanner nur im selben LAN verwenden, wählen Sie diese Option. IP-Pakete der Schicht 4 oder höher werden verschlüsselt.
	Tunnelmodus	Falls Sie den Scanner über ein internetfähiges Netzwerk wie IPsec-VPN verwenden, wählen Sie diese Option aus. Header und Daten der IP-Pakete werden verschlüsselt.
Remote-Gateway-Adresse	Falls **Tunnelmodus** für **Kapselung** ausgewählt wird, geben Sie eine Gateway-Adresse zwischen 1 und 39 Zeichen ein.	
Sicherheitsprotokoll	Wenn Sie **IPsec** für **Zugangssteuerung** wählen, wählen Sie eine Option.	
	ESP	Wählen Sie diese Option, um die Integrität einer Authentifizierung und der Daten sicherzustellen und die Daten zu verschlüsseln.
	AH	Wählen Sie diese Option, um die Integrität einer Authentifizierung und der Daten sicherzustellen. Selbst wenn die Verschlüsselung von Daten nicht erlaubt ist, können Sie IPsec verwenden.
Algorithmuseinstellungen		

Optionen	Einstellungen und Erläuterung	
IKE	Verschlüsselung	Wählen Sie den Verschlüsselungsalgorithmus für IKE aus. Die Punkte hängen von der verwendeten IKE-Version ab.
	Authentifizierung	Wählen Sie den Authentifizierungsalgorithmus für IKE aus.
	Schlüsselaustausch	Wählen Sie den Algorithmus zum Schlüsseltausch für IKE aus. Die Punkte hängen von der verwendeten IKE-Version ab.
ESP	Verschlüsselung	Wählen Sie den Verschlüsselungsalgorithmus für ESP aus. Dies ist verfügbar, wenn **ESP** als **Sicherheitsprotokoll** ausgewählt ist.
	Authentifizierung	Wählen Sie den Authentifizierungsalgorithmus für ESP aus. Dies ist verfügbar, wenn **ESP** als **Sicherheitsprotokoll** ausgewählt ist.
AH	Authentifizierung	Wählen Sie den Authentifizierungsalgorithmus für AH aus. Dies ist verfügbar, wenn **AH** als **Sicherheitsprotokoll** ausgewählt ist.

Zugehörige Informationen

➡ „Konfigurieren von Gruppenrichtlinie“ auf Seite 75

➡ „Kombination aus Lokale Adresse (Scanner) und Remote-Adresse(Host) in Gruppenrichtlinie“ auf Seite 80

➡ „Verweise auf Servicename in Gruppenrichtlinie“ auf Seite 80

Kombination aus Lokale Adresse (Scanner) und Remote-Adresse(Host) in Gruppenrichtlinie

		Einstellung Lokale Adresse (Scanner)		
		IPv4	IPv6*2	Beliebige Adressen*3
Einstellung Remote-Adresse(Host)	IPv4*1	✓	–	✓
	IPv6*1, *2	–	✓	✓
	Leer	✓	✓	✓

*1 Falls **IPsec** ausgewählt ist für **Zugangssteuerung**, kann keine Präfixlänge ausgewählt werden.

*2 Falls **IPsec** ausgewählt ist für **Zugangssteuerung**, kann eine Link-Local-Adresse (fe80::) ausgewählt werden, aber die Gruppenrichtlinie wird deaktiviert sein.

*3 Außer IPv6-Link-Local-Adressen.

Verweise auf Servicename in Gruppenrichtlinie

Hinweis:
Nicht verfügbare Dienste werden angezeigt, können jedoch nicht ausgewählt werden.

Servicename	Protokolltyp	Lokale Portnummer	Remote-Portnummer	Kontrollierte Funktionen
Beliebig	–	–	–	Alle Services
ENPC	UDP	3289	Beliebiger Port	Scannersuche über Anwendungen wie EpsonNet Config und einem Scannertreiber
SNMP	UDP	161	Beliebiger Port	MIB-Erfassung und -Konfiguration über Anwendungen wie EpsonNet Config und dem Epson-Scannertreiber
WSD	TCP	Beliebiger Port	5357	WSD-Kontrolle
WS-Discovery	UDP	3702	Beliebiger Port	Scannersuche über WSD
Network Scan	TCP	1865	Beliebiger Port	Weiterleitung von Scandaten über Document Capture Pro
Network Push Scan Discovery	UDP	2968	Beliebiger Port	Suche nach einem Computer vom Scanner aus.
Network Push Scan	TCP	Beliebiger Port	2968	Erfassung von Auftragsinformationen für Push-Scan über Document Capture Pro oder Document Capture
HTTP (Lokal)	TCP	80	Beliebiger Port	HTTP(S)-Server (Weiterleitung von Web Config- und WSD-Daten)
HTTPS (Lokal)	TCP	443	Beliebiger Port	
HTTP (Remote)	TCP	Beliebiger Port	80	HTTP(S)-Client (Kommunikation zwischen Aktualisierung der Firmware und des Stammzertifikats)
HTTPS (Remote)	TCP	Beliebiger Port	443	

Konfigurationsbeispiele für IPsec/IP-Filterung

Nur Empfang von IPsec-Paketen

In diesem Beispiel wird nur eine Standardrichtlinie konfiguriert.

