EPSON
EXCEED YOUR VISION

DS-790WN

Beheerdershandleiding

NPD6726-00 NL

Copyright

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

Handelsmerken

- ❏ EPSON, EPSON EXCEED YOUR VISION, EXCEED YOUR VISION en de bijbehorende logo's zijn gedeponeerde handelsmerken of handelsmerken van Seiko Epson.
- ❏ Microsoft®, Windows®, and Windows Server® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- ❏ Chrome is a trademark of Google LLC.
- ❏ The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- ❏ Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- ❏ FeliCa en PaSoRi zijn geregistreerde handelsmerken van Sony Corporation.
- ❏ MIFARE is een geregistreerd handelsmerk van NXP Semiconductor Corporation.
- ❏ Algemene kennisgeving: andere productnamen die hier worden gebruikt, zijn alleen voor identificatiedoeleinden en kunnen handelsmerken zijn van hun respectieve eigenaars. Epson maakt geen enkele aanspraak op enige rechten op deze handelsmerken.

Inhoudsopgave

Basisinstellingen voor beveiliging

Geavanceerde beveiligingsinstellingen

Verificatie-instellingen

Onderhoud

Inleiding

De inhoud van dit document

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

❏ Netwerkinstellingen

❏ De scanfunctie voorbereiden

❏ Beveiligingsinstellingen inschakelen en beheren

❏ Verificatie-instellingen inschakelen en beheren

❏ Dagelijks onderhoud uitvoeren

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

Opmerking:
In dit document worden de Verificatie-instellingen uitgelegd waarmee afzonderlijke verificatie zonder gebruik van een verificatieserver mogelijk is. Naast de Verificatie-instellingen die in deze handleiding aan bod komen, kunt u ook een verificatiesysteem opzetten met een verificatieserver. Gebruik Document Capture Pro Server Authentication Edition (de afgekorte naam is Document Capture Pro Server AE) om een systeem op te zetten.

Neem voor meer informatie contact op met uw lokale Epson-kantoor.

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.

Besturingssysteemreferenties

Windows

In deze handleiding wordt met termen als "Windows 10", "Windows 8.1", "Windows 8", "Windows 7", "Windows Server 2019", "Windows Server 2016", "Windows Server 2012 R2", "Windows Server 2012" en "Windows Server 2008 R2" verwezen naar de volgende besturingssystemen. Daarnaast wordt "Windows" gebruikt om te verwijzen naar alle versies en wordt "Windows Server" gebruikt om te verwijzen naar "Windows Server 2019", "Windows Server 2016", "Windows Server 2012 R2", "Windows Server 2012" en "Windows Server 2008 R2".

- ❏ Besturingssysteem Microsoft® Windows® 10
- ❏ Besturingssysteem Microsoft® Windows® 8.1
- ❏ Besturingssysteem Microsoft® Windows® 8
- ❏ Besturingssysteem Microsoft® Windows® 7
- ❏ 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

Mac OS

In deze handleiding wordt "Mac OS" gebruikt om te verwijzen naar macOS Big Sur, macOS Catalina, macOS Mojave, macOS High Sierra, macOS Sierra, OS X El Capitan en OS X Yosemite.

Vereiste instellingen voor verschillende doeleinden

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 14
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 20

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 e-mailserver configureren" op pagina 42 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 64
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 gedeelde netwerkmap instellen" op pagina 45 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 64
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 78

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 87
Ik wil het gebruik van scanners met USB-verbindingen uitschakelen.	Schakel de externe interface uit. "De externe interface uitschakelen" op pagina 93

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 99
Ik wil het communicatiepad versleutelen.	1. Configureer uw digitale certificaat. "Een digitaal certificaat gebruiken" op pagina 102 2. Configureer SSL/TLS-communicatie. "SSL/TLS-communicatie met de scanner" op pagina 107
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 109
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 120

Instellingen die met de scanner moeten worden geverifieerd

Doel	Vereiste instellingen
Ik wil Verificatie-instellingen inschakelen.	Raadpleeg de volgende informatie over de beschikbare Verificatie-instellingen en de Verificatiemethode. "Over Verificatie-instellingen" op pagina 130 "Over Verificatiemethode" op pagina 131

Het verificatiesysteem van een server gebruiken

Met Document Capture Pro Server Authentication Edition (ingekort tot Document Capture Pro Server AE) kunt u een verificatiesysteem bouwen dat een server gebruikt voor de verificatie.

Neem voor meer informatie contact op met uw lokale Epson-kantoor.

Netwerkinstellingen

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.

❏ *Instellen via de website*

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

http://epson.sn

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

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

Voor het maken van netwerkverbinding

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

Informatie over de verbindingsinstelling verzamelen

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

Divisies	Items	Opmerking
Apparaatverbindingsmethode	❏ Ethernet ❏ 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	❏ IP-adres ❏ Subnetmasker ❏ 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	❏ SSID ❏ Wachtwoord	Dit omvat de SSID (netwerknaam) 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 28
DNS-serverinformatie	❏ IP-adres voor primaire DNS ❏ IP-adres voor secondaire DNS	Deze zijn vereist bij het opgeven van DNS-servers. De DNS is ingesteld wanneer het systeem een redundante configuratie heeft en er een secondaire 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	❏ Proxyservernaam	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. Bij de volgende functies maakt de scanner rechtstreeks verbinding met internet. ❏ Epson Connect Services ❏ Cloudservices van andere bedrijven ❏ Firmware-updates ❏ Gescande afbeeldingen verzenden naar SharePoint (WebDAV)
Poortnummerinformatie	❏ Nummer van poort die moet worden vrijgegeven	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. Raadpleeg het volgende voor het poortnummer dat door de scanner wordt gebruikt. "Poort voor de scanner gebruiken" op pagina 30

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, standaardgatewaygateway, 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 wort 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 secondaire 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 verbindingsmethode 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.

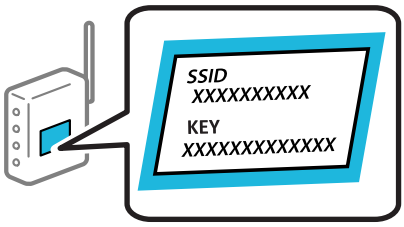
Als de draadloze router WPS ondersteunt, kunt u de instellingen configureren met drukknopinstellingen.

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.)

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 verbindingsdetails 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 netwerkverbindingsstatus 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 is mogelijk het wachtwoord vermeld, bijvoorbeeld aangeduid als "Network Key" of "Wireless Password". Als u de draadloze router met de standaardinstellingen wilt gebruiken, gebruikt u het wachtwoord dat op het label is geschreven.*

Gerelateerde informatie

➡ "De status van de netwerkverbinding controleren" op pagina 26

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 verbindingsdetails 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 netwerkverbindingsstatus van de scanner wilt controleren.

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

Gerelateerde informatie

➡ "De status van de netwerkverbinding controleren" op pagina 26

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 verbindingsdetails 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 netwerkverbindingsstatus 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 26

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

❏ Instellen via de website

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

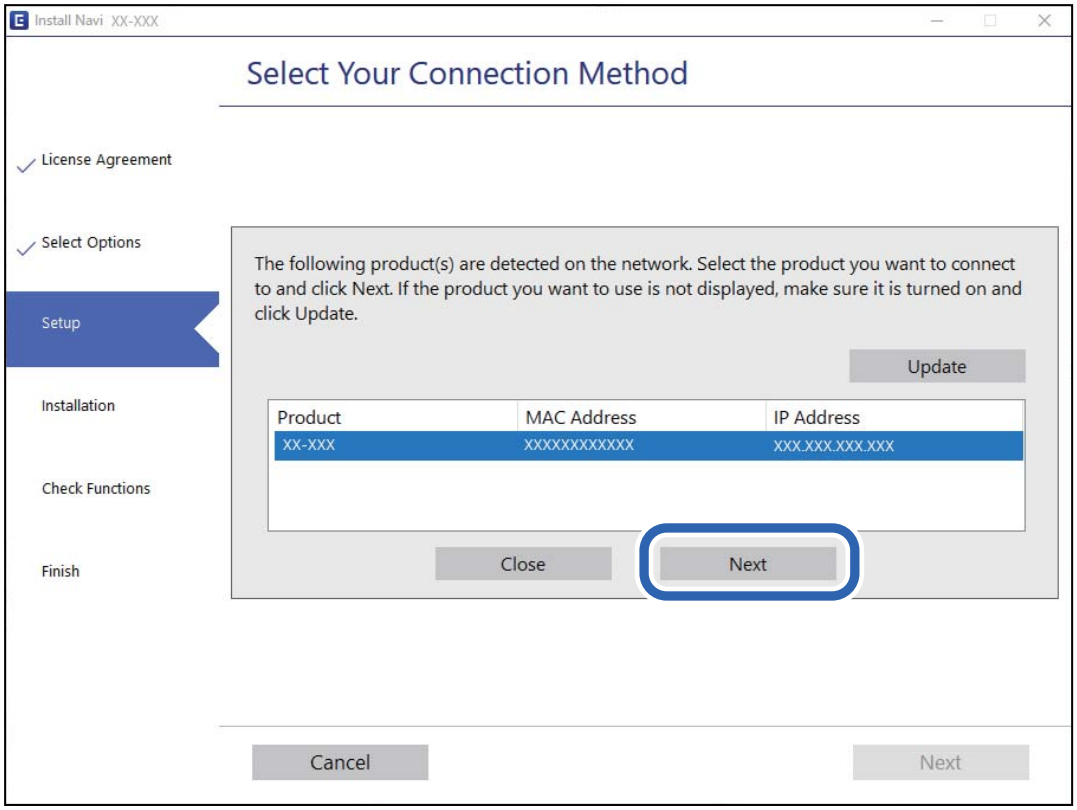
http://epson.sn

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

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

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 25

Verbinden via Wi-Fi Direct

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

Meer details hieronder.

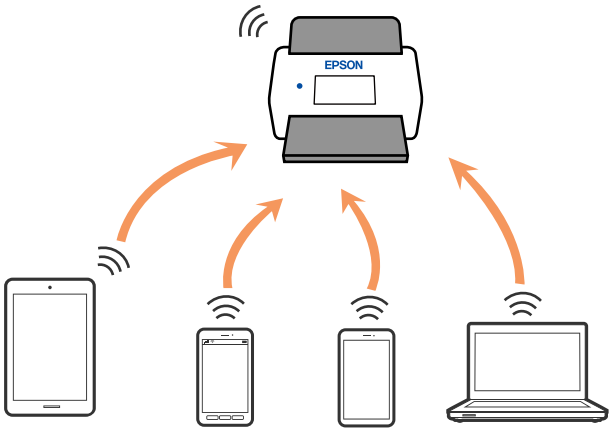
"Een smart device rechtstreeks verbinden met een scanner (Wi-Fi Direct)" op pagina 22

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 startscherm  .
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-tekens 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-tekens 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 verbindingsmethode 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 de het installatieprogramma te gebruiken om de scanner te verbinden met een computer. U kunt het installatieprogramma op een van de volgende manieren uitvoeren.

❏ Instellen via de website

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

http://epson.sn

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

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

De verbindingsmethode selecteren

Volg de instructies op het scherm. Selecteer in het scherm **Uw bewerking selecteren** 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 31

Instellingen voor verbinding met het smart device configureren

U kunt de scanner gebruiken vanaf een smart device wanneer u de scanner verbindt met hetzelfde Wi-Fi-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 configureer de instellingen.

http://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 de het installatieprogramma te gebruiken om de scanner te verbinden met een computer. U kunt het installatieprogramma op de volgende manier uitvoeren.

❏ Instellen via de website

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

http://epson.sn

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

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

Volg de instructies op het scherm.

De methode voor verbinding met de computer wijzigen

In dit gedeelte wordt uitgelegd hoe u de verbindingsmethode 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 18

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 stel de installatie in met een andere verbindingsmethode.

❏ Instellen via de website

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

http://epson.sn

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

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

De verbindingsmethode wijzigen selecteren

Volg de instructies op het scherm. Selecteer in het scherm **Uw bewerking selecteren** 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 netwerkverbindingsstatus 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 netwerkverbindingsstatus 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.

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

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
Australië Nieuw-Zeeland Taiwan Zuid-Korea	Tabel B

Tabel A

Normen	IEEE 802.11b/g/n*1
Frequentiebereik	2,4 GHz
Maximaal radiofrequentievermogen dat wordt uitgezonden	2400–2483.5 MHz: 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. Zie voor meer informatie 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 IPv4/IPv6

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

Functies	Ondersteund
Document Capture Pro Server	IPv4, IPv6

Beveiligingsprotocol

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

* U moet verbindingsapparaat 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
		NetBIOS (TCP)	139
	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
POP voor SMTP-verbinding (wanneer vanaf de scanner scannen naar e-mail wordt gebruikt)	POP-server	POP3 (TCP)	110

Gebruiken	Bestemming (server)	Protocol	Poortnummer
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

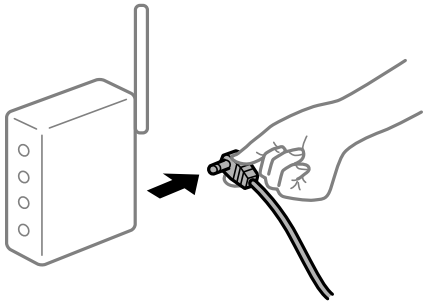
Kan geen verbinding maken met een netwerk

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 dichter bij 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

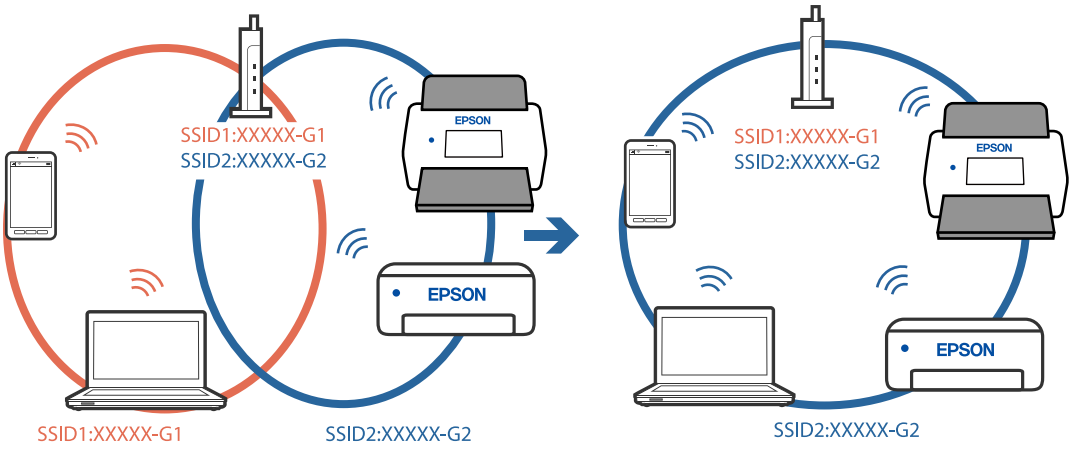
Configureer de verbindingsinstellingen opnieuw, zodat deze overeenkomen met de nieuwe draadloze router.

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.
   "Webconfiguratie uitvoeren op een webbrowser" op pagina 36
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

Web Config

Web Config is een toepassing die op een computer in webbrowsers zoals Internet Explorer en Safari wordt uitgevoerd. U kunt de scannerstatus controleren of de netwerkservice en de scannerinstellingen wijzigen. Aangezien de scanners rechtstreeks via het netwerk worden bediend, kan één scanner tegelijk worden geconfigureerd. Als u Web Config wilt gebruiken, moet u uw computer met hetzelfde netwerk verbinden als de scanner.

De volgende browsers worden ondersteund.

Microsoft Edge, Windows Internet Explorer 8 of hoger, Firefox*, Chrome*, Safari*

* Gebruik de nieuwste versie.

Webconfiguratie uitvoeren op een webbrowser

1. Controleer het IP-adres van de scanner.

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

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

   Indeling:

   IPv4: http://het IP-adres van de scanner/

   IPv6: http://[het IP-adres van de scanner]/

   Voorbeelden:

   IPv4: http://192.168.100.201/

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

   Opmerking:
   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.

3. Log in als beheerder om de scannerinstellingen te wijzigen.

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

   Opmerking:
   ❏ *Hieronder staan de beginwaarden voor de beheerdersinformatie van Web Config.*

   ·Gebruikersnaam: geen (leeg)

   ·Wachtwoord: het serienummer van de scanner

   U vindt het serienummer op het etiket aan de achterzijde van de scanner.

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

Web Config uitvoeren op Windows

Volg de onderstaande stappen om Web Config uit te voeren wanneer u via WSD een computer verbindt met de scanner.

1. Open de scannerlijst op de computer.
   - ❏ Windows 10

     Klik op de startknop en selecteer vervolgens **Windows-systeem** > **Configuratiescherm** > **Apparaten en printers weergeven** in **Hardware en geluiden**.
   - ❏ Windows 8.1/Windows 8

     Selecteer **Bureaublad** > **Instellingen** > **Configuratiescherm** > **Apparaten en printers weergeven** in **Hardware en geluiden** (of **Hardware**).
   - ❏ Windows 7

     Klik op de startknop en selecteer **Configuratiescherm** > **Apparaten en printers weergeven** bij **Hardware en geluiden**.
2. Klik met de rechtermuisknop op uw scanner en selecteer **Eigenschappen**.
3. Selecteer het tabblad **Webservice** en klik op de URL.

   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.

   Opmerking:
   - ❏ *Hieronder staan de beginwaarden voor de beheerdersinformatie van Web Config.*

     ·Gebruikersnaam: geen (leeg)

     ·Wachtwoord: het serienummer van de scanner

     U vindt het serienummer op het etiket aan de achterzijde van de scanner.
   - ❏ *Als rechtsboven in het scherm **Afmelding beheerder** wordt weergegeven, bent u al ingelogd als beheerder.*

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.

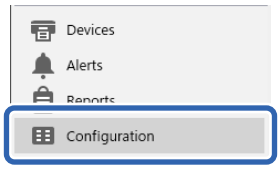
Configuratiesjabloon

De configuratiesjabloon maken

Maak de nieuwe configuratiesjabloon.

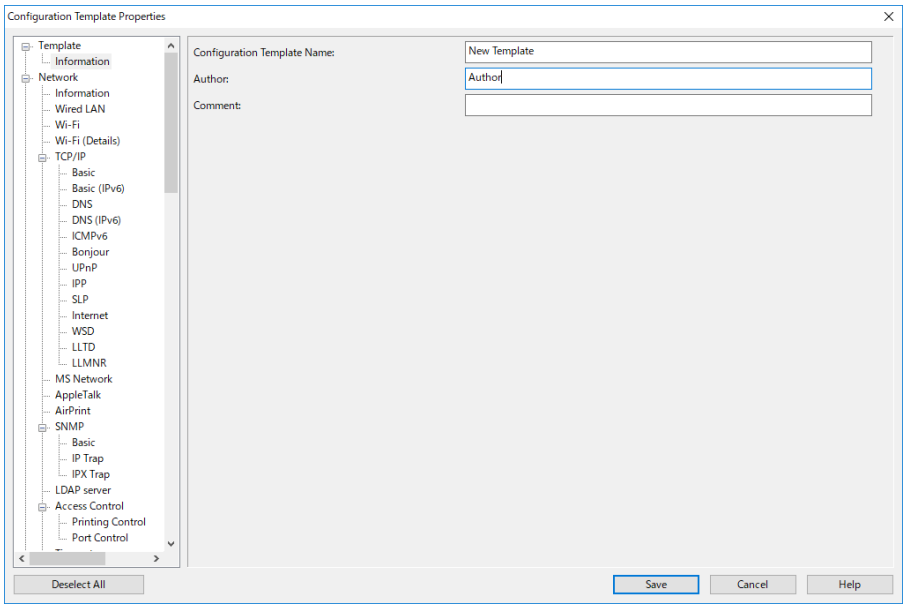
1. Start Epson Device Admin.

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

5. 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.

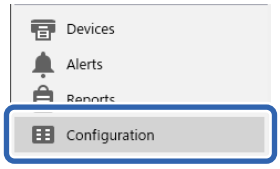
*1. Selecteer in het lintmenu in het scherm "Apparatenlijst" **Opties** > **Wachtwoordbeheer**.*

*2. Selecteer **Automatisch wachtwoordbeheer inschakelen** en klik vervolgens op **Wachtwoordbeheer**.*

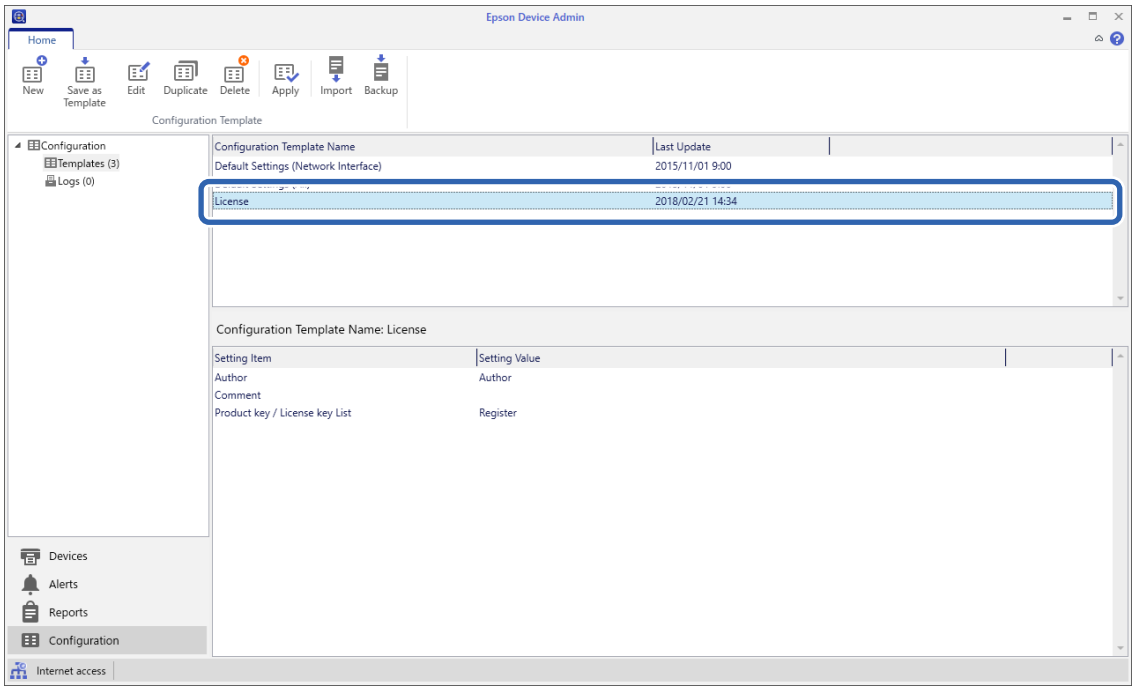
*3. Selecteer de juiste scanner en klik vervolgens op **Bewerken**.*

*4. Stel het wachtwoord in en klik op **OK**.*

1. Selecteer **Configuratie** in het taakmenu in de zijmarge.



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



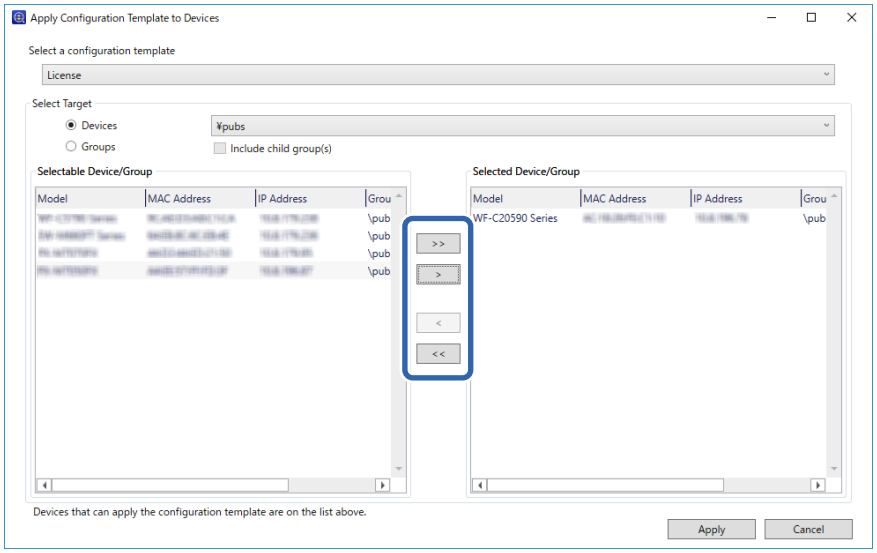
3. Klik op het lintmenu op **Toepassen**.

   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.*

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



6. Klik op **Toepassen**.

   Een bevestigingsscherm voor de toe te passen configuratiesjabloon verschijnt.

