



DS-900WN DS-800WN

Beheerdershandleiding

Vereiste instellingen voor verschillende doeleinden

Netwerkinstellingen

Vereiste instellingen voor scannen

Basisinstellingen voor beveiliging

Geavanceerde beveiligingsinstellingen

Epson Open Platform gebruiken

Copyright

Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar worden gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op enige andere manier, zonder voorafgaande schriftelijke toestemming van Seiko Epson Corporation. Er wordt geen patentaansprakelijkheid aanvaard met betrekking tot het gebruik van de informatie in deze handleiding. Evenmin wordt aansprakelijkheid aanvaard voor schade die voortvloeit uit het gebruik van de informatie in deze publicatie. De informatie in dit document is uitsluitend bestemd voor gebruik met dit Epson-product. Epson is niet verantwoordelijk voor gebruik van deze informatie in combinatie met andere producten.

Seiko Epson Corporation noch haar filialen kunnen verantwoordelijk worden gesteld door de koper van dit product of derden voor schade, verlies, kosten of uitgaven die de koper of derden oplopen ten gevolge van al dan niet foutief gebruik of misbruik van dit product of onbevoegde wijzigingen en herstellingen of (met uitzondering van de V.S.) het zich niet strikt houden aan de gebruiks- en onderhoudsvoorschriften van Seiko Epson Corporation.

Seiko Epson Corporation en haar dochterondernemingen kunnen niet verantwoordelijk worden gehouden voor schade of problemen voortvloeiend uit het gebruik van andere dan originele onderdelen of verbruiksgoederen kenbaar als Original Epson Products of Epson Approved Products by Seiko Epson.

Seiko Epson Corporation kan niet verantwoordelijk worden gesteld voor schade voortvloeiend uit elektromagnetische interferentie als gevolg van het gebruik van andere interfacekabels die door Seiko Epson Corporation worden aangeduid als Epson Approved Products.

© 2024 Seiko Epson Corporation

De inhoud van deze handleiding en de specificaties van dit product kunnen zonder aankondiging worden gewijzigd.

Handelsmerken

- Microsoft, Windows, Windows Server, Microsoft Edge, SharePoint, and Internet Explorer are trademarks of the Microsoft group of companies.
- Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- Chrome, Chromebook and Android are trademarks of Google LLC.
- Wi-Fi®, Wi-Fi Direct®, and Wi-Fi Protected Access® are registered trademarks of Wi-Fi Alliance®. Wi-Fi Protected Setup™, WPA2™, WPA3™ are trademarks of Wi-Fi Alliance®.
- The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- The Mopria™ word mark and the Mopria™ Logo are registered and/or unregistered trademarks of Mopria Alliance, Inc. in the United States and other countries. Unauthorized use is strictly prohibited.
- Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- Algemene kennisgeving: alle overige handelsmerken zijn het eigendom van hun respectieve eigenaren en dienen uitsluitend voor identificatiedoeleinden.

Inhoudsopgave

Copyright

Handelsmerken

Inleiding

De inhoud van dit document.	8
Deze handleiding gebruiken.	8
Markeringen en symbolen.	8
Beschrijvingen die in deze handleiding worden gebruikt.	8
Referenties voor besturingssystemen.	8

Opmerkingen over het beheerderswachtwoord

Opmerkingen over het beheerderswachtwoord.	11
Oorspronkelijk beheerderswachtwoord.	11
Bewerkingen waarvoor het beheerderswachtwoord vereist is.	11
Het beheerderswachtwoord wijzigen.	11
Het beheerderswachtwoord resetten.	12

Vereiste instellingen voor verschillende doeleinden

Vereiste instellingen voor verschillende doeleinden.	14
---	----

Netwerkinstellingen

De scanner met het netwerk verbinden.	17
Voor het maken van netwerkverbinding.	17
Verbinding maken met het netwerk via het bedieningspaneel.	19
De computer of apparaten toevoegen of vervangen.	23
Verbinding maken met een scanner die met het netwerk is verbonden.	23
Een smart device rechtstreeks verbinden met een scanner (Wi-Fi Direct).	25
De netwerkverbinding opnieuw instellen.	27
De status van de netwerkverbinding controleren.	29
De netwerkverbindingstatus controleren op het bedieningspaneel.	29
Netwerkspecificaties.	31
Wifi-specificaties.	31

Ethernet-specificaties.	32
Netwerkfuncties en ondersteuning voor IPv4/IPv6.	33
Beveiligingsprotocol.	33
Poort voor de scanner gebruiken.	33
Problemen oplossen.	35
Kan geen verbinding maken met een netwerk.	35

Software voor configuratie van de scanner

Toepassing voor het configureren van scannerbewerkingen (Web Config).	39
Web Config uitvoeren in een webbrowser.	39
Epson Device Admin.	40
Configuratiejabloon.	41

Vereiste instellingen voor scannen

Een mailserver registreren.	46
De verbinding met een mailserver controleren.	47
Een netwerkmap maken.	49
Contactpersonen beschikbaar maken.	55
Contactpersonen configureren — vergelijking.	56
Een bestemming opslaan in de contactpersonenlijst met Web Config.	56
Bestemmingen als groep registreren met Web Config.	58
Contactpersonen importeren en een back-up maken.	59
Contactpersonen exporteren en in bulk registreren met een hulpprogramma.	60
Samenwerking tussen de LDAP-server en gebruikers.	62
Instellen van AirPrint.	65
Problemen bij het voorbereiden van scannen via het netwerk.	66
Tips voor het oplossen van problemen.	66
Geen toegang tot Web Config.	66

Weergave van het bedieningspaneel aanpassen

Presets opslaan.	69
Menuopties van Presets.	70
Het startscherm van het bedieningspaneel bewerken.	71

De Indeling van het startscherm wijzigen.	71
Pictogram toevoegen.	72
Pictogram verwijderen.	73
Pictogram verplaatsen.	74

Basisinstellingen voor beveiliging

Informatie over functies voor productbeveiliging. . .	76
Beheerdersinstellingen.	76
Het beheerderswachtwoord configureren.	76
Instelling vergrendelen gebruiken voor het bedieningspaneel.	78
Als beheerder inloggen op het bedieningspaneel.	81
Beschikbare functies beperken (Toegangsbeheer). .	82
Een gebruikersaccount maken.	82
De Toegangsbeheer inschakelen.	83
Inloggen op een scanner waarop Toegangsbeheer is ingeschakeld.	83
De externe interface uitschakelen.	84
Programmaverificatie inschakelen bij opstarten. . .	85
Scannen via het netwerk vanaf de computer uitschakelen.	85
WSD-scanner in- of uitschakelen.	85
Een externe scanner beheren.	86
Informatie over een externe scanner controleren.	86
E-mailmeldingen ontvangen bij gebeurtenissen. .	86
De stroomtoevoer naar de scanner regelen met Web Config.	87
De standaardinstellingen herstellen.	88
Informatie over Epson Remote Services.	88
Problemen oplossen.	88
Beheerderswachtwoord vergeten.	88

Geavanceerde beveiligingsinstellingen

Beveiligingsinstellingen en voorkomen van gevaar. .	90
Instellingen van de beveiligingsfunctie.	91
Beheren met protocollen.	91
Protocollen beheren.	91
Protocollen die u kunt inschakelen of uitschakelen.	91
Protocolinstellingsitems.	92
Een digitaal certificaat gebruiken.	94
Digitale certificering.	94
Een CA-ondertekend Certificaat configureren. .	95
Een zelfondertekend certificaat bijwerken. . . .	98

Een CA-certificaat configureren.	99
SSL/TLS-communicatie met de scanner.	99
Basale SSL/TLS-instellingen configureren. . . .	100
Een servercertificaat voor de scanner configureren.	100
Versleutelde communicatie met IPsec/IP-filtering. .	101
Over IPsec/IP-filter.	101
Standaardbeleid configureren.	101
Groepsbeleid configureren.	104
Configuratievoorbelden van IPsec/IP-filter. . .	110
Een certificaat voor IPsec/IP-filtering configureren.	111
De scanner verbinden met een IEEE802.1X- netwerk.	111
Een IEEE 802.1X-netwerk configureren.	111
Een certificaat voor IEEE 802.1X configureren. .	113
Problemen met geavanceerd beveiliging oplossen. .	113
De beveiligingsinstellingen herstellen.	113
Problemen met het gebruik van netwerkbeveiligingsfuncties.	114
Problemen met het gebruik van een digitaal certificaat.	116

Epson Open Platform gebruiken

Overzicht van Epson Open Platform.	121
Epson Open Platform configureren.	121
Epson Open Platform valideren.	121

Een verificatieapparaat aansluiten

Het verificatieapparaat aansluiten.	124
Bedieningscontrole voor verificatieapparaat. . . .	124
Controleren of de verificatiekaart is herkend. . . .	124
Problemen met het verificatieapparaat oplossen. .	125
Kan de verificatiekaart niet lezen.	125

Onderhoud

De buitenzijde van de scanner schoonmaken. . . .	127
De binnenzijde van de scanner schoonmaken. . . .	127
De rollerset vervangen.	132
Codes voor de rollenset.	137
Het aantal scans opnieuw instellen na vervanging van de rollen.	137
Energiebesparing.	138
De scanner vervoeren.	138
Een back-up maken van de instellingen.	139
De instellingen exporteren.	139

De instellingen importeren.	140
Standaardinst. herstellen.	140
Toepassingen en firmware bijwerken.	141
De scannerfirmware bijwerken via het bedieningspaneel.	142
Firmware bijwerken met Web Config.	142
Firmware bijwerken zonder verbinding te maken met internet.	142



Inleiding

De inhoud van dit document.	8
Deze handleiding gebruiken.	8

De inhoud van dit document

In dit document staat de volgende informatie voor beheerders van scanners.

- Netwerkinstellingen
- De scanfunctie voorbereiden
- Beveiligingsinstellingen inschakelen en beheren
- Dagelijks onderhoud uitvoeren

Raadpleeg de *Gebruikershandleiding* voor het standaardgebruik van de scanner.

Deze handleiding gebruiken

Markeringen en symbolen



Let op:

Instructies die nauwkeurig moeten worden gevolgd om lichamelijk letsel te voorkomen.



Belangrijk:

Instructies die moeten worden nageleefd om schade aan de apparatuur te voorkomen.

Opmerking:

Biedt aanvullende en referentie-informatie.

Gerelateerde informatie

➔ Koppelingen naar gerelateerde gedeelten.

Beschrijvingen die in deze handleiding worden gebruikt

- Schermafbeeldingen voor de toepassingen zijn van Windows 10 of macOS High Sierra. De inhoud die wordt weergegeven op het scherm verschilt, afhankelijk van het model en de situatie.
- Afbeeldingen die in deze handleiding worden gebruikt, zijn uitsluitend bedoeld als referentie. Hoewel ze iets kunnen verschillen van het eigenlijke product, zijn de bedieningsmethoden dezelfde.

Referenties voor besturingssystemen

Windows

In deze handleiding verwijzen termen zoals "Windows 11", "Windows 10", "Windows 8.1", "Windows 8", "Windows 7", "Windows Server 2022", "Windows Server 2019", "Windows Server 2016", "Windows Server 2012 R2", "Windows Server 2012", "Windows Server 2008 R2", en "Windows Server 2008" naar de volgende besturingssystemen. Bovendien wordt "Windows" gebruikt om alle versies ervan aan te duiden.

- Microsoft® Windows® 11 besturingssysteem
- Microsoft® Windows® 10 besturingssysteem
- Microsoft® Windows® 8.1 besturingssysteem
- Microsoft® Windows® 8 besturingssysteem
- Microsoft® Windows® 7 besturingssysteem
- Microsoft® Windows Server® 2022 besturingssysteem
- Microsoft® Windows Server® 2019 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

Mac OS

In deze handleiding wordt "Mac OS" gebruikt om te verwijzen naar Mac OS X 10.9 of hoger en naar macOS 11 of hoger.

Opmerkingen over het beheerderswachtwoord

Opmerkingen over het beheerderswachtwoord.	11
Oorspronkelijk beheerderswachtwoord.	11
Bewerkingen waarvoor het beheerderswachtwoord vereist is.	11
Het beheerderswachtwoord wijzigen.	11
Het beheerderswachtwoord resetten.	12

Opmerkingen over het beheerderswachtwoord

U kunt op dit apparaat een beheerderswachtwoord instellen om te voorkomen dat onbevoegde derden, wanneer het apparaat met een netwerk verbonden is, toegang krijgen tot de apparaat- of netwerkinstellingen die op het apparaat zijn opgeslagen en deze kunnen wijzigen.

Als u een beheerderswachtwoord instelt, moet u het wachtwoord invoeren wanneer u instellingen wilt wijzigen in configuratiesoftware zoals Web Config.

Het oorspronkelijke beheerderswachtwoord is op de scanner ingesteld, maar u kunt het in een willekeurig wachtwoord wijzigen.

Oorspronkelijk beheerderswachtwoord

Het oorspronkelijke beheerderswachtwoord varieert afhankelijk van het etiket op het product. Als er een PASSWORD-etiket op de achterkant zit, voert u het achtcijferige getal in dat op het etiket staat. Als er geen "PASSWORD"-etiket op de scanner zit, voert u serienummer in als het oorspronkelijke beheerderswachtwoord. U vindt het serienummer op het etiket aan de achterkant van het product.

We raden u aan het initiële beheerderswachtwoord te wijzigen.

Opmerking:

Er is geen standaard gebruikersnaam ingesteld.

Bewerkingen waarvoor het beheerderswachtwoord vereist is

Als u tijdens de volgende bewerkingen naar het beheerderswachtwoord wordt gevraagd, voert u het beheerderswachtwoord in dat in het product is ingesteld.

- Inloggen bij de geavanceerde instellingen van Web Config
- Een menu van het bedieningspaneel gebruiken dat door de beheerder is vergrendeld
- De apparaatinstellingen wijzigen in de toepassing
- De firmware van het apparaat bijwerken
- Het beheerderswachtwoord wijzigen of resetten

Het beheerderswachtwoord wijzigen

U kunt het wijzigen via het bedieningspaneel van het product of in Web Config.

Wanneer u het wachtwoord wijzigt, moet het nieuwe wachtwoord minimaal 8 en maximaal 20 tekens lang zijn en mag het alleen alfanumerieke single-bytetekens en -symbolen bevatten.

Het beheerderswachtwoord resetten

U kunt het beheerderswachtwoord via het bedieningspaneel van het product of in Web Config terugzetten naar de oorspronkelijke instelling.

Als u het wachtwoord bent vergeten en de standaardinstellingen niet kunt resetten, moet het product worden gerepareerd. Neem contact op met de lokale leverancier.

Vereiste instellingen voor verschillende doeleinden

Vereiste instellingen voor verschillende doeleinden.	14
--	----

Vereiste instellingen voor verschillende doeleinden

Raadpleeg de volgende informatie over de benodigde instellingen voor verschillende doeleinden.

De scanner met het netwerk verbinden

Doel	Vereiste instellingen
Ik wil de scanner met het netwerk verbinden.	Configureer uw scanner voor scannen via het netwerk. "De scanner met het netwerk verbinden" op pagina 17
Ik wil de scanner met een nieuwe computer verbinden.	Configureer de netwerkinstellingen voor uw scanner op de nieuwe computer. "De computer of apparaten toevoegen of vervangen" op pagina 23

Instellingen voor scannen

Doel	Vereiste instellingen
Ik wil gescande beelden via e-mail verzenden. (Scannen naar e-mail)	1. Configureer de mailserver waarmee u verbinding wilt maken. "Een mailserver registreren" op pagina 46 2. Sla het e-mailadres van de ontvanger op in Contactpersonen (optioneel). Als u het e-mailadres opslaat, hoeft u het niet steeds opnieuw in te voeren wanneer u iets wilt verzenden. U kunt het dan in de lijst met contactpersonen selecteren. "Contactpersonen beschikbaar maken" op pagina 55
Ik wil gescande afbeeldingen opslaan in een map in het netwerk. (Scannen naar netwerkmap /FTP)	1. Maak een map in het netwerk waarin u de afbeeldingen wilt opslaan. "Een netwerkmap maken" op pagina 49 2. Sla het pad naar de map op in Contactpersonen (optioneel). Als u het mappad opslaat, hoeft u het niet steeds opnieuw in te voeren wanneer u iets wilt verzenden. U kunt het dan in de lijst met contactpersonen selecteren. "Contactpersonen beschikbaar maken" op pagina 55
Ik wil gescande afbeeldingen opslaan in een cloudservice. (Scannen naar cloud)	Installeer Epson Connect. Raadpleeg de portaalsite van Epson Connect voor meer informatie over de installatie. Tijdens de installatie hebt u een gebruikersaccount nodig voor de online opslagservice waarmee u verbinding wilt maken. https://www.epsonconnect.com/ http://www.epsonconnect.eu (alleen Europa)

Weergave van het bedieningspaneel aanpassen

Doel	Vereiste instellingen
Ik wil de items wijzigen die op het bedieningspaneel van de scanner worden weergegeven.	Stel Presets of Startscherm bewerken in. U kunt uw favoriete scaninstellingen opslaan op het bedieningspaneel en de weergegeven items bewerken. "Weergave van het bedieningspaneel aanpassen" op pagina 68

Standaard beveiligingsfuncties instellen

Doel	Vereiste instellingen
Ik wil voorkomen dat andere mensen dan de beheerder de scannerinstellingen kunnen wijzigen.	Stel een beheerderswachtwoord in voor de scanner. "Beheerdersinstellingen" op pagina 76
Ik wil het gebruik van scanners met USB-verbindingen uitschakelen.	Schakel de externe interface uit. "De externe interface uitschakelen" op pagina 84

Geavanceerde beveiligingsfuncties instellen

Doel	Vereiste instellingen
Ik wil bepalen welke protocollen moeten worden gebruikt.	Schakel de protocollen in of uit. "Beheren met protocollen" op pagina 91
Ik wil het communicatiepad versleutelen.	1. Configureer uw digitale certificaat. "Een digitaal certificaat gebruiken" op pagina 94 2. Configureer SSL/TLS-communicatie. "SSL/TLS-communicatie met de scanner" op pagina 99
Ik wil versleutelde communicatie gebruiken (IPsec). Ik wil de software alleen op een specifieke computer kunnen gebruiken (IP-filtering).	Stel beleid in voor het filteren van verkeer. "Versleutelde communicatie met IPsec/IP-filtering" op pagina 101
Ik wil een scanner in een IEEE802.1X-netwerk gebruiken.	Configureer IEEE802.1X voor de scanner. "De scanner verbinden met een IEEE802.1X-netwerk" op pagina 111

De scanner synchroniseren met een verificatiesysteem

Vraag een productcode aan via de speciale website en activeer Epson Open Platform op uw scanner.

["Epson Open Platform gebruiken" op pagina 120](#)

Een verificatieoptie gebruiken (Epson Print Admin/Epson Print Admin Serverless)

U hebt een licentiesleutel nodig om de optie te gebruiken.

Neem contact op met uw leverancier voor meer informatie.

Opmerking:

U kunt Epson Print Admin Serverless niet gebruiken wanneer het systeem is gesynchroniseerd met Epson Open Platform.

Netwerkinstellingen

De scanner met het netwerk verbinden.	17
De computer of apparaten toevoegen of vervangen.	23
De status van de netwerkverbinding controleren.	29
Netwerkspecificaties.	31
Problemen oplossen.	35

De scanner met het netwerk verbinden

In dit gedeelte wordt uitgelegd hoe u de scanner via het bedieningspaneel van de scanner met het netwerk verbindt.

Opmerking:

Als de scanner en computer zich in hetzelfde segment bevinden, kunt u ze ook verbinden met behulp van het installatieprogramma.

Ga naar de volgende website en voer de productnaam in om het installatieprogramma te openen. Ga naar **Instellen** en start de configuratie.

<https://epson.sn>

U kunt bedieningsinstructies bekijken in de Webfilmhandleidingen. Klik op de volgende URL.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Voor het maken van netwerkverbinding

Als u verbinding wilt maken met het netwerk, controleert u eerst de verbindingsmethode en instellingsinformatie.

Informatie over de verbindinginstelling verzamelen

Bereid de benodigde instellingsinformatie voor om verbinding te maken. Controleer vooraf de volgende gegevens.

Divisies	Items	Opmerking
Apparaatverbindingmethode	<input type="checkbox"/> Ethernet <input type="checkbox"/> Wifi	Kies hoe de scanner met het netwerk moet worden verbonden. Voor een bekabeld LAN wordt verbinding gemaakt via de LAN-switch. Voor wifi wordt verbinding gemaakt met het netwerk (SSID) van het toegangspunt.
Informatie over LAN-verbinding	<input type="checkbox"/> IP-adres <input type="checkbox"/> Subnetmasker <input type="checkbox"/> Standaardgateway	Kies het IP-adres dat aan de scanner moet worden toegewezen. Wanneer u een statisch IP-adres toewijst, zijn alle waarden vereist. Wanneer u een dynamisch IP-adres toewijst met de DHCP-functie, zijn deze gegevens niet vereist omdat het IP-adres automatisch wordt ingesteld.
Gegevens voor wifi-verbinding	<input type="checkbox"/> SSID <input type="checkbox"/> Wachtwoord	Dit omvat de SSID (netwerknnaam) en het wachtwoord van het toegangspunt waarmee de scanner verbinding maakt. Als MAC-adresfiltering is ingesteld, registreert u het MAC-adres van de scanner voordat u de scanner registreert. Raadpleeg het volgende voor de ondersteunde standaarden. "Netwerkspecificaties" op pagina 31
DNS-serverinformatie	<input type="checkbox"/> IP-adres voor primaire DNS <input type="checkbox"/> IP-adres voor secundaire DNS	Deze zijn vereist bij het opgeven van DNS-servers. De DNS is ingesteld wanneer het systeem een redundante configuratie heeft en er een secundaire DNS-server is. Als u zich in een kleine organisatie bevindt en de DNS-server niet instelt, stelt u het IP-adres van de router in.

Divisies	Items	Opmerking
Proxyserverinformatie	<input type="checkbox"/> Proxyservernaam	<p>Stel deze optie in wanneer de proxyserver in uw netwerkomgeving wordt gebruikt om via intranet toegang te krijgen tot internet en u de functie gebruikt waarmee de scanner rechtstreeks toegang heeft tot internet.</p> <p>Bij de volgende functies maakt de scanner rechtstreeks verbinding met internet.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Epson Connect Services <input type="checkbox"/> Cloudservices van andere bedrijven <input type="checkbox"/> Firmware-updates <input type="checkbox"/> Gescande afbeeldingen verzenden naar SharePoint (WebDAV)
Poortnummerinformatie	<input type="checkbox"/> Nummer van poort die moet worden vrijgegeven	<p>Controleer het poortnummer dat door de scanner en de computer wordt gebruikt. Geef vervolgens indien nodig de poort vrij die door een firewall wordt geblokkeerd.</p> <p>Raadpleeg het volgende voor het poortnummer dat door de scanner wordt gebruikt.</p> <p>"Poort voor de scanner gebruiken" op pagina 33</p>

IP-adrestoewijzing

De volgende soorten IP-adressen kunnen worden toegewezen.

Statisch IP-adres:

Wijs handmatig het vooraf bepaalde IP-adres toe aan de scanner (host).

De gegevens die benodigd zijn voor verbinding met het netwerk (subnetmasker, standaardgateway, DNS-server enzovoort) moeten handmatig worden ingesteld.

Het IP-adres wijzigt niet, ook niet wanneer het apparaat wordt uitgeschakeld. Dit is nuttig als u apparaten wilt beheren in een omgeving waarin het IP-adres niet kan worden gewijzigd of als u apparaten wilt beheren aan de hand van het IP-adres. Instelling wordt aanbevolen voor scanners, servers enzovoort waartoe veel computers toegang hebben. Ook als u beveiligingsfuncties gebruikt, zoals IPsec/IP-filtering, wordt aanbevolen een vast IP-adres toe te wijzen, zodat dit niet wijzigt.

Automatische toewijzing via de DHCP-functie (dynamisch IP-adres):

Wijs het IP-adres automatisch toe aan de scanner (host) met de DHCP-functie van de DHCP-server of router.

De gegevens die benodigd zijn voor verbinding met het netwerk (subnetmasker, standaardgateway, DNS-server enzovoort) wordt automatisch ingesteld, zodat u het apparaat eenvoudig kunt verbinden met het netwerk.

Als het apparaat of de router wordt uitgeschakeld, of op basis van de instellingen van de DHCP-server, kan het IP-adres wijzigen wanneer opnieuw verbinding wordt gemaakt.

Dit wordt aanbevolen wanneer apparaten niet op basis van het IP-adres worden beheerd en wanneer wordt gecommuniceerd met protocollen waarmee het IP-adres kan worden gevolgd.

Opmerking:

Wanneer u de reserveringsfunctie van de DHCP voor het IP-adres gebruikt, kunt u op elk moment hetzelfde IP-adres toewijzen aan de apparaten.

DNS-server en proxyserver

De DNS-server heeft onder andere een hostnaam en domeinnaam van het e-mailadres dat overeenkomt met de IP-adresinformatie.

Communicatie is niet mogelijk als de andere partij met bijvoorbeeld de hostnaam of domeinnaam wordt aangeduid en de computer of de scanner via IP communiceert.

Er wordt dan een aanvraag voor informatie naar de DNS-server verzonden, maar de andere partij reageert met een IP-adres. Dit proces heet naamomzetting.

Hierdoor kunnen apparaten als computers en scanners communiceren via het IP-adres.

Naamomzetting is noodzakelijk om de scanner te kunnen laten communiceren via de e-mailfunctie of de functie voor internetverbinding.

Wanneer u deze functies gebruikt, configureert u de DNS-serverinstellingen.

Wanneer u het IP-adres van de scanner toewijst met behulp van de DHCP-functie van de DHCP-server of de router, wordt dit automatisch ingesteld.

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

Wanneer u via een proxyserver verbinding maakt met internet, configureert u de proxyserver op de scanner.

Verbinding maken met het netwerk via het bedieningspaneel

Verbind de scanner met het netwerk via het bedieningspaneel van de scanner.

Het IP-adres toewijzen

Stel de basisonderdelen in, zoals hostadres, Subnetmasker en Standaardgateway.

In dit gedeelte wordt de procedure uitgelegd voor het instellen van een statisch IP-adres:

1. Schakel de scanner in.
2. Selecteer **Instel.** op het startscherm van het bedieningspaneel van de scanner.
3. Selecteer **Netwerkinstellingen > Geavanceerd > TCP/IP.**
4. Selecteer **Handmatig** voor **IP-adres ophalen.**

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 5 tot 6 ook automatisch ingesteld. Ga daarom verder naar stap 7.

5. Voer het IP-adres in.

De focus wordt verplaatst naar het voorste of laatste segment, gescheiden met een punt als u ◀ en ▶ selecteert.

Bevestig de waarde uit het voorgaande scherm.

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

Bevestig de waarde uit het voorgaande scherm.



Belangrijk:

*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.*

7. Voer het IP-adres voor de primaire DNS-server in.

Bevestig de waarde uit het voorgaande scherm.

Opmerking:

*Wanneer u **Auto** selecteert voor de instellingen voor het toewijzen 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 9.*

8. Voer het IP-adres van de secundaire DNS-server in.

Bevestig de waarde uit het voorgaande scherm.

9. Tik op **Start installatie**.

De proxyserver instellen

Stel de proxyserver in als beide punten hieronder opgaan.

- De proxyserver is bestemd voor een internetverbinding.
- Wanneer een functie wordt gebruikt waarin een scanner rechtstreeks verbinding met internet heeft, zoals de Epson Connect-service of een cloudservice van een ander bedrijf.

1. Selecteer in het startscherm **Instel..**

Wanneer u instellingen configureert nadat het IP-adres is ingesteld, wordt het scherm **Geavanceerd** weergegeven. Ga naar stap 3.

2. Selecteer **Netwerkinstellingen > Geavanceerd**.

3. Selecteer **Proxy-server**.

4. Selecteer **Gebr.** voor **Instellingen proxyserver**.

5. Voer het adres voor de proxyserver in IPv4- of FQDN-indeling in.

Bevestig de waarde uit het voorgaande scherm.


6. Voer het poortnummer voor de proxyserver in.

Bevestig de waarde uit het voorgaande scherm.

7. Tik op **Start installatie**.

Verbinding maken met ethernet

Verbind de scanner met behulp van een LAN-kabel met het netwerk en controleer de verbinding.

1. Verbind de scanner en hub (LAN-switch) met een LAN-kabel.
2. Selecteer  in het startscherm.
3. Selecteer **Router**.
4. Controleer of de instellingen bij Verbinding en IP-adres juist zijn.
5. Tik op **Sluiten**.

Verbinding maken met draadloos LAN (wifi)

U kunt de scanner op verschillende manieren met het draadloze LAN (wifi) verbinden. Kies de verbindingmethode die overeenkomt met uw omgeving en de voorwaarden die u gebruikt.

Als u beschikt over de informatie voor de draadloze router, zoals de SSID en het wachtwoord, kunt u de instellingen handmatig configureren.

Als de draadloze router WPS ondersteunt, kunt u de instellingen configureren met drukknopinstellingen.

Nadat de scanner verbinding heeft gemaakt met het netwerk, maakt u verbinding tussen de scanner en het apparaat dat u wilt gebruiken (computer, smart device, tablet, enz.)

Opmerking bij het gebruik van een 5 GHz wifi-verbinding

Dit product gebruikt normaal gesproken W52 (36ch) als kanaal wanneer verbinding wordt gemaakt met Wi-Fi Direct (eenvoudig toegangspunt). Aangezien het kanaal voor de draadloze LAN-verbinding (wifi) automatisch wordt geselecteerd, kan het gebruikte kanaal afwijken wanneer het tegelijkertijd als Wi-Fi Direct-verbinding wordt gebruikt. Als de kanalen verschillen, kan de datacommunicatie met de scanner traag zijn. Maak verbinding met de SSID op de 2,4 GHz-band als het gebruik hierdoor niet wordt gehinderd. Op de 2,4 GHz-band zullen de gebruikte kanalen overeenkomen.

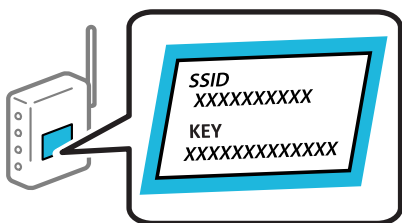
Wanneer u het draadloze LAN instelt op 5 GHz, raden wij u aan Wi-Fi Direct uit te schakelen.

Wifi-instellingen configureren door de SSID en het wachtwoord in te voeren



U kunt een wifi-netwerk instellen door op het bedieningspaneel van de scanner de gegevens in te voeren die nodig zijn voor verbinding met een draadloze router. Als u op deze wijze de instellingen wilt configureren, hebt u de SSID en het wachtwoord van de draadloze router nodig.

Opmerking:

Als u een draadloze router met de standaardinstellingen gebruikt, gebruikt u de SSID en het wachtwoord die op het label vermeld staan. Als u de SSID en het wachtwoord niet weet, neem dan contact op met degene die de draadloze router heeft ingesteld of raadpleeg de documentatie van de draadloze router.





1. Tik op het startscherm op  .

2. Selecteer **Router**.

3. Tik op **Start de instelling**.

Als de netwerkverbinding al is ingesteld, worden de verbindingdetails weergegeven. Tik op **Wijzig naar Wi-Fi-verbinding**, of **Instellingen wijzigen** om de instellingen te wijzigen.

4. Selecteer **Wizard Wi-Fi instellen**.

5. Volg de instructies op het scherm om de SSID te selecteren, voer het wachtwoord van de draadloze router in en start de configuratie.

Klik op de koppeling hieronder voor gerelateerde informatie als u na de configuratie de netwerkverbindingstatus van de scanner wilt controleren.

Opmerking:

- Als u de SSID niet kent, controleert u of de informatie op het label van de draadloze router is vermeld. Als u de draadloze router met de standaardinstellingen wilt gebruiken, gebruikt u de SSID die op het label is vermeld. Als u geen gegevens kunt vinden, raadpleegt u de documentatie die bij de draadloze router is meegeleverd.
- Het wachtwoord is hoofdlettergevoelig.
- Als u het wachtwoord niet kent, controleert u of de informatie op het label van de draadloze router is vermeld. Op het label kan het wachtwoord zijn vermeld als "Network Key" of "Wireless Password", enzovoort. Als u de draadloze router met de standaardinstellingen wilt gebruiken, gebruikt u het wachtwoord dat op het label is geschreven.
- Als u de SSID waarmee u verbinding wilt maken niet ziet, gebruik dan software of een app om wifi in te stellen via uw computer of smart device, zoals een smartphone of tablet. Voer voor meer informatie "<https://epson.sn>" in uw browser in om de website te openen, voer de naam van uw product in en ga naar **Instellen**.

Gerelateerde informatie

➔ "[De status van de netwerkverbinding controleren](#)" op pagina 29

Wifi-instellingen configureren via de drukknopinstelling (WPS)



U kunt automatisch een Wi-Fi-netwerk instellen door op een knop op de draadloze router te drukken. Als aan de volgende voorwaarden wordt voldaan, kunt u de verbinding via deze methode instellen.

- De draadloze router is compatibel met WPS (Wi-Fi Protected Setup).
- De huidige Wi-Fi-verbinding is tot stand gebracht door op een knop op de draadloze router te drukken.

Opmerking:

Als u de knop niet kunt vinden of als u de installatie uitvoert met de software, raadpleegt u de documentatie die bij de draadloze router is geleverd.



1. Tik op het startscherm op  .

2. Selecteer **Router**.

3. Tik op **Start de instelling**.

Als de netwerkverbinding al is ingesteld, worden de verbindingdetails weergegeven. Tik op **Wijzig naar Wi-Fi-verbinding**, of **Instellingen wijzigen** om de instellingen te wijzigen.

4. Selecteer **Instellen met drukknop (WPS)**.

5. Volg de instructies op het scherm.

Klik op de koppeling hieronder voor gerelateerde informatie als u na de configuratie de netwerkverbindingstatus van de scanner wilt controleren.

Opmerking:


Als de verbinding mislukt, start de draadloze router dan opnieuw, zet deze dicht bij de scanner en probeer het nog een keer.

Gerelateerde informatie

➔ [“De status van de netwerkverbinding controleren” op pagina 29](#)

Wifi-instellingen configureren via de pincode-instelling (WPS)

U kunt automatisch verbinding maken met een draadloze router door gebruik te maken van een pincode. U kunt deze methode gebruiken als uw draadloze router WPS (Wi-Fi Protected Setup) ondersteunt. Gebruik een computer om een pincode in te voeren in de draadloze router.

1. Tik op het startscherm op .

2. Selecteer **Router**.

3. Tik op **Start de instelling**.

Als de netwerkverbinding al is ingesteld, worden de verbindingdetails weergegeven. Tik op **Wijzig naar Wi-Fi-verbinding**, of **Instellingen wijzigen** om de instellingen te wijzigen.

4. Selecteer **Overige > Instellen met PIN (WPS)**

5. Volg de instructies op het scherm.

Klik op de koppeling hieronder voor gerelateerde informatie als u na de configuratie de netwerkverbindingstatus van de scanner wilt controleren.

Opmerking:

Raadpleeg de documentatie van de draadloze router voor meer informatie over het invoeren van een pincode.

Gerelateerde informatie

➔ [“De status van de netwerkverbinding controleren” op pagina 29](#)

De computer of apparaten toevoegen of vervangen

Verbinding maken met een scanner die met het netwerk is verbonden

Wanneer de scanner al is verbonden met een netwerk, kunt u een computer of een smart device via het netwerk met de scanner verbinden.