Standardrichtlinie:

❏ **IPsec/IP-Filterung**: **Aktivieren**

❏ **Zugangssteuerung**: **IPsec**

❏ **Authentisierungsmethode**: **Vorinstallierter Schlüssel**

❏ **Vorinstallierter Schlüssel**: Geben Sie bis zu 127 Zeichen ein.

Gruppenrichtlinie:

Nicht konfigurieren.

Übernehmen des Scans mit Epson Scan 2 und Scanner-Einstellungen

Dieses Beispiel zeigt die Kommunikation von Scannerdaten und der Scannerkonfiguration angegebener Dienste.

Standardrichtlinie:

❏ **IPsec/IP-Filterung**: **Aktivieren**

❏ **Zugangssteuerung**: **Zugang verweigern**

Gruppenrichtlinie:

❏ **Diese Gruppenrichtlinie aktivieren**: Aktivieren Sie das Kontrollkästchen.

❏ **Zugangssteuerung**: **Zugang erlauben**

❏ **Remote-Adresse(Host)**: IP-Adresse des Clients

❏ **Methode zur Anschlussauswahl**: **Servicename**

❏ **Servicename**: Aktivieren Sie die Kontrollkästchen **ENPC**, **SNMP**, **Network Scan**, **HTTP (Lokal)** und **HTTPS (Lokal)**.

Nur eingehender Zugriff von einer festgelegten IP-Adresse

In diesem Beispiel wird einer festgelegten IP-Adresse der Zugriff auf den Scanner erlaubt.

Standardrichtlinie:

❏ **IPsec/IP-Filterung**: **Aktivieren**

❏ **Zugangssteuerung**:**Zugang verweigern**

Gruppenrichtlinie:

❏ **Diese Gruppenrichtlinie aktivieren**: Aktivieren Sie das Kontrollkästchen.

❏ **Zugangssteuerung**: **Zugang erlauben**

❏ **Remote-Adresse(Host)**: IP-Adresse eines Administrator-Clients

Hinweis:
Ungeachtet einer Richtlinienkonfiguration kann der Client auf den Scanner zugreifen und ihn konfigurieren.

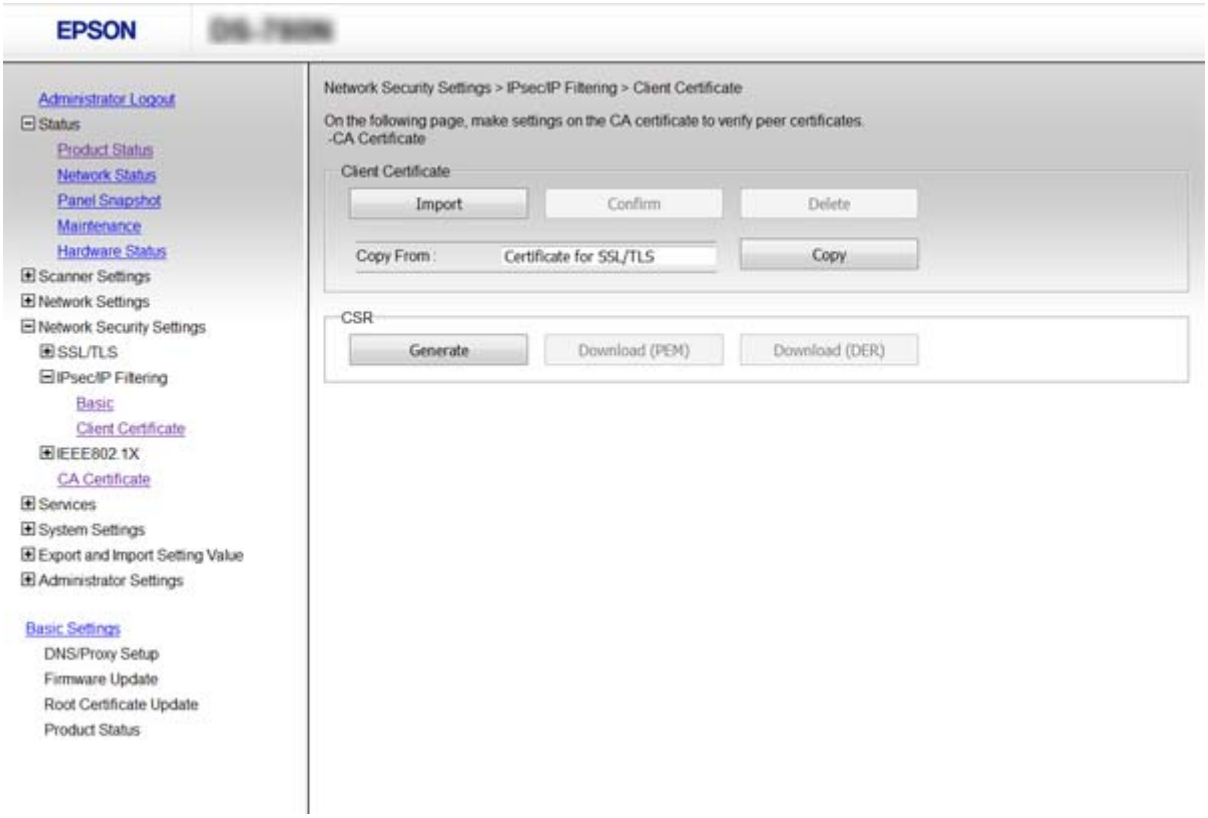
Ein Zertifikat für IPsec/IP-Filterung konfigurieren

Konfigurieren Sie das Client-Zertifikat für IPsec/IP-Filterung. Wenn Sie die Zertifizierungsbehörde konfigurieren möchten, wählen Sie **CA-Zertifikat**.