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

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

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

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

10. Klik op **Sluiten**.

Vereiste instellingen voor scannen

Een e-mailserver configureren

Stel de mailserver in met Web Config.

Wanneer de mailserver zo is ingesteld dat de scanner e-mailberichten kan verzenden, zijn de volgende mogelijkheden beschikbaar.

❏ Scanresultaten verzenden per e-mail

❏ E-mailmeldingen van de scanner ontvangen

Controleer het onderstaande voordat u de instellingen configureert.

❏ De scanner is verbonden met het netwerk dat toegang heeft tot de mailserver.

❏ De computer is ingesteld op hetzelfde mailserver als de scanner.

Opmerking:

❏ *Wanneer de mailserver gebruikt via internet, bevestigt u de instellingsinformatie van de provider of de website.*

❏ *U kunt de mailserver instellen vanaf het bedieningspaneel van de scanner. Volg de onderstaande stappen.*

Instel. > ***Netwerkinstellingen*** > ***Geavanceerd*** > ***E-mailserver*** > ***Serverinstellingen***

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

   De instellingen die u hebt geselecteerd, worden weergegeven.

Gerelateerde informatie

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

Instellingen voor de e-mailserver

Items	Instellingen en toelichting	
Verificatiemethode	Geef hier de verificatiemethode op die de scanner moet gebruiken voor toegang tot de e-mailserver.	
	Uit	Verificatie is uitgeschakeld wanneer met de e-mailserver wordt gecommuniceerd.
	SMTP-verificatie	Hiervoor is vereist dat een e-mailserver SMTP-verificatie ondersteunt.
	POP voor SMTP	Wanneer u deze methode selecteert, moet u de POP3-server configureren.
Geverifieerd account	Als u **SMTP-verificatie** of **POP voor SMTP** selecteert als de **Verificatiemethode**, voert u de geverifieerde accountnaam in met 0 tot 255 tekens in ASCII (0x20 tot 0x7E).	
Geverifieerd wachtwoord	Als u **SMTP-verificatie** of **POP voor SMTP** selecteert als de **Verificatiemethode**, voert u het geverifieerde wachtwoord in met 0 tot 20 tekens in ASCII (0x20 tot 0x7E).	

Items	Instellingen en toelichting	
E-mailadres afzender	Voer hier het e-mailadres van de afzender in. U kunt tussen 0 en 255 tekens invoeren in ASCII (0x20–0x7E), behalve: ( ) < > [ ] ; ¥. Het eerste teken mag geen punt (".") zijn.	
Adres SMTP-server	Voer hier 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 verbindingsmethode op voor de e-mailserver.	
	Geen	Als u **POP voor SMTP** selecteert in **Verificatiemethode**, wordt de verbindingsmethode 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**.
Certificaatvalidatie	Het certificaat is gevalideerd wanneer dit is ingeschakeld. Wij raden aan dit in te stellen op **Inschakelen**.	
Adres POP3-server	Als u **POP voor SMTP** selecteert als **Verificatiemethode**, voert u het POP3-serveradres in dat tussen 0 en 255 tekens lang is en bestaat uit A–Z a–z 0–9 . -. U kunt IPv4 of FQDN gebruiken.	
Poortnummer POP3-server	Als u **POP voor SMTP** selecteert als **Verificatiemethode**, voert u een cijfer in tussen 1 en 65535.	

De verbinding met de e-mailserver controleren

U kunt de verbinding met de mailserver controleren door een verbindingscontrole uit te voeren.

1. Open Web Config en selecteer het tabblad **Netwerk** > **E-mailserver** > **Verbindingstest**.
2. Selecteer **Starten**.

   De verbindingstest met de mailserver is gestart. Na de test wordt het controlerapport weergegeven.

   Opmerking:
   U kunt de verbinding met de mailserver ook controleren op het bedieningspaneel. Volg de onderstaande stappen.

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

Referenties verbindingstest e-mailserver

Meldingen	Oorzaak
De verbindingstest is gelukt.	Deze melding wordt weergegeven wanneer de verbinding met de server is gemaakt.

Meldingen	Oorzaak
SMTP-servercommunicatiefout. Controleer het volgende. - Netwerkinstellingen	Deze melding wordt in de volgende gevallen weergegeven: ❏ De scanner is niet verbonden met een netwerk ❏ De SMTP-server is uitgeschakeld ❏ De netwerkverbinding is verbroken tijdens de communicatie ❏ Er zijn onvolledige gegevens ontvangen
POP3-servercommunicatiefout. Controleer het volgende. - Netwerkinstellingen	Deze melding wordt in de volgende gevallen weergegeven: ❏ De scanner is niet verbonden met een netwerk ❏ De POP3-server is uitgeschakeld ❏ De netwerkverbinding is verbroken tijdens de communicatie ❏ Er zijn onvolledige gegevens ontvangen
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: ❏ Verbinden met een DNS-server is mislukt ❏ 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: ❏ Verbinden met een DNS-server is mislukt ❏ Naamresolutie voor een POP3-server is mislukt
SMTP-serververificatiefout. Controleer het volgende. - Verificatiemethode - Geverifieerde account - Geverifieerd wachtwoord	Deze melding wordt weergegeven wanneer de verificatie voor de SMTP-server is mislukt.
POP3-serververificatiefout. Controleer het volgende. - Verificatiemethode - Geverifieerde account - Geverifieerd wachtwoord	Deze melding wordt weergegeven wanneer de verificatie voor 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 tijdinstelling van de scanner onjuist is of als het certificaat verlopen is.
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 als een CA-certificaat niet is geïmporteerd.

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

Een gedeelde netwerkmap instellen

Stel een gedeelde netwerkmap in voor het opslaan van de gescande afbeelding.

Wanneer een bestand in de map wordt opgeslagen, logt de scanner in als de gebruiker van de computer waarop de map is gemaakt.

Een gedeelde map maken

Gerelateerde informatie

➡ “Voorafgaand aan het maken van de gedeelde map” op pagina 45
➡ “Het netwerkprofiel controleren” op pagina 46
➡ “Locatie waar de gedeelde map wordt gemaakt en voorbeeld van de beveiliging” op pagina 46
➡ “Een groep of gebruiker toevoegen die toegang heeft” op pagina 60

Voorafgaand aan het maken van de gedeelde map

Controleer de volgende punten voordat u de gedeelde map maakt.

❏ De scanner is verbonden met het netwerk waarin deze toegang heeft tot de computer waarop de gedeelde map wordt gemaakt.

❏ De naam van de computer waarop de gedeelde map wordt gemaakt, bevat geen multibyte tekens.

Belangrijk:

Wanneer de naam van de computer een multibyte teken bevat, kan het bestand mogelijk niet in de gedeelde map worden opgeslagen.

Wijzig in dat geval de naam van de computer of gebruik een computer waarvan de naam geen multibyte teken bevat.

Wanneer u de naam van de computer wijzigt, zorg er dan voor dat u dit vooraf bespreekt met de beheerder. Het wijzigen van de naam kan invloed hebben op bepaalde instellingen, zoals computerbeheer, toegang tot resources enz.

Het netwerkprofiel controleren

Op de computer waarop de gedeelde map wordt gemaakt, controleert u of het delen van mappen is ingeschakeld.

1. Meld u met het gebruikersaccount van de beheerder aan bij de computer waarop de gedeelde map wordt gemaakt.
2. Selecteer **Bedieningspaneel** > **Netwerk en internet** > **Netwerkcentrum**.
3. Klik op **Geavanceerde instellingen voor delen wijzigen** en klik vervolgens op voor het profiel met **(huidige profiel)** in de weergegeven netwerkprofielen.
4. Controleer of **Bestands- en printerdeling inschakelen** is ingeschakeld bij **Bestands- en printerdeling**.

   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.

Locatie waar de gedeelde map wordt gemaakt en voorbeeld van de beveiliging

Afhankelijk van de locatie waar de gedeelde map wordt gemaakt, kunnen de beveiliging en het gemak variëren.

Als u de gedeelde map wilt gebruiken vanaf de scanners of andere computers, zijn de volgende machtigingen voor lezen en wijzigen vereist voor de map.

❏ Tabblad **Delen** > **Geavanceerd delen** > **Machtigingen**

Hiermee controleert u de machtigingen voor netwerktoegang voor de gedeelde map.

❏ Toegangsmachtigingen voor het tabblad **Beveiliging**

Hiermee controleert u de machtigingen voor netwerktoegang en lokale toegang voor de gedeelde map.

Wanneer u **Iedereen** instelt voor de gedeelde map die als voorbeeld op het bureaublad is gemaakt, krijgen alle gebruikers die toegang hebben tot de computer toegangsmachtigingen.

Gebruikers zonder machtiging hebben echter geen toegang omdat het bureaublad (de map) wordt beheerd via de gebruikersmap. De beveiligingsinstellingen van de gebruikersmap zijn hierop van toepassing. Gebruikers die toegang hebben op het tabblad **Beveiliging** (in dit geval gebruiker aangemeld als beheerder) heeft machtigingen voor de map.

Zie onder voor instructies voor het maken van de juiste locatie.

Dit voorbeeld is voor het maken van de "scan_folder" folder.

Gerelateerde informatie

➡ "Voorbeeld van configuratie voor bestandsserver" op pagina 47

➡ "Voorbeeld van configuratie voor een pc" op pagina 54

Voorbeeld van configuratie voor bestandsserver

Deze uitleg vormt een voorbeeld voor het maken van een gedeelde map in de hoofdmap van de schijf van de gedeelde computer, zoals een bestandsserver, met de volgende voorwaarde.

Gebruikers waarvoor de toegang kan worden beheerd, zoals iemand die zich in hetzelfde domein bevindt als de computer waarop een gedeelde map wordt gemaakt, hebben toegang tot de gedeelde map.

Stel deze configuratie in wanneer u elke gebruiker lees- en schrijftoegang wilt geven voor de gedeelde map op de computer, zoals een bestandsserver of gedeelde computer.

❏ Locatie om gedeelde map te maken: hoofdmap van schijf

❏ Mappad: C:\scan_folder

❏ Toegangsmachtiging via het netwerk (Sharemachtigingen): Iedereen

❏ Toegangsmachtiging op het bestandssysteem (Beveiliging): Geverifieerde gebruikers

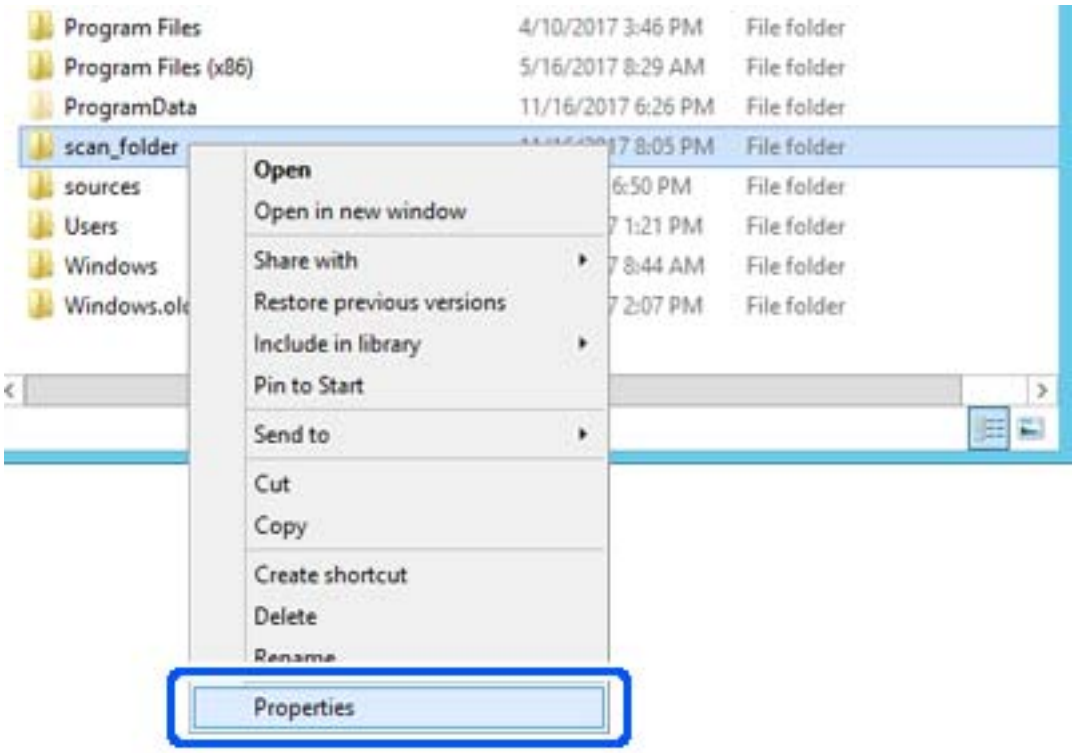
1. Meld u met het gebruikersaccount van de beheerder aan bij de computer waarop de gedeelde map wordt gemaakt.

2. Open de verkenner.

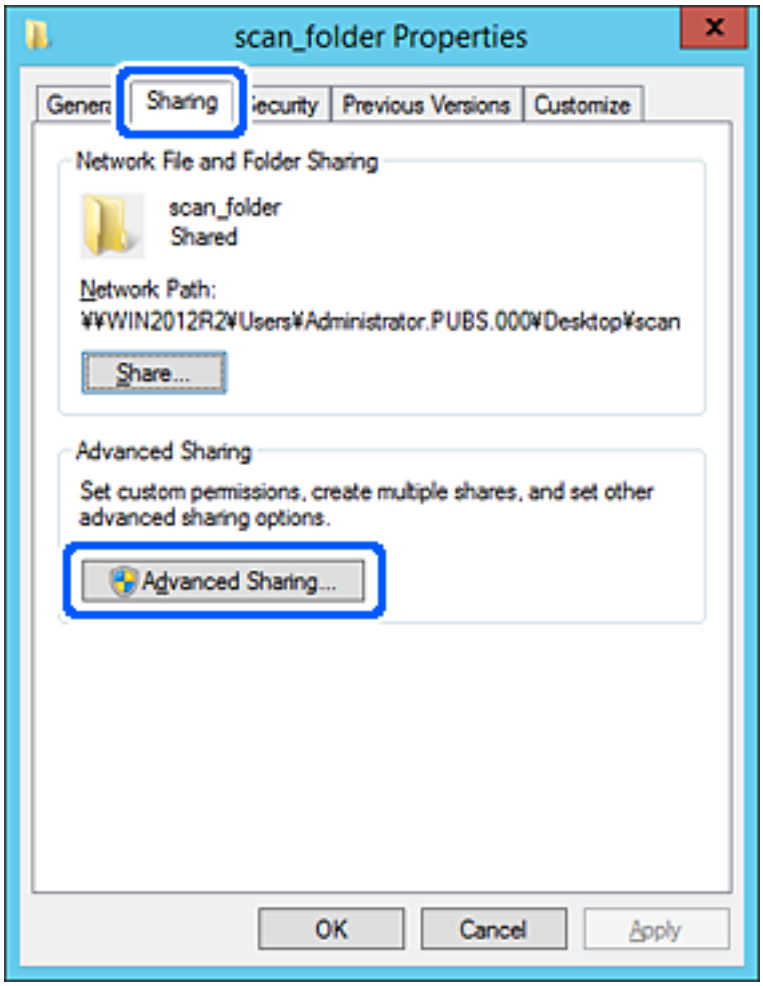
3. Maak de map in de hoofdmap van de schijf en noem deze "scan_folder".

   Voer voor de mapnaam tussen 1 en 12 alfanumerieke tekens in. Als u de tekenlimiet voor de mapnaam overschrijdt, hebt u mogelijk vanuit een andere omgeving geen toegang tot de map.

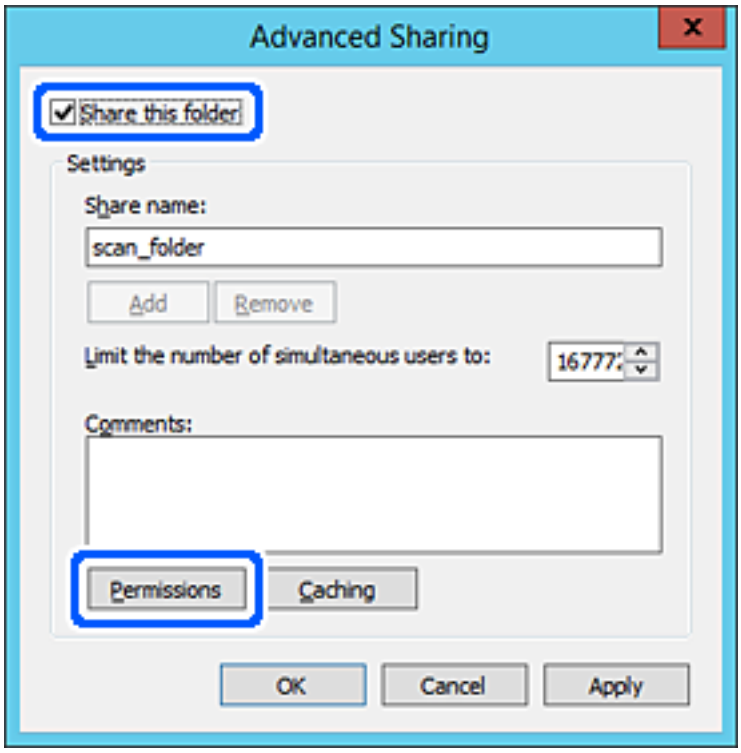
4. Klik met de rechtermuisknop op de map en selecteer **Eigenschappen**.



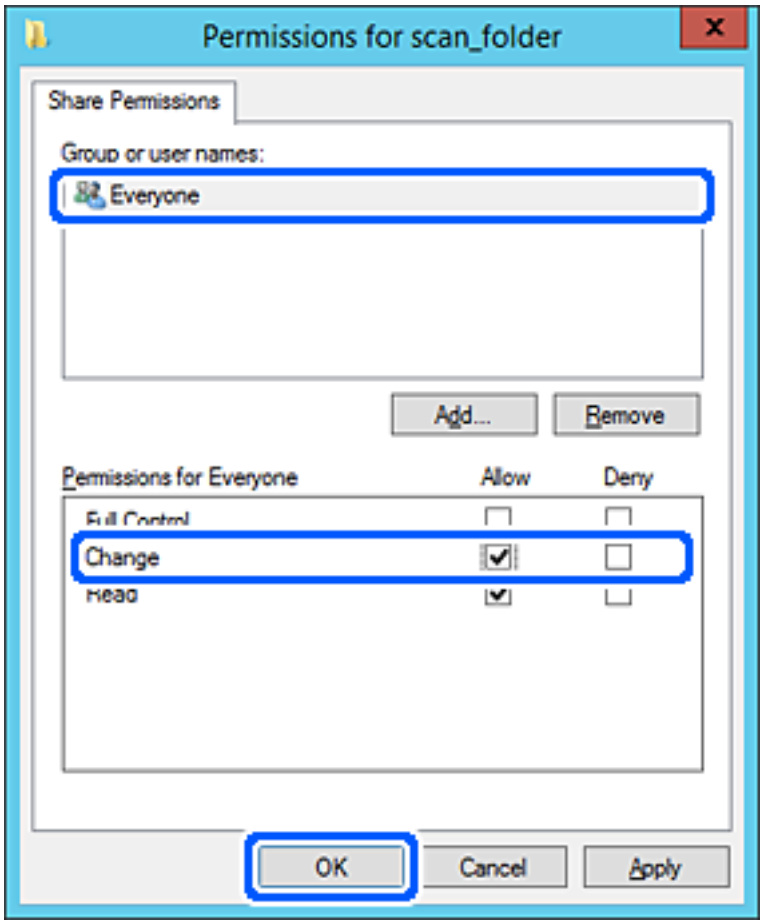
5. Klik op **Geavanceerd delen** op het tabblad **Delen**.



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

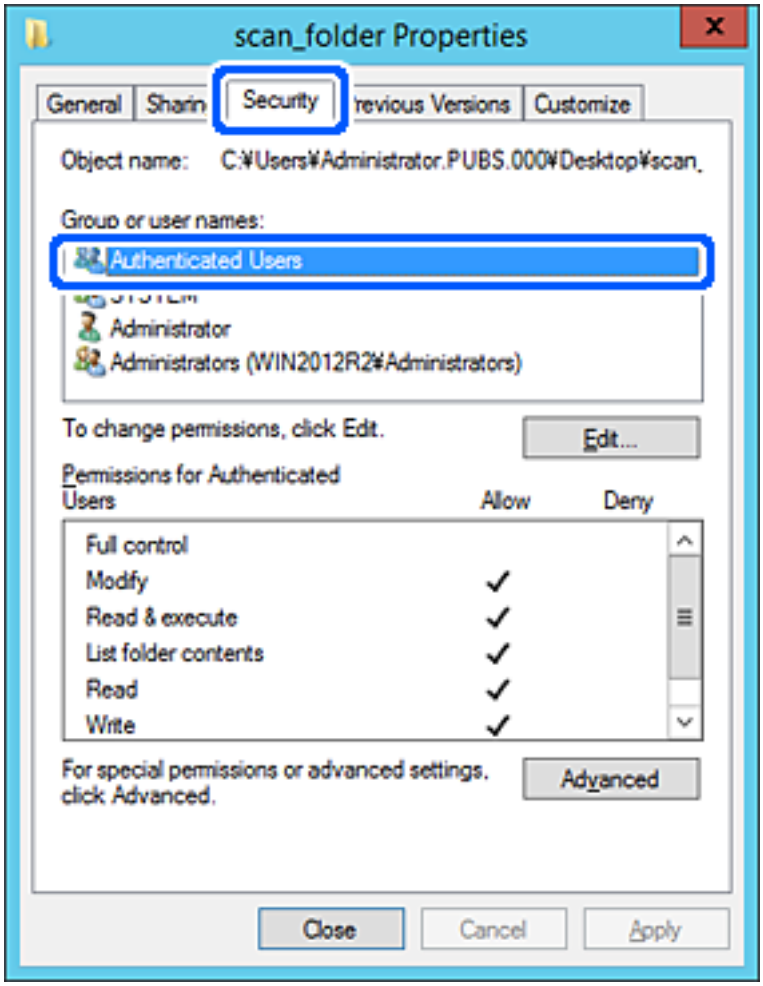


7. Selecteer de groep **Iedereen** bij **Groep of gebruikersnamen**, selecteer **Toestaan** bij **Wijzigen** en klik vervolgens op **OK**.



8. Klik op **OK**.

9. Selecteer het tabblad **Beveiliging** en selecteer vervolgens **Geverifieerde gebruikers** bij **Groep of gebruikersnamen**.

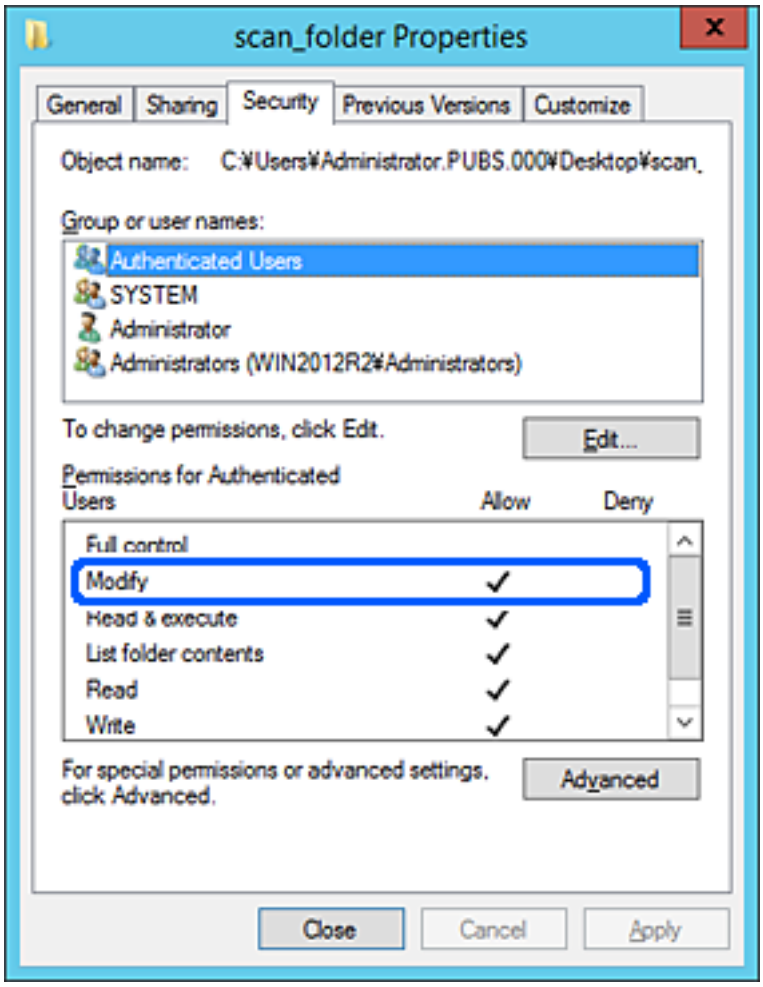


"Geverifieerde gebruikers" is de speciale groep die alle gebruikers omvat die zich bij dat domein of die computer kunnen aanmelden. Deze groep wordt alleen weergegeven als de map direct onder de hoofdmap wordt gemaakt.

