

Handleiding beveiligingsfuncties

Belangrijke informatie met betrekking tot de beveiliging

- Het standaardwachtwoord voor het beheer van de apparaatinstellingen vindt u op de onderzijde van het apparaat bij "**Pwd**". Het verdient de aanbeveling het standaardwachtwoord onmiddellijk te wijzigen om onbevoegde toegang tot het apparaat te voorkomen.
- Wanneer u het apparaat wilt verbinden met een extern netwerk zoals het internet, zorg er dan voor dat u uw netwerkomgeving goed beschermt met een aparte firewall (of andere oplossing) om te voorkomen dat informatie kan uitlekken als gevolg van onjuiste instellingen of onbevoegde toegang door kwaadwillenden.
- Als er een signaal in de buurt beschikbaar is, kunt u met een draadloos LAN een netwerkverbinding instellen. Als de beveiligingsinstellingen echter niet goed zijn geconfigureerd, kan het signaal worden onderschept door kwaadwillenden, met de volgende risico's:
 - Diefstal van persoonlijke of vertrouwelijke gegevens
 - Verzenden van gegevens naar partijen die zich voordoen als een bepaalde persoon
 - Ongewenste verspreiding van onderschepte communicatie



Verwante informatie

- [Netwerk](#)
-

Certificaten configureren voor een veilig apparaat

U moet een certificaat configureren om uw netwerkkapparaat veilig te kunnen beheren met SSL/TLS. U moet Beheer via een webbrowser gebruiken om een certificaat te configureren.

- [Overzicht eigenschappen beveiligingscertificaten](#)
- [Een certificaat maken en installeren](#)
- [Een zelf ondertekend certificaat aanmaken](#)
- [Een ondertekeningsverzoek \(CSR\) aanmaken en een certificaat van een certificeringsinstantie \(CA\) installeren](#)
- [Het certificaat en de private sleutel importeren en exporteren](#)
- [Een CA-certificaat importeren en exporteren](#)

Overzicht eigenschappen beveiligingscertificaten

Uw apparaat ondersteunt het gebruik van meerdere beveiligingscertificaten, zodat het apparaat veilig kan worden geverifieerd en er veilig mee kan worden gecommuniceerd. De volgende functies voor beveiligingscertificaten kunnen op het apparaat worden gebruikt:



De ondersteunde functies, opties en instellingen kunnen per model verschillen.

- SSL/TLS-communicatie
- IEEE 802.1x-verificatie
- IPsec

Uw apparaat ondersteunt het volgende:

- Vooraf geïnstalleerd certificaat

Uw apparaat bevat een vooraf geïnstalleerd zelf-ondertekend certificaat. Met dit certificaat kunt u gebruikmaken van SSL/TLS-communicatie zonder een ander certificaat te hoeven maken of installeren.



Het voorgeïnstalleerde zelfondertekende certificaat beschermt uw communicatie tot op zeker niveau. Voor een betere beveiliging raden wij u aan een certificaat te gebruiken dat uitgevaardigd werd door een vertrouwde organisatie.

- Zelf-ondertekend certificaat

Deze afdrukserver geeft zijn eigen certificaat uit. Met dit certificaat kunt u eenvoudig gebruikmaken van SSL/TLS-communicatie zonder een ander certificaat van een CA te moeten maken of installeren.

- Certificaat van een certificeringsinstantie (CA)

U kunt een certificaat van een certificeringsinstantie (CA) op twee manieren installeren. Als u al een certificaat van een CA hebt of een certificaat van een externe betrouwbare CA wilt gebruiken:

- Bij gebruik van een CSR (ondertekeningsverzoek) van deze afdrukserver.
- Bij het importeren van een certificaat en een geheime sleutel.

- Certificaat van certificeringsinstantie (CA)

Om een CA-certificaat te gebruiken dat de CA identificeert en over de private sleutel ervan beschikt, dient u vóór de configuratie van de netwerkbeveiligingsfuncties een CA-certificaat van de CA te importeren.



- Als u gebruik wil maken van SSL/TLS-communicatie raden we u aan eerst advies in te winnen bij de systeembeheerder.
- Als u fabrieksinstellingen van de afdrukserver herstelt, worden het certificaat en de geheime sleutel die zijn geïnstalleerd verwijderd. Als u hetzelfde certificaat en dezelfde geheime sleutel wilt behouden, exporteer ze dan voorafgaand aan het herstellen van de fabrieksinstellingen en installeer ze na afloop opnieuw.