1. Rufen Sie Web Config auf, und wählen Sie dann **Netzwerksicherheitseinstellungen** > **IPsec/IP-Filterung** > **Client-Zertifikat** aus.

2. Importieren Sie das Zertifikat in **Client-Zertifikat**.

   Falls Sie bereits ein durch eine Zertifizierungsbehörde veröffentlichtes Zertifikat in IEEE802.1X oder SSL/TLS importiert haben, können Sie das Zertifikat kopieren und in IPsec/IP-Filterung nutzen. Wählen Sie zum Kopieren das Zertifikat von **Kopieren von**, klicken Sie dann auf **Kopie**.



Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

➡ „Erhalten und Importieren eines CA-signierten Zertifikats“ auf Seite 64

Verwenden des SNMPv3-Protokolls

Über SNMPv3

SNMP ist ein Protokoll, das Überwachungs- und Kontrollfunktionen übernimmt, um Daten von Netzwerkgeräten zu erfassen. SNMPv3 ist eine erweiterte Sicherheitsfunktion für die Verwaltung.

Bei der Nutzung von SNMPv3 lassen sich Zustandsüberwachung und Einstellungsänderungen der SNMP-Kommunikationspakete authentifizieren und verschlüsseln, um die Pakete vor Netzwerkrisiken wie Abhören, Identitätswechsel und Fälschung zu schützen.

Konfiguration von SNMPv3

Falls der Scanner das SNMPv3-Protokoll unterstützt, lassen sich Zugriffe auf den Scanner überwachen und kontrollieren.

1. Rufen Sie Web Config aus, und wählen Sie dann **Services** > **Protokoll** aus.
2. Geben Sie für jedes Element von **SNMPv3-Einstellungen** einen Wert ein.
3. Klicken Sie auf **Weiter**.

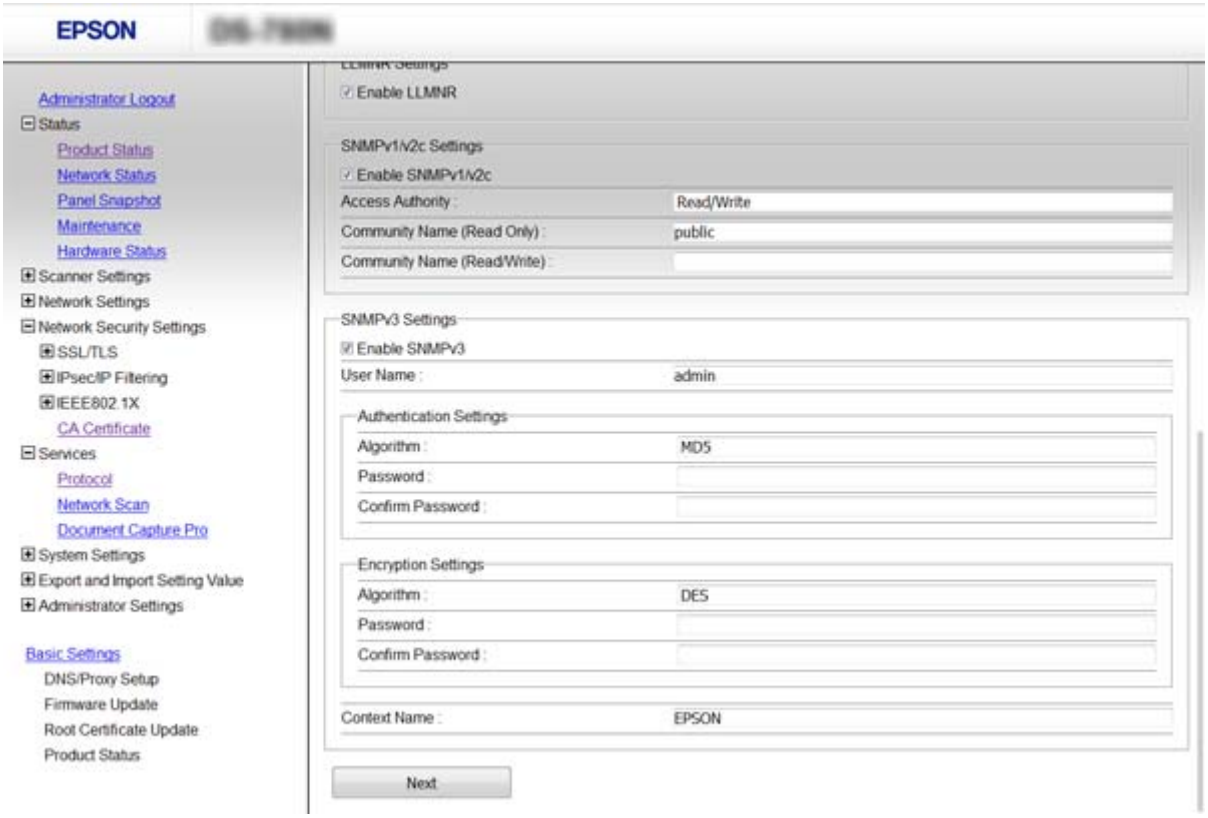
   Eine Bestätigungsmeldung wird angezeigt.
4. Klicken Sie auf **OK**.