Een netwerkscanner gebruiken vanaf een tweede computer

Het wordt aanbevolen het installatieprogramma te gebruiken om de scanner te verbinden met een computer.

Ga naar de volgende website en voer de productnaam in om het installatieprogramma te openen. Ga naar **Instellen** en start de configuratie.

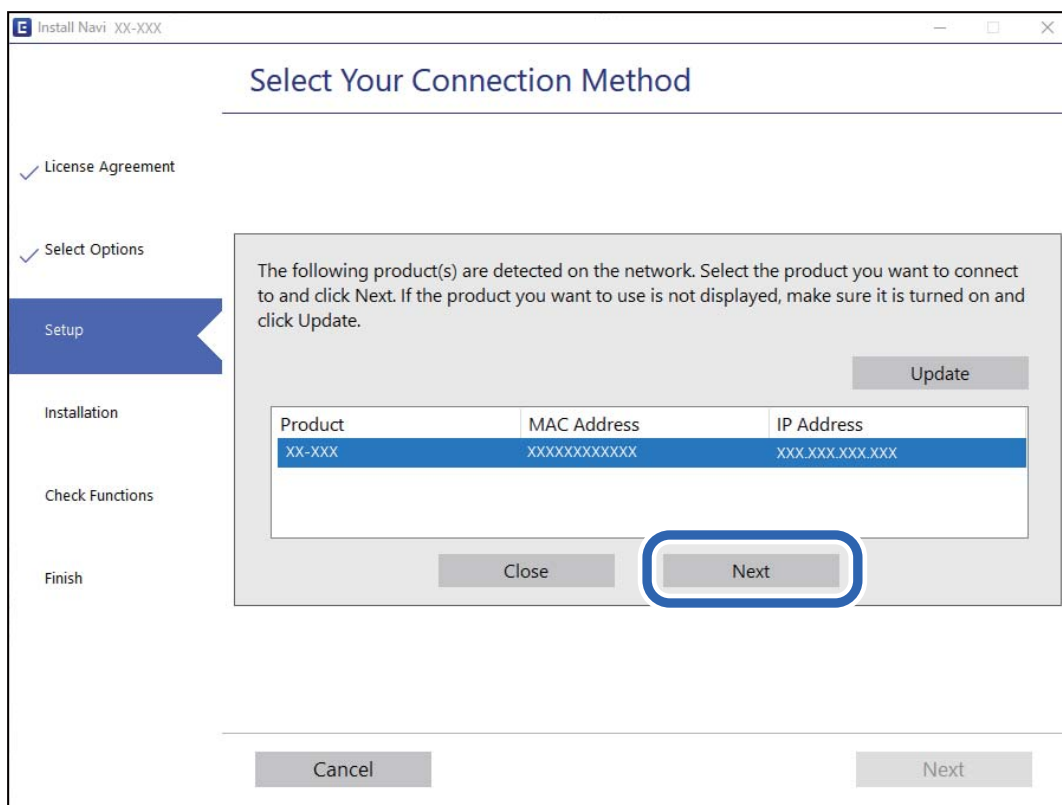
<https://epson.sn>

U kunt bedieningsinstructies bekijken in de Webfilmhandleidingen. Klik op de volgende URL.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

De scanner selecteren

Volg de instructies op het scherm totdat het volgende scherm wordt weergegeven. Selecteer de naam van de scanner waarmee u verbinding wilt maken en klik vervolgens op **Volgende**.



Volg de instructies op het scherm.

Een netwerkscanner gebruiken vanaf een smart device

U kunt een smart device op een van de volgende manieren met de scanner verbinden.

Verbinden via een draadloze router

Verbind het smart device met hetzelfde wifi-netwerk (SSID) als de scanner.

Meer details hieronder.

[“Instellingen voor verbinding met het smart device configureren” op pagina 28](#)

Verbinden via Wi-Fi Direct

Verbind het smart device rechtstreeks met de scanner zonder draadloze router.

Meer details hieronder.

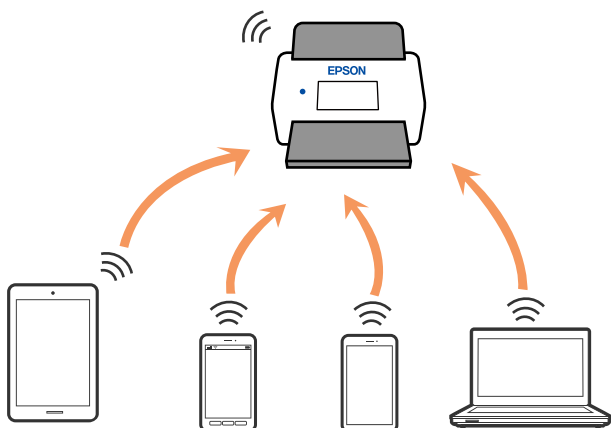
[“Een smart device rechtstreeks verbinden met een scanner \(Wi-Fi Direct\)” op pagina 25](#)

Een smart device rechtstreeks verbinden met een scanner (Wi-Fi Direct)

Met Wi-Fi Direct (eenvoudig toegangspunt) kunt u een smart device rechtstreeks zonder draadloze router op de scanner aansluiten en vanaf het smart device afdrukken.

Over Wi-Fi Direct

Gebruik deze verbindingsmethode wanneer u thuis of op kantoor geen Wi-Fi hebt of wanneer u de scanner en het smart device rechtstreeks met elkaar wilt verbinden. In deze modus fungeert de scanner als draadloze router en kunt u maximaal vier apparaten met de scanner verbinden zonder dat u een gewone draadloze router nodig hebt. Apparaten die rechtstreeks op de scanner zijn aangesloten, kunnen echter niet via de scanner met elkaar communiceren.



De scanner kan tegelijk verbinding hebben via Wi-Fi of ethernet en Wi-Fi Direct (eenvoudig toegangspunt). Als u echter een netwerkverbinding maakt via Wi-Fi Direct (eenvoudig toegangspunt) en de scanner via Wi-Fi is verbonden, wordt de Wi-Fi-verbinding tijdelijk verbroken.

Verbinding maken met een smart device via Wi-Fi Direct

Met deze methode kunt u de scanner zonder draadloze router rechtstreeks met smart devices verbinden.

1. Selecteer in het startschermd .
2. Selecteer **Wi-Fi Direct**.
3. Selecteer **Start de instelling**.
4. Start Epson Smart Panel op uw smart device.

5. Volg de instructies die worden weergegeven in Epson Smart Panel om verbinding te maken met de scanner. Ga naar de volgende stap wanneer het smart device met de scanner is verbonden.
6. Selecteer **Volledig** op het bedieningspaneel van de scanner.

De verbinding met Wi-Fi Direct (eenvoudig toegangspunt) verbreken

Er zijn twee methoden beschikbaar om een Wi-Fi Direct-verbinding (eenvoudig toegangspunt) uit te schakelen. U kunt alle verbindingen uitschakelen via het bedieningspaneel van de scanner of u schakelt alle verbindingen uit via de computer of het smart device.

Wanneer u alle verbindingen wilt uitschakelen, selecteert u  > **Wi-Fi Direct** > **Start de instelling** > **Wijzigen** > **Wi-Fi Direct uitschakelen**.

Belangrijk:

Wanneer de Wi-Fi Direct-verbinding (eenvoudig toegangspunt) wordt uitgeschakeld, wordt de verbinding voor alle computers en smart devices die via een Wi-Fi Direct-verbinding (eenvoudig toegangspunt) met de scanner zijn verbonden verbroken.

Opmerking:

Als u de verbinding met een specifiek apparaat wilt verbreken, doe dit dan op het apparaat in kwestie en niet op de scanner. Gebruik een van de volgende methodes om de Wi-Fi Direct-verbinding (eenvoudig toegangspunt) te verbreken met het apparaat.

- Verbreek de wifi-verbinding met de netwerknaam (SSID) van de scanner.
- Maak verbinding met een andere netwerknaam (SSID).

De instellingen voor Wi-Fi Direct (eenvoudig toegangspunt) wijzigen, zoals de SSID

Wanneer een Wi-Fi Direct-verbinding (eenvoudig toegangspunt) is ingeschakeld, kunt u de instellingen wijzigen in



> **Wi-Fi Direct** > **Start de instelling** > **Wijzigen** en worden de volgende menuopties weergegeven.

Netwerknaam wijzigen

Wijzig de netwerknaam (SSID) voor Wi-Fi Direct (eenvoudig toegangspunt) voor het maken van een verbinding met de scanner in een naam naar keuze. U kunt de netwerknaam (SSID) instellen in ASCII-teken die zijn weergegeven op het softwaretoetsenbord van het bedieningspaneel. U kunt maximaal 22 tekens invoeren.

Wanneer u de netwerknaam (SSID) wijzigt, wordt de verbinding met alle verbonden apparaten verbroken. Gebruik de nieuwe netwerknaam (SSID) als u opnieuw verbinding wilt maken met het apparaat.

Wachtwoord wijzigen

Wijzig het wachtwoord voor Wi-Fi Direct (eenvoudig toegangspunt) voor het maken van verbinding met de scanner in een waarde naar keuze. U kunt het wachtwoord instellen in ASCII-teken die zijn weergegeven op het softwaretoetsenbord van het bedieningspaneel. U kunt 8 tot 22 tekens invoeren.

Wanneer u het wachtwoord wijzigt, wordt de verbinding met alle verbonden apparaten verbroken. Gebruik het nieuwe wachtwoord als u opnieuw verbinding wilt maken met het apparaat.

Frequentiebereik wijzigen

Wijzig het frequentiebereik van Wi-Fi Direct dat wordt gebruikt voor het maken van een verbinding met de scanner. U kunt kiezen tussen 2,4 GHz of 5 GHz.

Wanneer u het frequentiebereik wijzigt, wordt de verbinding met alle verbonden apparaten verbroken. Maak opnieuw verbinding met het apparaat.

Als u het frequentiebereik wijzigt naar 5 GHz, kunt u niet opnieuw verbinding maken met apparaten die geen ondersteuning bieden voor 5 GHz.

Deze instelling wordt mogelijk niet in alle regio's weergegeven.

Wi-Fi Direct uitschakelen

Schakel de instellingen voor Wi-Fi Direct (eenvoudig toegangspunt) van de scanner uit. Wanneer u deze optie uitschakelt, wordt de verbinding van alle apparaten die via Wi-Fi Direct (eenvoudig toegangspunt) met de scanner zijn verbonden verbroken.

Standaardinst. herstellen

Herstel alle instellingen voor Wi-Fi Direct (eenvoudig toegangspunt) naar de standaardwaarden.

De op de scanner opgeslagen verbindingsgegevens voor Wi-Fi Direct (eenvoudig toegangspunt) van het smart device worden verwijderd.

Opmerking:

*U kunt de volgende instellingen ook configureren via het tabblad **Netwerk** > **Wi-Fi Direct** in Web Config.*

- Wi-Fi Direct (eenvoudig toegangspunt) in- of uitschakelen*
- De netwerknaam (SSID) wijzigen*
- Wachtwoord wijzigen*
- Het frequentiebereik wijzigen*
Deze instelling wordt mogelijk niet in alle regio's weergegeven.
- De instellingen voor Wi-Fi Direct (eenvoudig toegangspunt) herstellen*

De netwerkverbinding opnieuw instellen

In dit gedeelte wordt uitgelegd hoe u de instellingen voor de netwerkverbinding kunt configureren en de verbindingmethode kunt wijzigen bij vervanging van de draadloze router of de computer.

Vervanging van de draadloze router

Wanneer u de draadloze router vervangt, moet u de verbinding tussen de computer of het smart device en de scanner instellen.

U moet deze instellingen configureren als u bijvoorbeeld van internetprovider verandert.

Instellingen voor verbinding met de computer configureren

Het wordt aanbevolen het installatieprogramma te gebruiken om de scanner te verbinden met een computer.

Ga naar de volgende website en voer de productnaam in om het installatieprogramma te openen. Ga naar **Instellen** en start de configuratie.

<https://epson.sn>

U kunt bedieningsinstructies bekijken in de Webfilmhandleidingen. Klik op de volgende URL.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Een verbindingmethode selecteren

Volg de instructies op het scherm. Selecteer in het scherm **Selecteer de installatie-optie** de optie **Breng de verbinding van Printer opnieuw tot stand (voor nieuwe netwerkrouter of om USB te wijzigen naar netwerk, enz.)** en klik vervolgens op **Volgende**.

Volg de afdrukinstructies op het scherm om de configuratie te voltooien.

Als u geen verbinding kunt maken, lees dan het volgende om het probleem op te lossen.

[“Kan geen verbinding maken met een netwerk” op pagina 35](#)

Instellingen voor verbinding met het smart device configureren

U kunt de scanner gebruiken vanaf een smart device wanneer u de scanner verbindt met hetzelfde wifi-netwerk (SSID) als het smart device. Open de volgende website en voer de productnaam in om de scanner vanaf een smart device te gebruiken. Ga naar **Instellen** en start de configuratie.

<https://epson.sn>

Open de website vanaf een smart device waarmee u verbinding wilt maken met de scanner.

Vervanging van de computer

Wanneer u de computer vervangt, moet u de verbinding tussen de computer en de scanner instellen.

Instellingen voor verbinding met de computer configureren

Het wordt aanbevolen het installatieprogramma te gebruiken om de scanner te verbinden met een computer.

Ga naar de volgende website en voer de productnaam in om het installatieprogramma te openen. Ga naar **Instellen** en start de configuratie.

<https://epson.sn>

U kunt bedieningsinstructies bekijken in de Webfilmhandleidingen. Klik op de volgende URL.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Volg de instructies op het scherm.

De methode voor verbinding met de computer wijzigen

In dit gedeelte wordt uitgelegd hoe u de verbindingmethode kunt wijzigen wanneer de computer en de scanner zijn verbonden.

De netwerkverbinding wijzigen van ethernet in wifi

Wijzig de ethernetverbinding via het bedieningspaneel van de scanner in een wifi-verbinding. De methode voor wijziging van de verbinding is in feite dezelfde als die voor het instellen van een wifi-verbinding.

Gerelateerde informatie

➔ “Verbinding maken met draadloos LAN (wifi)” op pagina 21

De netwerkverbinding wijzigen van wifi in ethernet

Volg onderstaande stappen om de wifi-verbinding te wijzigen in een ethernetverbinding.

1. Selecteer in het startscherm **Instel.**
2. Selecteer **Netwerkinstellingen > Bekabelde LAN-installatie.**
3. Volg de instructies op het scherm.

Een USB-verbinding wijzigen in een netwerkverbinding

Gebruik het installatieprogramma en kies een andere verbindingsmethode.

Ga naar de volgende website en voer de productnaam in. Ga naar **Instellen** en start de configuratie.

<https://epson.sn>

De verbindingsmethode wijzigen selecteren

Volg de instructies in elk venster. Selecteer in het scherm **Selecteer de installatie-optie** de optie **Breng de verbinding van Printer opnieuw tot stand (voor nieuwe netwerkrouter of om USB te wijzigen naar netwerk, enz.)** en klik vervolgens op **Volgende.**

Selecteer de netwerkverbinding die u wilt gebruiken (**Verbinden via draadloos netwerk (Wi-Fi)** of **Verbinden via vaste LAN-verbinding (ethernet)**) en klik op **Volgende.**

Volg de afdrukinstructies op het scherm om de configuratie te voltooien.

De status van de netwerkverbinding controleren

U kunt de netwerkstatus als volgt controleren.

De netwerkverbindingstatus controleren op het bedieningspaneel

U kunt de status van de netwerkverbinding controleren aan de hand van het netwerkpictogram of de netwerkinformatie op het bedieningspaneel van de scanner.

De netwerkverbindingstatus controleren met het netwerkpictogram

U kunt de status van de netwerkverbinding en kracht van het radiosignaal controleren aan de hand van het netwerkpictogram op het startscherm van de scanner.



	<p>Hiermee geeft u de status van de netwerkverbinding weer.</p> <p>Selecteer het pictogram om de instellingen te controleren en te wijzigen. Dit is de snelkoppeling naar het volgende menu.</p> <p>Instel. > Netwerkinstellingen > Wi-Fi instellen</p>
	<p>De scanner is niet verbonden met een draadloos (wifi-)netwerk.</p>
	<p>De scanner zoekt naar een SSID, het IP-adres is niet ingesteld of er is een probleem met het draadloze (wifi-)netwerk.</p>
	<p>De scanner is verbonden met een draadloos (wifi-)netwerk.</p> <p>Het aantal balkjes geeft de sterkte van de verbinding weer. Hoe meer balkjes, des te sterker de verbinding is.</p>
	<p>De scanner is niet verbonden met een draadloos (wifi-)netwerk in de modus Wi-Fi Direct (eenvoudig toegangspunt).</p>
	<p>De scanner is verbonden met een draadloos (wifi-)netwerk in de modus Wi-Fi Direct (eenvoudig toegangspunt).</p>
	<p>De scanner is niet verbonden met een bekabeld (ethernet)netwerk of de verbinding is verbroken.</p>
	<p>De scanner is verbonden met een bekabeld (ethernet)netwerk.</p>

De gedetailleerde netwerkinformatie weergeven op het bedieningspaneel

Wanneer uw scanner verbinding heeft met het netwerk, kunt u ook andere netwerkgerelateerde informatie bekijken door de netwerkmenu's te selecteren die u wilt controleren.

1. Selecteer in het startscherm **Instel.**
2. Selecteer **Netwerkinstellingen > Netwerkstatus.**
3. Als u deze informatie wilt controleren, selecteert u de menu's die u wilt nakijken.

Status vast netwerk/Wi-Fi

Hiermee geeft u de netwerkinformatie weer (apparaatnaam, verbinding, signaalsterkte, enz.) voor ethernet- of wifi-verbindingen.

Wi-Fi Direct-status

Geeft weer of Wi-Fi Direct is in- of uitgeschakeld, en de SSID, het wachtwoord enzovoort voor Wi-Fi Direct-verbindingen.

Status e-mailserver

Geeft de netwerkinformatie voor de e-mailserver weer.

Netwerkspecificaties

Wifi-specificaties

Raadpleeg de volgende tabel voor de wifi-specificaties.

Andere landen of regio's dan onderstaande	Tabel A
Ierland, Verenigd Koninkrijk, Oostenrijk, Duitsland, Liechtenstein, Zwitserland, Frankrijk, België, Luxemburg, Nederland, Italië, Portugal, Spanje, Denemarken, Finland, Noorwegen, Zweden, IJsland, Kroatië, Cyprus, Griekenland, Noord-Macedonië, Servië, Slovenië, Malta, Bosnië en Herzegovina, Kosovo, Montenegro, Albanië, Bulgarije, Tsjechië, Estland, Hongarije, Letland, Litouwen, Polen, Roemenië, Slowakije, Israël, Australië, Nieuw-Zeeland, Taiwan	Tabel B
Turkije	DS-900WN: Serienummers die beginnen met XDA8: Tabel A Serienummers die beginnen met XDA7: Tabel B
	DS-800WN: Serienummers die beginnen met XDA2: Tabel A Serienummers die beginnen met XD9Z: Tabel B

Tabel A

Normen	IEEE 802.11b/g/n*1
Frequentiebereik	2400-2483,5 MHz
Maximaal uitgezonden radiofrequentievermogen	20 dBm (EIRP)
Kanalen	1/2/3/4/5/6/7/8/9/10/11/12/13
Verbindingsmodi	Infrastructuur, Wi-Fi Direct (eenvoudig toegangspunt)*2*3
Beveiligingsprotocollen*4	WEP (64/128bit), WPA2-PSK (AES)*5, WPA3-SAE (AES), WPA2/WPA3-Enterprise

*1 Alleen beschikbaar voor de HT20.

*2 Niet ondersteund voor IEEE 802.11b.

*3 Infrastructuur en modi voor Wi-Fi Direct of een ethernetverbinding kunnen tegelijkertijd worden gebruikt.

*4 Wi-Fi Direct ondersteunt alleen WPA2-PSK (AES).

*5 Voldoet aan WPA2-standaarden met ondersteuning voor WPA/WPA2 Personal.

Tabel B

Normen	IEEE 802.11a/b/g/n*1/ac		
Frequentiebereiken	IEEE 802.11b/g/n: 2,4 GHz, IEEE 802.11a/n/ac: 5 GHz		
Kanalen	Wifi	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12*2/13*2
		5 GHz*3	W52 (36/40/44/48), W53 (52/56/60/64), W56 (100/104/108/112/116/120/124/128/132/136/140/144), W58 (149/153/157/161/165)
	Wi-Fi Direct	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12*2/13*2
		5 GHz*3	W52 (36/40/44/48) W58 (149/153/157/161/165)
Verbindingsmodi	Infrastructuur, Wi-Fi Direct (eenvoudig toegangspunt)*4, *5		
Beveiligingsprotocollen*6	WEP (64/128bit), WPA2-PSK (AES)*7, WPA3-SAE (AES), WPA2/WPA3-Enterprise		

*1 Alleen beschikbaar voor de HT20.

*2 Niet beschikbaar in Taiwan.

*3 De beschikbaarheid van deze kanalen en gebruik van het product buitenshuis via deze kanalen verschilt per locatie. Ga voor meer informatie naar <http://support.epson.net/wifi5ghz/>

*4 Niet ondersteund voor IEEE 802.11b.

*5 Infrastructuur en modi voor Wi-Fi Direct of een ethernetverbinding kunnen tegelijkertijd worden gebruikt.

*6 Wi-Fi Direct ondersteunt alleen WPA2-PSK (AES).

*7 Voldoet aan WPA2-standaarden met ondersteuning voor WPA/WPA2 Personal.

Ethernet-specificaties

Normen	IEEE802.3i (10BASE-T)*1 IEEE802.3u (100BASE-TX)*1 IEEE802.3ab (1000BASE-T)*1 IEEE802.3az (Energy Efficient Ethernet)*2
Communicatiemodus	Automatisch, 10 Mbps volledig duplex, 10 Mbps half-duplex, 100 Mbps volledig duplex, 100 Mbps half-duplex
Connector	RJ-45

*1 Gebruik een STP-kabel (Shielded twisted pair) van categorie 5e of hoger om het risico op radio-interferentie te voorkomen.

*2 Het verbonden apparaat moet voldoen aan IEEE802.3az-standaarden.

Netwerkfuncties en ondersteuning voor IPv4/IPv6

Functies	Ondersteund
Epson Scan 2	IPv4, IPv6
Document Capture Pro/Document Capture	IPv4

Beveiligingsprotocol

IEEE802.1X*	
IPsec/IP-filtering	
SSL/TLS	HTTPS Server/Client
SMTPS (STARTTLS, SSL/TLS)	
SNMPv3	

* U moet verbindingssysteem gebruiken dat voldoet aan IEEE802.1X.

Poort voor de scanner gebruiken

De scanner gebruikt de volgende poort. Deze poorten moeten naar behoefte beschikbaar worden gesteld door de netwerkbeheerder.

Wanneer de scanner de afzender (client) is

Gebruiken	Bestemming (server)	Protocol	Poortnummer	
Bestandsverzending (wanneer vanaf de scanner scannen naar netwerkmap wordt gebruikt)	FTP/FTPS-server	FTP/FTPS (TCP)	20	
			21	
	Bestandsserver	SMB (TCP)	445	
			NetBIOS (UDP)	137
				138
	WebDAV-server	Protocol HTTP (TCP)	80	
Protocol HTTPS(TCP)			443	
Verzending via e-mail (wanneer vanaf de scanner scannen naar e-mail wordt gebruikt)	SMTP-server	SMTP (TCP)	25	
		SMTP SSL/TLS (TCP)	465	
		SMTP STARTTLS (TCP)	587	

Gebruiken	Bestemming (server)	Protocol	Poortnummer
POP voor SMTP-verbinding (wanneer vanaf de scanner scannen naar e-mail wordt gebruikt)	POP-server	POP3 (TCP)	110
Wanneer Epson Connect wordt gebruikt	Epson Connect-server	HTTPS	443
		XMPP	5222
Gebruikersgegevens verzamelen (de contactpersonen uit de scanner gebruiken)	LDAP-server	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
Gebruikersverificatie tijdens het verzamelen van gebruikersgegevens (wanneer de contactpersonen uit de scanner worden gebruikt) Gebruikersverificatie wanneer vanaf de scanner scannen naar netwerkmap (SMB) wordt gebruikt	KDC-server	Kerberos	88
WSD beheren	Clientcomputer	WSD (TCP)	5357
De computer zoeken wanneer push-scan vanuit een toepassing wordt uitgevoerd	Clientcomputer	Netwerkdetectie voor push-scan	2968

Wanneer de afzender (client) de clientcomputer is

Gebruiken	Bestemming (server)	Protocol	Poortnummer
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 vanuit een toepassing doorsturen	Scanner	Scannen in netwerk (TCP)	1865
De taakinformatie verzamelen wanneer push-scan vanuit een toepassing wordt uitgevoerd toepassing	Scanner	Push-scan in het netwerk	2968
Web Config	Scanner	HTTP (TCP)	80
		HTTPS (TCP)	443

Problemen oplossen

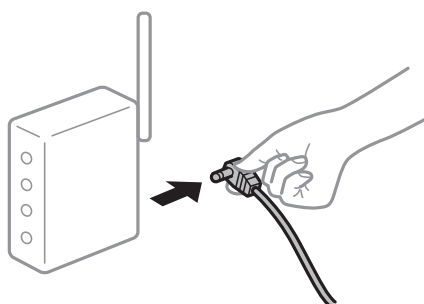
Kan geen verbinding maken met een netwerk

Een van de volgende problemen kan de oorzaak zijn.

■ Er is iets mis met de netwerkapparaten voor de wifi-verbinding.

Oplossingen

Schakel de apparaten die u met het netwerk wilt verbinden uit. Wacht circa 10 seconden en schakel de apparaten in de volgende volgorde weer in: de draadloze router, de computer of het smart device en tenslotte de scanner. Verklein de afstand tussen de scanner en de computer of het smart device enerzijds en de draadloze router anderzijds om de radiocommunicatie te vereenvoudigen, en probeer vervolgens opnieuw de netwerkinstellingen te configureren.



■ Apparaten kunnen geen signaal ontvangen van de draadloze router, omdat ze te ver uit elkaar staan.

Oplossingen

Zet de computer of het smart device en de scanner dichterbij de draadloze router. Schakel de draadloze router vervolgens uit en weer in.

■ Wanneer u de draadloze router vervangt, komen de instellingen niet overeen met de nieuwe router.

Oplossingen

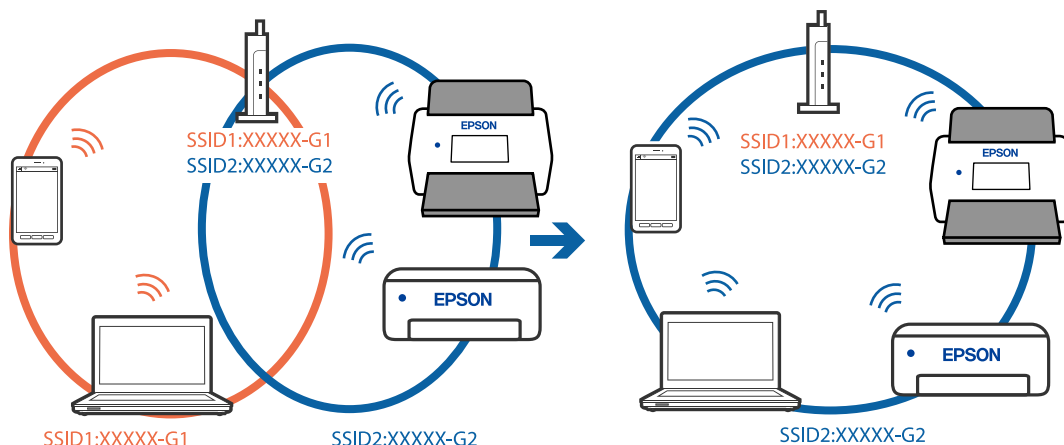
Configureer de verbindinginstellingen opnieuw, zodat deze overeenkomen met de nieuwe draadloze router.

■ De SSID's voor verbinding met de computer of het smart device en de computer verschillen.

Oplossingen

Wanneer u meerdere draadloze routers tegelijk gebruikt of de draadloze router meerdere SSID's heeft en apparaten met verschillende SSID's zijn verbonden, kunt u geen verbinding maken met de draadloze router.

Verbind de computer of het smart device met hetzelfde SSID als de scanner.



Privacyscheiding is beschikbaar voor de draadloze router.

Oplossingen

De meeste draadloze routers hebben een functie voor privacyscheiding waarmee communicatie tussen verbonden apparaten wordt geblokkeerd. Als er geen communicatie mogelijk is tussen de scanner en de computer of het smart device, terwijl deze zijn verbonden met hetzelfde netwerk, schakelt u de privacyscheiding op de draadloze router uit. Zie voor meer informatie de bij de draadloze router geleverde handleiding.

Het IP-adres is niet juist toegewezen.

Oplossingen

Als het aan de scanner toegewezen IP-adres 169.254.XXX.XXX is, en het subnetmasker 255.255.0.0 is, is het IP-adres mogelijk niet correct toegewezen.

Selecteer op het bedieningspaneel van de scanner **Instel.** > **Netwerkinstellingen** > **Geavanceerd** > **TCP/IP-instelling** en controleer vervolgens het IP-adres en het subnetmasker die aan de scanner zijn toegewezen.

Start de draadloze router opnieuw of stel de netwerkinstellingen van de scanner opnieuw in.

Er is een probleem opgetreden met de netwerkinstellingen op de computer.

Oplossingen

Probeer op de computer een internetpagina te openen om te controleren of de netwerkinstellingen van de computer correct zijn. Als u geen internetpagina's kunt openen, is er een probleem met de computer.

Controleer de netwerkverbinding van de computer. Raadpleeg de documentatie van de computer voor meer informatie.

De scanner is met ethernet verbonden via apparaten die IEEE 802.3az (Energie-efficiënt Ethernet) ondersteunen.

Oplossingen

Wanneer u de scanner met ethernet verbindt via apparaten die IEEE 802.3az (Energie-efficiënt Ethernet) ondersteunen, kunnen de volgende problemen optreden, afhankelijk van de hub of router die u gebruikt.

- De verbinding wordt instabiel, de scanner is verbonden en vervolgens wordt de verbinding steeds opnieuw verbroken.

- Kan geen verbinding maken met de scanner.
- De communicatiesnelheid wordt traag.

Volg de onderstaande stappen om IEEE 802.3az uit te schakelen voor de scanner en maak verbinding.

1. Verwijder de ethernetkabel die is aangesloten op de computer en de scanner.
 2. Wanneer IEEE 802.3az voor de computer is ingeschakeld, schakelt u dit uit.
Raadpleeg de documentatie van de computer voor meer informatie.
 3. Sluit de computer en de scanner met een ethernetkabel op elkaar aan.
 4. Controleer op de scanner de netwerkinstellingen.
Selecteer **Instel.** > **Netwerkinstellingen** > **Netwerkstatus** > **Status vast netwerk/Wi-Fi**.
 5. Controleer het IP-adres van de scanner.
 6. Ga op de computer naar Web Config.
Open een webbrowser en voer vervolgens het IP-adres van de scanner in.
[“Web Config uitvoeren in een webbrowser” op pagina 39](#)
 7. Selecteer het tabblad **Netwerk** > **Vast netwerk**.
 8. Selecteer **Uit** bij **IEEE 802.3az**.
 9. Klik op **Volgende**.
 10. Klik op **OK**.
 11. Verwijder de ethernetkabel die is aangesloten op de computer en de scanner.
 12. Als u bij stap 2 IEEE 802.3az hebt uitgeschakeld voor de computer, schakelt u dit weer in.
 13. Sluit de ethernetkabels die u hebt verwijderd bij stap 1 aan op de computer en de scanner.
- Als het probleem nog steeds optreedt, zijn het mogelijk andere apparaten dan de scanner die het probleem veroorzaken.

De scanner is uitgeschakeld.

Oplossingen

Controleer of de scanner is ingeschakeld.

Wacht tot het statuslampje dat aangeeft dat de scanner klaar is om te scannen, stopt met knipperen.

Software voor configuratie van de scanner

Toepassing voor het configureren van scannerbewerkingen (Web Config)	39
Epson Device Admin.	40

Toepassing voor het configureren van scannerbewerkingen (Web Config)

Web Config is een toepassing die draait in webbrowsers, zoals Microsoft Edge of Safari, op een computer of smart device. U kunt de scannerstatus controleren of de netwerkservice en de scannerinstellingen wijzigen. Verbind de scanner en de computer of het apparaat met hetzelfde netwerk om Web Config te gebruiken.

De volgende browsers worden ondersteund. Gebruik de nieuwste versie.

Microsoft Edge, Windows Internet Explorer, Firefox, Chrome en Safari

Opmerking:

Tijdens het gebruik van dit apparaat wordt u mogelijk gevraagd het beheerderswachtwoord in te voeren. Raadpleeg de volgende informatie over het beheerderswachtwoord.

[“Opmerkingen over het beheerderswachtwoord” op pagina 11](#)

Gerelateerde informatie

➔ [“Geen toegang tot Web Config” op pagina 66](#)

Web Config uitvoeren in een webbrowser

De scanner wordt geleverd met ingebouwde software genaamd Web Config (een webpagina waar u instellingen kunt configureren). Voor toegang tot Web Config voert u in uw browser gewoon het IP-adres in van een scanner die met het netwerk is verbonden.

1. Controleer het IP-adres van de scanner.

Selecteer **Instel.** > **Netwerkinstellingen** > **Netwerkstatus** op het bedieningspaneel van de scanner. Selecteer vervolgens de actieve verbindingmethode (**Status vast netwerk/Wi-Fi** of **Wi-Fi Direct-status**) om het IP-adres van de scanner te bevestigen.

Voorbeeld van IP-adres: 192.168.100.201

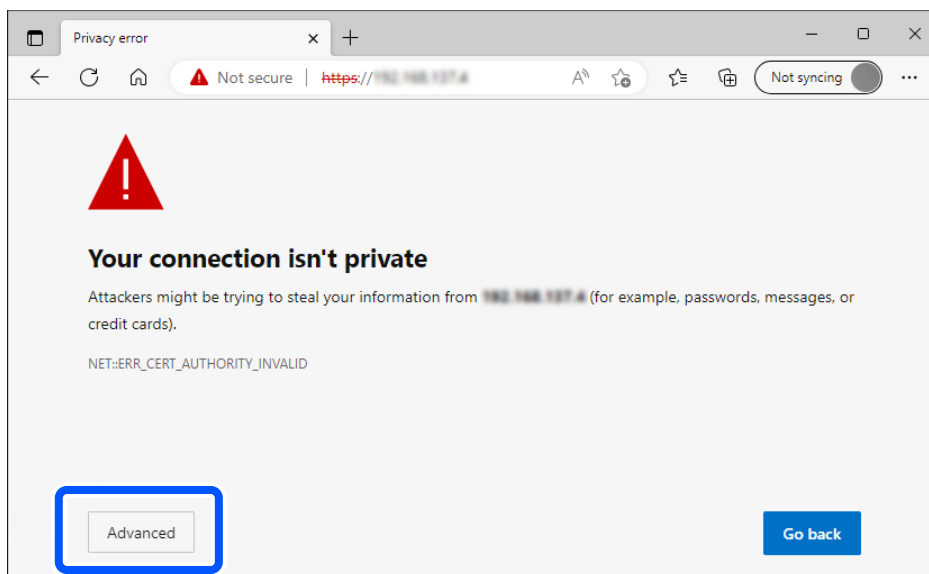
2. Open een browser op een computer of smart device en voer vervolgens in de adresbalk het IP-adres van de scanner in.

