EPSON
EXCEED YOUR VISION

Beheerdershandleiding

NPD5668-00 NL

Inhoudsopgave

Bijlage

Geavanceerde beveiligingsinstellingen voor bedrijven

Copyright

Handelsmerken

- ❏ EPSON® is een gedeponeerd handelsmerk en EPSON EXCEED YOUR VISION of EXCEED YOUR VISION is een handelsmerk van 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.
- ❏ Algemene opmerking: andere productnamen vermeld in deze uitgave, dienen uitsluitend als identificatie en kunnen handelsmerken zijn van hun respectievelijke eigenaars. Epson maakt geen enkele aanspraak op enige rechten op deze handelsmerken.

Deze handleiding

Tekens en symbolen

> ⚠ ***Let op:***
> *Aanwijzingen die u zorgvuldig moet opvolgen om letsel te voorkomen.*

> ***Belangrijk:***
> *Aanwijzingen die u moet opvolgen om schade aan uw apparatuur te voorkomen.*

Opmerking:
Aanwijzingen die handige tips bevatten en beperkingen aangeven voor het gebruik van de scanner.

Gerelateerde informatie

➡ Wanneer u op dit pictogram klikt, gaat u naar verwante informatie.

Beschrijvingen gebruikt in deze handleiding

❏ Screenshots van de schermen van het scannerstuurprogram en Epson Scan 2 (scannerstuurprogramma) zijn van Windows 10 of OS X El Capitan. De inhoud die op de schermen wordt weergegeven, is afhankelijk van het model en de situatie.

❏ De illustraties die in deze handleiding worden gebruikt, dienen puur als voorbeeld. Er zijn kleine verschillen tussen elk model, maar de gebruiksmethode blijft hetzelfde.

❏ Sommige menu-items op de display variëren naargelang het model en de instellingen.

Referenties voor besturingssystemen

Windows

In deze handleiding verwijzen termen als "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" en "Windows Server 2003" naar de volgende besturingssystemen. Bovendien wordt "Windows" gebruikt om alle versies ervan aan te duiden.

❏ Microsoft® Windows® 10 besturingssysteem

❏ Microsoft® Windows® 8.1 besturingssysteem

❏ Microsoft® Windows® 8 besturingssysteem

❏ Microsoft® Windows® 7 besturingssysteem

❏ Microsoft® Windows Vista® besturingssysteem

❏ Microsoft® Windows® XP besturingssysteem

Deze handleiding

- ❏ Microsoft® Windows® XP Professional x64 Edition besturingssysteem
- ❏ Microsoft® Windows Server® 2016 besturingssysteem
- ❏ Microsoft® Windows Server® 2012 R2 besturingssysteem
- ❏ Microsoft® Windows Server® 2012 besturingssysteem
- ❏ Microsoft® Windows Server® 2008 R2 besturingssysteem
- ❏ Microsoft® Windows Server® 2008 besturingssysteem
- ❏ Microsoft® Windows Server® 2003 R2 besturingssysteem
- ❏ Microsoft® Windows Server® 2003 besturingssysteem

Mac OS

In deze handleiding wordt "Mac OS" gebruikt om te verwijzen naar macOS Sierra, OS X El Capitan, OS X Yosemite, OS X Mavericks, OS X Mountain Lion, Mac OS X v10.7.x en Mac OS X v10.6.8.

Inleiding

Componenthandleiding

Deze handleiding is voor de apparaatbeheerder die verantwoordelijk is voor het verbinden van de printer of scanner met het netwerk, en bevat informatie over het configureren van instellingen om de functies te gebruiken.

Zie de *Gebruikershandleiding* voor informatie over het gebruik van functies.

Voorbereiding

Bevat informatie over de taken van de beheerder, hoe apparaten moeten worden ingesteld en de beheerderssoftware.

Verbinding

Bevat informatie over hoe het apparaat moet worden verbonden met het netwerk of een telefoonlijn. Bevat tevens informatie over de netwerkomgeving, zoals het gebruik van een poort voor het apparaat, en informatie over DNS en proxyservers.

Functie-instellingen

Hierin worden de instellingen voor elke functie van het apparaat verklaard.

Basisinstellingen voor beveiliging

Bevat informatie over de instellingen voor elke functie, zoals afdrukken, scannen en faxen.

Instellingen voor bediening en beheer

Bevat informatie over de bewerkingen nadat de apparaten in gebruik zijn genomen, zoals informatiecontrole en onderhoud.

Problemen oplossen

Bevat informatie over initialisatie van instellingen en het oplossen van problemen in het netwerk.

Geavanceerde beveiligingsinstellingen voor bedrijven

Bevat informatie over de instellingsmethode voor het verbeteren van de beveiliging van het apparaat, zoals het gebruik van een CA-certificaat, SSL/TLS-communicatie en IPsec/IP-filtering.

Afhankelijk van het model worden sommige functies in dit hoofdstuk mogelijk niet ondersteund.

Definitie van termen die in deze handleiding worden gebruikt

In deze handleiding worden de volgende termen gebruikt.

Inleiding

Beheerder

Degene die verantwoordelijk is voor het installeren en instellen van het apparaat of het netwerk van een kantoor of organisatie. In kleine organisaties is deze persoon mogelijk verantwoordelijk voor zowel apparaat- als netwerkbeheer. In grote organisaties hebben beheerders zeggenschap over het netwerk of over apparaten in de groepseenheid van een afdeling of divisie, en zijn netwerkbeheerders verantwoordelijk voor de instellingen voor communicatie naar buiten de organisatie, zoals internet.

Netwerkbeheerder

Degene die verantwoordelijk is voor netwerkcommunicatie. Degene die de router, proxyserver, DNS-server en e-mailserver instelt om communicatie via internet of het netwerk te beheren.

Gebruiker

Degene die apparaten, zoals printers of scanners, gebruikt.

Web Config (webpagina van het apparaat)

De webserver die in het apparaat is geïntegreerd. Dit heeft Web Config. U kunt de status van het apparaat controleren en wijzigen met de browser.

Hulpprogramma

Een algemene term voor software voor het instellen of beheren van een apparaat, zoals Epson Device Admin, EpsonNet Config, EpsonNet SetupManager, enz.

Push-scan

Een algemene term voor scannen vanaf het bedieningspaneel van het apparaat.

ASCII (American Standard Code for Information Interchange)

Een van de standaard tekencodes. Er zijn 128 tekens vastgelegd, waaronder tekens als het alfabet (a–z, A–Z), Arabische cijfers (0–9), symbolen, blanco tekens en stuurtekens. Wanneer in deze handleiding "ASCII" wordt beschreven, wordt hiermee de onderstaande lijst 0x20–0x7E (hex-nummer) aangeduid, exclusief stuurtekens.

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	{	|	}	~	

* Spatieteken.

Unicode (UTF-8)

Een internationale standaardcode, geschikt voor de wereldtalen. Wanneer in deze handleiding "UTF-8" wordt beschreven, wordt hiermee het coderen van tekens in UTF-8-indeling aangeduid.

Voorbereiding

Dit hoofdstuk bevat informatie over de rol van de beheerder en voorbereiding vóór het configureren van instellingen.

Stroom van scannerinstellingen en -beheer

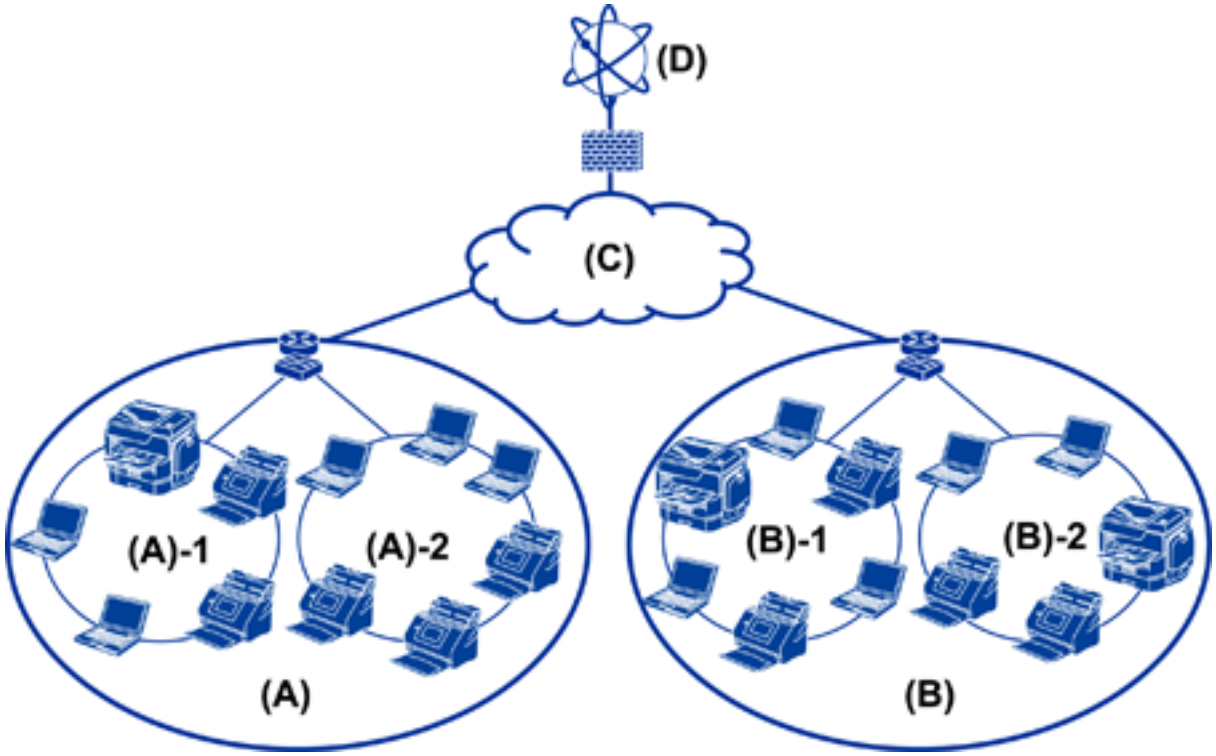
De beheerder configureert de instellingen voor de netwerkverbinding, de eerste instelling en het onderhoud voor de scanner zodat deze beschikbaar zijn voor de gebruikers.

1. Voorbereiden
   - ❏ De informatie voor de verbindingsinstellingen verzamelen
   - ❏ Keuze van de verbindingsmethode
2. Verbinden
   - ❏ Netwerkverbinding vanaf het bedieningspaneel van de scanner
3. De functies instellen
   - ❏ Instellingen van het scannerstuurprogramma
   - ❏ Andere geavanceerde instellingen
4. Beveiligingsinstellingen
   - ❏ Beheerdersinstellingen
   - ❏ SSL/TLS
   - ❏ Protocolbeheer
   - ❏ Geavanceerd beveiligingsinstellingen (optioneel)
5. Bedienen en beheren
   - ❏ De apparaatstatus controleren
   - ❏ Gebeurtenissen afhandelen
   - ❏ Een back-up maken van de apparaatinstellingen

Gerelateerde informatie

➡ “Voorbereiding” op pagina 10
➡ “Verbinding” op pagina 15
➡ “Functie-instellingen” op pagina 22
➡ “Basisinstellingen voor beveiliging” op pagina 32
➡ “Instellingen voor bediening en beheer” op pagina 40

Voorbeeld van een netwerkomgeving



(A): Kantoor 1

❏ (A) – 1: LAN 1

❏ (A) – 2: LAN 2

(B): Kantoor 2

❏ (B) – 1: LAN 1

❏ (B) – 2: LAN 2

(C): WAN

(D): Internet

Introductie van voorbeeld voor scannerverbindingsinstelling

Er zijn twee verbindingsmethoden, afhankelijk van de manier waarop u de scanner gebruikt. Met beide methoden verbindt u de scanner met behulp van de computer en via de hub met het netwerk.

❏ Server/clientverbinding (scanner gebruikt Windows-server, taakbeheer)

❏ Peer-to-peer-verbinding (directe verbinding met de clientcomputer)

Gerelateerde informatie

➡ “Server/clientverbinding” op pagina 12

➡ “Peer to Peer-verbinding” op pagina 12

Server/clientverbinding

Centraliseer scanner- en taakbeheer met Document Capture Pro Server dat op de server is geïnstalleerd. Dit is het meest geschikt voor werk waarbij meerdere scanners worden gebruikt om een groot aantal documenten in een bepaalde indeling te scannen.

Gerelateerde informatie

➡ "Definitie van termen die in deze handleiding worden gebruikt" op pagina 8

Peer to Peer-verbinding

Gebruik een afzonderlijke scanner en een op de clientcomputer geïnstalleerd printerstuurprogramma, zoals Epson Scan 2. Als u Document Capture Pro (Document Capture) op de clientcomputer installeert, kunt u taken uitvoeren op de afzonderlijke clientcomputers van de scanner.

Gerelateerde informatie

➡ "Definitie van termen die in deze handleiding worden gebruikt" op pagina 8

Verbinding met een netwerk voorbereiden

Informatie over de verbindingsinstelling verzamelen

Voor elke netwerkverbinding moet u een IP-adres, gatewayadres, enz. hebben. Controleer vooraf het volgende.

Divisies	Items	Opmerking
Apparaatverbindingsmethode	❏ Ethernet	Gebruik een STP-kabel (Shielded Twisted Pair) van categorie 5e of hoger voor Ethernet-verbindingen.
Informatie over LAN-verbinding	❏ IP-adres ❏ Subnetmasker ❏ Standaardgateway	Als u het IP-adres automatisch instelt met de DHCP-functie van de router, is dit niet vereist.
DNS-serverinformatie	❏ IP-adres voor primaire DNS ❏ IP-adres voor secondaire DNS	Als u als IP-adres een statisch IP-adres gebruikt, moet u de DNS-server configureren. Configureer wanneer u automatisch toewijst met de DHCP-functie en wanneer de DNS-server niet automatisch kan worden toegewezen.
Proxyserverinformatie	❏ Proxyservernaam ❏ Poortnummer	Configureer wanneer u een proxyserver gebruikt voor de internetverbinding en wanneer u de Epson Connect-service of de automatische updatefunctie van de firmware gebruikt.

Scannerspecificaties

De specificatie die de scanner standaard ondersteunt of de verbindingsmodus, zie de *Gebruikershandleiding*.

Poortnummer gebruiken

Zie "Bijlage" voor het poortnummer dat de scanner gebruikt.

Gerelateerde informatie

➡ "Poort voor de scanner gebruiken" op pagina 60

Type IP-adrestoewijzing

Er zijn twee typen voor het toewijzen van een IP-adres aan de scanner.

Statisch IP-adres:

Wijs het vooraf bepaalde, unieke IP-adres toe aan de scanner.

Het IP-adres wordt zelfs niet gewijzigd wanneer de scannerprinter of router wordt uitgeschakeld. U kunt het apparaat dus beheren via het IP-adres.

Dit type is geschikt voor een netwerk waarin veel scanners worden beheerd, zoals een groot kantoor of een school.

Automatische toewijzing door de DHCP-functie:

Het juiste IP-adres wordt automatisch toegewezen wanneer de communicatie tussen de scanner en de router die de DHCP-functie ondersteunt, tot stand wordt gebracht.

Als het onhandig is om het IP-adres voor een bepaald apparaat te wijzigen, reserveert u het IP-adres vooraf en wijst u dit vervolgens toe.

DNS-server en proxyserver

Configureer de DNS-server als u een internetverbindingsservice gebruikt. Als u deze server niet configureert, moet u het IP-adres opgeven. De oplossing met de naam werkt mogelijk niet.

De proxyserver bevindt zich op de gateway tussen het netwerk en internet, en communiceert met en namens de computer, scanner en internet (overstaande server). De overstaande server communiceert alleen met de proxyserver. Scannerinformatie zoals het IP-adres en het poortnummer kunnen daarom niet worden gelezen, waarmee de beveiliging wordt verbeterd.

U kunt de toegang tot een specifieke URL verbieden met de filterfunctie, omdat de proxyserver de inhoud van de communicatie kan controleren.

Methode voor het instellen van de netwerkverbinding

Ga als volgt te werk voor het instellen van verbindingsinstellingen, zoals het IP-adres van de scanner, het subnetmasker en de standaard gateway.

Het bedieningspaneel gebruiken:

Configureer met het bedieningspaneel van elke scanner de instellingen. Maak verbinding met het netwerk nadat u de verbindingsinstellingen voor de scanner hebt geconfigureerd.

Het installatieprogramma gebruiken:

Als u het installatieprogramma gebruikt, worden het netwerk van de scanner en de clientcomputer automatisch ingesteld. U kunt deze instelling configureren als u de instructies van het installatieprogramma volgt, zelfs als u geen diepgaande kennis van het netwerk hebt.

Een hulpprogramma gebruiken:

Gebruik een hulpprogramma vanaf de computer van de beheerder. U kunt een scanner detecteren en vervolgens instellen, of een SYLK-bestand maken om batch-instellingen voor scanners te maken. U kunt veel scanners instellen. Voordat u ze kunt instellen, moeten ze echter fysiek zijn verbinden via de Ethernet-kabel. Dit wordt aanbevolen als u een Ethernet voor de instelling kunt maken.

Gerelateerde informatie

➡ "Verbinding maken met het netwerk vanaf het bedieningspaneel" op pagina 15

➡ "Verbinding maken met het netwerk met behulp van het installatieprogramma" op pagina 19

➡ "Een IP-adres toewijzen met EpsonNet Config" op pagina 56

Verbinding

In dit hoofdstuk wordt de omgeving of de procedure behandeld voor het verbinden van de scanner met het netwerk.

Verbinding maken met het netwerk

Verbinding maken met het netwerk vanaf het bedieningspaneel

Verbindt de printer met het netwerk via het bedieningspaneel van de scanner.

Zie de *Gebruikershandleiding* voor meer informatie over het bedieningspaneel van de scanner.

Het IP-adres toewijzen

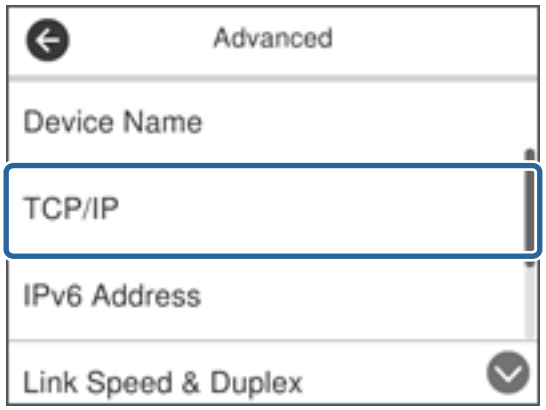
Stel de basisitems in, zoals IP-adres, Subnetmasker en Standaardgateway.

1. Schakel de scanner in.
2. Schuif het scherm op het bedieningspaneel van de scanner naar links en tik vervolgens op **Instel.**.

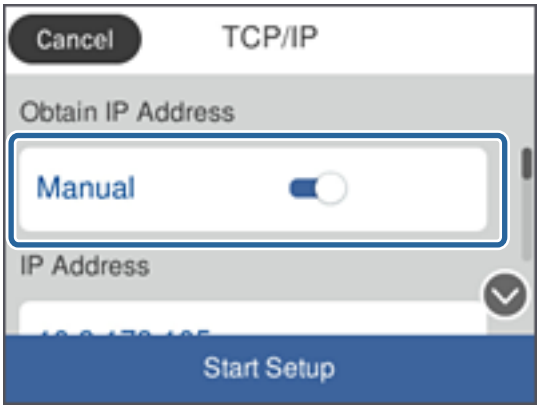
3. Tik op **Netwerkinstellingen** > **Instellingen wijzigen**.

   Als het item niet wordt weergegeven, veegt u het scherm naar boven om dit weer te geven.

4. Tik op **TCP/IP**.

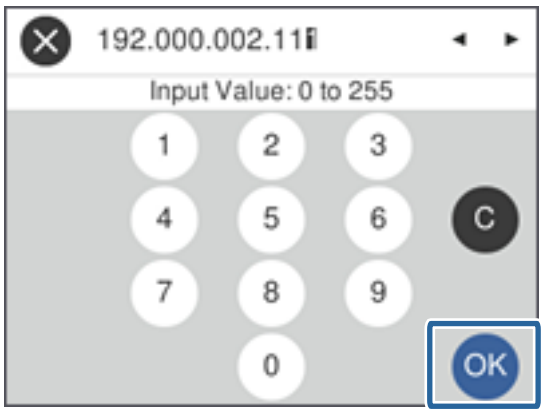


5. Selecteer **Handmatig** voor **IP-adres ophalen**.



Opmerking:
Wanneer u het IP-adres automatisch instelt met de DHCP-functie van de router, selecteert u ***Auto****. In dat geval worden* ***IP-adres****,* ***Subnetmasker*** *en* ***Standaardgateway*** *in stap 6 tot 7 ook automatisch ingesteld. Ga daarom verder naar stap 8.*

6. Tik op het veld **IP-adres**, voer het IP-adres in met het toetsenbord dat op het scherm wordt weergegeven en tik vervolgens op **OK**.



Bevestig de waarde uit het voorgaande scherm.

7. Stel het **Subnetmasker** en de **Standaardgateway** in.

   Bevestig de waarde uit het voorgaande scherm.

   Opmerking:
   *Als de combinatie van IP-adres, Subnetmasker en Standaardgateway onjuist is, dan is **Start installatie** inactief en kunt u niet doorgaan met instellen. Controleer of de invoer geen fouten bevat.*

8. Tik op het veld **Primaire DNS** voor de **DNS-server**, voer met het toetsenbord dat op het scherm wordt weergegeven het IP-adres in voor de primaire DNS-server en tik vervolgens op **OK**.

   Bevestig de waarde uit het voorgaande scherm.

   Opmerking:
   *Wanneer u **Auto** selecteert voor het toewijzen van instellen van het IP-adres, kunt u de instellingen voor de DNS-server selecteren uit **Handmatig** of **Auto**. Als u het DNS-serveradres niet handmatig kunt verkrijgen, selecteert u **Handmatig** en voert u het DNS-serveradres in. Voer daarna het adres van de secundaire DNS-server rechtstreeks in. Als u **Auto** selecteert, gaat u verder naar stap 10.*

9. Tik op het veld **Secundaire DNS**, voer met het toetsenbord dat op het scherm wordt weergegeven het IP-adres in voor de secondaire DNS-server en tik vervolgens op **OK**.

   Bevestig de waarde uit het voorgaande scherm.

10. Tik op **Start installatie**.

11. Tik op het bevestigingsscherm op **Sluiten**.

    Het scherm sluit automatisch na een vastgestelde tijd als u niet op **Sluiten** tikt.

Verbinding maken met Ethernet

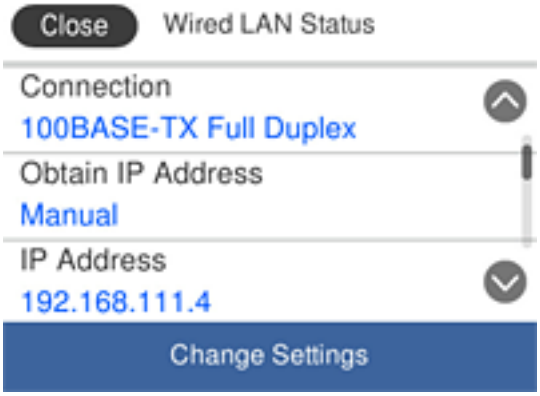
Verbind de scanner met het netwerk met de Ethernet-kabel en controleer de verbinding.

1. Sluit de scanner en hub (L2-switch) aan met een Ethernet-kabel.

   Het pictogram op het startscherm verandert in  .

2. Tik op het startscherm op  .

3. Veeg het scherm naar boven en controleer of de verbindingsstatus en het IP-adres correct zijn.



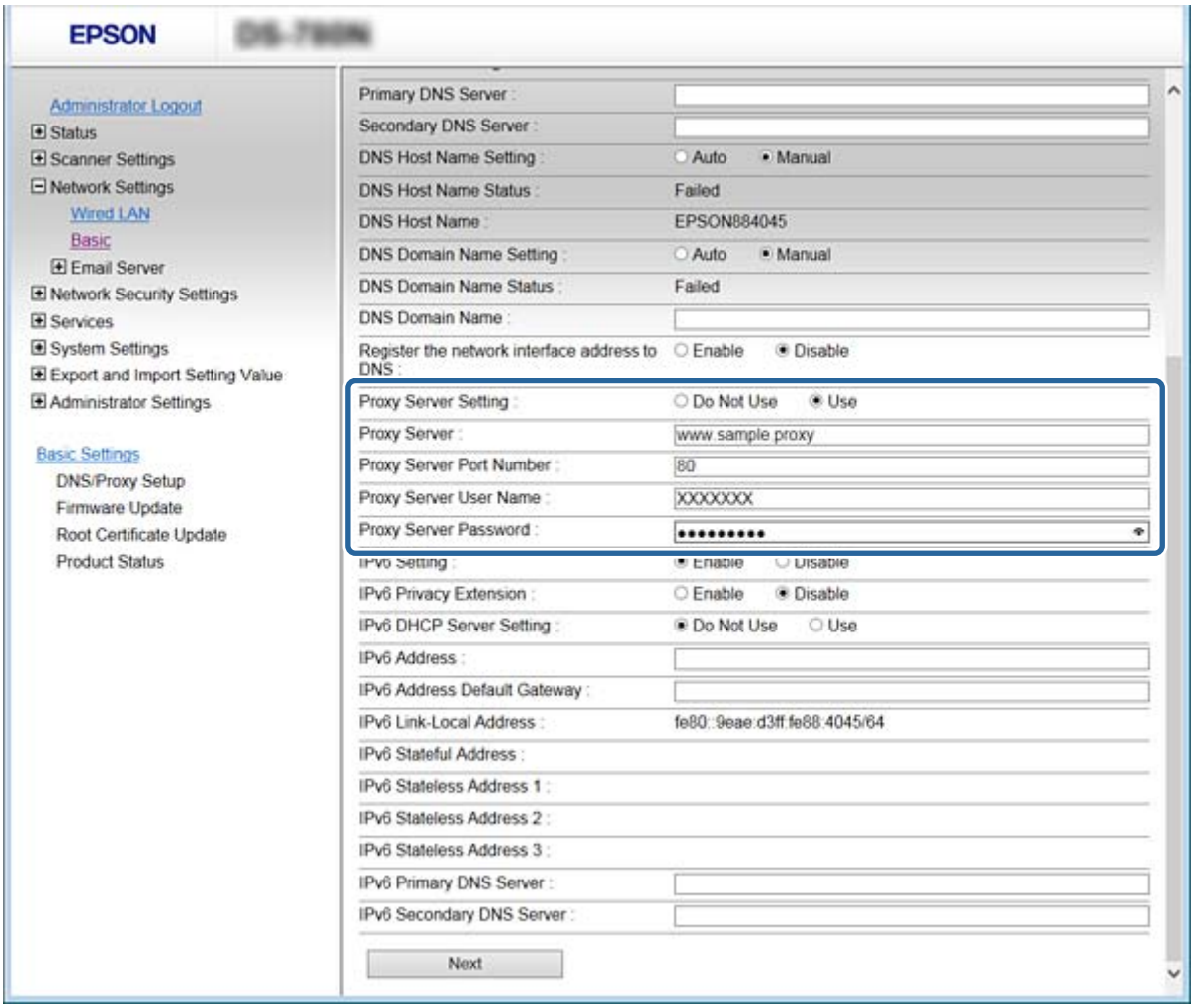
De proxyserver instellen

De proxyserver kan niet worden ingesteld op het paneel. Configureer met Web Config.