   Der Scanner ist aktualisiert.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23
➡ „SNMPv3-Einstellungselemente“ auf Seite 84

SNMPv3-Einstellungselemente



Bezeichnung	Einstellungen und Erläuterung
SNMPv3 aktivieren	Bei aktiviertem Kontrollkästchen ist SNMPv3 aktiviert.

Bezeichnung	Einstellungen und Erläuterung
Benutzername	Geben Sie 1 bis 32 1-Byte-Zeichen ein.
Authentifizierungseinstellungen	
Algorithmus	Wählen Sie einen Algorithmus für die Authentifizierung.
Kennwort	Geben Sie 8 bis 32 ASCII-Zeichen (0x20-0x7E) ein.
Kennwort bestätigen	Geben Sie zur Bestätigung das konfigurierte Kennwort ein.
Verschlüsselungseinstellungen	
Algorithmus	Wählen Sie einen Algorithmus für die Verschlüsselung.
Kennwort	Geben Sie 8 bis 32 ASCII-Zeichen (0x20-0x7E) ein.
Kennwort bestätigen	Geben Sie zur Bestätigung das konfigurierte Kennwort ein.
Kontextname	Geben Sie 1 bis 32 1-Byte-Zeichen ein.

Zugehörige Informationen

➡ „Konfiguration von SNMPv3“ auf Seite 84

Verbinden des Scanners mit einem IEEE802.1X-Netzwerk

Konfiguration eines IEEE802.1X-Netzwerks

Wenn der Scanner IEEE802.1X unterstützt, können Sie ihn in einem Netzwerk mit Authentifizierung, das mit einem RADIUS-Server und einem Hub als Authentifizierer verbunden ist, verwenden.

1. Rufen Sie Web Config auf, und wählen Sie dann **Netzwerksicherheitseinstellungen** > **IEEE802.1X** > **Grundlegend** aus.
2. Geben Sie für jedes Element einen Wert ein.
3. Klicken Sie auf **Weiter**.

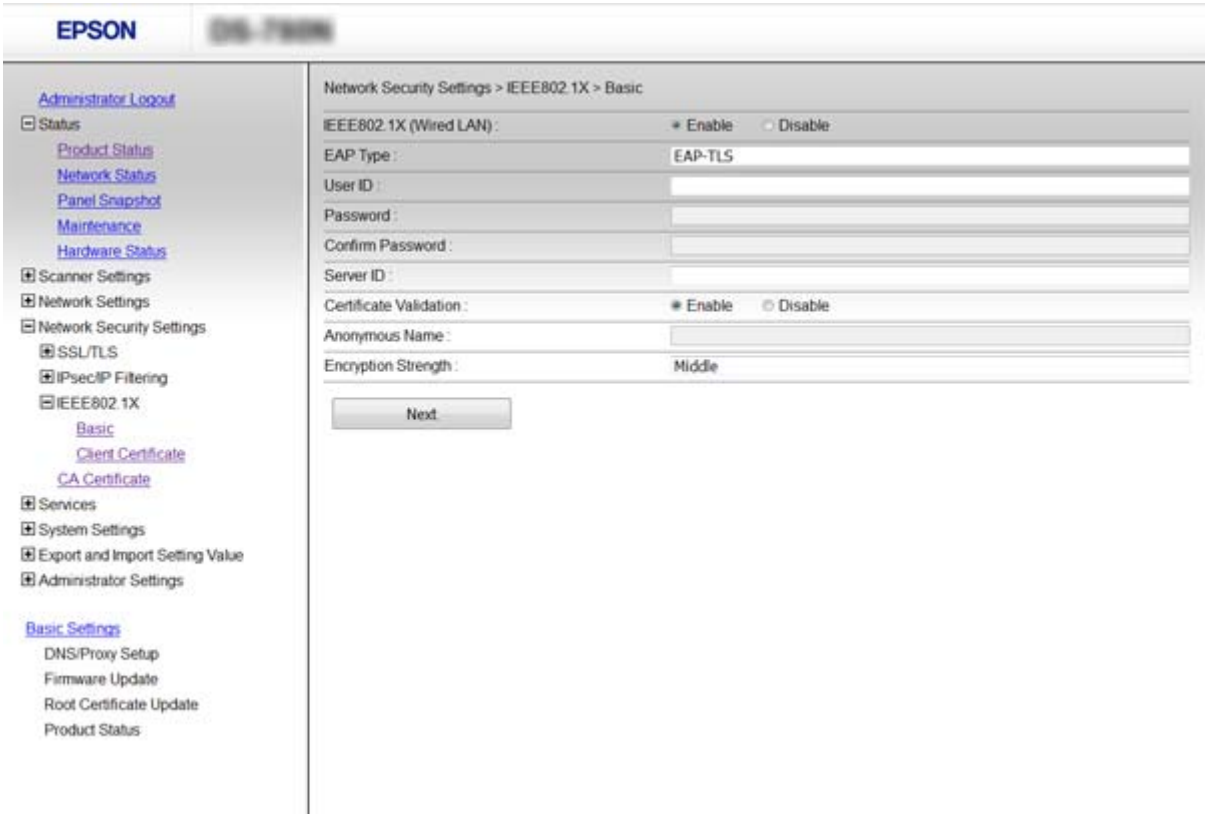
   Eine Bestätigungsmeldung wird angezeigt.
4. Klicken Sie auf **OK**.