Opmaak: http://IP-adres van de scanner/

Voorbeeld: http://192.168.100.201/

Als in uw browser een waarschuwingsscherm verschijnt, kunt u de waarschuwing gerust negeren en de webpagina openen (Web Config). Aangezien de scanner een zelfondertekend certificaat gebruikt bij toegang tot HTTPS, wordt in de browser een waarschuwing weergegeven wanneer u Web Config start. Deze waarschuwing wijst niet op een probleem en kan worden genegeerd. Afhankelijk van uw browser moet u wellicht op **Geavanceerde instellingen** klikken om de webpagina te bekijken.

Voorbeeld: voor Microsoft Edge



Opmerking:

Als er geen waarschuwingsscherm verschijnt, gaat u naar de volgende stap.

Gebruik voor IPv6-adressen de volgende opmaak.

Opmaak: `http://[IP-adres van de scanner]/`

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

3. Als u de scannerinstellingen wilt wijzigen, moet u inloggen als Web Config-beheerder.

Klik op **aanmelden** rechtsboven in het scherm. Voer **Gebruikersnaam** en **Huidig wachtwoord** in en klik op **OK**.

Hieronder staan de beginwaarden voor de beheerdersgegevens van Web Config.

· Gebruikersnaam: geen (leeg)

· Wachtwoord: afhankelijk van het etiket op het product.

Als er een PASSWORD-etiket op de achterkant zit, voert u het achtcijferige getal in dat op het etiket staat. Als er geen "PASSWORD"-etiket op de scanner zit, voert u serienummer in als het oorspronkelijke beheerderswachtwoord. U vindt het serienummer op het etiket aan de achterkant van het product.

Opmerking:

Als rechtsboven in het scherm **afmelden** wordt weergegeven, bent u al ingelogd als beheerder.

U wordt automatisch uitgelogd nadat er ongeveer 20 minuten geen activiteit is geweest.

Epson Device Admin

Epson Device Admin is een multifunctionele toepassing waarmee u apparaten in een netwerk kunt beheren.

U kunt configuratiesjablonen gebruiken om dezelfde instellingen toe te passen op meerdere scanners in een netwerk, waardoor u meerdere scanners kunt installeren en beheren.

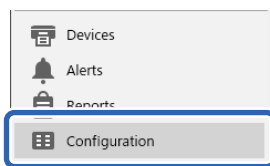
U kunt Epson Device Admin downloaden van de ondersteuningswebsite van Epson. Raadpleeg de documentatie of Help van Epson Device Admin voor meer informatie over het gebruik van deze toepassing.

Configuratiesjabloon

De configuratiesjabloon maken

Maak de nieuwe configuratiesjabloon.

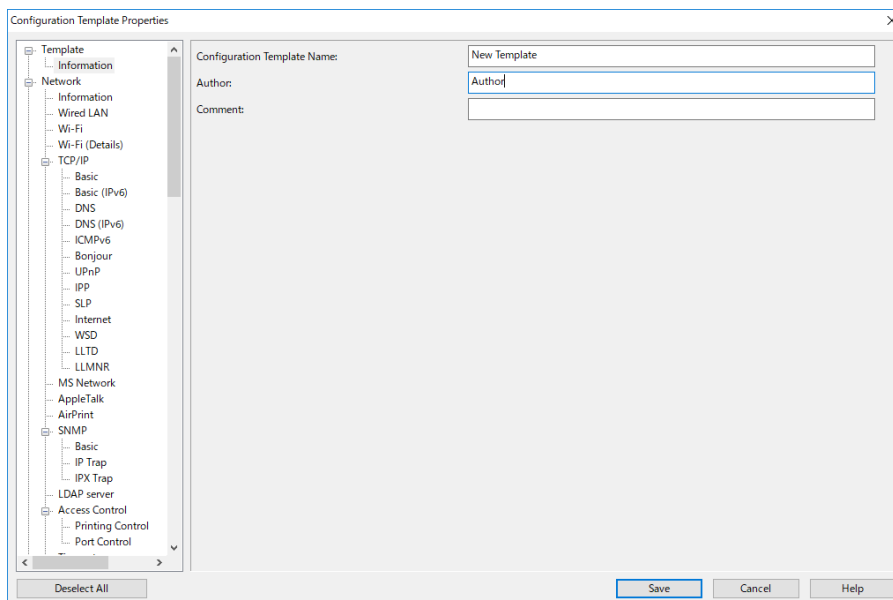
1. Start Epson Device Admin.
2. Selecteer **Configuratie** in het taakmenu in de zijmarge.



3. Selecteer op het lintmenu de optie **Nieuw**.



4. Stel elk item in.



Item	Uitleg
Naam configuratiesjabloon	Naam van de configuratiesjabloon. Voer maximaal 1024 tekens in Unicode (UTF-8) in.
Auteur	Informatie over de maker van de sjabloon. Voer maximaal 1024 tekens in Unicode (UTF-8) in.

Item	Uitleg
Opmerking	Voer arbitraire gegevens in. Voer maximaal 1024 tekens in Unicode (UTF-8) in.

- Selecteer aan de linkerzijde de items die u wilt instellen.

Opmerking:

Klik op de menuoptie aan de linkerzijde om naar de betreffende schermen te schakelen. De ingestelde waarde wordt behouden als u naar een ander scherm schakelt, maar niet als u het scherm annuleert. Als u alle instellingen hebt geconfigureerd, klikt u op **Opslaan**.

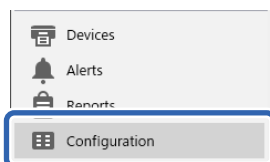
De configuratiesjabloon toepassen

Pas de opgeslagen configuratiesjabloon toe op de scanner. De in de sjabloon geselecteerde items worden toegepast. Als de doelscanner niet over de juiste functie beschikt, wordt de sjabloon niet toegepast.

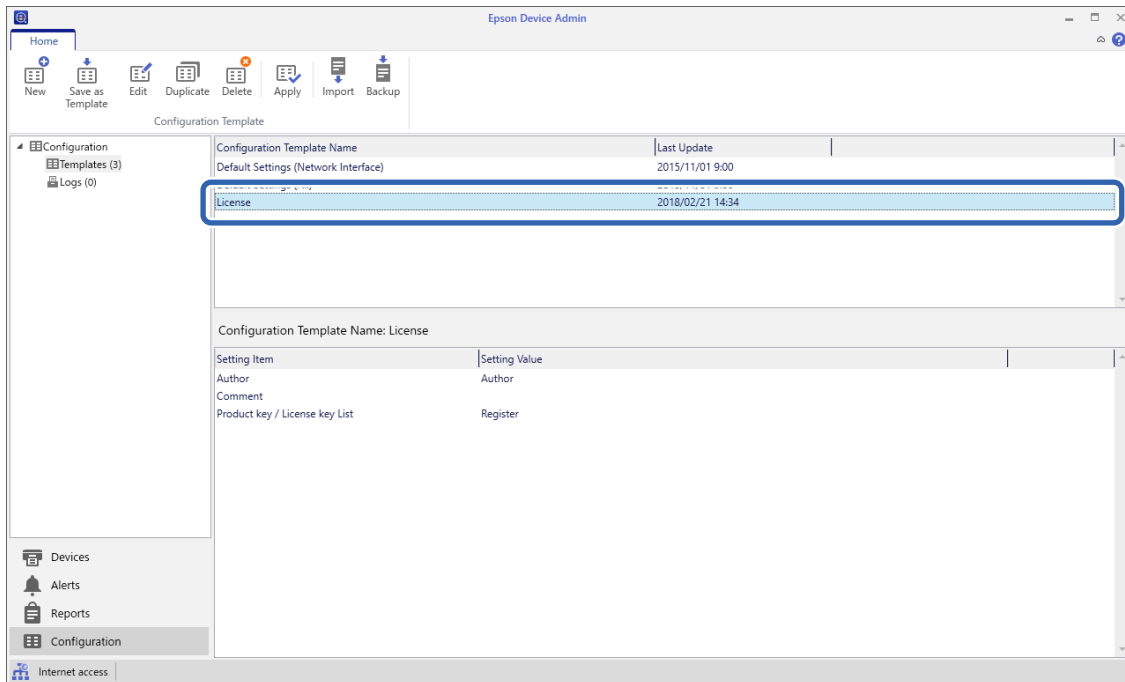
Opmerking:

Wanneer een beheerderswachtwoord is ingesteld op de scanner, configureert u eerst het wachtwoord.

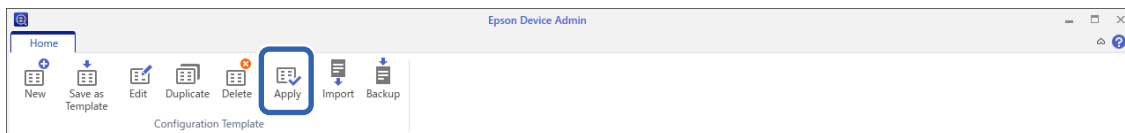
- Selecteer in het lintmenu in het scherm "Apparatenlijst" **Opties > Wachtwoordbeheer**.
 - Selecteer **Automatisch wachtwoordbeheer inschakelen** en klik vervolgens op **Wachtwoordbeheer**.
 - Selecteer de juiste scanner en klik vervolgens op **Bewerken**.
 - Stel het wachtwoord in en klik op **OK**.
- Selecteer **Configuratie** in het taakmenu in de zijmarge.



2. Selecteer de configuratiesjabloon die u wilt toepassingen in **Naam configuratiesjabloon**.



3. Klik op het lintmenu op **Toepassen**.
Het apparaatselectiescherm wordt weergegeven.

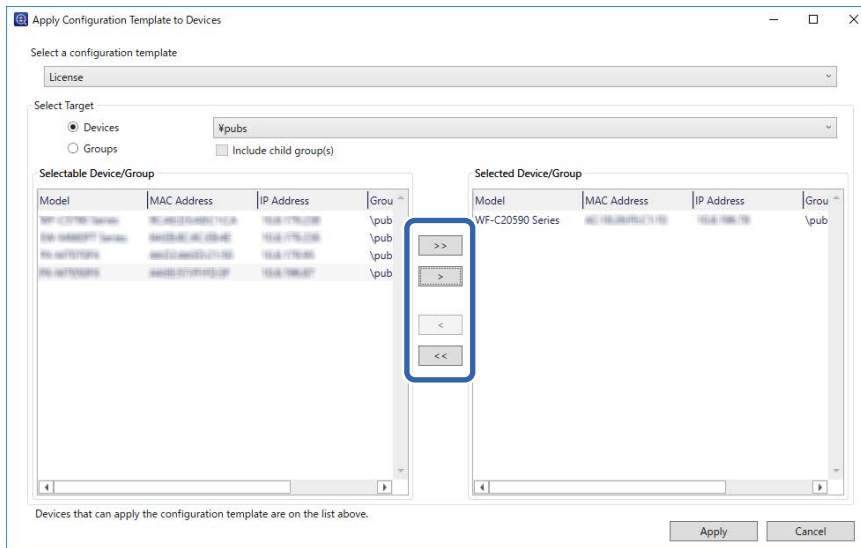


4. Selecteer de configuratiesjabloon die u wilt toepassen.

Opmerking:

- Als u in de vervolgkeuzelijst **Apparaten** en groepen apparaten selecteert, wordt elk apparaat weergegeven.
- Groepen worden weergegeven als u **Groepen** selecteert. Selecteer **Onderliggende groep(en) opnemen** om automatisch onderliggende groepen binnen de geselecteerde groep te selecteren.

- Verplaats de scanner of groepen waarop u de sjabloon wilt toepassen naar **Geselecteerd apparaat/groep**.



- Klik op **Toepassen**.

Een bevestigingsscherm voor de toe te passen configuratiesjabloon verschijnt.

- Klik op **OK** om de configuratiesjabloon toe te passen.

- Wanneer het bericht wordt weergegeven dat de procedure is voltooid, klikt u op **OK**.

- Klik op **Details** en lees de informatie.

Wanneer wordt weergegeven op de items die u hebt toegepast, is de bewerking gelukt.

- Klik op **Sluiten**.

Vereiste instellingen voor scannen

Een mailservers registreren.	46
Een netwerkmap maken.	49
Contactpersonen beschikbaar maken.	55
Instellen van AirPrint.	65
Problemen bij het voorbereiden van scannen via het netwerk.	66

Een mailservers registreren

Controleer het volgende voordat u de mailservers configureert.

- De scanner is verbonden met het netwerk.
- Configuratiegegevens voor de mailservers
 - Controleer de configuratiegegevens van de provider of website wanneer u een internetmailservers gebruikt.

Registreren

Open Web Config en selecteer het tabblad **Netwerk > E-mailservers > Basis**.

[“Web Config uitvoeren in een webbrowser” op pagina 39](#)

U kunt instellingen ook configureren via het bedieningspaneel van de scanner. Selecteer **Instel. > Netwerkinstellingen > Geavanceerd > E-mailservers > Serverinstellingen**.

Instellingen voor mailservers

Item	Instellingen en toelichting	
Verificatiemethode	Geef hier de verificatiemethode op die de scanner moet gebruiken voor toegang tot de mailservers.	
	Uit	Verificatie is uitgeschakeld wanneer met een mailservers wordt gecommuniceerd.
	SMTP-verificatie	De mailservers moet SMTP-verificatie ondersteunen.
	POP voor SMTP	Wanneer u deze optie selecteert, moet u een POP3-server instellen.
Geverifieerd account	Als u SMTP-verificatie of POP voor SMTP selecteert bij Verificatiemethode , moet u de geverifieerde accountnaam invoeren. Voer minimaal 0 en maximaal 255 tekens in ASCII (0x20 – 0x7E) in.	
Geverifieerd wachtwoord	Als u SMTP-verificatie of POP voor SMTP selecteert bij Verificatiemethode , moet u het geverifieerde wachtwoord invoeren. Voer minimaal 0 en maximaal 20 tekens in ASCII (0x20 – 0x7E) in.	
E-mailadres afzender	Stel het e-mailadres in waarnaar e-mails moeten worden verzonden vanaf de scanner. Hoewel u een bestaand e-mailadres kunt gebruiken, raden wij u aan een speciaal e-mailadres in te stellen, zodat u e-mails die vanaf de scanner worden verzonden gemakkelijk kunt onderscheiden. Voer minimaal 0 en maximaal 255 tekens in ASCII (0x20 – 0x7E) in, behalve: () < > [] ; ¥. Het eerste teken mag geen punt (".") zijn.	
Adres SMTP-server	Voer tussen 0 en 255 tekens in. Gebruik A – Z, a – z, 0 – 9. -. U kunt IPv4 of FQDN gebruiken.	
Poortnummer SMTP-server	Voer een getal tussen 1 en 65535 in.	
Veilige verbinding	Geef de beveiligde verbindingmethode op voor de mailservers.	
	Geen	Als u POP voor SMTP selecteert in Verificatiemethode , wordt de verbindingmethode ingesteld op Geen .
	SSL/TLS	Deze optie is beschikbaar wanneer Verificatiemethode is ingesteld op Uit of SMTP-verificatie .
	STARTTLS	Deze optie is beschikbaar wanneer Verificatiemethode is ingesteld op Uit of SMTP-verificatie .

Item	Instellingen en toelichting
Certificaatvalidatie (alleen Web Config)	Het certificaat is gevalideerd wanneer dit is ingeschakeld. Het wordt aanbevolen deze optie in te stellen op Inschakelen wanneer Veilige verbinding op iets anders is ingesteld dan Geen .
Adres POP3-server	Als u POP voor SMTP selecteert bij Verificatiemethode , voert u het serveradres van de POP3-server in. U kunt minimaal 0 en maximaal 255 tekens invoeren. Gebruik A – Z, a – z, 0 – 9. U kunt IPv4 of FQDN gebruiken.
Poortnummer POP3-server	Stel deze optie in wanneer u POP voor SMTP selecteert bij Verificatiemethode . Voer een getal tussen 1 en 65.535 in.

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser” op pagina 39](#)

De verbinding met een mailserver controleren

1. Selecteer het menu voor het testen van de verbinding.

Instellen via Web Config:

Selecteer het tabblad **Netwerk** > **E-mailserver** > **Verbindingstest** > **Starten**.

Instellen via het bedieningspaneel:

Selecteer **Instel.** > **Netwerkinstellingen** > **Geavanceerd** > **E-mailserver** > **Verbinding controleren**.

De verbindingstest voor de mailserver is gestart.

2. Controleer de testresultaten.

De test is geslaagd wanneer de melding **De verbindingstest is gelukt**. wordt weergegeven.

Als een fout wordt weergegeven, volgt u de instructies in de melding om de fout op te lossen.

[“Referenties voor verbindingstest voor mailserver” op pagina 47](#)

Referenties voor verbindingstest voor mailserver

Melding	Oorzaak
SMTP-servercommunicatiefout. Controleer het volgende. - Netwerkinstellingen	Deze melding wordt in de volgende gevallen weergegeven: <ul style="list-style-type: none"> <input type="checkbox"/> De scanner is niet verbonden met een netwerk. <input type="checkbox"/> De SMTP-server is uitgeschakeld. <input type="checkbox"/> De netwerkverbinding is verbroken tijdens de communicatie. <input type="checkbox"/> Er zijn onvolledige gegevens ontvangen.
POP3-servercommunicatiefout. Controleer het volgende. - Netwerkinstellingen	Deze melding wordt in de volgende gevallen weergegeven: <ul style="list-style-type: none"> <input type="checkbox"/> De scanner is niet verbonden met een netwerk. <input type="checkbox"/> De POP3-server is uitgeschakeld. <input type="checkbox"/> De netwerkverbinding is verbroken tijdens de communicatie. <input type="checkbox"/> Er zijn onvolledige gegevens ontvangen.

Melding	Oorzaak
Er is een fout opgetreden bij het verbinden met de SMTP-server. Controleer het volgende. - SMTP-serveradres - DNS-server	Deze melding wordt in de volgende gevallen weergegeven: <ul style="list-style-type: none"> <input type="checkbox"/> Verbinden met een DNS-server is mislukt. <input type="checkbox"/> Naamresolutie voor een SMTP-server is mislukt.
Er is een fout opgetreden bij het verbinden met de POP3-server. Controleer het volgende. - POP3-serveradres - DNS-server	Deze melding wordt in de volgende gevallen weergegeven: <ul style="list-style-type: none"> <input type="checkbox"/> Verbinden met een DNS-server is mislukt. <input type="checkbox"/> Naamresolutie voor een POP3-server is mislukt.
SMTP-serververificatiefout. Controleer het volgende. - Verificatiemethode - Geverifieerde account - Geverifieerd wachtwoord	Deze melding wordt weergegeven wanneer authenticatie van de SMTP-server is mislukt.
POP3-serververificatiefout. Controleer het volgende. - Verificatiemethode - Geverifieerde account - Geverifieerd wachtwoord	Deze melding wordt weergegeven wanneer authenticatie van de POP3-server is mislukt.
Niet-ondersteunde communicatiemethode. Controleer het volgende. - SMTP-serveradres - SMTP-serverpoortnummer	Deze melding wordt weergegeven wanneer u probeert te communiceren met niet-ondersteunde protocollen.
Verbinding met SMTP-server is mislukt. Wijzig Veilige verbinding naar Geen.	Deze melding wordt weergegeven wanneer een SMTP-verschil optreedt tussen een server en een client, of wanneer de server geen beveiligde SMTP-verbinding (SSL-verbinding) ondersteunt.
Verbinding met SMTP-server is mislukt. Wijzig Veilige verbinding naar SSL/TLS.	Deze melding wordt weergegeven wanneer een SMTP-verschil optreedt tussen een server en een client, of wanneer de server een SSL/TLS-verbinding wil gebruiken als beveiligde SMTP-verbinding.
Verbinding met SMTP-server is mislukt. Wijzig Veilige verbinding naar STARTTLS.	Deze melding wordt weergegeven wanneer een SMTP-verschil optreedt tussen een server en een client, of wanneer de server een STARTTLS-verbinding wil gebruiken als beveiligde SMTP-verbinding.
De verbinding is niet-vertrouwd. Controleer het volgende. - Datum en tijd	Deze melding wordt weergegeven wanneer de datum- en tijdstelling van de scanner onjuist is of het certificaat is verlopen.
De verbinding is niet-vertrouwd. Controleer het volgende. - CA-certificaat	Deze melding wordt weergegeven wanneer de scanner geen basiscertificaat heeft dat overeenkomt met de server of wanneer geen CA-certificaat is geïmporteerd.
De verbinding is niet beveiligd.	Deze melding wordt weergegeven wanneer het verkregen certificaat beschadigd is.
SMTP-serververificatie is mislukt. Wijzig de verificatiemethode naar SMTP-AUTH.	Deze melding wordt weergegeven wanneer een verschil optreedt in de authenticatiemethode tussen een server en een client. De server ondersteunt SMTP-verificatie.
SMTP-serververificatie is mislukt. Wijzig de verificatiemethode naar POP voor SMTP.	Deze melding wordt weergegeven wanneer een verschil optreedt in de authenticatiemethode tussen een server en een client. De server ondersteunt geen SMTP-verificatie.
Het e-mailadres van de afzender is onjuist. Wijzig naar het e-mailadres voor uw e-mailservice.	Deze melding wordt weergegeven wanneer het opgegeven e-mailadres van de afzender onjuist is.

Melding	Oorzaak
Kan geen toegang krijgen tot het product tot de verwerking is voltooid.	Deze melding wordt weergegeven wanneer de scanner bezet is.

Een netwerkmap maken

Maak een netwerkmap op uw computer. De computer moet met hetzelfde netwerk zijn verbonden als de scanner.


De methode voor het instellen van de netwerkmap is afhankelijk van de omgeving. Hier volgt een voorbeeld voor het maken van een netwerkmap op het bureaublad van een computer in de volgende omgeving.

- Besturingssysteem: Windows 10
- Locatie voor het maken van een gedeelde map: bureaublad
- Mappad: C:\Gebruikers\xxxx\Bureaublad\scan_folder (maak een netwerkmap met de naam scan_folder op het bureaublad)

1. Meld u met een gebruikersaccount met beheerdersbevoegdheid aan op de computer waarop u de netwerkmap wilt maken.

Opmerking:

Als u niet weet welk gebruikersaccount beheerdersbevoegdheid heeft, neemt u contact op met de computerbeheerder.

2. Zorg ervoor dat de apparaatnaam (computernaam) geen double-bytetekens bevat. Klik op de startknop van Windows en selecteer  **Instellingen** > **Systeem** > **Info**.

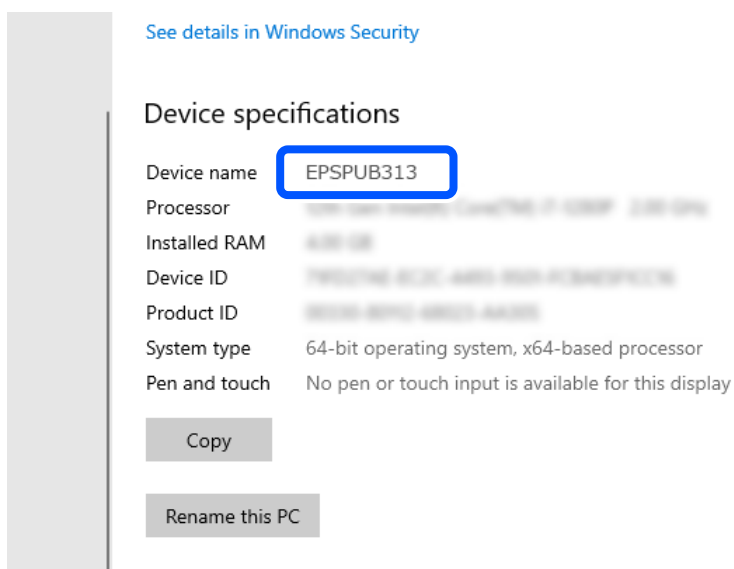
Opmerking:

Als de apparaatnaam double-bytetekens bevat, kan het opslaan van bestanden mislukken.

3. Controleer of de tekenreeks die bij **Apparaatspecificaties** > **Apparaatnaam** wordt weergegeven geen double-bytetekens bevat.

Er zouden geen problemen moeten zijn als de apparaatnaam slechts uit single-bytetekens bestaat. Sluit het scherm.

Voorbeeld: EPSPUB313



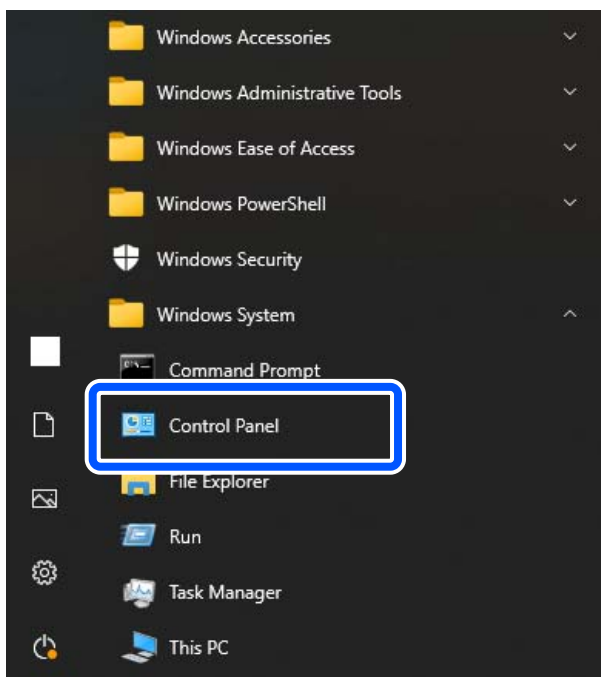
! **Belangrijk:**

Als de apparaatnaam double-bytetekens bevat, gebruik dan een computer die geen double-bytetekens gebruikt of wijzig de naam van het apparaat.

Als u de naam van het apparaat moet wijzigen, moet u dit vooraf met de computerbeheerder overleggen. Dit kan namelijk gevolgen hebben voor het computerbeheer en de toegang tot bronnen.

Controleer vervolgens de instellingen van uw computer.

4. Klik op de startknop van Windows en selecteer **Systeem > Configuratiescherm**.



5. Klik op het bedieningspaneel op **Netwerk en internet > Netwerkcentrum > Geavanceerde instellingen voor delen wijzigen**.

Het netwerkprofiel wordt weergegeven.

6. Controleer of **Delen van bestanden en printers inschakelen** is geselecteerd bij **Delen van bestanden en printers** voor het netwerkprofiel (huidige profiel).

Als de optie al is geselecteerd, klikt u op **Annuleren** en sluit u het venster.

Wanneer u de instellingen wijzigt, klikt u op **Wijzigingen opslaan** en sluit u het venster.

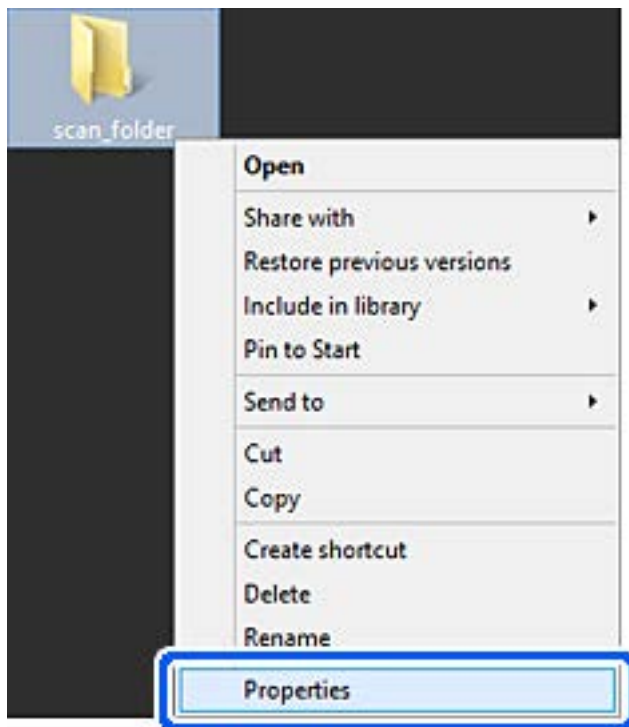
Maak vervolgens een netwerkmap.

7. Maak een map op het bureaublad en geef deze een naam.

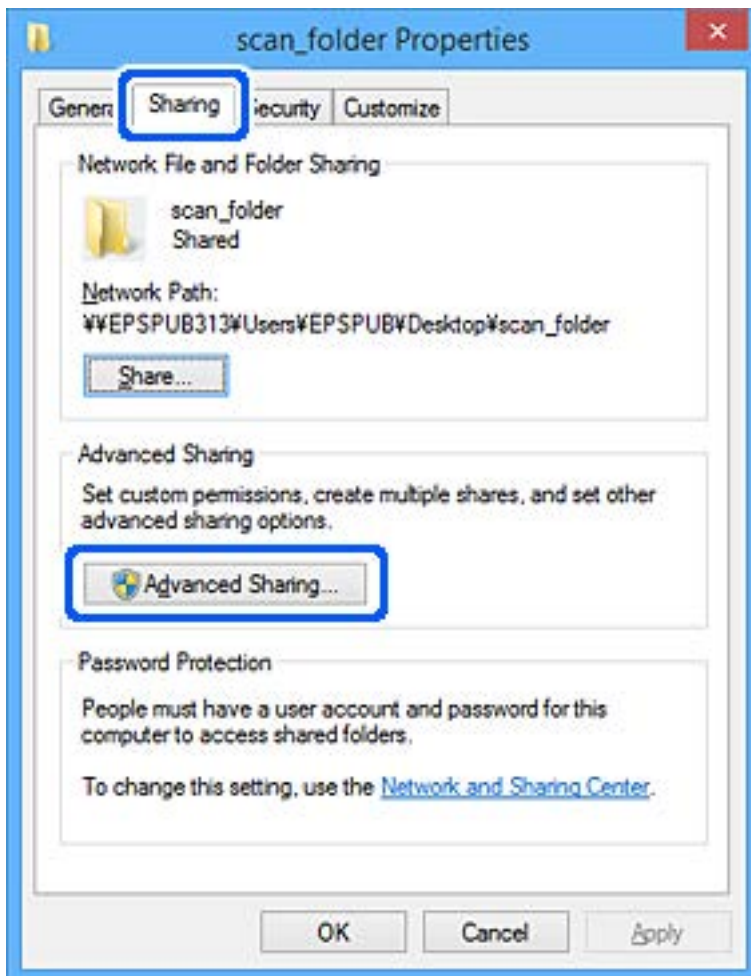
Gebruik voor de mapnaam minimaal 1 en maximaal 12 alfanumerieke tekens. Als de naam langer is dan 12 tekens, kunt u de map mogelijk niet openen. Dit is afhankelijk van de omgeving.

Voorbeeld: scan_folder

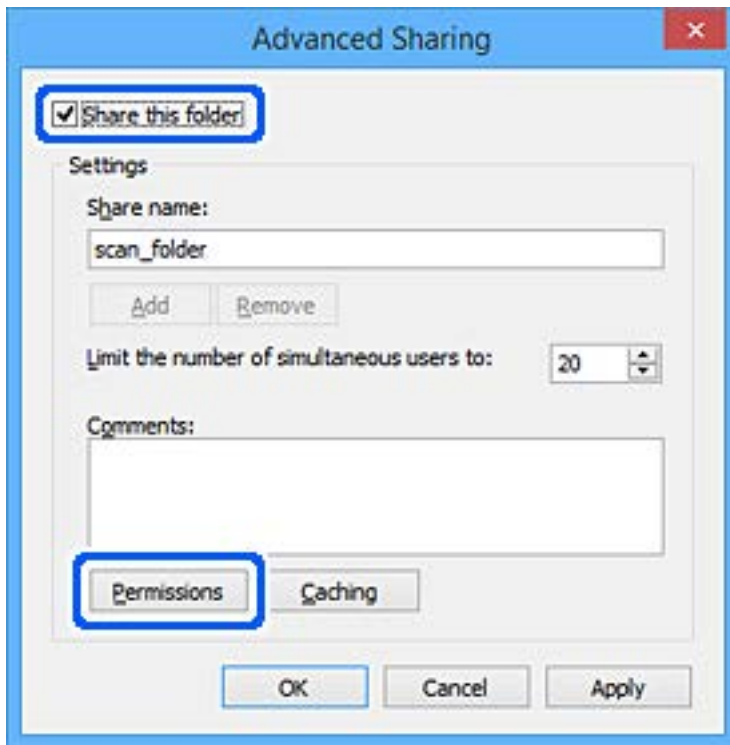
8. Klik met de rechtermuisknop op de map en selecteer **Eigenschappen**.



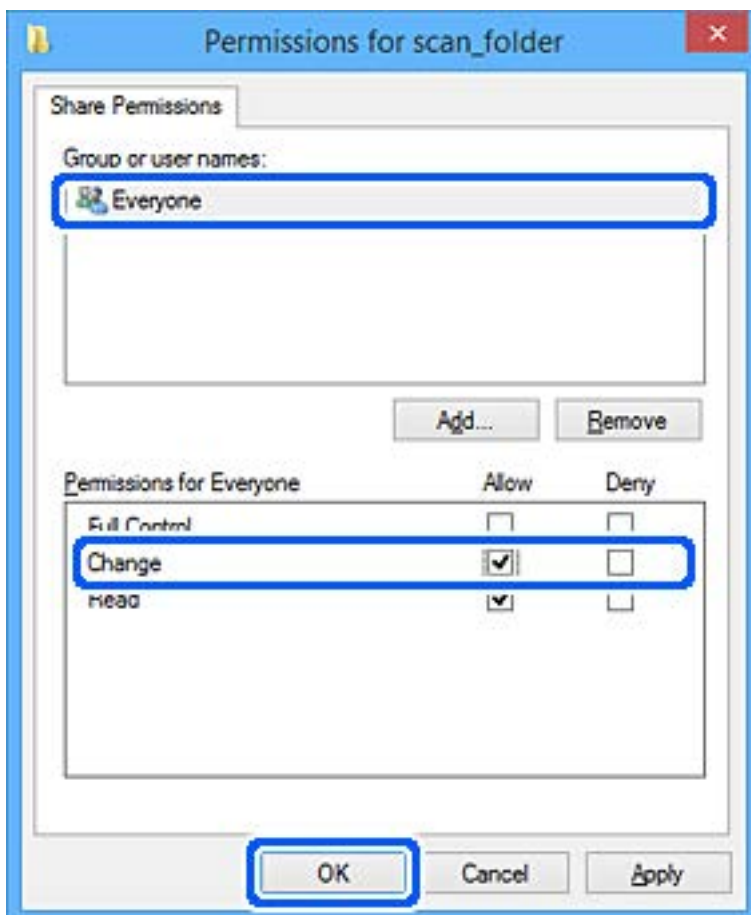
9. Klik op **Geavanceerd delen** op het tabblad **Delen**.



10. Selecteer **Deze map delen** en klik vervolgens op **Machtigingen**.



11. Selecteer **Iedereen** bij **Groep of gebruikersnamen**, selecteer **Toestaan** bij **Wijzigen** en klik vervolgens op **OK**.