1. Open Web Config en selecteer **Network Settings** > **Basic**.
2. Selecteer **Use** in **Proxy Server Setting**.
3. Geef de proxyserver op in IPv4-address of FQDN-indeling in **Proxy-server** en voer vervolgens in **Proxy Server Port Number** het poortnummer in.

   Voor proxyservers waarvoor verificatie is vereis, voert u de gebruikersnaam en het wachtwoord voor de proxyserververificatie in.

4. Klik op de knop **Next**.



5. Bevestig de instellingen en klik vervolgens op **Instel.**.

Gerelateerde informatie

➡ "Web Config openen" op pagina 23

Verbinding maken met het netwerk met behulp van het installatieprogramma

Het wordt aanbevolen de het installatieprogramma te gebruiken om de scanner te verbinden met een computer. U kunt het installatieprogramma op een van de volgende manieren uitvoeren.

❏ Instellen vanaf de website

Open de volgende website en voer de productnaam in. Ga naar **Instellen** en configureer de instellingen.

http://epson.sn

❏ Instellen met de software-cd (alleen voor modellen die worden geleverd met een software-cd en gebruikers die beschikken over een computer met een schijfstation.)

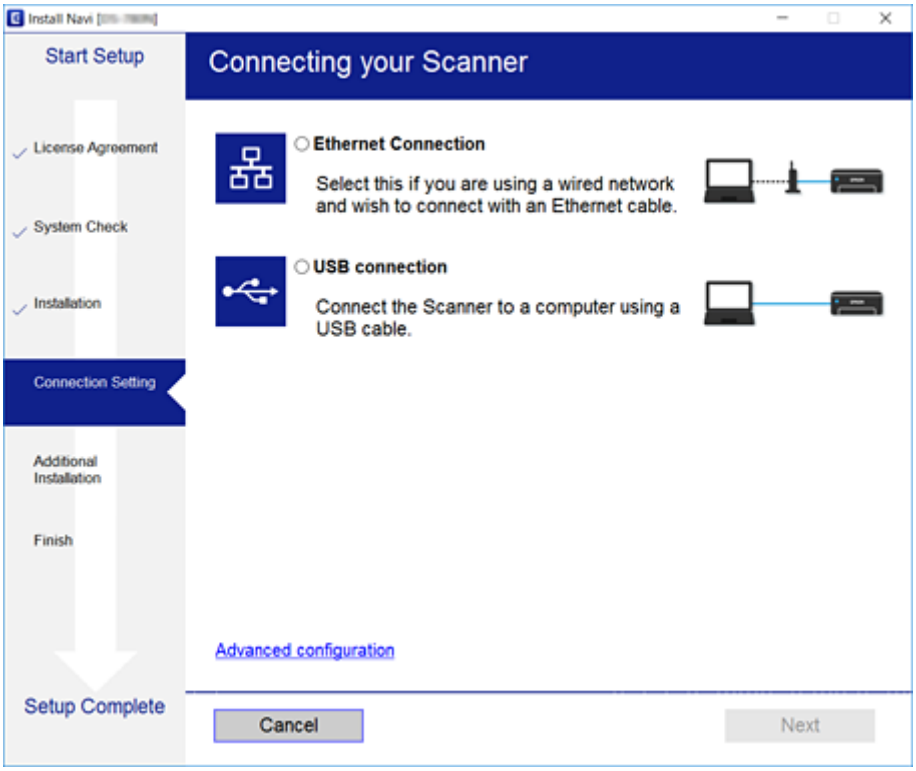
Plaats de software-cd in de computer en volg de instructies op het scherm.

De verbindingsmethoden selecteren

Volg de instructies op het scherm totdat het volgende scherm wordt weergegeven en selecteer vervolgens de gewenste methode om de scanner met de computer te verbinden.

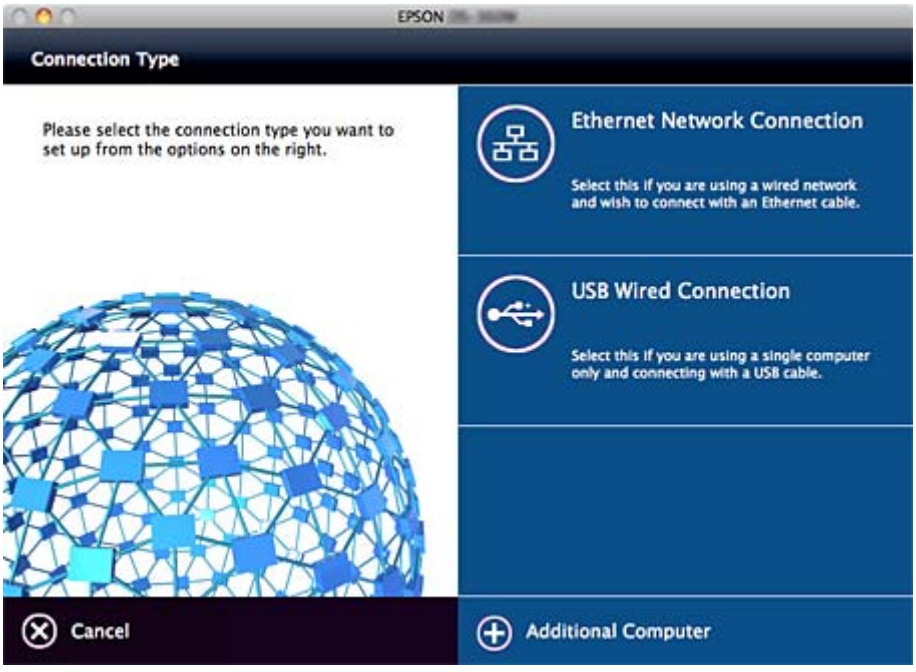
❏ Windows

Selecteer het verbindingstype en klik vervolgens op **Volgende**.



❏ Mac OS

Selecteer het verbindingstype.



Verbinding

Volg de instructies op het scherm. De benodigde software wordt geïnstalleerd.

Functie-instellingen

Dit hoofdstuk bevat informatie over de eerste instellingen die nodig zijn om elke functie van het apparaat te kunnen gebruiken.

Software voor het configureren van instellingen

Dit onderwerp bevat informatie over de procedure voor het configureren van instellingen vanaf de computer van de beheerder met Web Config.

Web Config (webpagina voor apparaat)

Over Web Config

Web Config is een toepassing die draait in een browser en dient om de instellingen van de scanner te configureren.

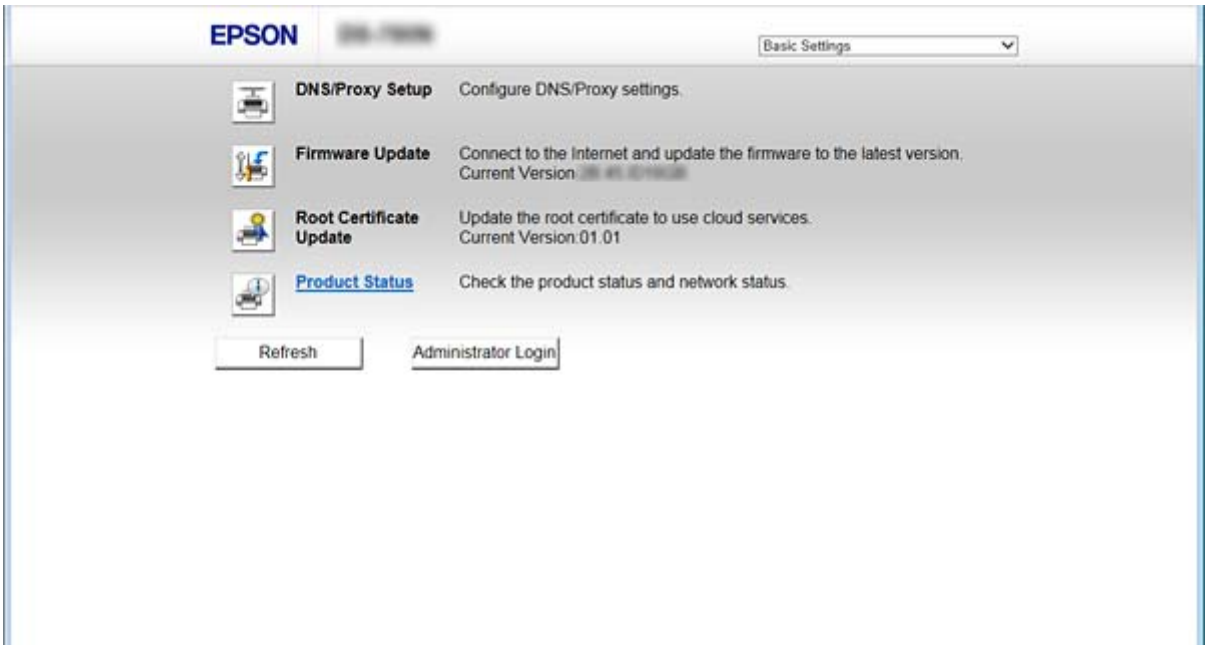
Voordat u toegang krijgt tot Web Config moet u eerst IP-adres toewijzen aan de scanner.

Opmerking:
U kunt de instellingen vergrendelen door een beheerderswachtwoord in te stellen op de scanner.

Er zijn twee pagina's met instellingen (zie hierna).

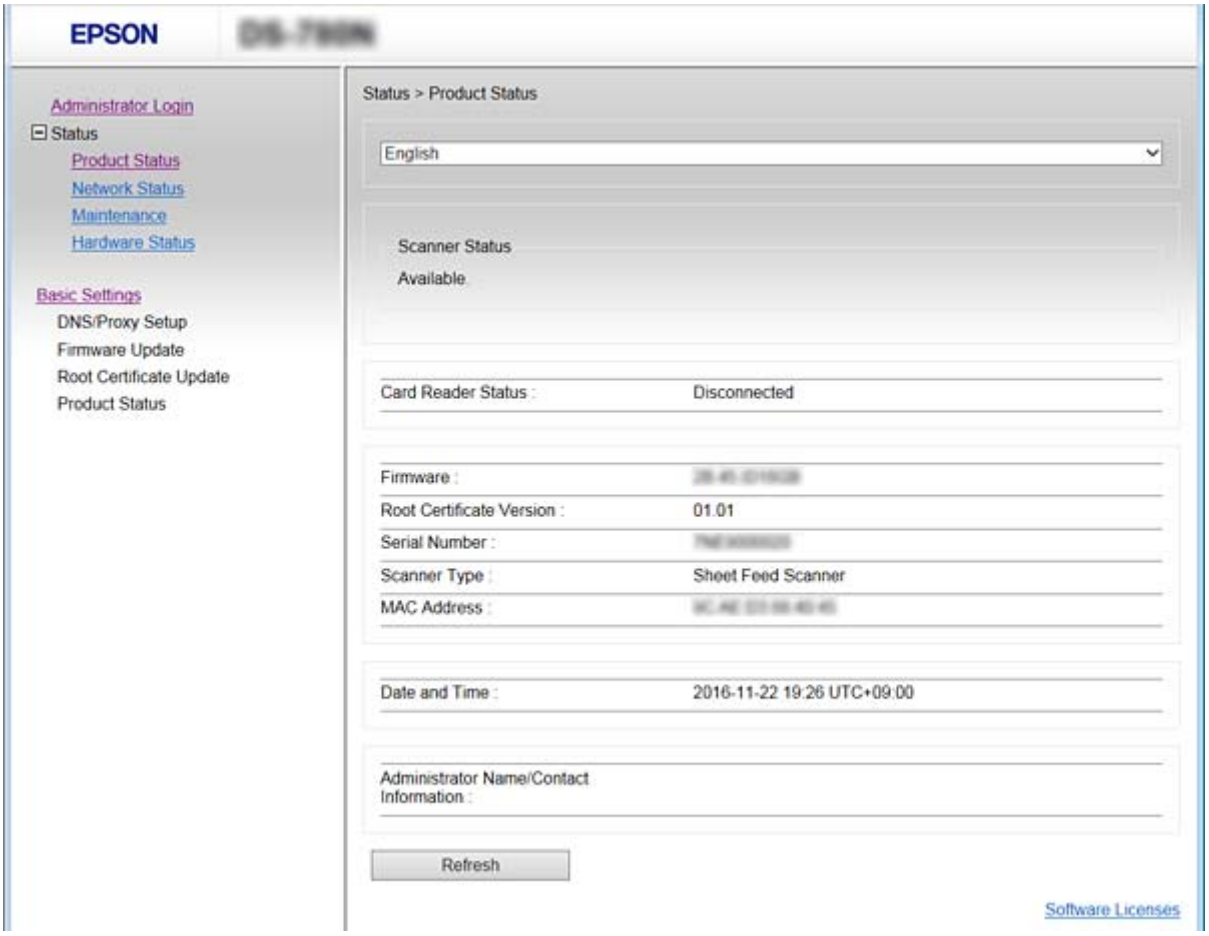
❏ **Basic Settings**

Op deze pagina kunt u de basisinstellingen voor de scanner configureren.



❏ **Advanced Settings**

Op deze pagina kunt u de geavanceerde instellingen voor de scanner configureren. Deze pagina is vooral bedoeld voor systeembeheerders.



Web Config openen

Voer het IP-adres van de scanner in een webbrowser in. JavaScript moet ingeschakeld zijn. Wanneer u Web Config opent via HTTPS, wordt in de browser een waarschuwingsbericht weergegeven, omdat een zelfondertekend certificaat wordt gebruikt, dat in de scanner is opgeslagen.

❏ Openen via HTTPS

IPv4: https://<IP-adres van scanner> (zonder < >)

IPv6: https://[IP-adres van scanner]/ (met [ ])

❏ Openen via HTTP

IPv4: http://<IP-adres van scanner> (zonder < >)

IPv6: http://[IP-adres van scanner]/ (met [ ])

Opmerking:

❏ *Voorbeelden*

IPv4:

https://192.0.2.111/

http://192.0.2.111/

IPv6:

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

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

❏ *Als de scannernaam bij de DNS-server is geregistreerd, kunt u de naam van de scanner gebruiken in plaats van het IP-adres.*

Gerelateerde informatie

➡ "SSL/TLS-communicatie met de scanner" op pagina 63

➡ "Digitale certificering" op pagina 63

Scanfuncties gebruiken

Afhankelijk van de manier waarop u de scanner gebruikt, installeert u de volgende software en configureert u de instellingen voor het gebruik.

❏ **Scannen vanaf een computer**

❏ Bevestig de geldigheid van de netwerkscanservice met Web Config (geldig bij fabriekslevering).

❏ Installeer Epson Scan 2 op uw computer en stel het IP-adres in

❏ Wanneer u scant met behulp van taken, installeert u Document Capture Pro (Document Capture) en configureert u de taakinstellingen.

❏ **Scannen vanaf het bedieningspaneel**

❏ Wanneer u Document Capture Pro of Document Capture Pro Server gebruikt:

Installeer Document Capture Pro of Document Capture Pro Server

DCP-instelling (servermodus, clientmodus).

❏ Wanneer u het WSD-protocol gebruikt:

Bevestig de geldigheid van WSD in Web Config of het bedieningspaneel (geldig bij fabriekslevering)

Aanvullende apparaatinstellingen (Windows-computer).

Scannen vanaf een computer

Installeer de software en controleer of de netwerkscanservice is ingeschakeld om via het netwerk te scannen vanaf de computer.

Gerelateerde informatie

➡ "Software die moet worden geïnstalleerd" op pagina 25

➡ "Netwerkscannen inschakelen" op pagina 25

Software die moet worden geïnstalleerd

❏ Epson Scan 2

Dit is een scannerstuurprogramma. Als u het apparaat gebruikt vanaf een computer, moet u het stuurprogramma op elke clientcomputer installeren. Als Document Capture Pro/Document Capture is geïnstalleerd, kunt u de bewerkingen uitvoeren die aan de knoppen van het apparaat zijn toegewezen.

Met EpsonNet SetupManager kunnen printerstuurprogramma's ook samen in pakketten worden gedistribueerd.

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

Installeer op de clientcomputer. Vanaf een computer of het bedieningspaneel van de scanner kunt u via het netwerk taken oproepen en uitvoeren die zijn geregistreerd op een computer waarop Document Capture Pro/Document Capture is geïnstalleerd.

U kunt ook scannen vanaf de computer via het netwerk. Epson Scan 2 is vereist om te kunnen scannen.

Gerelateerde informatie

➡ "EpsonNet SetupManager" op pagina 56

Stel het IP-adres van de scanner in op Epson Scan 2

Geef het IP-adres van de scanner op zodat de scanner in het netwerk kan worden gebruikt.

1. Start **Epson Scan 2 Utility** vanuit **Start** > **Alle programma's** > **EPSON** > **Epson Scan 2**.

   Als er al een andere scanner is geregistreerd, gaat u verder naar stap 2.

   Als er nog geen scanner is geregistreerd, gaat u verder naar stap 4.

2. Klik op ▼ bij **Scanner**.
3. Klik op **Instellingen**.
4. Klik op **Bewerken inschakelen** en klik vervolgens op **Toevoegen**.
5. Selecteer de naam van het scannermodel in **Model**.
6. Selecteer het IP-adres van de scanner die moet worden gebruikt bij **Adres** in **Netwerk zoeken**.

   Klik op  en klik op  om de lijst bij te werken. Als u het IP-adres van de scanner niet kunt vinden, selecteert u **Adres opgeven** en voert u het IP-adres in.

7. Klik op **Toevoegen**.
8. Klik op **OK**.

Netwerkscannen inschakelen

U kunt de netwerkscanservice inschakelen wanneer u via het netwerk scant vanaf een clientcomputer. De standaardinstelling wordt ingeschakeld.

1. Open Web Config en selecteer **Services** > **Network Scan**.

2. Controleer of **Enable scanning** voor **EPSON Scan** is geselecteerd.

   Als deze optie is geselecteerd, is deze taak voltooid. Sluit Web Config.

   Als het selectievakje niet is ingeschakeld, schakelt u dit in en gaat u verder naar de volgende stap.

3. Klik op **Next**.

4. Klik op **OK**.

   Er wordt opnieuw verbinding gemaakt met het netwerk en de instellingen worden ingeschakeld.

Gerelateerde informatie

➡ "Web Config openen" op pagina 23

Scannen via het bedieningspaneel

De functies scannen naar map en scannen naar e-mail via het bedieningspaneel van de scanner, evenals de overdracht van scanresultaten naar e-mail, mappen enz. worden uitgevoerd door de taak vanaf de computer uit te voeren.

Als u scanresultaten wilt overbrengen, stelt u de taak in met Document Capture Pro Server of Document Capture Pro.

Raadpleeg voor meer informatie over instellingen en het instellen van de taak de documentatie of Help van Document Capture Pro Server of Document Capture Pro.

Gerelateerde informatie

➡ "Instellingen voor Document Capture Pro Server/Document Capture Pro" op pagina 26

➡ "Servers en mappen instellen" op pagina 27

Software die op de computer moet worden geïnstalleerd

❏ **Document Capture Pro Server**

Dit is de serverversie van Document Capture Pro. Installeer deze software op een Windows-server. Door de server kunnen meerdere apparaten en taken centraal worden beheerd. Taken kunnen tegelijkertijd op meerdere scanners worden uitgevoerd.

Als u de gecertificeerde versie van Document Capture Pro Server gebruikt, kunt u taken en scangeschiedenis beheren die zijn gekoppeld aan gebruikers en groepen.

Neem voor meer informatie over Document Capture Pro Server contact op met uw plaatselijke Epson-kantoor.

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

Net zoals u vanaf een computer kunt scannen, kunt u taken die op de computer zijn geregistreerd oproepen vanaf het bedieningspaneel en deze uitvoeren. Het is niet mogelijk om taken die op een computer zijn geregistreerd op meerdere scanners tegelijk uit te voeren.

Instellingen voor Document Capture Pro Server/Document Capture Pro

Configureer instellingen voor het gebruik van de scanfunctie vanaf het bedieningspaneel van de scanner.

1. Open Web Config en selecteer **Services** > **Document Capture Pro**.

2. Selecteer **Bedieningsmodus**.

   ❏ Server Mode:

   Selecteer deze optie wanneer u Document Capture Pro Server gebruikt of wanneer u Document Capture Pro alleen gebruikt voor taken die zijn ingesteld voor een specifieke computer.

   ❏ Client Mode:

   Stel deze optie in wanneer u de taakinstelling selecteert vanuit Document Capture Pro (Document Capture) die op elke clientcomputer in het netwerk is geïnstalleerd zonder de computer op te geven.

3. Stel het volgende in op basis van de geselecteerde modus.

   ❏ Server Mode:

   Geef in **Server Address** de server op waarop Document Capture Pro Server is geïnstalleerd. Deze mag tussen 2 en 252 tekens lang zijn. Gebruik de IPv4-, IPv6- of FQDN-indeling of de hostnaam. In de FQDN-indeling mogen US-ASCII-letters, -cijfers, -alfabetten en koppelstreepjes (met uitzondering van het begin en het eind) worden gebruikt.

   ❏ Client Mode:

   Geef het **Group Settings** op om een scannergroep te gebruiken die is opgegeven in Document Capture Pro (Document Capture).

4. Klik op **Instel.**.

Gerelateerde informatie

➡ "Web Config openen" op pagina 23

Servers en mappen instellen

Document Capture Pro en Document Capture Pro Server slaan de gescande gegevens een keer op naar de server of de clientcomputer en gebruiken de overdrachtsfunctie om de functies scannen naar map en scannen naar e-mail uit te voeren.

U hebt de machtigingen en de informatie nodig voor overdracht vanaf de computer waarop Document Capture Pro, Document Capture Pro Server is geïnstalleerd naar de computer of cloudservice.

Bereid aan de hand van het onderstaande de informatie voor de functie die u gaat gebruiken voor.

U kunt instellingen voor deze functies configureren met Document Capture Pro of Document Capture Pro Server. Raadpleeg voor meer informatie over de instellingen de documentatie of Help van Document Capture Pro Server of Document Capture Pro.

Naam	Instellingen	Vereiste
Scannen naar netwerkmap (SMB)	Delen van de map voor opslag maken en instellen	Het beheerdersaccount voor de computer waarop mappen voor opslag worden gemaakt.
	Bestemming voor scannen naar netwerkmap (SMB)	Gebruikersnaam en wachtwoord voor aanmelden op de computer waarop zich de map voor opslaan bevindt, en de machtiging om de map voor opslaan bij te werken.
Scannen naar netwerkmap (FTP)	Instellen voor aanmelden bij de FTP-server	Aanmeldinformatie voor de FTP-server en de machtiging om de map voor opslaan bij te werken.

Naam	Instellingen	Vereiste
Scannen naar e-mail	Instellen voor e-mailserver	Instelinformatie voor e-mailserver
Scannen naar Document Capture Pro (wanneer u Document Capture Pro Server gebruikt)	Instellingen voor logboekregistratie in cloudservices	Omgeving voor internetverbinding Registratie van het account voor cloudservices

WSD-scan gebruiken (alleen Windows)

Als op de computer Windows Vista of nieuwer wordt uitgevoerd, kunt u WSD-scan gebruiken.

Als het WSD-protocol kan worden gebruikt, wordt het menu **Computer (WSD)** weergegeven op het bedieningspaneel van de scanner.

1. Open Web Config en selecteer **Services** > **Protocol**.
2. Controleer of **Enable WSD** is ingeschakeld in **WSD Settings**.

   Als dit is ingeschakeld, is uw taak voltooid en kunt u Web Config sluiten.

   Als dit niet is ingeschakeld, schakelt u dit nu in en gaat u verder naar de volgende stap.
3. Klik op de knop **Next**.
4. Bevestig de instellingen en klik op **Instel.**.

Systeeminstellingen configureren

De systeeminstellingen configureren op het bedieningspaneel

De helderheid van het scherm instellen

Stel de helderheid van het lcd-scherm in.

1. Tik op het startscherm op **Instel.**.
2. Tik op **Algemene instellingen** > **Lcd-helderheid**.
3. Tik op  of  om de helderheid aan te passen.

   U kunt de helderheid aanpassen van 1 tot 9.
4. Tik op **OK**.

Het geluid instellen

Stel het bedieningsgeluid en het foutgeluid in.

1. Tik op het startscherm op **Instel.**.
2. Tik op **Algemene instellingen** > **Geluid**.
3. Configureer desgewenst de volgende instellingen.
   - ❏ Bedieningsgeluid
     Stel het volume in van het bedieningsgeluid van het bedieningspaneel.
   - ❏ Foutgeluid
     Stel het volume in van het foutgeluid.
4. Tik op **OK**.

Gerelateerde informatie

➡ "Web Config openen" op pagina 23

Dubbele invoer van origineel detecteren

Bepaal of u de functie wilt instellen voor detectie van dubbele invoer van het origineel en om het scannen te stoppen wanneer dubbele invoer plaatsvindt.

Schakel de functie uit voor originelen die altijd dubbel worden ingevoerd, zoals enveloppen of papieren met stickers.

Opmerking:
De functie kan worden ingesteld in Web Config of Epson Scan 2.

1. Tik op het startscherm op **Instel.**.
2. Tik op **Externe Scaninstellingen** > **Ultrasone detectie dubbele toevoer**.
3. Tik op **Ultrasone detectie dubbele toevoer** om de functie in of uit te schakelen.
4. Tik op **Sluiten**.

De modus voor lage snelheid instellen

Stel deze optie in als u op lage snelheid wilt scannen, om te voorkomen dat papier vastloopt, bijvoorbeeld bij het scannen van dunne originelen, zoals doorslagen.

1. Tik op het startscherm op **Instel.**.
2. Tik op **Externe Scaninstellingen** > **Langzaam**.
3. Tik op **Langzaam** om de functie in of uit te schakelen.
4. Tik op **Sluiten**.