   Der Scanner ist aktualisiert.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23
➡ „Einstellungselemente für IEEE802.1X-Netzwerk“ auf Seite 86
➡ „Zugriff auf den Drucker oder Scanner nach Konfiguration von IEEE802.1X nicht möglich“ auf Seite 91

Einstellungselemente für IEEE802.1X-Netzwerk



Optionen	Einstellungen und Erläuterung	
IEEE802.1X (Kabel-LAN)	Sie können Einstellungen der Seite (**IEEE802.1X** > **Grundlegend**) für IEEE802.1X (kabelgebundenes LAN) aktivieren oder deaktivieren.	
EAP-Typ	Wählen Sie eine Option für die Authentifizierungsmethode zwischen dem Scanner und einem RADIUS-Server.	
	EAP-TLS	Sie müssen ein CA-signiertes Zertifikat beziehen und importieren.
	PEAP-TLS	
	PEAP/MSCHAPv2	Sie müssen ein Kennwort konfigurieren.
Benutzer-ID	Konfigurieren Sie eine ID zur Nutzung für eine Authentifizierung von einem RADIUS-Server. Geben Sie 1 bis 128 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein.	
Kennwort	Konfigurieren Sie ein Passwort für die Authentifizierung des Druckers. Geben Sie 1 bis 128 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein. Wenn Sie einen Windows-Server als RADIUS-Server nutzen, können Sie bis zu 127 Zeichen eingeben.	
Kennwort bestätigen	Geben Sie das zur Bestätigung konfigurierte Kennwort ein.	
Server-ID	Sie können eine Server-ID zur Authentifizierung mit einem spezifizierten RADIUS-Server konfigurieren. Der Authentifizierer prüft, ob eine Server-ID im Feld „subject/subjectAltName“ eines von einem RADIUS-Server gesendeten Serverzertifikats enthalten ist. Geben Sie 0 bis 128 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein.	

Optionen	Einstellungen und Erläuterung	
Zertifikatsvalidierung	Sie können die Zertifikatsvalidierung unabhängig von der Authentifizierungsmethode festlegen. Importieren Sie das Zertifikat in **CA-Zertifikat**.	
Anonymer Name	Wenn Sie **PEAP-TLS** oder **PEAP/MSCHAPv2** als **Authentisierungsmethode** wählen, können Sie für die Phase 1 einer PEAP-Authentifizierung einen anonymen Namen anstelle einer Benutzer-ID eingeben. Geben Sie 0 bis 128 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein.	
Verschlüsselungsstärke	Sie können eine der Folgenden auswählen.	
	Hoch	AES256/3DES
	Mittel	AES256/3DES/AES128/RC4

Zugehörige Informationen

➡ „Konfiguration eines IEEE802.1X-Netzwerks“ auf Seite 85

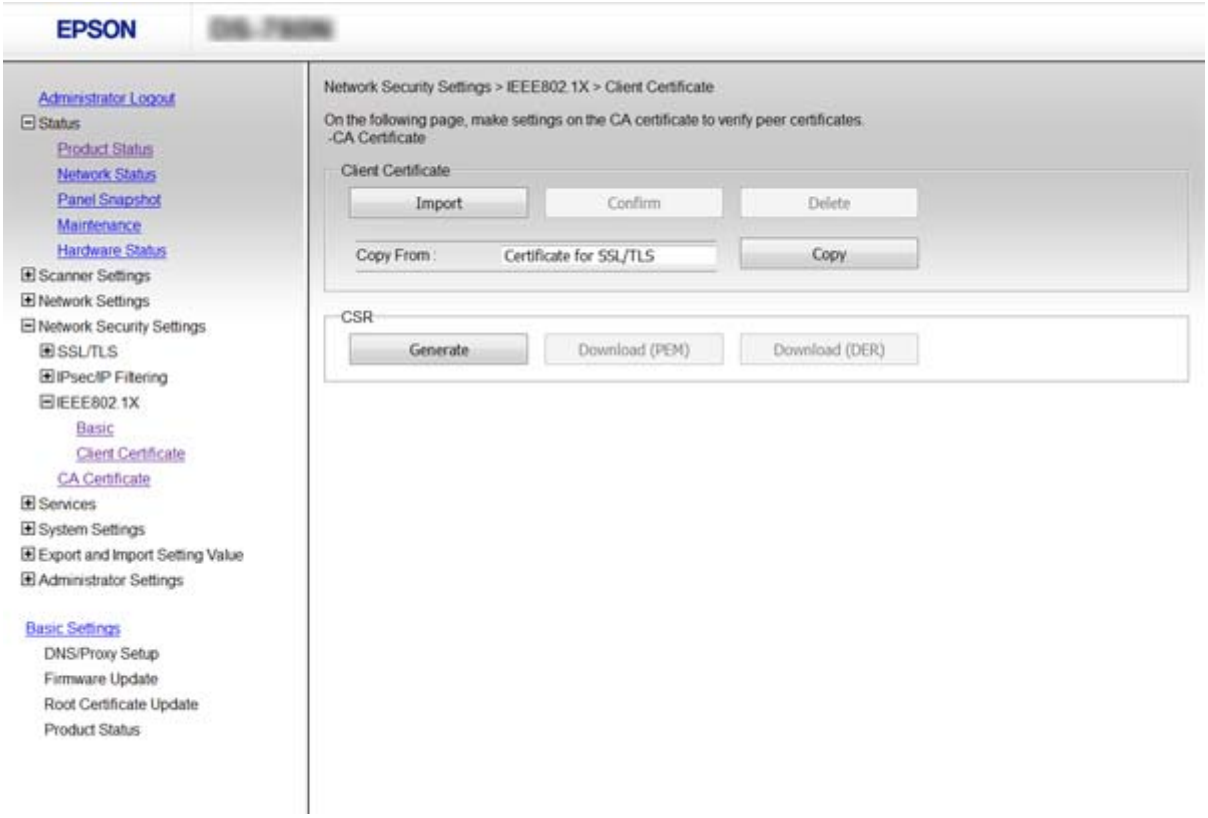
Ein Zertifikat für IEEE802.1X konfigurieren