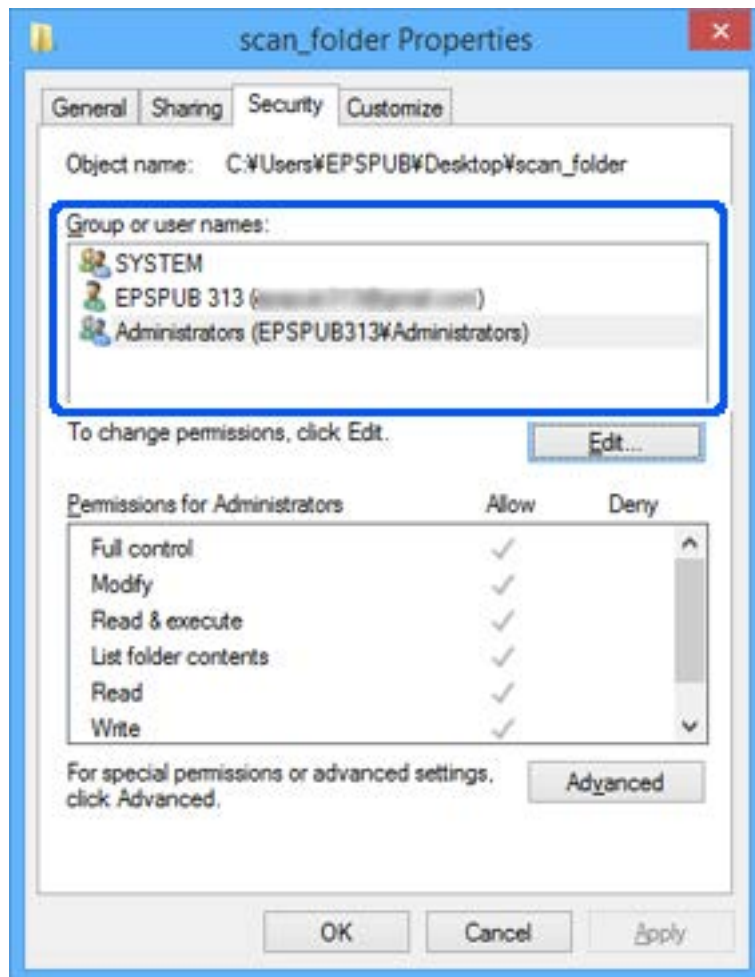


12. Klik op **OK** om het scherm te sluiten en terug te gaan naar het venster met eigenschappen.

Opmerking:

Op het tabblad **Beveiliging** > **Groep of gebruikersnamen** kunt u controleren welke groepen of gebruikers toegang hebben tot de netwerkmap.

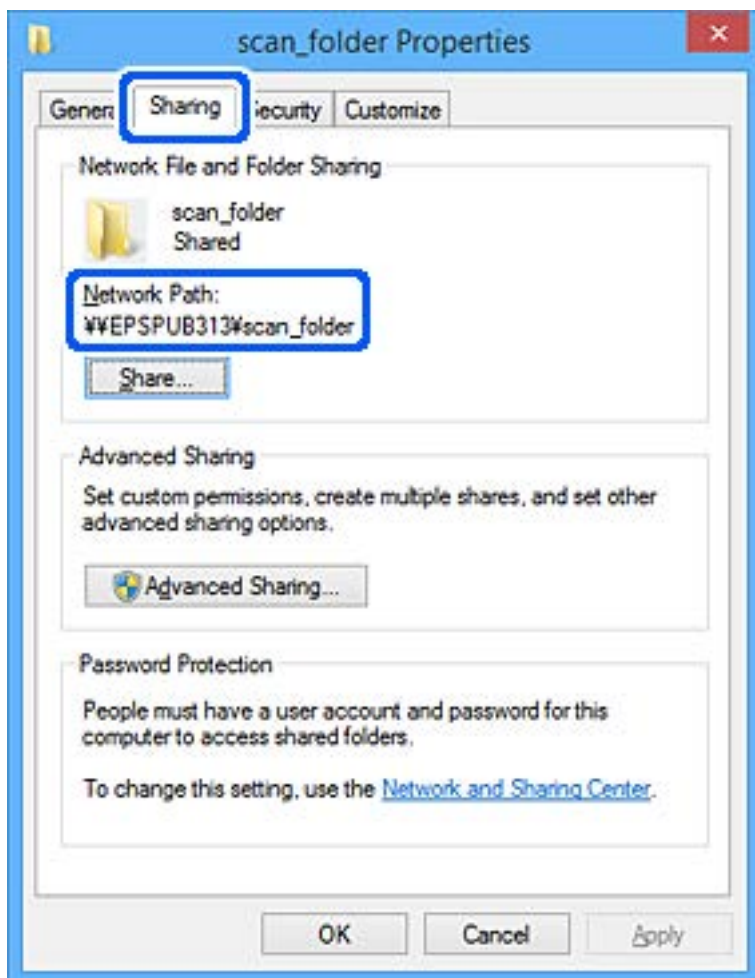
Voorbeeld: wanneer zowel de gebruiker die op de computer is aangemeld als beheerders toegang hebben tot de netwerkmap.



13. Selecteer het tabblad **Delen**.

Het netwerkpad voor de netwerkmap wordt weergegeven. Dit wordt gebruikt bij het registreren van de contactpersonen in de scanner. Noteer dit.

Voorbeeld: \\EPSPUB313\scan_folder



14. Klik op **Sluiten** of **OK** om het venster te sluiten.

Hiermee is het maken van een netwerkmap voltooid.

Contactpersonen beschikbaar maken

Als u bestemmingen in de contactpersonenlijst van de scanner registreert, kunt u de bestemming eenvoudig invoeren tijdens het scannen.

De lijst met contactpersonen kan de volgende soorten bestemmingen bevatten. U kunt in totaal maximaal 300 items registreren.

Opmerking:

U kunt ook een LDAP-server gebruiken om een bestemming te kiezen (LDAP-zoekopdracht).

E-mail	Bestemming voor e-mail. U moet de instellingen van de e-mailserver van tevoren configureren.
Netwerkmap	Bestemming voor scangegevens. U moet de netwerkmap van tevoren voorbereiden.

Gerelateerde informatie

➔ [“Samenwerking tussen de LDAP-server en gebruikers” op pagina 62](#)

Contactpersonen configureren — vergelijking

Er zijn drie hulpprogramma's om contactpersonen te configureren op de scanner: Web Config, Epson Device Admin en het bedieningspaneel van de scanner. De verschillen tussen de drie manieren van werken worden weergegeven in de onderstaande tabel.

Functies	Web Config*	Epson Device Admin	Bedieningspaneel van de scanner
Bestemming registreren	✓	✓	✓
Bestemming bewerken	✓	✓	✓
Groep toevoegen	✓	✓	✓
Groep bewerken	✓	✓	✓
Bestemming of groepen verwijderen	✓	✓	✓
Alle bestemmingen verwijderen	✓	✓	–
Bestand importeren	✓	✓	–
Exporteren naar bestand	✓	✓	–

* Log in als beheerder om instellingen te configureren.

Een bestemming opslaan in de contactpersonenlijst met Web Config

Opmerking:

U kunt contactpersonen ook opslaan via het bedieningspaneel van de scanner.

1. Open Web Config en selecteer het tabblad **Scannen > Contactpersonen**.
2. Selecteer het nummer dat u wilt registreren en klik vervolgens op **Bewerken**.
3. Voer **Naam** en **Indexwoord** in.
4. Selecteer het type bestemming voor de optie **Type**.

Opmerking:

*Nadat de registratie is voltooid, kunt u de optie **Type** niet meer wijzigen. Als u het type wilt wijzigen, wist u de bestemming en registreert u deze opnieuw.*

5. Voer voor elk item een waarde in en klik vervolgens op **Toepassen**.

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser” op pagina 39](#)

Items voor het instellen van de bestemming

Items	Instellingen en toelichting
Algemene instellingen	
Naam	Voer een naam in die in de contactpersonen wordt weergegeven. Deze mag maximaal 30 tekens bevatten in Unicode (UTF-16). Als u dit niet opgeeft, laat u dit leeg.
Indexwoord	Voer een naam van maximaal 30 tekens in Unicode (UTF-16) in om de contactpersonen op het bedieningspaneel van de scanner te zoeken. Als u dit niet opgeeft, laat u dit leeg.
Type	Selecteer het type adres dat u wilt opslaan.
Toewijzen aan frequent gebruik	Selecteer deze optie om het opgeslagen adres in te stellen als veelgebruikt adres. Wanneer u dit instelt als veelgebruikt adres, wordt dit bovenaan het scherm voor scannen weergegeven en kunt u de bestemming opgeven zonder de contactpersonen weer te geven.
E-mail	
E-mailadres	Voer minimaal 1 en maximaal 255 tekens in. Gebruik A-Z a-z 0-9 ! # \$ % & ' * + - . / = ? ^ _ { } ~ @.
Netwerkmap (SMB)	
Opslaan in	\\"Mappad" Voer de locatie van de doelmap in. Gebruik minimaal 1 en maximaal 253 tekens in Unicode (UTF-16) en laat "\\" weg. Voer het netwerkpad in dat wordt weergegeven in het eigenschappenscherf van de map. Raadpleeg de volgende informatie over het instellen van het netwerkpad. “Een netwerkmap maken” op pagina 49
Gebruikersnaam	Voer een gebruikersnaam in voor toegang tot een netwerkmap. Deze mag maximaal 30 tekens bevatten in Unicode (UTF-16). Vermijd hierbij het gebruik van stuurcodes (0x00 tot 0x1F, 0x7F).
Wachtwoord	Voer een wachtwoord in voor toegang tot een netwerkmap. Dit moet minimaal 0 en maximaal 20 tekens bevatten in Unicode (UTF-16). Vermijd hierbij het gebruik van stuurcodes (0x00 tot 0x1F, 0x7F).
FTP	
Veilige verbinding	Selecteer FTP of FTPS, afhankelijk van het protocol voor bestandsoverdracht dat door de FTP-server wordt ondersteund. Selecteer FTPS om communicatie door de scanner met beveiligingsmaatregelen toe te staan.
Opslaan in	Voer de servernaam in. Gebruik minimaal 1 en maximaal 253 tekens in Unicode (UTF-16) en laat "ftp://" of "ftps://" weg.

Items	Instellingen en toelichting
Gebruikersnaam	Voer een gebruikersnaam in voor toegang tot een FTP-server. Deze mag maximaal 30 tekens bevatten in Unicode (UTF-16). Vermijd hierbij het gebruik van stuurcodes (0x00 tot 0x1F, 0x7F). Als de server anonieme verbindingen toestaat, voert u als gebruikersnaam bijvoorbeeld Anoniem en FTP in. Als u dit niet opgeeft, laat u dit leeg.
Wachtwoord	Voer een wachtwoord in voor toegang tot een FTP-server. Dit moet minimaal 0 en maximaal 20 tekens bevatten in Unicode (UTF-16). Vermijd hierbij het gebruik van stuurcodes (0x00 tot 0x1F, 0x7F). Als u dit niet opgeeft, laat u dit leeg.
Aansluitmodus	Selecteer de verbindingmodus in het menu. Als tussen de scanner en de FTP-server een firewall is ingesteld, selecteert u Passieve modus .
Poortnummer	Voer een FTP-serverpoortnummer tussen 1 en 65535 in.
Certificaatvalidatie	Het certificaat van de FTP-server is geldig wanneer dit is ingeschakeld. Dit is beschikbaar wanneer FTPS is geselecteerd voor Veilige verbinding . Als u dit wilt configureren, moet u het CA-certificaat naar de scanner importeren.
SharePoint(WebDAV)*	
Veilige verbinding	Selecteer HTTP of HTTPS, afhankelijk van het protocol voor bestandsoverdracht dat door de server wordt ondersteund. Selecteer HTTPS om communicatie door de scanner met beveiligingsmaatregelen toe te staan.
Opslaan in	Voer de servernaam in. Gebruik minimaal 1 en maximaal 253 tekens in Unicode (UTF-16) en laat "http://" of "https://" weg.
Gebruikersnaam	Voer een gebruikersnaam voor toegang tot een server in. Deze mag maximaal 30 tekens bevatten in Unicode (UTF-16). Vermijd hierbij het gebruik van stuurcodes (0x00 tot 0x1F, 0x7F). Als u dit niet opgeeft, laat u dit leeg.
Wachtwoord	Voer een wachtwoord in voor toegang tot een server. Dit moet minimaal 0 en maximaal 20 tekens bevatten in Unicode (UTF-16). Vermijd hierbij het gebruik van stuurcodes (0x00 tot 0x1F, 0x7F). Als u dit niet opgeeft, laat u dit leeg.
Certificaatvalidatie	Het certificaat van de server wordt gevalideerd wanneer dit is ingeschakeld. Dit is beschikbaar wanneer HTTPS is geselecteerd voor Veilige verbinding . Als u dit wilt configureren, moet u het CA-certificaat naar de scanner importeren.
Proxyserver	Selecteer of u al dan niet een proxyserver wilt gebruiken.

* SharePoint Online wordt niet ondersteund bij scannen naar een netwerkmap via het bedieningspaneel van de scanner.

Als u de gescande afbeelding wilt opslaan naar SharePoint Online, gebruikt u Document Capture Pro nadat u de SharePoint Online Connector hebt geïnstalleerd. Raadpleeg de handleiding van Document Capture Pro voor meer informatie.

<https://support.epson.net/dcp/>

Bestemmingen als groep registreren met Web Config

Als het type bestemming is ingesteld op **E-mail**, kunt u de bestemmingen als groep registreren.

1. Open Web Config en selecteer het tabblad **Scannen > Contactpersonen**.

2. Selecteer het nummer dat u wilt registreren en klik vervolgens op **Bewerken**.
3. Selecteer een groep in **Type**.
4. Klik op **Selecteren** voor **Contact(en) voor Groep**.
De beschikbare bestemmingen worden weergegeven.
5. Selecteer de bestemming die u voor de groep wilt registreren en klik vervolgens op **Selecteren**.
6. Voer een **Naam** en **Indexwoord** in.
7. Selecteer of u de geregistreerde groep wilt toewijzen aan de veelgebruikte groep.

Opmerking:

Bestemmingen kunnen worden geregistreerd voor meerdere groepen.

8. Klik op **Toepassen**.

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser” op pagina 39](#)

Contactpersonen importeren en een back-up maken

Met Web Config of andere hulpprogramma's kunt u belangrijke contactpersonen importeren of hiervan een back-up maken.

Met Web Config kunt u een back-up maken van contactpersonen door de scannerinstellingen met contactpersonen te exporteren. Het geëxporteerde bestand is een binair bestand en kan daarom niet worden bewerkt.

Wanneer u de scannerinstellingen naar de scanner importeert, worden de contactpersonen overschreven.

Met Epson Device Admin kunnen alleen contactpersonen worden geëxporteerd vanaf het eigenschappenschermb van het apparaat. Als u de beveiligingsitems niet exporteert, kunt u de geëxporteerde contactpersonen bewerken en deze importeren omdat dit bestand kan worden opgeslagen in SYLK- of CSV-indeling.

Contactpersonen importeren met Web Config

Als u een scanner hebt waarmee u een back-up kunt maken van contactpersonen en die compatibel is met deze scanner, kunt u eenvoudig contactpersonen registreren door het back-upbestand te importeren.

Opmerking:

Raadpleeg de handleiding die bij de scanner is meegeleverd voor instructies voor het maken van een back-up van de contactpersonen op de scanner.

Volg de onderstaande stappen om de contactpersonen naar de scanner te importeren.

1. Open Web Config en selecteer het tabblad **Apparaatbeheer > Instelwaarde exporteren en importeren > Importeren**.
2. Selecteer het back-upbestand dat u hebt gemaakt in **Bestand**, voer het wachtwoord in en klik vervolgens op **Volgende**.
3. Schakel het selectievakje **Contactpersonen** in en klik vervolgens op **Volgende**.

Een back-op maken van contactpersonen via Web Config

Gegevens van contactpersonen kunnen verloren gaan bij scannerstoringen. Het wordt aanbevolen elke keer dat u gegevens hebt bijgewerkt een back-up te maken. Epson is niet verantwoordelijk voor gegevensverlies, voor de back-up of het ophalen van gegevens en/of instellingen, zelfs niet tijdens een garantieperiode.

Met Web Config kunt u op de computer een back-up maken van de contactgegevens die in de scanner zijn opgeslagen.

1. Open Web Config en selecteer vervolgens het tabblad **Apparaatbeheer > Instelwaarde exporteren en importeren > Exporteren**.
2. Selecteer het selectievakje **Contactpersonen** bij de categorie **Scannen**.
3. Voer een wachtwoord in om het geëxporteerde bestand te versleutelen.
U hebt dit wachtwoord nodig om het bestand te importeren. Laat dit leeg als u het bestand niet wilt versleutelen.
4. Klik op **Exporteren**.

Contactpersonen exporteren en in bulk registreren met een hulpprogramma

Als u Epson Device Admin gebruikt, kunt u een back-up maken van alleen de contactpersonen, de geëxporteerde bestanden bewerken en alle contactpersonen in een keer registreren.

Dit is nuttig wanneer u alleen van de contactpersonen een back-up wilt maken, of als u de scanner vervangt en de contactpersonen van de oude scanner op de nieuwe wilt overzetten.

Contactpersonen exporteren

Sla de gegevens van de contactpersonen op naar een bestand.

U kunt bestanden die in SYLK-indeling zijn opgeslagen bewerken via een gegevensbladtoepassing of teksteditor. U kunt deze allemaal tegelijk registreren nadat u gegevens hebt verwijderd of gewijzigd.

Informatie die beveiligingsitems bevat, zoals wachtwoorden en persoonlijke gegevens, kunnen in binaire indeling worden opgeslagen en met een wachtwoord worden beveiligd. Dit bestand kunt u niet bewerken. Dit kan worden gebruikt als back-upbestand met gegevens inclusief beveiligingsitems.

1. Start Epson Device Admin.
2. Selecteer **Apparaten** in het taakmenu in de zijmarge.
3. Selecteer het apparaat dat u wilt configureren in de lijst.
4. Klik op **Apparaatconfiguratie** op het tabblad **Start** op het lintmenu.
Wanneer het beheerderswachtwoord is ingesteld, voert u het wachtwoord in en klikt u op **OK**.
5. Klik op **Algemeen > Contacten**.

6. Selecteer de exportindeling in **Exporteren > Items exporteren**.

Alle items

Exporteer het versleutelde binaire bestand. Selecteer deze optie wanneer u beveiligingsitems wilt opnemen, zoals wachtwoorden en persoonlijke gegevens. Dit bestand kunt u niet bewerken. Als u deze optie selecteert, moet u een wachtwoord instellen. Klik op **Configuratie** en stel een wachtwoord in tussen 8 en 63 tekens in ASCII. Dit wachtwoord is vereist voor het importeren van het binaire bestand.

Items behalve Beveiligingsinformatie

Exporteer de bestanden in SYLK- of CSV-indeling. Selecteer deze optie wanneer u de gegevens in het geëxporteerde bestand wilt bewerken.

7. Klik op **Exporteren**.

8. Geef op waar het bestand moet worden opgeslagen, selecteer de indeling en klik op **Opslaan**.

Na afloop wordt een bericht over voltooiing weergegeven.

9. Klik op **OK**.

Controleer of het bestand op de opgegeven locatie wordt opgeslagen.

Contactpersonen importeren

Importeer de gegevens van de contactpersonen vanuit het bestand.

U kunt de bestanden importeren die zijn opgeslagen in SYLK- of CSV-indeling, of het binaire back-upbestand waarin beveiligingsitems zijn opgenomen.

1. Start Epson Device Admin.

2. Selecteer **Apparaten** in het taakmenu in de zijmarge.

3. Selecteer het apparaat dat u wilt configureren in de lijst.

4. Klik op **Apparaatconfiguratie** op het tabblad **Start** op het lintmenu.

Wanneer het beheerderswachtwoord is ingesteld, voert u het wachtwoord in en klikt u op **OK**.

5. Klik op **Algemeen > Contacten**.

6. Klik op **Bladeren bij Importeren**.

7. Selecteer de het bestand dat u wilt importeren en klik vervolgens op **Openen**.

Wanneer u het binaire bestand selecteert, voert u in **Wachtwoord** het wachtwoord in dat u bij het exporteren hebt ingesteld.

8. Klik op **Importeren**.

Het bevestigingsscherm wordt weergegeven.

9. Klik op **OK**.

Het resultaat van de validatie wordt weergegeven.

De geladen informatie bewerken

Klik wanneer u afzonderlijke gegevens wilt bewerken.

- Meer bestanden laden

Klik wanneer u meerdere bestanden wilt importeren.

10. Klik op **Importeren** en klik vervolgens op **OK** in het bevestigingsscherm.

Ga terug naar het eigenschappenschermb van het apparaat.

11. Klik op **Verzenden**.

12. Klik op **OK** in het bevestigingsbericht.

De instellingen worden naar de scanner verzonden.

13. Klik op het voltooiingsscherm voor verzenden op **OK**.

De gegevens van de scanner zijn bijgewerkt.

Open de contactpersonen vanuit Web Config of het bedieningspaneel van de scanner en controleer of de contactpersoon is bijgewerkt.

Samenwerking tussen de LDAP-server en gebruikers

Tijdens samenwerking met de LDAP-server kunt u de adresinformatie die is vastgelegd in de LDAP-server gebruiken als bestemming voor een e-mail.

De LDAP-server configureren

Als u de gegevens van de LDAP-server wilt gebruiken, registreert u deze in de scanner.

1. Open Web Config en selecteer het tabblad **Netwerk > LDAP-server > Basis**.
2. Voer voor elk item een waarde in.
3. Selecteer **OK**.

De instellingen die u hebt geselecteerd, worden weergegeven.

Items voor LDAP-serverinstellingen

Items	Instellingen en toelichting
LDAP-server gebruiken	Selecteer Gebruiken of Niet gebruiken .
LDAP-serveradres	Voer het adres van de LDAP-server in. Voer tussen 1 en 255 tekens in. Gebruik de IPv4-, IPv6- of FQDN-indeling. Voor FQDN kunt u alfanumerieke tekens in ASCII (0x20–0x7E) en "-" gebruiken, behalve aan het begin en eind van het adres.
Poortnummer LDAP-server	Voer het LDAP-serverpoortnummer tussen 1 en 65535 in.
Veilige verbinding	Geef hier de verificatiemethode op die de scanner moet gebruiken voor toegang tot de LDAP-server.

Items	Instellingen en toelichting
Certificaatvalidatie	Wanneer deze optie is ingeschakeld, wordt het certificaat van de LDAP-server gevalideerd. Wij raden aan dit in te stellen op Inschakelen . Voor de configuratie moet het CA-certificaat naar de scanner worden geïmporteerd.
Time-out zoeken (sec)	Stel de tijdsduur voor zoeken tussen 5 en 300 in voordat een time-out optreedt.
Verificatiemethode	Selecteer een van de methoden. Als u Kerberos-verificatie selecteert, selecteert u Kerberos-instellingen om de instellingen voor Kerberos te configureren. Voor het uitvoeren van Kerberos-verificatie is de volgende omgeving vereist. <ul style="list-style-type: none"> <input type="checkbox"/> De scanner en de DNS-server kunnen communiceren. <input type="checkbox"/> De tijd van de scanner, de KDC-server en de server die vereist is voor verificatie (LDAP-server, SMTP-server, bestandserver) is gesynchroniseerd. <input type="checkbox"/> Wanneer de serviceserver is aangewezen als IP-adres, is de FQDN van de serviceserver geregistreerd in de zone voor reverse lookup van de DNS-server.
Te gebruiken Kerberos-realm	Als u Kerberos-verificatie selecteert als Verificatiemethode , selecteert u het Kerberos-domein dat u wilt gebruiken.
Beheerders-DN / Gebruikersnaam	Voer de gebruikersnaam in om toegang te krijgen tot de LDAP-server. Deze mag maximaal 128 tekens bevatten in Unicode (UTF-8). U kunt geen stuurcodes gebruiken, zoals 0x00–0x1F en 0x7F. Deze instelling wordt niet gebruikt wanneer Anonieme verificatie is geselecteerd als Verificatiemethode . Als u dit niet opgeeft, laat u dit leeg.
Wachtwoord	Voer een wachtwoord in om toegang te krijgen tot de LDAP-serververificatie. Deze mag maximaal 128 tekens bevatten in Unicode (UTF-8). U kunt geen stuurcodes gebruiken, zoals 0x00–0x1F en 0x7F. Deze instelling wordt niet gebruikt wanneer Anonieme verificatie is geselecteerd als Verificatiemethode . Als u dit niet opgeeft, laat u dit leeg.

Kerberos-instellingen

Als u **Kerberos-verificatie** selecteert als **Verificatiemethode** voor **LDAP-server > Basis**, configureert u de volgende Kerberos-instellingen op het tabblad **Netwerk > Kerberos-instellingen**. U kunt tot 10 instellingen registreren. voor de Kerberos-instellingen.

Items	Instellingen en toelichting
Realm (domein)	Voer hier het realm van de Kerberos-verificatie in, maximaal 255 tekens in ASCII (0x20–0x7E). Als u dit niet registreert, laat u dit leeg.
KDC-adres	Voer het adres van de Kerberos-verificatieserver in. Voer maximaal 255 tekens in IPv4-, IPv6- of FQDN-indeling in. Als u dit niet registreert, laat u dit leeg.
Poortnummer (Kerberos)	Voer het Kerberos-serverpoortnummer, tussen 1 en 65535, in.

De zoekinstellingen configureren voor de LDAP-server

Als u de zoekinstellingen instelt, kunt u e-mailadressen gebruiken die in de LDAP-server zijn geregistreerd.

1. Open Web Config en selecteer het tabblad **Netwerk > LDAP-server > Zoekinstellingen**.

2. Voer voor elk item een waarde in.
3. Klik op **OK** om het resultaat van de instellingen weer te geven.
De instellingen die u hebt geselecteerd, worden weergegeven.

Items voor zoekinstellingen voor LDAP-server

Items	Instellingen en toelichting
Zoekdatabase (Gedistingeerde naam)	Als u in een willekeurig domein wilt zoeken, geeft u de domeinnaam van de LDAP-server op. Voer tussen 0 en 128 tekens in Unicode (UTF-8) in. Als u geen willekeurig kenmerk zoekt, laat u dit leeg. Voorbeeld voor de lokale serverdirectory: dc=server,dc=local
Aantal zoekgegevens	Geef het aantal zoekitems op, tussen 5 en 500. Het opgegeven aantal zoekitems wordt tijdelijk opgeslagen en weergegeven. Zelfs als het aantal zoekitems het opgegeven aantal overschrijdt en een foutmelding wordt weergegeven, kan de zoekactie worden voltooid.
Kenmerk gebruikersnaam	Geef de kenmerknaam op die moet worden weergegeven als u naar gebruikersnamen zoekt. Voer tussen 1 en 255 tekens in Unicode (UTF-8) in. Het eerste teken moet a-z of A-Z zijn. Voorbeeld: cn, uid
Kenmerk weergave gebruikersnaam	Geef de kenmerknaam op die moet worden weergegeven als gebruikersnaam. Voer tussen 0 en 255 tekens in Unicode (UTF-8) in. Het eerste teken moet a-z of A-Z zijn. Voorbeeld: cn, sn
Kenmerk e-mailadres	Geef de kenmerknaam op die moet worden weergegeven als u naar e-mailadressen zoekt. Voer een combinatie van 1 tot 255 tekens in. Gebruik A-Z, a-z, 0-9 en -. Het eerste teken moet a-z of A-Z zijn. Voorbeeld: mail
Arbitrair kenmerk 1 - Arbitrair kenmerk 4	U kunt tevens andere willekeurige kenmerken opgeven waarnaar u wilt zoeken. Voer tussen 0 en 255 tekens in Unicode (UTF-8) in. Het eerste teken is verplicht een a-z of A-Z. Als u niet wilt zoeken op arbitraire kenmerken, laat u deze optie leeg. Voorbeeld: o, ou

De verbinding met de LDAP-server controleren

Voer de verbindingstest met de LDAP-server uit met de parameter die is ingesteld bij **LDAP-server > Zoekinstellingen**.

1. Open Web Config en selecteer het tabblad **Netwerk > LDAP-server > Verbindingstest**.
2. Selecteer **Starten**.
De verbindingstest wordt gestart. Na de test wordt het controlerapport weergegeven.

Referenties verbindingstest LDAP-server

Berichten	Uitleg
De verbindingstest is gelukt.	Deze melding wordt weergegeven wanneer de verbinding met de server is gemaakt.
Verbindingstest is mislukt. Controleer de instellingen.	Deze melding wordt weergegeven wanneer: <ul style="list-style-type: none"> <input type="checkbox"/> Het LDAP-serveradres of het poortnummer onjuist is. <input type="checkbox"/> Er een time-out is opgetreden. <input type="checkbox"/> Niet gebruiken is geselecteerd voor LDAP-server gebruiken. <input type="checkbox"/> Als Kerberos-verificatie is geselecteerd als Verificatiemethode en instellingen als Realm (domein), KDC-adres en Poortnummer (Kerberos) onjuist zijn.
Verbindingstest is mislukt. Controleer datum en tijd op uw product of server.	Deze melding wordt weergegeven wanneer het maken van verbinding mislukt omdat de tijdstellingen van de scanner en de LDAP-server niet overeenkomen.
Verificatie mislukt. Controleer de instellingen.	Deze melding wordt weergegeven wanneer: <ul style="list-style-type: none"> <input type="checkbox"/> Gebruikersnaam en/of Wachtwoord onjuist is. <input type="checkbox"/> Als Kerberos-verificatie is geselecteerd als Verificatiemethode en de tijd/ datum niet is geconfigureerd.
Kan geen toegang krijgen tot het product tot de verwerking is voltooid.	Deze melding wordt weergegeven wanneer de scanner bezet is.

Instellen van AirPrint

Open Web Config, selecteer het tabblad **Netwerk** en selecteer vervolgens **AirPrint setup**.

Items	Uitleg
Bonjour gebruikersnaam	Voer de naam van de Bonjour-service in. Gebruik maximaal 41 tekens in ASCII (0x20–0x7E).
Bonjour locatie	Voer een omschrijving van de scannerlocatie in. Gebruik maximaal 127 bytes in Unicode (UTF-8).
Wide-Area Bonjour	Stel in of u Wide-Area Bonjour wilt gebruiken. Als u deze optie gebruikt, moeten de scanner bij de DNS-server zijn geregistreerd om de scanner in het segment te kunnen zoeken.
AirPrint inschakelen	Bonjour en AirPrint (scanservice) worden ingeschakeld. Deze knop is alleen beschikbaar wanneer AirPrint is uitgeschakeld. Opmerking: <i>Als AirPrint is uitgeschakeld, is scannen met Mopria via Chromebooks, Windows en de Mopria Scan-app ook uitgeschakeld.</i>

Problemen bij het voorbereiden van scannen via het netwerk

Tips voor het oplossen van problemen

De foutmelding controleren

Wanneer een fout is opgetreden, controleert u eerst of op het bedieningspaneel van de scanner of het scherm van het stuurprogramma meldingen worden weergegeven. Wanneer u hebt ingesteld dat u een e-mailmelding wilt ontvangen wanneer gebeurtenissen optreden, weet u snel wat de status is.

De communicatiestatus controleren

Controleer de communicatiestatus van de servercomputer of clientcomputer met behulp van een opdracht, zoals ping of ipconfig.

Verbindingstest

Voer een verbindingstest uit vanaf de scanner om de verbinding tussen de scanner en de mailserver te controleren. Controleer tevens de verbinding van de clientcomputer met de server om de communicatiestatus te controleren.

De instellingen initialiseren

Als uit de instellingen en de communicatiestatus geen problemen naar voren komen, kunnen de problemen mogelijk worden opgelost door de netwerkinstellingen van de scanner uit te schakelen of te initialiseren en de instellingen opnieuw te configureren.

Geen toegang tot Web Config

■ Het IP-adres is niet toegewezen aan de scanner.

Oplossingen

Mogelijk is geen geldig IP-adres toegewezen aan de scanner. Configureer het IP-adres via het bedieningspaneel van de scanner. U kunt de huidige instellingen controleren via het bedieningspaneel van de scanner.

■ De webbrowser ondersteunt de versleutelingssterkte voor SSL/TLS niet.

Oplossingen

SSL/TLS heeft de Codeersterkte. U kunt Web Config openen in een webbrowser die bulkversleuteling als volgt ondersteunt. Controleer of u een ondersteunde browser gebruikt.

80-bits: AES256/AES128/3DES

112-bits: AES256/AES128/3DES

128-bits: AES256/AES128

192-bits: AES256

256-bits: AES256

CA-ondertekend Certificaat is verlopen.

Oplossingen

Als er een probleem is met de vervaldatum van het certificaat, wordt het bericht "Het certificaat is verlopen" weergegeven wanneer verbinding wordt gemaakt met Web Config via SSL/TLS-communicatie (https). Als het bericht vóór de vervaldatum wordt weergegeven, moet u controleren of de datum van de scanner juist is geconfigureerd.

De algemene naam van het certificaat en de scanner komen niet overeen.

Oplossingen

Als de algemene naam van het certificaat en de scanner niet overeenkomen, wordt het bericht "De naam van het certificaat en de scanner komen niet overeen..." weergegeven wanneer u Web Config opent via SSL/TLS-communicatie (HTTPS). Dit gebeurt omdat de volgende IP-adressen niet overeen komen.

- Het IP-adres van de scanner dat is ingevoerd voor de algemene naam voor het maken van een Zelfondertekend certificaat of CSR.
- Het IP-adres dat is ingevoerd voor de webbrowser tijdens het uitvoeren van Web Config

Werk voor het Zelfondertekend certificaat het certificaat bij.

Haal voor CA-ondertekend Certificaat het certificaat opnieuw op voor de scanner.

De proxyserverinstelling of het lokale adres is niet ingesteld op de webbrowser.

Oplossingen

Wanneer de scanner is ingesteld voor het gebruik van een proxyserver, configureert u de webbrowser zodanig dat deze niet via de proxyserver verbinding maakt met het lokale adres.

- Windows:

Selecteer **Configuratiescherm > Netwerk en internet > Internetopties > Verbindingen > LAN-instellingen > Proxyserver** en stel vervolgens in dat de proxyserver niet moet worden gebruikt voor LAN (lokale adressen).

- Mac OS:

Selecteer **Systeemvoorkeuren (of Systeeminstellingen) > 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

DHCP is uitgeschakeld in de instellingen van de computer.

Oplossingen

Als de DHCP-functie voor het ophalen van een IP-adres automatisch is uitgeschakeld op de computer, hebt u geen toegang tot Web Config. Schakel DHCP in.

Voorbeeld voor Windows 10:

Open het bedieningspaneel en klik op **Netwerk en internet > Netwerkkentrum > Adapterinstellingen wijzigen**. Open het eigenschappenschermb van de gebruikte verbinding en open vervolgens het eigenschappenschermb voor **Internetprotocol versie 4 (TCP/IPv4)** of **Internetprotocol versie 6 (TCP/IPv6)**. Controleer of **Automatisch een IP-adres verkrijgen** is geselecteerd in het weergegeven scherm.

Weergave van het bedieningspaneel aanpassen

Presets opslaan. 69

Het startscherm van het bedieningspaneel bewerken. 71

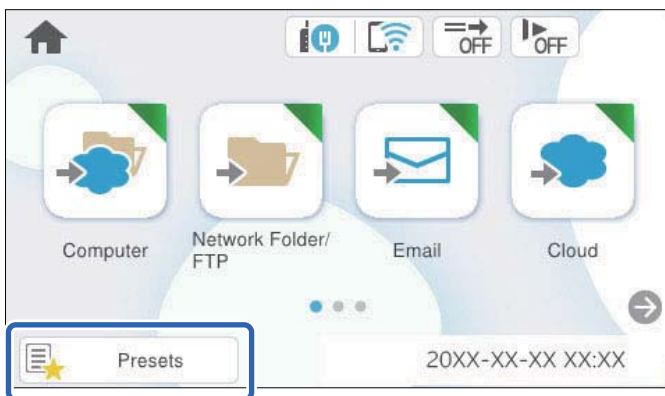
Presets opslaan

U kunt veelgebruikte scaninstellingen opslaan als **Presets**. U kunt maximaal 48 voorinstellingen opslaan.