Als deze niet wordt weergegeven, klikt u op **Bewerken** om deze toe te voegen. Raadpleeg voor meer informatie Gerelateerde informatie.

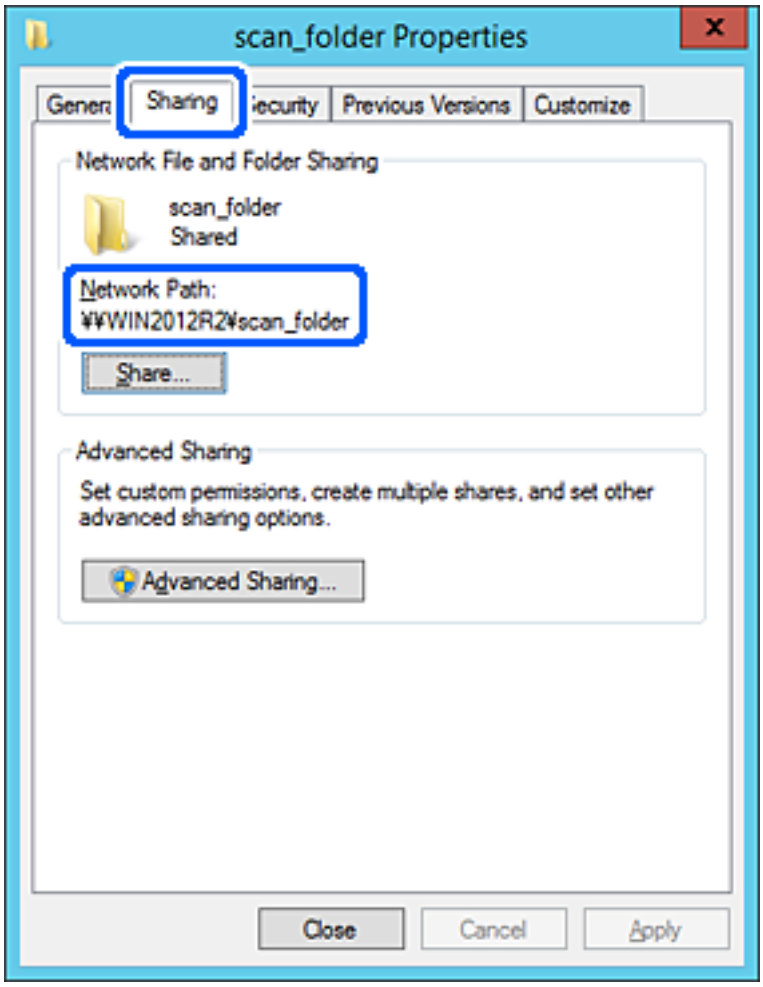
10. Controleer of **Toestaan** is geselecteerd bij **Wijzigen** in **Machtigingen voor geverifieerde gebruikers**.

    Als deze optie niet is geselecteerd, selecteert u **Geverifieerde gebruikers**, klikt u op **Bewerken**, selecteert u **Toestaan** bij **Bewerken** in **Machtigingen voor geverifieerde gebruikers** en klikt u op **OK**.



11. Selecteer het tabblad **Delen**.

    Het netwerkpad van de gedeelde map wordt weergegeven. Dit wordt gebruik bij het registreren van de contactpersonen in de scanner. Noteer dit.



12. Klik op **OK** of **Sluiten** om het scherm te sluiten.

    Controleer of het vanaf de computers in hetzelfde domein mogelijk is om het bestand in de gedeelde map te lezen of hiernaar te schrijven.

Gerelateerde informatie

➡ "Een groep of gebruiker toevoegen die toegang heeft" op pagina 60

➡ "Een bestemming opslaan in de contactpersonenlijst met Web Config" op pagina 65

Voorbeeld van configuratie voor een pc

Deze uitleg vormt een voorbeeld voor het maken van een gedeelde map op het bureaublad van de gebruiker die momenteel bij de computer is aangemeld.

De gebruiker die zich aanmeldt bij de computer en beheerdersrechten heeft, heeft toegang tot de bureaubladmap en de documentmap onder de gebruikersmap.

Stel deze configuratie in wanneer u lezen en schrijven in de gedeelde map door andere gebruikers van een pc NIET wilt toestaan.

- ❏ Locatie om gedeelde map te maken: bureaublad
- ❏ Mappad: C:\Gebruikers\xxxx\Bureaublad\scan_folder
- ❏ Toegangsmachtiging via het netwerk (Sharemachtigingen): Iedereen
- ❏ Toegangsmachtiging op het bestandssysteem (Beveiliging): voeg dit niet toe of voeg Gebruikers-/Groepsnamen in om toegang toe te staan

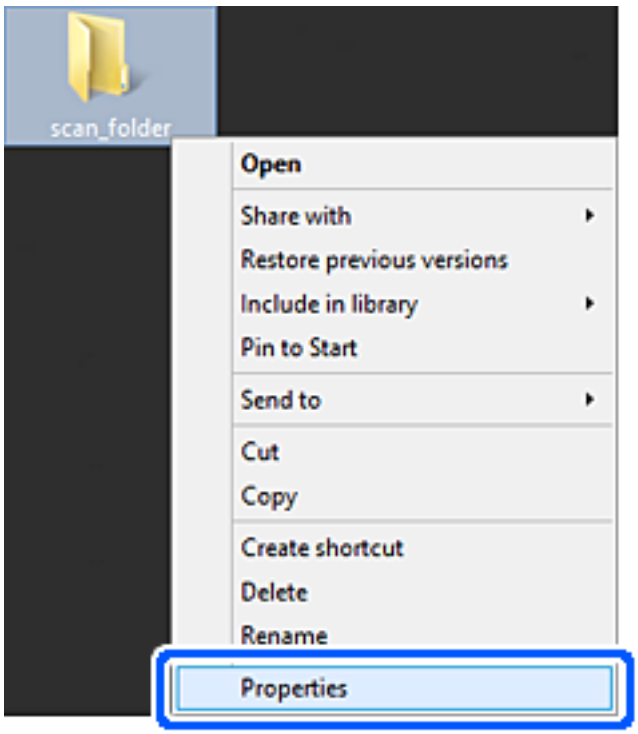
1. Meld u met het gebruikersaccount van de beheerder aan bij de computer waarop de gedeelde map wordt gemaakt.

2. Open de verkenner.

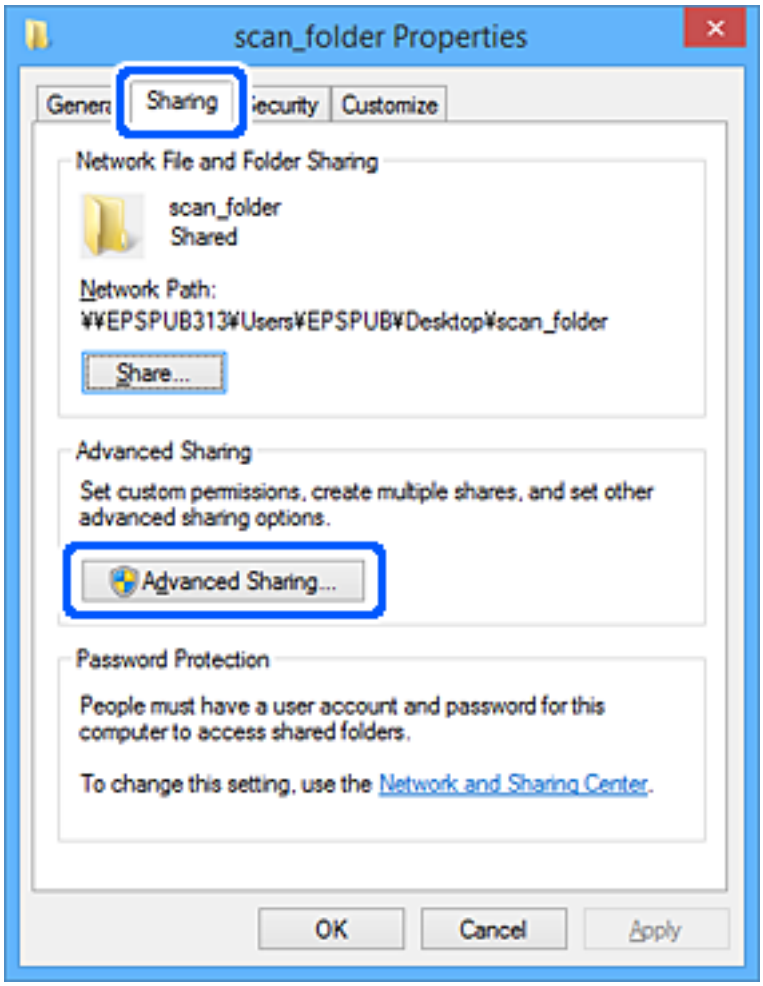
3. Maak de map op het bureaublad en noem deze "scan_folder".

   Voer voor de mapnaam tussen 1 en 12 alfanumerieke tekens in. Als u de tekenlimiet voor de mapnaam overschrijdt, hebt u mogelijk vanuit een andere omgeving geen toegang tot de map.

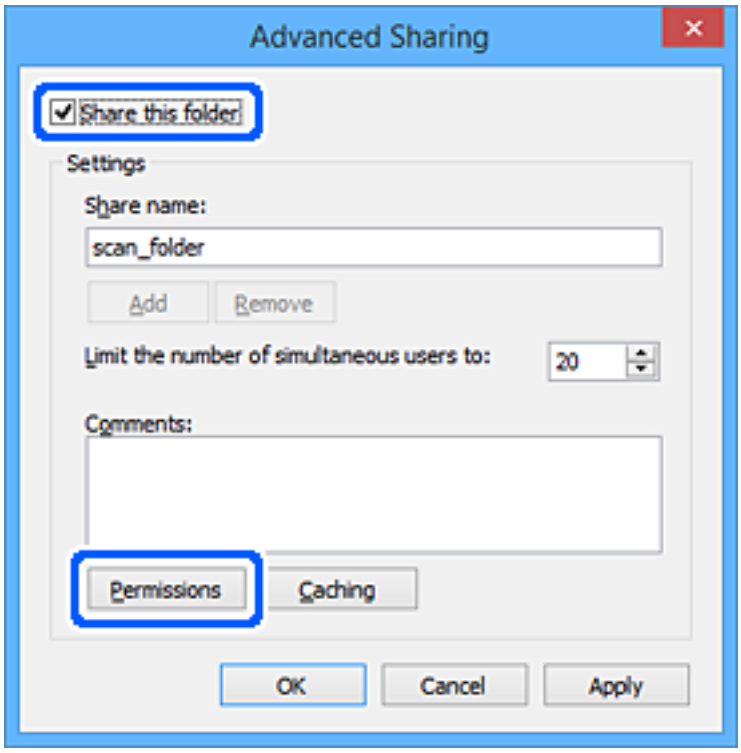
4. Klik met de rechtermuisknop op de map en selecteer **Eigenschappen**.



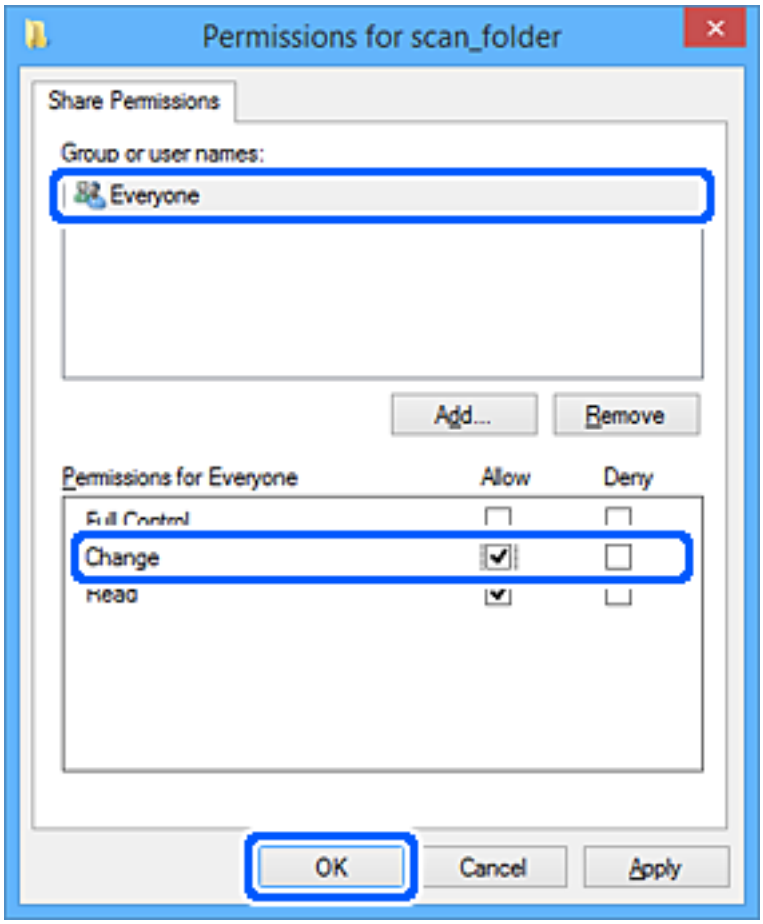
5. Klik op **Geavanceerd delen** op het tabblad **Delen**.



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



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



8. Klik op **OK**.

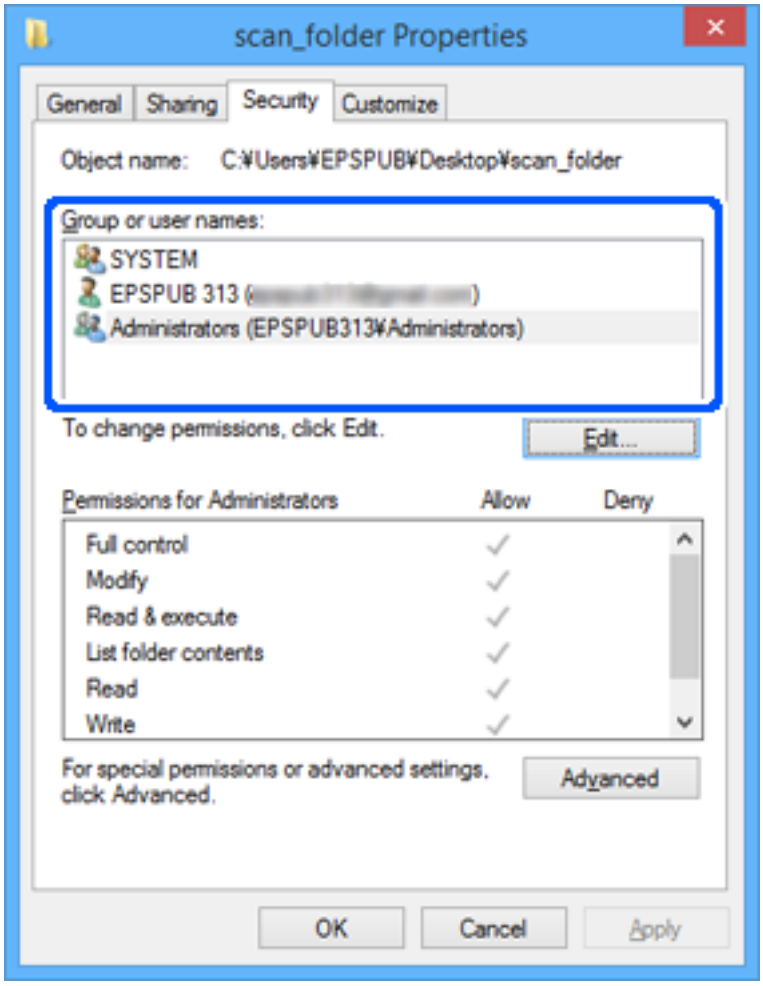
9. Selecteer het tabblad **Beveiliging**.

10. Controleer de groep of gebruiker bij **Groep of gebruikersnamen**.

    De hier weergegeven groep of gebruiker heeft toegang tot de gedeelde map.

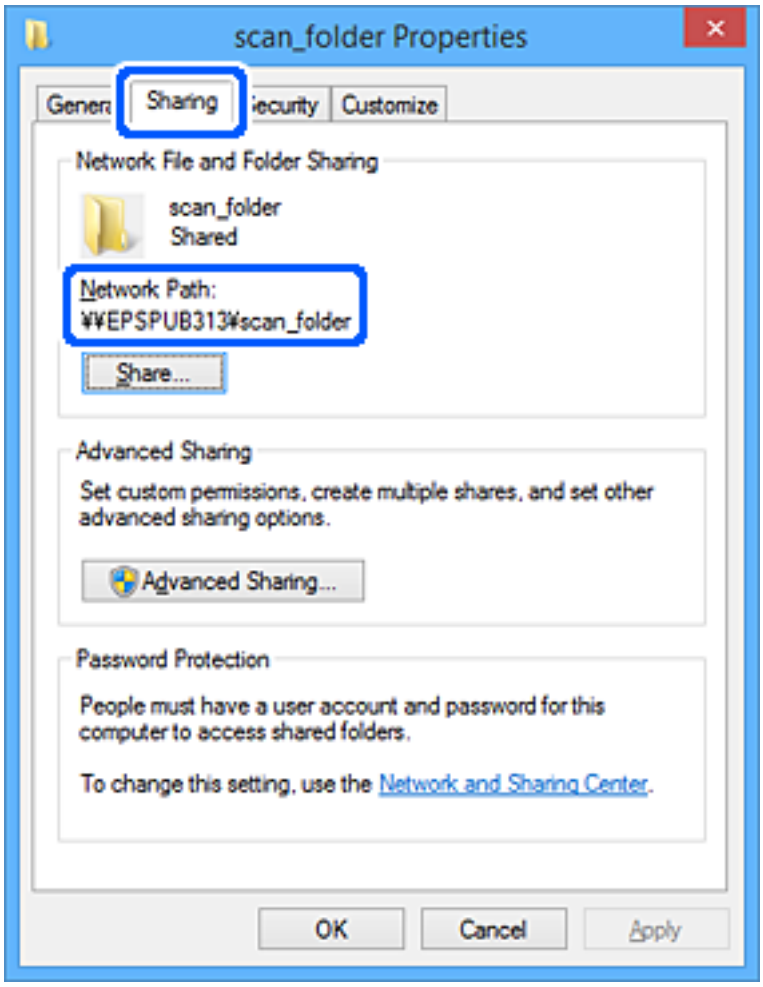
    In dit geval hebben de gebruiker die zich bij deze computer aanmeldt en de beheerder toegang tot de gedeelde map.

Voeg indien nodig toegangsmachtigingen toe. Klik op **Bewerken** om deze toe te voegen. Raadpleeg voor meer informatie Gerelateerde informatie.



11. Selecteer het tabblad **Delen**.

    Het netwerkpad van de gedeelde map wordt weergegeven. Dit wordt gebruik bij het registreren van de contactpersonen in de scanner. Noteer dit.



12. Klik op **OK** of **Sluiten** om het scherm te sluiten.

    Controleer of het vanaf de computers van groepen of gebruikers met toegangsmachtigingen mogelijk is om het bestand in de gedeelde map te lezen of hiernaar te schrijven.

Gerelateerde informatie

➡ "Een groep of gebruiker toevoegen die toegang heeft" op pagina 60
➡ "Een bestemming opslaan in de contactpersonenlijst met Web Config" op pagina 65

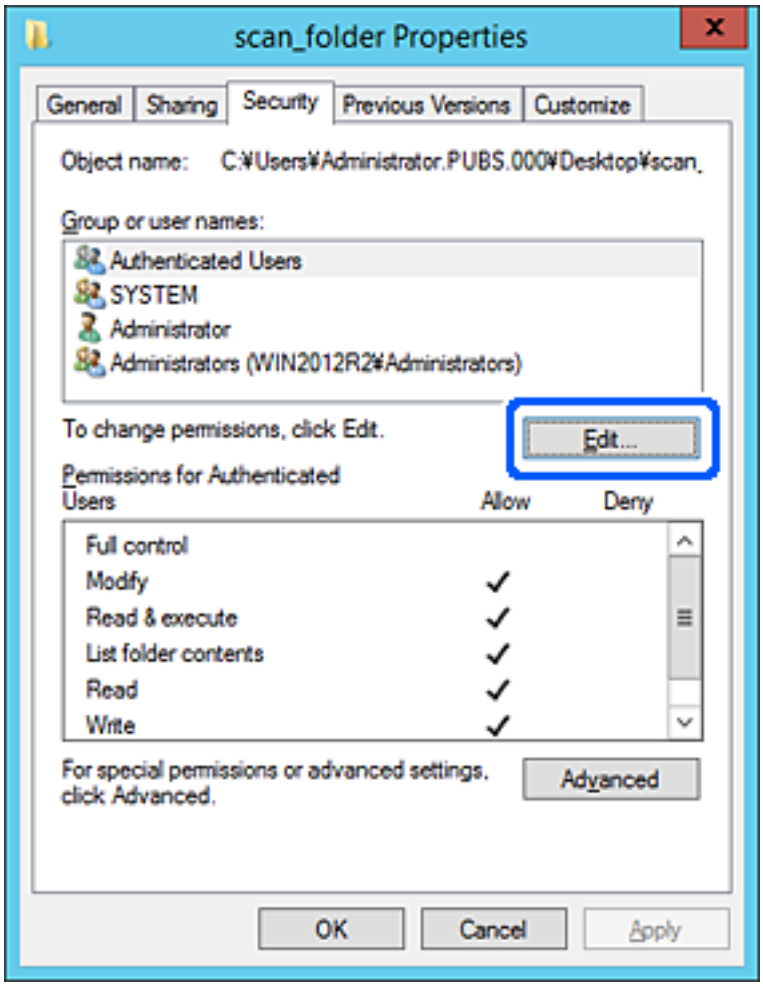
Een groep of gebruiker toevoegen die toegang heeft

U kunt groepen of gebruikers toevoegen die toegang hebben.

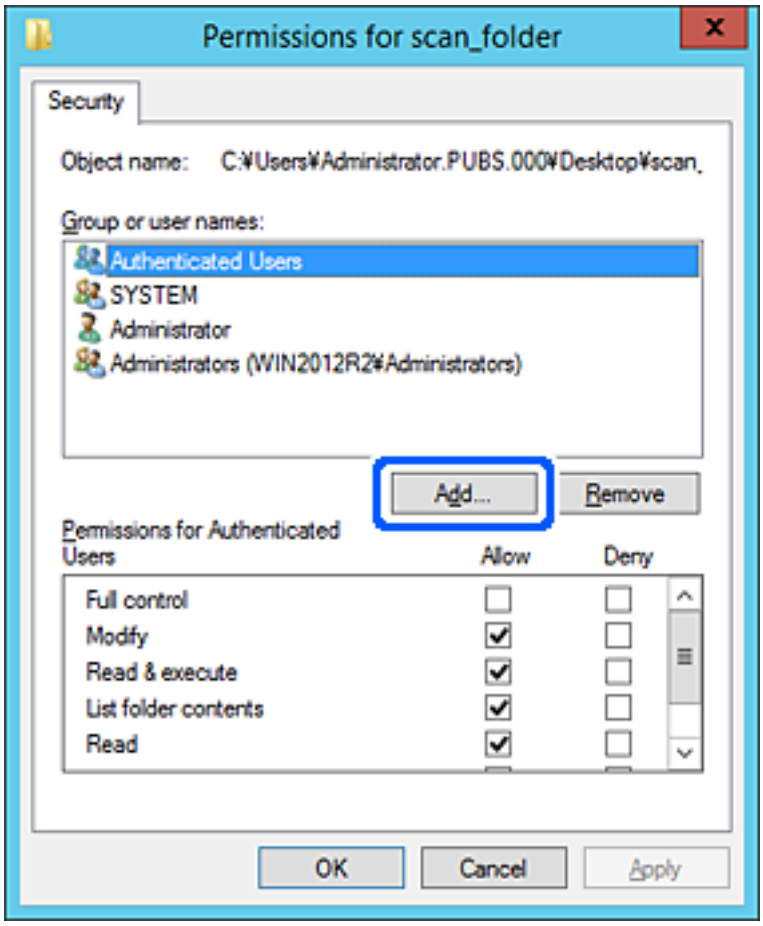
1. Klik met de rechtermuisknop op de map en selecteer **Eigenschappen**.