Systeeminstellingen configureren met Web Config

Instellingen voor energiebesparing tijdens inactiviteit

Configureer de instellingen voor energiebesparing tijdens perioden van inactiviteit van de scanner. Stel de tijd in op basis van uw gebruiksomgeving.

Opmerking:
Op het bedieningspaneel van de scanner kunt u ook de instellingen voor energiebesparing configureren.

1. Open Web Config en selecteer **System Settings** > **Power Saving**.
2. Voer de tijdsduur in waarna de **Sleep Timer** energiebesparing moet inschakelen in geval van inactiviteit.

   U kunt dit per minuut instellen op een periode tot maximaal 240 minuten.
3. Selecteer de uitschakeltijd voor de **Power Off Timer**.
4. Klik op **OK**.

Gerelateerde informatie

➡ "Web Config openen" op pagina 23

Het bedieningspaneel instellen

Instellen van het bedieningspaneel van de scanner. U kunt dit als volgt instellen.

1. Open Web Config en selecteer **System Settings** > **Control Panel**.
2. Configureer desgewenst de volgende instellingen.
   - ❏ Language

     Selecteer de taal die op het bedieningspaneel wordt weergegeven.
   - ❏ Panel Lock

     Als u **ON** selecteert, is het beheerderswachtwoord vereist wanneer u een bewerking uitvoert waarvoor beheerderstoestemming vereist is. Als het beheerderswachtwoord niet is ingesteld, is paneelvergrendeling uitgeschakeld.
   - ❏ Operation Timeout

     Als u **ON** selecteert wordt u, als u bent aangemeld als beheerder, automatisch afgemeld en gaat u naar het beginscherm als er gedurende een vastgestelde periode geen activiteit is.

     U kunt dit per seconde instellen op een periode tussen 10 seconden en 240 minuten.
3. Klik op **OK**.

Gerelateerde informatie

➡ "Web Config openen" op pagina 23

Beperking voor de externe interface instellen

U kunt de USB-verbinding vanaf de computer beperken. Stel deze optie in om scannen via een andere methode dan via het netwerk te beperken.

1. Open Web Config en selecteer **System Settings** > **External Interface**.
2. Selecteer **Enable** of **Disable**.

   Om een beperking in te stellen, selecteert u **Disable**.
3. Tik op **OK**.

Datum en tijd synchroniseren met de tijdserver

Als u een CA-certificaat gebruikt, kunt u gedoe met de tijd voorkomen.

1. Open Web Config en selecteer **System Settings** > **Date and Time** > **Time Server**.
2. Selecteer **Use** voor **Use Time Server**.
3. Voer het tijdserveradres in voor **Time Server Address**.

   U kunt IPv4, IPv6 of FQDN-indeling gebruiken. Voer maximaal 252 tekens in. Laat dit leeg als u dit niet wilt opgeven.
4. Voer de **Update Interval (min)** in.

   U kunt dit per minuut instellen op een periode tot maximaal 10.800 minuten.
5. Klik op **OK**.

   Opmerking:
   *U kunt de verbindingsstatus met de tijdserver bevestigen in **Time Server Status**.*

Gerelateerde informatie

➡ “Web Config openen” op pagina 23

Basisinstellingen voor beveiliging

Dit hoofdstuk bevat informatie over de basisinstellingen voor beveiliging waarvoor geen speciale omgeving vereist is.

Inleiding tot basisfuncties voor beveiliging

In dit hoofdstuk introduceren we de basisfuncties voor beveiliging van Epson-apparaten.

Functienaam	Type functie	Wat kunt u instellen	Wat voorkomt u
Instellen van beheerderswachtwoord	Vergrendel de instellingen die met het systeem verband houden, zoals instellingen voor het netwerk en de USB-verbinding, zodat deze alleen kunnen worden gewijzigd door de beheerder.	Het wachtwoord voor het apparaat wordt ingesteld door een beheerder. Configureren of bijwerken zijn overal beschikbaar vanuit Web Config, het bedieningspaneel, Epson Device Admin, en EpsonNet Config.	Voorkom het illegaal lezen en wijzigen van de informatie die in het apparaat is opgeslagen, zoals id, wachtwoord, netwerkinstellingen en contacten. Verminder het aantal beveiligingsrisico's zoals het lekken van informatie voor de netwerkomgeving of het beveiligingsbeleid.
SSL/TLS-communicatie	Wanneer u een Epson-server opent op internet vanaf een apparaat, bijvoorbeeld bij communicatie met een computer via een browser of een firmware-update, wordt de inhoud van de communicatie versleuteld met SSL/TLS-communicatie.	Verkrijg een CA-ondertekend certificaat en importeer dit naar de scanner.	Als u een identificatie wist van het apparaat met een CA-ondertekend certificaat, voorkomt u imitatie en ongeoorloofde toegang. Bovendien wordt communicatie-inhoud van SSL/TLS beschermd en wordt lekken van inhoud voor het afdrukken van gegevens in instellingsinformatie voorkomen.
Beheer van protocollen	Beheert protocollen die worden gebruikt voor communicatie tussen apparaten en computers en schakelt functies in en uit.	Een protocol dat of een service die is toegepast op afzonderlijk toegestane of verboden functies.	Voorkomen van beveiligingsrisico's die kunnen optreden via onbedoeld gebruik door gebruik van onnodige functies door gebruikers te voorkomen.

Gerelateerde informatie

➡ “Over Web Config” op pagina 22
➡ “EpsonNet Config” op pagina 55
➡ “Epson Device Admin” op pagina 55
➡ “Het beheerderswachtwoord configureren” op pagina 33
➡ “Protocollen beheren” op pagina 35

Het beheerderswachtwoord configureren

Wanneer u het beheerderswachtwoord instelt, kunnen gebruikers die geen beheerder zijn de instellingen voor het systeembeheer niet wijzigen. U kunt het beheerderswachtwoord instellen en wijzigen met Web Config, het bedieningspaneel van de scanner, of met de volgende software: (Epson Device Admin of EpsonNet Config). Wanneer u de software gebruikt, raadpleegt u de documentatie voor het betreffende softwarepakket.

Gerelateerde informatie

➡ "Het beheerderswachtwoord configureren vanaf het bedieningspaneel" op pagina 33

➡ "Het beheerderswachtwoord configureren met Web Config" op pagina 33

➡ "EpsonNet Config" op pagina 55

➡ "Epson Device Admin" op pagina 55

Het beheerderswachtwoord configureren vanaf het bedieningspaneel

U kunt het beheerderswachtwoord instellen vanaf het bedieningspaneel van de scanner.

1. Tik op het startscherm op **Instel.**.
2. Tik op **Systeembeheer** > **Beheerdersinstellingen**.

   Als het item niet wordt weergegeven, veegt u het scherm naar boven om het item weer te geven.
3. Tik op **Beheerderswachtwoord** > **Registreren**.
4. Voer het nieuwe wachtwoord in en tik vervolgens op **OK**.
5. Voer het wachtwoord opnieuw in en tik vervolgens op **OK**.
6. Tik op het bevestigingsscherm op **OK**.

   Het scherm met beheerdersinstellingen wordt weergegeven.
7. Tik op **Instelling vergrendelen** en tik vervolgens op het bevestigingsscherm op **OK**.

   Instelling vergrendelen is ingesteld op **Aan** en het beheerderswachtwoord moet worden ingevoerd wanneer u het vergrendelde menu-item wilt bedienen.

Opmerking:

❏ *Als u **Instel.** > **Algemene instellingen** > **Time-out bewerking** instelt op **Aan**, wordt u na een vastgestelde periode van inactiviteit bij het bedieningspaneel afgemeld.*

❏ *U kunt het beheerderswachtwoord wijzigen of wissen wanneer u **Wijzigen** of **Resetten** selecteert in het scherm **Beheerderswachtwoord** en het wachtwoord invoert.*

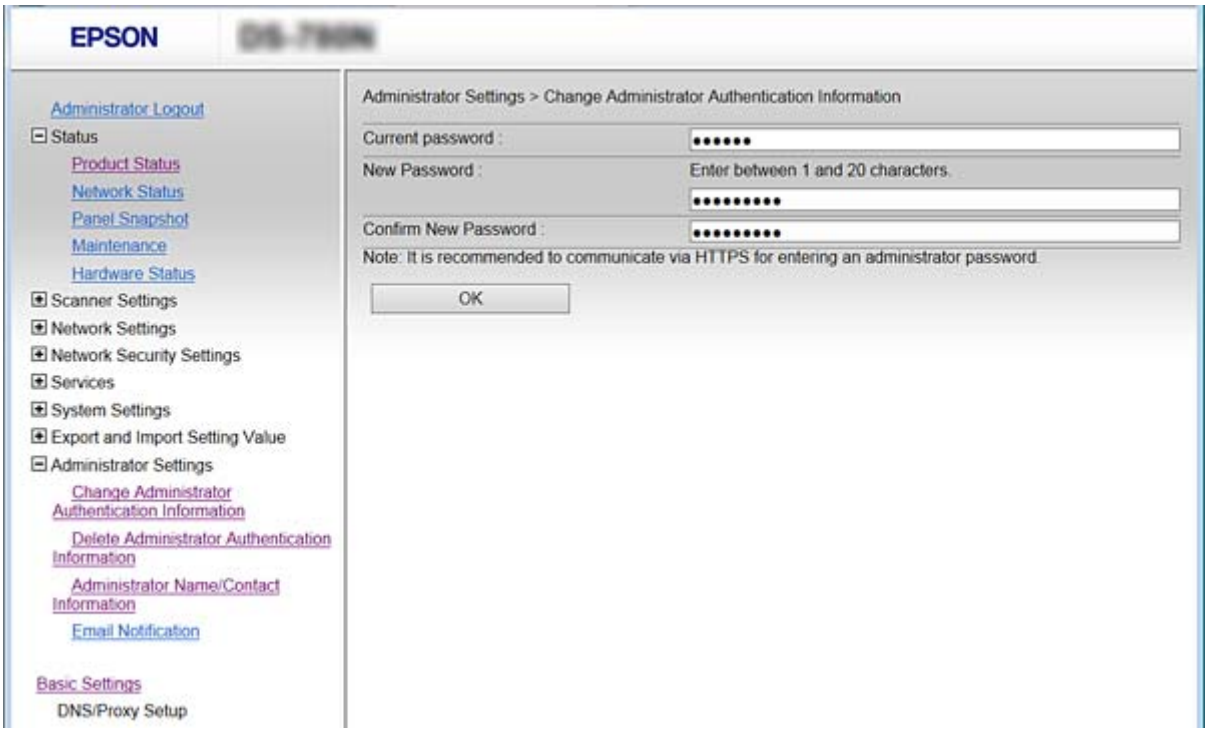
Het beheerderswachtwoord configureren met Web Config

Met Web Config kunt u het beheerderswachtwoord instellen.

1. Open Web Config en selecteer **Administrator Settings** > **Change Administrator Authentication Information**.

2. Voer een wachtwoord in bij **New Password** en **Confirm New Password**. Voer indien nodig de gebruikersnaam in.

   Voer het huidige wachtwoord in als u dit wilt veranderen in een nieuw wachtwoord.



3. Selecteer **OK**.

   Opmerking:

   ❏ *Als u de vergrendelde menu-items wilt instellen of wijzigen, klikt u op **Administrator Login** en voert u het beheerderswachtwoord in.*

   ❏ *Als u het beheerderswachtwoord wilt wissen, klikt u op **Administrator Settings** > **Delete Administrator Authentication Information** en voer u het beheerderswachtwoord in.*

Gerelateerde informatie

➡ "Web Config openen" op pagina 23

Items die moeten worden vergrendeld met een beheerderswachtwoord

Beheerders hebben machtigingen voor instellen en wijzigen voor alle functies op de apparaten.

Als u het beheerderswachtwoord instelt op het apparaat, kunt u dit bovendien vergrendelen zodat de instellingen voor apparaatbeheer niet kunnen worden gewijzigd.

De volgende items kunnen worden beheerd door een beheerder.

Item	Beschrijving
Scannerinstelling	De detectie voor dubbele invoer en de modus voor lage snelheid instellen.

Basisinstellingen voor beveiliging

Item	Beschrijving
Verbindingsinstellingen voor Ethernet	De naam van apparaten en het IP-adres wijzigen, de DNS-server of proxyserver instellen en instellingen wijzigen die verband houden met de netwerkverbindingen.
Instelling voor gebruikersservices	Instelling voor het beheren van communicatieprotocollen, scannen via het netwerk en Document Capture Pro-services.
Instelling e-mailserver	Instellen van een e-mailserver waar apparaten rechtstreeks mee communiceren.
Beveiligingsinstelling	Instellingen voor netwerkbeveiliging, zoals SSL/TLS-communicatie, IPsec/IP-filtering en IEEE802.1X.
Update voor basiscertificaat	Update van basiscertificaat vereist voor Document Capture Pro Server-verificatie en firmware-update van Web Config.
Firmware-update	De firmware van apparaten controleren en bijwerken.
Tijd, timerinstelling	Overgangstijd slaapmodus, automatisch uitschakelen, datum/tijd, timer voor inactiviteit, andere timerinstellingen.
Standaardinstellingen herstellen	Instelling om de standaardinstellingen van de scanner te herstellen.
Beheerdersinstelling	Instellen van beheerdersvergrendeling of beheerderswachtwoord.
Instelling van gecertificeerd apparaat	Instellen van de id van het verificatieapparaat. Stel deze optie in wanneer u de scanner gebruikt in een verificatiesysteem dat ondersteuning biedt voor verificatieapparaten.

Protocollen beheren

U kunt scannen via verschillende paden en protocollen. U kunt netwerkscannen ook gebruiken vanaf een niet nader gespecificeerd aantal netwerkcomputers. Bijvoorbeeld alleen scannen via opgegeven paden en protocollen is toegestaan. U kunt ondoelmatige beveiligingsrisico's verminderen door scannen vanaf specifieke paden te beperken of door de beschikbare functies te beheren.

Configureer de protocol-instellingen.

1. Open Web Config en selecteer **Services** > **Protocol**.
2. Configureer elk item.
3. Klik op **Next**.
4. Klik op **OK**.

   De instellingen worden toegepast op de scanner.

Gerelateerde informatie

➡ “Web Config openen” op pagina 23
➡ “Protocollen die u kunt inschakelen of uitschakelen” op pagina 36
➡ “Protocolinstellingsitems” op pagina 37

Protocollen die u kunt inschakelen of uitschakelen

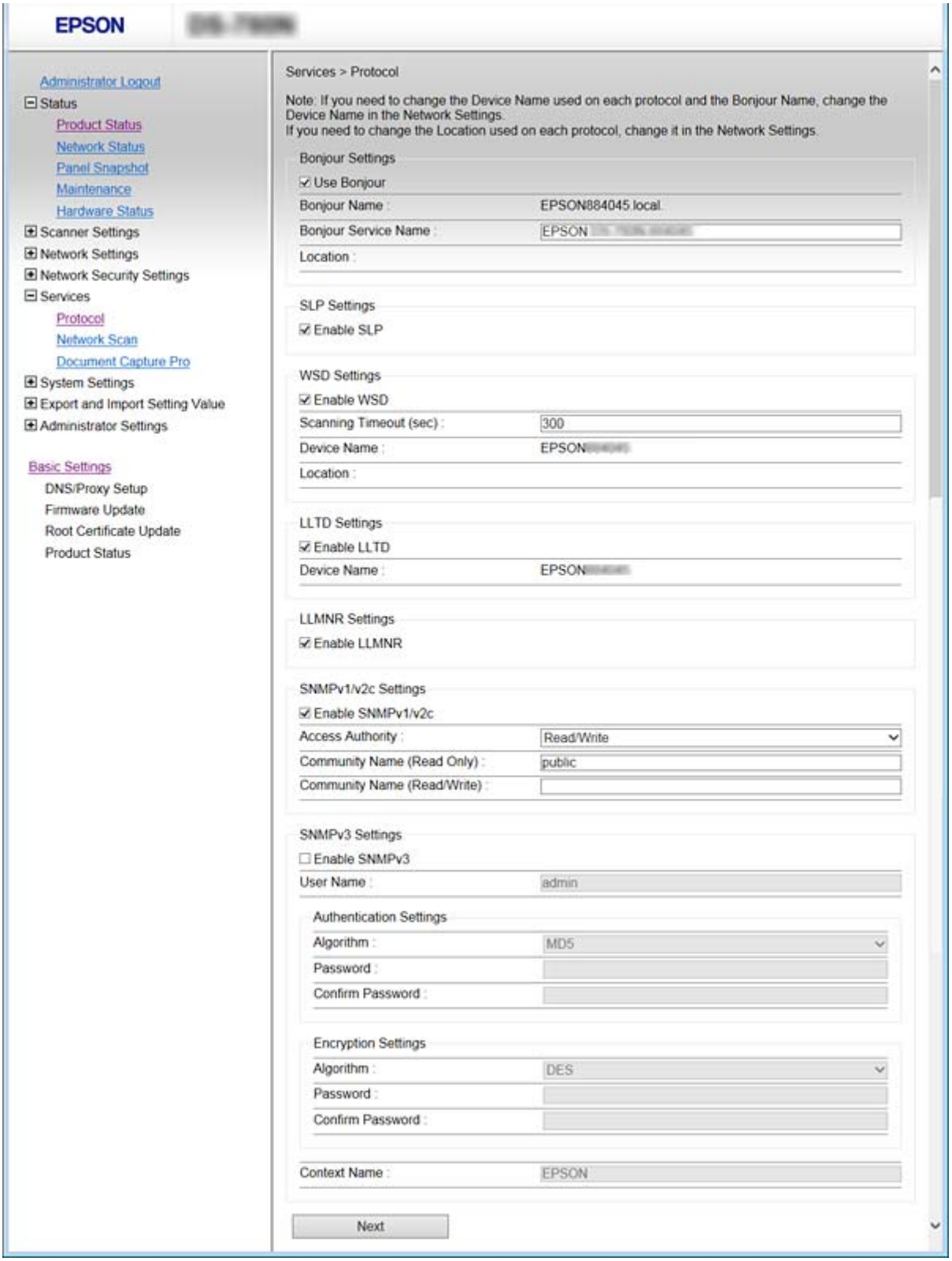
Protocol	Beschrijving
Bonjour Settings	U kunt opgeven of Bonjour moet worden gebruikt. Bonjour wordt gebruikt voor het zoeken van apparaten, scannen, enz.
SLP Settings	U kunt de SLP-functie in- of uitschakelen. SLP wordt gebruikt voor Epson Scan 2 en netwerk zoeken in EpsonNet Config.
WSD Settings	U kunt de WSD-functie in- of uitschakelen. Wanneer dit is ingeschakeld, kunt u WSD-apparaten toevoegen of scannen vanaf de WSD-poort.
LLTD Settings	U kunt de LLTD-functie in- of uitschakelen. Wanneer dit is ingeschakeld, wordt dit weergegeven in de Windows-netwerkmap.
LLMNR Settings	U kunt de LLMNR-functie in- of uitschakelen. Wanneer dit is ingeschakeld, kunt u de naamresolutie gebruiken zonder NetBIOS, zelfs als u DNS niet kunt gebruiken.
SNMPv1/v2c Settings	U kunt opgeven of u SNMPv1/v2c al dan niet wilt inschakelen. Dit wordt gebruikt voor het instellen van apparaten, bewaking enz.
SNMPv3 Settings	U kunt opgeven of u SNMPv3 al dan niet wilt inschakelen. Dit wordt gebruikt voor het instellen van versleutelde apparaten, bewaking enz.

Gerelateerde informatie

➡ “Protocollen beheren” op pagina 35

➡ “Protocolinstellingsitems” op pagina 37

Protocolinstellingsitems



Items	Instelwaarde en beschrijving
Bonjour Settings	

Basisinstellingen voor beveiliging

Items	Instelwaarde en beschrijving
Use Bonjour	Selecteer dit om apparaten te zoeken of gebruiken via Bonjour.
Bonjour Name	Toont de Bonjour-naam.
Bonjour Service Name	U kunt naam van de Bonjour-service weergeven en instellen.
Location	Toont de Bonjour-locatienaam.
SLP Settings	
Enable SLP	Selecteer dit om de SLP-functie in te schakelen. Dit wordt gebruikt voor netwerkdetectie in Epson Scan 2 en EpsonNet Config.
WSD Settings	
Enable WSD	Selecteer dit om het toevoegen van apparaten die WSD gebruiken toe te voegen en om af te drukken en te scannen vanaf de WSD-poort.
Scanning Timeout (sec)	Voer de time-outwaarde voor de communicatie voor WSD-scan in van 3 tot 3.600 seconden.
Device Name	Toont de WSD-apparaatnaam.
Location	Toont de WSD-locatienaam.
LLTD Settings	
Enable LLTD	Selecteer dit om LLTD in te schakelen. De scanner wordt weergegeven in de Windows-netwerkmap.
Device Name	Toont de LLTD-apparaatnaam.
LLMNR Settings	
Enable LLMNR	Selecteer dit om LLMNR in te schakelen. U kunt de naamresolutie gebruiken zonder NetBIOS, zelfs als u DNS niet kunt gebruiken.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	Selecteer dit om SNMPv1/v2c in te schakelen. Alleen scanners die SNMPv3 ondersteunen, worden weergegeven.
Access Authority	Stel de toegangsmachtiging in wanneer SNMPv1/v2c is ingeschakeld. Selecteer **Read Only** of **Read/Write**.
Community Name (Read Only)	Voer 0 tot 32 ASCII-tekens (0x20 tot 0x7E) in.
Community Name (Read/Write)	Voer 0 tot 32 ASCII-tekens (0x20 tot 0x7E) in.
SNMPv3 Settings	
Enable SNMPv3	SNMPv3 wordt ingeschakeld wanneer het selectievakje wordt ingeschakeld.
User Name	Voer tussen 1 en 32 tekens in. Gebruik 1-bits tekens.
Authentication Settings	

Basisinstellingen voor beveiliging

Items	Instelwaarde en beschrijving
Algorithm	Selecteer een algoritme voor een verificatie voor SNMPv3.
Password	Voer het wachtwoord in voor een verificatie voor SNMPv3. Voer tussen 8 en 32 tekens in ASCII (0x20–0x7E) in. Laat dit leeg als u dit niet wilt opgeven.
Confirm Password	Voer het geconfigureerde wachtwoord in ter bevestiging.
Encryption Settings	
Algorithm	Selecteer een algoritme voor een versleuteling voor SNMPv3.
Password	Voer het wachtwoord in voor een versleuteling voor SNMPv3. Voer tussen 8 en 32 tekens in ASCII (0x20–0x7E) in. Laat dit leeg als u dit niet wilt opgeven.
Confirm Password	Voer het geconfigureerde wachtwoord in ter bevestiging.
Context Name	Voer maximaal 32 tekens in Unicode (UTF-8) in. Laat dit leeg als u dit niet wilt opgeven. Het aantal tekens dat kan worden ingevoerd, varieert afhankelijk van de taal.

Gerelateerde informatie

➡ “Protocollen beheren” op pagina 35

➡ “Protocollen die u kunt inschakelen of uitschakelen” op pagina 36

Instellingen voor bediening en beheer

Dit hoofdstuk bevat informatie over de items die verband houden met het dagelijkse bedrijf en beheer van het apparaat.

Informatie van een apparaat bevestigen

Met Web Config kunt u de volgende informatie van het bedienende apparaat controleren via **Status**.

❏ Product Status

Controleer taal, status, productnummer, MAC-adres enz.

❏ Network Status

Controleer de informatie van de netwerkverbindingsstatus, het IP-adres, de DNS-server, enz.

❏ Panel Snapshot

Geef een afbeelding weer op het bedieningspaneel van het apparaat.

❏ Maintenance

Controleer de startdatum, scaninformatie, enz.

❏ Hardware Status

Controleer de status van de scanner.

Gerelateerde informatie

➡ "Web Config openen" op pagina 23

Apparaten beheren (Epson Device Admin)

Met Epson Device Admin kunt u veel apparaten beheren en bedienen. Met Epson Device Admin kunt u apparaten beheren in een ander netwerk. Hieronder worden de belangrijkste beheersfuncties uiteengezet.

Raadpleeg de documentatie of de Help van Epson Device Admin voor meer informatie over de functies en het gebruik van de software.

❏ Apparaten detecteren

U kunt apparaten detecteren in het netwerk en deze vervolgens vastleggen in een lijst. Als Epson-apparaten, zoals printers en scanners, zijn verbonden met hetzelfde netwerksegment als de computer van de beheerder, kun u ze zelfs vinden als er geen IP-adres aan de apparaten is toegewezen.

U kunt tevens apparaten detecteren die via een USB-kabel zijn verbonden met computers in het netwerk. U moet de Epson Device USB Agent op de computer installeren.

❏ Apparaten instellen

U kunt een sjabloon maken met de ingestelde items, zoals de netwerkinterface en de papierbron, en dit als gedeelde instellingen toepassen op andere apparaten. Wanneer het apparaat is verbonden met het netwerk, kunt u een IP-adres toewijzen aan een apparaat waaraan nog geen IP-adres is toegewezen.

❏ Apparaten bewaken

U kunt regelmatig de status en gedetailleerde informatie over apparaten in het netwerk ophalen. U kunt ook apparaten bewaken die via een USB-kabel zijn verbonden met computers in het netwerk, en apparaten van andere bedrijven die in de apparatenlijst zijn vastgelegd. Als u apparaten wilt bewaken die zijn verbonden via een USB-kabel, moet u de Epson Device USB Agent installeren.

❏ Waarschuwingen beheren

U kunt waarschuwingen over de status van apparaten en verbruiksartikelen bewaken. Het systeem verzendt automatisch meldingen per e-mail naar de beheerder op basis van ingestelde voorwaarden.

❏ Rapporten beheren

U kunt op vastgestelde momenten rapporten maken op basis van de gegevens over apparaatgebruik en verbruiksartikelen die door het systeem worden verzameld. U kunt deze rapporten opslaan en per e-mail verzenden.

Gerelateerde informatie

➡ "Epson Device Admin" op pagina 55

E-mailmeldingen ontvangen bij gebeurtenissen

Over e-mailmeldingen

U kunt deze functie gebruiken om bij bepaalde gebeurtenissen een waarschuwing per e-mail te ontvangen. U kunt tot 5 e-mailadressen registreren en kiezen voor welke gebeurtenissen u een melding wilt ontvangen.

Om deze functie te gebruiken, moet de e-mailserver zijn geconfigureerd.