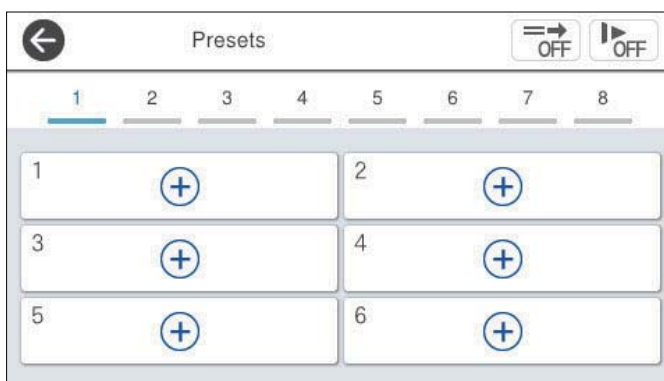
Opmerking:

- U kunt de huidige instellingen opslaan door  te selecteren in het startscherm voor scannen.
- U kunt **Presets** ook opslaan in Web Config.
Selecteer het tabblad **Scannen** > **Presets**.
- Als u **Scan naar computer** selecteert tijdens het opslaan, kunt u de taak die in Document Capture Pro is gemaakt, opslaan als **Presets**. Deze optie is alleen beschikbaar voor computers die met een netwerk zijn verbonden. Sla de taak van tevoren op in Document Capture Pro.
- Als de verificatiefunctie is ingeschakeld, kan alleen de beheerder **Presets** opslaan.

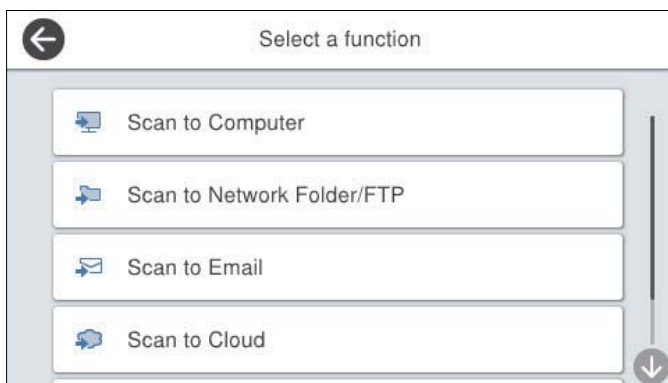
1. Selecteer **Presets** op het startscherm van het bedieningspaneel van de scanner.




2. Selecteer .



3. Selecteer het menu waarmee u een voorinstelling wilt opslaan.

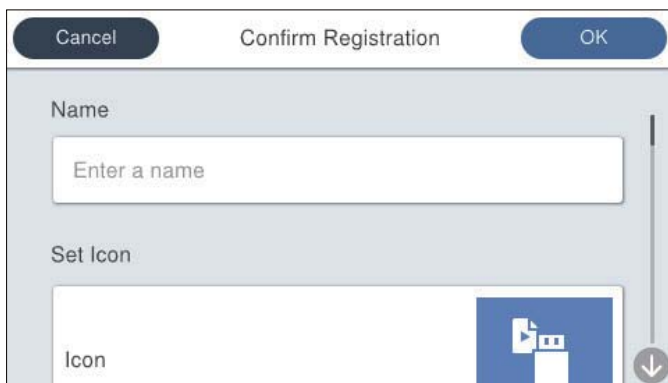


4. Stel elk item in en selecteer .

Opmerking:


Wanneer u **Scan naar computer** selecteert, moet u de computer selecteren waarop Document Capture Pro is geïnstalleerd. Selecteer vervolgens een opgeslagen taak. Deze optie is alleen beschikbaar voor computers die met een netwerk zijn verbonden.

5. Configureer de vooraf ingestelde instellingen.
 - Naam:** stel de naam in.
 - Pictogram instellen:** stel de afbeelding en kleur in voor het weer te geven pictogram.
 - Instelling Snel verzenden:** wanneer u de voorinstelling selecteert, kunt u meteen gaan scannen zonder dat u de bewerking hoeft te bevestigen.
 - Inhoud:** controleer de scaninstellingen.



6. Selecteer **OK**.

Menuopties van Presets

U kunt de instellingen van een voorinstelling wijzigen door  te selecteren in een voorinstelling.

Naam wijzigen:

Hiermee wijzigt u de naam van een voorinstelling.

Pictogram wijzigen:

Hiermee wijzigt u het pictogram en de kleur van een voorinstelling.

Instelling Snel verzenden:

Wanneer u de voorinstelling selecteert, kunt u meteen gaan scannen zonder dat u de bewerking hoeft te bevestigen.

Positie wijzigen:

Hiermee wijzigt u de volgorde van de voorinstellingen.

Wissen:

Hiermee verwijdert u de voorinstelling.

Pictogram toevoegen aan of verwijderen van Home:

Hiermee verwijdert u het pictogram van een voorinstelling van het startscherm of voegt u het eraan toe.

Details bevestigen:

Hiermee kunt u de instellingen van een voorinstelling bekijken. U kunt de voorinstelling laden door **Gebruik deze instelling** te selecteren.

Het startscherm van het bedieningspaneel bewerken

U kunt het startscherm aanpassen door **Instel.** > **Startscherm bewerken** te selecteren op het bedieningspaneel van de scanner.

- Indeling: hiermee wijzigt u de weergave van de menupictogrammen.
[“De Indeling van het startscherm wijzigen” op pagina 71](#)
- Pictogram toevoegen: hiermee kunt u pictogrammen toevoegen aan de **Presets** die u hebt geconfigureerd of pictogrammen herstellen die van het scherm zijn verwijderd.
[“Pictogram toevoegen” op pagina 72](#)
- Pictogram verwijderen: hiermee verwijdert u pictogrammen van het startscherm.
[“Pictogram verwijderen” op pagina 73](#)
- Pictogram verplaatsen: hiermee wijzigt u de volgorde van de pictogrammen.
[“Pictogram verplaatsen” op pagina 74](#)
- Standaard pictogramweergave herstellen: hiermee kunt u de standaardinstellingen voor het startscherm terugzetten.

De Indeling van het startscherm wijzigen

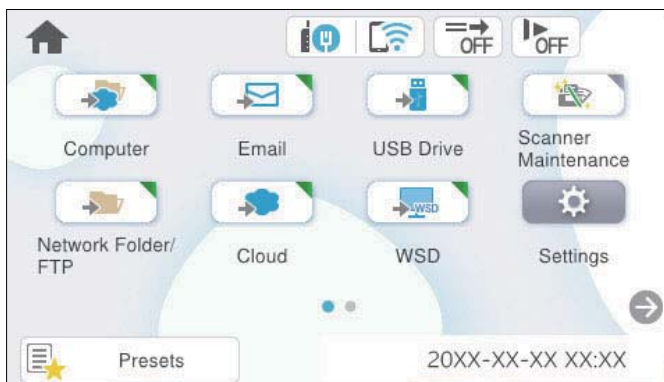
1. Selecteer **Instel.** > **Startscherm bewerken** > **Indeling** op het bedieningspaneel van de scanner.

2. Selecteer **Lijn** of **Matrix**.

Lijn:



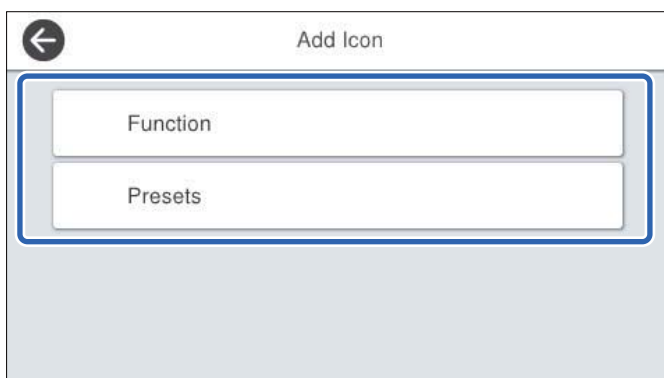
Matrix:



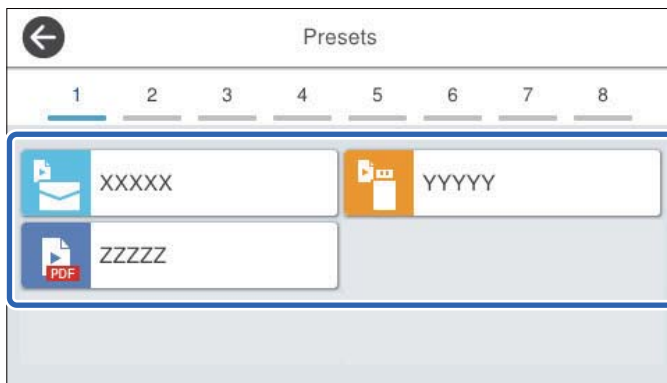
3. Selecteer  om terug te keren naar het startscherm en dit te controleren.

Pictogram toevoegen

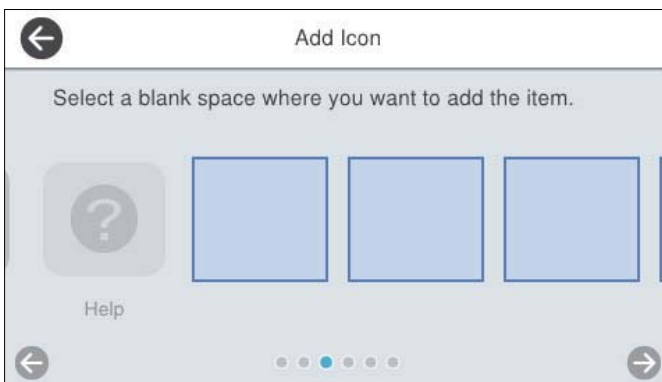
1. Selecteer **Instel.** > **Startscherm bewerken** > **Pictogram toevoegen** op het bedieningspaneel van de scanner.
2. Selecteer **Functie** of **Presets**.
 - Functie:** hiermee kunt u de standaardfuncties bekijken die op het startscherm worden weergegeven.
 - Presets:** hiermee geeft u de opgeslagen voorinstellingen weer.



3. Selecteer het item dat u aan het startscherm wilt toevoegen.



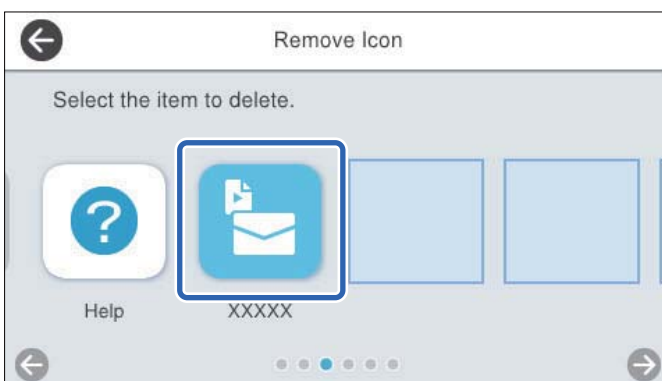
4. Selecteer de lege ruimte waar u het item wilt toevoegen.
Herhaal stap 3 en 4 om meer pictogrammen toe te voegen.




5. Selecteer  om terug te keren naar het startscherm en dit te controleren.

Pictogram verwijderen

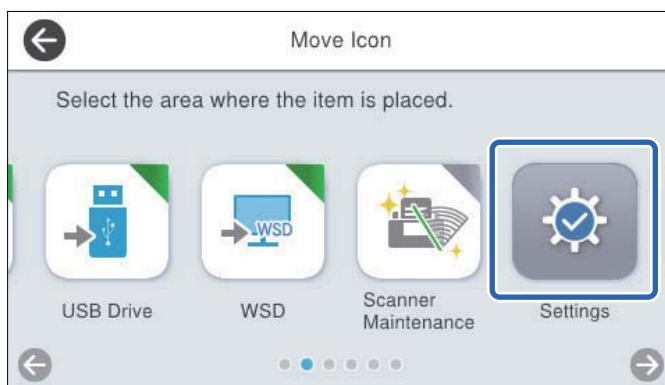
1. Selecteer **Instel.** > **Startscherm bewerken** > **Pictogram verwijderen** op het bedieningspaneel van de scanner.
2. Selecteer het pictogram dat u wilt verwijderen.



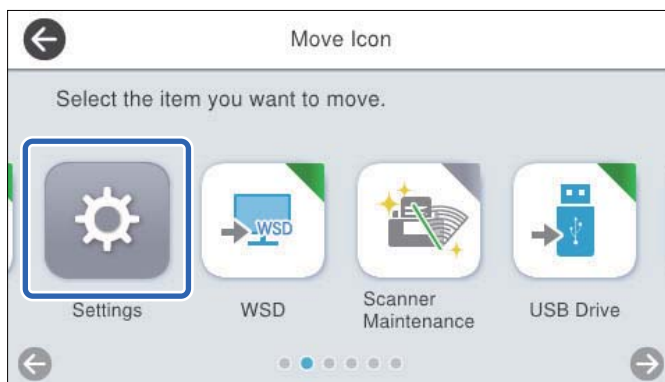
3. Selecteer **Ja** om de bewerking te voltooien.
Herhaal stap 2 en 3 om meer pictogrammen te verwijderen.
4. Selecteer  om terug te keren naar het startscherm en dit te controleren.

Pictogram verplaatsen

1. Selecteer **Instel.** > **Startscherm bewerken** > **Pictogram verplaatsen** op het bedieningspaneel van de scanner.
2. Selecteer het pictogram dat u wilt verplaatsen.



3. Selecteer het bestemmingskader.
Als in het bestemmingskader al een pictogram is ingesteld, wordt het pictogram vervangen.



4. Selecteer  om terug te keren naar het startscherm en dit te controleren.

Basisinstellingen voor beveiliging

Informatie over functies voor productbeveiliging.	76
Beheerdersinstellingen.	76
Beschikbare functies beperken (Toegangsbeheer).	82
De externe interface uitschakelen.	84
Programmaverificatie inschakelen bij opstarten.	85
Scannen via het netwerk vanaf de computer uitschakelen.	85
WSD-scanner in- of uitschakelen.	85
Een externe scanner beheren.	86
De standaardinstellingen herstellen.	88
Informatie over Epson Remote Services.	88
Problemen oplossen.	88

Informatie over functies voor productbeveiliging

In dit deel worden de beveiligingsfuncties van Epson-apparaten vermeld.

Funcienaam	Funcietype	Wat kunt u instellen?	Wat kunt u voorkomen?
Het beheerderswachtwoord configureren	Hiermee vergrendelt u de systeeminstellingen, zoals de verbindinginstelling voor netwerk of USB.	Een beheerder stelt een wachtwoord in voor het apparaat. U kunt dit instellen of wijzigen via zowel Web Config als het bedieningspaneel van de scanner.	Voorkom het illegaal lezen en wijzigen van de informatie die in het apparaat is opgeslagen, zoals id, wachtwoord, netwerkinstellingen enzovoort. Verminder daarnaast het aantal beveiligingsrisico's, zoals het lekken van gegevens voor de netwerkomgeving of het beveiligingsbeleid.
Instellingen toegangsbeheer	Als u op het apparaat inlogt met een gebruikersaccount dat vooraf is geregistreerd, kunt u het apparaat gebruiken.	Registreer een gebruikersaccount. U kunt maximaal 10 gebruikersaccounts registreren.	Door gebruikers te beperken, voorkomt u ongeoorloofd gebruik van het apparaat.
Instellingen voor externe interface	Hiermee beheert u de interface voor verbinding met het apparaat.	Schakel de USB-verbinding met de computer in of uit.	USB-verbinding met computer: hiermee voorkomt u ongeoorloofd gebruik van het apparaat doordat scannen alleen in het netwerk is toegestaan.

Gerelateerde informatie

- ➔ [“Het beheerderswachtwoord configureren” op pagina 76](#)
- ➔ [“De externe interface uitschakelen” op pagina 84](#)

Beheerdersinstellingen

Het beheerderswachtwoord configureren

Wanneer u een beheerderswachtwoord instelt, kunt u voorkomen dat gebruikers de systeembeheerinstellingen wijzigen. De standaardwaarden zijn af fabriek ingesteld. U kunt ze desgewenst wijzigen.

Opmerking:

Hieronder staan de standaardwaarden voor de beheerdersgegevens.

- Gebruikersnaam (alleen voor Web Config): geen (leeg)
- Wachtwoord: afhankelijk van het etiket op het product.

Als er een PASSWORD-etiket op de achterkant zit, voert u het achtcijferige getal in dat op het etiket staat. Als er geen “PASSWORD”-etiket op de scanner zit, voert u serienummer in als het oorspronkelijke beheerderswachtwoord. U vindt het serienummer op het etiket aan de achterkant van het product.

U kunt het beheerderswachtwoord wijzigen via Web Config, het bedieningspaneel van de scanner of Epson Device Admin. Raadpleeg de gebruikershandleiding of de Help van Epson Device Admin wanneer u Epson Device Admin gebruikt.

Het beheerderswachtwoord wijzigen via Web Config

Wijzig het beheerderswachtwoord in Web Config.

1. Open Web Config en selecteer het tabblad **Productbeveiliging > Beheerderswachtwoord wijzigen**.
2. Voer de benodigde informatie in bij **Huidig wachtwoord**, **Gebruikersnaam**, **Nieuw wachtwoord** en **Bevestig het nieuwe wachtwoord**.

Het nieuwe wachtwoord moet minimaal 8 en maximaal 20 tekens lang zijn en mag alleen alfanumerieke single-bytetekens en -symbolen bevatten.

Opmerking:

Hieronder staan de standaardwaarden voor de beheerdersgegevens.

- Gebruikersnaam: geen (leeg)*
- Wachtwoord: afhankelijk van het etiket op het product.*

Als er een PASSWORD-etiket op de achterkant zit, voert u het achtcijferige getal in dat op het etiket staat. Als er geen "PASSWORD"-etiket op de scanner zit, voert u serienummer in als het oorspronkelijke beheerderswachtwoord. U vindt het serienummer op het etiket aan de achterkant van het product.



Belangrijk:

Onthoud het ingestelde beheerderswachtwoord. Als u uw wachtwoord vergeet, kunt u dit niet opnieuw instellen en moet u hulp vragen aan een servicemedewerker.

3. Selecteer **OK**.

Gerelateerde informatie

➔ ["Web Config uitvoeren in een webbrowser"](#) op pagina 39

Het beheerderswachtwoord wijzigen op het bedieningspaneel van de scanner

U kunt het beheerderswachtwoord wijzigen via het bedieningspaneel van de scanner.

1. Selecteer **Instel.** op het bedieningspaneel van de scanner.
2. Selecteer **Systeembeheer > Beheerdersinstellingen**.
3. Selecteer **Beheerderswachtwoord > Wijzigen**.
4. Voer uw wachtwoord in.

Opmerking:

Het oorspronkelijke beheerderswachtwoord (standaard) op het moment van aankoop varieert afhankelijk van het etiket op het product. Als er een PASSWORD-etiket op de achterkant zit, voert u het achtcijferige getal in dat op het etiket staat. Als er geen "PASSWORD"-etiket op de scanner zit, voert u serienummer in als het oorspronkelijke beheerderswachtwoord. U vindt het serienummer op het etiket aan de achterkant van het product.

5. Voer uw nieuwe wachtwoord in.

Het nieuwe wachtwoord moet minimaal 8 en maximaal 20 tekens lang zijn en mag alleen alfanumerieke single-bytetekens en -symbolen bevatten.



Belangrijk:

Onthoud het ingestelde beheerderswachtwoord. Als u uw wachtwoord vergeet, kunt u dit niet opnieuw instellen en moet u hulp vragen aan een servicemedewerker.


6. Voer het nieuwe wachtwoord opnieuw in ter bevestiging.

Na afloop wordt een bericht over de voltooiing weergegeven.

Instelling vergrendelen gebruiken voor het bedieningspaneel

U kunt Instelling vergrendelen gebruiken om het bedieningspaneel te vergrendelen, zodat gebruikers de systeeminstellingen niet kunnen wijzigen.

Instelling vergrendelen instellen via het bedieningspaneel

1. Als u **Instelling vergrendelen** wilt uitschakelen nadat u de functie hebt ingeschakeld, tikt u op  in de rechterbovenhoek van het startscherm om in te loggen als beheerder.



Wordt niet weergegeven wanneer **Instelling vergrendelen** is uitgeschakeld. Ga naar de volgende stap als u deze functie wilt inschakelen.

2. Selecteer **Instel.**
3. Selecteer **Systeembeheer > Beheerdersinstellingen**.
4. Selecteer **Aan** of **Uit** bij **Instelling vergrendelen**.

Instelling vergrendelen instellen via Web Config

1. Selecteer het tabblad **Apparaatbeheer > Bedieningspaneel**.
2. Selecteer **Aan** of **Uit** als **Paneelvergrendeling**.
3. Klik op **OK**.

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser” op pagina 39](#)

Items voor Instelling vergrendelen in het menu Instel.


Dit is een lijst met items die met Instelling vergrendelen in het menu **Instel.** op het bedieningspaneel zijn vergrendeld.

✓: moet worden vergrendeld.

-: moet niet worden vergrendeld.

Menu Instel.		Instelling vergrendelen
Basisinstellingen		-
	Lcd-helderheid	-
	Geluiden	-
	Slaaptimer	✓
	Uitschakelingstimer	✓
	Direct inschakelen	✓
	Datum/tijd instellen	✓
	Taal/Language	✓/-*
	Toetsenbord (Afhankelijk van uw regio is deze functie mogelijk niet beschikbaar.)	-
	Time-out bewerking	✓
	PC-verbinding via USB	✓
Scannerinstellingen		-
	Langzaam	-
	Stoptiming voor dubbele toevoer	✓
	DFDS-functie	-
	Papierbescherming	✓
	Vuildetector	✓
	Ultrasone detectie dubbele toevoer	✓
	Time-out Automatische invoermodus	✓
	Ontvanger bevestigen	✓
Startscherm bewerken		✓
	Indeling	✓
	Pictogram toevoegen	✓
	Pictogram verwijderen	✓
	Pictogram verplaatsen	✓
	Standaard pictogramweergave herstellen	✓
Gebruikersinstellingen		✓


Menu Instel.		Instelling vergrendelen
	Netwerkmapp/FTP	✓
	E-mail	✓
	Cloud	✓
	USB-stick	✓
Netwerkinstellingen		✓
	Wi-Fi instellen	✓
	Bekabelde LAN-installatie	✓
	Netwerkstatus	✓
	Geavanceerd	✓
Webservice-instellingen		✓
	Epson Connect-services	✓
Document Capture Pro		-
	Instellingen wijzigen	✓
Contacten-beheer		-
	Registreren/Wissen	✓/!*
	Frequent	-
	Weergaveopties	-
	Zoekopties	-
Systeembeheer		✓
	Contacten-beheer	✓
	Beheerdersinstellingen	✓
	Beperkingen	✓
	Toegangsbeheer	✓
	Wachtwoordcodering	✓
	Klantonderzoek	✓
	WSD-instellingen	✓
	Standaardinst. herstellen	✓
	Firmware-update	✓
Apparaatgegevens		-

Menu Instel.		Instelling vergrendelen
	Serienummer	-
	Huidige versie	-
	Totaal aantal scans	-
	Aantal enkelzijdige scans	-
	Aantal dubbelzijdige scans	-
	Aantal scans van Draagblad	-
	Aantal scans na vervangen roller	-
	Aantal scans na Regelmatige reiniging	-
	Status verificatieapparaat	-
	Informatie Epson Open Platform	-
	 (Het aantal scans resetten)	✓
Onderhoud scanner		-
	Rolreiniging	-
	Vervanging onderhoudsroller	-
	Het aantal scans resetten	✓
	Vervangen	-
	Regelmatige reiniging	-
	Het aantal scans resetten	✓
	Reinigen	-
	Glas reinigen	-
Instelling waarschuwing rolvervanging		✓
	Inst. tellerwaarsch.	✓
Waarschuwinginstellingen standaardreiniging		✓
	Waarschuwinginst.	✓
	Inst. tellerwaarsch.	✓

* U kunt bij **Systeembeheer > Beperkingen** aangeven of het aanbrengen van wijzigingen is toegestaan.

Als beheerder inloggen op het bedieningspaneel

Wanneer **Instelling vergrendelen** is ingeschakeld, kunt u een van de volgende methoden gebruiken om via het bedieningspaneel van de scanner in te loggen.

1. Tik rechtsboven in het scherm op .
2. Wanneer het scherm **Selecteer gebruiker** wordt weergegeven, selecteert u **Beheerder**.
3. Voer het wachtwoord in om in te loggen.

Er wordt een bericht weergegeven dat het inloggen is voltooid en vervolgens wordt het startscherm op het bedieningspaneel weergegeven.

Als u wilt uitloggen, tikt u rechtsboven in het scherm op  of drukt u op de knop .

Beschikbare functies beperken (Toegangsbeheer)

U kunt gebruikers beperken door gebruikersaccounts op de scanner te registreren.

Wanneer Toegangsbeheer is ingeschakeld, kan de gebruiker scanfuncties gebruiken door het wachtwoord in te voeren op het bedieningspaneel van de scanner en in te loggen. Scannen is niet mogelijk zonder in te loggen.

U kunt scannen vanaf een computer door uw Gebruikersnaam en Wachtwoord te registreren in het scannerstuurprogramma (Epson Scan 2). Raadpleeg de Help van Epson Scan 2 of de *Gebruikershandleiding* van het product voor meer informatie over het configureren van instellingen.

Een gebruikersaccount maken

U kunt een Toegangsbeheer-account maken.

1. Open Web Config en selecteer vervolgens het tabblad **Productbeveiliging > Instellingen toegangsbeheer > Gebruikersinstellingen**.
2. Klik op **Toevoegen** voor het nummer dat u wilt registreren.

Belangrijk:

Wanneer u de scanner gebruikt met een verificatiesysteem van Epson of een ander bedrijf, registreert u de Gebruikersnaam bij Instellingen toegangsbeheer onder een nummer van 2 t/m 10.

Nummer 1 is bestemd voor toepassingssoftware zoals het verificatiesysteem, zodat de gebruikersnaam niet op het bedieningspaneel van de scanner wordt weergegeven.

3. Stel elk item in.
 - Gebruikersnaam:**
Voer de naam in die moet worden weergegeven in de gebruikerslijst. Gebruik minimaal 1 en maximaal 14 alfanumerieke tekens.
 - Wachtwoord:**
Voer een wachtwoord van maximaal 20 tekens in ASCII (0x20-0x7E) in. Laat dit veld leeg wanneer u het wachtwoord initialiseert.
 - Schakel het selectievakje in om elke functie in of uit te schakelen.
Selecteer **Scannen** als u de scanfuncties wilt toestaan.
4. Klik op **Toepassen**.

Een gebruikersaccount bewerken

U kunt het geregistreerde Toegangsbeheer-account bewerken.

1. Open Web Config en selecteer vervolgens het tabblad **Productbeveiliging** > **Instellingen toegangsbeheer** > **Gebruikersinstellingen**.
2. Klik op **Bewerken** voor het nummer dat u wilt bewerken.
3. Wijzig elk item.
4. Klik op **Toepassen**.

Een gebruikersaccount verwijderen

U kunt het geregistreerde Toegangsbeheer-account verwijderen.

1. Open Web Config en selecteer vervolgens het tabblad **Productbeveiliging** > **Instellingen toegangsbeheer** > **Gebruikersinstellingen**.
2. Klik op **Bewerken** voor het nummer dat u wilt verwijderen.
3. Klik op **Wissen**.



Belangrijk:

Wanneer u op **Wissen** klikt, wordt het gebruikersaccount verwijderd zonder dat een bevestiging wordt weergegeven. Let op wanneer u een account verwijdert.

De Toegangsbeheer inschakelen

Wanneer u Toegangsbeheer inschakelt, kan alleen de geregistreerde gebruiker de scanner gebruiken.

Opmerking:

Wanneer *Instellingen toegangsbeheer* is ingeschakeld, moet u de accountinformatie aan de gebruiker verstrekken.

1. Open Web Config en selecteer vervolgens het tabblad **Productbeveiliging** > **Instellingen toegangsbeheer** > **Basis**.
2. Selecteer **Schakelt toegangsbeheer in**.
Als u Instellingen toegangsbeheer inschakelt en wilt scannen vanaf een computer zonder verificatiegegevens, selecteert u **Afdrukken en scannen toestaan zonder verificatiegegevens van een computer**.
3. Klik op **OK**.

Inloggen op een scanner waarop Toegangsbeheer is ingeschakeld

Wanneer **Toegangsbeheer** is ingeschakeld, kunt u een van de volgende methoden gebruiken om via het bedieningspaneel van de scanner in te loggen.

1. Tik rechtsboven in het scherm op

2. Wanneer het scherm **Selecteer gebruiker** wordt weergegeven, selecteert u de gebruiker.

3. Voer het wachtwoord in om in te loggen.

Er wordt een bericht weergegeven dat het inloggen is voltooid en vervolgens wordt het startscherm op het bedieningspaneel weergegeven.

Als u wilt uitloggen, tikt u rechtsboven in het scherm op  of drukt u op de knop .

De externe interface uitschakelen

U kunt de interface die wordt gebruikt om het apparaat met de scanner te verbinden, uitschakelen. Configureer de beperkingsinstellingen om scannen via een andere methode dan het netwerk te beperken.

Opmerking:

U kunt de beperkingsinstellingen ook via het bedieningspaneel van de scanner configureren.

*PC-verbinding via USB: **Instel.** > **Basisinstellingen** > **PC-verbinding via USB***

1. Open Web Config en selecteer het tabblad **Productbeveiliging** > **Externe interface**.

2. Selecteer **Uitschakelen** voor de functies die u wilt instellen.

Selecteer **Inschakelen** wanneer u de controle wilt uitschakelen.

PC-verbinding via USB

U kunt het gebruik van de USB-verbinding vanaf de computer beperken. Als u dit wilt beperken, selecteert u **Uitschakelen**.

3. Klik op **OK**.

4. Controleer of de uitgeschakelde poort inderdaad niet kan worden gebruikt.

PC-verbinding via USB

Als de driver op de computer is geïnstalleerd

Sluit de scanner met een USB-kabel aan op de computer en controleer vervolgens of de scanner niet kan scannen.

Als de driver niet op de computer is geïnstalleerd

Windows:

Open Apparaatbeheer. Sluit de scanner met een USB-kabel aan op de computer en controleer of de inhoud van Apparaatbeheer ongewijzigd blijft.

Mac OS:

Sluit de scanner met een USB-kabel aan op de computer en controleer vervolgens of de printer niet kan worden toegevoegd via **Printers en scanners**.

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser” op pagina 39](#)

Programmaverificatie inschakelen bij opstarten

Als u de functie Programmaverificatie inschakelt, wordt tijdens het opstarten een verificatie uitgevoerd om te controleren of onbevoegde derden veranderingen aan het programma hebben aangebracht. Als er problemen worden gedetecteerd, start de scanner niet.

Opmerking:

Als u deze functie inschakelt, duurt het langer voordat de scanner is opgestart.

1. Open Web Config en selecteer vervolgens het tabblad **Productbeveiliging > Programmaverificatie bij opstarten**.

Opmerking:

U kunt instellingen ook configureren via het bedieningspaneel van de scanner.

Instel. > **Systeembeheer** > **Programmaverificatie bij opstarten**

2. Selecteer **Aan** om **Programmaverificatie bij opstarten** in te schakelen.
3. Klik op **OK**.

Scannen via het netwerk vanaf de computer uitschakelen

U kunt de volgende instellingen configureren bij Web Config om netwerkscannen met Epson Scan 2 vanaf uw computer uit te schakelen.

1. Open Web Config en selecteer vervolgens het tabblad **Scannen > Netwerkscan**.
2. Schakel bij **Epson Scan 2** het selectievakje **Scannen inschakelen** uit.
3. Klik op **Volgende**.
Het bevestigingsscherm voor de instelling wordt weergegeven.
4. Klik op **OK**.

WSD-scanner in- of uitschakelen

Opmerking:

*U kunt instellingen ook configureren via het bedieningspaneel van de scanner. Selecteer **Instel.** > **Systeembeheer** > **WSD-instellingen**.*

U kunt de WSD-scanner in- of uitschakelen.

Als u niet wilt dat de scanner als WSD-scanner wordt geconfigureerd, moet u de WSD-instellingen uitschakelen.

1. Open Web Config en selecteer vervolgens het tabblad **Netwerkbeveiliging > Protocol**.
2. Verander bij **WSD-instellingen** het selectievakje **WSD inschakelen**.

3. Klik op **Volgende**.

Het bevestigingsscherm voor de instelling wordt weergegeven.

4. Klik op **OK**.

Opmerking:

*Als de scanner nog steeds als een WSD-scanner wordt geconfigureerd, selecteert u het tabblad **Scannen** > **Netwerkscan** en schakelt u het selectievakje **Scannen inschakelen** bij **AirPrint** uit.*

Als AirPrint is uitgeschakeld, is scannen met Mopria via Chromebooks, Windows en de Mopria Scan-app ook uitgeschakeld.

Een externe scanner beheren

Informatie over een externe scanner controleren

Met Web Config kunt u de volgende informatie over de gebruikte scanner controleren via **Status**.

Productstatus

Hiermee controleert u de status, de cloudservice, het productnummer, het MAC-adres enzovoort.

Netwerkstatus

Hiermee controleert u de informatie van de netwerkverbindingstatus, het IP-adres, de DNS-server enzovoort.

Verbruik status

Hiermee controleert u de eerste dag van scannen, het aantal scans enzovoort.

Hardwarestatus

Hiermee controleert u de status van alle functies van de scanner.

Schermopname paneel

Hiermee kunt u een afbeelding bekijken van het scherm dat op het bedieningspaneel van de scanner is weergegeven.

E-mailmeldingen ontvangen bij gebeurtenissen

Over e-mailmeldingen

Dit is de meldingsfunctie waarmee, wanneer het scannen wordt onderbroken of een scannerfout optreedt, een e-mailbericht naar het opgegeven adres wordt gestuurd.

U kunt maximaal vijf bestemmingen invoeren en de meldingsinstellingen voor elke bestemming configureren.

Als u deze functie wilt gebruiken, moet u de mailserver instellen voordat u meldingen configureert.

Gerelateerde informatie

➔ [“Een mailserver registreren” op pagina 46](#)

E-mailmeldingen configureren

Configureer e-mailmeldingen met Web Config.

1. Open Web Config en selecteer het tabblad **Apparaatbeheer > E-mailmelding**.

2. Stel het onderwerp voor de e-mailmelding in.

Selecteer de inhoud die in het onderwerp wordt weergegeven uit de twee vervolgkeuzelijsten.

- De geselecteerde inhoud wordt weergegeven naast **Onderwerp**.
- U kunt niet links en rechts dezelfde inhoud instellen.
- Wanneer het aantal tekens bij **Locatie** groter is dan 32 byte, worden de tekens verwijderd waarmee de 32 byte wordt overschreden.

3. Voer het e-mailadres in voor het verzenden van de e-mailmelding.

Gebruik A-Z a-z 0-9 ! # \$ % & ' * + - . / = ? ^ _ { | } ~ @, en voer tussen 1 en 255 tekens in.