2. Selecteer het tabblad **Beveiliging**.

3. Klik op **Bewerken**.



4. Klik op **Toevoegen** onder **Groep of gebruikersnamen**.

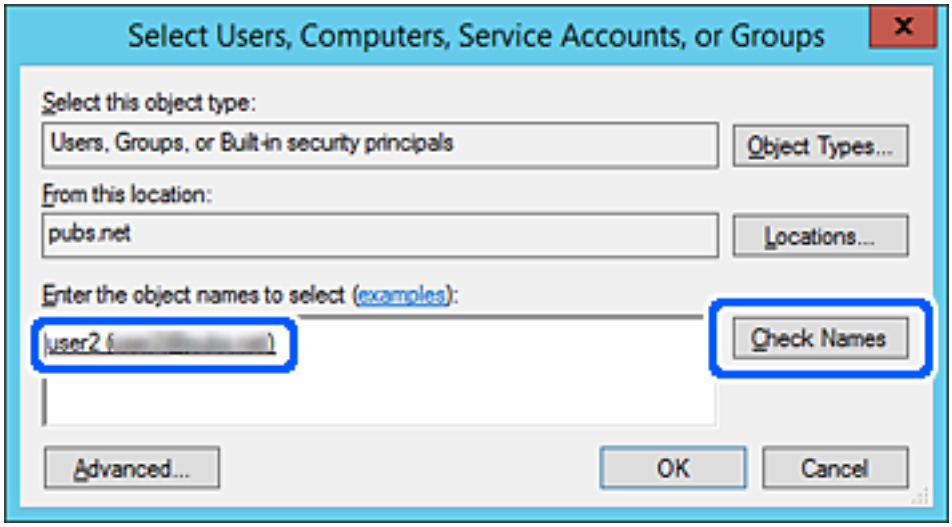


5. Voer de naam in van de groep of gebruiker die u toegang wilt geven en klik vervolgens op **Namen controleren**.

   De naam wordt onderstreept.

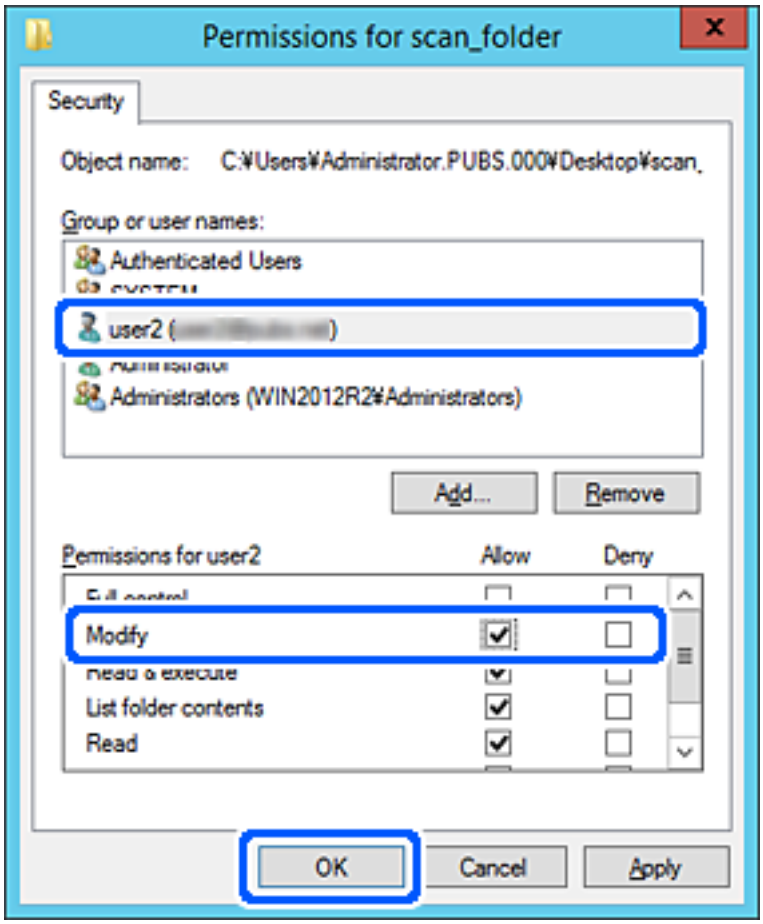
Opmerking:
Als u de volledige naam van de groep of de gebruiker niet weet, voert u een gedeelte van de naam in en klikt u vervolgens op ***Namen controleren****. De namen van groepen of gebruikers die overeenkomen met het gedeelte van de naam, worden weergegeven. U kunt vervolgens de volledige naam uit de lijst selecteren.*

Als slechts een naam overeenkomt, wordt de volledige naam onderstreept weergegeven in ***Geef de namen van de objecten op****.*



6. Klik op **OK**.

7. Selecteer op het tabblad Machtigingen de gebruikersnaam die al is ingevoerd in **Groep of gebruikersnamen**, selecteer de toegangsmachtiging bij **Wijziging** en klik op **OK**.



8. Klik op **OK** of **Sluiten** om het scherm te sluiten.

   Controleer of het vanaf de computers van groepen of gebruikers met toegangsmachtigingen mogelijk is om het bestand in de gedeelde map te lezen of hiernaar te schrijven.

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 71

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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

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-8). Als u dit niet opgeeft, laat u dit leeg.
Indexwoord	Voer een naam v an maximaal 30 tekens in Unicode (UTF-8) 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 registreren.
Toewijzen aan frequent gebruik	Selecteer om het geregistreerde 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 hier tussen 1 en 255 tekens in. Gebruik A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.
Netwerkmap (SMB)	
Opslaan in	\\"Mappad" Voer de locatie van de doelmap in. Deze locatie mag tussen 1 en 253 tekens bevatten in Unicode (UTF-8), zonder "\\". Voer het netwerkpad in dat wordt weergegeven in het eigenschappenscherm van de map. Raadpleeg de volgende informatie over het instellen van het netwerkpad. "Voorbeeld van configuratie voor een pc" op pagina 54
Gebruikersnaam	Voer een gebruikersnaam in van maximaal 30 tekens in Unicode (UTF-8) om een netwerkmap te openen. Vermijd hierbij het gebruik van stuurcodes (0x00 tot 0x1F, 0x7F).
Wachtwoord	Voer een wachtwoord in van maximaal 20 tekens in Unicode (UTF-8) om een netwerkmap te openen. 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 ASCII (0x20–0x7E) en laat "ftp://" of "ftps://" weg.

Items	Instellingen en toelichting
Gebruikersnaam	Voer een gebruikersnaam in van maximaal 30 tekens in Unicode (UTF-8) om toegang te krijgen tot een FTP-server. 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 van maximaal 20 tekens in Unicode (UTF-8) om toegang te krijgen tot een FTP-server. Vermijd hierbij het gebruik van stuurcodes (0x00 tot 0x1F, 0x7F). Als u dit niet opgeeft, laat u dit leeg.
Aansluitmodus	Selecteer de verbindingsmodus 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 ASCII (0x20–0x7E) en laat "http://" of "https://" weg.
Gebruikersnaam	Voer een gebruikersnaam van maximaal 30 tekens in Unicode (UTF-8) in om toegang te krijgen tot een server. Vermijd hierbij het gebruik van stuurcodes (0x00 tot 0x1F, 0x7F). Als u dit niet opgeeft, laat u dit leeg.
Wachtwoord	Voer een wachtwoord van maximaal 20 tekens in Unicode (UTF-8) in om toegang te krijgen tot een server. 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.

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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

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 eigenschappenscherm 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 eigenschappenscherm 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.

Items	Instellingen en toelichting
Veilige verbinding	Geef hier de verificatiemethode op die de scanner moet gebruiken voor toegang tot de LDAP-server.
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. ❏ De scanner en de DNS-server kunnen communiceren. ❏ De tijd van de scanner, de KDC-server en de server die vereist is voor verificatie (LDAP-server, SMTP-server, bestandsserver) is gesynchroniseerd. ❏ 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: ❏ Het LDAP-serveradres of het poortnummer onjuist is. ❏ Er een time-out is opgetreden. ❏ **Niet gebruiken** is geselecteerd voor **LDAP-server gebruiken**. ❏ 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 tijdinstellingen van de scanner en de LDAP-server niet overeenkomen.
Verificatie mislukt. Controleer de instellingen.	Deze melding wordt weergegeven wanneer: ❏ **Gebruikersnaam** en/of **Wachtwoord** onjuist is. ❏ 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.

Document Capture Pro Server gebruiken

Met Document Capture Pro Server kunt u de sorteermethode, de indeling voor opslaan en de bestemming voor doorsturen beheren voor een document dat is gescand vanaf het bedieningspaneel van de scanner. U kunt een eerder op de server vastgelegde taak oproepen en uitvoeren vanaf het bedieningspaneel van de scanner.

Installeer dit op de servercomputer.

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

De servermodus instellen

Als u Document Capture Pro Server wilt gebruiken, stelt u dit als volgt in.

1. Open Web Config en selecteer het tabblad **Scannen** > **Document Capture Pro**.

2. Selecteer **Servermodus** voor **Modus**.

3. Voer het adres in van de server waarop Document Capture Pro Server is geïnstalleerd bij **Serveradres**.

   Voer tussen 2 en 255 tekens in. Gebruik de IPv4-, IPv6- of FQDN-indeling of de hostnaam. Voor FQDN kunt u alfanumerieke tekens in ASCII (0x20–0x7E) en "-" gebruiken, behalve aan het begin en eind van het adres.

4. Klik op **OK**.

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

AirPrint instellen

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) zijn ingeschakeld.

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** > **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** > **Netwerkcentrum** > **Adapterinstellingen wijzigen**. Open het eigenschappenscherm van de gebruikte verbinding en open vervolgens het eigenschappenscherm 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

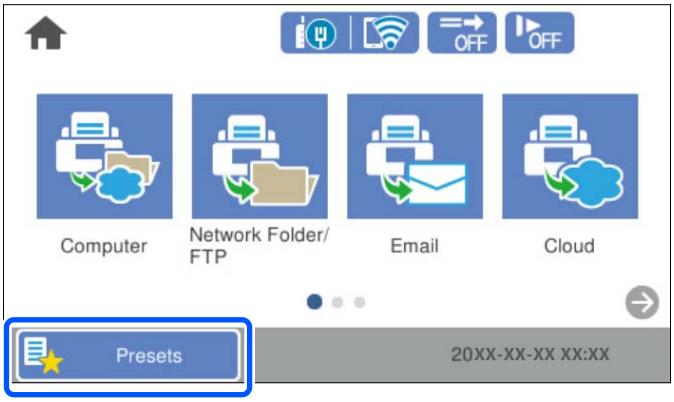
U kunt veelgebruikte scaninstellingen opslaan als **Presets**. U kunt maximaal 48 voorinstellingen opslaan.

Opmerking:

- *U kunt de huidige instellingen opslaan door* ☆ *te selecteren in het startscherm voor scannen.*
- *U kunt **Presets** ook opslaan in Web Config.*

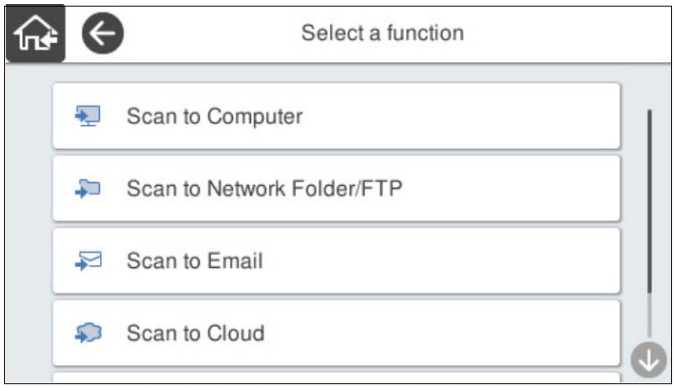
  *Selecteer het tabblad **Scannen** > **Presets**.*
- *Als u **Scan naar computer** selecteert tijdens het opslaan, kunt u de taak die in Document Capture Pro is gemaakt, opslaan als **Presets**. Deze optie is alleen beschikbaar voor computers die met een netwerk zijn verbonden. Sla de taak van tevoren 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.

  Wanneer u Document Capture Pro Server gebruikt, krijgt **Instelling Snel verzenden** in de voorinstellingen van de scanner voorrang op de software, zelfs als u de software zo instelt dat de inhoud van een taak moet worden bevestigd voor het scannen.
- ❏ **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 81
- ❏ 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 82
- ❏ Pictogram verwijderen: hiermee verwijdert u pictogrammen van het startscherm.
  "Pictogram verwijderen" op pagina 83
- ❏ Pictogram verplaatsen: hiermee wijzigt u de volgorde van de pictogrammen.
  "Pictogram verplaatsen" op pagina 84
- ❏ Standaard pictogramweergave herstellen: hiermee kunt u de standaardinstellingen voor het startscherm terugzetten.
- ❏ Achtergrondafbeelding: hiermee kunt u de achtergrondkleur van het startscherm wijzigen.

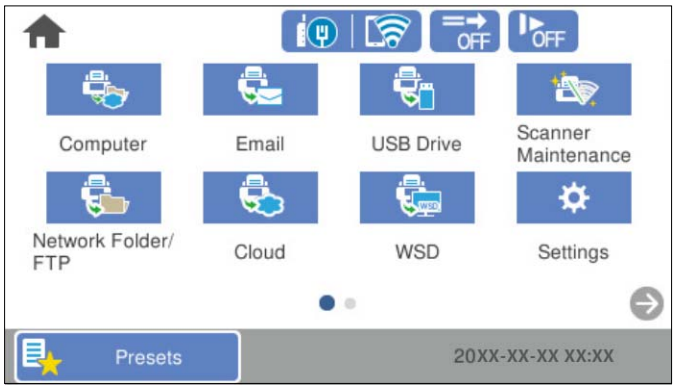
De Indeling van het startscherm wijzigen

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

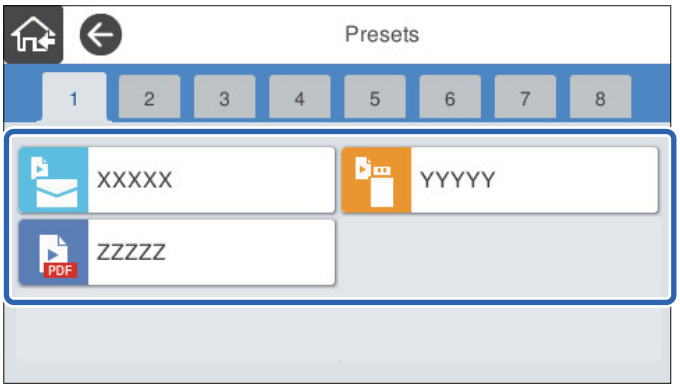
1. Selecteer **Instel.** > **Startscherm bewerken** > **Pictogram toevoegen** op het bedieningspaneel van de scanner.

2. Selecteer **Functie** of **Presets**.

   ❏ Functie: hiermee kunt u de standaardfuncties bekijken die op het startscherm worden weergegeven.

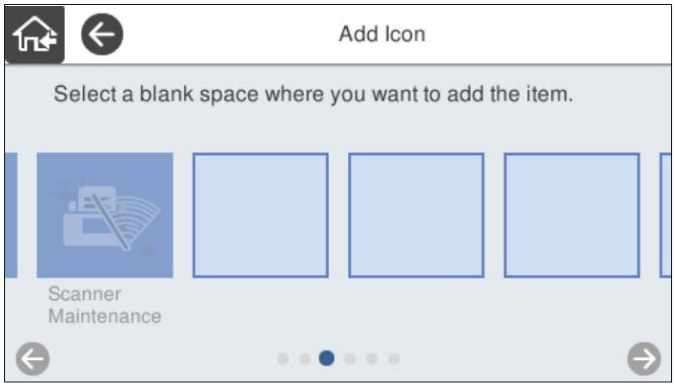
❏ Presets: hiermee geeft u de opgeslagen voorinstellingen weer.

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.

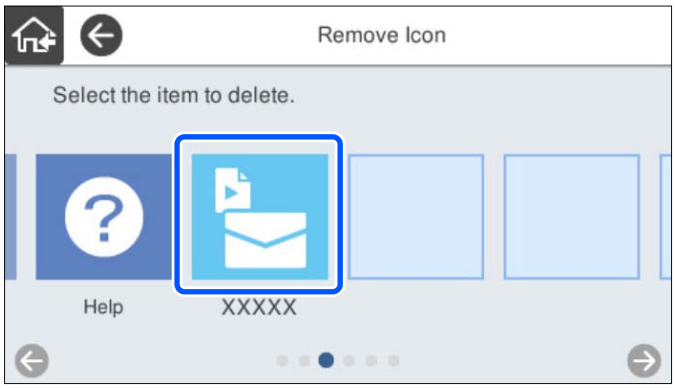


5. Selecteer om terug te keren naar het startscherm en dit te controleren.

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.

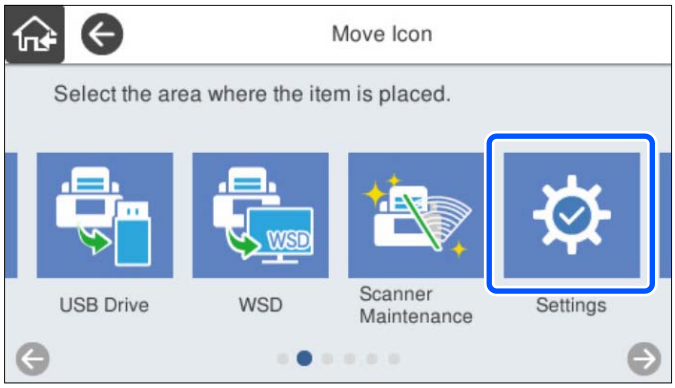
   Herhaal stap 2 en 3 om meer pictogrammen te verwijderen.

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

Pictogram verplaatsen

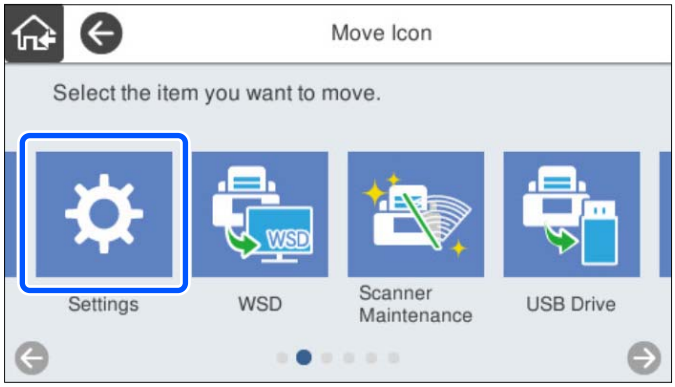
1. Selecteer **Instel.** > **Startscherm bewerken** > **Pictogram verplaatsen** op het bedieningspaneel van de scanner.

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

Inleiding tot functies voor productbeveiliging

In dit deel maakt u kennis met de beveiligingsfuncties van Epson-apparaten.

Functienaam	Functietype	Wat moet worden ingesteld	Wat moet worden voorkomen
Instelling voor het beheerderswachtwoord	Hiermee vergrendelt u de systeeminstellingen, zoals de verbindingsinstelling 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 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 87
➡ "De externe interface uitschakelen" op pagina 93

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: het serienummer van de scanner*

U vindt het serienummer op het etiket aan de achterzijde van de scanner.

U kunt het beheerderswachtwoord wijzigen via Web Config, het bedieningspaneel van de scanner of Epson Device Admin. Raadpleeg de gebruikershandleiding of Help-functie 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.**.

   Voer ten minste één teken in voor het nieuw wachtwoord.

   Opmerking:
   Hieronder staan de standaardwaarden voor de beheerdersgegevens.

   ❏ *Gebruikersnaam: geen (leeg)*

   ❏ *Wachtwoord: het serienummer van de scanner*

   U vindt het serienummer op het etiket aan de achterzijde van de scanner.

   > ***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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

Het beheerderswachtwoord wijzigen op het bedieningspaneel

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:
   De fabrieksinstelling (standaardwaarde) voor het beheerderswachtwoord is het serienummer van de scanner.

   U vindt het serienummer op het etiket aan de achterzijde van de scanner.

5. Voer uw nieuwe wachtwoord in.

   Voer ten minste één teken in.

> ***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.

Opmerking:
Als u Verificatie-instellingen inschakelt op de scanner, wordt Instelling vergrendelen ook ingeschakeld voor het bedieningspaneel. Het bedieningspaneel kan niet worden ontgrendeld wanneer Verificatie-instellingen is ingeschakeld.

Ook als u Verificatie-instellingen uitschakelt, blijft Instelling vergrendelen ingeschakeld. Als u deze optie wilt uitschakelen, kunt u dit doen via het bedieningspaneel of Web Config.

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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

Items voor Instelling vergrendelen in het menu Instel.

Dit is een lijst met items die bij 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	✓
	Datum/tijd instellen	✓
	Taal/Language	✓/-*
	Toetsenbord (Afhankelijk van uw regio is deze functie mogelijk niet beschikbaar.)	-
	Time-out bewerking	✓
	PC-verbinding via USB	✓
	Direct inschakelen	✓
Scannerinstellingen		-
	Langzaam	-
	Stoptiming voor dubbele toevoer	✓
	DFDS-functie	-
	Papierbescherming	✓
	Vuildetector	✓
	Ultrasone detectie dubbele toevoer	✓
	Time-out Automatische invoermodus	✓
	Ontvanger bevestigen	✓
Startscherm bewerken		✓

Menu Instel.		**Instelling vergrendelen**
	Indeling	✓
	Pictogram toevoegen	✓
	Pictogram verwijderen	✓
	Pictogram verplaatsen	✓
	Standaard pictogramweergave herstellen	✓
	Achtergrondafbeelding	✓
Gebruikersinstellingen		✓
	Netwerkmap/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		✓

Menu Instel.			**Instelling vergrendelen**
	Contacten-beheer		✓
	Beheerdersinstellingen		✓
	Beperkingen		✓
	Wachtwoordcodering		✓
	Klantonderzoek		✓
	WSD-instellingen		✓
	Standaardinst. herstellen		✓
	Firmware-update		✓
Apparaatgegevens			-
	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		-
	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.		✓
Waarschuwingsinstellingen standaardreiniging			✓

Menu Instel.		Instelling vergrendelen
	Waarschuwingsinst.	✓
	Inst. tellerwaarsch.	✓

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

Als beheerder inloggen op het bedieningspaneel

U kunt een van de volgende methoden gebruiken via het bedieningspaneel van de scanner in te loggen als beheerder.

1. Tik rechtsboven in het scherm op  .
   - ❏ Wanneer Verificatie-instellingen is ingeschakeld, wordt het pictogram weergegeven op het scherm **Welkom** (het stand-byscherm voor verificatie).
   - ❏ Wanneer Verificatie-instellingen is uitgeschakeld, wordt het pictogram weergegeven op het startscherm.
2. Tik op **Ja** wanneer het bevestigingsscherm wordt weergegeven.
3. Voer het beheerderswachtwoord in.

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

Tik om uit te loggen rechtsboven in het startscherm op  .

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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

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 netwerkverbindingsstatus, 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 e-mailserver configureren" op pagina 42

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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

Items voor e-mailmeldingen

Items	Instellingen en toelichting
Beheerderswachtwoord gewijzigd	Melding wanneer het beheerderswachtwoord is gewijzigd.

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

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: het serienummer van de scanner*

U vindt het serienummer op het etiket aan de achterzijde van de scanner. Als u de standaardinstellingen voor het beheerderswachtwoord herstelt, worden de beginwaarden teruggezet.

Geavanceerde beveiligingsinstellingen

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-pakketeenheid beschermt (versleuteling en verificatie), kunt u veilig onbeveiligde protocollen communiceren.	Maak een basisbeleid en een afzonderlijk beleid om de client of gegevenstypen die 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 99

➡ “SSL/TLS-communicatie met de scanner” op pagina 107

➡ “Versleutelde communicatie met IPsec/IP-filtering” op pagina 109

➡ "De scanner verbinden met een IEEE802.1X-netwerk" op pagina 120

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.

Configureeer 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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

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-netwerkmap.

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-locatienaam.
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-locatienaam.

LLTD-instellingen

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

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-tekens (0x20 tot 0x7E) in.
Communitynaam (lezen/schrijven)	Voer 0 tot 32 ASCII-tekens (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 103

➡ “Een zelfondertekend certificaat bijwerken” op pagina 106

➡ “Een CA-certificaat configureren” op pagina 107

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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

Instellingen voor een CSR

Items	Instellingen en toelichting
Sleutellengte	Selecteer een sleutellengte voor een CSR.
Algemene naam	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. Het eerste element wordt opgeslagen als de algemene naam. Andere elementen worden opgeslagen in het aliasveld van de certificaathouder. Voorbeeld: IP-adres van de scanner: 192.0.2.123, scannernaam: EPSONA1B2C3 Algemene naam: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

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 privésleutelbestand 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 privésleutel 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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36
➡ "Een CA-ondertekend Certificaat configureren" op pagina 103

➡ "Een CA-certificaat configureren" op pagina 107

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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

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-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**.