Verwante informatie

- [Certificaten configureren voor een veilig apparaat](#)

Gerelateerde onderwerpen:

- [IEEE 802.1x-verificatie configureren voor uw netwerk met behulp van Beheer via een webbrowser](#)

Een certificaat maken en installeren

U kunt uit twee soorten beveiligingscertificaten kiezen: gebruik een zelfondertekend certificaat of gebruik een certificaat van een certificeringsinstantie (CA).

Optie 1

Zelf-ondertekend certificaat

1. Maak een zelfondertekend certificaat aan met Beheer via een webbrowser.
2. Installeer het zelfondertekende certificaat op uw computer.

Optie 2

Certificaat van een CA

1. Maak een CSR (Certificate Signing Request) aan met Beheer via een webbrowser.
2. Installeer het certificaat uitgevaardigd door de CA op uw Brother-apparaat met Beheer via een webbrowser.
3. Installeer het certificaat op uw computer.



Verwante informatie

- [Certificaten configureren voor een veilig apparaat](#)
-

Een zelf ondertekend certificaat aanmaken

1. Start uw webbrowser.
2. Voer "https://IP-adres van apparaat" in de adresbalk van uw browser in (waarbij "IP-adres van apparaat" staat voor het IP-adres van het apparaat).

Bijvoorbeeld:

https://192.168.1.2

Het IP-adres van uw apparaat vindt u in het netwerkconfiguratierapport.

3. Voer zo nodig het wachtwoord in in het veld **Inloggen** en klik vervolgens op **Inloggen**.



Het standaardwachtwoord voor het beheer van de apparaatinstellingen vindt u op de achter- of onderzijde van het apparaat bij "**Pwd**". Wijzig het standaardwachtwoord aan de hand van de aanwijzingen op het scherm wanneer u zich voor het eerst aanmeldt.

4. Klik op **Netwerk** > **Beveiliging** > **Certificaat** in de linkernavigatiebalk.



Als de linkernavigatiebalk niet zichtbaar is, begint u te navigeren bij ☰.

5. Klik op **Zelf ondertekend certificaat maken**.
6. Voer een **Algemene naam** en een **Geldigheidsdatum** in.
 - De lengte van de **Algemene naam** is minder dan 64 bytes. Voer een identicator in zoals een IP-adres, naam van een knooppunt of domeinnaam die u zult gebruiken om toegang te krijgen tot dit apparaat via SSL/TLS-communicatie. De naam van het knooppunt wordt standaard weergegeven.
 - Een waarschuwing wordt weergegeven als u het IPPS- of HTTPS-protocol gebruikt en een andere naam in de URL invoert dan de **Algemene naam** die werd gebruikt voor het zelfondertekende certificaat.
7. Selecteer uw instelling in de vervolgkeuzelijst **Algoritme van openbare sleutel**.
8. Selecteer uw instelling in de vervolgkeuzelijst **Digest-algoritme**.
9. Klik op **Indienen**.



Verwante informatie

- [Certificaten configureren voor een veilig apparaat](#)

Een ondertekeningverzoek (CSR) aanmaken en een certificaat van een certificeringsinstantie (CA) installeren

Als u al over een certificaat van een externe betrouwbare certificeringsinstantie (CA) beschikt, kunt u het certificaat en de geheime sleutel opslaan op het apparaat en deze beheren via importeren en exporteren. Als u niet over een certificaat van een externe betrouwbare CA beschikt, maakt u een ondertekeningverzoek (CSR) aan, stuurt u dit naar een certificeringsinstantie (CA) ter verificatie en installeert u het ontvangen certificaat op uw apparaat.

- [Een CSR \(Certificate Signing Request\) aanmaken](#)
- [Een certificaat installeren op uw apparaat](#)

Een CSR (Certificate Signing Request) aanmaken

Een CSR (Certificate Signing Request) is een aanvraag die naar een certificeringsinstantie (CA) wordt verzonden om de kwalificaties in het certificaat te verifiëren.

Het is aan te raden een hoofdcertificatie van de CA op de computer te installeren voordat u de CSR aanmaakt.

1. Start uw webbrowser.
2. Voer "https://IP-adres van apparaat" in de adresbalk van uw browser in (waarbij "IP-adres van apparaat" staat voor het IP-adres van het apparaat).

Bijvoorbeeld:

https://192.168.1.2

Het IP-adres van uw apparaat vindt u in het netwerkconfiguratierapport.

3. Voer zo nodig het wachtwoord in in het veld **Inloggen** en klik vervolgens op **Inloggen**.



Het standaardwachtwoord voor het beheer van de apparaatinstellingen vindt u op de achter- of onderzijde van het apparaat bij "**Pwd**". Wijzig het standaardwachtwoord aan de hand van de aanwijzingen op het scherm wanneer u zich voor het eerst aanmeldt.