4. Selecteer de taal voor de e-mailmeldingen.

5. Schakel het selectievakje in voor de gebeurtenis waarvoor u een melding wilt ontvangen.

Het aantal **Meldingsinstellingen** is gekoppeld aan het aantal **E-mailadresinstellingen** voor het doel.

Voorbeeld:

Wanneer het papier in de printer op is en u een melding wilt verzenden naar het e-mailadres dat is ingesteld bij nummer 1 in **E-mailadresinstellingen**, schakelt u het selectievakje in bij kolom **1** op de regel **Beheerderswachtwoord gewijzigd**.

6. Klik op **OK**.

Controleer of een e-mailmelding wordt verzonden door de betreffende gebeurtenis na te bootsen.

Voorbeeld: Het beheerderswachtwoord is gewijzigd.

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser” op pagina 39](#)

Items voor e-mailmeldingen

Items	Instellingen en toelichting
Beheerderswachtwoord gewijzigd	Melding wanneer het beheerderswachtwoord is gewijzigd.
Scannerfout	Melding wanneer een scannerfout is opgetreden.
Wi-Fi-fout	Melding wanneer een fout is opgetreden in de LAN-interface voor draadloos netwerk.

De stroomtoevoer naar de scanner regelen met Web Config

Als uw computer zich niet in de buurt van de scanner bevindt, kunt u Web Config nog steeds gebruiken om de scanner uit te schakelen of opnieuw te starten.

1. Open Web Config en selecteer vervolgens het tabblad **Apparaatbeheer > Voeding**.
2. Selecteer **Uitschakelen** of **Opnieuw opstarten**.
3. Klik op **Uitvoeren**.

De standaardinstellingen herstellen

U kunt netwerkinstellingen of andere instellingen die de scanner zijn opgeslagen selecteren en deze terugzetten naar de standaardwaarden.

1. Open Web Config en selecteer vervolgens het tabblad **Apparaatbeheer > Standaardinstellingen herstellen**.

Opmerking:

U kunt instellingen ook configureren via het bedieningspaneel van de scanner.

Instel. > **Systeembeheer** > **Standaardinst. herstellen**

2. Selecteer de items die u wilt herstellen.
3. Klik op **Uitvoeren**.
Volg tot slot de instructies op het scherm.

Informatie over Epson Remote Services

Epson Remote Services is een service waarmee regelmatig via internet scannerinformatie wordt verzameld. Deze informatie kan worden gebruikt om te voorspellen wanneer verbruiksartikelen en onderdelen moeten worden vervangen of aangevuld en om fouten of problemen snel op te lossen.

Neem contact op met uw leverancier voor meer informatie over Epson Remote Services.

Problemen oplossen

Beheerderswachtwoord vergeten

U hebt hulp nodig van een servicemedewerker. Neem contact op met de lokale leverancier.

Opmerking:

Hieronder staan de beginwaarden voor de Web Config-beheerder.

- Gebruikersnaam: geen (leeg)*
- Wachtwoord: afhankelijk van het etiket op het product.*

Als er een PASSWORD-etiket op de achterkant zit, voert u het achtcijferige getal in dat op het etiket staat.

Als er geen "PASSWORD"-etiket op de scanner zit, voert u serienummer in als het oorspronkelijke beheerderswachtwoord. U vindt het serienummer op het etiket aan de achterkant van het product.

Als u het beheerderswachtwoord herstelt, wordt dit teruggezet naar de beginwaarde op het moment van aankoop.

Geavanceerde beveiligingsinstellingen

Beveiligingsinstellingen en voorkomen van gevaar.	90
Beheren met protocollen.	91
Een digitaal certificaat gebruiken.	94
SSL/TLS-communicatie met de scanner.	99
Versleutelde communicatie met IPsec/IP-filtering.	101
De scanner verbinden met een IEEE802.1X-netwerk.	111
Problemen met geavanceerd beveiliging oplossen.	113

Beveiligingsinstellingen en voorkomen van gevaar

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

Op scanners die niet zijn beschermd tegen toegang van buitenaf, is het mogelijk om via internet de contactpersonen in te zien die in de scanner zijn opgeslagen.

Om deze risico's te vermijden, zijn Epson-scanners uitgerust met allerlei beveiligingstechnologieën.

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

Naam	Functietype	Wat moet worden ingesteld	Wat moet worden voorkomen
Beheer van protocollen	Hiermee beheert u protocollen en services die worden gebruikt voor communicatie tussen scanners en computers, en schakelt u functies in en uit.	Een protocol dat of een service die wordt toegepast op afzonderlijk toegestane of verboden functies.	Beveiligingsrisico's als gevolg van onbedoeld gebruik verminderen door te voorkomen dat gebruikers onnodige functies kunnen gebruiken.
SSL/TLS-communicatie	De communicatie-inhoud wordt versleuteld met SSL/TLS-communicatie wanneer u vanaf de scanner toegang krijgt tot de Epson-server op internet, bijvoorbeeld tijdens communicatie met de computer via de webbrowser, gebruik van Epson Connect en het bijwerken van firmware.	Vraag een CA-ondertekend certificaat op en importeer dit naar de scanner.	Als u met een CA-ondertekend certificaat de identiteit van de scanner kunt aantonen, voorkomt u imitatie en ongeoorloofde toegang. Bovendien wordt communicatie-inhoud van SSL/TLS beveiligd en wordt het lekken van scan- en instellingsgegevens voorkomen.
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-pakketenheid beschermt (versleuteling en verificatie), kunt u veilig onbeveiligde protocollen communiceren.	Maak een basisbeleid en een afzonderlijk beleid om de toegang krijgen tot de scanner in te stellen.	Voorkom ongeoorloofde toegang, het ongewenst wijzigen van gegevens en het onderscheppen van communicatiegegevens naar de scanner.
IEEE 802.1X	Hiermee kunnen alleen geverifieerde gebruikers verbinding maken met het netwerk. Alleen een gebruiker met toestemming kan de scanner gebruiken.	Verificatie-instelling op de RADIUS-server (verificatieserver).	Voorkom ongeoorloofde toegang en ongeoorloofd gebruik van de scanner.

Gerelateerde informatie

- ➔ [“Beheren met protocollen” op pagina 91](#)
- ➔ [“SSL/TLS-communicatie met de scanner” op pagina 99](#)
- ➔ [“Versleutelde communicatie met IPsec/IP-filtering” op pagina 101](#)

➔ [“De scanner verbinden met een IEEE802.1X-netwerk” op pagina 111](#)

Instellingen van de beveiligingsfunctie

Wanneer u IPsec/IP-filtering of IEEE 802.1X instelt, is het raadzaam om Web Config via SSL/TLS te openen voor het doorgeven van instellingsgegevens om beveiligingsrisico's zoals fraude of onderschepping terug te dringen.

Configureer het beheerderswachtwoord voordat u IPsec/IP-filtering of IEEE 802.1X instelt.

Beheren met protocollen

U kunt scannen via verschillende paden en protocollen. U kunt netwerkscannen ook gebruiken vanaf een niet nader gespecificeerd aantal netwerkcomputers.

U kunt ondoelmatige beveiligingsrisico's verminderen door scannen vanaf specifieke paden te beperken of door de beschikbare functies te beheren.

Protocollen beheren

Configureer de protocolinstellingen die door de scanner worden ondersteund.

1. Open Web Config en selecteer vervolgens het tabblad **Netwerkbeveiliging** tab > **Protocol**.
2. Configureer elk item.
3. Klik op **Volgende**.
4. Klik op **OK**.

De instellingen worden toegepast op de scanner.

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser” op pagina 39](#)

Protocollen die u kunt inschakelen of uitschakelen

Protocol	Beschrijving
Bonjour-instellingen	U kunt opgeven of Bonjour moet worden gebruikt. Bonjour wordt gebruikt voor het zoeken van apparaten, scannen, enz.
SLP-instellingen	U kunt de SLP-functie in- of uitschakelen. SLP wordt gebruikt voor push-scan en netwerk zoeken in EpsonNet Config.
WSD-instellingen	U kunt de WSD-functie in- of uitschakelen. Wanneer deze optie is ingeschakeld, kunt u WSD-apparaten toevoegen en scannen via de WSD-poort.
LLTD-instellingen	U kunt de LLTD-functie in- of uitschakelen. Wanneer dit is ingeschakeld, wordt dit weergegeven in de Windows-netwerkmapp.

Protocol	Beschrijving
LLMNR-instellingen	U kunt de LLMNR-functie in- of uitschakelen. Wanneer deze optie is ingeschakeld, kunt u naamomzetting gebruiken zonder NetBIOS, zelfs als u DNS niet kunt gebruiken.
SNMPv1/v2c-instellingen	U kunt SNMPv1/v2c in- en uitschakelen. Dit wordt gebruikt voor het instellen van apparaten, bewaking enz.
SNMPv3-instellingen	U kunt SNMPv3 in- en uitschakelen. Dit wordt gebruikt voor het instellen van versleutelde apparaten, bewaking enz.

Protocolinstellingsitems

Bonjour-instellingen

Items	Instelwaarde en beschrijving
Bonjour gebruiken	Selecteer dit om apparaten te zoeken of gebruiken via Bonjour.
Bonjour-naam	Toont de Bonjour-naam.
Bonjour gebruikersnaam	Toont de Bonjour-servicenaam.
Locatie	Toont de Bonjour-locatiennaam.
Wide-Area Bonjour	Stel in of u Wide-Area Bonjour wilt gebruiken.

SLP-instellingen

Items	Instelwaarde en beschrijving
SLP inschakelen	Selecteer dit om de SLP-functie in te schakelen. Dit wordt bijvoorbeeld gebruikt voor netwerk zoeken in EpsonNet Config.

WSD-instellingen

Items	Instelwaarde en beschrijving
WSD inschakelen	Selecteer deze optie om apparaten die WSD gebruiken toe te voegen en om via de WSD-poort te scannen.
Time-out scan (sec)	Voer de time-outwaarde voor de communicatie voor WSD-scan in van 3 tot 3.600 seconden.
Apparaatnaam	Toont de WSD-apparaatnaam.
Locatie	Toont de WSD-locatiennaam.

LLTD-instellingen

Items	Instelwaarde en beschrijving
LLTD inschakelen	Selecteer dit om LLTD in te schakelen. De scanner wordt weergegeven in de Windows-netwerkmapp.

Items	Instelwaarde en beschrijving
Apparaatnaam	Toont de LLTD-apparaatnaam.

LLMNR-instellingen

Items	Instelwaarde en beschrijving
LLMNR inschakelen	Selecteer dit om LLMNR in te schakelen. U kunt naamomzetting gebruiken zonder NetBIOS, zelfs als u DNS niet kunt gebruiken.

SNMPv1/v2c-instellingen

Items	Instelwaarde en beschrijving
SNMPv1/v2c inschakelen	Selecteer dit om SNMPv1/v2c in te schakelen.
Toegangsmachtiging	Stel de toegangsmachtiging in wanneer SNMPv1/v2c is ingeschakeld. Selecteer Alleen lezen of Lezen/schrijven .
Communitynaam (alleen lezen)	Voer 0 tot 32 ASCII-teken (0x20 tot 0x7E) in.
Communitynaam (lezen/schrijven)	Voer 0 tot 32 ASCII-teken (0x20 tot 0x7E) in.

SNMPv3-instellingen

Items	Instelwaarde en beschrijving
SNMPv3 inschakelen	SNMPv3 wordt ingeschakeld wanneer het selectievakje wordt ingeschakeld.
Gebruikersnaam	Voer tussen 1 en 32 tekens in. Gebruik 1-bits tekens.
Verificatie-instellingen	
Algoritme	Selecteer een algoritme voor een verificatie voor SNMPv3.
Wachtwoord	Voer het wachtwoord in voor een verificatie voor SNMPv3. Voer tussen 8 en 32 tekens in ASCII (0x20–0x7E) in. Als u dit niet opgeeft, laat u dit leeg.
Wachtwoord bevestigen	Voer het geconfigureerde wachtwoord in ter bevestiging.
Codeerinstellingen	
Algoritme	Selecteer een algoritme voor een versleuteling voor SNMPv3.
Wachtwoord	Voer het wachtwoord in voor een versleuteling voor SNMPv3. Voer tussen 8 en 32 tekens in ASCII (0x20–0x7E) in. Als u dit niet opgeeft, laat u dit leeg.
Wachtwoord bevestigen	Voer het geconfigureerde wachtwoord in ter bevestiging.

Items	Instelwaarde en beschrijving
Contextnaam	Voer maximaal 32 tekens in Unicode (UTF-8) in. Als u dit niet opgeeft, laat u dit leeg. Het aantal tekens dat kan worden ingevoerd, varieert afhankelijk van de taal.

Een digitaal certificaat gebruiken

Digitale certificering

CA-ondertekend Certificaat

Dit is een certificaat dat door de CA (certificeringsinstantie) is ondertekend. U kunt dit aanvragen bij de certificeringsinstantie. Met dit certificaat wordt het bestaan van de scanner bevestigd. Daarnaast wordt het gebruikt voor SSL/TLS-communicatie, zodat de veiligheid van uw datacommunicatie is gewaarborgd.

Wanneer het wordt gebruikt voor SSL/TLS-communicatie, doet het dienst als servercertificaat

Wanneer het is ingesteld op IPsec/IP-filtering of IEEE 802.1X-communicatie, doet het dienst als clientcertificaat.

CA-certificaat

Dit is een certificaat in de ketting van het CA-ondertekend Certificaat en wordt ook wel het tussenliggende CA-certificaat genoemd. Het wordt door de webbrowser gebruikt om het pad van het scannercertificaat te valideren bij toegang tot de server van de andere partij of Web Config.

Voor het CA-certificaat: stel in wanneer het pad van het servercertificaat moet worden gevalideerd bij toegang vanaf de scanner. Voor de scanner: stel certificering van het pad van het CA-ondertekend Certificaat voor een SSL/TLS-verbinding in.

U kunt het CA-certificaat van de scanner opvragen bij de certificeringsinstantie die het CA-certificaat heeft afgegeven.

U kunt het CA-certificaat dat wordt gebruikt voor validatie van de server van de andere partij ook opvragen bij de certificeringsinstantie die het CA-ondertekend Certificaat van de andere server heeft afgegeven.

Zelfondertekend certificaat

Dit is een certificaat dat door de scanner zelf wordt ondertekend en uitgegeven. Dit wordt ook wel het basiscertificaat genoemd. Omdat de uitgever zichzelf certificeert, is het niet betrouwbaar en kan imitatie niet worden voorkomen.

Gebruik het tijdens het configureren van de beveiligingsinstellingen en het uitvoeren van eenvoudige SSL/TLS-communicatie zonder het CA-ondertekend Certificaat.

Als u dit certificaat voor SSL/TLS-communicatie gebruikt, kan in de webbrowser een beveiligingswaarschuwing worden weergegeven, omdat het certificaat niet bij de webbrowser is geregistreerd. U kunt het Zelfondertekend certificaat alleen gebruiken voor SSL/TLS-communicatie.

Gerelateerde informatie

- ➔ [“Een CA-ondertekend Certificaat configureren” op pagina 95](#)
- ➔ [“Een zelfondertekend certificaat bijwerken” op pagina 98](#)
- ➔ [“Een CA-certificaat configureren” op pagina 99](#)

Een CA-ondertekend Certificaat configureren

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 het tabblad **Netwerkbeveiliging**. Selecteer vervolgens **SSL/TLS > Certificaat of IPsec/IP-filter > Clientcertificaat of IEEE802.1X > Clientcertificaat**.

Ongeacht de keuze kunt u hetzelfde certificaat ophalen en algemeen gebruiken.

2. Klik op **Genereren** 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 de tab **Netwerkbeveiliging**. Selecteer vervolgens **SSL/TLS > Certificaat of IPsec/IP-filter > Clientcertificaat of IEEE802.1X > Clientcertificaat**.

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-ondertekend Certificaat mogelijk niet importeren.

7. Stuur de CSR naar een certificeringsinstantie. Daarmee vraagt u een door een CA-ondertekend Certificaat aan. Volg de regels van de desbetreffende certificeringsinstantie voor de wijze van verbinding en de vorm.

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

Het verkrijgen van een CA-ondertekend Certificaat is voltooid zodra u een certificaat opslaat op een bestemming.

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser”](#) op pagina 39

Instellingen voor een CSR

Items	Instellingen en toelichting
Sleutellengte	Selecteer een sleutellengte voor een CSR.
Algemene naam	<p>U kunt tussen 1 en 128 tekens invoeren. Als dit een IP-adres is, moet het een statisch IP-adres zijn. U kunt 1 tot 5 IPv4-adressen, IPv6-adressen, hostnamen, FQDN's invoeren. Scheid deze met komma's.</p> <p>Het eerste element wordt opgeslagen als de algemene naam. Andere elementen worden opgeslagen in het aliasveld van de certificaathouder.</p> <p>Voorbeeld:</p> <p>IP-adres van de scanner: 192.0.2.123, scannernaam: EPSONA1B2C3</p> <p>Algemene naam: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123</p>
Organisatie/ Organisatorische eenheid/ Plaats/ Staat/provincie	U kunt tussen 0 en 64 tekens in ASCII (0x20–0x7E) invoeren. U kunt de distinguished-namen (CN) met een komma scheiden.
Land	Voer een landcode in. Gebruik een tweecijferige code conform ISO-3166.
E-mailadres afzender	U kunt het e-mailadres van de afzender invoeren bij de e-mailserverinstelling. Voer hetzelfde e-mailadres in als bij E-mailadres afzender op het tabblad Netwerk > E-mailserver > Basis .

Een door een CA ondertekend certificaat importeren

Importeer het verkregen CA-ondertekend Certificaat naar de scanner.



Belangrijk:

- Zorg ervoor dat de datum en tijd van de scanner goed zijn ingesteld. Het certificaat is mogelijk ongeldig.
- 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 het tabblad **Netwerkbeveiliging**. Selecteer vervolgens **SSL/TLS > Certificaat of IPsec/IP-filter > Clientcertificaat of IEEE802.1X > Clientcertificaat**.

2. Klik op **Importeren**

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

3. Voer voor elk item een waarde in. Stel **CA-certificaat 1** en **CA-certificaat 2** in wanneer u het pad naar het certificaat verifieert vanuit de webbrowser die toegang geeft tot de scanner.

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
 - Persoonlijke sleutel:** niet configureren. De scanner bevat een persoonlijke sleutel.
 - Wachtwoord:** niet configureren.
 - CA-certificaat 1/CA-certificaat 2:** optioneel

- Een certificaat met de indeling PEM/DER afkomstig van een computer
 - Persoonlijke sleutel:** Wel instellen.
 - Wachtwoord:** niet configureren.
 - CA-certificaat 1/CA-certificaat 2:** optioneel
- Een certificaat met de indeling PKCS#12 afkomstig van een computer
 - Persoonlijke sleutel:** niet configureren.
 - Wachtwoord:** optioneel
 - CA-certificaat 1/CA-certificaat 2:** Niet configureren.

4. Klik op **OK**.

Na afloop wordt een bericht over voltooiing weergegeven.

Opmerking:

Klik op **Bevestigen** om de certificaatgegevens te controleren.

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser” op pagina 39](#)

Instellingsitems voor het importeren van door een CA ondertekende certificaten

Items	Instellingen en toelichting
Servercertificaat of Clientcertificaat	Selecteer een certificaatindeling. Voor een SSL/TLS-verbinding wordt het Servercertificaat weergegeven. Voor IPsec/IP-filtering of IEEE 802.1X wordt het Clientcertificaat weergegeven.
Persoonlijke sleutel	Als u een certificaat met een PEM/DER-indeling ophaalt met een CSR dat op een computer is gemaakt, moet u een privé sleutelbestand opgeven dat overeenkomt met een certificaat.
Wachtwoord	Als de bestandsindeling Certificaat met persoonlijke sleutel (PKCS#12) is, voert u het wachtwoord in voor versleuteling van de privé sleutel die wordt toegepast wanneer u het certificaat ophaalt.
CA-certificaat 1	Als uw certificaat de indeling Certificaat (PEM/DER) heeft, importeert u een certificaat van een certificeringsinstantie die CA-ondertekend Certificaat uitgeeft dat als servercertificaat wordt gebruikt. Geef indien nodig een bestand op.
CA-certificaat 2	Als uw certificaat de indeling Certificaat (PEM/DER) heeft, importeert u een certificaat van een certificeringsinstantie die CA-certificaat 1 uitgeeft. Geef indien nodig een bestand op.

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 het tabblad **Netwerkbeveiliging**. Selecteer vervolgens **SSL/TLS > Certificaat of IPsec/IP-filter > Clientcertificaat of IEEE802.1X > Clientcertificaat**.
2. Klik op **Wissen**.
3. Bevestig dat u het certificaat in het weergegeven bericht wilt verwijderen.

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser” op pagina 39](#)

Een zelfondertekend certificaat bijwerken

Omdat het Zelfondertekend certificaat door de scanner wordt uitgegeven, kunt u dit vernieuwen wanneer het is verlopen of wanneer de omschreven inhoud wordt gewijzigd.

1. Open Web Config en selecteer het tabblad **Netwerkbeveiliging** tab > **SSL/TLS > Certificaat**.
2. Klik op **Update**.
3. Voer de **Algemene naam** in.

U kunt tot 5 IPv4-adressen, IPv6-adressen, hostnamen, FQDN's tussen 1 en 128 tekens invoeren. Scheid deze met komma's. De eerste parameter wordt opgeslagen als de algemene naam. De overige elementen worden opgeslagen in het aliasveld van het certificaat.

Voorbeeld:

IP-adres van de scanner: 192.0.2.123, naam scanner: EPSONA1B2C3

Algemene naam: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123

4. Geef een geldigheidsperiode op voor het certificaat.
5. Klik op **Volgende**.
Er wordt een bevestiging weergegeven.
6. Klik op **OK**.
De scanner wordt bijgewerkt.

Opmerking:

U kunt de certificaatgegevens controleren op het tabblad **Netwerkbeveiliging > SSL/TLS > Certificaat > Zelfondertekend certificaat**. Klik tenslotte op **Bevestigen**.

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser” op pagina 39](#)

Een CA-certificaat configureren

Wanneer u het CA-certificaat instelt, kunt u het pad verifiëren naar het CA-certificaat van de server waartoe de scanner toegang krijgt. Hiermee kan imitatie worden voorkomen.

U kunt het CA-certificaat ophalen bij de certificeringsinstantie waar het CA-ondertekend Certificaat is uitgegeven.

Een CA-certificaat importeren

Importeer het CA-certificaat naar de scanner.

1. Open Web Config en selecteer vervolgens het tabblad **Netwerkbeveiliging > CA-certificaat**.
2. Klik op **Importeren**.
3. Geef het CA-certificaat op dat u wilt importeren.
4. Klik op **OK**.

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

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser” op pagina 39](#)

Een CA-certificaat verwijderen

U kunt een geïmporteerd CA-certificaat verwijderen.

1. Open Web Config en selecteer vervolgens het tabblad **Netwerkbeveiliging > CA-certificaat**.
2. Klik op **Wissen** naast het CA-certificaat dat u wilt verwijderen.
3. Bevestig dat u het certificaat in het weergegeven bericht wilt verwijderen.
4. Klik op **Netwerk opnieuw opstarten** en controleer of het verwijderde CA-certificaat niet in het bijgewerkte scherm wordt weergegeven.

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser” op pagina 39](#)

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.

Basale SSL/TLS-instellingen configureren

Als de scanner HTTPS-servers ondersteunt, kunt u de communicatie versleutelen met SSL/TLS. U kunt de scanner met Web Config in een beveiligde omgeving configureren en beheren.

Configureer de sterkte van de versleuteling en de omleidingsfunctie.

1. Open Web Config en selecteer het tabblad **Netwerkbeveiliging** > **SSL/TLS** > **Basis**.
2. Selecteer voor elk item een waarde.
 - Codeersterkte
Selecteer de sterkte van de versleuteling.
 - HTTP omleiden naar HTTPS
Stel in dat een omleiding naar HTTPS plaatsvindt bij het openen van HTTP.
3. Klik op **Volgende**.
Er wordt een bevestiging weergegeven.
4. Klik op **OK**.
De scanner wordt bijgewerkt.

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser”](#) op pagina 39

Een servercertificaat voor de scanner configureren

1. Open Web Config en selecteer het tabblad **Netwerkbeveiliging** > **SSL/TLS** > **Certificaat**.
2. Geef bij **Servercertificaat** op welk certificaat u wilt gebruiken.
 - Zelfondertekend certificaat
Een zelfondertekend certificaat is gegenereerd door de scanner. Selecteer deze optie als u geen certificaat gebruikt dat door een CA is ondertekend.
 - CA-ondertekend Certificaat
U kunt ook een door een CA ondertekend certificaat aanvragen en dit importeren.
3. Klik op **Volgende**.
Er wordt een bevestiging weergegeven.
4. Klik op **OK**.
De scanner wordt bijgewerkt.

Gerelateerde informatie

- ➔ [“Web Config uitvoeren in een webbrowser”](#) op pagina 39
- ➔ [“Een CA-ondertekend Certificaat configureren”](#) op pagina 95
- ➔ [“Een CA-certificaat configureren”](#) op pagina 99

Versleutelde communicatie met IPsec/IP-filtering

Over IPsec/IP-filter

Met de functie voor IPsec/IP-filtering kunt u verkeer filteren dat is gebaseerd op IP-adressen, services en poorten. 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.

Opmerking:

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

Standaardbeleid configureren

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.

1. Open Web Config en selecteer vervolgens het tabblad **Netwerkbeveiliging > IPsec/IP-filter > Basis**.
2. Voer voor elk item een waarde in.
3. Klik op **Volgende**.
Er wordt een bevestiging weergegeven.
4. Klik op **OK**.
De scanner wordt bijgewerkt.

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser” op pagina 39](#)

Instellingen voor Standaard beleid

Standaard beleid

Items	Instellingen en toelichting
IPsec/IP-filter	U de functie IPsec/IP-filtering in- of uitschakelen.

Toegangsbeheer

Hiermee bepaalt u hoe het IP-verkeer wordt beheerd.

Items	Instellingen en toelichting
Toegang toestaan	Selecteer deze optie om de geconfigureerde IP-pakketten door te laten.
Toegang weigeren	Selecteer deze optie om de geconfigureerde IP-pakketten te weigeren.
IPsec	Selecteer deze optie om de geconfigureerde IPsec-pakketten door te laten.

IKE-versie

Selecteer **IKEv1** of **IKEv2** als **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-versie**.

Items	Instellingen en toelichting
Verificatiemethode	Als u Certificaat wilt gebruiken, moet u op voorhand een door een CA ondertekend certificaat aanvragen en importeren.
Vooraf gedeelde sleutel	Als u Vooraf gedeelde sleutel selecteert bij Verificatiemethode , voer dan een vooraf gedeelde sleutel in van minimaal 1 en maximaal 127 tekens.
Vooraf gedeelde sleutel bevestigen	Voer de geconfigureerde sleutel in ter bevestiging.

IKEv2

De volgende items worden weergegeven wanneer u **IKEv2** selecteert voor **IKE-versie**.

Items	Instellingen en toelichting	
Lokaal	Verificatiemethode	Als u Certificaat wilt gebruiken, moet u op voorhand een door een CA ondertekend certificaat aanvragen en importeren.
	ID-type	Als u Vooraf gedeelde sleutel selecteert als Verificatiemethode , selecteert u 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. Eenduidige naam: voer 1 tot 255 1-byte ASCII-tekens (0x20 tot 0x7E) in. U moet "=" gebruiken. IP-adres: voer IPv4- of IPv6-indeling in. FQDN: voer een combinatie van 1 tot 255 tekens in. Gebruik A-Z, a-z, 0-9, - en "" E-mailadres: voer 1 tot 255 1-byte ASCII-tekens (0x20 tot 0x7E) in. U moet "@" gebruiken. Toets ID: voer 1 tot 255 1-byte ASCII-tekens (0x20 tot 0x7E) in.
	Vooraf gedeelde sleutel	Als u Vooraf gedeelde sleutel selecteert bij Verificatiemethode , voer dan een vooraf gedeelde sleutel in van minimaal 1 en maximaal 127 tekens.
	Vooraf gedeelde sleutel bevestigen	Voer de geconfigureerde sleutel in ter bevestiging.

Items		Instellingen en toelichting
Extern	Verificatiemethode	Als u Certificaat wilt gebruiken, moet u op voorhand een door een CA ondertekend certificaat aanvragen en importeren.
	ID-type	Als u Vooraf gedeelde sleutel selecteert als Verificatiemethode , selecteert u het id-type voor 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. Eenduidige naam: voer 1 tot 255 1-byte ASCII-teken (0x20 tot 0x7E) in. U moet "=" gebruiken. IP-adres: voer IPv4- of IPv6-indeling in. FQDN: voer een combinatie van 1 tot 255 tekens in. Gebruik A-Z, a-z, 0-9, - en " ". E-mailadres: voer 1 tot 255 1-byte ASCII-teken (0x20 tot 0x7E) in. U moet "@" gebruiken. Toets ID: voer 1 tot 255 1-byte ASCII-teken (0x20 tot 0x7E) in.
	Vooraf gedeelde sleutel	Als u Vooraf gedeelde sleutel selecteert bij Verificatiemethode , voer dan een vooraf gedeelde sleutel in van minimaal 1 en maximaal 127 tekens.
	Vooraf gedeelde sleutel bevestigen	Voer de geconfigureerde sleutel in ter bevestiging.

Inkapseling

Als u **IPsec** selecteert bij **Toegangsbeheer**, moet u een vorm van inkapseling configureren.

Items	Instellingen en toelichting
Transportmodus	Selecteer deze optie als u de scanner alleen gebruikt in hetzelfde LAN. IP-pakketten van laag 4 of hoger worden versleuteld.
Tunnelmodus	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. Externe gateway (Tunnelmodus): als u Tunnelmodus selecteert bij Inkapseling , voer dan een gatewayadres in van minimaal 1 en maximaal 39 tekens.

Beveiligingsprotocol

Als u **IPsec** selecteert bij **Toegangsbeheer**, moet u een optie selecteren.

Items	Instellingen en toelichting
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.

❑ Algoritme-instellingen

Het wordt aanbevolen **Alle** te selecteren voor alle instellingen, of om een andere optie dan **Alle** te selecteren voor elke instelling. Als u **Alle** selecteert voor een aantal instellingen en een andere optie dan **Alle** selecteert voor de andere instellingen, communiceert het apparaat mogelijk niet, afhankelijk van het andere apparaat dat u wilt verifiëren.

Items		Instellingen en toelichting
IKE	Codering	Selecteer het versleutelingsalgoritme voor IKE. De items variëren afhankelijk van de IKE-versie.
	Verificatie	Selecteer het verificatiealgoritme voor IKE.
	Toetsuitwisseling	Selecteer het sleuteluitwisselingsalgoritme voor IKE. De items variëren afhankelijk van de IKE-versie.
ESP	Codering	Selecteer het versleutelingsalgoritme voor ESP. Dit is beschikbaar wanneer ESP is geselecteerd voor Beveiligingsprotocol .
	Verificatie	Selecteer het verificatiealgoritme voor ESP. Dit is beschikbaar wanneer ESP is geselecteerd voor Beveiligingsprotocol .
AH	Verificatie	Selecteer het versleutelingsalgoritme voor AH. Dit is beschikbaar wanneer AH is geselecteerd voor Beveiligingsprotocol .

Groepsbeleid configureren

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.

1. Open Web Config en selecteer vervolgens het tabblad **Netwerkbeveiliging > IPsec/IP-filter > Basis**.
2. Klik op een genummerd tabblad dat u wilt configureren.
3. Voer voor elk item een waarde in.
4. Klik op **Volgende**.
Er wordt een bevestiging weergegeven.
5. Klik op **OK**.
De scanner wordt bijgewerkt.

Instellingen voor Groepsbeleid

Items	Instellingen en toelichting
Dit Groepsbeleid inschakelen	Hiermee schakelt u het groepsbeleid in of uit.

Toegangsbeheer

Hiermee bepaalt u hoe het IP-verkeer wordt beheerd.

Items	Instellingen en toelichting
Toegang toestaan	Selecteer deze optie om de geconfigureerde IP-pakketten door te laten.
Toegang weigeren	Selecteer deze optie om de geconfigureerde IP-pakketten te weigeren.
IPsec	Selecteer deze optie om de geconfigureerde IPsec-pakketten door te laten.

Lokaal adres (scanner)

Selecteer een IPv4-adres of een IPv6-adres dat overeenkomt met uw netwerkomgeving. Als er automatisch een IP-adres wordt toegewezen, kunt u **Automatisch verkregen IPv4-adres gebruiken** gebruiken.

Opmerking:

Als een IPv6-adres automatisch wordt toegewezen, is de verbinding mogelijk niet beschikbaar. Configureer een statisch IPv6-adres.

Extern adres (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.

Methode van poortkeuze

Hiermee bepaalt u hoe de poorten worden opgegeven.

- Servicenaam

Als u **Servicenaam** selecteert bij **Methode van poortkeuze**, moet u een optie selecteren.

- Transportprotocol

Als u **Poortnummer** selecteert bij **Methode van poortkeuze**, moet u een vorm van inkapseling configureren.

Items	Instellingen en toelichting
Elk 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.

- Lokale poort

Als u **Poortnummer** selecteert voor **Methode van poortkeuze** en **TCP** of **UDP** selecteert voor **Transportprotocol**, 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.

Externe poort

Als u **Poortnummer** selecteert voor **Methode van poortkeuze** en **TCP** of **UDP** selecteert voor **Transportprotocol**, 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-versie

Selecteer **IKEv1** of **IKEv2** als **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-versie**.

Items	Instellingen en toelichting
Verificatiemethode	Als u IPsec selecteert bij Toegangsbeheer , moet u een optie selecteren. Het gebruikte certificaat is gelijk aan dat van het standaardbeleid.
Vooraf gedeelde sleutel	Als u Vooraf gedeelde sleutel selecteert bij Verificatiemethode , voer dan een vooraf gedeelde sleutel in van minimaal 1 en maximaal 127 tekens.
Vooraf gedeelde sleutel bevestigen	Voer de geconfigureerde sleutel in ter bevestiging.

IKEv2

De volgende items worden weergegeven wanneer u **IKEv2** selecteert voor **IKE-versie**.

Items		Instellingen en toelichting
Lokaal	Verificatiemethode	Als u IPsec selecteert bij Toegangsbeheer , moet u een optie selecteren. Het gebruikte certificaat is gelijk aan dat van het standaardbeleid.
	ID-type	Als u Vooraf gedeelde sleutel selecteert als Verificatiemethode , selecteert u 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. Eenduidige naam: voer 1 tot 255 1-byte ASCII-tekens (0x20 tot 0x7E) in. U moet "=" gebruiken. IP-adres: voer IPv4- of IPv6-indeling in. FQDN: voer een combinatie van 1 tot 255 tekens in. Gebruik A–Z, a–z, 0–9, - en " ". E-mailadres: voer 1 tot 255 1-byte ASCII-tekens (0x20 tot 0x7E) in. U moet "@" gebruiken. Toets ID: voer 1 tot 255 1-byte ASCII-tekens (0x20 tot 0x7E) in.
	Vooraf gedeelde sleutel	Als u Vooraf gedeelde sleutel selecteert bij Verificatiemethode , voer dan een vooraf gedeelde sleutel in van minimaal 1 en maximaal 127 tekens.
	Vooraf gedeelde sleutel bevestigen	Voer de geconfigureerde sleutel in ter bevestiging.
Extern	Verificatiemethode	Als u IPsec selecteert bij Toegangsbeheer , moet u een optie selecteren. Het gebruikte certificaat is gelijk aan dat van het standaardbeleid.
	ID-type	Als u Vooraf gedeelde sleutel selecteert als Verificatiemethode , selecteert u het id-type voor 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. Eenduidige naam: voer 1 tot 255 1-byte ASCII-tekens (0x20 tot 0x7E) in. U moet "=" gebruiken. IP-adres: voer IPv4- of IPv6-indeling in. FQDN: voer een combinatie van 1 tot 255 tekens in. Gebruik A–Z, a–z, 0–9, - en " ". E-mailadres: voer 1 tot 255 1-byte ASCII-tekens (0x20 tot 0x7E) in. U moet "@" gebruiken. Toets ID: voer 1 tot 255 1-byte ASCII-tekens (0x20 tot 0x7E) in.
	Vooraf gedeelde sleutel	Als u Vooraf gedeelde sleutel selecteert bij Verificatiemethode , voer dan een vooraf gedeelde sleutel in van minimaal 1 en maximaal 127 tekens.
	Vooraf gedeelde sleutel bevestigen	Voer de geconfigureerde sleutel in ter bevestiging.