Gerelateerde informatie

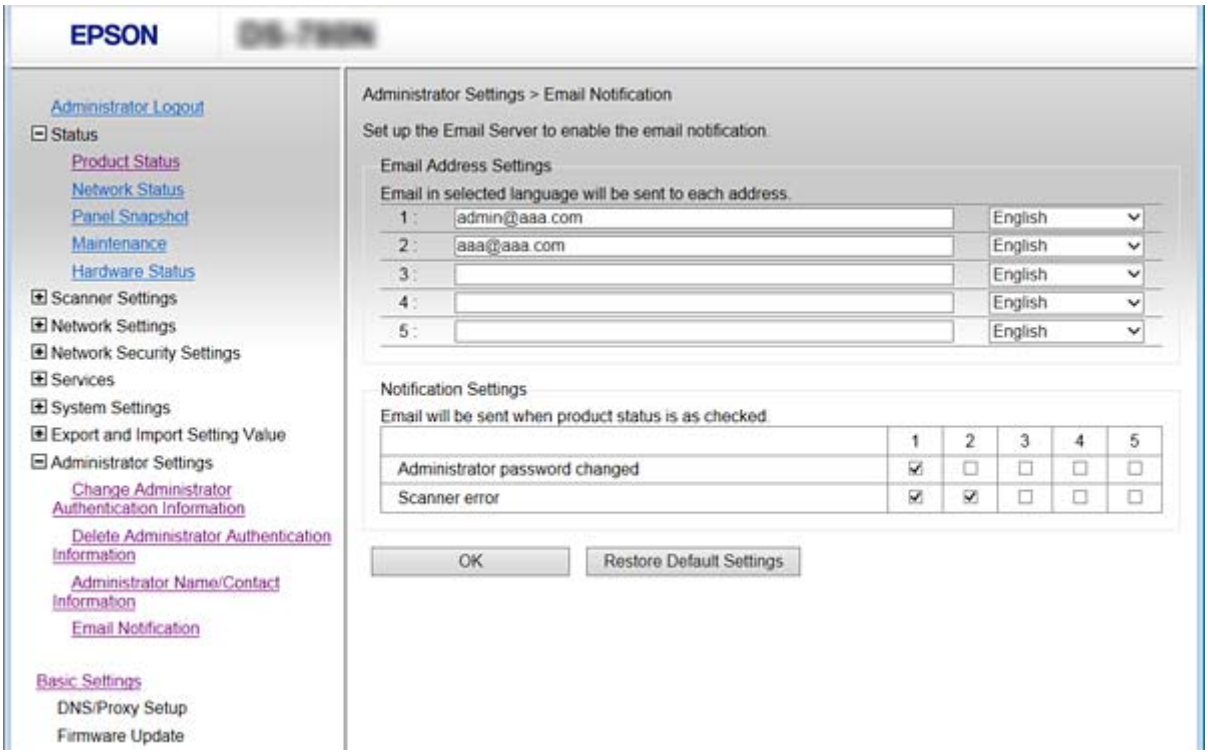
➡ "Een e-mailserver configureren" op pagina 42

E-mailmeldingen configureren

Als u de functie wilt gebruiken, moet u een e-mailserver configureren.

1. Open Web Config en selecteer **Administrator Settings** > **Email Notification**.
2. Voer een e-mailadres in dat u wilt gebruiken om e-mailmeldingen te ontvangen.
3. Selecteer de taal voor de e-mailmeldingen.

4. Schakel de selectievakjes in voor de meldingen die u wilt ontvangen.



5. Klik op **OK**.

Gerelateerde informatie

➡ "Web Config openen" op pagina 23
➡ "Een e-mailserver configureren" op pagina 42

Een e-mailserver configureren

Controleer het volgende voordat u de configuratie uitvoert.

❏ De scanner is verbonden met een netwerk.

❏ Informatie van de e-mailserver van de computer.

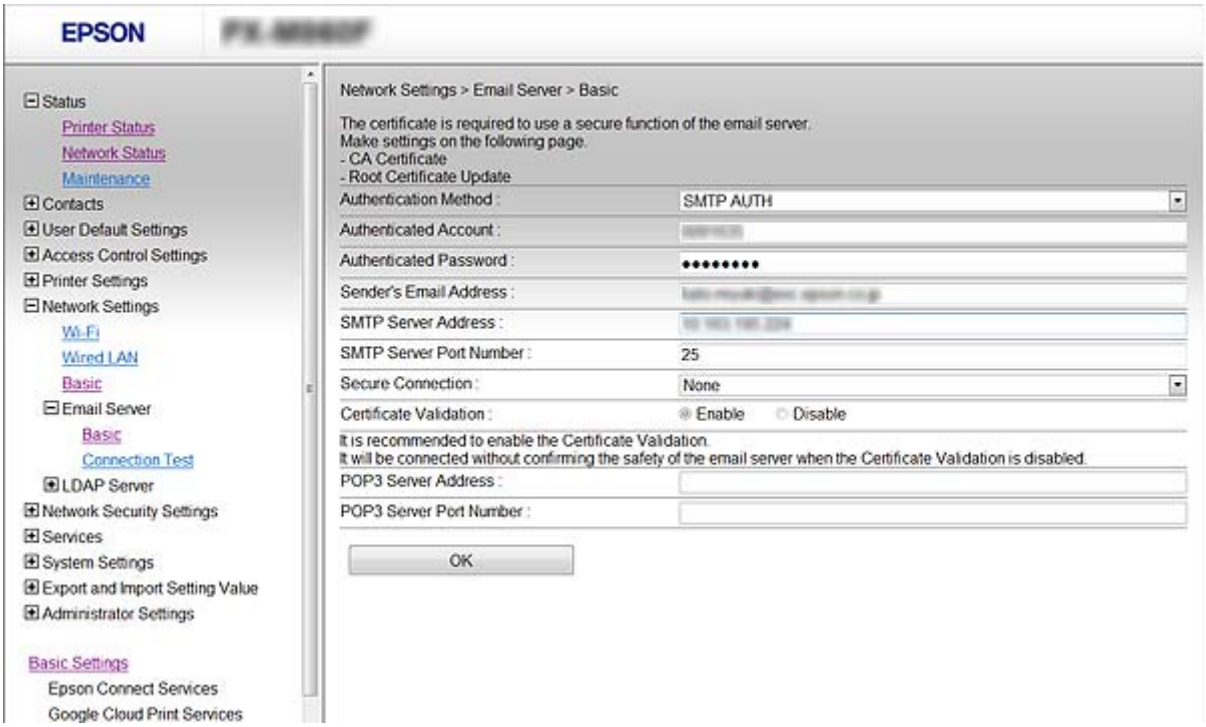
1. Open Web Config en selecteer **Network Settings** > **Email Server** > **Basic**.
2. Voer voor elk item een waarde in.
3. Selecteer **OK**.

   De geselecteerde instellingen worden weergegeven.

Gerelateerde informatie

➡ "Web Config openen" op pagina 23
➡ "Instellingen voor de e-mailserver" op pagina 43

Instellingen voor de e-mailserver



Items	Instellingen en uitleg	
Authentication Method	Geef hier de verificatiemethode op die de scanner moet gebruiken voor toegang tot de e-mailserver.	
	Off	Verificatie is uitgeschakeld wanneer met de e-mailserver wordt gecommuniceerd.
	SMTP AUTH	Hiervoor is vereist dat een e-mailserver SMTP-verificatie ondersteunt.
	POP before SMTP	Wanneer u deze methode selecteert, moet u de POP3-server configureren.
Authenticated Account	Als u **SMTP AUTH** of **POP before SMTP** selecteert als de **Authentication Method**, voert u de geverifieerde accountnaam in met 0 tot 255 tekens in ASCII (0x20 tot 0x7E).	
Authenticated Password	Als u **SMTP AUTH** of **POP before SMTP** selecteert als **Authentication Method**, voert u het geverifieerde wachtwoord in dat tussen 0 en 20 tekens lang is en bestaat uit A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.	
Sender's Email Address	Voer hier het e-mailadres van de afzender in. U kunt tussen 0 en 255 tekens invoeren in ASCII (0x20–0x7E), behalve : ( ) < > [ ] ; ¥. Het eerste teken mag geen punt (".") zijn.	
SMTP Server Address	Voer hier tussen 0 en 255 tekens in. Gebruik A–Z a–z 0–9. - . U kunt IPv4 of FQDN gebruiken.	
SMTP Server Port Number	Voer een getal tussen 1 en 65535 in.	

Items	Instellingen en uitleg	
Secure Connection	Geef de beveiligde verbindingsmethode op voor de e-mailserver.	
	None	Als u **POP before SMTP** selecteert in **Authentication Method**, wordt de verbindingsmethode ingesteld op **None**.
	SSL/TLS	Dit is beschikbaar wanneer **Authentication Method** is ingesteld op **Off** of **SMTP AUTH**.
	STARTTLS	Dit is beschikbaar wanneer **Authentication Method** is ingesteld op **Off** of **SMTP AUTH**.
Certificate Validation	Het certificaat is gevalideerd wanneer dit is ingeschakeld. Wij raden aan dit in te stellen op **Enable**.	
POP3 Server Address	Als u **POP before SMTP** selecteert als **Authentication Method**, voert u het POP3-serveradres in dat tussen 0 en 255 tekens lang is en bestaat uit A–Z a–z 0–9 . - . U kunt IPv4 of FQDN gebruiken.	
POP3 Server Port Number	Als u **POP before SMTP** selecteert als **Authentication Method**, voert u een cijfer in tussen 1 en 65535.	

Gerelateerde informatie

➡ “Een e-mailserver configureren” op pagina 42

De verbinding met de e-mailserver controleren

1. Open Web Config en selecteer **Network Settings** > **Email Server** > **Connection Test**.
2. Selecteer **Start**.

   De verbindingstest met de mailserver is gestart. Na de test wordt een testverslag weergegeven.

Gerelateerde informatie

➡ “Web Config openen” op pagina 23
➡ “Referenties verbindingstest e-mailserver” op pagina 44

Referenties verbindingstest e-mailserver

Berichten	Uitleg
Connection test was successful.	Dit bericht wordt weergegeven wanneer de verbinding met de server is geslaagd.
SMTP server communication error. Check the following. - Network Settings	Dit bericht verschijnt in de volgende gevallen ❏ De scanner is niet verbonden met een netwerk ❏ De SMTP-server is uitgeschakeld ❏ De netwerkverbindingen zijn verbroken tijdens de communicatie ❏ Er zijn onvolledige gegevens ontvangen

Instellingen voor bediening en beheer

Berichten	Uitleg
POP3 server communication error. Check the following. - Network Settings	Dit bericht verschijnt in de volgende gevallen ❏ De scanner is niet verbonden met een netwerk ❏ De POP3-server is uitgeschakeld ❏ De netwerkverbindingen zijn verbroken tijdens de communicatie ❏ Er zijn onvolledige gegevens ontvangen
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Dit bericht verschijnt in de volgende gevallen ❏ Verbinden met een DNS-server is mislukt ❏ Naamresolutie voor een SMTP-server is mislukt
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Dit bericht verschijnt in de volgende gevallen ❏ Verbinden met een DNS-server is mislukt ❏ Naamresolutie voor een POP3-server is mislukt
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Dit bericht verschijnt wanneer de SMTP-serververificatie is mislukt.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Dit bericht verschijnt wanneer de POP3-serververificatie is mislukt.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Dit bericht verschijnt wanneer u probeert te communiceren met niet-ondersteunde protocollen.
Connection to SMTP server failed. Change Secure Connection to None.	Dit bericht verschijnt wanneer een SMTP niet overeenkomt tussen een server en een client of wanneer de server geen beveiligde SMTP-verbinding ondersteunt (SSL-verbinding).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Dit bericht verschijnt wanneer een SMTP niet overeenkomt tussen een server en een client of wanneer de server het gebruik van een SSL/TLS-verbinding vraagt voor een beveiligde SMTP-verbinding.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Dit bericht verschijnt wanneer een SMTP niet overeenkomt tussen een server en een client of wanneer de server het gebruik van een STARTTLS-verbinding vraagt voor een beveiligde SMTP-verbinding.
The connection is untrusted. Check the following. - Date and Time	Dit bericht verschijnt wanneer de datum- en tijdinstelling van de scanner onjuist is of als het certificaat verlopen is.
The connection is untrusted. Check the following. - CA Certificate	Dit bericht verschijnt wanneer de scanner geen basiscertificaat heeft dat overeenkomt met de server of als een CA Certificate niet is geïmporteerd.
The connection is not secured.	Dit bericht wordt weergegeven wanneer het verkregen certificaat beschadigd is.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Dit bericht verschijnt wanneer een verificatiemethode niet overeenkomt tussen een server en een client. De server ondersteunt SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Dit bericht verschijnt wanneer een verificatiemethode niet overeenkomt tussen een server en een client. De server biedt geen ondersteuning voor SMTP AUTH.

Berichten	Uitleg
Sender's Email Address is incorrect. Change to the email address for your email service.	Dit bericht verschijnt wanneer het opgegeven e-mailadres van de afzender onjuist is.
Cannot access the product until processing is complete.	Dit bericht wordt weergegeven wanneer de scanner bezet is.

Gerelateerde informatie

➡ "De verbinding met de e-mailserver controleren" op pagina 44

Firmware bijwerken

Firmware bijwerken met Web Config

Firmware wordt bijgewerkt met Web Config. Het apparaat moet verbinding hebben met internet.

1. Open Web Config en selecteer **Basic Settings** > **Firmware Update**.
2. Klik op **Start**.

   De firmwarebevestiging begint en de firmware-informatie wordt weergegeven als er nieuwere firmware beschikbaar is.
3. Klik op **Start** en volg de instructies op het scherm.

Opmerking:
U kunt de firmware ook bijwerken met Epson Device Admin. U kunt de firmware-informatie visueel controleren in de apparaatlijst. Dit is handig wanneer u de firmware van meerdere apparaten wilt bijwerken. Raadpleeg de handleiding of de help van Epson Device Admin voor meer informatie.

Gerelateerde informatie

➡ "Web Config openen" op pagina 23
➡ "Epson Device Admin" op pagina 55

Firmware bijwerken met Epson Firmware Updater

U kunt de firmware van het apparaat downloaden naar de computer vanaf de website van Epson, en vervolgens het apparaat via een USB-kabel aansluiten op de computer om de firmware bij te werken. Gebruik deze methode als u niet kunt bijwerken via het netwerk.

1. Ga naar de website van Epson en download de firmware.
2. Sluit het apparaat met een USB-kabel aan op de computer waarop de gedownloade firmware is opgeslagen.
3. Dubbelklik op het gedownloade EXE-bestand.

   Epson Firmware Updater wordt gestart.

4. Volg de instructies op het scherm.

Een back-up maken van de instellingen

Als u de instellingsitems in Web Config exporteert, kunt u de items kopiëren naar de andere scanners.

De instellingen exporteren

Exporteer elke instelling voor de scanner.

1. Open Web Config en selecteer vervolgens **Export and Import Setting Value** > **Export**.
2. Selecteer de instellingen die u wilt exporteren.

   Selecteer de instellingen die u wilt exporteren. Als u de bovenliggende categorie selecteert, worden ook subcategorieën geselecteerd. Subcategorieën die echter fouten veroorzaken door het dupliceren binnen hetzelfde netwerk (zoals IP-adressen enz.), kunnen niet worden geselecteerd.
3. Voer een wachtwoord in om het geëxporteerde bestand te coderen.

   U hebt het wachtwoord nodig voor het importeren van het bestand. Laat dit leeg als u het bestand niet wilt coderen.
4. Klik op **Export**.

> ***Belangrijk:***
>
> *Als u de netwerkinstellingen van de scanner, zoals de scannernaam en het IP-adres exporteert, selecteert u **Enable to select the individual settings of device** en kiest u meer items. Gebruik alleen de geselecteerde waarden voor de vervangingsscanner.*

Gerelateerde informatie

➡ "Web Config openen" op pagina 23

De instellingen importeren

Importeer het geëxporteerde Web Config-bestand naar de scanner.

> ***Belangrijk:***
>
> *Wanneer waarden die individuele informatie, zoals een scannernaam of IP-adres, bevatten worden geïmporteerd, moet u controleren of hetzelfde IP-adres niet op hetzelfde netwerk staat. Als het IP-adres overlapt, weerspiegelt de scanner de waarde niet.*

1. Open Web Config en selecteer vervolgens **Export and Import Setting Value** > **Import**.
2. Selecteer het geëxporteerde bestand en voer dan het gecodeerde wachtwoord in.
3. Klik op **Next**.

4. Selecteer de instellingen die u wilt importeren en klik vervolgens op **Next**.
5. Klik op **OK**.

De instellingen worden toegepast op de scanner.

Gerelateerde informatie

➡ "Web Config openen" op pagina 23

Problemen oplossen

Tips voor het oplossen van problemen

U kunt meer informatie vinden in de volgende handleiding.

❏ Gebruikershandleiding

Aanwijzingen voor het gebruik van de scanner, onderhoud en het oplossen van problemen.

Logboek voor server en netwerkapparaat controleren

Bij netwerkproblemen is het in sommige gevallen mogelijk de oorzaak te achterhalen door het logboekbestand van de mailserver, LDAP-server, enz. te bevestigen, de status te controleren aan de hand van het netwerklogboek van systeemapparaten en opdrachten, zoals routers.

De netwerkinstellingen initialiseren

De netwerkinstellingen herstellen op het bedieningspaneel

U kunt alle netwerkinstellingen terugzetten op de standaardinstellingen.

1. Tik op het startscherm op **Instel.**.
2. Tik op **Systeembeheer** > **Standaardinst. herstellen** > **Netwerkinstellingen**.
3. Controleer het bericht en tik vervolgens op **Ja**.
4. Wanneer een voltooiingsbericht wordt weergegeven, tikt u op **Sluiten**.

   Het scherm sluit automatisch na een vastgestelde tijd als u niet op **Sluiten** tikt.

De communicatie tussen apparaten en computers controleren

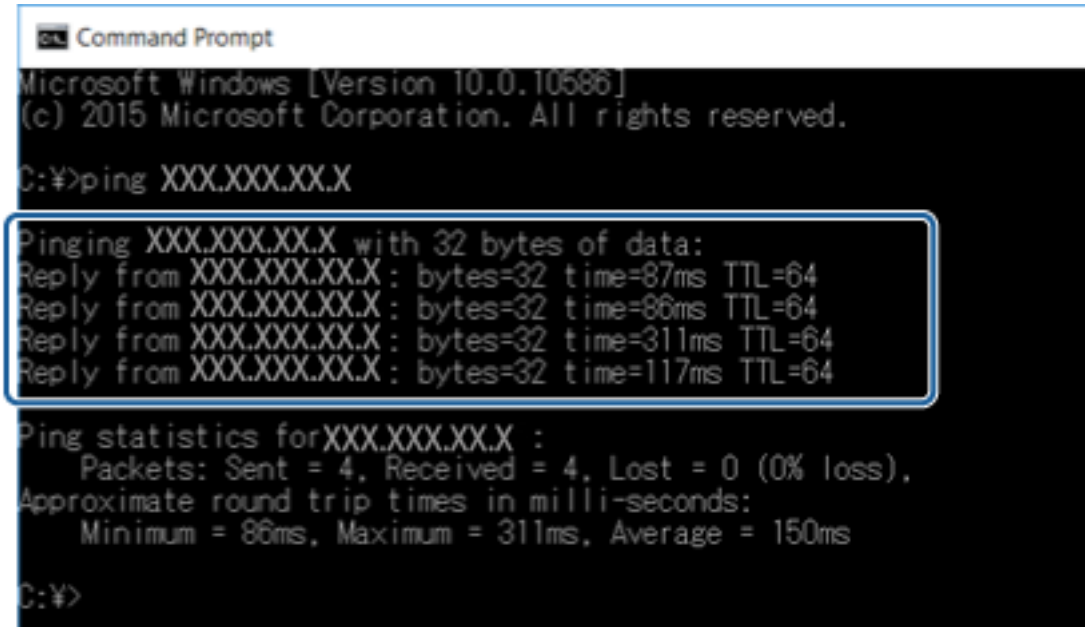
De verbinding controleren met de opdracht Ping — Windows

Met een Ping-opdracht kunt u controleren of de computer is verbonden met de scanner. Volg de onderstaande stappen om de verbinding te controleren met een Ping-opdracht.

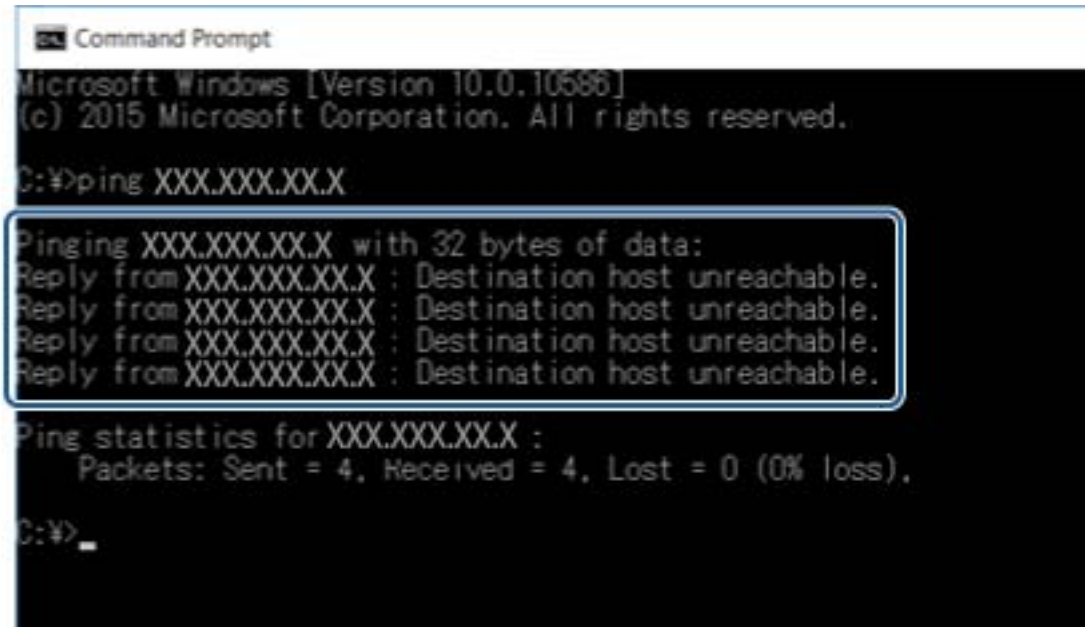
1. Controleer het IP-adres dat de scanner gebruikt voor de verbinding die u wilt controleren.

   U kunt dit controleren met Epson Scan 2.

2. Geef op de computer het scherm met de opdrachtprompt weer.
   - ❏ Windows 10
     Klik met de rechtermuisknop op de knop Start of houd deze ingedrukt en selecteer **Opdrachtprompt**.
   - ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
     Geef het scherm met toepassingen weer en selecteer **Opdrachtprompt**.
   - ❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 of lager
     Klik op de knop Start, selecteer **Alle programma's** of **Programma's** > **Bureau-accessoires** > **Opdrachtprompt**.
3. Typ "ping xxx.xxx.xxx.xxx" en druk vervolgens op de toets Enter.
   Voer in plaats van xxx.xxx.xxx.xxx het IP-adres van de scanner in.
4. Controleer de communicatiestatus.
   Als de scanner en computer met elkaar communiceren, wordt het volgende bericht weergegeven.



Als de scanner en computer niet met elkaar communiceren, wordt het volgende bericht weergegeven.



De verbinding controleren met de opdracht Ping — Mac OS

Met een Ping-opdracht kunt u controleren of de computer is verbonden met de scanner. Volg de onderstaande stappen om de verbinding te controleren met een Ping-opdracht.

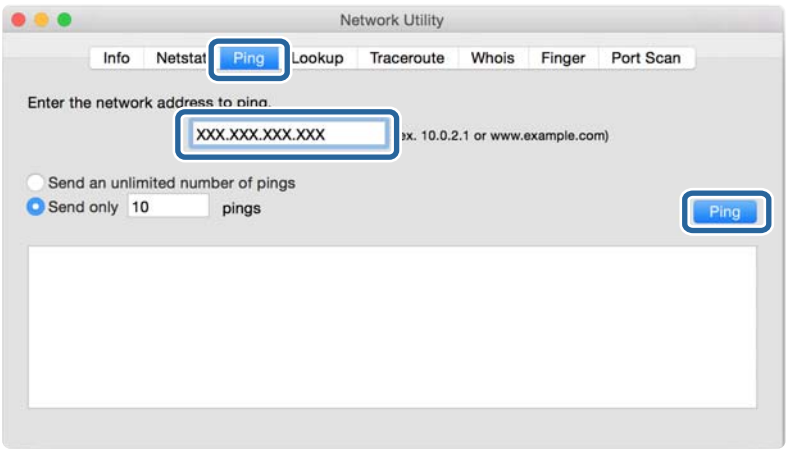
1. Controleer het IP-adres dat de scanner gebruikt voor de verbinding die u wilt controleren.

   U kunt dit controleren met Epson Scan 2.

2. Start Network Utility.

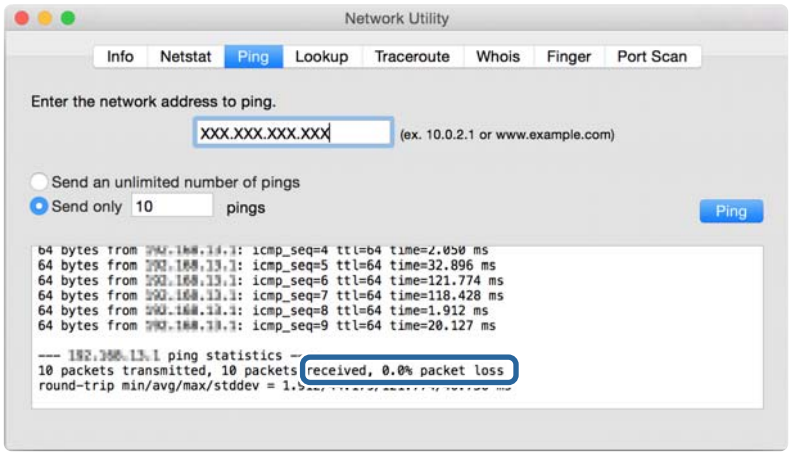
   Ga naar Network Utility in **Spotlight**.