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	Alle adressen*3

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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

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

➡ “Webconfiguratie uitvoeren op een webbrowser” op pagina 36

➡ “Een CA-ondertekend Certificaat configureren” op pagina 103

➡ “Een CA-certificaat configureren” op pagina 107

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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

Instellingen voor een IEEE 802.1X-netwerk

Items	Instellingen en toelichting	
IEEE802.1X (bekabeld LAN)	U kunt de instellingen van de pagina in- of uitschakelen (**IEEE802.1X** > **Basis**) voor IEEE802.1X (bekabeld LAN).	
IEEE802.1X (Wi-Fi)	De verbindingsstatus van IEEE802.1X (Wi-Fi) wordt weergegeven.	
Verbindingsmethode	De verbindingsmethode van het huidige netwerk wordt weergegeven.	
EAP-type	Selecteer een optie voor een verificatiemethode tussen de scanner en een RADIUS-server.	
	EAP-TLS	U moet een door een CA ondertekend certificaat aanvragen en importeren.
	PEAP-TLS	
	PEAP/MSCHAPv2	U moet een wachtwoord configureren.
	EAP-TTLS	
Gebruikers-ID	Configureer een id die moet worden gebruikt voor een verificatie van een RADIUS-server. Voer 1 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in.	
Wachtwoord	Configureer hier een wachtwoord voor verificatie van de scanner. Voer 1 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in. Als u een Windows-server gebruikt als RADIUS-server, kunt u maximaal 127 tekens invoeren.	
Wachtwoord bevestigen	Voer het geconfigureerde wachtwoord in ter bevestiging.	
Server-ID	U kunt een server-id configureren voor verificatie bij een opgegeven RADIUS-server. De verificator controleert of de server-id al dan niet voorkomt in het veld subject/subjectAltName van het servercertificaat dat wordt verzonden door een RADIUS-server. Voer 0 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in.	

Items	Instellingen en toelichting	
Certificaatvalidatie	U kunt de certificaatvalidatie instellen, ongeacht de verificatiemethode. Importeer het certificaat in **CA-certificaat**.	
Anonieme naam	Als u **PEAP-TLS** of **PEAP/MSCHAPv2** selecteert bij **EAP-type**, kunt u voor fase 1 van de PEAP-verificatie een anonieme naam opgeven in plaats van een gebruikers-id. Voer 0 tot 128 1-byte ASCII-tekens (0x20 tot 0x7E) in.	
Codeersterkte	U kunt kiezen uit het volgende.	
	Hoog	AES256/3DES
	Midden	AES256/3DES/AES128/RC4

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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36
➡ "Versleutelde communicatie met IPsec/IP-filtering" op pagina 109

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 109

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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

➡ "Versleutelde communicatie met IPsec/IP-filtering" op pagina 109

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 109

Geen toegang tot de scanner na het configureren van IEEE 802.1X

De IEEE 802.1X-instellingen 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.

Verbind de scanner en een computer en configureer IEEE 802.1X opnieuw.

Gerelateerde informatie

➡ "Een IEEE 802.1X-netwerk configureren" op pagina 120

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:

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

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

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

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

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 104

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 106

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 103

Er wordt een waarschuwing over een digitaal certificaat weergegeven

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

Berichten	Oorzaak/Wat doen
Ongeldig bestand.	**Oorzaak:** U importeert geen certificaatbestand in de indeling X509. **Wat doen:** Selecteer het juiste certificaat dat afkomstig is van een vertrouwde certificeringsinstantie.
	Oorzaak: Het bestand dat u hebt geïmporteerd, is te groot. De bestandsgrootte is maximaal 5 kB. **Wat doen:** Als u het juiste bestand hebt geselecteerd, is het certificaat mogelijk beschadigd of vals.
	Oorzaak: De keten in het certificaat is ongeldig. **Wat doen:** Zie de website van de certificeringsinstantie voor meer informatie over certificaten.
Kan geen Servercertificaten gebruiken die meer dan drie CA-certificaten bevatten.	**Oorzaak:** Het certificaatbestand in de indeling PKCS#12 bevat meer dan drie CA-certificaten. **Wat doen:** Importeer elk certificaat door conversie van PKCS#12 in PEM of importeer het certificaatbestand in de indeling PKCS#12 (maximaal twee CA-certificaten).
Het Certificaat is verlopen. Controleer of het Certificaat geldig is of controleer de datum en tijd op het product.	**Oorzaak:** Het certificaat is vervallen. **Wat doen:** ❏ Als het certificaat vervallen is, moet u een nieuw certificaat aanvragen en importeren. ❏ Als het certificaat niet vervallen is, zorg er dan voor dat de datum en tijd van de scanner goed zijn ingesteld.
Persoonlijke sleutel vereist.	**Oorzaak:** Er is geen private sleutel aan het certificaat gekoppeld. **Wat doen:** ❏ Als het certificaat de indeling PEM/DER heeft en is verkregen met een CSR en een computer, geef dan het sleutelbestand op. ❏ Als het certificaat de indeling PKCS#12 heeft en is verkregen met een CSR en een computer, maak dan een bestand met daarin de sleutel.
	Oorzaak: U hebt het PEM/DER-certificaat dat is verkregen met een CSR en Web Config opnieuw geïmporteerd. **Wat doen:** Als het certificaat de indeling PEM/DER heeft en is verkregen met een CSR en Web Config, kunt u het maar eenmaal importeren.

Berichten	Oorzaak/Wat doen
Setup mislukt.	**Oorzaak:** De configuratie kan niet worden voltooid, omdat de communicatie tussen de scanner en computer is mislukt of het bestand kan niet worden gelezen als gevolg van fouten. **Wat doen:** Controleer het opgegeven bestand en de communicatie en importeer het bestand opnieuw.

Gerelateerde informatie

➡ “Digitale certificering” op pagina 102

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.

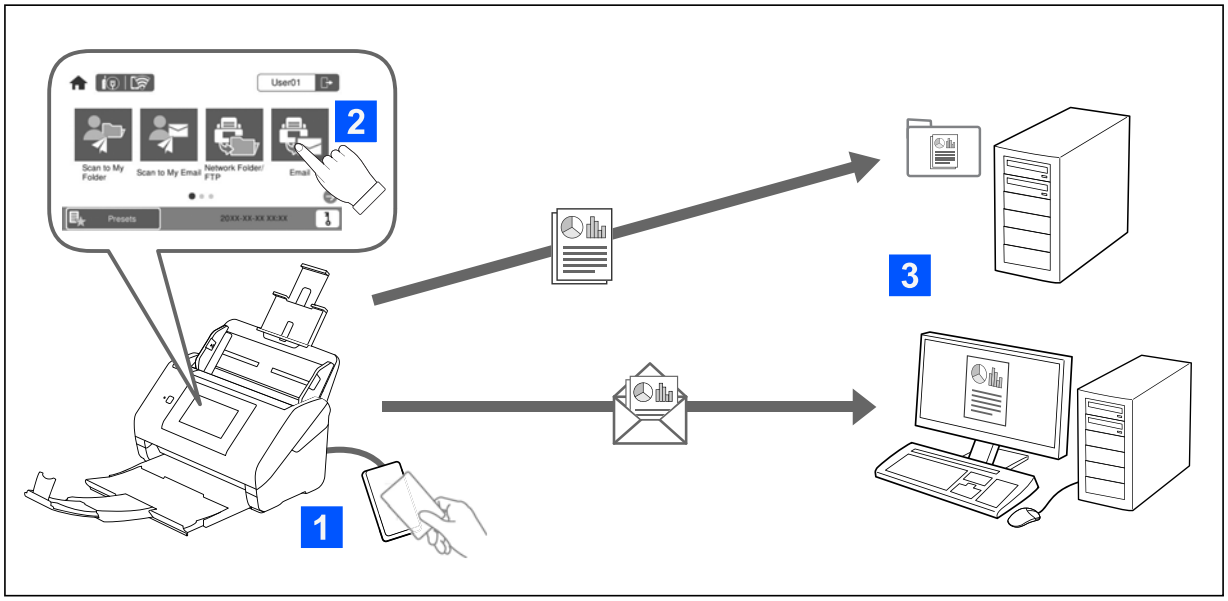
Als u een certificaat hebt op basis van een CSR die u met Web Config hebt gemaakt, kunt u het verwijderde certificaat niet opnieuw importeren. Maak een CSR en vraag een nieuw certificaat aan.

Gerelateerde informatie

➡ “Een door een CA ondertekend certificaat importeren” op pagina 104
➡ “Een door een CA ondertekend certificaat verwijderen” op pagina 105

Verificatie-instellingen

Over Verificatie-instellingen



Wanneer Verificatie-instellingen is ingeschakeld, is gebruikersverificatie vereist om het scannen te starten. U kunt de scanmethoden instellen die door elke gebruiker kunnen worden gebruikt en onbedoelde bewerkingen voorkomen.

U kunt het e-mailadres van de geverifieerde gebruiker opgeven als de scanbestemming (Scan naar Mijn e-mail) of gegevens van elke gebruiker opslaan in een persoonlijke map (Scannen naar Mijn map). U kunt ook andere scanmethoden opgeven.

Opmerking:

❏ *Wanneer Verificatie-instellingen is ingeschakeld, kunt u niet vanaf een computer of smart device scannen.*

❏ *Naast de Verificatie-instellingen die in deze handleiding aan bod komen, kunt u ook een verificatiesysteem opzetten met een verificatieserver. Gebruik Document Capture Pro Server Authentication Edition (de afgekorte naam is Document Capture Pro Server AE) om een systeem op te zetten. Neem voor meer informatie contact op met uw lokale Epson-kantoor.*

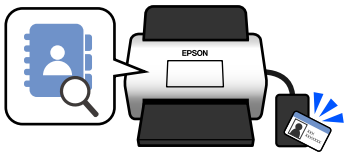
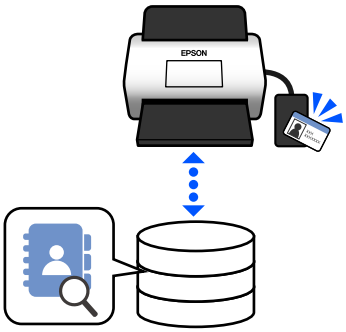
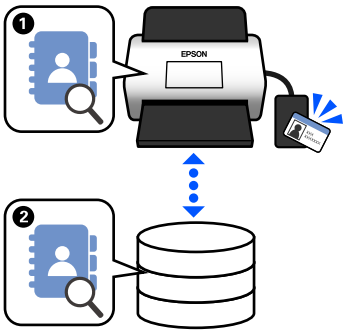
Beschikbare functies voor Verificatie-instellingen

Scanfunctie op het bedieningspaneel	Verificatie-instellingen	
	Wanneer de functie is ingeschakeld	Wanneer de functie is uitgeschakeld
Scannen naar Mijn map Afbeeldingen worden opgeslagen in de map die aan de geverifieerde gebruiker is toegewezen.	✓	-
Scannen naar Mijn e-mail Afbeeldingen worden verstuurd naar het e-mailadres van de geverifieerde gebruiker.	✓	-

Scanfunctie op het bedieningspaneel	Verificatie-instellingen	
	Wanneer de functie is ingeschakeld	**Wanneer de functie is uitgeschakeld**
Scan naar netwerkmap/FTP Afbeeldingen worden opgeslagen in een map in het netwerk.	✓	✓
Scan naar computer Afbeeldingen worden naar een verbonden computer verstuurd met behulp van taken die via Document Capture Pro (Windows)/Document Capture (Mac OS) zijn gemaakt. * Wanneer Verificatie-instellingen is ingeschakeld, kunt u alleen taken gebruiken die in **Presets** zijn geregistreerd.	✓*	✓
Scan naar e-mail Afbeeldingen worden verstuurd naar het e-mailadres dat u hebt ingesteld.	✓	✓
Scan naar cloud Afbeeldingen worden verstuurd naar de cloudservice die u hebt ingesteld.	✓	✓
Scannen naar USB-stick Afbeeldingen worden opgeslagen op een USB-stick die met de scanner is verbonden. Deze optie is alleen beschikbaar wanneer er geen verificatie-apparaat met de scanner is verbonden.	✓	✓
Scan naar WSD Afbeeldingen worden met behulp van de WSD-functie opgeslagen op een verbonden computer.	-	✓
Presets U kunt maximaal 48 vooraf ingestelde scanfuncties opslaan. U kunt maximaal vijf Presets toewijzen aan gebruikers die in de Lokale DB zijn geregistreerd. Toegewezen Presets zijn alleen beschikbaar voor gebruikers waaraan ze zijn toegewezen. Presets die niet aan gebruikers zijn toegewezen, kunnen door alle gebruikers worden gebruikt.	✓	✓

Over Verificatiemethode

Met deze scanner kunt u met behulp van de volgende methoden gegevens verifiëren zonder dat u een verificatieserver hoeft te bouwen.

	Lokale DB	LDAP	Lokale DB en LDAP
Locatie van gebruikers gegevens	**Scannergeheugen** Met deze verificatiemethode worden de gebruikersgegevens die in de scanner zijn geregistreerd gecontroleerd en vergeleken met de gebruiker die de scanfunctie gebruikt.	**LDAP-server*** Met deze verificatiemethode worden de gebruikersgegevens op de LDAP-server die met de scanner wordt gesynchroniseerd gecontroleerd. Aangezien maximaal 300 gebruikersgegevens op de LDAP-server tijdelijk in het cachegeheugen van de scanner kunnen worden opgeslagen, kan de verificatie met behulp van het cachegeheugen worden uitgevoerd als de LDAP-server uitvalt. * Een server die een directoryservice biedt om via LDAP te communiceren.	**Scannergeheugen en LDAP-server** De gebruikersgegevens die in de scanner zijn geregistreerd, worden eerst gecontroleerd (❶). Als er geen overeenkomst is, worden de gebruikersgegevens op de LDAP-server gecontroleerd (❷).
			
Aantal geregistreerde gebruikers	50 (scannergeheugen)	Onbeperkt (LDAP-server)	50 (scannergeheugen) Onbeperkt (LDAP-server)
Cachegeheugen van de scanner	-	300	Max. 300 (50 van de cachesleuven worden gedeeld met de Gebruikersinstellingen in de Lokale DB)
Inlogmethoden	U kunt de volgende methoden gebruiken. ❏ Een verificatiekaart gebruiken of een **Gebruikers-ID** en **Wachtwoord** invoeren ❏ Een verificatiekaart gebruiken of een **Identiteitsnummer** invoeren ❏ Een **Gebruikers-ID** en **Wachtwoord** invoeren ❏ Een **Gebruikers-ID** invoeren ❏ Een **Identiteitsnummer** invoeren		
Limieten van de functie "Scannen naar"	Voor elke gebruiker afzonderlijk instellen	Dezelfde instellingen voor alle LDAP-gebruikers	Lokale DB-gebruikers: afzonderlijk instellen LDAP-gebruikers: dezelfde instellingen voor alle gebruikers

	Lokale DB	LDAP	Lokale DB en LDAP
Presets toewijzen aan gebruikers	Maximaal 5 per gebruiker	- (Kan niet afzonderlijk worden ingesteld)	Lokale DB-gebruikers: maximaal 5 per gebruiker LDAP-gebruikers: -

Configuratiesoftware

Gebruik Web Config of Epson Device Admin voor de configuratie.

❏ Als u Web Config gebruikt, kunt u de scanner alleen via een webbrowser configureren.

"Web Config" op pagina 36

❏ Als u Epson Device Admin gebruikt, kunt u meerdere scanners tegelijk configureren met een configuratiesjabloon.

"Epson Device Admin" op pagina 37

De firmware van de scanner bijwerken

Werk de firmware van de scanner bij naar de nieuwste versie voordat u Verificatie-instellingen inschakelt. Verbind de scanner van te voren met internet.

Belangrijk:

Schakel de computer of scanner niet uit tijdens het bijwerken.

Instellen via Web Config:

Selecteer het tabblad **Apparaatbeheer** > **Firmware-update** en volg de instructies op het scherm om de firmware bij te werken.

Instellen via Epson Device Admin:

Select **Start** > **Firmware** > **Update** in het scherm "Apparatenlijst" en volg de instructies op het scherm om de firmware bij te werken.

Opmerking:

Als de nieuwste firmware al is geïnstalleerd, hoeft u niet bij te werken.

Een verificatieapparaat aansluiten en configureren

Als u een verificatieapparaat zoals een IC-kaartlezer wilt aansluiten en gebruiken, moet u eerst het apparaat configureren. Dit is niet nodig als u geen verificatieapparaat gebruikt.

Gerelateerde informatie

➡ "Het verificatieapparaat aansluiten" op pagina 136

➡ "Instellingen van verificatieapparaat" op pagina 137

Lijst met compatibele kaartlezers

Deze lijst garandeert niet dat de kaartlezers op de lijst werken.

Ja: ondersteund (de id-informatie kan worden gelezen met standaard kaartlezerinstellingen.)

Nee: niet compatibel

Fabrikant	Model	Modelnummer	Verificatiekaart							Modus
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
RF IDEAS	pcProx Plus	RDR-80081AKU	Ja	Ja*1	Ja*1	Ja*1	Nee	Nee	Nee	Toetsenbord
RF IDEAS	pcProx	RDR-7081BKU	Ja*1	Nee	Ja	Ja	Nee	Nee	Nee	Toetsenbord
RF IDEAS	pcProx	RDR-7581AKU	Ja	Nee	Ja*1	Ja*1	Nee	Nee	Nee	Toetsenbord
ELATEC	TWN3 MIFARE	T3DT-MB2BEL T3DT-MB2WEL	Nee	Nee	Ja	Ja	Nee	Nee	Nee	Toetsenbord
ELATEC	TWN3 MIFARE NFC	T3DT-FB2BEL T3DT-FB2WEL	Ja	Nee	Ja	Ja	Ja	Ja	Ja	Toetsenbord
ELATEC	TWN4 MULTI-TECH	T4DT-FB2BEL-PI T4DT-FB2WEL-PI	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Toetsenbord
ELATEC	TWN4 Multi-Tech 2 BLE-PI	T4LK-FB4BLZ-PI	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Toetsenbord
ELATEC	TWN4 Slim	T4QC-FC3B7	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Toetsenbord

Fabrikant	Model	Modelnummer	Verificatiekaart							Modus
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
HID Global	OMNIKEY 5427	OMNIKEY5427CK OMNIKEY5427CK gen2	Ja	Ja	Ja	Ja	Ja	Nee	Ja	Toetsenbord[*1]
ACS	ACR122U	ACR122U	Nee	Nee	Ja[*2]	Ja[*2]	Ja	Nee	Ja[*2]	PC/SC
ACS	ACR1252	ACR1252	Nee	Nee	Ja[*2]	Ja[*2]	Ja	Ja	Ja[*2]	PC/SC
Sony	PaSoRi	RC-S330/S	Nee	Nee	Ja[*2]	Ja[*2]	Ja[*2]	Ja[*2]	Ja[*2]	PaSoRi
Sony	PaSoRi	RC-S380/P RC-S380/S	Nee	Nee	Ja[*2]	Ja[*2]	Ja[*2]	Ja[*2]	Ja[*2]	PaSoRi
DMZ	Leitor RFID Universal	DMZ008	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Toetsenbord
DMZ	Leitor RFID Multi-125	DMZ087	Nee	Ja	Nee	Nee	Nee	Nee	Nee	Toetsenbord
DMZ	Leitor RFID Mifare	DMZ088	Nee	Nee	Ja	Ja	Nee	Nee	Nee	Toetsenbord
DMZ	Biometric & RFID Reader	DMZ073	Nee	Ja	Nee	Nee	Nee	Nee	Nee	Toetsenbord
inepro	SCR708	SCR708	Ja[*1]	Ja[*1]	Ja[*1]	Ja[*1]	Ja[*1]	Ja[*1]	Ja[*1]	Toetsenbord
Y Soft	YU03088 001	MU038 8	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Toetsenbord

Fabrikant	Model	Modelnummer	Verificatiekaart							Modus
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
Cartadis	TCM3 Cartadis MiFare Card Reader	ZTCM3-MIFARE	Nee	Nee	Ja	Ja	Nee	Nee	Ja	Toetsenbord
MICI Network Co., Ltd.	EM & Mifare Card Reader	mCR-600	Nee	Nee	Ja	Ja	Nee	Nee	Ja	Toetsenbord
NT-ware	MiCard Multi-Tech4-PI	T4DT-FB4WUF-PI	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Toetsenbord
NT-ware	MiCard Plus-2-V2	RDR-80081AGU-NT2-20	Ja*1	Ja*1	Ja*1	Ja*1	Nee	Nee	Nee	Toetsenbord
NT-ware	MiCard V3 Multi	MiCard V3 Multi	Ja	Ja	Ja	Ja	Ja	Ja	Nee	Toetsenbord

*1 U moet de instellingen van de kaartlezer wijzigen met behulp van de propriëtaire software van de fabrikant van de kaartlezer.

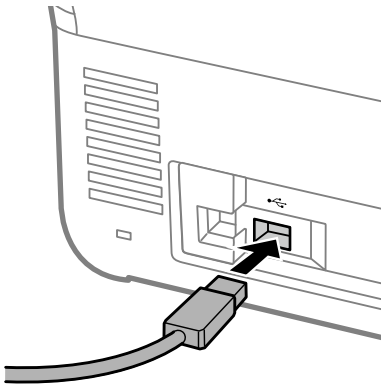
*2 Neem contact op met uw Epson-partner of lokale vertegenwoordiger voor meer informatie over het instellen van het product als u gegevens in een bepaald gebied op de kaart anders dan de standaard-id van de kaart als verificatie-id wilt gebruiken door de productinstellingen te configureren.

Het verificatieapparaat aansluiten

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 verbindingsstatus en verificatiekaartherkenning voor het verificatieapparaat controleren via het bedieningspaneel van de scanner.

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

Instellingen van verificatieapparaat

Stel de leesindeling in voor de ontvangen verificatiegegevens van een verificatiekaart.

U kunt de volgende leesmethode instellen voor het verificatieapparaat.

❏ Het specifieke gebied van de verificatiekaart lezen, zoals het werknemersnummer of de persoonlijke id.

❏ De verificatiekaartgegevens gebruiken, met uitzondering van de UID (unieke id-informatie zoals het serienummer).

Met een hulpprogramma kunt u de operationele parameters genereren. Neem contact op met uw leverancier voor meer informatie.

Opmerking:
Verificatiekaarten van verschillende fabrikanten gebruiken:

Door de UID (unieke id-informatie zoals het serienummer) te gebruiken, kunt u verschillende soorten verificatiekaarten door elkaar gebruiken. Bij het gebruik van andere kaartgegevens kunnen verschillende soorten verificatiekaarten niet door elkaar worden gebruikt.

Instellen via Web Config:

Selecteer het tabblad **Apparaatbeheer** > **Kaartlezer**.

Instellen via Epson Device Admin:

Selecteer **Beheerinstellingen** > **Verificatie-instellingen** > **Kaartlezer** in de configuratiesjabloon.

Item	Uitleg
Vendor ID	Stel de verkoper-id van het verificatieapparaat in waarmee het gebruik wordt beperkt. Gebruik hiervoor een code van 4 alfanumerieke tekens uit de reeks 0000 tot FFFF. Als u geen beperking wilt instellen, stelt u 0000 in.

Item	Uitleg
Product ID	Stel de product-id van het verificatieapparaat in waarmee het gebruik wordt beperkt. Gebruik hiervoor een code van 4 alfanumerieke tekens uit de reeks 0000 tot FFFF. Als u geen beperking wilt instellen, stelt u 0000 in.
Operationele parameter	Stel de bewerkingsparameter van het verificatieapparaat in. Gebruik hiervoor tussen 0 en 8192 tekens. Hiervoor zijn A–Z, a–z, 0–9, +, /, =, spatie en nieuwe regel zijn beschikbaar.
Kaartlezer	Selecteer de conversie-indeling voor het verificatieapparaat. U kunt de indelingsgegevens controleren. Klik op de koppeling in de productbeschrijving.
Opslagformaat Verificatiekaart-ID	Selecteer de conversie-indeling voor de verificatiegegevens van een id-kaart. U kunt de indelingsgegevens controleren. Klik op de koppeling in de productbeschrijving.
Bereik kaart-id instellen	Schakel specificatie van de leespositie in.
Beginpositie tekst	Geef de startpositie op voor het lezen van de id-informatie. U kunt een waarde tussen 1 en 4096 invoeren.
Aantal tekens	Geef het aantal tekens op dat moet worden gelezen vanaf de startpositie van de id-informatie. U kunt een waarde tussen 1 en 4096 invoeren.