Inkapseling

Als u **IPsec** selecteert bij **Toegangsbeheer**, moet u een vorm van inkapseling configureren.

Items	Instellingen en toelichting
Transportmodus	Selecteer deze optie als u de scanner alleen gebruikt in hetzelfde LAN. IP-pakketten van laag 4 of hoger worden versleuteld.
Tunnelmodus	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. Externe gateway (Tunnelmodus): als u Tunnelmodus selecteert bij Inkapseling , voer dan een gatewayadres in van minimaal 1 en maximaal 39 tekens.

Beveiligingsprotocol

Als u **IPsec** selecteert bij **Toegangsbeheer**, moet u een optie selecteren.

Items	Instellingen en toelichting
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.

Algoritme-instellingen

Het wordt aanbevolen **Alle** te selecteren voor alle instellingen, of om een andere optie dan **Alle** te selecteren voor elke instelling. Als u **Alle** selecteert voor een aantal instellingen en een andere optie dan **Alle** selecteert voor de andere instellingen, communiceert het apparaat mogelijk niet, afhankelijk van het andere apparaat dat u wilt verifiëren.

Items	Instellingen en toelichting	
IKE	Codering	Selecteer het versleutelingsalgoritme voor IKE. De items variëren afhankelijk van de IKE-versie.
	Verificatie	Selecteer het verificatiealgoritme voor IKE.
	Toetsuitwisseling	Selecteer het sleuteluitwisselingsalgoritme voor IKE. De items variëren afhankelijk van de IKE-versie.
ESP	Codering	Selecteer het versleutelingsalgoritme voor ESP. Dit is beschikbaar wanneer ESP is geselecteerd voor Beveiligingsprotocol .
	Verificatie	Selecteer het verificatiealgoritme voor ESP. Dit is beschikbaar wanneer ESP is geselecteerd voor Beveiligingsprotocol .
AH	Verificatie	Selecteer het versleutelingsalgoritme voor AH. Dit is beschikbaar wanneer AH is geselecteerd voor Beveiligingsprotocol .

Combinatie van Lokaal adres (scanner) en Extern adres (host) op Groepsbeleid

	Instelling van Lokaal adres (scanner)		
		IPv4	IPv6* ²

Instelling van Extern adres (host)	IPv4* ¹	✓	–	✓
	IPv6* ¹ , * ²	–	✓	✓
	Leeg	✓	✓	✓

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

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

*3 Met uitzondering van IPv6 lokaal gekoppelde adressen.

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser” op pagina 39](#)

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
Alle	–	–	–	Alle diensten
ENPC	UDP	3289	Willekeurige poort	Een scanner zoeken vanuit toepassingen als Epson Device Admin en het scannerstuurprogramma
SNMP	UDP	161	Willekeurige poort	MIB-informatie verzamelen en configureren vanuit toepassingen als Epson Device Admin en het Epson-scannerstuurprogramma
WSD	TCP	Willekeurige poort	5357	WSD beheren
WS-Discovery	UDP	3702	Willekeurige poort	WSD-scanners zoeken
Network Scan	TCP	1865	Willekeurige poort	Gescande gegevens doorsturen vanuit Document Capture Pro
Network Push Scan	TCP	Willekeurige poort	2968	Taakinformatie ophalen voor push-scans vanuit Document Capture Pro
Network Push Scan Discovery	UDP	2968	Willekeurige poort	Een computer zoeken vanaf de scanner
FTP-gegevens (extern)	TCP	Willekeurige poort	20	FTP-client (gescande gegevens doorsturen) Hiermee kan echter alleen een FTP-server worden beheerd die externe poort 20 gebruikt.
FTP-beheer (extern)	TCP	Willekeurige poort	21	FTP-client (doorsturen van gescande gegevens beheren)

Servicenaam	Protocoltype	Nummer lokale poort	Nummer externe poort	Gecontroleerde kenmerken
CIFS (extern)	TCP	Willekeurige poort	445	CIFS-client (gescande gegevens doorsturen naar een map)
NetBIOS Name Service (extern)	UDP	Willekeurige poort	137	CIFS-client (gescande gegevens doorsturen naar een map)
NetBIOS Datagram Service (extern)	UDP	Willekeurige poort	138	
NetBIOS Session Service (extern)	TCP	Willekeurige poort	139	
HTTP (lokaal)	TCP	80	Willekeurige poort	HTTP(S)-server (gegevens van Web Config en WSD doorsturen)
HTTPS (lokaal)	TCP	443	Willekeurige poort	
HTTP (extern)	TCP	Willekeurige poort	80	HTTP(S)-client (firmware en basiscertificaat bijwerken)
HTTPS (extern)	TCP	Willekeurige poort	443	

Configuratievoorbeelden van IPsec/IP-filter

Alleen IPsec-pakketten ontvangen

Dit voorbeeld is alleen voor configuratie van een standaardbeleid.

Standaard beleid:

- IPsec/IP-filter: **Inschakelen**
- Toegangsbeheer: **IPsec**
- Verificatiemethode: **Vooraf gedeelde sleutel**
- Vooraf gedeelde sleutel: voer hier maximaal 127 tekens in.

Groepsbeleid: niet configureren.

Scangegevens en scannerinstellingen ontvangen

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

Standaard beleid:

- IPsec/IP-filter: **Inschakelen**
- Toegangsbeheer: **Toegang weigeren**

Groepsbeleid:

- Dit Groepsbeleid inschakelen: schakel het selectievakje in.
- Toegangsbeheer: **Toegang toestaan**
- Extern adres (host): het IP-adres van een client

Methode van poortkeuze: Servicenaam

Servicenaam: schakel het selectievakje in bij **ENPC, SNMP, HTTP (lokaal), HTTPS (lokaal)** en **Network Scan**.

Alleen toegang vanaf een bepaald IP-adres toestaan

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

Standaard beleid:

IPsec/IP-filter: Inschakelen

Toegangsbeheer: Toegang weigeren

Groepsbeleid:

Dit Groepsbeleid inschakelen: schakel het selectievakje in.

Toegangsbeheer: Toegang toestaan

Extern adres (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 voor IPsec/IP-filtering configureren

Configureer het cliencertificaat voor IPsec/IP-filtering. Wanneer u het certificaat instelt, kunt u het gebruiken als verificatiemethode voor IPsec/IP-filtering. Als u de certificeringsinstantie wilt configureren, gaat u naar **CA-certificaat**.

1. Open Web Config en selecteer vervolgens het tabblad **Netwerkbeveiliging > IPsec/IP-filter > Clientcertificaat**.
2. Importeer het certificaat in **Clientcertificaat**.

Als u al een certificaat hebt geïmporteerd dat door een certificeringsinstantie is gepubliceerd, kunt u het certificaat kopiëren en in het IPsec/IP-filter gebruiken. Selecteer het certificaat in **Kopiëren van** en klik vervolgens op **Kopiëren** om het te kopiëren.

Gerelateerde informatie

- ➔ [“Web Config uitvoeren in een webbrowser”](#) op pagina 39
- ➔ [“Een CA-ondertekend Certificaat configureren”](#) op pagina 95
- ➔ [“Een CA-certificaat configureren”](#) op pagina 99

De scanner verbinden met een IEEE802.1X-netwerk

Een IEEE 802.1X-netwerk configureren

Wanneer u op de scanner IEEE 802.1X instelt, kunt u dit gebruiken op het netwerk dat is verbonden met een RADIUS-server, een LAN-switch met verificatiefunctie of een toegangspunt.

1. Open Web Config en selecteer vervolgens het tabblad **Netwerkbeveiliging > IEEE802.1X > Basis**.
2. Voer voor elk item een waarde in.
 Als u de scanner wilt gebruiken in een Wi-Fi-netwerk, klikt u op **Wi-Fi instellen** en selecteert u een SSID of voert u deze in.
Opmerking:
U kunt de instellingen delen tussen Ethernet en Wi-Fi.
3. Klik op **Volgende**.
 Er wordt een bevestiging weergegeven.
4. Klik op **OK**.
 De scanner wordt bijgewerkt.

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser” op pagina 39](#)

Instellingsitems voor een IEEE802.1X-netwerk

Items	Instellingen en toelichting	
IEEE802.1X (bekabeld LAN)	U kunt instellingen in- en uitschakelen op de pagina (IEEE802.1X > Basis) voor IEEE802.1X (bekabeld LAN).	
IEEE802.1X (Wi-Fi)	De verbindingstatus van IEEE802.1X (Wi-Fi) wordt weergegeven.	
Verbindingsmethode	De verbindingmethode van een actief netwerk wordt weergegeven.	
EAP-type	Selecteer een verificatiemethode tussen de scanner en een RADIUS-server.	
	EAP-TLS	U moet een CA-ondertekend certificaat ophalen en importeren.
	PEAP-TLS	
	PEAP/MSCHAPv2	U moet een wachtwoord configureren.
EAP-TTLS		
Gebruikers-ID	Configureer een id voor verificatie van een RADIUS-server. Voer 1 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in.	
Wachtwoord	Configureer een wachtwoord voor verificatie van de scanner. Voer 1 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in. Als u een Windows-server als RADIUS-server gebruikt, kunt u maximaal 127 tekens invoeren.	
Wachtwoord bevestigen	Voer het geconfigureerde wachtwoord in ter bevestiging.	
Server-ID	U kunt een server-id configureren voor verificatie met een opgegeven RADIUS-server. Authenticator controleert of een server-ID voorkomt in het Subject/SubjectAltName-veld van een servercertificaat dat door een RADIUS-server is verzonden. Voer 0 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in.	

Items	Instellingen en toelichting	
Certificaatvalidatie (bekabeld LAN)	Als u Certificaatvalidatie wilt uitvoeren met IEEE802.1X (bekabeld LAN) , selecteert u Inschakelen . Zie de gerelateerde informatie en importeer het CA-certificaat als u Inschakelen selecteert. Certificaatvalidatie is altijd ingeschakeld bij IEEE802.1X (Wi-Fi). Importeer het CA-certificaat.	
Anonieme naam	Als u PEAP-TLS of PEAP/MSCHAPv2 selecteert bij EAP-type , kunt u een anonieme naam in plaats van een gebruikers-id instellen voor fase 1 van een PEAP-verificatie. Voer 0 tot 128 1-byte ASCII-teken (0x20 tot 0x7E) in.	
Codeersterkte	U kunt een van de volgende opties selecteren.	
	Hoog	AES256/3DES
	Midden	AES256/3DES/AES128/RC4

Gerelateerde informatie

➔ [“Een CA-certificaat configureren” op pagina 99](#)

Een certificaat voor IEEE 802.1X configureren

Configureer het cliencertificaat voor IEEE802.1X. Wanneer u het instelt, kunt u **EAP-TLS** en **PEAP-TLS** gebruiken al verificatiemethode van IEEE 802.1X. Als u het certificaat van de certificeringsinstantie wilt configureren, gaat u naar **CA-certificaat**.

1. Open Web Config en selecteer vervolgens het tabblad **Netwerkbeveiliging > IEEE802.1X > Clientcertificaat**.
2. Voer een certificaat in bij **Clientcertificaat**.

Als u al een certificaat hebt geïmporteerd dat door een certificeringsinstantie is gepubliceerd, kunt u het certificaat kopiëren en in IEEE802.1X gebruiken. Selecteer het certificaat in **Kopiëren van** en klik vervolgens op **Kopiëren** om het te kopiëren.

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser” op pagina 39](#)

Problemen met geavanceerd beveiliging oplossen

De beveiligingsinstellingen herstellen

Wanneer u een hoog beveiligde omgeving configureert, bijv. IPsec/IP-filtering, 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 met Web Config

U kunt IPsec/IP-filter uitschakelen met Web Config.

1. Open Web Config en selecteer het tabblad **Netwerkbeveiliging > IPsec/IP-filter > Basis**.
2. Schakel de optie **IPsec/IP-filter** uit.

Problemen met het gebruik van netwerkbeveiligingsfuncties

Een vooraf gedeelde sleutel vergeten

Configureer een vooraf gedeelde sleutel opnieuw.

Als u de sleutel wilt wijzigen, opent u Web Config en selecteert u het tabblad **Netwerkbeveiliging > IPsec/IP-filter > Basis > Standaard beleid** of **Groepsbeleid**.

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

Gerelateerde informatie

- ➔ [“Web Config uitvoeren in een webbrowser” op pagina 39](#)
- ➔ [“Versleutelde communicatie met IPsec/IP-filtering” op pagina 101](#)

Geen communicatie mogelijk met IPsec-communicatie

Geef het algoritme op dat niet wordt ondersteund door de scanner of de computer.

De scanner ondersteunt de volgende algoritmen. Controleer de instellingen van de computer.

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 Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30*
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 101](#)

Plotseling geen communicatie mogelijk

Het IP-adres van de scanner is gewijzigd of kan niet worden gebruikt.

Wanneer het IP-adres dat als het lokale adres is geregistreerd bij Groepsbeleid is gewijzigd of kan niet worden gebruikt, is IPsec-communicatie niet mogelijk. 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 (tabblad **Netwerkbeveiliging** > **IPsec/IP-filter** > **Basis** > **Groepsbeleid** > **Lokaal adres (scanner)**) van de scanner mogelijk niet gevonden.

Gebruik een statisch IP-adres.

Het IP-adres van de computer is gewijzigd of kan niet worden gebruikt.

Wanneer het IP-adres dat als het externe adres is geregistreerd bij Groepsbeleid is gewijzigd of kan niet worden gebruikt, is IPsec-communicatie niet mogelijk.

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 (tabblad **Netwerkbeveiliging** > **IPsec/IP-filter** > **Basis** > **Groepsbeleid** > **Extern adres (host)**) van de scanner mogelijk niet gevonden.

Gebruik een statisch IP-adres.

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser” op pagina 39](#)

➔ [“Versleutelde communicatie met IPsec/IP-filtering” op pagina 101](#)

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

De instellingen voor IPsec/IP-filtering zijn incorrect.

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 101](#)

Geen toegang tot het apparaat na het configureren van IEEE 802.1X

De instellingen voor IEEE 802.1X zijn onjuist.

Schakel IEEE 802.1X en wifi uit op het bedieningspaneel van de scanner. Verbind de scanner en een computer en configureer IEEE 802.1X opnieuw.

Gerelateerde informatie

➔ [“Een IEEE 802.1X-netwerk configureren” op pagina 111](#)

Problemen met het gebruik van een digitaal certificaat

Kan geen CA-ondertekend Certificaat importeren

CA-ondertekend Certificaat en de informatie op de CSR komen niet overeen.

Als het CA-ondertekend Certificaat en de CSR niet dezelfde gegevens bevatten, kan de CSR niet worden geïmporteerd. Controleer de volgende punten:

- Probeer 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.

CA-ondertekend Certificaat is groter dan 5 kB.

Een CA-ondertekend Certificaat dat groter is dan 5 kB kan niet worden geïmporteerd.

Het wachtwoord voor het importeren van het certificaat is onjuist.

Voer het juiste wachtwoord in. Als u het wachtwoord niet meer weet, kunt u het certificaat niet importeren. Haal het CA-ondertekend Certificaat opnieuw op.

Gerelateerde informatie

➔ [“Een door een CA ondertekend certificaat importeren” op pagina 96](#)

Zelfondertekend certificaat kan niet worden bijgewerkt

De Algemene naam is niet ingevoerd.

Er moet een **Algemene naam** worden ingevoerd.

Er zijn niet-ondersteunde tekens ingevoerd voor Algemene naam.

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

De algemene naam bevat een komma of een spatie.

Als een komma is ingevoerd, wordt de **Algemene naam** 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 98](#)

CSR kan niet worden gemaakt

De Algemene naam is niet ingevoerd.

Er moet een **Algemene naam** worden ingevoerd.

Er zijn niet-ondersteunde tekens ingevoerd voor Algemene naam, Organisatie, Organisatorische eenheid, Plaats of Staat/provincie.

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

De Algemene naam bevat een komma of een spatie.

Als een komma is ingevoerd, wordt de **Algemene naam** 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 95](#)

Er wordt een waarschuwing over een digitaal certificaat weergegeven

Berichten	Oorzaak/Wat doen
Voer een Servercertificaat in.	<p>Oorzaak:</p> <p>U hebt geen bestand geselecteerd om te importeren.</p> <p>Wat doen:</p> <p>Selecteer een bestand en klik op Importeren.</p>
CA-certificaat 1 is niet ingevoerd.	<p>Oorzaak:</p> <p>CA-certificaat 1 is niet ingevoerd. Alleen CA-certificaat 2 is ingevoerd.</p> <p>Wat doen:</p> <p>Importeer eerst CA-certificaat 1.</p>
Ongeldige waarde hieronder.	<p>Oorzaak:</p> <p>Het bestandspad en/of wachtwoord bevat(ten) tekens die niet mogen worden gebruikt.</p> <p>Wat doen:</p> <p>Gebruik de juiste tekens voor het item.</p>
Ongeldige datum en tijd.	<p>Oorzaak:</p> <p>De datum en tijd van de scanner zijn niet ingesteld.</p> <p>Wat doen:</p> <p>Stel de datum en tijd in met Web Config of EpsonNet Config.</p>
Ongeldig wachtwoord.	<p>Oorzaak:</p> <p>Het ingevoerde wachtwoord is niet gelijk aan het wachtwoord dat is ingesteld voor het CA-certificaat.</p> <p>Wat doen:</p> <p>Voer het juiste wachtwoord in.</p>

Berichten	Oorzaak/Wat doen
Ongeldig bestand.	<p>Oorzaak:</p> <p>U importeert geen certificaatbestand in de indeling X509.</p> <p>Wat doen:</p> <p>Selecteer het juiste certificaat dat afkomstig is van een vertrouwde certificeringsinstantie.</p>
	<p>Oorzaak:</p> <p>Het bestand dat u hebt geïmporteerd, is te groot. De bestandsgrootte is maximaal 5 kB.</p> <p>Wat doen:</p> <p>Als u het juiste bestand hebt geselecteerd, is het certificaat mogelijk beschadigd of vals.</p>
	<p>Oorzaak:</p> <p>De keten in het certificaat is ongeldig.</p> <p>Wat doen:</p> <p>Zie de website van de certificeringsinstantie voor meer informatie over certificaten.</p>
Kan geen Servercertificaten gebruiken die meer dan drie CA-certificaten bevatten.	<p>Oorzaak:</p> <p>Het certificaatbestand in de indeling PKCS#12 bevat meer dan drie CA-certificaten.</p> <p>Wat doen:</p> <p>Importeer elk certificaat door conversie van PKCS#12 in PEM of importeer het certificaatbestand in de indeling PKCS#12 (maximaal twee CA-certificaten).</p>
Het Certificaat is verlopen. Controleer of het Certificaat geldig is of controleer de datum en tijd op het product.	<p>Oorzaak:</p> <p>Het certificaat is vervallen.</p> <p>Wat doen:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Als het certificaat vervallen is, moet u een nieuw certificaat aanvragen en importeren. <input type="checkbox"/> Als het certificaat niet vervallen is, zorg er dan voor dat de datum en tijd van de scanner goed zijn ingesteld.
Persoonlijke sleutel vereist.	<p>Oorzaak:</p> <p>Er is geen private sleutel aan het certificaat gekoppeld.</p> <p>Wat doen:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Als het certificaat de indeling PEM/DER heeft en is verkregen met een CSR en een computer, geef dan het sleutelbestand op. <input type="checkbox"/> 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.
	<p>Oorzaak:</p> <p>U hebt het PEM/DER-certificaat dat is verkregen met een CSR en Web Config opnieuw geïmporteerd.</p> <p>Wat doen:</p> <p>Als het certificaat de indeling PEM/DER heeft en is verkregen met een CSR en Web Config, kunt u het maar eenmaal importeren.</p>

Berichten	Oorzaak/Wat doen
Setup mislukt.	<p>Oorzaak:</p> <p>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.</p> <p>Wat doen:</p> <p>Controleer het opgegeven bestand en de communicatie en importeer het bestand opnieuw.</p>

Gerelateerde informatie

➔ [“Digitale certificering” op pagina 94](#)

Door CA ondertekend bestand per ongeluk verwijderd

Er is geen back-upbestand voor het CA-ondertekende 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 importeren” op pagina 96](#)

➔ [“Een door een CA ondertekend certificaat verwijderen” op pagina 97](#)

Epson Open Platform gebruiken

Overzicht van Epson Open Platform.	121
Epson Open Platform configureren.	121
Epson Open Platform valideren.	121

Overzicht van Epson Open Platform

Epson Open Platform is een platform waarmee u verificatiesystemen met deze scanner kunt gebruiken.

Het platform kan worden gebruikt met Epson Print Admin (Epson-verificatiesysteem) of een verificatiesysteem van een externe leverancier. U kunt logboeken per apparaat en gebruiker opvragen, apparaten configureren die gebruikers en groepen kunnen gebruiken, limieten instellen voor functies, enzovoort.

Als u een verificatieapparaat koppelt, kunt u ook gebruikersverificatie uitvoeren met de id-kaart.

Epson Open Platform configureren

Schakel Epson Open Platform in, zodat u het apparaat vanuit het verificatiesysteem kunt gebruiken.

1. Vraag een productcode aan via de speciale website.
Raadpleeg de handleiding van Epson Open Platform voor meer informatie over hoe u bijvoorbeeld de productcode ophaalt.
2. Open Web Config en selecteer vervolgens het tabblad **Epson Open Platform > Productsleutel of Licentiecode**.
3. Controleer elk item en stel ze in.
 - Serienummer
Het serienummer van het apparaat wordt weergegeven.
 - Versie Epson Open Platform
Selecteer de versie van Epson Open Platform. De overeenkomstige versie verschilt afhankelijk van het verificatiesysteem.
 - Productsleutel of Licentiecode
Voer de verkregen productcode in.
4. Klik op **Volgende**.
Het bevestigingsscherm voor de instelling wordt weergegeven.
5. Klik op **OK**.
De instellingen worden toegepast op de scanner.

Opmerking:

U kunt Epson Print Admin Serverless niet gebruiken wanneer het systeem is synchroniseerd met Epson Open Platform.

Epson Open Platform valideren

U kunt de geldigheid van Epson Open Platform op de volgende manieren controleren.

- Web Config
Er is een productsleutel ingevoerd op het tabblad **Epson Open Platform > Productsleutel of Licentiecode > Productsleutel of Licentiecode**. Het tabblad **Epson Open Platform > Verificatiesysteem** wordt links in de menustructuur weergegeven.

- Bedieningspaneel van de scanner

Controleer of de productcode wordt weergegeven bij **Instel.** > **Apparaatgegevens** > **Informatie Epson Open Platform.**

Een verificatieapparaat aansluiten

Het verificatieapparaat aansluiten.	124
Bedieningscontrole voor verificatieapparaat.	124
Controleren of de verificatiekaart is herkend.	124
Problemen met het verificatieapparaat oplossen.	125

Het verificatieapparaat aansluiten

Opmerking:

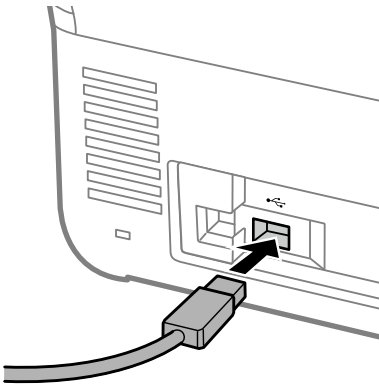
Een verificatieapparaat wordt gebruikt wanneer een verificatiesysteem in gebruik is.



Belangrijk:

Wanneer u het verificatieapparaat meerdere scanners wilt aansluiten, moet u een product met hetzelfde modelnummer gebruiken.

Sluit de USB-kabel van de kaartlezer aan op de USB-poort van de scanner voor externe interfaces.



Bedieningscontrole voor verificatieapparaat

U kunt de verbindingstatus en verificatiekaartherkenning voor het verificatieapparaat controleren via het bedieningspaneel van de scanner.

Als u **Instel.** > **Apparaatgegevens** > **Status verificatieapparaat** selecteert, wordt informatie weergegeven.

Controleren of de verificatiekaart is herkend

U kunt controleren of verificatiekaarten kunnen worden herkend met Web Config.

1. Open Web Config en selecteer vervolgens het tabblad **Apparaatbeheer** > **Kaartlezer**.
2. Houd de verificatiekaart boven de verificatiekaartlezer.
3. Klik op **Controleren**.

Het resultaat wordt weergegeven.

Problemen met het verificatieapparaat oplossen

Kan de verificatiekaart niet lezen

Controleer het volgende.

- Controleer of het verificatieapparaat correct op de scanner is aangesloten.
 - Sluit het verificatieapparaat aan op de USB-poort voor externe interfaces aan de achterzijde van de scanner.
- Controleer of het verificatieapparaat en de verificatiekaart zijn gecertificeerd.
 - Neem contact op met uw dealer voor informatie over ondersteunde verificatie-apparaten en -kaarten.

Onderhoud

De buitenzijde van de scanner schoonmaken.	127
De binnenzijde van de scanner schoonmaken.	127
De rollerset vervangen.	132
Het aantal scans opnieuw instellen na vervanging van de rollen.	137
Energiebesparing.	138
De scanner vervoeren.	138
Een back-up maken van de instellingen.	139
Standaardinst. herstellen.	140
Toepassingen en firmware bijwerken.	141


De buitenzijde van de scanner schoonmaken

Veeg met een droge doek of een vochtige doek met een mild reinigingsmiddel en water eventuele vlekken van de behuizing.



Belangrijk:

- Maak de scanner nooit schoon met alcohol, thinner of bijtende oplosmiddelen. Er kan vervorming of kleurverandering optreden.*
- Zorg ervoor dat er geen water in het apparaat komt. Hierdoor kan een storing optreden.*
- Verwijder nooit de behuizing van de scanner.*

1. Druk op de knop  om de scanner uit te schakelen.
2. Koppel de lichtnetadapter los van de scanner.
3. Maak de behuizing schoon met water met een mild schoonmaakmiddel.

Opmerking:

Veeg het touchscreen af met een zachte, droge doek.

De binnenzijde van de scanner schoonmaken

Nadat u de scanner een tijdje hebt gebruikt, kunnen papierstof en stof uit de omgeving op de rol of het glas in de scanner problemen veroorzaken bij de papierinvoer of kwaliteitsproblemen opleveren bij de gescande afbeeldingen. Reinig de binnenzijde van de scanner elke 5,000 scans.


U kunt de recentste tellerstand voor het aantal scans controleren op het bedieningspaneel of in Epson Scan 2 Utility.

Als het oppervlak is vervuild met een moeilijk te verwijderen materiaal, gebruikt u een originele Epson-reinigingsset om de vlekken te verwijderen. Gebruik een beperkte hoeveelheid reinigingsmiddel op de reinigingsdoek om de vlekken te verwijderen.

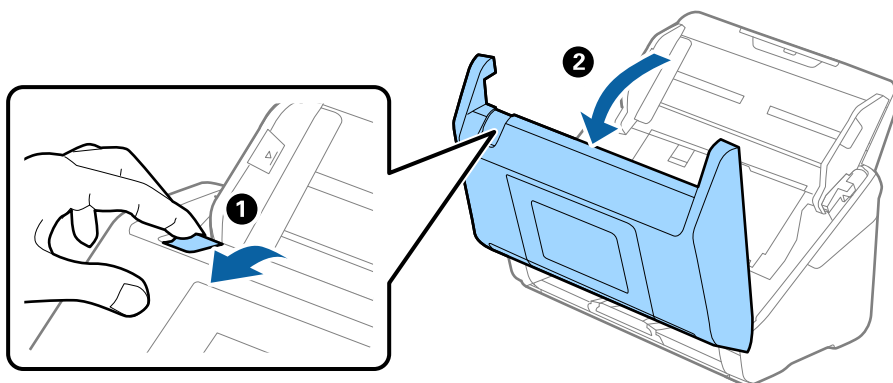


Belangrijk:

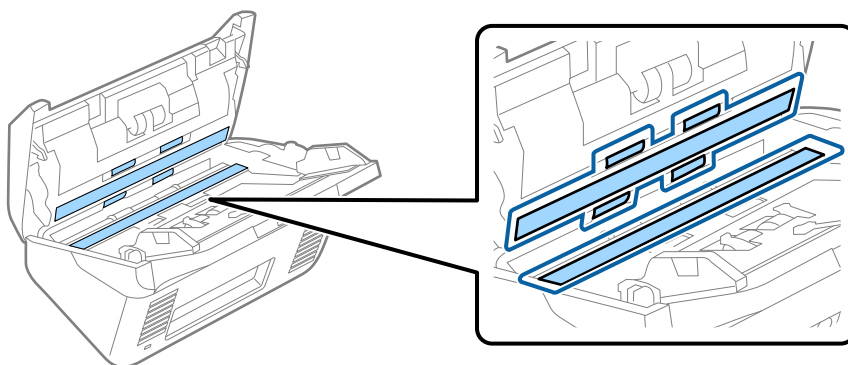
- Maak de scanner nooit schoon met alcohol, thinner of bijtende oplosmiddelen. Er kan vervorming of kleurverandering optreden.*
- Spuit nooit vloeistof of smeermiddel op de scanner. Schade aan de apparatuur of onderdelen kan leiden tot ongewone bewerkingen.*
- Verwijder nooit de behuizing van de scanner.*

1. Druk op de knop  om de scanner uit te schakelen.
2. Koppel de lichtnetadapter los van de scanner.

3. Trek aan de hendel en open het scannerdeksel.



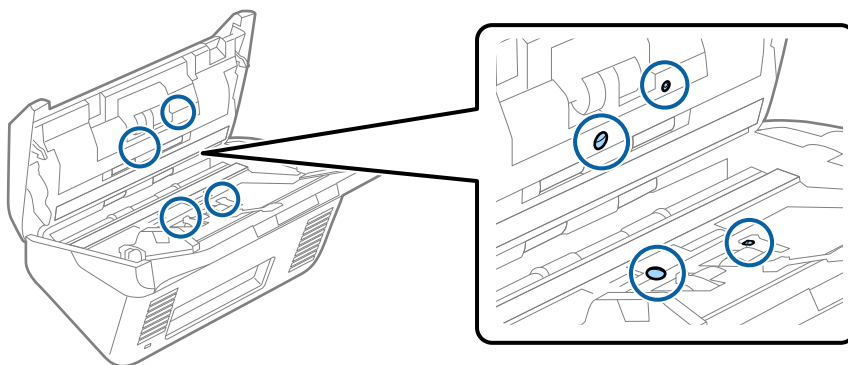
4. Veeg eventuele vlekken van de plastic rol (op vier plekken) en de glasplaat aan de onderkant van het scannerdeksel. Gebruik een zachte, pluisvrije doek die met een kleine hoeveelheid speciaal reinigingsmiddel of water is bevochtigd.



Belangrijk:

- Druk niet te hard op de glasplaat.
- Gebruik geen borstel of hard gereedschap. Krassen op de glasplaat kunnen de scankwaliteit beïnvloeden.
- Spuit geen reiniger direct op de glasplaat.

5. Veeg met een wattenstaafje vlekken van de sensoren.

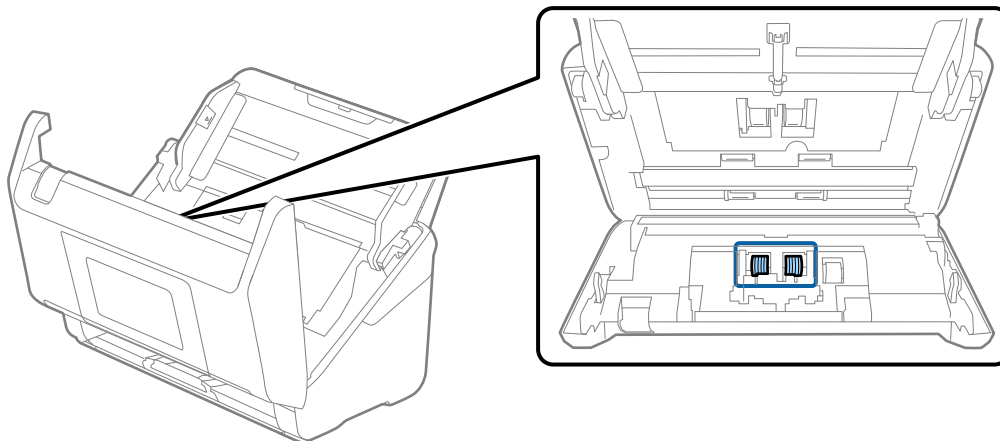




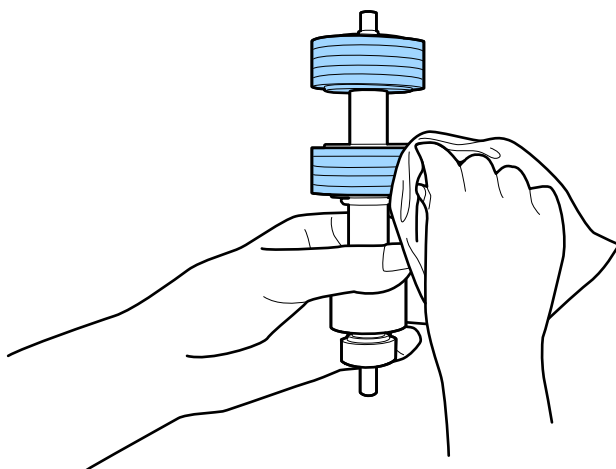
Belangrijk:

Gebruik geen vloeistoffen, zoals reinigingsmiddel, op een wattenstaafje.

6. Open het deksel en verwijder de scheidingsrol.
Raadpleeg voor meer informatie “De rollenset vervangen”.



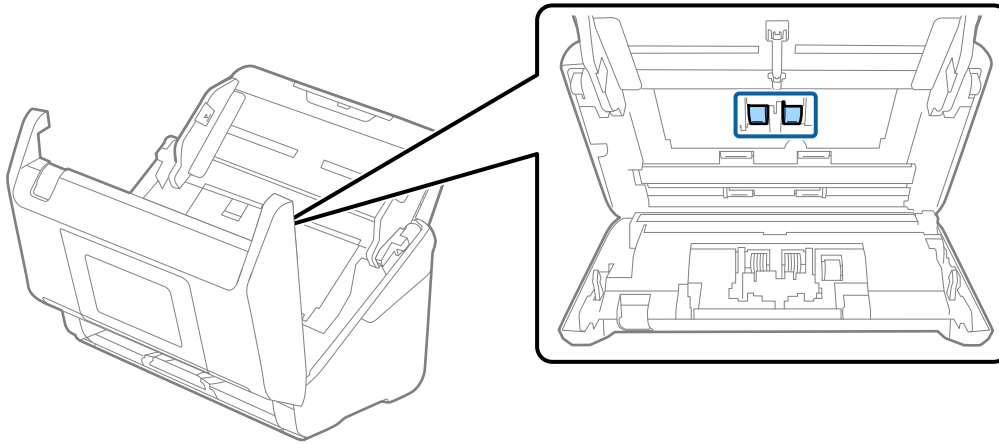
7. Veeg de scheidingsrol af. Gebruik een zachte, pluïsvrije doek die met een kleine hoeveelheid speciaal reinigingsmiddel of water is bevochtigd.