4. Klik op **Netwerk > Beveiliging > Certificaat** in de linkernavigatiebalk.



Als de linkernavigatiebalk niet zichtbaar is, begint u te navigeren bij .

5. Klik op **CSR maken**.
6. Voer een **Algemene naam** (vereist) in en voeg bijkomende informatie over uw **Organisatie** toe (optioneel).



- U moet de coördinaten van uw bedrijf verschaffen zodat een CA uw identiteit kan controleren en bevestigen aan een buitenstaander.
- De lengte van de **Algemene naam** moet minder dan 64 bytes zijn. Voer een identicator in zoals een IP-adres, naam van een knooppunt of domeinnaam die u zult gebruiken om toegang te krijgen tot dit apparaat via SSL/TLS-communicatie. De naam van het knooppunt wordt standaard weergegeven. De **Algemene naam** is vereist.
- Een waarschuwing wordt weergegeven als u een andere naam in de URL invoert dan de openbare naam die werd gebruikt voor het certificaat.
- De lengte van de **Organisatie**, de **Organisatorische eenheid**, de **Plaats** en de **Provincie** moet minder dan 64 bytes zijn.
- De **Land/Regio** moet een ISO 3166-landcode van twee tekens zijn.
- Als u een X.509v3-certificaatextensie configureert, vinkt u het vakje **Uitgebreide partitie configureren** aan en selecteert u vervolgens **Automatisch (IPv4 registreren)** of **Handmatig**.

7. Selecteer uw instelling in de vervolgkeuzelijst **Algoritme van openbare sleutel**.

8. Selecteer uw instelling in de vervolgkeuzelijst **Digest-algoritme**.

9. Klik op **Indienen**.

De CSR wordt weergegeven op uw scherm. Sla de CSR op als bestand of kopieer het naar een online CSR-formulier van een certificeringsinstantie.

10. Klik op **Opslaan**.



- Volg het beleid van uw CA aangaande de methode om een CSR te versturen naar uw CA.
- Als u gebruikmaakt van de basis-CA van onderneming van Windows Server, raden wij u aan de webserver te gebruiken als certificaatsjabloon voor het aanmaken van het veilige clientcertificaat. Als u een clientcertificaat aanmaakt voor een IEEE 802.1x-omgeving met EAP-TLS-verificatie, raden wij u aan Gebruiker te gebruiken als certificaatsjabloon.



Verwante informatie

- Een ondertekeningverzoek (CSR) aanmaken en een certificaat van een certificeringsinstantie (CA) installeren
-

Een certificaat installeren op uw apparaat

Wanneer u een certificaat ontvangt van een certificeringsinstantie (CA), volgt u onderstaande stappen om het te installeren op de afdrukserver:

Alleen een certificaat dat uitgevaardigd is met de aanvraag voor certificaatondertekening (CSR) van uw apparaat kan op uw apparaat worden geïnstalleerd. Als u een andere CSR wilt aanmaken, dient u ervoor te zorgen dat het certificaat geïnstalleerd is voordat u de nieuwe CSR aanmaakt. Maak pas een andere CSR aan nadat u het certificaat op het apparaat hebt geïnstalleerd, want anders is de CSR die u had aangemaakt vóór installatie van de nieuwe CSR ongeldig.

1. Start uw webbrowser.
2. Voer "https://IP-adres van apparaat" in de adresbalk van uw browser in (waarbij "IP-adres van apparaat" staat voor het IP-adres van het apparaat).
Bijvoorbeeld:
https://192.168.1.2
Het IP-adres van uw apparaat vindt u in het netwerkconfiguratierapport.
3. Voer zo nodig het wachtwoord in in het veld **Inloggen** en klik vervolgens op **Inloggen**.



Het standaardwachtwoord voor het beheer van de apparaatinstellingen vindt u op de achter- of onderzijde van het apparaat bij "**Pwd**". Wijzig het standaardwachtwoord aan de hand van de aanwijzingen op het scherm wanneer u zich voor het eerst aanmeldt.

4. Klik op **Netwerk > Beveiliging > Certificaat** in de linkernavigatiebalk.



Als de linkernavigatiebalk niet zichtbaar is, begint u te navigeren bij .

5. Klik op **Certificaat installeren**.
6. Blader naar het bestand met het certificaat dat werd uitgevaardigd door de CA en klik vervolgens op **Indienen**.