3. Klik op het tabblad **Ping**, voer het IP-adres in dat u in stap 1 hebt gevonden en klik vervolgens op **Ping**.

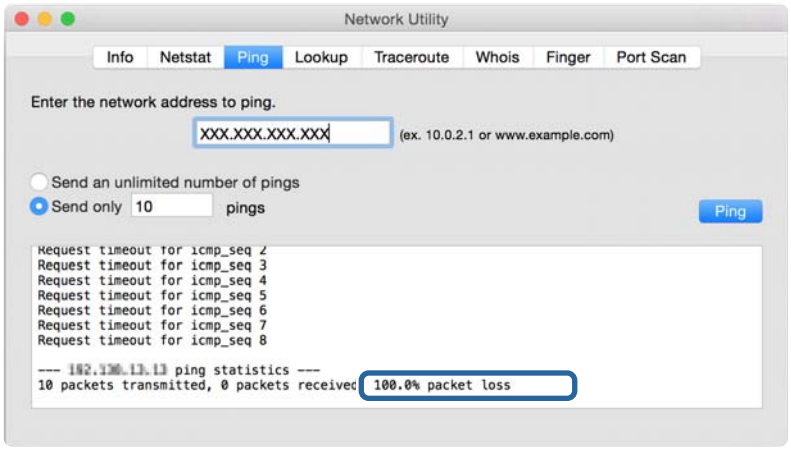


4. Controleer de communicatiestatus.

   Als de scanner en computer met elkaar communiceren, wordt het volgende bericht weergegeven.



   Als de scanner en computer niet met elkaar communiceren, wordt het volgende bericht weergegeven.



Problemen met het gebruik van netwerksoftware

Geen toegang tot Web Config

Is het IP-adres van de scanner correct geconfigureerd?

Configureer het IP-adres met Epson Device Admin of EpsonNet Config.

Ondersteunt uw browser bulkversleuteling voor de Encryption Strength voor SSL/TLS?

De bulkversleutelingen voor de Encryption Strength voor SSL/TLS zijn als volgt. U hebt alleen toegang tot Web Config in een browser die de volgende bulkversleutelingen ondersteunt. Controleer welke vorm van versleuteling uw browser ondersteunt.

❏ 80-bits: AES256/AES128/3DES

❏ 112-bits: AES256/AES128/3DES

❏ 128-bits: AES256/AES128

❏ 192-bits: AES256

❏ 256-bits: AES256

Bij het openen van Web Config met SSL-communicatie (https) wordt het bericht "Vervaldatum voorbij" weergegeven.

Als het certificaat vervallen is, moet u een nieuw certificaat aanvragen. Als het bericht wordt weergegeven vóór de vervaldatum, controleer dan of de scannerdatum goed is geconfigureerd.

Bij het openen van Web Config met SSL-communicatie (https) wordt het bericht "Naam van het beveiligingscertificaat stemt niet overeen" weergegeven.

Het IP-adres van de scanner dat bij **Common Name** is ingevoerd voor het maken van een zelfondertekend certificaat of CSR, is niet gelijk aan het adres dat in de browser is ingevoerd. Vraag een nieuw certificaat aan en importeer dit, of wijzig de scannernaam.

De scanner wordt benaderd via een proxyserver.

Als u voor uw scanner een proxyserver gebruikt, moet u de proxyinstellingen van de browser configureren.

❏ Windows:

Selecteer **Configuratiescherm** > **Netwerk en internet** > **Internetopties** > **Verbindingen** > **LAN-instellingen** > **Proxyserver** en geef vervolgens aan dat u de proxyserver niet wilt gebruiken voor lokale adressen.

❏ Mac OS:

Selecteer **Systeemvoorkeuren** > **Netwerk** > **Geavanceerd** > **Proxy's** en registreer vervolgens het lokale adres bij **Negeer proxy-instellingen voor deze hosts en domeinen**.

Voorbeeld:

192.168.1.*: Lokaal adres 192.168.1.XXX, subnetmasker 255.255.255.0

192.168.*.*: Lokaal adres 192.168.XXX.XXX, subnetmasker 255.255.0.0

Gerelateerde informatie

➡ “Web Config openen” op pagina 23

➡ “Het IP-adres toewijzen” op pagina 15

➡ “Een IP-adres toewijzen met EpsonNet Config” op pagina 56

Modelnaam en/of IP-adres niet weergegeven in EpsonNet Config

Hebt u Block, Cancel of Shut down geselecteerd toen een Windows-beveiligingsscherm of een firewallscherm werd weergegeven?

Als u **Blokkeren**, **Annuleren** of **Afsluiten** hebt geselecteerd, worden het IP-adres en de modelnaam niet weergegeven in EpsonNet Config of EpsonNet Setup.

U kunt dit verhelpen door EpsonNet Config als uitzondering op te geven in Windows Firewall en andere in de handel verkrijgbare beveiligingssoftware. Als u een antivirus- of beveiligingsprogramma gebruikt, sluit dit programma dan en probeer vervolgens EpsonNet Config te gebruiken.

Is de tijd voor een time-out bij communicatiefouten te kort?

Start EpsonNet Config en selecteer **Tools** > **Options** > **Timeout**. Verhoog vervolgens de tijdsduur voor **Communication Error**. Als gevolg hiervan kan EpsonNet Config langzamer werken.

Problemen oplossen

Gerelateerde informatie

➡ “EpsonNet Config starten — Windows” op pagina 56
➡ “EpsonNet Config starten — Mac OS” op pagina 56

Bijlage

Inleiding tot de netwerksoftware

Hieronder vindt u informatie over de software waarmee u apparaten configureert en beheert.

Epson Device Admin

Epson Device Admin is een toepassing waarmee u apparaten op het netwerk kunt installeren en deze apparaten vervolgens kunt configureren en beheren. U kunt gedetailleerde informatie verkrijgen over apparaten, zoals de status en verbruiksartikelen, meldingen of waarschuwingen verzenden, en rapporten over apparaatgebruik maken. U kunt ook een sjabloon maken met de ingestelde items en dit als gedeelde instellingen toepassen op andere apparaten. U kunt Epson Device Admin downloaden van de ondersteuningssite van Epson. Zie voor meer informatie de documentatie of Help van Epson Device Admin.

Epson Device Admin uitvoeren (alleen Windows)

Selecteer **Alle programma's** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

Opmerking:
Als de firewall een waarschuwing weergeeft, moet u Epson Device Admin toegang geven.

EpsonNet Config

Met EpsonNet Config kan de systeembeheerder de netwerkinstellingen van de scanner configureren. Zo is het bijvoorbeeld mogelijk om een IP-adres toe te wijzen en de verbindingsmodus te wijzigen. Onder Windows is het mogelijk om dit batchgewijs te doen. Zie voor meer informatie de documentatie of Help van EpsonNet Config.

EpsonNet Config starten — Windows

Selecteer **Alle programma's** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

Opmerking:
Als de firewall een waarschuwing weergeeft, moet u EpsonNet Config toegang geven.

EpsonNet Config starten — Mac OS

Selecteer **Start** > **Toepassingen** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

EpsonNet SetupManager

EpsonNet SetupManager is software waarmee een pakket kan worden gemaakt voor een eenvoudige scannerinstallatie, bijvoorbeeld met installatie en configuratie van de scannerdriver en installatie van Document Capture Pro. Met deze software maakt de systeembeheerder softwarepakketten op maat voor distributie naar de desbetreffende groepen.

Ga naar uw regionale Epson-website voor meer informatie.

Een IP-adres toewijzen met EpsonNet Config

Met EpsonNet Config kunt u een IP-adres toewijzen aan de scanner. Met EpsonNet Config kunt u een IP-adres toewijzen aan een scanner waaraan nog geen IP-adres is toegewezen nadat deze met een Ethernet-kabel is verbonden.

Een IP-adres toewijzen met batch-instellingen

Het bestand voor batch-instellingen maken

Met het MAC-adres en de modelnaam als sleutel kunt u een nieuw SYLK-bestand maken om het IP-adres in te stellen.

1. Open een spreadsheet-toepassing (bijv. Microsoft Excel) of een tekstverwerkingsprogramma.

2. Voer in de eerste rij "Info_MACAddress", "Info_ModelName" en "TCPIP_IPAddress" in als de namen voor de instellingsitems.

   Voer de instellingsitems in voor de volgende vier teksttekenreeksen. Als u onderscheid wilt maken tussen hoofdletters/kleine letters en dubbelbyte-/enkelbyte-tekens, wordt het item niet herkend als er slechts één teken anders is.

   Voer de naam van het instellingsitem in, zoals hieronder beschreven. EpsonNet Config kan de instellingsitems anders niet herkennen.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. Voer het MAC-adres, de modelnaam en het IP-adres voor elke netwerkinterface in.

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. Geef een naam op en sla op als SYLK-bestand (*.slk).

Batch-instellingen maken met het configuratiebestand

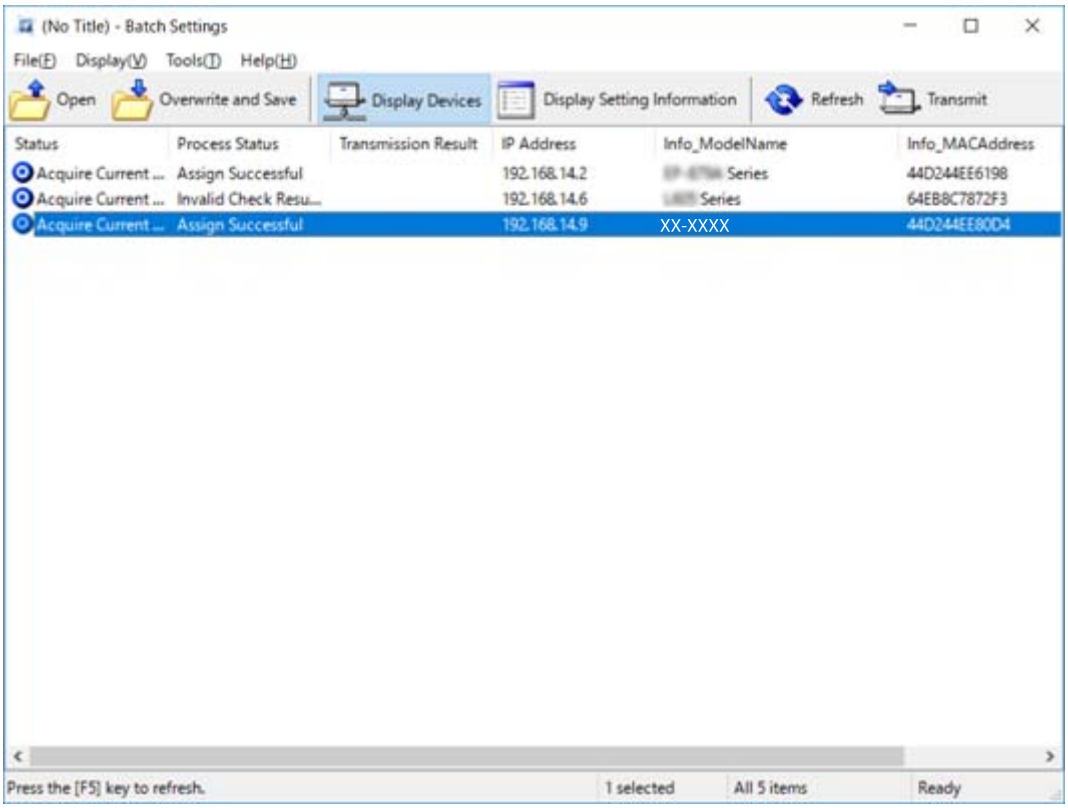
Wijs IP-adressen in één keer toe in het configuratiebestand (SYLK-bestand). U moet het configuratiebestand maken voordat u adressen kunt toewijzen.

1. Verbind alle apparaten met het netwerk met Ethernet-kabels.
2. Schakel de scanner in.
3. Start EpsonNet Config.

   Er wordt een lijst met de scanners in het netwerk weergegeven. Het kan even duren voordat deze worden weergegeven.
4. Klik op **Tools** > **Batch Settings**.
5. Klik op **Open**.
6. Selecteer in het bestandsselectiescherm, het SYLK-bestand (*.slk) dat de instellingen bevat en klik vervolgens op **Open**.

7. Selecteer de apparaten waarvoor u de batch-instellingen wilt uitvoeren terwijl de kolom **Status** is ingesteld op **Unassigned** en de **Process Status** is ingesteld op **Assign Successful**.

   Wanneer u meerdere selecties maakt, houdt u Ctrl of Shift ingedrukt en klikt u of sleept u met de muis.



8. Klik op **Transmit**.

9. Wanneer het scherm voor wachtwoordinvoer wordt weergegeven, voert u het wachtwoord in en klikt u vervolgens op **OK**.

   Draag de instellingen over.

   Opmerking:
   De gegevens zijn overgedragen naar de netwerkinterface wanneer de voortgangsbalk is voltooid. Schakel het apparaat of de draadloze adapter niet uit en verzend geen gegevens naar het apparaat.

10. Klik op het scherm **Transmitting Settings** op **OK**.

11. Controleer de status van het apparaat dat u hebt ingesteld.

    Voor apparaten waarvoor  of  wordt weergegeven, controleert u de inhoud van het instellingenbestand, en of het apparaat normaal opnieuw is opgestart.

Pictogram	Status	Process Status	Uitleg
	Setup Complete	Setup Successful	De instelling is normaal voltooid.
	Setup Complete	Rebooting	Wanneer gegevens is overgedragen, moet elk apparaat opnieuw worden opgestart om de instellingen te activeren. Er wordt een controle uitgevoerd om te bepalen er na het opnieuw opstarten verbinding kan worden gemaakt met het apparaat.
	Setup Complete	Reboot Failed	Kan het apparaat niet controleren na het overdragen van de instellingen. Controleer of het apparaat is ingeschakeld en of het normaal opnieuw is opgestart.
	Setup Complete	Searching	Zoeken naar het apparaat dat in het instellingenbestand is aangegeven.*
	Setup Complete	Search Failed	Kan geen apparaten controleren die al zijn ingesteld. Controleer of het apparaat is ingeschakeld en of het normaal opnieuw is opgestart.*

    * Alleen wanneer instellingsinformatie wordt weergegeven.

Gerelateerde informatie

➡ "EpsonNet Config starten — Windows" op pagina 56

➡ "EpsonNet Config starten — Mac OS" op pagina 56

Aan elk apparaat een IP-adres toewijzen

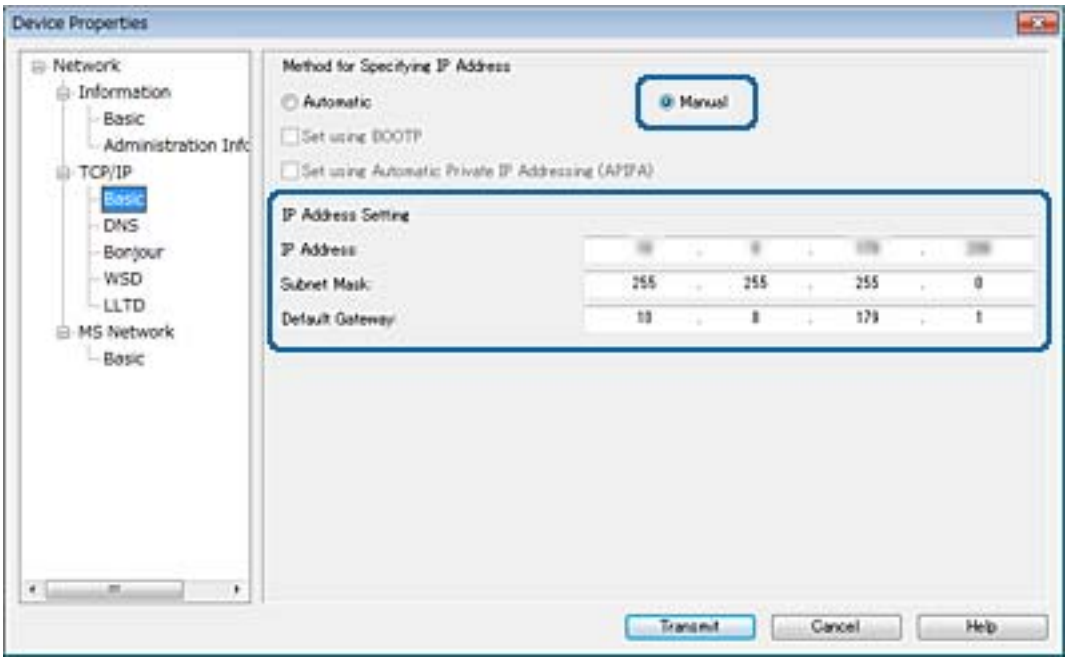
Wijs een IP-adres toe aan de scanner met EpsonNet Config.

1. Schakel de scanner in.
2. Verbind de scanner met het netwerk met een Ethernet-kabel.
3. Start EpsonNet Config.

   Er wordt een lijst met de scanners in het netwerk weergegeven. Het kan even duren voordat deze worden weergegeven.
4. Dubbelklik op de scanner waaraan u wilt toewijzen.

   Opmerking:
   Als u meerdere scanners van hetzelfde model hebt verbonden, kunt u de scanner identificeren aan de hand van het MAC-adres.
5. Selecteer **Network** > **TCP/IP** > **Basic**.

6. Voer de adressen in voor **IP Address**, **Subnet Mask** en **Default Gateway**.



Opmerking:
Voer een statisch adres in wanneer de scanner verbindt met een beveiligd netwerk.

7. Klik op **Transmit**.

   Het scherm waarop overdracht wordt bevestigd, wordt weergegeven.

8. Klik op **OK**.

   Het scherm met waarop wordt aangegeven dat de overdracht is voltooid, wordt weergegeven.

   Opmerking:
   De informatie wordt overgedragen naar het apparaat en het bericht "De configuratietaken zijn voltooid" wordt weergegeven. Schakel het apparaat niet uit en verzend geen gegevens naar de service.

9. Klik op **OK**.

Gerelateerde informatie

➡ "EpsonNet Config starten — Windows" op pagina 56
➡ "EpsonNet Config starten — Mac OS" op pagina 56

Poort voor de scanner gebruiken

De scanner gebruikt de volgende poort. Deze poorten moeten door de netwerkbeheerder indien nodig beschikbaar worden gesteld.

Bijlage

Verzender (client)	Gebruiken	Doel (server)	Protocol	Poortnummer
Scanner	Verzenden via e-mail (e-mailmelding)	SMTP-server	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	POP voor SMTP-verbinding (e-mailmelding)	POP-server	POP3 (TCP)	110
	Controle-WSD	Clientcomputer	WSD (TCP)	5357
	De computer zoeken wanneer push-scan vanuit Document Capture Pro wordt uitgevoerd	Clientcomputer	Netwerkdetectie tijdens push-scan	2968
	De taakinformatie verzamelen wanneer push-scan vanuit Document Capture Pro wordt uitgevoerd	Clientcomputer	Netwerkpush-scan	2968
Clientcomputer	Detecteer de scanner vanuit een toepassing als EpsonNet Config en scannerstuurprogramma.	Scanner	ENPC (UDP)	3289
	Verzamel de MIB-informatie en stel deze in vanuit een toepassing als EpsonNet Config en scannerstuurprogramma.	Scanner	SNMP (UDP)	161
	WSD-scanner zoeken	Scanner	WS-Discovery (UDP)	3702
	De scangegevens doorsturen vanuit Document Capture Pro	Scanner	Netwerkscan (TCP)	1865

Geavanceerde beveiligingsinstellingen voor bedrijven

In dit hoofdstuk worden geavanceerde beveiligingsfuncties beschreven.

Beveiligingsinstellingen en voorkomen van gevaar

Wanneer een apparaat verbonden is met een netwerk, hebt u hier toegang toe vanaf een externe locatie. Bovendien kunnen veel personen het apparaat delen, wat nuttig is voor het verbeteren van de operationele efficiëntie en het gebruiksgemak. Risico's zoals illegale toegang, illegaal gebruik en knoeien met gegevens nemen hierdoor echter toe. Als u het apparaat gebruikt in een omgeving waarin u toegang hebt tot internet, zijn nemen de risico's nog verder toe.

Om dit risico's te vermijden, zijn Epson-apparaten uitgerust met een verscheidenheid aan beveiligingstechnologieën.

Stel het apparaat in op basis van de omgevingsvoorwaarden die zijn opgesteld met de omgevingsinformatie van de klant.

Naam	Type functie	Wat kunt u instellen	Wat voorkomt u
SSL/TLS-communicatie	Het communicatiepad van een computer en apparaat wordt versleuteld met SSL/TLS-communicatie. De inhoud van de communicatie via een browser wordt beveiligd.	Stel voor de server een CA-certificaat in dat is ondertekend door een CA (certificeringsinstantie) voor het apparaat.	Voorkom lekkage van instellingsinformatie en de inhoud van overgedragen gegevens naar de scanner vanaf de computer. Toegang vanaf het apparaat naar de Epson-server op internet kan tevens worden beveiligd met een firmware-update enz.
IPsec/IP-filtering	U kunt instellen of u het scheiden en afbreken van gegevens van een bepaalde client of van een bepaald type wilt toestaan. Omdat IPsec de gegevens per IP-pakketeenheid beschermt (versleuteling en verificatie), kunt u veilig onbeveiligde scanprotocollen communiceren.	Maak een basisbeleid en een individueel beleid om de client die of het type gegevens dat in te stellen dat toegang kan krijgen tot het apparaat.	Voorkom ongeoorloofde toegang, het ongewenst wijzigen van gegevens en het onderscheppen van communicatiegegevens naar het apparaat.
SNMPv3	Er zijn nieuwe functies toegevoegd, zoals bewaken van verbonden apparaten in het netwerk, de integriteit van de gegevens naar het te beheren SNMP-protocol, versleuteling, gebruikersverificatie, enz.	Schakel SNMPv3 in en stel vervolgens de verificatiemethode en de versleutelingsmethode in.	Bewaak het wijzigen van instellingen via het netwerk, vertrouwelijkheid in toestandbewaking.

Geavanceerde beveiligingsinstellingen voor bedrijven

Naam	Type functie	Wat kunt u instellen	Wat voorkomt u
IEEE802.1X	Staat alleen een gebruiker die is geverifieerd via Ethernet toe om verbinding te maken. Staat alleen een toegestane gebruiker het apparaat te gebruiken.	Verificatie-instelling op de RADIUS-server (verificatiesever).	Voorkom ongeoorloofde toegang en ongeoorloofd gebruik van het apparaat.
Id-kaart lezen	U kunt het apparaat gebruiken met een id-kaart voor het verbonden geverifieerde apparaat. U kunt het ophalen van logboeken voor elke gebruiker en elk apparaat beperken en het beschikbare gebruik van apparaten en de beschikbare functies voor elke gebruiker en groep beperken.	Verbind een verificatieapparaat en configureer de informatie van een gebruiker in het verificatiesysteem.	Voorkom ongeoorloofd gebruik en spoofing van het apparaat.

Gerelateerde informatie

➡ “SSL/TLS-communicatie met de scanner” op pagina 63

➡ “Versleutelde communicatie met IPsec/IP-filtering” op pagina 71

➡ “Het protocol SNMPv3 gebruiken” op pagina 83

➡ “De scanner verbinden met een IEEE802.1X-netwerk” op pagina 85

Instellingen voor de beveiligingsfunctie

Wanneer IPsec/IP-filtering of IEEE802.1X wordt ingesteld, wordt aanbevolen Web Config te openen met SSL/TLS om informatie over instellingen te communiceren, om zo beveiligingsrisico's, zoals ongewenst wijzigen van instellingen of onderscheppen, te verminderen.

SSL/TLS-communicatie met de scanner

Wanneer het servercertificaat is ingesteld op gebruik van SSL/TLS-communicatie (Secure Sockets Layer/Transport Layer Security) met de scanner, kunt u het communicatiepad tussen computers versleutelen. Hiermee voorkomt u externe en ongeautoriseerde toegang.

Digitale certificering

❏ Certificaat ondertekend door een CA

Een certificaat dat door een CA (Certificate Authority of certificeringsinstantie) is ondertekend, moet eerst bij een certificeringsinstantie worden aangevraagd. Met een certificaat dat door een CA is ondertekend, maakt u veilige communicatie mogelijk. Voor elke beveiligingsfunctie kunt u een certificaat gebruiken dat door een CA is ondertekend.

❏ CA-certificaat

Een CA-certificaat geeft aan dat de identiteit van een server is gecontroleerd door derden. Dit is een belangrijke component voor beveiliging die uitgaat van een 'web van vertrouwen'. U moet voor de verificatie van de server een CA-certificaat aanvragen bij een CA die deze certificaten afgeeft.

❏ Zelfondertekend certificaat

Een zelfondertekend certificaat is een certificaat dat de scanner zelf afgeeft en ondertekent. Dit certificaat is onbetrouwbaar en kan spoofing niet voorkomen. Als u dit certificaat gebruikt voor een SSL/TLS-certificaat, kan een browser een beveiligingswaarschuwing weergeven. U kunt dit certificaat alleen gebruiken voor SSL/TLS-communicatie.

Gerelateerde informatie

➡ "Een door een CA ondertekend certificaat aanvragen en importeren" op pagina 64

➡ "Een door een CA ondertekend certificaat verwijderen" op pagina 68

➡ "Een zelfondertekend certificaat bijwerken" op pagina 68

Een door een CA ondertekend certificaat aanvragen en importeren

Een door een CA ondertekend certificaat aanvragen

Als u een certificaat wilt aanvragen dat door een CA is ondertekend, moet u eerst een CSR (Certificate Signing Request of aanvraag voor certificaatondertekening) maken en indienen bij de certificeringsinstantie. U kunt een CSR maken met Web Config en een computer.

Volg de stappen om met Web Config een CSR te maken en een door een CA ondertekend certificaat te ontvangen. Wanneer u een CSR maakt met Web Config, krijgt het certificaat de indeling PEM/DER.

1. Open Web Config en selecteer vervolgens **Network Security Settings**. Selecteer vervolgens **SSL/TLS** > **Certificate** of **IPsec/IP Filtering** > **Client Certificate** of **IEEE802.1X** > **Client Certificate**.

2. Klik op **Generate** voor de **CSR**.

   Er wordt een pagina voor het maken van een CSR geopend.

3. Voer voor elk item een waarde in.

   Opmerking:
   De beschikbare sleutellengte en afkortingen verschillen per certificeringsinstantie. Stel een aanvraag op volgens de regels van de certificeringsinstantie in kwestie.

4. Klik op **OK**.

   Na afloop wordt een bericht over voltooiing weergegeven.

5. Selecteer **Network Security Settings**. Selecteer vervolgens **SSL/TLS** > **Certificate** of **IPsec/IP Filtering** > **Client Certificate** of **IEEE802.1X** > **Client Certificate**.

6. Klik op een van de downloadknoppen voor de **CSR** met de opgegeven indeling volgens de certificeringsinstantie om de CSR te downloaden op een computer.

> ***Belangrijk:***
>
> *Genereer geen CSR opnieuw. Als u dat toch doet, kunt u een verstrekt CA-signed Certificate mogelijk niet importeren.*

7. Stuur de CSR naar een certificeringsinstantie. Daarmee vraagt u een door een CA-signed Certificate aan.

   Volg de regels van de desbetreffende certificeringsinstantie voor de wijze van verbinding en de vorm.