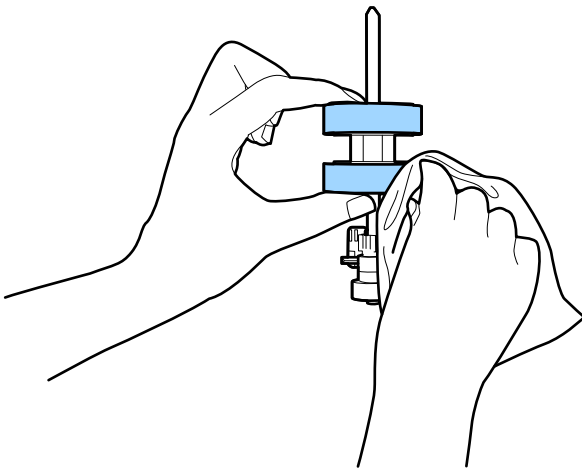
Belangrijk:

Gebruik een originele Epson-reinigingsset of een zachte, vochtige doek om de rol te reinigen. Als u een droge doek gebruikt, beschadigt u mogelijk het oppervlak van de rol.

- Open het deksel en verwijder de transportrol.
Raadpleeg voor meer informatie "De rollerset vervangen".



- Veeg de transportrol af. Gebruik een zachte, pluïsvrije doek die met een kleine hoeveelheid speciaal reinigingsmiddel of water is bevochtigd.

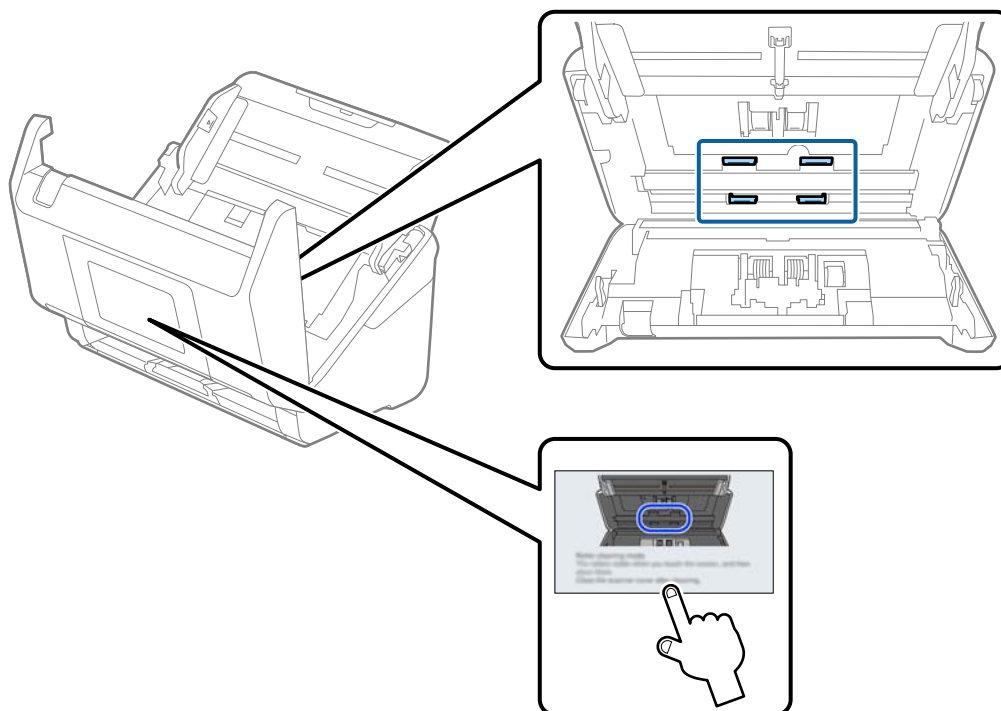


Belangrijk:

Gebruik een originele Epson-reinigingsset of een zachte, vochtige doek om de rol te reinigen. Als u een droge doek gebruikt, beschadigt u mogelijk het oppervlak van de rol.

- Sluit het scannerdeksel.
- Sluit de lichtnetadapter aan en schakel de scanner in.
- Selecteer in het startscherm **Onderhoud scanner**.
- Selecteer in het scherm **Onderhoud scanner** de optie **Rolreiniging**.
- Trek aan de hendel om het scannerdeksel te openen.
De rolreinigingsmodus van de scanner wordt ingeschakeld.

15. Verdraai langzaam de rollen onderaan door op een willekeurige plek op het lcd-scherm te tikken. Veeg het oppervlak van de rollen af met een originele Epson-reinigingsset of met een zachte, vochtige doek. Herhaal dit totdat de rollen schoon zijn.



Let op:

Zorg ervoor dat uw handen of uw haren niet in het mechanisme klem komen te zitten terwijl u de rol bedient. Hierdoor kan letsel ontstaan.

16. Sluit het scannerdeksel.

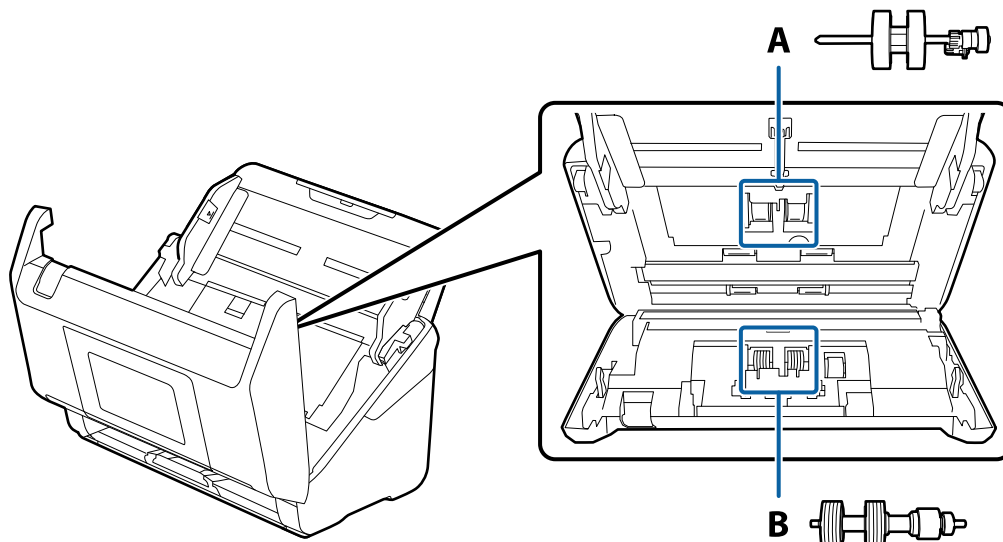
De rolreinigingsmodus van de scanner wordt uitgeschakeld.

Gerelateerde informatie


➔ [“De rollerset vervangen” op pagina 132](#)

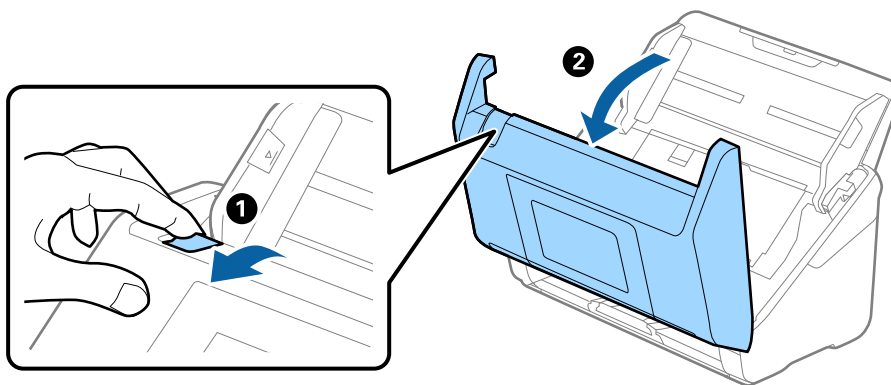
De rollerset vervangen

De rollerset (de transportrol en de scheidingsrol) moeten worden vervangen wanneer het aantal scan de levensduur van de rollen heeft overschreden. Wanneer een vervangingsbericht wordt weergegeven op het bedieningspaneel of het computerscherm, volgt u de onderstaande stappen om de vervanging uit te voeren.

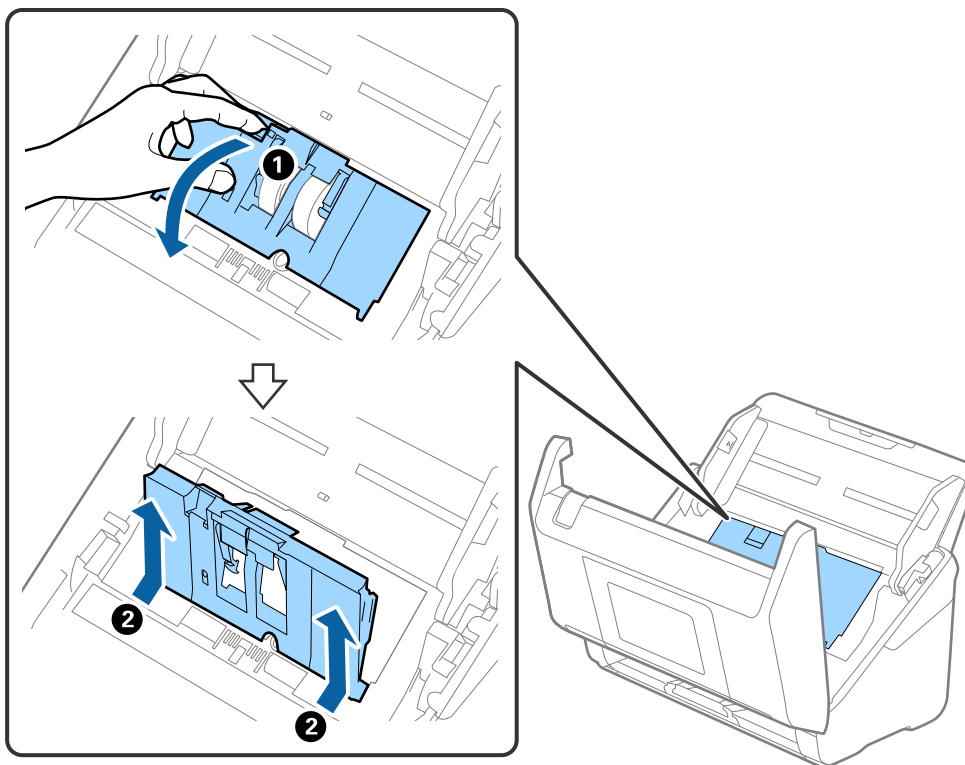


A: transportrol, B: scheidingsrol

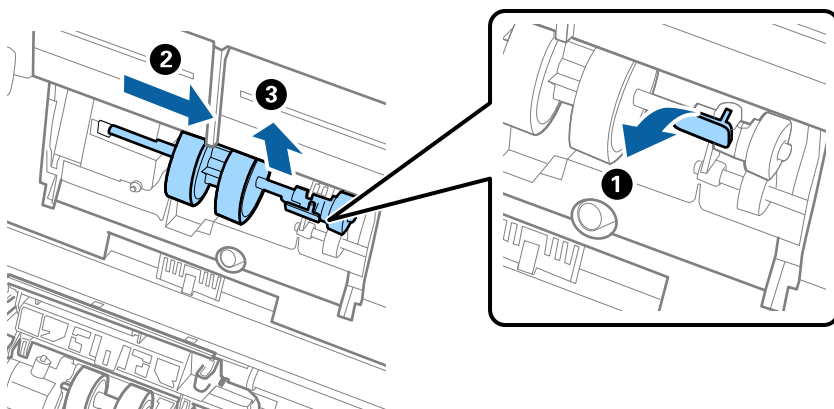
1. Druk op de knop  om de scanner uit te schakelen.
2. Koppel de lichtnetadapter los van de scanner.
3. Trek aan de hendel en open het scannerdeksel.



4. Op de kap van de transportrol en schuif deze opzij om te verwijderen.



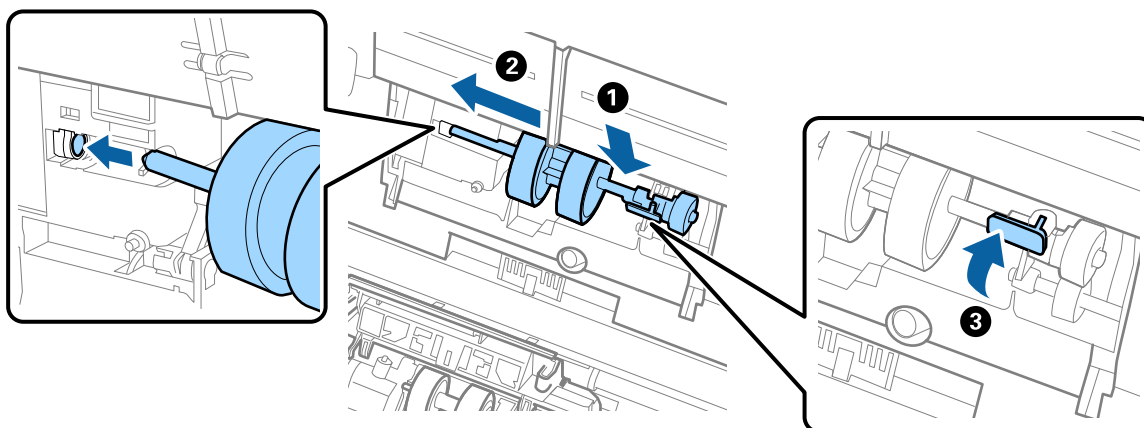
5. Trek de houder van de rolas naar beneden en schuif de geplaatste transportrollen opzij om ze te verwijderen.



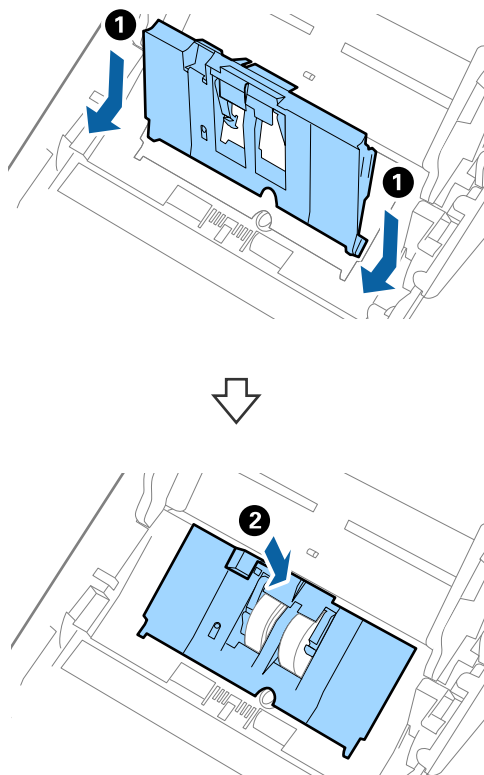
Belangrijk:

Verwijder de transportrol niet met te veel kracht. Hierdoor kan de binnenzijde van de scanner beschadigd raken.

6. Houd de houder naar beneden, schuif de nieuwe transportrol naar links en plaats hem in het gat in de scanner. Duw de houder weer vast.

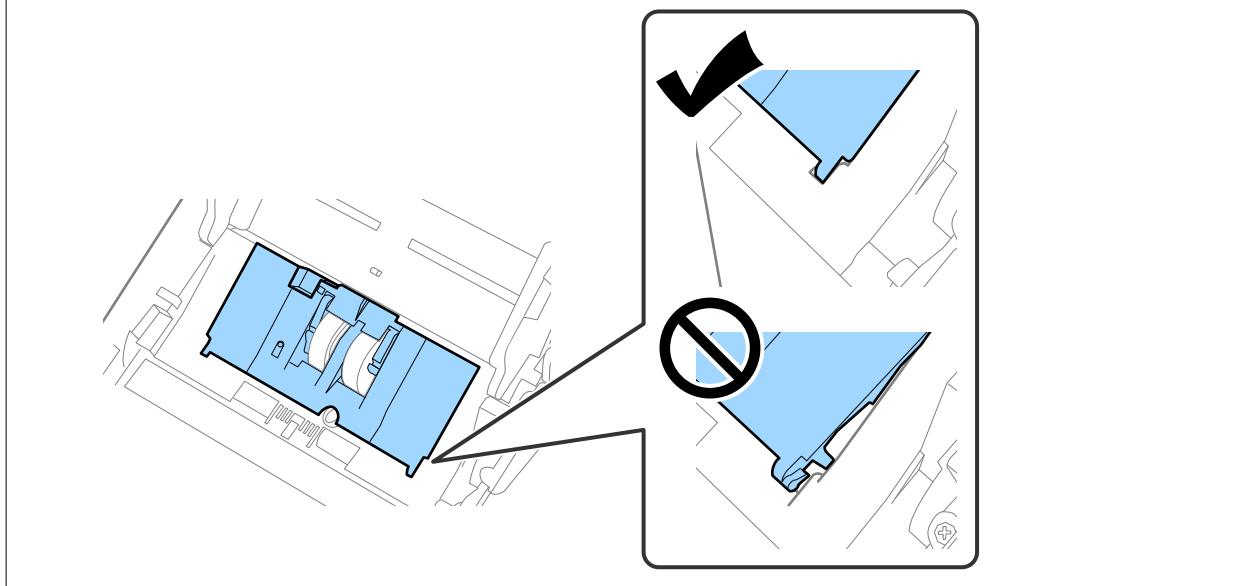


7. Plaats de rand van de kap van de transportrol in de sleuf en schuif hem dicht. Sluit de kap goed.

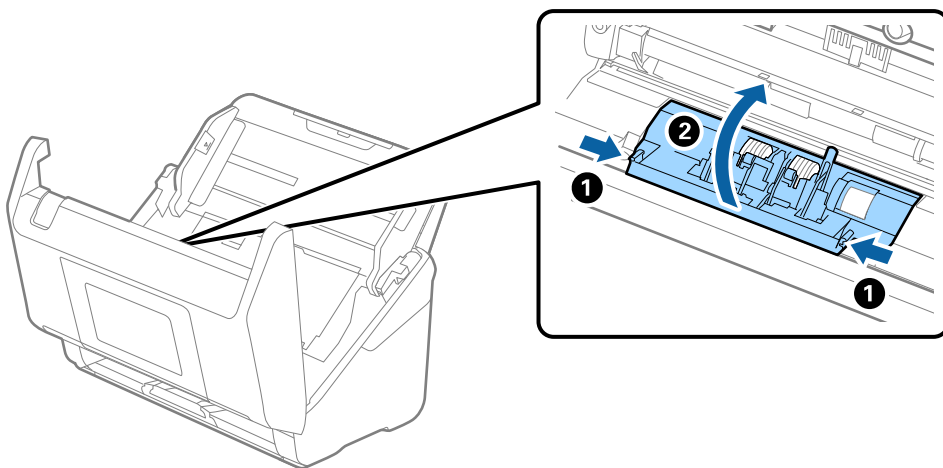


! **Belangrijk:**

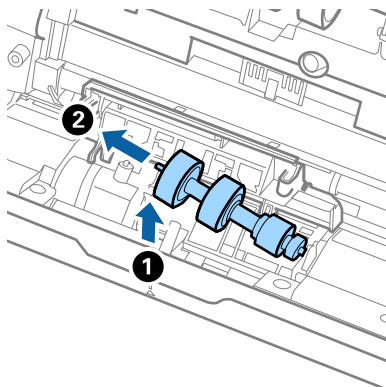
- Controleer of de kap van de transportrol correct is gesloten.
- Controleer of de invoerrollen correct zijn geplaatst als u moeite hebt met het sluiten van de kap.
- Sluit de kap niet wanneer deze omhoog staat.



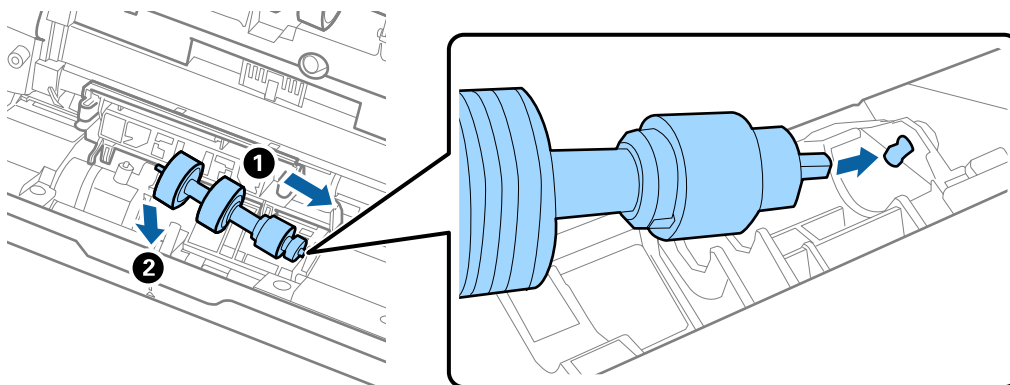
8. Duw op de haken aan beide zijden van de kap van de scheidingsrol om de kap te openen.



9. Til de linkerzijde van de scheidingsrol op en schuif de geplaatste scheidingsrollen opzij om ze te verwijderen.



10. Plaats de as van de nieuwe scheidingsrol in het gat in de rechterzijde en laat de rol zakken.



11. Sluit de kap van de scheidingsrol.



Belangrijk:

Controleer of de scheidingsrollen correct zijn geplaatst als het deksel moeilijk kan worden gesloten.

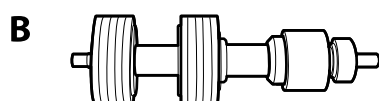
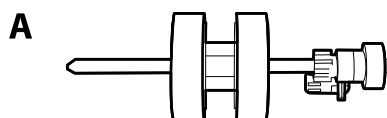
12. Sluit het scannerdeksel.
13. Sluit de lichtnetadapter aan en schakel de scanner in.
14. Reset de teller voor het aantal scans op het bedieningspaneel.

Opmerking:

Voer de transportrol en de scheidingsrol af overeenkomstig de wet- en regelgeving van de plaatselijke overheid. Haal deze niet uit elkaar.

Codes voor de rollenset

Onderdelen (de transportrol en de scheidingsrol) moeten worden vervangen wanneer het aantal scans het onderhoudsaantal heeft overschreden. U kunt de recentste tellerstand voor het aantal scans controleren op het bedieningspaneel of in Epson Scan 2 Utility.



A: transportrol, B: scheidingsrol

Naam van onderdeel	Codes	Levensduur
Rollenset 2	B12B819711 B12B819721 (alleen voor India)	200,000*

* Dit aantal is bereikt door voortdurend scannen met originele papieren voor het uitvoeren van tests voor Epson en vormt een richtlijn voor de vervangingscyclus. De vervangingscyclus kan variëren afhankelijk van verschillende papiersoorten, zoals papier dat veel papierstof produceert of papier met een ruw oppervlak waardoor de levensduur kan worden verkort.

Het aantal scans opnieuw instellen na vervanging van de rollen

Reset de teller voor het aantal scans via het bedieningspaneel of met Epson Scan 2 Utility nadat u de rollenset hebt vervangen.

In dit gedeelte wordt uitgelegd hoe u kunt resetten via het bedieningspaneel.

1. Tik in het startscherf op **Onderhoud scanner**.
2. Tik op **Vervanging onderhoudsroller**.
3. Tik op **Het aantal scans resetten**.
4. Selecteer **Aantal scans na vervangen roller** en tik vervolgens op **Ja**.

Opmerking:

Als u met Epson Scan 2 Utility wilt resetten, start u Epson Scan 2 Utility, klikt u op het tabblad **Volgnummer** en vervolgens op **Reset bij Assembleerkit van rollen**.

Gerelateerde informatie

➔ [“De rollerset vervangen” op pagina 132](#)

Energiebesparing

U kunt energie besparen door de slaapstand of de modus voor automatische uitschakeling te gebruiken wanneer de scanner niet wordt gebruikt. U kunt de duur instellen voordat de slaapstand wordt ingeschakeld en de scanner automatisch wordt uitgeschakeld. Elke verhoging is van invloed op de energiezuinigheid van het product. Denk aan eventuele effecten op het milieu voordat u wijzigingen aanbrengt.


1. Selecteer in het startscherm **Instel.**
2. Selecteer **Basisinstellingen.**
3. Selecteer **Slaaptimer** of **Uitschakelinst.** en stel dan de instellingen in.

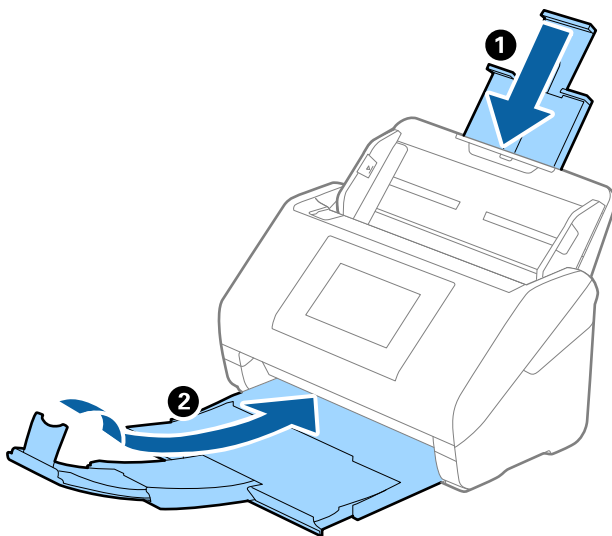
Opmerking:

Welke functies beschikbaar zijn, is afhankelijk van de plaats van aankoop.

De scanner vervoeren

Als u uw scanner moet verplaatsen of vervoeren voor reparatie, volg dan de onderstaande stappen voor het inpakken van de scanner.

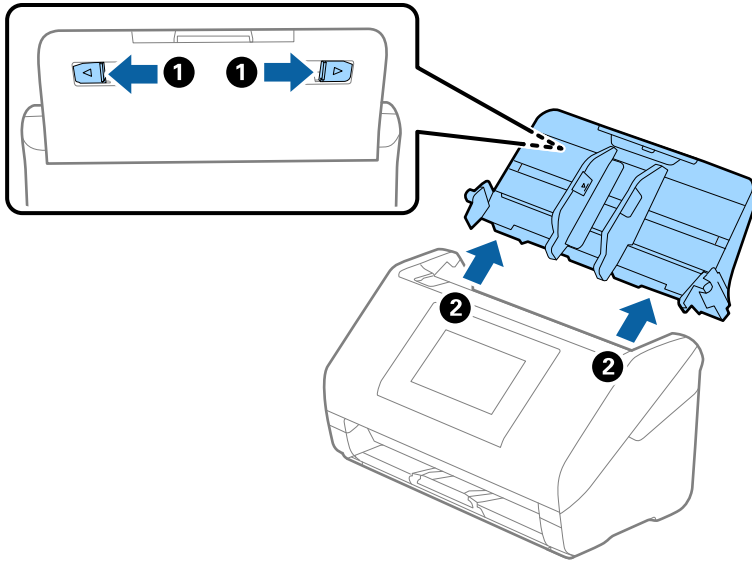
1. Druk op de knop  om de scanner uit te schakelen.
2. Koppel de lichtnetadapter los.
3. Verwijder de kabels en de apparaten.
Verwijder de optionele of meegeleverde Paper Alignment Plate als deze is bevestigd.
4. Sluit het verlengstuk van de invoerlade en de uitvoerlade.



Belangrijk:

Zorg ervoor dat u de uitvoerlade goed sluit, anders zou tijdens het transport schade kunnen ontstaan.

5. Verwijder de invoerlade.



6. Gebruik het originele verpakkingsmateriaal en doe alles weer in de originele doos of in een andere stevige doos.

Een back-up maken van de instellingen

U kunt de instellingswaarde die in Web Config is ingesteld, exporteren naar het bestand. U kunt dit gebruiken om een back-up maken van de contactpersonen, instellingswaarden, vervanging van de scanner enz.

Het geëxporteerde bestand is een binair bestand en kan daarom niet worden bewerkt.

De instellingen exporteren

Exporteer de instellingen voor de scanner.

1. Open Web Config en selecteer vervolgens het tabblad **Apparaatbeheer > Instelwaarde exporteren en importeren > Exporteren**.

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 versleutelen.

U hebt dit wachtwoord nodig om het bestand te importeren. Laat dit leeg als u het bestand niet wilt versleutelen.

4. Klik op **Exporteren**.



Belangrijk:

*Als u de netwerkinstellingen van de scanner, zoals de apparaatnaam en het IPv6-adres exporteert, selecteert u **Inschakelen om de individuele instellingen van apparaat te selecteren** en kiest u meer items. Gebruik alleen de geselecteerde waarden voor de vervangingsscanner.*

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser” op pagina 39](#)

De instellingen importeren

Importeer het geëxporteerde Web Config-bestand naar de scanner.



Belangrijk:

Wanneer u waarden importeert die individuele gegevens bevatten, zoals een scannernaam of IP-adres, moet u ervoor zorgen dat hetzelfde IP-adres niet al voorkomt in hetzelfde netwerk.

1. Open Web Config en selecteer vervolgens het tabblad **Apparaatbeheer > Instelwaarde exporteren en importeren > Importeren**.
2. Selecteer het geëxporteerde bestand en voer het versleutelde wachtwoord in.
3. Klik op **Volgende**.
4. Selecteer de instellingen die u wilt importeren en klik vervolgens op **Volgende**.
5. Klik op **OK**.

De instellingen worden toegepast op de scanner.

Gerelateerde informatie

➔ [“Web Config uitvoeren in een webbrowser” op pagina 39](#)

Standaardinst. herstellen

Selecteer op het bedieningspaneel **Instel. > Systeembeheer > Standaardinst. herstellen**. Selecteer vervolgens de items die u wilt terugzetten naar de standaardwaarden.

- Netwerkinstellingen: hiermee herstelt u netwerkgerelateerde instellen naar hun standaardwaarden.
- Alles behalve Netwerkinstellingen: hiermee herstelt u andere instellingen naar hun standaardwaarden, met uitzondering van netwerkgerelateerde instellingen.
- Alle instellingen: hiermee herstelt u alle instellingen naar de waarden van het moment van aankoop.



Belangrijk:

Als u **Alle instellingen** selecteert en uitvoert, worden alle instellingsgegevens die op de scanner zijn opgeslagen verwijderd, inclusief de contactpersonen. Verwijderde instellingen kunnen niet worden hersteld.

Opmerking:

U kunt instellingen ook configureren in Web Config.

Tabblad **Apparaatbeheer** > **Standaardinstellingen herstellen**

Toepassingen en firmware bijwerken

U kunt bepaalde problemen oplossen en functies verbeteren of toevoegen door de toepassingen en de firmware bij te werken. Zorg dat u de laatste versie van de toepassingen en firmware gebruikt.



Belangrijk:

Schakel de computer of scanner niet uit tijdens het bijwerken.

Opmerking:

Wanneer de scanner verbinding kan maken met internet, kunt u de firmware bijwerken via Web Config. Selecteer het tabblad **Apparaatbeheer** > **Firmware-update**, controleer de weergegeven melding en klik op **Starten**.

1. Controleer of de scanner en computer zijn aangesloten en of de computer is aangesloten op het internet.
2. Start EPSON Software Updater en werk de toepassingen of de firmware bij.

Opmerking:

Windows Server-besturingssystemen worden niet ondersteund.

Windows 11

Klik op de knop Start en selecteer dan **Alle apps** > **Epson Software** > **EPSON Software Updater**.

Windows 10

Klik op de startknop en selecteer **Epson Software** > **EPSON Software Updater**.

Windows 8.1/Windows 8

Voer in het zoekvenster de naam van de toepassing in en selecteer het weergegeven pictogram.

Windows 7

Klik op de knop Start en selecteer dan **Alle programma's** of **Programma's** > **Epson Software** > **EPSON Software Updater**.

Mac OS

Selecteer **Finder** > **Ga** > **Toepassingen** > **Epson Software** > **EPSON Software Updater**.

Opmerking:

Als u de toepassing die u wilt bijwerken niet kunt vinden in de lijst, kunt u deze niet bijwerken met de EPSON Software Updater. Controleer of de nieuwste versies van de toepassing beschikbaar zijn op uw lokale Epson-website.

<http://www.epson.com>

De scannerfirmware bijwerken via het bedieningspaneel

Als de scanner verbinding kan maken met internet, kunt u de firmware van de scanner bijwerken via het bedieningspaneel. U kunt ook instellen dat de scanner regelmatig zelf controleert of er nieuwe firmware is en zo ja, dat u daar dan bericht van krijgt.

1. Selecteer in het startscherm **Instel.**
2. Selecteer **Systeembeheer > Firmware-update > Bijwerken.**

Opmerking:

Selecteer **Melding > Aan** om de scanner regelmatig te laten controleren op beschikbare firmware-updates.

3. Controleer het bericht dat op het scherm wordt weergegeven en start het zoeken naar beschikbare updates.
4. Als op het display wordt weergegeven dat er een firmware-update beschikbaar is, volg dan de aanwijzingen op het scherm om de update te starten.



Belangrijk:

- Schakel de scanner niet uit en trek de stekker niet uit het stopcontact zolang de update bezig is, anders kan de scanner defect raken.
- Als de firmware-update niet goed wordt afgerond of mislukt, start de scanner niet goed op en wordt Recovery Mode weergegeven op het display de volgende keer dat de scanner wordt aangezet. In dit geval moet u de firmware opnieuw bijwerken maar dan met behulp van een computer. Sluit de scanner met een USB-kabel aan op de computer. Wanneer Recovery Mode wordt weergegeven op de scanner, kunt u de firmware niet via een netwerkverbinding bijwerken. Ga op de computer naar uw lokale Epson-website en download de meest recente scannerfirmware. Zie de aanwijzingen op de website voor de volgende stappen.

Firmware bijwerken met Web Config

Wanneer de scanner verbinding kan maken met internet, kunt u de firmware bijwerken via Web Config.

1. Open Web Config en selecteer het tabblad **Apparaatbeheer > Firmware-update.**
2. Klik op **Starten** en volg de instructies op het scherm.

De firmwarebevestiging begint en de firmware-informatie wordt weergegeven als er nieuwere firmware beschikbaar is.

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 uitvoeren in een webbrowser”](#) op pagina 39

Firmware bijwerken zonder verbinding te maken met internet

U kunt de firmware van het apparaat van de Epson-website downloaden op uw computer. Vervolgens kunt u het apparaat via een USB-kabel aansluiten op de computer om de firmware bij te werken. If you cannot update over the network, try this method.

Opmerking:

Controleer voordat u gaat bijwerken of het scannerstuurprogramma Epson Scan 2 op uw computer is geïnstalleerd. Installeer Epson Scan 2 als dit niet is geïnstalleerd.

1. Ga naar de Epson-website voor de nieuwste firmware-updates.
<http://www.epson.com>
 - Download de firmware voor uw scanner en ga naar de volgende stap.
 - Als er geen firmware-informatie op de website staat, gebruikt u al de nieuwste firmware.
2. Sluit de scanner 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.