Konfigurieren Sie das Client-Zertifikat für IEEE802.1X. Wenn Sie das Zertifikat der Zertifizierungsbehörde konfigurieren möchten, wählen Sie **CA-Zertifikat**.

1. Rufen Sie Web Config auf, und wählen Sie dann **Netzwerksicherheitseinstellungen** > **IEEE802.1X** > **Client-Zertifikat** aus.

2. Geben Sie ein Zertifikat unter **Client-Zertifikat** ein.

   Sie können das Zertifikat kopieren, wenn es durch eine Zertifizierungsbehörde veröffentlicht wurde. Wählen Sie zum Kopieren das Zertifikat von **Kopieren von**, klicken Sie dann auf **Kopie**.



Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

➡ „Erhalten und Importieren eines CA-signierten Zertifikats“ auf Seite 64

Beheben von Problemen für erweiterte Sicherheit

Wiederherstellen der Sicherheitseinstellungen

Beim Einsatz äußerst sicherer Verfahren wie IPsec/IP-Filterung oder IEEE802.1X kann es vorkommen, dass Sie aufgrund falscher Einstellungen oder Problemen auf dem Gerät oder Server nicht mehr mit den Geräten kommunizieren können. Stellen Sie in einem solchen Fall die Sicherheitseinstellungen wieder her, um die richtigen Geräteeinstellungen erneut vorzunehmen oder temporären Zugriff zu gewähren.

Deaktivieren der Sicherheitsfunktion am Bedienfeld

Sie können die Funktionen IPsec/IP-Filterung und IEEE802.1X am Scannerbedienfeld deaktivieren.

1. Tippen Sie auf **Einstellungen** > **Netzwerkeinstellungen**.

2. Tippen Sie auf **Einstellungen ändern**.
3. Wählen Sie die Punkte aus, die Sie deaktivieren möchten.
   - ❏ **IPsec/IP-Filterung**
   - ❏ **IEEE802.1X**
4. Wenn eine Abschlussmeldung angezeigt wird, tippen Sie auf **Fortf.**.

Wiederherstellen der Sicherheitsfunktion mithilfe von Web Config

Beim Einsatz von IEEE802.1X werden Geräte möglicherweise nicht mehr im Netzwerk erkannt. Deaktivieren Sie in diesem Fall die Funktion über das Bedienfeld des Scanners.

Beim Einsatz von IPsec/IP-Filterung können Sie die Funktion deaktivieren, wenn Sie vom Computer aus Zugriff auf das Gerät haben.

Deaktivieren der IPsec/IP Filterung mit Web Config

1. Rufen Sie hierzu Web Config auf und wählen Sie **Netzwerksicherheitseinstellungen** > **IPsec/IP-Filterung** > **Grundlegend**.
2. Wählen Sie **Deaktivieren** als **IPsec/IP-Filterung** in **Standardrichtlinie**.
3. Klicken Sie auf **Weiter**, und deaktivieren Sie dann das Kontrollkästchen **Diese Gruppenrichtlinie aktivieren** für alle Gruppenrichtlinien.
4. Klicken Sie auf **OK**.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

Probleme bei Verwendung der Netzwerksicherheitsfunktionen

Ein PSA-Schlüssel wurde vergessen

Konfigurieren Sie den Schlüssel erneut mit Web Config.

Um den Schlüssel zu ändern, rufen Sie Web Config auf, und wählen Sie **Netzwerksicherheitseinstellungen** > **IPsec/IP-Filterung** > **Grundlegend** > **Standardrichtlinie** oder **Gruppenrichtlinie**.

Ändern Sie nach dem Wechsel des PSA-Schlüssels auch die auf den Computern hinterlegten PSA-Schlüssel.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

Keine IPsec-Kommunikation

Verwenden Sie für die Computereinstellungen einen nicht unterstützten Algorithmus?

Der Scanner unterstützt die folgenden Algorithmen.

Sicherheitsverfahren	Algorithmen
IKE-Verschlüsselungsalgorithmus	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE-Authentifizierungsalgorithmus	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE-Schlüsseltauschalgorithmus	DH-Gruppe 1, DH-Gruppe 2, DH-Gruppe 5, DH-Gruppe 14, DH-Gruppe 15, DH-Gruppe 16, DH-Gruppe 17, DH-Gruppe 18, DH-Gruppe 19, DH-Gruppe 20, DH-Gruppe 21, DH-Gruppe 22, DH-Gruppe 23, DH-Gruppe 24, DH-Gruppe 25, DH-Gruppe 26, DH-Gruppe 27*, DH-Gruppe 28*, DH-Gruppe 29*, DH-Gruppe 30*
ESP-Verschlüsselungsalgorithmus	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP-Authentifizierungsalgorithmus	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH-Authentifizierungsalgorithmus	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* Nur für IKEv2

Zugehörige Informationen

➡ „Verschlüsselte Kommunikation mit IPsec/IP-Filterung“ auf Seite 71

Plötzlich ausfallende Kommunikation

Ist die Scanner-IP-Adresse ungültig oder geändert worden?