8. Sla het uitgegeven CA-signed Certificate op een computer op die verbinding heeft met de scanner.

   Het verkrijgen van een CA-signed Certificate is voltooid zodra u een certificaat opslaat op een bestemming.

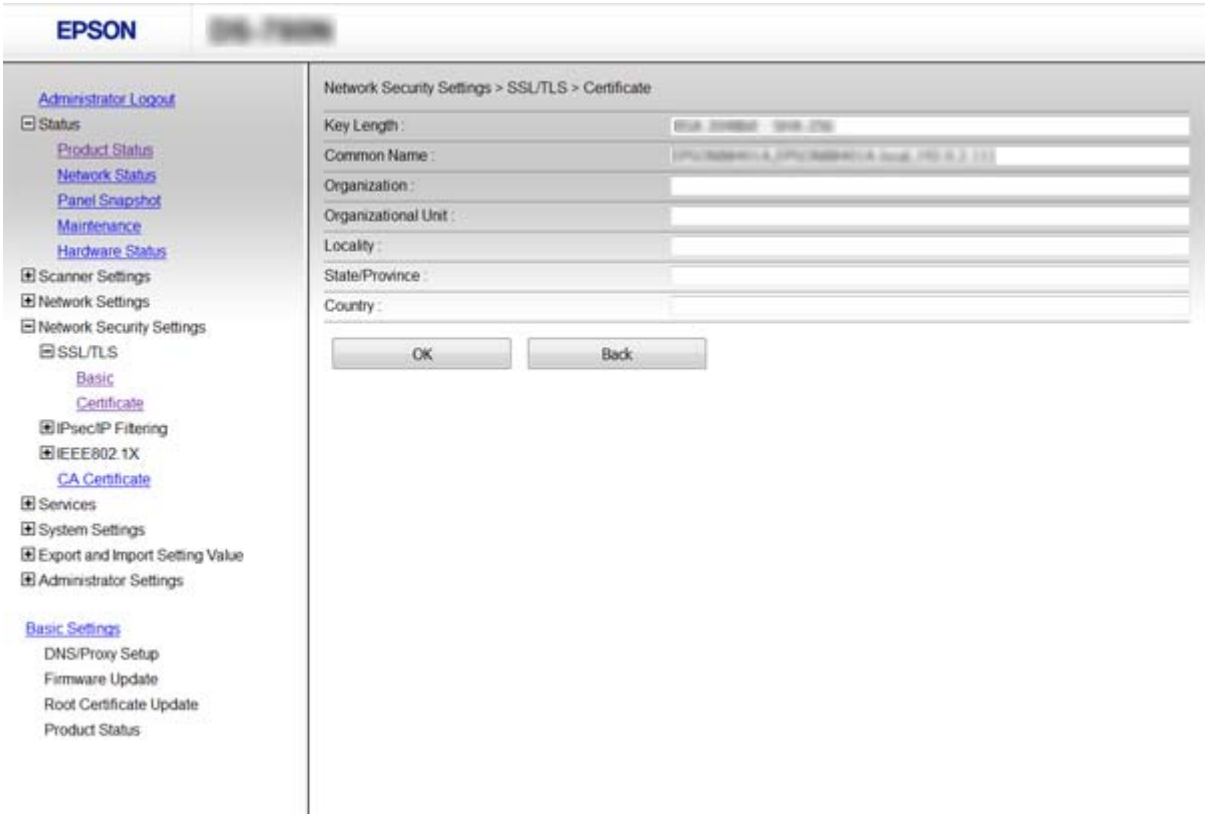
Gerelateerde informatie

➡ “Web Config openen” op pagina 23

➡ “Instellingen voor een CSR” op pagina 65

➡ “Een door een CA ondertekend certificaat importeren” op pagina 66

Instellingen voor een CSR



Items	Instellingen en uitleg
Key Length	Selecteer een sleutellengte voor een CSR.

Items	Instellingen en uitleg
Common Name	U kunt tussen 1 en 128 tekens invoeren. Als dit een IP-adres is, moet het een statisch IP-adres zijn. Voorbeeld: URL voor het benaderen van Web Config: https://10.152.12.225 Algemene naam: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	U kunt tussen 0 en 64 tekens in ASCII (0x20–0x7E) invoeren. U kunt de distinguished-namen (CN) met een komma scheiden.
Country	Voer een landcode in. Gebruik een tweecijferige code conform ISO-3166.

Gerelateerde informatie

➡ "Een door een CA ondertekend certificaat aanvragen" op pagina 64

Een door een CA ondertekend certificaat importeren

Belangrijk:

❏ *Zorg ervoor dat de datum en tijd van de scanner goed zijn ingesteld.*

❏ *Als u een certificaat ontvangt op basis van een CSR die u met Web Config hebt gemaakt, kunt u één keer een certificaat importeren.*

1. Open Web Config en selecteer vervolgens **Network Security Settings**. Selecteer vervolgens **SSL/TLS** > **Certificate** of **IPsec/IP Filtering** > **Client Certificate** of **IEEE802.1X** > **Client Certificate**.

2. Klik op **Import**.

   Er wordt een pagina voor het importeren van een certificaat geopend.

3. Voer voor elk item een waarde in.

   De vereiste instellingen zijn afhankelijk van de locatie waar u een CSR hebt gemaakt en de bestandsindeling van het certificaat. Stel de verschillende items in als volgt.

   ❏ Een certificaat met de indeling PEM/DER afkomstig uit Web Config

   ❏ **Private Key**: niet configureren. De scanner bevat een persoonlijke sleutel.

   ❏ **Password**: niet configureren.

   ❏ **CA Certificate 1**/**CA Certificate 2**: optie

   ❏ Een certificaat met de indeling PEM/DER afkomstig van een computer

   ❏ **Private Key**: wel instellen.

   ❏ **Password**: niet configureren.

   ❏ **CA Certificate 1**/**CA Certificate 2**: optie

❏ Een certificaat met de indeling PKCS#12 afkomstig van een computer

❏ **Private Key**: niet configureren.

❏ **Password**: optie

❏ **CA Certificate 1/CA Certificate 2**: niet configureren.

4. Klik op **OK**.

   Na afloop wordt een bericht over voltooiing weergegeven.

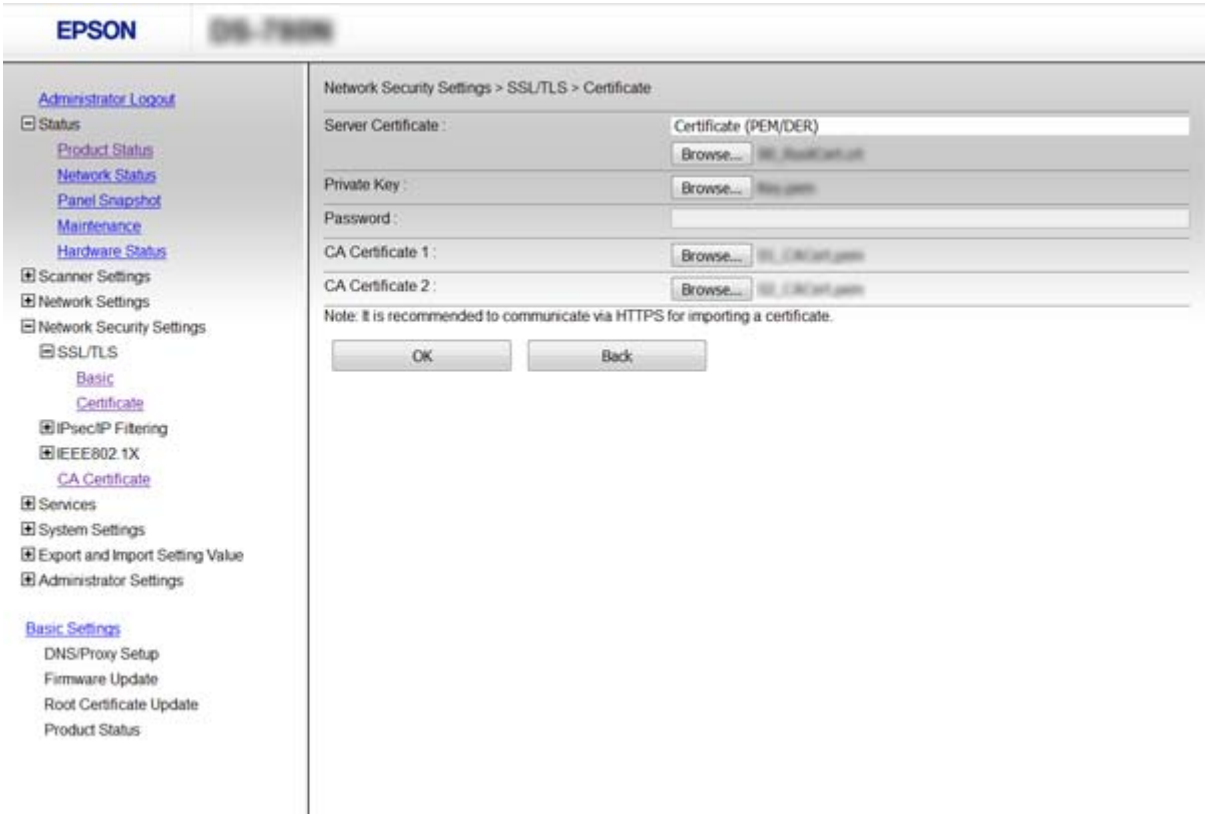
Opmerking:
*Klik op **Confirm** om de certificaatgegevens te controleren.*

Gerelateerde informatie

➡ "Web Config openen" op pagina 23

➡ "Instellingen voor het importeren van een door een CA ondertekend certificaat" op pagina 67

Instellingen voor het importeren van een door een CA ondertekend certificaat



Items	Instellingen en uitleg
Server Certificate of Client Certificate	Selecteer hier de indeling van het certificaat.
Private Key	Als u een certificaat met de indeling PEM/DER hebt op basis van een CSR die op een computer is gemaakt, geef dan hier het bestand op met de private sleutel voor het certificaat.
Password	Voer hier een wachtwoord in om de private sleutel te versleutelen.

Items	Instellingen en uitleg
CA Certificate 1	Als het certificaat de indeling **Certificate (PEM/DER)** heeft, importeer dan hier een certificaat van een certificeringsinstantie die servercertificaten afgeeft. Geef zo nodig een bestand op.
CA Certificate 2	Als het certificaat de indeling **Certificate (PEM/DER)** heeft, importeer dan hier een certificaat van een certificeringsinstantie die een **CA Certificate 1** afgeeft. Geef zo nodig een bestand op.

Gerelateerde informatie

➡ "Een door een CA ondertekend certificaat importeren" op pagina 66

Een door een CA ondertekend certificaat verwijderen

U kunt een geïmporteerd certificaat verwijderen wanneer het certificaat is vervallen of wanneer een versleutelde verbinding niet meer nodig is.

> ***Belangrijk:***
> *Als u een certificaat hebt op basis van een CSR die u met Web Config hebt gemaakt, kunt u het verwijderde certificaat niet opnieuw importeren. In dit geval moet u een CSR maken voor een nieuw certificaat.*

1. Open Web Config en selecteer vervolgens **Network Security Settings**. Selecteer vervolgens **SSL/TLS** > **Certificate** of **IPsec/IP Filtering** > **Client Certificate** of **IEEE802.1X** > **Client Certificate**.
2. Klik op **Delete**.
3. Bevestig dat u het certificaat in het weergegeven bericht wilt verwijderen.

Gerelateerde informatie

➡ "Web Config openen" op pagina 23

Een zelfondertekend certificaat bijwerken

Als de scanner HTTPS-servers ondersteunt, kunt u een zelfondertekend certificaat bijwerken. Wanneer u Web Config opent met een zelfondertekend certificaat, wordt een waarschuwing weergegeven.

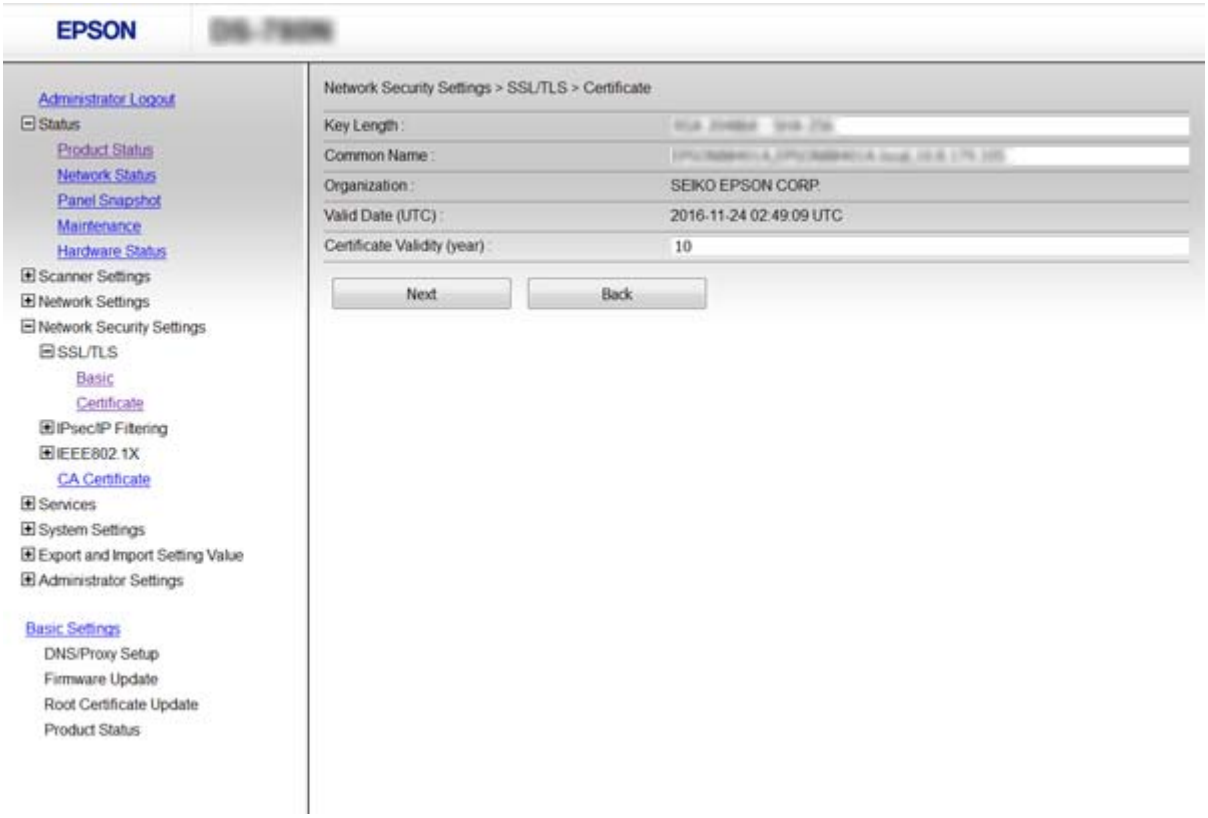
Gebruik tijdelijk een zelfondertekend certificaat totdat u een door een CA ondertekend certificaat ontvangt en importeert.

1. Open Web Config en selecteer **Network Security Settings** > **SSL/TLS** > **Certificate**.
2. Klik op **Update**.
3. Voer de **Common Name** in.

   Voer een IP-adres of een identificatie, zoals de FQDN-naam, voor de scanner in. U kunt tussen 1 en 128 tekens invoeren.

   Opmerking:
   U kunt distinguished-namen (CN) met een komma apart plaatsen.

4. Geef een geldigheidsperiode op voor het certificaat.



5. Klik op **Next**.

   Er wordt een bevestiging weergegeven.

6. Klik op **OK**.

   De scanner wordt bijgewerkt.

Opmerking:
*Klik op **Confirm** om de certificaatgegevens te controleren.*

Gerelateerde informatie

➡ "Web Config openen" op pagina 23

Configureer CA Certificate

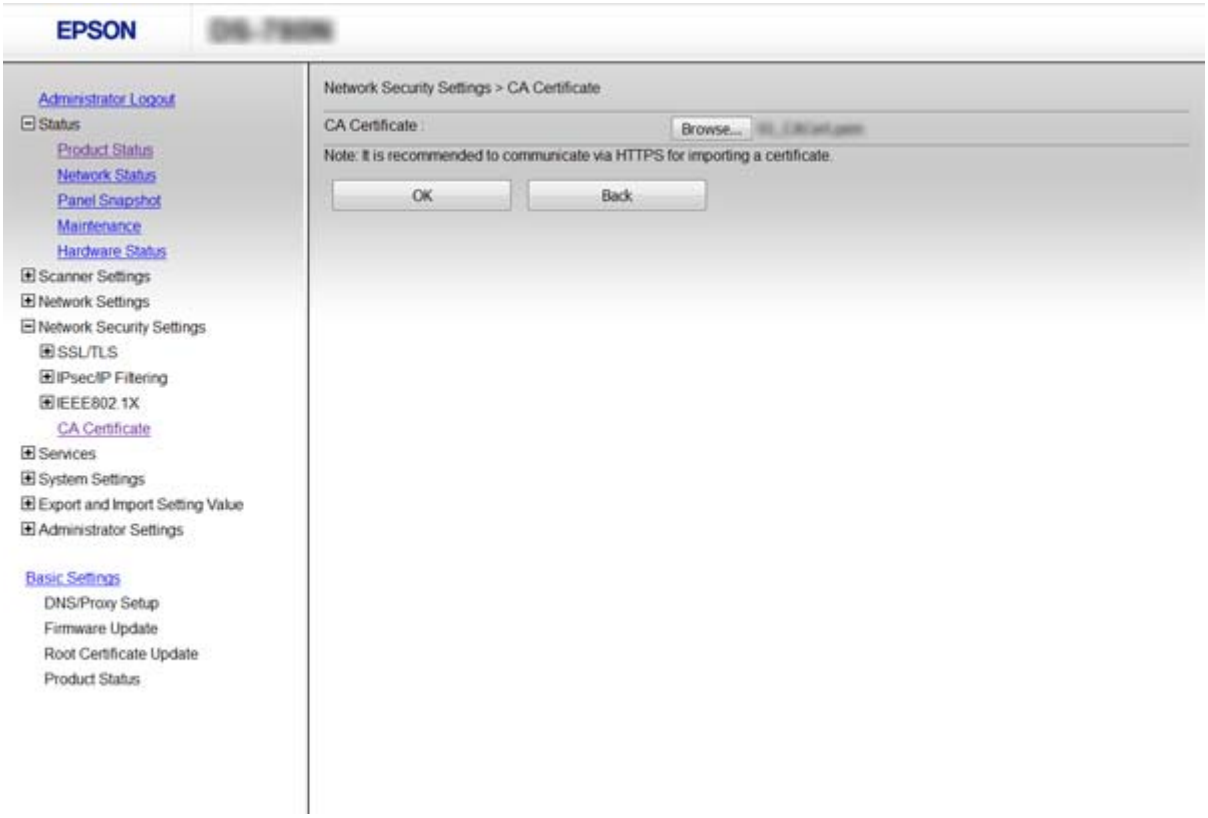
U kunt een CA Certificate importeren, weergeven of verwijderen.

Een CA Certificate importeren

1. Open Web Config en selecteer vervolgens **Network Security Settings** > **CA Certificate**.

2. Klik op **Import**.

3. Geef het CA Certificate op dat u wilt importeren.



4. Klik op **OK**.

Wanneer het importeren is voltooid, keert u terug naar het scherm **CA Certificate** en wordt het geïmporteerde CA Certificate weergegeven.

Gerelateerde informatie

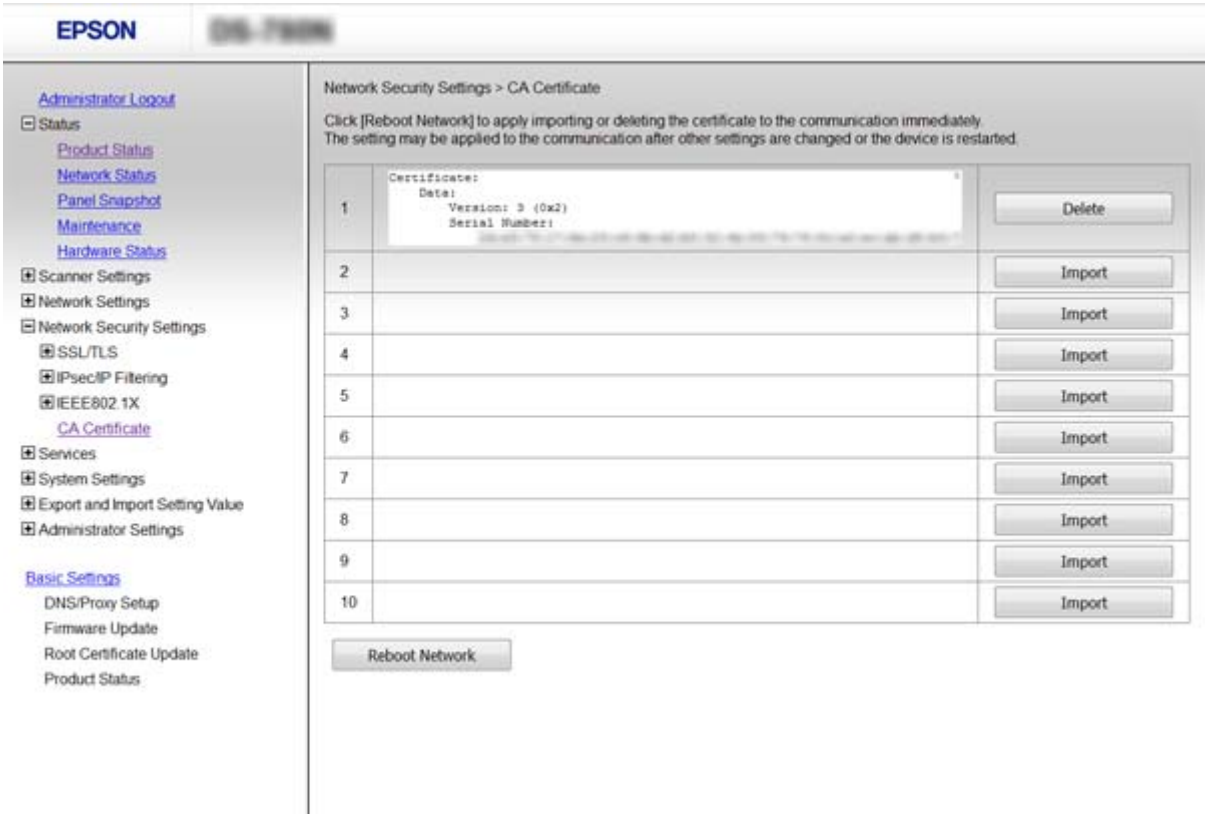
➡ "Web Config openen" op pagina 23

Een CA Certificate verwijderen

U kunt het geïmporteerde CA Certificate verwijderen.

1. Open Web Config en selecteer vervolgens **Network Security Settings** > **CA Certificate**.

2. Klik op **Delete** naast het CA Certificate dat u wilt verwijderen.



3. Bevestig dat u het certificaat in het weergegeven bericht wilt verwijderen.

Gerelateerde informatie

➡ "Web Config openen" op pagina 23

Versleutelde communicatie met IPsec/IP-filtering

Over IPsec/IP Filtering

Als de scanner IPsec/IP-filtering ondersteunt, kunt u het verkeer filteren op IP-adres, service en poort. Met een combinatie van filters kunt u de scanner zo configureren dat specifieke clients en data worden geaccepteerd of geblokkeerd. Bovendien is het met IPsec mogelijk om de beveiliging verder te verbeteren.

Configureer een standaardbeleid voor het filteren van het verkeer. Het standaardbeleid geldt voor elke gebruiker of groep die verbinding maakt met de scanner. Voor een meer fijnmazig beheer van gebruikers en groepen gebruikers kunt u ook met een groepsbeleid werken. Een groepsbeleid is een verzameling van regels die gelden voor een gebruiker of gebruikersgroep. De scanner monitort de IP-pakketten die overeenkomen met het geconfigureerde beleid. IP-pakketten worden eerst geverifieerd in volgorde van groepsbeleid 1 tot en met 10, daarna volgt het standaardbeleid.

Opmerking:
Computers met Windows Vista of hoger, of Windows Server 2008 of hoger ondersteunen IPsec.

Default Policy configureren

1. Open Web Config en selecteer **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Voer voor elk item een waarde in.
3. Klik op **Next**.

   Er wordt een bevestiging weergegeven.
4. Klik op **OK**.

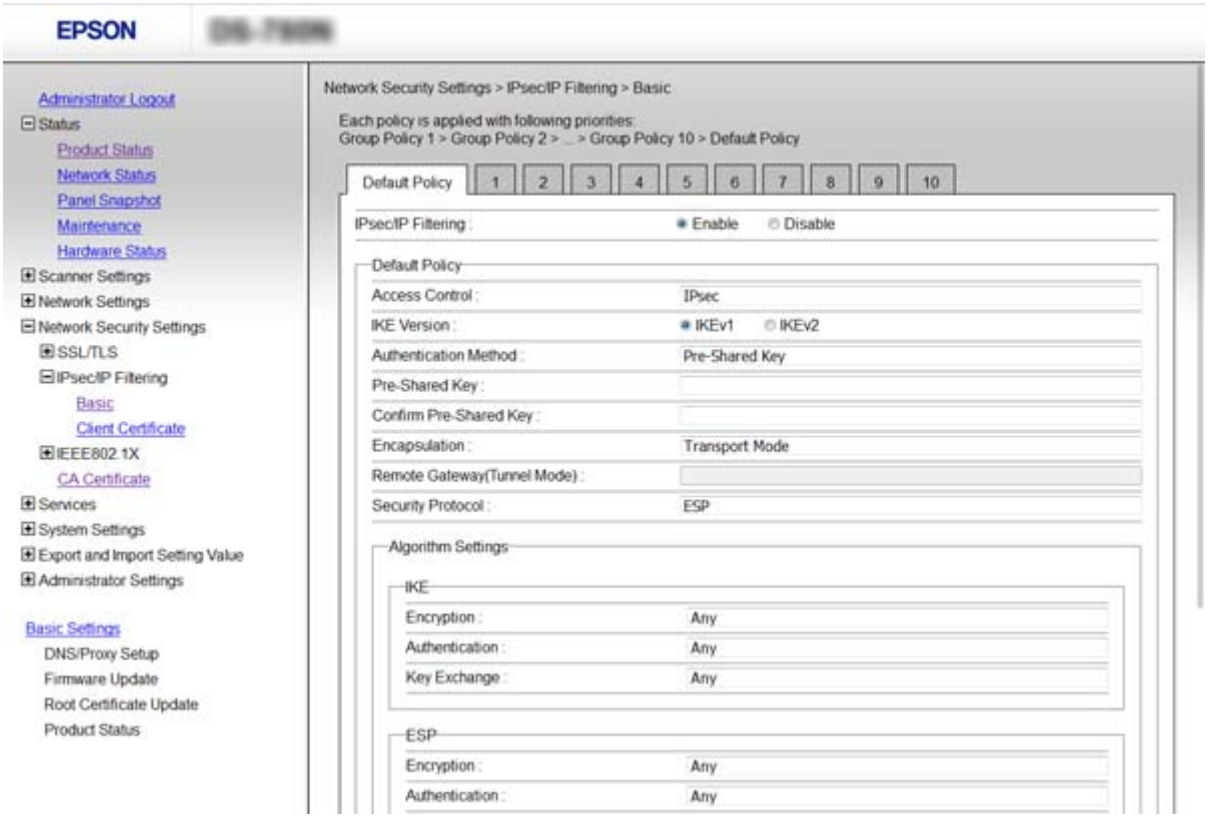
   De scanner wordt bijgewerkt.