Het certificaat wordt aangemaakt en opgeslagen in het geheugen van het apparaat.

Om SSL/TLS-communicatie te kunnen gebruiken, moet de hoofdcertificatie van de CA eveneens op uw computer worden geïnstalleerd. Neem contact op met uw netwerkbeheerder.



Verwante informatie

- [Een ondertekeningsverzoek \(CSR\) aanmaken en een certificaat van een certificeringsinstantie \(CA\) installeren](#)

Het certificaat en de private sleutel importeren en exporteren

Sla het certificaat en de geheime sleutel op het apparaat op en beheer deze via importeren en exporteren.

- [Een certificaat en geheime sleutel importeren](#)
- [Het certificaat en de private sleutel exporteren](#)

Een certificaat en geheime sleutel importeren

1. Start uw webbrowser.
2. Voer "https://IP-adres van apparaat" in de adresbalk van uw browser in (waarbij "IP-adres van apparaat" staat voor het IP-adres van het apparaat).

Bijvoorbeeld:

https://192.168.1.2

Het IP-adres van uw apparaat vindt u in het netwerkconfiguratierapport.

3. Voer zo nodig het wachtwoord in in het veld **Inloggen** en klik vervolgens op **Inloggen**.



Het standaardwachtwoord voor het beheer van de apparaatinstellingen vindt u op de achter- of onderzijde van het apparaat bij "**Pwd**". Wijzig het standaardwachtwoord aan de hand van de aanwijzingen op het scherm wanneer u zich voor het eerst aanmeldt.

4. Klik op **Netwerk** > **Beveiliging** > **Certificaat** in de linkernavigatiebalk.



Als de linkernavigatiebalk niet zichtbaar is, begint u te navigeren bij ☰.

5. Klik op **Certificaat en geheime sleutel importeren**.
6. Blader naar het bestand dat u wilt importeren en selecteer dat.
7. Typ het wachtwoord als het bestand versleuteld is en klik vervolgens op **Indienen**.

Het certificaat en de geheime sleutel zijn met succes geïmporteerd in uw apparaat.



Verwante informatie

- [Het certificaat en de private sleutel importeren en exporteren](#)

Het certificaat en de private sleutel exporteren

1. Start uw webbrowser.
2. Voer "https://IP-adres van apparaat" in de adresbalk van uw browser in (waarbij "IP-adres van apparaat" staat voor het IP-adres van het apparaat).

Bijvoorbeeld:

https://192.168.1.2

Het IP-adres van uw apparaat vindt u in het netwerkconfiguratierapport.

3. Voer zo nodig het wachtwoord in in het veld **Inloggen** en klik vervolgens op **Inloggen**.



Het standaardwachtwoord voor het beheer van de apparaatinstellingen vindt u op de achter- of onderzijde van het apparaat bij "**Pwd**". Wijzig het standaardwachtwoord aan de hand van de aanwijzingen op het scherm wanneer u zich voor het eerst aanmeldt.

4. Klik op **Netwerk > Beveiliging > Certificaat** in de linkernavigatiebalk.



Als de linkernavigatiebalk niet zichtbaar is, begint u te navigeren bij .

5. Klik op **Exporteren** naast **Certificaten**.
6. Voer het wachtwoord in als u het bestand wil versleutelen.
Als een leeg wachtwoord wordt gebruikt, wordt er geen versleuteling toegepast.
7. Voer het wachtwoord nogmaals in ter bevestiging en klik daarna op **Indienen**.
8. Klik op **Opslaan**.

Het certificaat en de geheime sleutel zijn geëxporteerd naar uw computer.

U kunt het certificaat ook importeren op uw computer.



Verwante informatie

- [Het certificaat en de private sleutel importeren en exporteren](#)

Een CA-certificaat importeren en exporteren

U kunt CA-certificaten op uw Brother-apparaat importeren, exporteren en opslaan.

- [Een CA-certificaat importeren](#)
- [Een CA-certificaat exporteren](#)

Een CA-certificaat importeren

1. Start uw webbrowser.
2. Voer "https://IP-adres van apparaat" in de adresbalk van uw browser in (waarbij "IP-adres van apparaat" staat voor het IP-adres van het apparaat).

Bijvoorbeeld:

https://192.168.1.2

Het IP-adres van uw apparaat vindt u in het netwerkconfiguratierapport.

3. Voer zo nodig het wachtwoord in in het veld **Inloggen** en klik vervolgens op **Inloggen**.



Het standaardwachtwoord voor het beheer van de apparaatinstellingen vindt u op de achter- of onderzijde van het apparaat bij "**Pwd**". Wijzig het standaardwachtwoord aan de hand van de aanwijzingen op het scherm wanneer u zich voor het eerst aanmeldt.