Informatie over opslaan en configureren

Instellen

Configureer de benodigde instellingen op basis van de Verificatiemethode en de scanmethode die u gebruikt.

Belangrijk:

Controleer voordat u met de configuratie begint of de tijdinstelling van de scanner correct is.

Als de tijdinstelling niet correct is, wordt de foutmelding "Licentie is verlopen" weergegeven. Dit kan ertoe leiden dat de configuratie van de scanner mislukt. Bovendien moet voor het gebruik van een beveiligingsfunctie als SSL/TLS-communicatie of IPsec de juiste tijd zijn ingesteld. U kunt de tijd als volgt instellen:

- *Web Config: tabblad **Apparaatbeheer** > **Datum en tijd** > **Datum en tijd**.*
- *Bedieningspaneel van de scanner: **Instel.** > **Basisinstellingen** > **Datum/tijd instellen**.*

Instellingen	Lokale DB	LDAP	Lokale DB en LDAP
Verificatie inschakelen U moet verificatie inschakelen voordat u de verificatie-instellingen configureert. "Verificatie inschakelen" op pagina 139	✓	✓	✓
Verificatie-instellingen De Verificatiemethode instellen en configureren hoe gebruikers worden geverifieerd. "Verificatie-instellingen" op pagina 140	✓	✓	✓

Instellingen	Lokale DB	LDAP	Lokale DB en LDAP
Gebruikersinstellingen opslaan Sla de instellingen voor elke gebruiker op. U kunt gebruikers ook in bulk registreren met behulp van een CSV-bestand. "Gebruikersinstellingen opslaan" op pagina 141	✓	–	✓
Synchroniseren met de LDAP-server Configureer de synchronisatie-instellingen voor de LDAP-server. "Synchroniseren met de LDAP-server" op pagina 148	–	✓	✓
De E-mailserver instellen Stel de mailserverinstellingen in. Stel deze optie in wanneer u functies gebruikt waarvoor mailserverinstellingen zoals Scan naar Mijn e-mail nodig zijn. "De mailserver instellen" op pagina 151	✓	✓	✓
Scannen naar Mijn map instellen Stel de doelmappen in. Stel deze optie in wanneer u de functie Scannen naar Mijn map gebruikt. "Scannen naar Mijn map instellen" op pagina 152	✓	✓	✓
One-touch-functies aanpassen Stel deze optie in wanneer u de items die op het bedieningspaneel van de scanner worden weergegeven wijzigt. U kunt alleen de pictogrammen die u nodig hebt weergeven op het bedieningspaneel of de volgorde van de pictogrammen wijzigen. "One-touch-functies aanpassen" op pagina 154	✓	✓	✓

Verificatie inschakelen

U moet verificatie inschakelen voordat u de verificatie-instellingen configureert.

Instellen via Web Config:

Selecteer **Aan (apparaat/LDAP-server)** op het tabblad **Productbeveiliging** > **Basis** > **Authenticatie**.

Instellen via Epson Device Admin:

Selecteer in de configuratiesjabloon **Aan (apparaat/LDAP-server)** bij **Beheerinstellingen** > **Verificatie-instellingen** > **Standaard** > **Authenticatie**.

Opmerking:
Als u Verificatie-instellingen inschakelt op de scanner, wordt Instelling vergrendelen ook ingeschakeld voor het bedieningspaneel. Het bedieningspaneel kan niet worden ontgrendeld wanneer Verificatie-instellingen is ingeschakeld.

Ook als u Verificatie-instellingen uitschakelt, blijft Instelling vergrendelen ingeschakeld. Als u deze optie wilt uitschakelen, kunt u dit doen via het bedieningspaneel of Web Config.

Gerelateerde informatie

➡ "Instelling vergrendelen instellen via het bedieningspaneel" op pagina 89

➡ "Instelling vergrendelen instellen via Web Config" op pagina 89

Verificatie-instellingen

De Verificatiemethode instellen en configureren hoe gebruikers worden geverifieerd.

Instellen via Web Config:

Selecteer het tabblad **Productbeveiliging** > **Verificatie-instellingen**.

Instellen via Epson Device Admin:

Selecteer **Beheerinstellingen** > **Verificatie-instellingen** > **Verificatie-instellingen** in de configuratiesjabloon.

Item	Uitleg
Verificatiemethode	Selecteer de Verificatiemethode. ❏ Lokale DB Voer de verificatie uit met de Gebruikersinstellingen die in de scanner zijn geregistreerd. De gebruiker moet in de scanner zijn geregistreerd. ❏ LDAP Voer de verificatie uit met de gebruikersgegevens op de LDAP-server die met de scanner wordt gesynchroniseerd. U moet de instellingen van de LDAP-server van tevoren configureren. ❏ Lokale DB en LDAP Voer de verificatie uit met de gebruikersgegevens die zijn geregistreerd in de scanner of op de LDAP-server die met de scanner wordt gesynchroniseerd. U moet de gebruiker in de scanner registreren en de LDAP-server configureren.
De gebruiker verifiëren	Selecteer hoe u een gebruiker wilt verifiëren. ❏ Kaart of Gebruikers-id en wachtwoord Gebruik een verificatiekaart om gebruikers te verifiëren. U kunt voor de verificatie ook een gebruikers-id en wachtwoord gebruiken. ❏ Gebruikers-id en wachtwoord Gebruik een gebruikers-id en wachtwoord om gebruikers te verifiëren. Als u deze functie selecteert, kunt u geen verificatiekaart gebruiken voor de verificatie. ❏ Gebruikers-ID Gebruik alleen een gebruikers-id om gebruikers te verifiëren. U hoeft geen wachtwoord in te stellen. ❏ Kaart of Identiteitsnummer Gebruik een verificatiekaart om gebruikers te verifiëren. U kunt tevens een Identiteitsnummer gebruiken. ❏ Identiteitsnummer Gebruik alleen een id-nummer om gebruikers te verifiëren.
Toestaan dat de gebruiker verificatiekaarten registreert	Schakel deze functie in zodat gebruikers de verificatiekaart bij het systeem kunnen registreren. Als u **LDAP** selecteert als **Verificatiemethode**, kunt u dit niet instellen. Zie "Een verificatiekaart registreren" in de *Gebruikershandleiding* voor meer informatie over hoe gebruikers hun verificatiekaart kunnen registreren.
Het laagste cijfer van Identiteitsnummer	Selecteer het minimale aantal tekens voor het id-nummer.

Item	Uitleg
Opslaan in cache voor door LDAP geverifieerde gebruikers	Bij verificatie via de LDAP-server kunt u instellen of gebruikersgegevens in het cachegeheugen moeten worden opgeslagen.
Gebruik gebruikersinformatie in SMTP-authenticatie	Bij gebruik van een gebruikers-id en wachtwoord voor verificatie kunt u instellen of gebruikersgegevens moeten worden gebruikt voor SMTP-verificatie. Het systeem gebruikt het laatste gebruikers-id en laatste wachtwoord waarmee werd ingelogd.
Beperkingen voor LDAP-geauthenticeerde gebruikers	Als u LDAP gebruikt, kunt u instellen welke functies beschikbaar zijn voor de gebruiker.

Gebruikersinstellingen opslaan

Sla de Gebruikersinstellingen op die voor verificatie van gebruikers worden gebruikt. U kunt hiervoor de volgende methoden gebruiken.

❏ Gebruikersinstellingen een voor een opslaan (Web Config)

❏ Meerdere Gebruikersinstellingen als batch opslaan met behulp van een CSV-bestand (Web Config)

❏ Gebruikersinstellingen voor meerdere scanners als batch opslaan met behulp van een configuratiesjabloon (Epson Device Admin)

Gerelateerde informatie

➡ “Gebruikersinstellingen afzonderlijk opslaan (Web Config)” op pagina 141

➡ “Meerdere Gebruikersinstellingen opslaan met behulp van een CSV-bestand (Web Config)” op pagina 142

➡ “Gebruikersinstellingen voor meerdere scanners als batch opslaan (Epson Device Admin)” op pagina 145

Gebruikersinstellingen afzonderlijk opslaan (Web Config)

Open Web Config en selecteer het tabblad **Productbeveiliging** > **Gebruikersinstellingen** > **Toevoegen**. Voer vervolgens de Gebruikersinstellingen in.

Item	Uitleg
Gebruikers-ID	Voer de gebruikers-id die u voor verificatie wilt gebruiken in. De waarde kan tussen 1 tot 83 bytes in Unicode (UTF-8) liggen. Aangezien de gebruikers-id niet hoofdlettergevoelig is, kunt u inloggen met hoofdletters of kleine letters.
Weergave gebruikersnaam	Voer de gebruikersnaam in die op het bedieningspaneel van de scanner wordt weergegeven. Gebruik hiervoor maximaal 32 tekens in Unicode (UTF-16). Dit kunt u leeg laten.
Wachtwoord	Voer het wachtwoord in dat u voor verificatie wilt gebruiken. Gebruik hiervoor maximaal 32 tekens in ASCII. Het wachtwoord is hoofdlettergevoelig. Laat dit leeg als u **Gebruikers-ID** selecteert bij **De gebruiker verifiëren**.

Item	Uitleg
Verificatiekaart-ID	Voer de verificatiekaart-id in. Gebruik hiervoor maximaal 116 tekens in ASCII. Dit kunt u leeg laten. Wanneer u **Toestaan dat de gebruiker verificatiekaarten registreert** selecteert bij **Verificatie-instellingen**, wordt het resultaat weergegeven dat door gebruikers is geregistreerd.
Identiteitsnummer	Dit item wordt weergegeven wanneer **Kaart of Identiteitsnummer** of **Identiteitsnummer** is geselecteerd bij **Verificatie-instellingen** > **De gebruiker verifiëren**. Voer een nummer in dat ergens ligt tussen het getal dat is ingesteld bij **Verificatie-instellingen** > **Het laagste cijfer van Identiteitsnummer** en uit maximaal 8 cijfers bestaat.
Automatisch genereren	Dit item wordt weergegeven wanneer **Kaart of Identiteitsnummer** of **Identiteitsnummer** is geselecteerd bij **Verificatie-instellingen** > **De gebruiker verifiëren**. Klik om automatische een id-nummer te genereren met hetzelfde aantal cijfers dat u bij **Het laagste cijfer van Identiteitsnummer** hebt geselecteerd.
Afdeling	Voer de afdelingsnaam en andere gegevens in waarmee de gebruiker wordt geïdentificeerd. Gebruik maximaal 40 tekens in Unicode (UTF-16). Dit kunt u leeg laten.
E-mailadres	Voer het e-mailadres van de gebruiker in. Gebruik maximaal 200 tekens in ASCII. Dit wordt gebruikt als het doel voor **Scan naar Mijn e-mail**. Dit kunt u leeg laten.
Scannen naar Mijn map	Stel de opslaglocaties afzonderlijk in wanneer u **Individueel** selecteert bij **Scannen naar Mijn map** > **Type instellingen**. Raadpleeg de volgende informatie over de instellingsitems. "Scannen naar Mijn map instellen" op pagina 152
Beperkingen	U kunt de functies voor elke gebruiker beperken. Selecteer de functie waarvan u het gebruik wilt toestaan.
Presets	U kunt maximaal vijf voorinstellingen instellen die alleen voor de geselecteerde gebruiker beschikbaar zijn in de Presets die in de scanner zijn opgeslagen. ❏ Presets die aan een gebruiker zijn toegewezen, kunnen alleen door die gebruiker worden gebruikt. Presets die niet aan gebruikers zijn toegewezen, kunnen door alle gebruikers worden gebruikt. ❏ Als voor een gebruiker bij Presets maar één voorinstelling beschikbaar is, wordt deze na verificatie automatische geladen. Als meerdere Presets beschikbaar zijn, wordt na verificatie een lijst met Presets weergegeven. ❏ U kunt geen Presets maken of weergeven als deze functies gebruiken die zijn beperkt bij **Beperkingen**.

Meerdere Gebruikersinstellingen opslaan met behulp van een CSV-bestand (Web Config)

Voer de instellingen voor elke gebruiker in een CSV-bestand in en sla ze als batch op.

Een CSV-bestand maken

Maak een CSV-bestand om Gebruikersinstellingen te importeren.

Opmerking:
Als u van tevoren een of meer Gebruikersinstellingen opslaat en vervolgens een opgemaakt bestand (CSV-bestand) exporteert, kunt u de opgeslagen instelling gebruiken als referentie voor het invoeren van instellingsitems.

1. Open Web Config en selecteer het tabblad **Productbeveiliging** > **Gebruikersinstellingen**.
2. Klik op **Exporteren**.
3. Selecteer de bestandsindeling bij **Bestandsindeling**.

   Zie onderstaande voor de selectie.

Item	Uitleg
CSV UTF-16 (gescheiden door tabs)	Selecteer deze optie wanneer u het bestand bewerkt in Microsoft Excel. Elke parameter wordt omgeven door "[ ]"(rechte haken). Voer de parameters tussen "[ ]" in. Als u het bestand bijwerkt, wordt aanbevolen het bestand te overschrijven. Als u het bestand opnieuw opslaat, selecteert u de bestandsindeling Unicode-tekst (*.txt).
CSV UTF-8 (gescheiden door komma's)	Selecteer deze optie wanneer u het bestand bewerkt met een teksteditor of macro zonder Microsoft Excel.
CSV UTF-8 (gescheiden door puntkomma's)	

4. Klik op **Exporteren**.
5. Bewerk het CSV-bestand in een spreadsheettoepassing, zoals Microsoft Excel, of in een teksteditor en sla dit vervolgens op.

> ***Belangrijk:***
> *Breng tijdens het bewerken van het bestand geen wijzigingen aan in de codering of koptekstinformatie.*

Instellingsitems voor CSV-bestanden

Item	Instellingen en toelichting
UserID	Voer de gebruikers-id voor verificatie in. Gebruik hiervoor tussen 1 en 83 bytes in Unicode.
UserName	Voer de gebruikersnaam in die op het bedieningspaneel van de scanner wordt weergegeven. Gebruik hiervoor maximaal 32 tekens in Unicode. Dit kunt u leeg laten.
Password	Voer het wachtwoord voor verificatie in. Gebruik hiervoor maximaal 32 tekens in ASCII. Bij importeren wordt dit ingesteld als het wachtwoord in plaats van **EncPassword**. Laat dit leeg als u **Gebruikers-ID** selecteert bij **De gebruiker verifiëren**. Bij exporteren is dit altijd leeg.

Item	Instellingen en toelichting
AuthenticationCardID	Stel het leesresultaat van de verificatiekaart in. Wanneer u **Toestaan dat de gebruiker verificatiekaarten registreert** selecteert bij **Verificatie-instellingen**, wordt het resultaat weergegeven dat door gebruikers is geregistreerd. Voer maximaal 116 tekens in ASCII in. Dit kunt u leeg laten.
IDNumber	Dit item wordt weergegeven wanneer **Kaart of Identiteitsnummer** of **Identiteitsnummer** is geselecteerd bij **Verificatie-instellingen** > **De gebruiker verifiëren**. Voer een nummer in dat ergens ligt tussen het getal dat is ingesteld bij **Verificatie-instellingen** > **Het laagste cijfer van Identiteitsnummer** en uit maximaal 8 cijfers bestaat. Een id-nummer kan niet worden gedupliceerd. Als dit wordt gedupliceerd, wordt tijdens het importeren van het bestand een waarschuwing weergegeven. Wanneer dit leeg wordt gelaten, wordt er automatisch een nummer aan toegewezen.
Department	Voer indien gewenst de afdelingsnaam in om gebruikers te kunnen onderscheiden. Voer maximaal 40 tekens in Unicode in. Dit kunt u leeg laten.
MailAddress	Stel het e-mailadres voor de gebruikers in. Dit wordt gebruikt als het doel voor **Scan naar Mijn e-mail**. U kunt A-Z, a-z, 0-9, !#'%&'*+-./=?^_{|}~@ gebruiken. Voer maximaal 200 tekens in. U kunt als eerste teken niet een "," (komma) gebruiken. Dit kunt u leeg laten.
FolderProtocol	Stel het type functie Scannen naar Mijn map in. Netwerkmap/FTP (SMB): 0, FTP: 1
FolderPath	Stel de bestemming voor opslaan voor de functie Scannen naar Mijn map in.
FolderUserName	Stel de gebruikersnaam in voor de functie Scannen naar Mijn map.
FolderPassword	Stel een wachtwoord in voor het verifiëren van de bestemmingsmap voor de functie Scannen naar Mijn map binnen 32 ASCII-tekens. Bij importeren wordt dit ingesteld als het wachtwoord in plaats van **EncPassword**. Bij exporteren is dit altijd leeg.
FtpPassive	Stel de verbindingsmodus in voor de FTP-server wanneer **FTP** wordt geselecteerd als het **Type** voor de functie Scannen naar Mijn map. Actieve modus: 0, Passieve modus: 1
FtpPort	Stel het poortnummer voor het verzenden van gescande gegevens naar de FTP-server in van 0 tot 65535 wanneer **FTP** wordt geselecteerd als het **Type** voor de functie Scannen naar Mijn map.
ScanToMemory	Stel de beperkingen in voor Scannen naar USB-stick. Niet toegestaan: 0, Toegestaan: 1
ScanToMail	Stel de beperkingen in voor Scannen naar e-mail. U kunt **Scannen naar Mijn e-mail** alleen instellen wanneer **Scannen naar e-mail** is ingeschakeld. Niet toegestaan: 0, Toegestaan: 1

Item	Instellingen en toelichting
ScanToFolder	Stel de beperkingen in voor Scannen naar netwerkmap /FTP. U kunt **Scannen naar Mijn map** alleen instellen wanneer **Scannen naar netwerkmap /FTP** is ingeschakeld. Niet toegestaan: 0, Toegestaan: 1
ScanToCloud	Stel de beperkingen in voor Scannen naar cloud. Niet toegestaan: 0, Toegestaan: 1
ScanToComputer	Stel de beperkingen in voor Scan naar computer. Niet toegestaan: 0, Toegestaan: 1
PresetIndex	Stel de Presets in die u aan de gebruiker wilt koppelen. U kunt maximaal vijf door een komma gescheiden registratienummers voor Presets instellen.
EncPassword	Wanneer u gebruikersinstellingen exporteert, wordt de parameter die is ingesteld voor **Password** versleuteld en wordt de waarde versleuteld met BASE64 en uitgevoerd. Wanneer u importeert met het nieuwe wachtwoord voor **Password**, wordt deze waarde genegeerd. Als **Password** leeg is, wordt deze waarde gebruikt en blijft het wachtwoord hetzelfde als voor exporteren.
EncFolderPassword	Bij exporteren wordt de parameter die is ingesteld voor **FolderPassword** versleuteld en wordt de waarde versleuteld met BASE64 en uitgevoerd. Wanneer u importeert met het nieuwe wachtwoord voor **FolderPassword**, wordt deze waarde genegeerd. Als **FolderPassword** leeg is, wordt deze waarde gebruikt en blijft het wachtwoord hetzelfde als voor exporteren.

Een CSV-bestand importeren

1. Open Web Config en selecteer het tabblad **Productbeveiliging** > **Gebruikersinstellingen**.
2. Klik op **Importeren**.
3. Selecteer het bestand dat u wilt importeren.
4. Klik op **Importeren**.
5. Controleer de weergegeven gegevens en klik vervolgens op **OK**.

Gebruikersinstellingen voor meerdere scanners als batch opslaan (Epson Device Admin)

U kunt Gebruikersinstellingen die in Lokale DB worden gebruikt met behulp van een LDAP-server of een CSV/ENE-bestand als batch opslaan.

Opmerking:
*Een ENE-bestand is een binair bestand dat door Epson beschikbaar wordt gesteld voor het versleutelen en opslaan van informatie voor **Contacten**, zoals persoonsgegevens en Gebruikersinstellingen. Dit kan uit Epson Device Admin worden geëxporteerd en u kunt een wachtwoord instellen. Dit is handig wanneer u Gebruikersinstellingen wilt importeren vanuit een back-upbestand.*

Importeren vanuit CSV/ENE-bestand

1. Selecteer **Beheerinstellingen** > **Verificatie-instellingen** > **Gebruikersinstellingen** in de configuratiesjabloon.
2. Klik op **Importeren**.
3. Selecteer **CSV- of ENE-bestand** in **Importbron**.
4. Klik op **Bladeren**.

   Het scherm voor bestandsselectie wordt weergegeven.
5. Selecteer het bestand dat u wilt importeren en open het.
6. Selecteer een importmethode.
   - ❏ Overschrijven en toevoegen: hiermee wordt een bestaande gebruikers-id overschreven en wordt een nieuwe id toegevoegd als er nog geen id is.
   - ❏ Alles vervangen: hiermee wordt alles vervangen door de gebruikersinstellingen die u wilt importeren.
7. Klik op **Importeren**.

   Het bevestigingsscherm voor de instelling wordt weergegeven.
8. Klik op **OK**.

   Het resultaat van de validatie wordt weergegeven.

   Opmerking:
   - ❏ *Als het aantal geïmporteerde gebruikersinstellingen groter is dan het aantal dat kan worden geïmporteerd, wordt een bericht weergegeven waarin u wordt gevraagd enkele gebruikersinstellingen te verwijderen. Verwijder overtollige gebruikersinstellingen voordat u gaat importeren.*
   - ❏ *Selecteer de gebruikersinstellingen die u wilt verwijderen voordat u gaat importeren en klik op **Verwijderen**.*
9. Klik op **Importeren**.

   De gebruikersinstellingen worden in de configuratiesjabloon geïmporteerd.

Importeren vanaf de LDAP-server

1. Selecteer **Beheerinstellingen** > **Verificatie-instellingen** > **Gebruikersinstellingen** in de configuratiesjabloon.
2. Klik op **Importeren**.
3. Selecteer **LDAP** in **Importbron**.

4. Klik op **Instellingen**.

   De instellingen voor de **LDAP-server** worden weergegeven.

   Opmerking:
   Met deze LDAP-serverinstelling kunt u de gebruikersinstellingen vanaf de LDAP-server importeren. De geïmporteerde (gekopieerde) gebruikersinstellingen worden gebruikt om gebruikers te verifiëren behulp van de scanner.

   *Wanneer u daarentegen **LDAP** of **Lokale DB en LDAP** als de verificatiemethode selecteert, worden gebruikers geverifieerd middels communicatie met de LDAP-server.*

5. Stel elk item in.

   Tijdens het importeren van gebruikersinstellingen vanaf een LDAP-server kunt u naast de LDAP-instellingen ook de volgende instellingen configureren.

   Zie de gerelateerde informatie voor andere items.

Item			Uitleg
Instellingen LDAP-server	LDAP-servertype		Hiermee kunt u het type LDAP-server selecteren.
Zoekinstellingen	Zoekfilter		U kunt de tekst instellen die voor het LDAP-zoekfilter wordt gebruikt. Selecteer **Aangepast** om de zoektekst te bewerken.
	Opties	Type	U kunt het type opslaglocatie instellen voor **Scannen naar mijn map**.
		Verbindingsmodus	Wanneer **Type** is ingesteld op **FTP**, kunt u de FTP-verbindingsmodus instellen.
		Poortnummer	Wanneer **Type** is ingesteld op **FTP**, kunt u het poortnummer instellen.

6. Voer indien nodig de verbindingstest uit door op **Verbindingstest** te klikken.

   Hiermee worden 10 gebruikersinstellingen van de LDAP-server opgehaald en weergegeven.

7. Klik op **OK**.

8. Selecteer een importmethode.

   ❏ Overschrijven en toevoegen: hiermee wordt een bestaande gebruikers-id overschreven en wordt een nieuwe id toegevoegd als er nog geen id is.

   ❏ Alles vervangen: hiermee wordt alles vervangen door de gebruikersinstellingen die u wilt importeren.

9. Klik op **Importeren**.

   Het bevestigingsscherm voor de instelling wordt weergegeven.

10. Klik op **OK**.

    Het resultaat van de validatie wordt weergegeven.

11. Klik op **Importeren**.

    De gebruikersinstellingen worden in de configuratiesjabloon geïmporteerd.

Gerelateerde informatie

➡ "Een LDAP-server configureren" op pagina 148
➡ "De zoekinstellingen voor de LDAP-server configureren" op pagina 150

Synchroniseren met de LDAP-server

Configureer de instellingen van de LDAP-server voor de scanner.

Configureer indien nodig de instellingen voor de primaire en de secundaire server.

Opmerking:
*De instellingen van de **LDAP-server** worden gedeeld met **Contactpersonen**.*

Beschikbare diensten

De volgende directoryservices worden ondersteund.