Deaktivieren Sie IPsec im Scannerbedienfeld.

Falls der DHCP-Server veraltet ist, neu startet oder die IPv6-Adresse veraltet oder nicht abgerufen wurde, kann die für Web Config (**Netzwerksicherheitseinstellungen** > **IPsec/IP-Filterung** > **Grundlegend** > **Gruppenrichtlinie** > **Lokale Adresse (Scanner)**) des Scanners registrierte IP-Adresse vielleicht nicht gefunden werden.

Verwenden Sie eine statische IP-Adresse.

Ist die Computer-IP-Adresse ungültig oder geändert worden?

Deaktivieren Sie IPsec im Scannerbedienfeld.

Falls der DHCP-Server veraltet ist, neu startet oder die IPv6-Adresse veraltet oder nicht abgerufen wurde, kann die für Web Config (**Netzwerksicherheitseinstellungen** > **IPsec/IP-Filterung** > **Grundlegend** > **Gruppenrichtlinie** > **Remote-Adresse(Host)**) des Scanners registrierte IP-Adresse vielleicht nicht gefunden werden.

Verwenden Sie eine statische IP-Adresse.

Zugehörige Informationen

➡ „Aufrufen von Web Config“ auf Seite 23

➡ „Verschlüsselte Kommunikation mit IPsec/IP-Filterung“ auf Seite 71

Verbindung nach Konfiguration von IPsec/IP-Filterung nicht möglich

Möglicherweise ist der eingestellte Wert falsch.

Deaktivieren Sie IPsec/IP-Filterung im Scannerbedienfeld. Verbinden Sie Scanner und Computer und nehmen Sie die Einstellungen von IPsec/IP-Filterung erneut vor.

Zugehörige Informationen

➡ „Verschlüsselte Kommunikation mit IPsec/IP-Filterung“ auf Seite 71

Zugriff auf den Drucker oder Scanner nach Konfiguration von IEEE802.1X nicht möglich

Die Einstellungen sind möglicherweise ungültig.

Deaktivieren Sie IEEE802.1X vom Bedienfeld des Scanners aus. Verbinden Sie den Scanner mit einem Computer, und konfigurieren Sie dann IEEE802.1X erneut.

Zugehörige Informationen

➡ „Konfiguration eines IEEE802.1X-Netzwerks“ auf Seite 85

Probleme bei der Verwendung eines digitalen Zertifikats

Importieren eines CA-signierten Zertifikats nicht möglich

Stimmen das CA-signierte Zertifikat und die Daten auf dem CSR überein?

Wenn das CA-signierte Zertifikat andere Daten als der CSR enthält, kann das Zertifikat nicht importiert werden. Prüfen Sie Folgendes:

❏ Versuchen Sie, das Zertifikat auf ein Gerät zu importieren, das nicht dieselben Informationen enthält?

Prüfen Sie die Informationen auf dem CSR und importieren Sie dann das Zertifikat auf ein Gerät, das dieselben Informationen enthält.

❏ Haben Sie den im Scanner gespeicherten CSR nach dem Senden an eine Zertifizierungsbehörde überschrieben?

Beziehen Sie mit dem CSR erneut ein CA-signiertes Zertifikat.

Ist das CA-signierte Zertifikat größer als 5 KB?

Ein CA-signiertes Zertifikat, das größer als 5 KB ist, kann nicht importiert werden.

Ist das Kennwort zum Importieren des Zertifikats richtig?

Wenn Sie das Kennwort vergessen haben, können Sie das Zertifikat nicht importieren.

Zugehörige Informationen

➡ „Importieren eines CA-signierten Zertifikats“ auf Seite 66

Aktualisieren eines selbstsignierten Zertifikats nicht möglich

Wurde der Allgemeiner Name eingegeben?

Allgemeiner Name muss eingegeben werden.

Wurden im Allgemeiner Name nicht unterstützte Zeichen eingegeben? Japanisch wird z. B. nicht unterstützt.

Geben Sie 1 bis 128 ASCII-Zeichen (0x20-0x7E) im IPv4-, IPv6-, Hostnamen- oder FQDN-Format ein.

Enthält der Allgemeiner Name ein Komma oder Leerzeichen?

Enthält der **Allgemeiner Name** ein Komma, wird er an dieser Stelle geteilt. Wenn vor oder nach einem Komma nur ein Leerzeichen steht, tritt ein Fehler auf.

Zugehörige Informationen

➡ „Aktualisieren eines selbstsignierten Zertifikats“ auf Seite 68

Ein CSR kann nicht erstellt werden

Wurde der Allgemeiner Name eingegeben?

Der **Allgemeiner Name** muss eingegeben werden.

Wurden im Allgemeiner Name, Organisation, Organisationseinheit, Ort, Staat/Bundesland nicht unterstützte Zeichen eingegeben? Japanisch wird z. B. nicht unterstützt.

Geben Sie ASCII-Zeichen (0x20-0x7E) im IPv4-, IPv6-, Hostnamen- oder FQDN-Format ein.

Enthält der Allgemeiner Name ein Komma oder Leerzeichen?