Gerelateerde informatie

➡ "Web Config openen" op pagina 23

➡ "Instellingen voor Default Policy" op pagina 72

Instellingen voor Default Policy



Items	Instellingen en uitleg
IPsec/IP Filtering	U de functie IPsec/IP-filtering in- of uitschakelen.

Geavanceerde beveiligingsinstellingen voor bedrijven

Items	Instellingen en uitleg	
Access Control	Hiermee bepaalt u hoe het IP-verkeer wordt beheerd.	
	Permit Access	Selecteer deze optie om de geconfigureerde IP-pakketten door te laten.
	Refuse Access	Selecteer deze optie om de geconfigureerde IP-pakketten te weigeren.
	IPsec	Selecteer deze optie om de geconfigureerde IPsec-pakketten door te laten.
IKE Version	Selecteer IKEv1 of IKEv2 voor de IKE-versie. Selecteer een van beide op basis van het apparaat waarop de scanner wordt aangesloten.	
IKEv1	De volgende items worden weergegeven wanneer u **IKEv1** selecteert voor **IKE Version**.	
	Authentication Method	Als u **Certificate** wilt gebruiken, moet u op voorhand een door een CA ondertekend certificaat aanvragen en importeren.
	Pre-Shared Key	Als u **Pre-Shared Key** selecteert bij **Authentication Method**, voer dan een vooraf gedeelde sleutel in van minimaal 1 en maximaal 127 tekens.
	Confirm Pre-Shared Key	Voer de geconfigureerde sleutel in ter bevestiging.
IKEv2	De volgende items worden weergegeven wanneer u **IKEv2** selecteert voor **IKE Version**.	
Local	Authentication Method	Als u **Certificate** wilt gebruiken, moet u op voorhand een door een CA ondertekend certificaat aanvragen en importeren.
	ID Type	Selecteer het id-type voor de scanner.
	ID	Voer de scanner-id in die overeenkomt met het id-type. U kunt als eerste teken niet "@", "#", of "=" gebruiken. **Distinguished Name**: voer 1 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in. U moet "=" gebruiken. **IP Address**: voer IPv4- of IPv6-indeling in. **FQDN**: voer een combinatie van 1 tot 255 tekens in. Gebruik A–Z, a–z, 0–9, - en ".". **Email Address**: voer 1 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in. U moet "@" gebruiken. **Key ID**: voer 1 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in.
	Pre-Shared Key	Als u **Pre-Shared Key** selecteert bij **Authentication Method**, voer dan een vooraf gedeelde sleutel in van minimaal 1 en maximaal 127 tekens.
	Confirm Pre-Shared Key	Voer de geconfigureerde sleutel in ter bevestiging.

Geavanceerde beveiligingsinstellingen voor bedrijven

Items	Instellingen en uitleg	
Remote	Authentication Method	Als u **Certificate** wilt gebruiken, moet u op voorhand een door een CA ondertekend certificaat aanvragen en importeren.
	ID Type	Selecteer het id-type van het apparaat dat u wilt verifiëren.
	ID	Voer de scanner-id in die overeenkomt met het id-type. U kunt als eerste teken niet "@", "#", of "=" gebruiken. **Distinguished Name**: voer 1 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in. U moet "=" gebruiken. **IP Address**: voer IPv4- of IPv6-indeling in. **FQDN**: voer een combinatie van 1 tot 255 tekens in. Gebruik A–Z, a–z, 0–9, - en ".". **Email Address**: voer 1 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in. U moet "@" gebruiken. **Key ID**: voer 1 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in.
	Pre-Shared Key	Als u **Pre-Shared Key** selecteert bij **Authentication Method**, voer dan een vooraf gedeelde sleutel in van minimaal 1 en maximaal 127 tekens.
	Confirm Pre-Shared Key	Voer de geconfigureerde sleutel in ter bevestiging.
Encapsulation	Als u **IPsec** selecteert bij **Access Control**, moet u een vorm van inkapseling configureren.	
	Transport Mode	Selecteer deze optie als u de scanner alleen gebruikt in hetzelfde LAN. IP-pakketten van laag 4 of hoger worden versleuteld.
	Tunnel Mode	Als u de scanner gebruikt in een netwerk met internetmogelijkheid, zoals IPsec-VPN, selecteert u deze optie. De header en data van de IP-pakketten worden versleuteld.
Remote Gateway(Tunnel Mode)	Als u **Tunnel Mode** selecteert bij **Encapsulation**, voer dan een gatewayadres in van minimaal 1 en maximaal 39 tekens.	
Security Protocol	**IPsec** voor **Access Control**, selecteer een optie.	
	ESP	Selecteer deze optie om de integriteit van de verificatie en data te waarborgen en de data te versleutelen.
	AH	Selecteer deze optie om de integriteit van de verificatie en data te waarborgen. Ook als het versleutelen van data verboden is, kunt u IPsec toch gebruiken.
Algorithm Settings		
IKE	Encryption	Selecteer het versleutelingsalgoritme voor IKE. De items variëren afhankelijk van de IKE-versie.
	Authentication	Selecteer het verificatiealgoritme voor IKE.
	Key Exchange	Selecteer het sleuteluitwisselingsalgoritme voor IKE. De items variëren afhankelijk van de IKE-versie.

Items	Instellingen en uitleg	
ESP	Encryption	Selecteer het versleutelingsalgoritme voor ESP. Dit is beschikbaar wanneer **ESP** is geselecteerd voor **Security Protocol**.
	Authentication	Selecteer het verificatiealgoritme voor ESP. Dit is beschikbaar wanneer **ESP** is geselecteerd voor **Security Protocol**.
AH	Authentication	Selecteer het versleutelingsalgoritme voor AH. Dit is beschikbaar wanneer **AH** is geselecteerd voor **Security Protocol**.

Gerelateerde informatie

➡ "Default Policy configureren" op pagina 72

Group Policy configureren

1. Open Web Config en selecteer **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Klik op een genummerd tabblad dat u wilt configureren.
3. Voer voor elk item een waarde in.
4. Klik op **Next**.

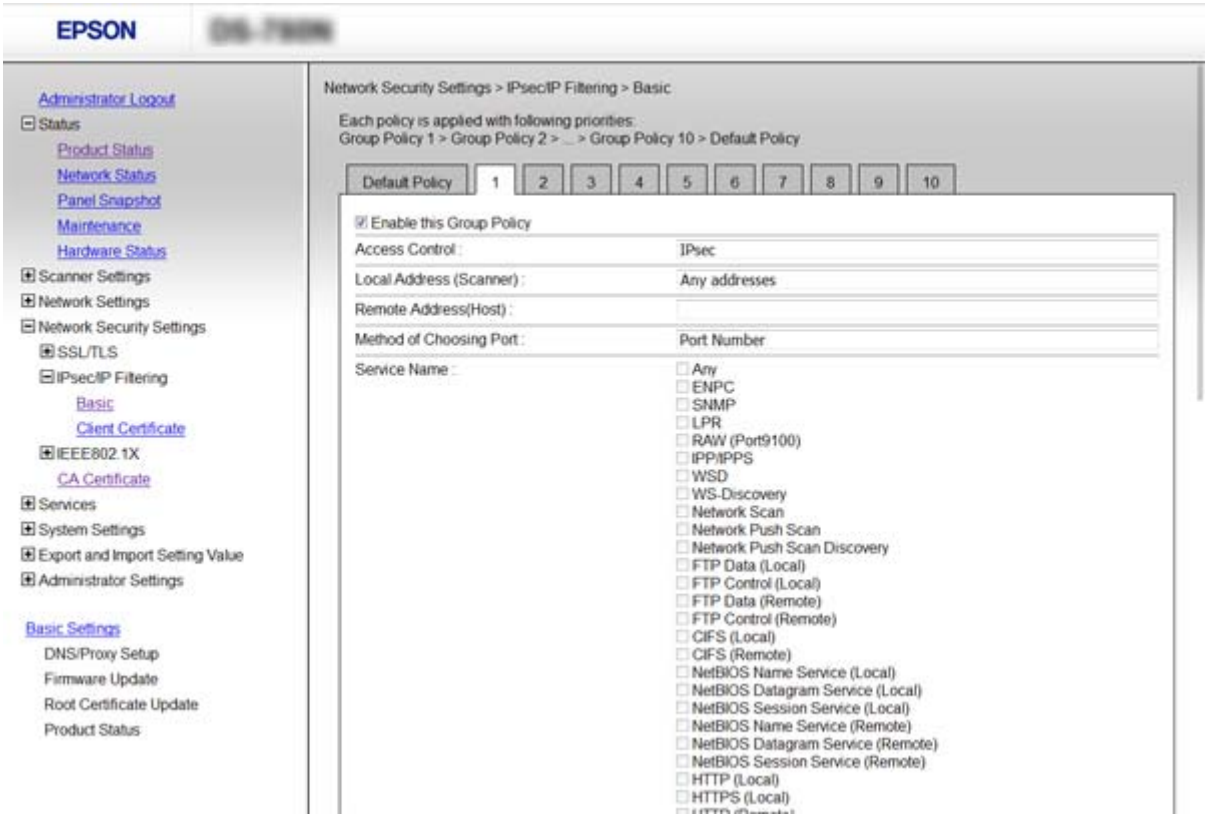
   Er wordt een bevestiging weergegeven.
5. Klik op **OK**.

   De scanner wordt bijgewerkt.

Gerelateerde informatie

➡ "Web Config openen" op pagina 23
➡ "Instellingen voor Group Policy" op pagina 76

Instellingen voor Group Policy



Items	Instellingen en uitleg	
Enable this Group Policy	Hiermee schakelt u het groepsbeleid in of uit.	
Access Control	Hiermee bepaalt u hoe het IP-verkeer wordt beheerd.	
	Permit Access	Selecteer deze optie om de geconfigureerde IP-pakketten door te laten.
	Refuse Access	Selecteer deze optie om de geconfigureerde IP-pakketten te weigeren.
	IPsec	Selecteer deze optie om de geconfigureerde IPsec-pakketten door te laten.
Local Address (Scanner)	Selecteer een IPv4-adres of een IPv6-adres dat overeenkomt met uw netwerkomgeving. Als er automatisch een IP-adres wordt toegewezen, kunt u **Use auto-obtained IPv4 address** gebruiken.	
Remote Address(Host)	Hier voert u het IP-adres van een apparaat in om te toegang te regelen. Het IP-adres mag maximaal 43 tekens lang zijn. Als u geen IP-adres opgeeft, worden alle adressen beheerd. ***Opmerking:*** *Als een IP-adres automatisch wordt toegewezen (met DHCP bijvoorbeeld), is de verbinding mogelijk niet beschikbaar. Configureer een statisch IP-adres.*	
Method of Choosing Port	Hiermee bepaalt u hoe de poorten worden opgegeven.	
Service Name	Als u **Service Name** selecteert bij **Method of Choosing Port**, moet u een optie selecteren.	

Geavanceerde beveiligingsinstellingen voor bedrijven

Items	Instellingen en uitleg	
Transport Protocol	Als u **Port Number** selecteert bij **Method of Choosing Port**, moet u een vorm van inkapseling configureren.	
	Any Protocol	Selecteer deze optie om alle protocoltypen aan te sturen.
	TCP	Selecteer deze optie om de gegevens voor unicast aan te sturen.
	UDP	Selecteer deze optie om de gegevens voor broadcast en multicast aan te sturen.
	ICMPv4	Selecteer deze optie om een pingopdracht aan te sturen.
Local Port	Als u **Port Number** selecteert voor **Method of Choosing Port** en **TCP** of **UDP** selecteert voor **Transport Protocol**, geeft u poortnummers op, gescheiden door komma's, om het ontvangen van pakketten te controleren. U kunt maximaal tien poortnummers invoeren. Voorbeeld: 20,80,119,5220 Als u geen poortnummer opgeeft, worden alle poorten gebruikt.	
Remote Port	Als u **Port Number** selecteert voor **Method of Choosing Port** en **TCP** of **UDP** selecteert voor **Transport Protocol**, geeft u poortnummers op, gescheiden door komma's, om het verzenden van pakketten te controleren. U kunt maximaal tien poortnummers invoeren. Voorbeeld: 25,80,143,5220 Als u geen poortnummer opgeeft, worden alle poorten gebruikt.	
IKE Version	Selecteer IKEv1 of IKEv2 voor de IKE-versie. Selecteer een van beide op basis van het apparaat waarop de scanner wordt aangesloten.	
IKEv1	De volgende items worden weergegeven wanneer u **IKEv1** selecteert voor **IKE Version**.	
	Authentication Method	Als u **IPsec** selecteert bij **Access Control**, moet u een optie selecteren. Het gebruikte certificaat is gelijk aan dat van het standaardbeleid.
	Pre-Shared Key	Als u **Pre-Shared Key** selecteert bij **Authentication Method**, voer dan een vooraf gedeelde sleutel in van minimaal 1 en maximaal 127 tekens.
	Confirm Pre-Shared Key	Voer de geconfigureerde sleutel in ter bevestiging.
IKEv2	De volgende items worden weergegeven wanneer u **IKEv2** selecteert voor **IKE Version**.	

Geavanceerde beveiligingsinstellingen voor bedrijven

Items	Instellingen en uitleg	
Local	Authentication Method	Als u **IPsec** selecteert bij **Access Control**, moet u een optie selecteren. Het gebruikte certificaat is gelijk aan dat van het standaardbeleid.
	ID Type	Selecteer het id-type voor de scanner.
	ID	Voer de scanner-id in die overeenkomt met het id-type. U kunt als eerste teken niet "@", "#", of "=" gebruiken. **Distinguished Name**: voer 1 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in. U moet "=" gebruiken. **IP Address**: voer IPv4- of IPv6-indeling in. **FQDN**: voer een combinatie van 1 tot 255 tekens in. Gebruik A–Z, a–z, 0–9, - en ".". **Email Address**: voer 1 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in. U moet "@" gebruiken. **Key ID**: voer 1 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in.
	Pre-Shared Key	Als u **Pre-Shared Key** selecteert bij **Authentication Method**, voer dan een vooraf gedeelde sleutel in van minimaal 1 en maximaal 127 tekens.
	Confirm Pre-Shared Key	Voer de geconfigureerde sleutel in ter bevestiging.
Remote	Authentication Method	Als u **IPsec** selecteert bij **Access Control**, moet u een optie selecteren. Het gebruikte certificaat is gelijk aan dat van het standaardbeleid.
	ID Type	Selecteer het id-type van het apparaat dat u wilt verifiëren.
	ID	Voer de scanner-id in die overeenkomt met het id-type. U kunt als eerste teken niet "@", "#", of "=" gebruiken. **Distinguished Name**: voer 1 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in. U moet "=" gebruiken. **IP Address**: voer IPv4- of IPv6-indeling in. **FQDN**: voer een combinatie van 1 tot 255 tekens in. Gebruik A–Z, a–z, 0–9, - en ".". **Email Address**: voer 1 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in. U moet "@" gebruiken. **Key ID**: voer 1 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in.
	Pre-Shared Key	Als u **Pre-Shared Key** selecteert bij **Authentication Method**, voer dan een vooraf gedeelde sleutel in van minimaal 1 en maximaal 127 tekens.
	Confirm Pre-Shared Key	Voer de geconfigureerde sleutel in ter bevestiging.

Geavanceerde beveiligingsinstellingen voor bedrijven

Items	Instellingen en uitleg	
Encapsulation	Als u **IPsec** selecteert bij **Access Control**, moet u een vorm van inkapseling configureren.	
	Transport Mode	Selecteer deze optie als u de scanner alleen gebruikt in hetzelfde LAN. IP-pakketten van laag 4 of hoger worden versleuteld.
	Tunnel Mode	Als u de scanner gebruikt in een netwerk met internetmogelijkheid, zoals IPsec-VPN, selecteert u deze optie. De header en data van de IP-pakketten worden versleuteld.
Remote Gateway(Tunnel Mode)	Als u **Tunnel Mode** selecteert bij **Encapsulation**, voer dan een gatewayadres in van minimaal 1 en maximaal 39 tekens.	
Security Protocol	Als u **IPsec** selecteert bij **Access Control**, moet u een optie selecteren.	
	ESP	Selecteer deze optie om de integriteit van de verificatie en data te waarborgen en de data te versleutelen.
	AH	Selecteer deze optie om de integriteit van de verificatie en data te waarborgen. Ook als het versleutelen van data verboden is, kunt u IPsec toch gebruiken.
Algorithm Settings		
IKE	Encryption	Selecteer het versleutelingsalgoritme voor IKE. De items variëren afhankelijk van de IKE-versie.
	Authentication	Selecteer het verificatiealgoritme voor IKE.
	Key Exchange	Selecteer het sleuteluitwisselingsalgoritme voor IKE. De items variëren afhankelijk van de IKE-versie.
ESP	Encryption	Selecteer het versleutelingsalgoritme voor ESP. Dit is beschikbaar wanneer **ESP** is geselecteerd voor **Security Protocol**.
	Authentication	Selecteer het verificatiealgoritme voor ESP. Dit is beschikbaar wanneer **ESP** is geselecteerd voor **Security Protocol**.
AH	Authentication	Selecteer het verificatiealgoritme voor AH. Dit is beschikbaar wanneer **AH** is geselecteerd voor **Security Protocol**.

Gerelateerde informatie

➡ “Group Policy configureren” op pagina 75

➡ “Combinatie van Local Address (Scanner) en Remote Address(Host) op Group Policy” op pagina 80

➡ “Referenties van servicenaam in Groepsbeleid” op pagina 80

Combinatie van Local Address (Scanner) en Remote Address(Host) op Group Policy

		Instelling van Local Address (Scanner)		
		IPv4	IPv6*2	Any addresses*3
Instelling van Remote Address(Host)	IPv4*1	✓	–	✓
	IPv6*1, *2	–	✓	✓
	Leeg	✓	✓	✓

*1 Als **IPsec** is geselecteerd voor **Access Control** kunt u geen lengte opgeven voor een voorvoegsel.

*2 Als **IPsec** is geselecteerd voor **Access Control** kunt u een lokaal gekoppeld adres (fe80::) selecteren, maar wordt het groepsbeleid uitgeschakeld.

*3 Met uitzondering van IPv6 lokaal gekoppelde adressen.

Referenties van servicenaam in Groepsbeleid

Opmerking:
Services die niet beschikbaar zijn, worden weergegeven, maar kunnen niet worden geselecteerd.

Servicenaam	Protocoltype	Nummer lokale poort	Nummer externe poort	Gecontroleerde kenmerken
Any	–	–	–	Alle services
ENPC	UDP	3289	Willekeurige poort	Zoeken naar een scanner vanuit toepassingen als EpsonNet Config en een scannerstuurprogramma
SNMP	UDP	161	Willekeurige poort	Verkrijgen en configureren van MIB vanuit toepassingen als EpsonNet Config en het Epson-scannerstuurprogramma
WSD	TCP	Willekeurige poort	5357	WSD beheren
WS-Discovery	UDP	3702	Willekeurige poort	Zoeken naar een scanner vanuit WSD
Network Scan	TCP	1865	Willekeurige poort	Scangegevens doorsturen vanuit Document Capture Pro
Network Push Scan Discovery	UDP	2968	Willekeurige poort	Zoeken naar een computer vanaf de scanner.
Network Push Scan	TCP	Willekeurige poort	2968	Taakinformatie ophalen of push-scan gebruiken vanuit Document Capture Pro of Document Capture

Servicenaam	Protocoltype	Nummer lokale poort	Nummer externe poort	Gecontroleerde kenmerken
HTTP (Local)	TCP	80	Willekeurige poort	HTTP(S)-server (gegevens van Web Config en WSD doorsturen)
HTTPS (Local)	TCP	443	Willekeurige poort	
HTTP (Remote)	TCP	Willekeurige poort	80	HTTP(S)-client (communiceren tussen firmware bijwerken en basiscertificaat bijwerken)
HTTPS (Remote)	TCP	Willekeurige poort	443	

Configuratievoorbeelden van IPsec/IP Filtering

Alleen IPsec-pakketten ontvangen

Dit voorbeeld is alleen voor configuratie van een standaardbeleid.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

❏ **Authentication Method**: **Pre-Shared Key**

❏ **Pre-Shared Key**: voer hier maximaal 127 tekens in.

Group Policy:

niet configureren.

Scan accepteren met Epson Scan 2 en de scannerinstellingen

In dit voorbeeld is communicatie van scangegevens en scannerconfiguratie van bepaalde services toegestaan.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **Refuse Access**

Group Policy:

❏ **Enable this Group Policy**: schakel het selectievakje in.

❏ **Access Control**: **Permit Access**

❏ **Remote Address(Host)**: het IP-adres van een client

❏ **Method of Choosing Port**: **Service Name**

❏ **Service Name**: schakel het selectievakje in bij **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)** en **HTTPS (Local)**.

Alleen toegang vanaf een bepaald IP-adres toestaan

In dit voorbeeld wordt een bepaald IP-adres toegang gegeven om de scanner te benaderen.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**:**Refuse Access**

Group Policy:

❏ **Enable this Group Policy**: schakel het selectievakje in.

❏ **Access Control**: **Permit Access**

❏ **Remote Address(Host)**: het IP-adres van de client van een beheerder

Opmerking:
Ongeacht het geconfigureerde beleid heeft de client toegang tot de scanner om deze te configureren.

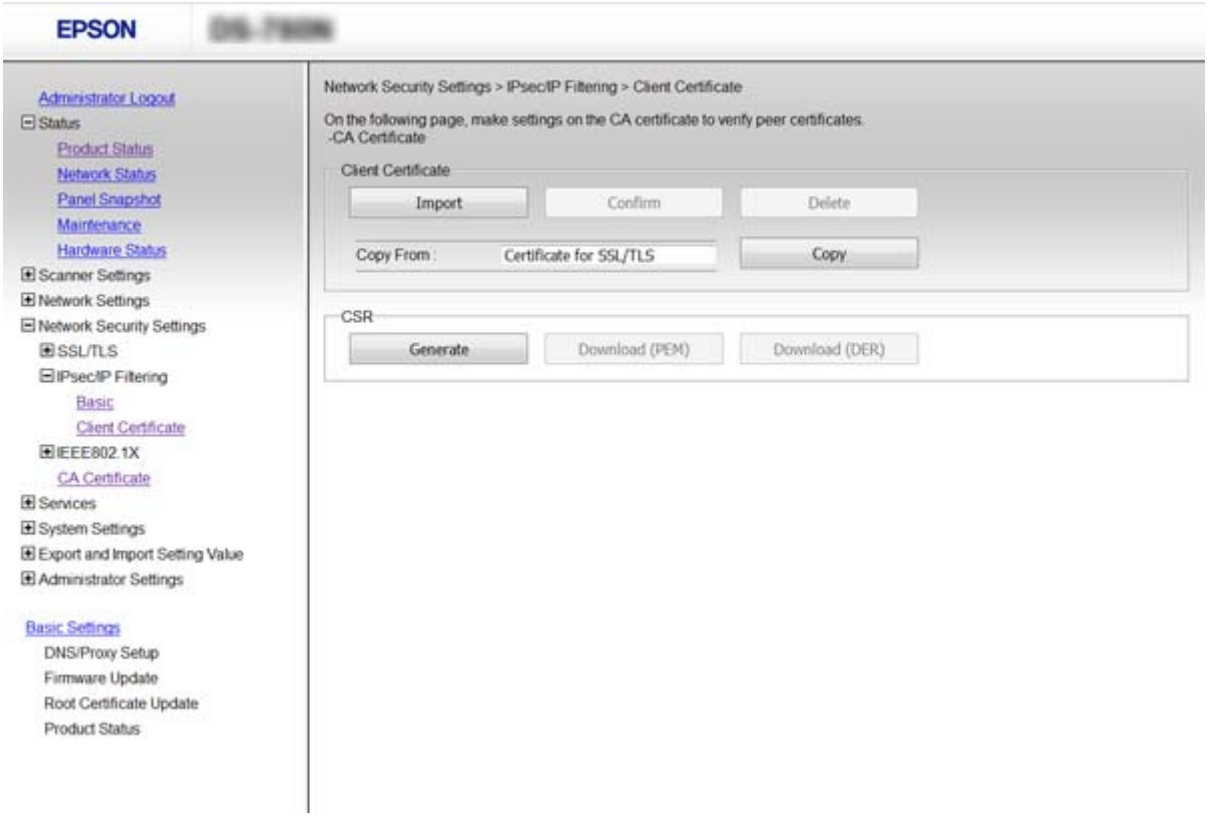
Een certificaat configureren voor IPsec/IP Filtering

Het clientcertificaat voor IPsec/IP-filter configureren. Als u de certificeringsinstantie wilt configureren, gaat u naar **CA Certificate**.

1. Open Web Config en selecteer **Network Security Settings** > **IPsec/IP Filtering** > **Client Certificate**.

2. Importeer het certificaat in **Client Certificate**.

   Als u al een certificaat hebt geïmporteerd dat door een certificeringsinstantie is gepubliceerd in IEEE802.1X of SSL/TLS, kunt u het certificaat kopiëren en dit gebruiken in IPsec/IP-filter. Om te kopiëren, selecteert u het certificaat in **Copy From** en klikt u vervolgens op **Copy**.



Gerelateerde informatie

➡ "Web Config openen" op pagina 23

➡ "Een door een CA ondertekend certificaat aanvragen en importeren" op pagina 64

Het protocol SNMPv3 gebruiken

Over SNMPv3

SNMP is een protocol dat bewaking en beheer uitvoert om informatie te verzamelen van de apparaten die met het netwerk zijn verbonden. SNMPv3 is de verbeterde versie van de beheersbeveiligingsfunctie.