Servicenaam	Versie
Active Directory	Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
OpenLDAP	Ver.2.3, Ver.2.4

Een LDAP-server configureren

Als u een LDAP-server wilt gebruiken, moet u eerst de LDAP-server configureren.

Instellen via Web Config:

Selecteer het tabblad **Netwerk** > **LDAP-server** > **Basis (Primaire server)** of **Basis (Secundaire server)**.

Als u **Kerberos-verificatie** selecteert bij **Verificatiemethode**, moet u **Netwerk** > **Kerberos-instellingen** selecteren om de instellingen voor Kerberos te configureren.

Instellen via Epson Device Admin:

Selecteer **Netwerk** > **LDAP-server** > **Serverinstellingen (Primaire server)** of **Serverinstellingen (Secundaire server)** in de configuratiesjabloon.

Als u **Kerberos-verificatie** selecteert bij **Verificatiemethode**, moet u **Netwerk** — **Beveiliging** > **Kerberos-instellingen** selecteren om de instellingen voor Kerberos te configureren.

Item	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 de FQDN-indeling kunt u alfanumerieke tekens in ASCII (0x20–0x7E) en koppeltekens gebruiken, behalve aan het begin en eind van het adres.
Poortnummer LDAP-server (Poortnummer)	Voer het LDAP-serverpoortnummer, tussen 1 en 65535, in.

Item	Instellingen en toelichting
Veilige verbinding	Geef de verificatiemethode op die de scanner moet gebruiken voor toegang tot de LDAP-server.
Certificaatvalidatie	Het certificaat van de LDAP-server wordt geverifieerd wanneer dit is ingeschakeld. Het wordt aangeraden om 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 seconden in voordat een time-out optreedt.
Verificatiemethode	Selecteer de verificatiemethode. Als u **Kerberos-verificatie** selecteert, moet u de instellingen voor Kerberos van tevoren configureren. Voor het uitvoeren van Kerberos-verificatie is de volgende omgeving vereist. ❏ De scanner en de DNS-server kunnen communiceren. ❏ De tijd voor de scanner, de KDC-server en de server die vereist is voor verificatie (LDAP-server, SMTP-server, bestandsserver) is gesynchroniseerd. ❏ Wanneer de serviceserver als het IP-adres is aangewezen, 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 tot 0x1F en 0X7F. Deze instelling wordt niet gebruikt wanneer **Anonieme verificatie** is geselecteerd als **Verificatiemethode**. Als u dit niet wilt opgeven, 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 tot 0x1F en 0X7F. Deze instelling wordt niet gebruikt wanneer **Anonieme verificatie** is geselecteerd als **Verificatiemethode**. Als u dit niet wilt opgeven, laat u dit leeg.

Kerberos-instellingen

Als u **Kerberos-verificatie** selecteert bij **Verificatiemethode**, moet u de instellingen voor Kerberos configureren. U kunt maximaal 10 Kerberos-instellingen registreren.

Instellen via Web Config:

Selecteer het tabblad **Netwerk** > **Kerberos-instellingen**.

Instellen via Epson Device Admin:

Selecteer **Netwerk** > **Beveiliging** > **Kerberos-instellingen** in de configuratiesjabloon.

Item	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 wilt registreren, 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 wilt registreren, laat u dit leeg.

Item	Instellingen en toelichting
Poortnummer (Kerberos)	Voer het Kerberos-serverpoortnummer, tussen 1 en 65535, in.

De zoekinstellingen voor de LDAP-server configureren

Hiermee stelt u de zoekattributen voor gebruikersinstellingen in.

Instellen via Web Config:

Selecteer het tabblad **Netwerk** > **LDAP-server** > **Zoekinstellingen (Authenticatie)**.

Instellen via Epson Device Admin:

Selecteer **Beheerinstellingen** > **Verificatie-instellingen** > **LDAP-server** > **Zoekinstellingen (Authenticatie)** in de configuratiesjabloon.

Item	Instellingen en toelichting
Zoekdatabase (Gedistingeerde naam)	Geef de startpositie op bij zoeken naar gebruikersgegevens op de LDAP-server. Voer tussen 0 en 128 tekens in Unicode (UTF-8) in. Als u geen willekeurig attribuut zoekt, laat u dit leeg. Voorbeeld voor de lokale serverdirectory: dc=server,dc=local
Kenmerk gebruikers-ID	Geef de attribuutnaam op die moet worden weergegeven als u naar de het id-nummer zoekt. Voer tussen 1 en 255 tekens in ASCII in. Het eerste teken moet a–z of A–Z zijn. Voorbeeld: cn, uid
Kenmerk weergave gebruikersnaam	Geef de attribuutnaam op die moet worden weergegeven als gebruikersnaam. Voer tussen 0 en 255 tekens in ASCII in. Het eerste teken moet a–z of A–Z zijn. Dit kunt u leeg laten. Voorbeeld: cn, name
Verificatie kenmerk kaart-ID	Geef de attribuutnaam op die moet worden weergegeven als verificatiekaart-id. Voer tussen 0 en 255 tekens in ASCII in. Het eerste teken moet a–z of A–Z zijn. Dit kunt u leeg laten. Voorbeeld: cn, sn
Kenmerk ID-nummer	Geef de attribuutnaam op die moet worden weergegeven als u naar de het id-nummer zoekt. Voer tussen 1 en 255 tekens in ASCII in. Het eerste teken moet a–z of A–Z zijn. Voorbeeld: cn, id
Afdelingskenmerk	Geef de attribuutnaam op die moet worden weergegeven als afdelingsnaam. Voer tussen 0 en 255 tekens in ASCII in. Het eerste teken moet a–z of A–Z zijn. Dit kunt u leeg laten. Voorbeeld: ou, ou-cl
Kenmerk e-mailadres	Geef de attribuutnaam op die moet worden weergegeven als u naar e-mailadressen zoekt. Voer tussen 1 en 255 tekens in ASCII in. Het eerste teken moet a–z of A–Z zijn. Voorbeeld: mail
Opslaan naar kenmerk	Geef de attribuutnaam op die verwijst naar de bestemming voor Scannen naar mijn map. Voer tussen 0 en 255 tekens in ASCII in. Voorbeeld: homeDirectory

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: ❏ Het LDAP-serveradres of het poortnummer onjuist is. ❏ Er een time-out is opgetreden. ❏ **Niet gebruiken** is geselecteerd voor **LDAP-server gebruiken**. ❏ 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 tijdinstellingen van de scanner en de LDAP-server niet overeenkomen.
Verificatie mislukt. Controleer de instellingen.	Deze melding wordt weergegeven wanneer: ❏ **Gebruikersnaam** en/of **Wachtwoord** onjuist is. ❏ 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.

De mailserver instellen

Wanneer u **Scan naar Mijn e-mail** gebruikt, moet u de mailserver instellen.

Opmerking:
*U kunt **Scan naar Mijn e-mail** alleen instellen wanneer **Scannen naar e-mail** is ingeschakeld.*

Instellen via Web Config:

Selecteer het tabblad **Netwerk** > **E-mailserver** > **Basis**.

Instellen via Epson Device Admin:

Selecteer **Algemeen** > **E-mailserver** > **Instellingen e-mailserver** in de configuratiesjabloon.

Item	Instellingen en toelichting	
Verificatiemethode	Geef hier de verificatiemethode op die de scanner moet gebruiken voor toegang tot de mailserver.	
	Uit	Verificatie is uitgeschakeld wanneer met een mailserver wordt gecommuniceerd.
	SMTP-verificatie	De mailserver 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 tussen 0 en 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 tussen 0 en 20 tekens in ASCII (0x20–0x7E) in.	
E-mailadres afzender	Voer hier het e-mailadres van de afzender in. Voer tussen 0 en 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 verbindingsmethode op voor de mailserver.	
	Geen	Als u **POP voor SMTP** selecteert in **Verificatiemethode**, wordt de verbindingsmethode 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**.
Certificaatvalidatie	Het certificaat is geverifieerd wanneer dit is ingeschakeld. Het wordt aangeraden om dit in te stellen op **Inschakelen**.	
Adres POP3-server	Als u **POP voor SMTP** selecteert bij **Verificatiemethode**, moet u het adres van de POP3-server invoeren. U kunt tussen 0 en 255 tekens invoeren. Gebruik A–Z, a–z, 0–9. U kunt IPv4 of FQDN gebruiken.	
Poortnummer POP3-server	Als u **POP voor SMTP** selecteert bij **Verificatiemethode**, moet u het poortnummer opgeven. Voer een getal tussen 1 en 65535 in.	

Scannen naar Mijn map instellen

Hiermee worden gescande afbeeldingen opgeslagen in de map die aan elke gebruiker is toegewezen. U kunt het volgende instellen als speciale map.

Opmerking:
*U kunt **Scannen naar mijn map** alleen instellen wanneer **Scannen naar netwerkmap /FTP** is ingeschakeld.*

Instelling Opslaan naar	Verificatiemethode	Locatie mappad
Geef één netwerkmap op voor alle Verificatie-instellingen om automatisch in de opgegeven map een persoonlijke map met als naam de gebruikers-id te maken.	❏ Lokale DB ❏ LDAP ❏ Lokale DB en LDAP	Scanner (instelling Scannen naar Mijn map)
Verschillende netwerkmappen afzonderlijk toewijzen aan elke gebruiker.	Lokale DB	Scanner (Gebruikersinstellingen)
	LDAP	LDAP-attributen
	Lokale DB en LDAP	Scanner (Gebruikersinstellingen) of LDAP-attributen

Instellen via Web Config:

Selecteer het tabblad **Productbeveiliging** > **Scannen naar netwerkmap /FTP**.

Instellen via Epson Device Admin:

Selecteer **Beheerinstellingen** > **Verificatie-instellingen** > **Scannen naar netwerkmap /FTP** > **Scannen naar Mijn map** in de configuratiesjabloon.

Item		Uitleg
Opslaan naar instelling	Type instellingen	❏ **Gedeeld**: Hiermee maakt u automatisch een map met als naam de id van de gebruiker aan in het mappad dat of de URL die is opgegeven bij **Opslaan in**. De scanresultaten worden in deze map opgeslagen. ❏ **Individueel**: Hiermee stelt u de bestemming voor het opslaan van scanresultaten voor elke gebruiker in. Lokale DB-gebruikers kunnen worden ingesteld in de gebruikersinstellingen. LDAP-gebruikers gebruiken de opslaglocatie die op basis van de zoekattributen van de LDAP-server is verkregen.
	Type	Selecteer het transmissieprotocol overeenkomstig de bestemming van de scanuitvoer. Voor een netwerkmap: **Netwerkmap (SMB)** Voor een FTP-server: **FTP**
	Opslaan in	Geef het pad of de URL van het uitvoerpad op. Voer maximaal 160 tekens in Unicode (UTF-16) in.
	Aansluitmodus	Stel deze optie in wanneer u **FTP** selecteert in **Type**. Selecteer een verbindingsmodus voor de FTP-server.
	Poortnummer	Stel deze optie in wanneer u **FTP** selecteert in **Type**. Voer het poortnummer in voor het verzenden van de gescande gegevens naar een FTP-server tussen 0 en 65535.

Item		Uitleg
Verificatie-instellingen	Type instellingen	Stel deze optie in wanneer u **Individueel** selecteert bij **Type instellingen** in **Opslaan naar instelling**. Stel de Gebruikersnaam en het Wachtwoord in voor toegang tot de map. ❏ **Gedeeld**: Gebruik een algemene **Gebruikersnaam** en een algemeen **Wachtwoord** voor alle gebruikers. ❏ **Individueel**: Stel de **Gebruikersnaam** en het **Wachtwoord** voor Lokale DB-gebruikers afzonderlijk in bij **Gebruikersinstellingen**. LDAP-gebruikers kunnen niet afzonderlijk worden geconfigureerd. De **Gebruikersnaam** en het **Wachtwoord** die met deze optie worden ingesteld, worden als batch gebruikt.
	Gebruikersnaam	Voer de gebruikersnaam in om toegang te krijgen tot de doelmap voor de scanuitvoer. Voer maximaal 30 tekens in Unicode (UTF-16) in. Stel deze optie in wanneer u een **Gedeeld** of LDAP-server gebruikt.
	Wachtwoord	Voer het wachtwoord in dat bij de **Gebruikersnaam** hoort. Voer maximaal 20 tekens in Unicode (UTF-16) in. Stel deze optie in wanneer u een **Gedeeld** of LDAP-server gebruikt.

Wijzigingen van het doel voor Scannen naar netwerkmap /FTP verbieden

Item	Uitleg
Handmatige invoer van bestemming verbieden	Wanneer deze optie is ingeschakeld, kan de gebruiker de standaardbestemming niet wijzigen.

One-touch-functies aanpassen

U kunt alleen noodzakelijke pictogrammen weergeven door het bewerken van de pictogramopmaak die wordt weergegeven op het startscherm voor het bedieningspaneel.

Instellen via Web Config:

Selecteer het tabblad **Productbeveiliging** > **One-touch-functies aanpassen**.

Instellen via Epson Device Admin:

Selecteer **Beheerinstellingen** > **Verificatie-instellingen** > **One-touch-functies aanpassen** in de configuratiesjabloon.

Opmerking:
In de volgende gevallen worden de pictogrammen voor de beschikbare functies niet op het startscherm weergegeven.

❏ *Wanneer u functies selecteert die niet zijn toegestaan vanwege **Beperkingen**.*

❏ *Wanneer het e-mailadres voor een aangemelde gebruiker niet is geregistreerd. (Scan naar Mijn e-mail)*

❏ *Wanneer de bestemmingsmap niet is ingesteld. (Scannen naar Mijn map)*

Item	Uitleg
Maximumfuncties per scherm	Selecteer de opmaak van de pictogrammen die op het bedieningspaneel worden weergegeven. Het beeld verandert overeenkomstig de geselecteerde opmaak.
Scherm(en)	Selecteer het aantal pagina's.
Aantal	Selecteert de functies die u voor elke genummerde positie wilt weergeven.

Rapporten met de Taakgeschiedenis maken met behulp van Epson Device Admin

U kunt een rapport met de Taakgeschiedenis voor elke groep en elke gebruiker maken met behulp van Epson Device Admin. U kunt maximaal 3000 gebruiksgeschiedenissen opslaan in de scanner. U kunt het rapport maken door een periode op te geven of door een standaard planning in te stellen.

Als u Taakgeschiedenis als rapport wilt uitvoeren, selecteert u **Opties** > **Epson Print Admin Serverless/ Authenticatie Instellingen** > **De Epson Print Admin Serverless/Authenticatie compatibele apparaten beheren** in het lintmenu in het scherm "Apparatenlijst".

Raadpleeg de documentatie voor Epson Device Admin voor meer informatie over het maken van een gebruikersrapport.

Items die in een rapport kunnen worden opgenomen

U kunt de volgende items in het gebruikersrapport opnemen.

Datum/Taak-ID/Bediening/Gebruikers-ID/Afdeling/Resultaat/Details resultaat/Scannen: Type bestemming/ Scannen: Bestemming/Scannen: Papierformaat/Scannen: Dubbelzijdig/Scannen: Kleur/Scannen: Pagina's/ Apparaten: Model/Apparaten: IP-adres/Apparaten: Serienummer/Apparaten: Afdeling/Apparaten: Locatie/ Apparaten: Opmerking/Apparaten: NB

Als beheerder inloggen op het bedieningspaneel

U kunt een van de volgende methoden gebruiken via het bedieningspaneel van de scanner in te loggen als beheerder.

1. Tik rechtsboven in het scherm op  .
   - ❏ Wanneer Verificatie-instellingen is ingeschakeld, wordt het pictogram weergegeven op het scherm **Welkom** (het stand-byscherm voor verificatie).
   - ❏ Wanneer Verificatie-instellingen is uitgeschakeld, wordt het pictogram weergegeven op het startscherm.
2. Tik op **Ja** wanneer het bevestigingsscherm wordt weergegeven.
3. Voer het beheerderswachtwoord in.

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

Tik om uit te loggen rechtsboven in het startscherm op  .

Verificatie-instellingen uitschakelen

U kunt Verificatie-instellingen uitschakelen met Web Config.

Opmerking:
De Gebruikersinstellingen die in de scanner zijn geregistreerd, worden ook opgeslagen als Verificatie-instellingen is uitgeschakeld. U kunt deze verwijderen door de standaardinstellingen van de scanner te herstellen.

1. Open Web Config.
2. Selecteer het tabblad **Productbeveiliging** > **Basis** > **Authenticatie**.
3. Selecteer **Uit**.
4. Klik op **Volgende**.
5. Klik op **OK**.

Opmerking:
Ook als u Verificatie-instellingen uitschakelt, blijft Instelling vergrendelen ingeschakeld. Als u deze optie wilt uitschakelen, kunt u dit doen via het bedieningspaneel of Web Config.

Gerelateerde informatie

➡ "Instelling vergrendelen instellen via het bedieningspaneel" op pagina 89
➡ "Instelling vergrendelen instellen via Web Config" op pagina 89

Verificatie-instellingen verwijderen (Standaardinst. herstellen)

Als u alle Verificatie-instellingen wilt verwijderen (Kaartlezer, Verificatiemethode, Gebruikersinstellingen enzovoort), moet u alle scannerinstellingen terugzetten naar de standaardinstellingen.

Selecteer **Instel.** > **Systeembeheer** > **Standaardinst. herstellen** > **Alle instellingen** op het bedieningspaneel.

Belangrijk:
Ook alle contactpersonen en andere netwerkinstellingen worden verwijderd. Verwijderde instellingen kunnen niet worden hersteld.

Problemen 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 worden ondersteund.

Onderhoud

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 roller 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.

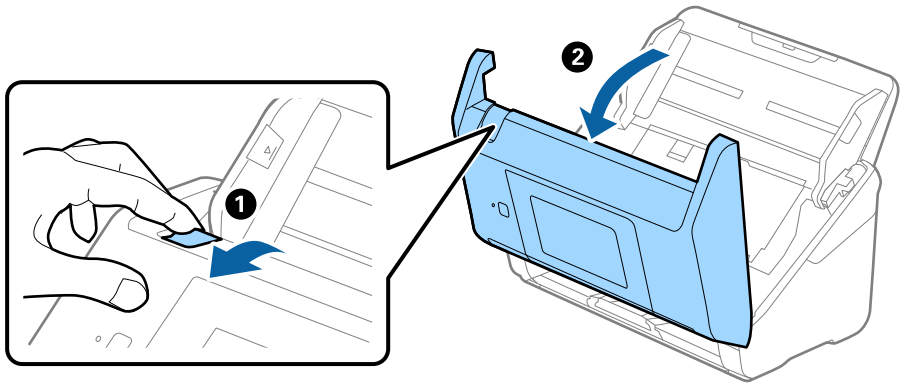
Als het oppervlak is vervuild met een moeilijk te verwijderen materiaal, gebruikt u een originele Epson-reinigingsset om de vlekken te verwijderen. Gebruik een beperkte hoeveelheid reinigingsmiddel op de reinigingsdoek om de vlekken te verwijderen.

Belangrijk:

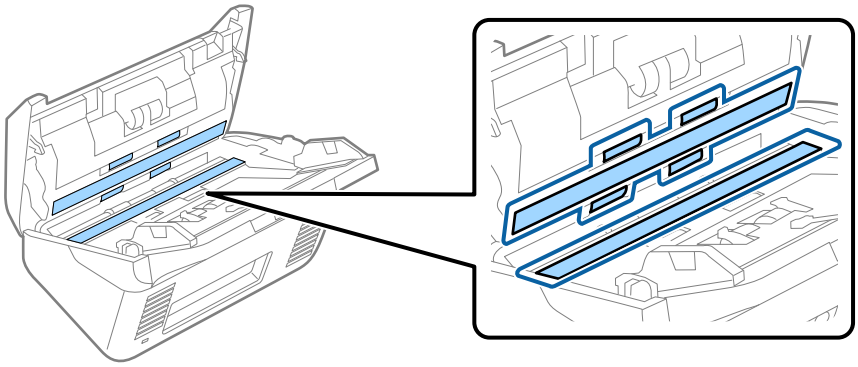
- ❏ *Maak de scanner nooit schoon met alcohol, thinner of bijtende oplosmiddelen. Er kan vervorming of kleurverandering optreden.*
- ❏ *Spuit nooit vloeistof of smeermiddel op de scanner. Schade aan de apparatuur of onderdelen kan leiden tot ongewone bewerkingen.*
- ❏ *Verwijder nooit de behuizing van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



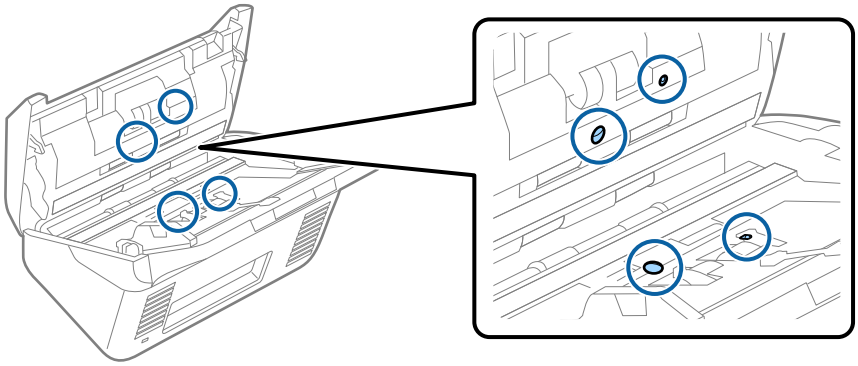
4. Veeg met een zachte doek of een originele Epson-reinigingsset vlekken van de plastic roller en de glasplaat onder in het scannerdeksel.



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.*

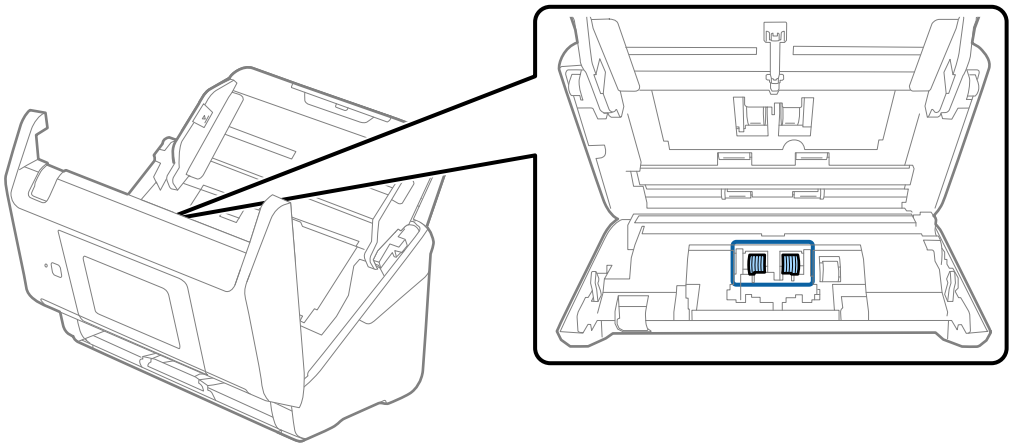
5. Veeg met een wattenstaafje vlekken van de sensoren.



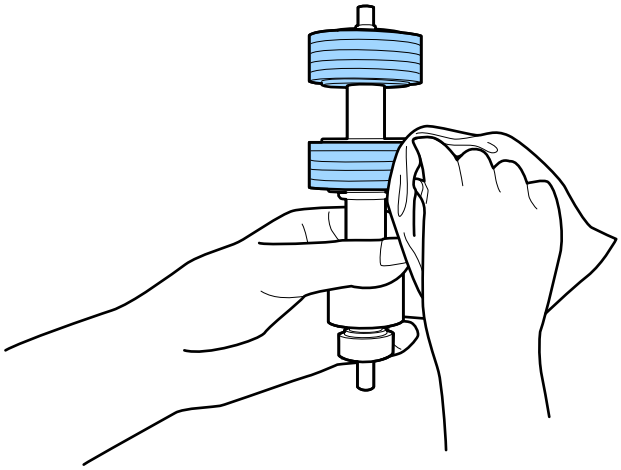
> ***Belangrijk:***
> *Gebruik geen vloeistoffen, zoals reinigingsmiddel, op een wattenstaafje.*

6. Open het deksel en verwijder de scheidingsrol.

   Raadpleeg voor meer informatie “De rollerset vervangen”.