Enthält der **Allgemeiner Name** ein Komma, wird er an dieser Stelle geteilt. Wenn vor oder nach einem Komma nur ein Leerzeichen steht, tritt ein Fehler auf.

Zugehörige Informationen

➡ „Erhalten eines CA-signierten Zertifikats“ auf Seite 64

Warnmeldung für ein digitales Zertifikat wird angezeigt

Meldungen	Ursache/Lösung
Ein Serverzertifikat eingeben.	**Ursache:** Es ist keine Datei für den Import ausgewählt. **Lösung:** Wählen Sie eine Datei und klicken Sie auf **Importieren**.

Erweiterte Sicherheitseinstellungen für Unternehmen

Meldungen	Ursache/Lösung
CA-Zertifikat 1 nicht eingegeben.	**Ursache:** CA-Zertifikat 1 ist nicht eingegeben und nur CA-Zertifikat 2 ist eingegeben. **Lösung:** Importieren Sie CA-Zertifikat 1 zuerst.
Der nachfolgende Wert ist ungültig.	**Ursache:** Der Dateipfad und/oder das Kennwort enthalten nicht unterstützte Zeichen. **Lösung:** Stellen Sie sicher, dass die Zeichen für das Element richtig eingegeben werden.
Datum und Zeit ungültig.	**Ursache:** Datum und Uhrzeit sind für den Scanner nicht eingestellt. **Lösung:** Stellen Sie Datum und Uhrzeit mit Web Config oder EpsonNet Config ein.
Kennwort ungültig.	**Ursache:** Das für das CA-Zertifikat festgelegte Kennwort und das eingegebene Kennwort stimmen nicht überein. **Lösung:** Geben Sie das richtige Kennwort ein.
Datei ungültig.	**Ursache:** Sie importieren keine Zertifikatsdatei im X509-Format. **Lösung:** Stellen Sie sicher, dass Sie das richtige, von einer vertrauenswürdigen Zertifizierungsbehörde gesendete Zertifikat gewählt haben.
	Ursache: Die importierte Datei ist zu groß. Die maximale Dateigröße beträgt 5 KB. **Lösung:** Wenn Sie die richtige Datei gewählt haben, ist das Zertifikat ggf. beschädigt oder fabriziert.
	Ursache: Die im Zertifikat enthaltene Kette ist ungültig. **Lösung:** Weitere Informationen zum Zertifikat finden Sie auf der Website der Zertifizierungsbehörde.
Kann Serverzertifikate nicht nutzen, die mehr als drei CA-Zertifikate beinhalten.	**Ursache:** Die Zertifikatsdatei im PKCS#12-Format enthält mehr als 3 CA-Zertifikate. **Lösung:** Importieren Sie jedes Zertifikat durch Konvertieren vom PKCS#12- ins PEM-Format oder importieren Sie die Zertifikatsdatei im PKCS#12-Format, die bis zu 2 CA-Zertifikate enthält.

Meldungen	Ursache/Lösung
Das Zertifikat ist abgelaufen. Prüfen Sie, ob das Zertifikat gültig ist, oder prüfen Sie Datum und Zeit auf dem Produkt.	**Ursache:** Das Zertifikat ist abgelaufen. **Lösung:** ❏ Wenn das Zertifikat abgelaufen ist, beziehen und importieren Sie ein neues Zertifikat. ❏ Wenn das Zertifikat nicht abgelaufen ist, stellen Sie sicher, dass Datum und Uhrzeit im Scanner richtig eingestellt sind.
Privater Schlüssel erforderlich.	**Ursache:** Mit dem Zertifikat ist kein privater Schlüssel verknüpft. **Lösung:** ❏ Bei einem Zertifikat im PEM/DER-Format, das über einen Computer mit einem CSR bezogen worden ist, geben Sie den privaten Schlüssel ein. ❏ Bei einem Zertifikat im PKCS#12-Format, das über einen Computer mit einem CSR bezogen worden ist, erstellen Sie eine Datei, die den privaten Schlüssel enthält.
	Ursache: Sie haben ein PEM/DER-Zertifikat, das über einen CSR mit Web Config bezogen worden ist, erneut importiert. **Lösung:** Ein Zertifikat im PEM/DER-Format, das mit Web Config und einem CSR bezogen worden ist, kann nur einmal importiert werden.
Einrichtung ist fehlgeschlagen.	**Ursache:** Die Konfiguration kann nicht abgeschlossen werden, weil die Kommunikation zwischen Scanner und Computer fehlgeschlagen ist oder die Datei wegen einiger Fehler nicht gelesen werden kann. **Lösung:** Prüfen Sie die angegebene Datei und Kommunikation und importieren Sie die Datei erneut.

Zugehörige Informationen

➡ „Über digitale Zertifizierung“ auf Seite 63

CA-signiertes Zertifikat versehentlich gelöscht

Existiert für das Zertifikat eine Sicherungsdatei?

Wenn Sie eine Sicherungsdatei haben, importieren Sie das Zertifikat erneut.

Wenn Sie ein Zertifikat beziehen, das mit einem in Web Config erstellten CSR beantragt worden ist, können Sie ein gelöschtes Zertifikat nicht noch einmal importieren. Erstellen Sie einen CSR und beziehen Sie ein neues Zertifikat.

Zugehörige Informationen

➡ „Löschen eines CA-signierten Zertifikats“ auf Seite 68

➡ „Importieren eines CA-signierten Zertifikats“ auf Seite 66