Wanneer u SNMPv3 gebruikt, kan bewaking van de status in het instellen van wijzigingen van de SNMP-communicatie (pakket) worden geverifieerd en versleuteld om SNMP-communicatie (pakket) te beschermen tegen netwerkrisico's, zoals aftappen, imitatie en ongewenste wijzigingen.

SNMPv3 configureren

Als de scanner het SNMPv3-protocol ondersteunt, kunt u de scanner bewaken en toegang tot de scanner controleren.

1. Open Web Config en selecteer **Services** > **Protocol**.
2. Voer voor elk item van **SNMPv3 Settings** een waarde in.
3. Klik op **Next**.

   Er wordt een bevestiging weergegeven.
4. Klik op **OK**.

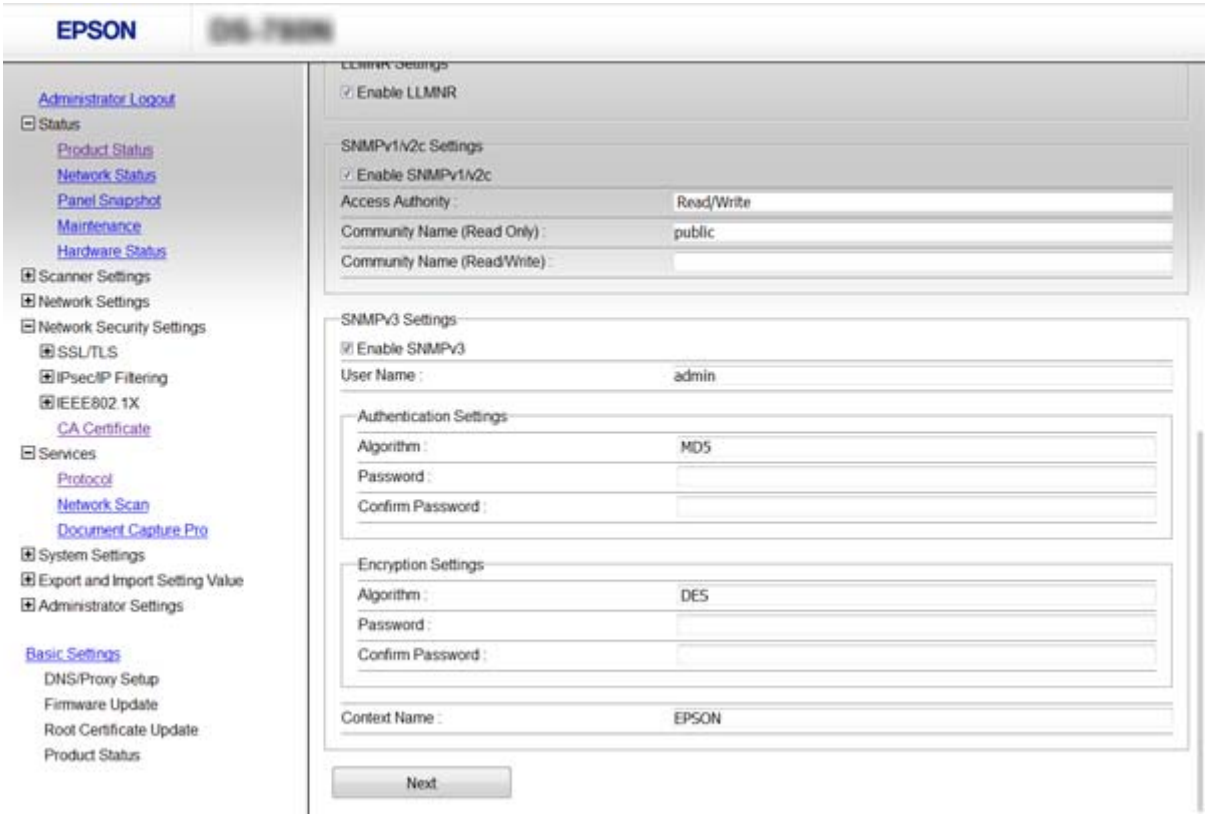
   De scanner wordt bijgewerkt.

Gerelateerde informatie

➡ “Web Config openen” op pagina 23

➡ “Instellingen voor SNMPv3” op pagina 84

Instellingen voor SNMPv3



Items	Instellingen en uitleg
Enable SNMPv3	Wanneer dit selectievakje is ingeschakeld, is SNMPv3 actief.
User Name	Voer hier tussen 1 en 32 tekens van 1 byte in.
Authentication Settings	
Algorithm	Selecteer een algoritme voor verificatie.
Password	Voer hier tussen 8 en 32 tekens in (ASCII (0x20-0x7E)).
Confirm Password	Voer hier het geconfigureerde wachtwoord in ter bevestiging.
Encryption Settings	
Algorithm	Selecteer hier een algoritme voor versleuteling.
Password	Voer hier tussen 8 en 32 tekens in (ASCII (0x20-0x7E)).
Confirm Password	Voer hier het geconfigureerde wachtwoord in ter bevestiging.
Context Name	Voer hier tussen 1 en 32 tekens van 1 byte in.

Gerelateerde informatie

➡ “SNMPv3 configureren” op pagina 83

De scanner verbinden met een IEEE802.1X-netwerk

Een IEEE802.1X-netwerk configureren

Als de scanner IEEE802.1X ondersteunt, kunt u de printer gebruiken in een netwerk met verificatie waarin een RADIUS-server wordt gebruikt in combinatie met een hub als verificator.

1. Open Web Config en selecteer **Network Security Settings** > **IEEE802.1X** > **Basic**.
2. Voer voor elk item een waarde in.
3. Klik op **Next**.

   Er wordt een bevestiging weergegeven.
4. Klik op **OK**.

   De scanner wordt bijgewerkt.

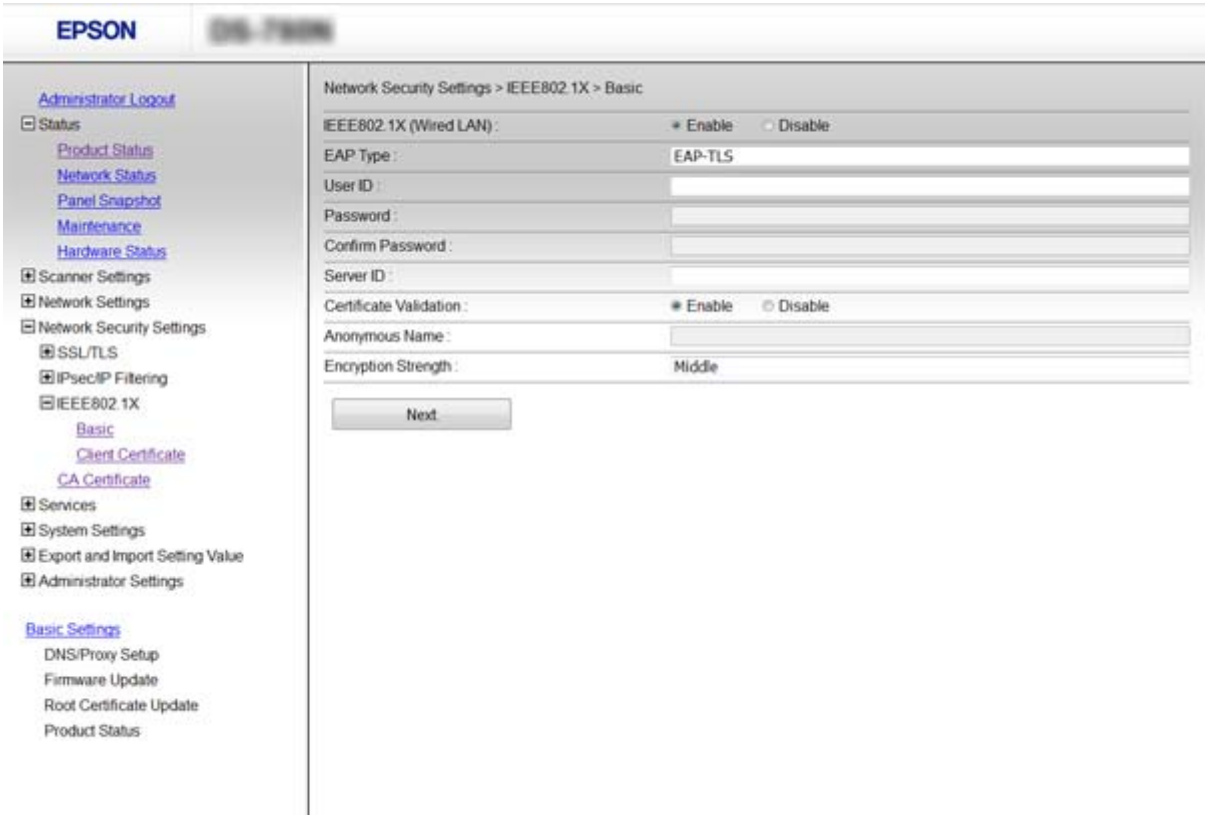
Gerelateerde informatie

➡ “Web Config openen” op pagina 23

➡ “Instellingen voor een IEEE802.1X-netwerk” op pagina 85

➡ “Geen toegang tot de printer of scanner na het configureren van IEEE802.1X” op pagina 90

Instellingen voor een IEEE802.1X-netwerk



Geavanceerde beveiligingsinstellingen voor bedrijven

Items	Instellingen en uitleg	
IEEE802.1X (Wired LAN)	U kunt de instellingen van de pagina in- of uitschakelen (**IEEE802.1X** > **Basic**) voor IEEE802.1X (bekabeld LAN).	
EAP Type	Selecteer een optie voor een verificatiemethode tussen de scanner en een RADIUS-server.	
	EAP-TLS	U moet een door een CA ondertekend certificaat aanvragen en importeren.
	PEAP-TLS	
	PEAP/MSCHAPv2	U moet een wachtwoord configureren.
User ID	Configureer een id die moet worden gebruikt voor een verificatie van een RADIUS-server. Voer 1 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in.	
Password	Configureer hier een wachtwoord voor verificatie van de scanner. Voer 1 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in. Als u een Windows-server gebruikt als RADIUS-server, kunt u maximaal 127 tekens invoeren.	
Confirm Password	Voer het geconfigureerde wachtwoord in ter bevestiging.	
Server ID	U kunt een server-id configureren voor verificatie bij een opgegeven RADIUS-server. De verificator controleert of de server-id al dan niet voorkomt in het veld subject/subjectAltName van het servercertificaat dat wordt verzonden door een RADIUS-server. Voer 0 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in.	
Certificate Validation	U kunt de certificaatvalidatie instellen, ongeacht de verificatiemethode. Importeer het certificaat in **CA Certificate**.	
Anonymous Name	Als u **PEAP-TLS** of **PEAP/MSCHAPv2** selecteert bij **Authentication Method**, kunt u voor fase 1 van de PEAP-verificatie een anonieme naam opgeven in plaats van een gebruikers-id. Voer 0 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in.	
Encryption Strength	U kunt kiezen uit het volgende.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Gerelateerde informatie

➡ “Een IEEE802.1X-netwerk configureren” op pagina 85

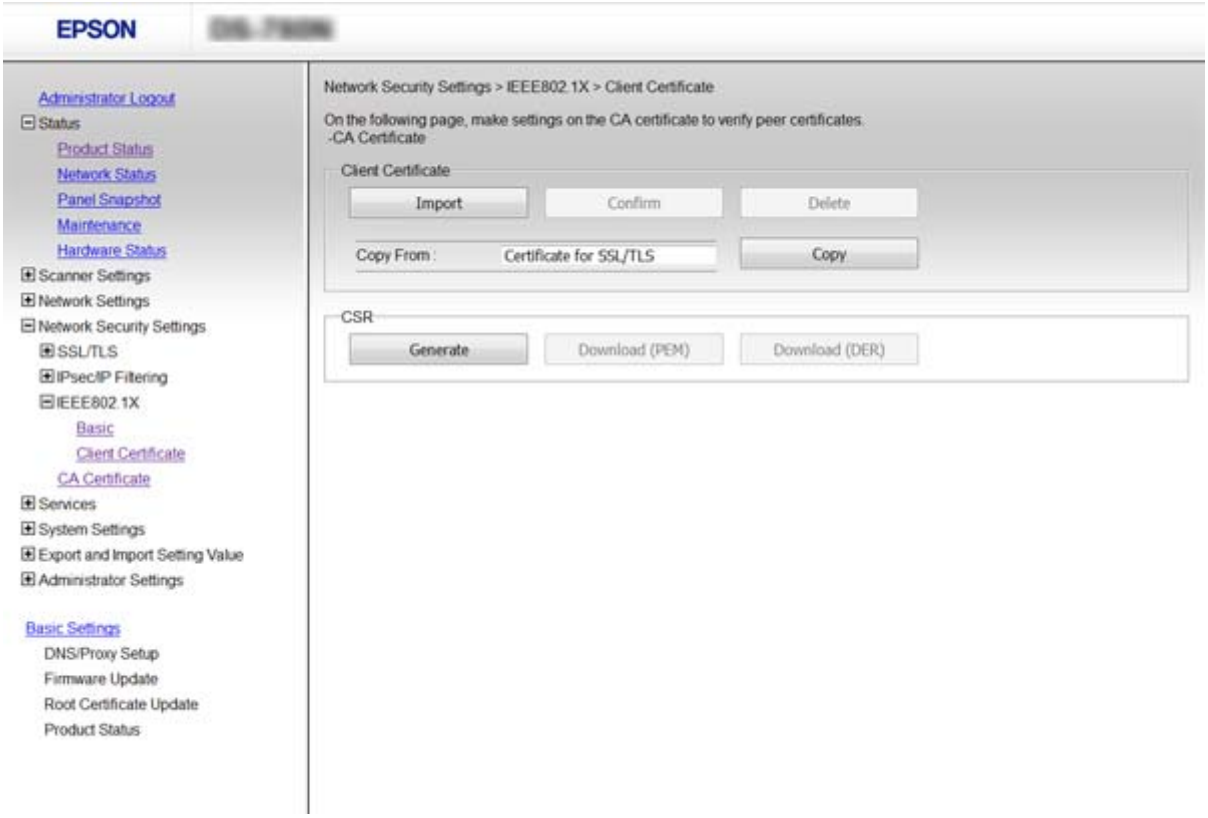
Een certificaat configureren voor IEEE802.1X

Configureer het clientcertificaat voor IEEE802.1X. Als u het certificaat van de certificaatinstantie wilt configureren, gaat u naar **CA Certificate**.

1. Open Web Config en selecteer **Network Security Settings** > **IEEE802.1X** > **Client Certificate**.

2. Voer een certificaat in **Client Certificate** in.

   U kunt het certificaat kopiëren als het wordt gepubliceerd door een certificeringsinstantie. Om te kopiëren, selecteert u het certificaat in **Copy From** en klikt u vervolgens op **Copy**.



Gerelateerde informatie

➡ “Web Config openen” op pagina 23

➡ “Een door een CA ondertekend certificaat aanvragen en importeren” op pagina 64

Problemen met geavanceerd beveiliging oplossen

De beveiligingsinstellingen herstellen

Wanneer u een in hoge mate beveiligde omgeving configureert, bijv. IPsec/IP-filtering of IEEE802.1X, kunt u mogelijk niet communiceren met apparaten vanwege onjuiste instellingen of problemen met het apparaat of de server. Herstel in dat geval de beveiligingsinstellingen om de instellingen voor het apparaat opnieuw te configureren of tijdelijk gebruik mogelijk te maken.

De beveiligingsfunctie uitschakelen vanaf het bedieningspaneel

U kunt IPsec/IP-filtering of IEEE802.1X uitschakelen vanaf het bedieningspaneel van de scanner.

1. Tik op **Instel.** > **Netwerkinstellingen**.

2. Tik op **Instellingen wijzigen**.
3. Tik op de items die u wilt uitschakelen.
   - ❏ **IPsec/IP-filter**
   - ❏ **IEEE802.1X**
4. Wanneer een voltooiingsbericht wordt weergegeven, tikt u op **Doorg.**.

De beveiligingsfunctie herstellen met Web Config

Met IEEE802.1X worden apparaten mogelijk niet herkend in het netwerk. Schakel in dat geval de functie uit via het bedieningspaneel van de scanner.

Voor IPsec/IP-filtering kunt u de functie uitschakelen als u vanaf de computer toegang hebt tot het apparaat.

IPsec/IP-filtering uitschakelen met Web Config

1. Open Web Config en selecteer **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Selecteer **Disable** voor **IPsec/IP Filtering** in **Default Policy**.
3. Klik op **Next** en wis **Enable this Group Policy** voor alle groepsbeleidsregels.
4. Klik op **OK**.

Gerelateerde informatie

➡ "Web Config openen" op pagina 23

Problemen met het gebruik van netwerkbeveiligingsfuncties

Een vooraf gedeelde sleutel vergeten

Configureer de sleutel opnieuw met Web Config.

Als u de sleutel wilt wijzigen, opent u Web Config en selecteert u **Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Default Policy** of **Group Policy**.

Wanneer u de vooraf gedeelde sleutel wijzigt, moet u de vooraf gedeelde sleutel voor computers configureren.

Gerelateerde informatie

➡ "Web Config openen" op pagina 23

Geen communicatie mogelijk met IPsec-communicatie

Gebruikt u voor de computerinstellingen een algoritme dat niet wordt ondersteund?

De scanner ondersteunt de volgende algoritmen.

Beveiligingsmethoden	Algoritmen
IKE-versleutelingsalgoritme	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE-verificatiealgoritme	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE-sleuteluitwisselingsalgoritme	DH-groep 1, DH-groep 2, DH-groep 5, DH-groep 14, DH-groep 15, DH-groep 16, DH-groep 17, DH-groep 18, DH-groep 19, DH-groep 20, DH-groep 21,DH-groep 22, DH-groep 23, DH-groep 24, DH-groep 25, DH-groep 26, DH-groep 27*, DH-groep 28*, DH-groep 29*, DH-groep 30*
ESP-versleutelingsalgoritme	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP-verificatiealgoritme	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH-verificatiealgoritme	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* alleen beschikbaar voor IKEv2

Gerelateerde informatie

➡ “Versleutelde communicatie met IPsec/IP-filtering” op pagina 71

Plotseling geen communicatie mogelijk

Is het IP-adres van de scanner ongeldig of is het gewijzigd?

Schakel IPsec uit op het bedieningspaneel van de scanner.

Als de DHCP vervallen is of opnieuw opstart, of als het IPv6-adres vervallen is of niet kan worden opgehaald, wordt het geregistreerde IP-adres voor de Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) van de scanner mogelijk niet gevonden.

Gebruik een statisch IP-adres.

Is het IP-adres van de computer ongeldig of is het gewijzigd?

Schakel IPsec uit op het bedieningspaneel van de scanner.

Als de DHCP vervallen is of opnieuw opstart, of als het IPv6-adres vervallen is of niet kan worden opgehaald, wordt het geregistreerde IP-adres voor de Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) van de scanner mogelijk niet gevonden.

Gebruik een statisch IP-adres.

Gerelateerde informatie

➡ “Web Config openen” op pagina 23

➡ “Versleutelde communicatie met IPsec/IP-filtering” op pagina 71

Kan geen verbinding maken naar het configureren van IPsec/IP-filter

De ingestelde waarde is mogelijk onjuist.

Schakel IPsec/IP-filter uit via het bedieningspaneel van de scanner. Sluit de scanner en computer aan en voer de instellingen voor IPsec/IP-filter opnieuw in.

Gerelateerde informatie

➡ "Versleutelde communicatie met IPsec/IP-filtering" op pagina 71

Geen toegang tot de printer of scanner na het configureren van IEEE802.1X

Mogelijk zijn de instellingen onjuist.

Schakel IEEE802.1X uit op het bedieningspaneel van de scanner. Verbind de scanner en een computer en configureer IEEE802.1X opnieuw.

Gerelateerde informatie

➡ "Een IEEE802.1X-netwerk configureren" op pagina 85

Problemen met het gebruik van een digitaal certificaat

Door CA ondertekend certificaat kan niet worden geïmporteerd

Stemmen het door de CA ondertekende certificaat en de gegevens van de CSR overeen?

Als het door de CA ondertekende certificaat en de CSR niet dezelfde gegevens bevatten, kan de CSR niet worden geïmporteerd. Controleer de volgende punten:

❏ Probeert u het certificaat te importeren op een apparaat dat niet dezelfde gegevens heeft?

Controleer de gegevens van de CSR en importeer het certificaat op een apparaat dat dezelfde gegevens bevat.

❏ Hebt u de CSR die in de scanner is opgeslagen overschreven na verzending van de CSR naar een certificeringsinstantie?

Vraag het door een CA ondertekende certificaat opnieuw aan met de CSR.

Is het door een CA ondertekende certificaat groter dan 5 kB?

Door een CA ondertekende certificaten van meer dan 5 kB kunnen niet worden geïmporteerd.

Gebruikt u het juiste wachtwoord voor het importeren van het certificaat?

Als u het wachtwoord niet meer weet, kunt u het certificaat niet importeren.

Gerelateerde informatie

➡ "Een door een CA ondertekend certificaat importeren" op pagina 66

Zelfondertekend certificaat kan niet worden bijgewerkt

Is de Common Name ingevoerd?

Er moet een **Common Name** worden ingevoerd.

Zijn er ongeschikte tekens gebruikt voor de Common Name? Japans bijvoorbeeld wordt niet ondersteund.

Voer tussen 1 en 128 tekens in. Gebruik de IPv4-, IPv6- of FQDN-indeling of de hostnaam in ASCII (0x20-0x7E).

Is er een komma of spatie gebruikt in de Common Name?

Als een komma is ingevoerd, wordt de **Common Name** op dat punt opgedeeld. Als er alleen een spatie is ingevoerd voor of na een komma, treedt er een fout op.

Gerelateerde informatie

➡ "Een zelfondertekend certificaat bijwerken" op pagina 68

CSR kan niet worden gemaakt

Is de Common Name ingevoerd?

Er moet een **Common Name** worden ingevoerd.

Zijn er ongeschikte tekens gebruikt voor de Common Name, Organization, Organizational Unit, Locality, State/Province? Japans bijvoorbeeld wordt niet ondersteund.

Gebruik de IPv4-, IPv6- of FQDN-indeling of de hostnaam in ASCII (0x20-0x7E).

Is er een komma of spatie gebruikt in de Common Name?

Als een komma is ingevoerd, wordt de **Common Name** op dat punt opgedeeld. Als er alleen een spatie is ingevoerd voor of na een komma, treedt er een fout op.

Gerelateerde informatie

➡ "Een door een CA ondertekend certificaat aanvragen" op pagina 64

Er wordt een waarschuwing over een digitaal certificaat weergegeven

Berichten	Oorzaak/Wat doen
Enter a Server Certificate.	**Oorzaak:** U hebt geen bestand geselecteerd om te importeren. **Wat doen:** Selecteer een bestand en klik op **Import**.

Geavanceerde beveiligingsinstellingen voor bedrijven

Berichten	Oorzaak/Wat doen
CA Certificate 1 is not entered.	**Oorzaak:** CA-certificaat 1 is niet ingevoerd. Alleen CA-certificaat 2 is ingevoerd. **Wat doen:** Importeer eerst CA-certificaat 1.
Invalid value below.	**Oorzaak:** Het bestandspad en/of wachtwoord bevat(ten) tekens die niet mogen worden gebruikt. **Wat doen:** Gebruik de juiste tekens voor het item.
Invalid date and time.	**Oorzaak:** De datum en tijd van de scanner zijn niet ingesteld. **Wat doen:** Stel de datum en tijd in met Web Config of EpsonNet Config.
Invalid password.	**Oorzaak:** Het ingevoerde wachtwoord is niet gelijk aan het wachtwoord dat is ingesteld voor het CA-certificaat. **Wat doen:** Voer het juiste wachtwoord in.
Invalid file.	**Oorzaak:** U importeert geen certificaatbestand in de indeling X509. **Wat doen:** Selecteer het juiste certificaat dat afkomstig is van een vertrouwde certificeringsinstantie.
	Oorzaak: Het bestand dat u hebt geïmporteerd, is te groot. De bestandsgrootte is maximaal 5 kB. **Wat doen:** Als u het juiste bestand hebt geselecteerd, is het certificaat mogelijk beschadigd of vals.
	Oorzaak: De keten in het certificaat is ongeldig. **Wat doen:** Zie de website van de certificeringsinstantie voor meer informatie over certificaten.
Cannot use the Server Certificates that include more than three CA certificates.	**Oorzaak:** Het certificaatbestand in de indeling PKCS#12 bevat meer dan drie CA-certificaten. **Wat doen:** Importeer elk certificaat door conversie van PKCS#12 in PEM of importeer het certificaatbestand in de indeling PKCS#12 (maximaal twee CA-certificaten).

Berichten	Oorzaak/Wat doen
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**Oorzaak:** Het certificaat is vervallen. **Wat doen:** ❏ Als het certificaat vervallen is, moet u een nieuw certificaat aanvragen en importeren. ❏ Als het certificaat niet vervallen is, zorg er dan voor dat de datum en tijd van de scanner goed zijn ingesteld.
Private key is required.	**Oorzaak:** Er is geen private sleutel aan het certificaat gekoppeld. **Wat doen:** ❏ Als het certificaat de indeling PEM/DER heeft en is verkregen met een CSR en een computer, geef dan het sleutelbestand op. ❏ Als het certificaat de indeling PKCS#12 heeft en is verkregen met een CSR en een computer, maak dan een bestand met daarin de sleutel.
	Oorzaak: U hebt het PEM/DER-certificaat dat is verkregen met een CSR en Web Config opnieuw geïmporteerd. **Wat doen:** Als het certificaat de indeling PEM/DER heeft en is verkregen met een CSR en Web Config, kunt u het maar eenmaal importeren.
Setup failed.	**Oorzaak:** De configuratie kan niet worden voltooid, omdat de communicatie tussen de scanner en computer is mislukt of het bestand kan niet worden gelezen als gevolg van fouten. **Wat doen:** Controleer het opgegeven bestand en de communicatie en importeer het bestand opnieuw.

Gerelateerde informatie

➡ “Digitale certificering” op pagina 63

Door CA ondertekend bestand per ongeluk verwijderd

Is er een back-upbestand voor het certificaat?

Als u een back-upbestand hebt, importeer het certificaat dan opnieuw.

Als u een certificaat hebt op basis van een CSR die u met Web Config hebt gemaakt, kunt u het verwijderde certificaat niet opnieuw importeren. Maak een CSR en vraag een nieuw certificaat aan.

Gerelateerde informatie

➡ “Een door een CA ondertekend certificaat verwijderen” op pagina 68

➡ “Een door een CA ondertekend certificaat importeren” op pagina 66