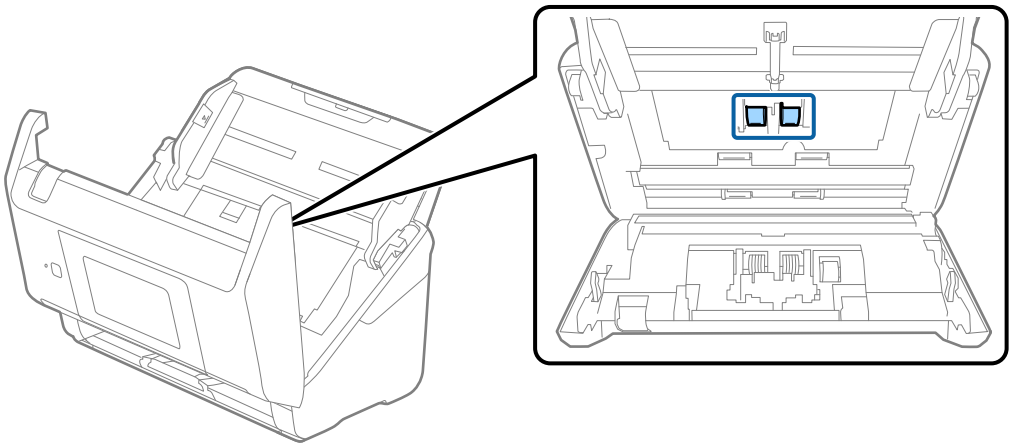
7. Veeg stof of vuil van de scheidingsrol met een originele Epson-reinigingsset of met een zachte, vochtige doek.



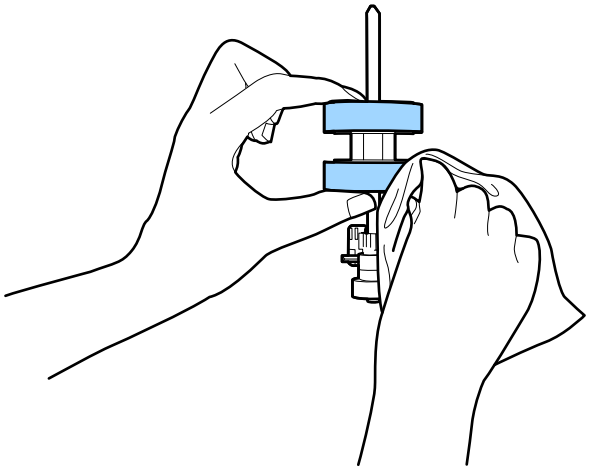
> ***Belangrijk:***
> *Gebruik een originele Epson-reinigingsset of een zachte, vochtige doek om de rol te reinigen. Als u een droge doek gebruikt, beschadigt u mogelijk het oppervlak van de rol.*

8. Open het deksel en verwijder de transportrol.

   Raadpleeg voor meer informatie “De rollerset vervangen”.



9. Veeg stof of vuil van de transportrol met een originele Epson-reinigingsset of met een zachte, vochtige doek.



> ***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.*

10. Sluit het scannerdeksel.

11. Sluit de lichtnetadapter aan en schakel de scanner in.

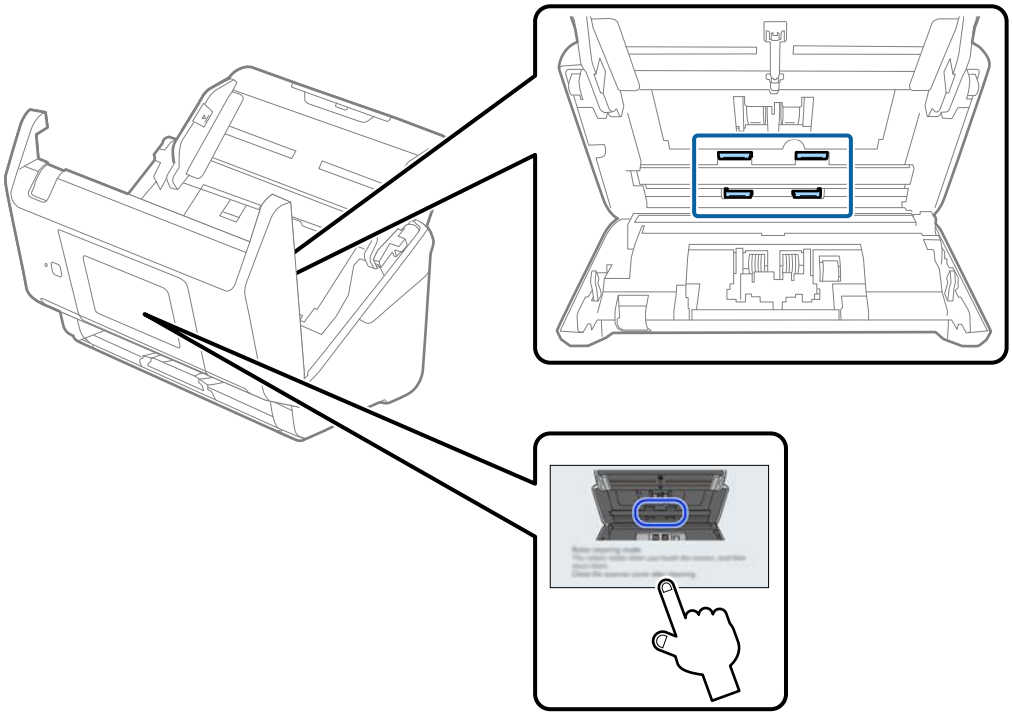
12. Selecteer in het startscherm **Onderhoud scanner**.

13. Selecteer in het scherm **Onderhoud scanner** de optie **Rolreiniging**.

14. 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.

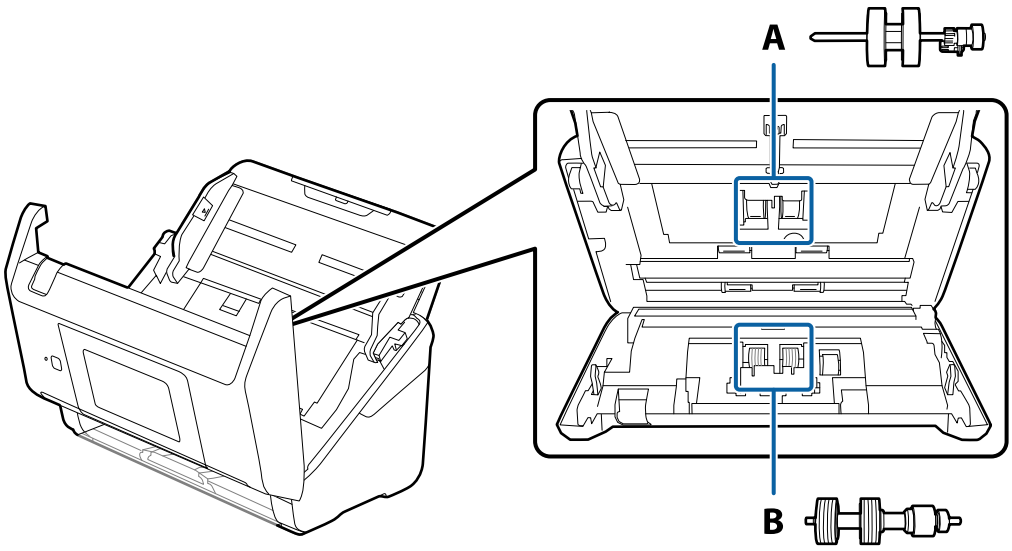
    De rolreinigingsmodus van de scanner wordt uitgeschakeld.

Gerelateerde informatie

➡ "De rollerset vervangen" op pagina 164

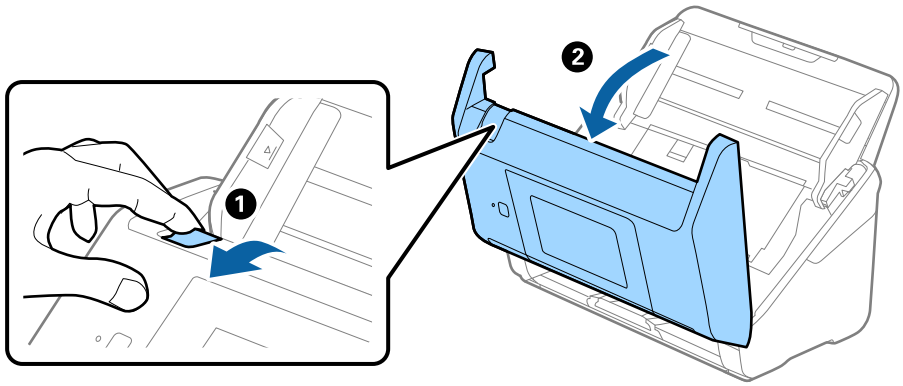
De rollerset vervangen

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.

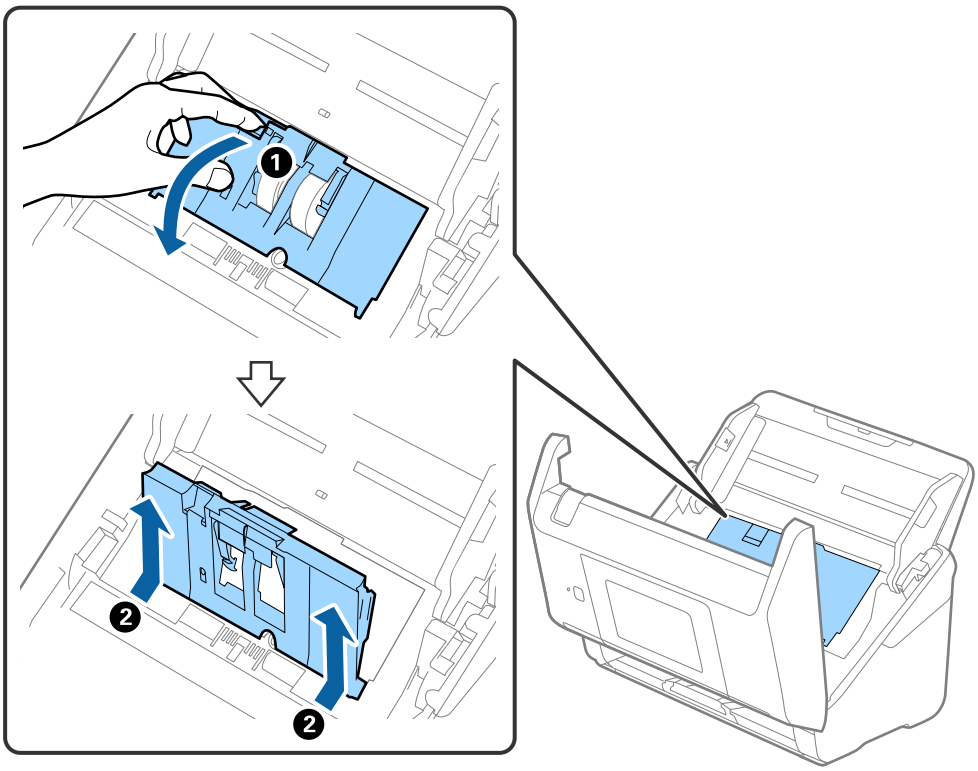


A: transportrol, B: scheidingsrol

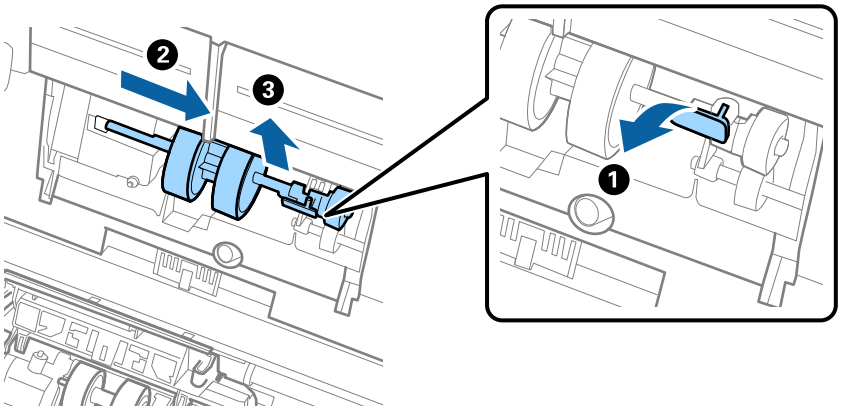
1. Druk op de knop ⏻ om de scanner uit te schakelen.
2. Koppel de lichtnetadapter los van de scanner.
3. Trek aan de hendel en open het scannerdeksel.



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



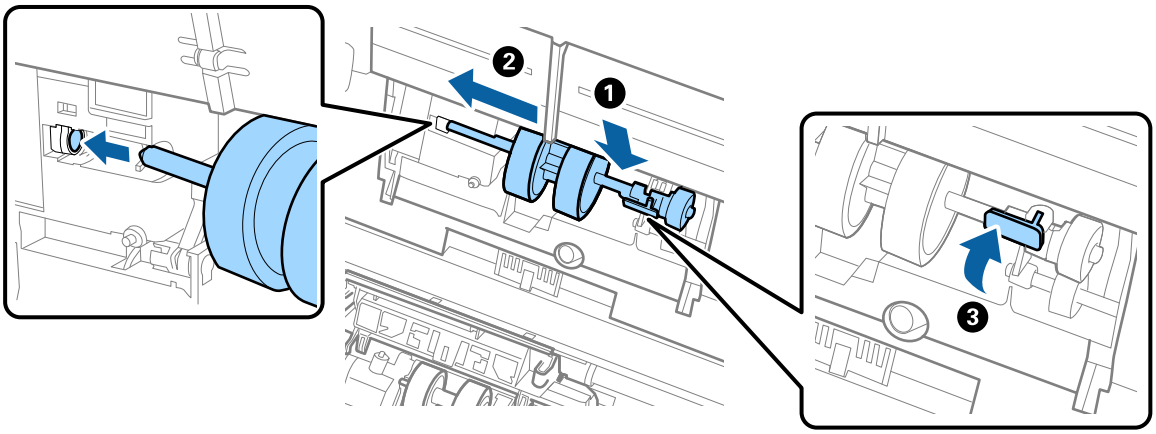
5. Trek de houder van de rolas naar beneden en schuif de geplaatste transportrollen opzij om ze te verwijderen.



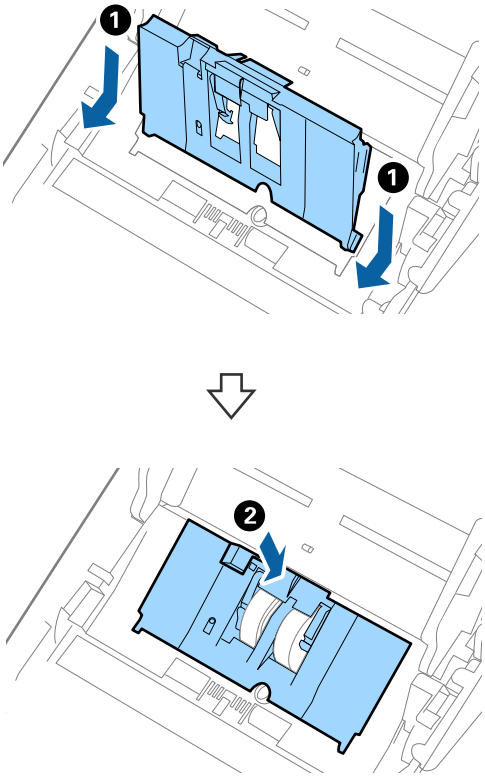
Belangrijk:

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.

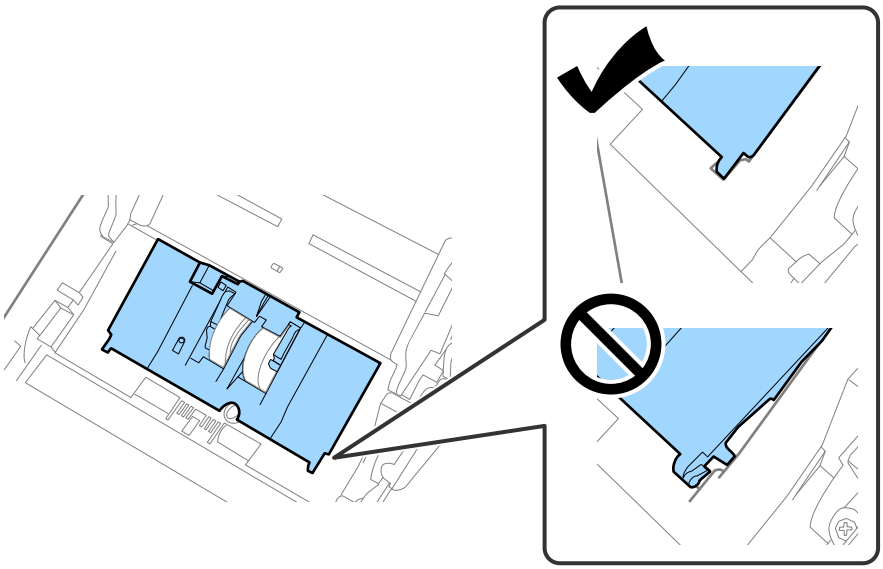


7. Plaats de rand van de kap van de transportrol in de sleuf en schuif hem dicht. Sluit de kap goed.

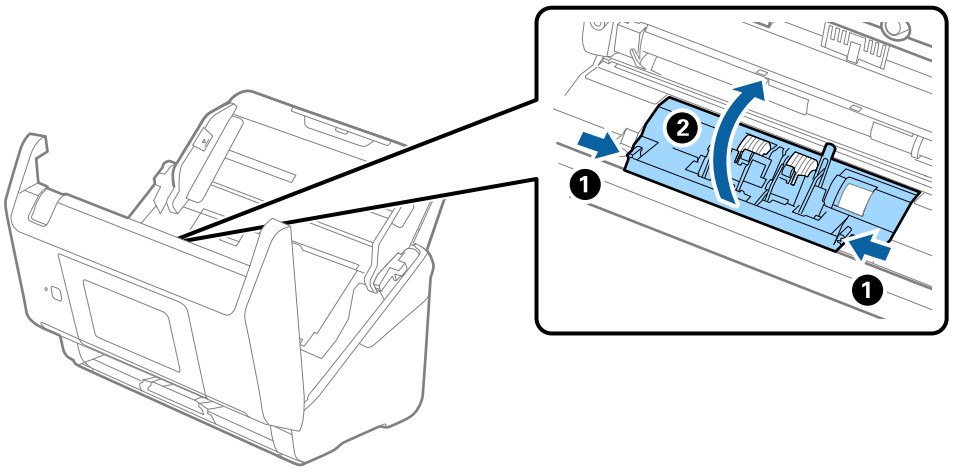


Belangrijk:

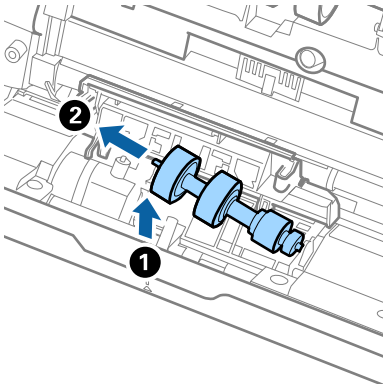
- ❏ *Controleer of de kap van de transportrol correct is gesloten.*
- ❏ *Controleer of de invoerrollen correct zijn geplaatst als u moeite hebt met het sluiten van de kap.*
- ❏ *Sluit de kap niet wanneer deze omhoog staat.*



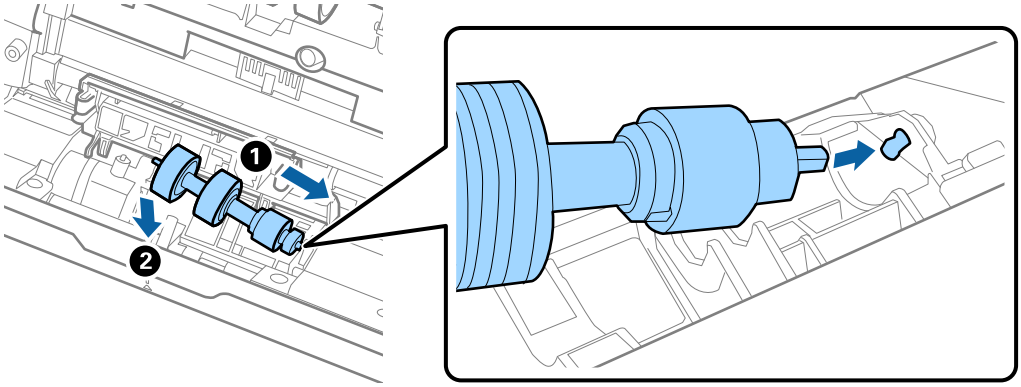
8. Duw op de haken aan beide zijden van de kap van de scheidingsrol om de kap te openen.



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.

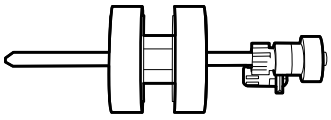
14. Reset de teller voor het aantal scans op het bedieningspaneel.

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

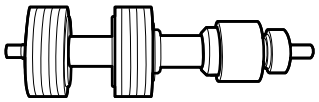
Codes voor de rollenset

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 via Epson Scan 2 Utility.

A



B



A: transportrol, B: scheidingsrol

Naam van onderdeel	Codes	Levensduur
Rollenset	B12B819671 B12B819681 (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

Stel het aantal scans na vervanging van de rollerset opnieuw in.

1. Selecteer **Instel.** > **Apparaatgegevens** > **Het aantal scans resetten** > **Aantal scans na vervangen roller** in het startscherm.
2. Tik op **Ja**.

Gerelateerde informatie

➡ "De rollerset vervangen" op pagina 164

Energiebesparing

U kunt energie besparen door de slaapmodus of de modus voor automatische uitschakeling te gebruiken wanneer de scanner niet wordt gebruikt. U kunt de duur instellen voordat de slaapmodus op de scanner wordt ingeschakeld en deze 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 **Uitschakelinst.** en configureer hier de instellingen.

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

De scanner vervoeren

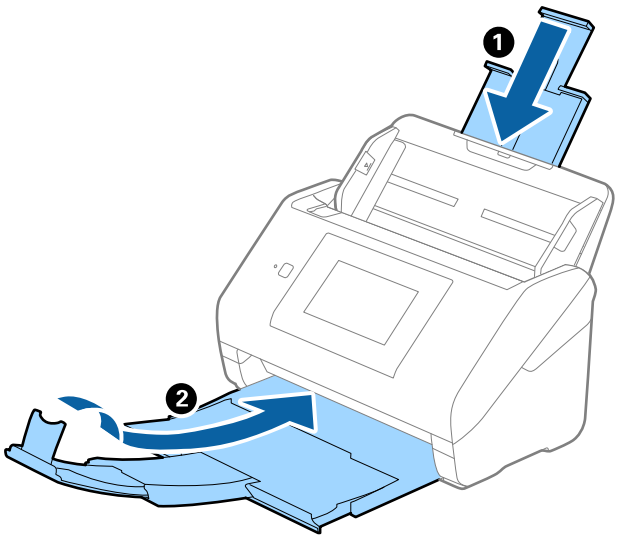
Als u uw scanner moet verplaatsen of vervoeren voor reparatie, volg dan de onderstaande stappen voor het inpakken van de scanner.

1. Druk op de knop ⏻ om de scanner uit te schakelen.

2. Koppel de lichtnetadapter los.

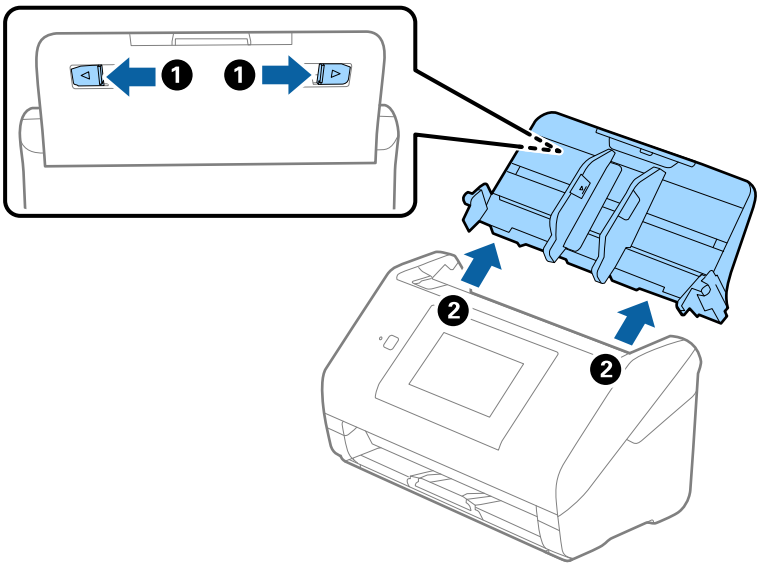
3. Verwijder de kabels en de apparaten.

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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

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, inclusief de contactpersonen en de verificatie-instellingen voor gebruikers, verwijderd. Verwijderde instellingen kunnen niet worden hersteld.*

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 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** > **Programma's** > **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

➡ "Webconfiguratie uitvoeren op een webbrowser" op pagina 36

Firmware bijwerken zonder verbinding te maken met internet

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

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.