4. Klik op **Netwerk > Beveiliging > CA-certificaat** in de linkernavigatiebalk.



Als de linkernavigatiebalk niet zichtbaar is, begint u te navigeren bij ☰.

5. Klik op **CA-certificaat importeren**.
6. Blader naar het bestand dat u wilt importeren.
7. Klik op **Indienen**.



Verwante informatie

- [Een CA-certificaat importeren en exporteren](#)

Een CA-certificaat exporteren

1. Start uw webbrowser.
2. Voer "https://IP-adres van apparaat" in de adresbalk van uw browser in (waarbij "IP-adres van apparaat" staat voor het IP-adres van het apparaat).

Bijvoorbeeld:

https://192.168.1.2

Het IP-adres van uw apparaat vindt u in het netwerkconfiguratie rapport.

3. Voer zo nodig het wachtwoord in in het veld **Inloggen** en klik vervolgens op **Inloggen**.



Het standaardwachtwoord voor het beheer van de apparaatinstellingen vindt u op de achter- of onderzijde van het apparaat bij "**Pwd**". Wijzig het standaardwachtwoord aan de hand van de aanwijzingen op het scherm wanneer u zich voor het eerst aanmeldt.

4. Klik op **Netwerk** > **Beveiliging** > **CA-certificaat** in de linkernavigatiebalk.



Als de linkernavigatiebalk niet zichtbaar is, begint u te navigeren bij ☰.

5. Selecteer het certificaat dat u wilt exporteren en klik op **Exporteren**.
6. Klik op **Indienen**.



Verwante informatie

- [Een CA-certificaat importeren en exporteren](#)

SSL/TLS gebruiken

- [Uw netwerk veilig beheren met SSL/TLS](#)
- [Documenten veilig afdrukken met SSL/TLS](#)
- [E-mailberichten veilig verzenden of ontvangen met SSL/TLS](#)

Uw netwerk veilig beheren met SSL/TLS

- [Een certificaat configureren voor SSL/TLS en beschikbare protocollen](#)
- [Beheer via een webbrowser gebruiken met SSL/TLS](#)
- [Het zelfondertekende certificaat voor Windows-gebruikers installeren als beheerder](#)
- [Certificaten configureren voor een veilig apparaat](#)

Een certificaat configureren voor SSL/TLS en beschikbare protocollen

Configureer met Beheer via een webbrowser een certificaat op uw apparaat voordat u SSL/TLS-communicatie gebruikt.

1. Start uw webbrowser.
2. Voer "https://IP-adres van apparaat" in de adresbalk van uw browser in (waarbij "IP-adres van apparaat" staat voor het IP-adres van het apparaat).

Bijvoorbeeld:

https://192.168.1.2

Het IP-adres van uw apparaat vindt u in het netwerkconfiguratierapport.

3. Voer zo nodig het wachtwoord in in het veld **Inloggen** en klik vervolgens op **Inloggen**.



Het standaardwachtwoord voor het beheer van de apparaatinstellingen vindt u op de achter- of onderzijde van het apparaat bij "**Pwd**". Wijzig het standaardwachtwoord aan de hand van de aanwijzingen op het scherm wanneer u zich voor het eerst aanmeldt.

4. Klik op **Netwerk > Netwerk > Protocol** in de linkernavigatiebalk.



Als de linkernavigatiebalk niet zichtbaar is, begint u te navigeren bij .

5. Klik op **HTTP-serverinstellingen**.
6. Selecteer het certificaat dat u wilt configureren in de vervolgkeuzelijst **Selecteer het certificaat**.
7. Klik op **Indienen**.
8. Klik op **Ja** om de afdrukserver opnieuw op te starten.



Verwante informatie

- [Uw netwerk veilig beheren met SSL/TLS](#)

Gerelateerde onderwerpen:

- [Documenten veilig afdrukken met SSL/TLS](#)

Beheer via een webbrowser gebruiken met SSL/TLS

Om uw netwerkapparaat veilig te kunnen beheren, dient u de beheerprogramma's met beveiligingsprotocollen te gebruiken.



- Om het HTTPS-protocol te gebruiken, moet HTTPS ingeschakeld zijn op uw apparaat. Het HTTPS-protocol is standaard ingeschakeld.
- U kunt de instellingen van het HTTPS-protocol wijzigen met Beheer via een webbrowser.

1. Start uw webbrowser.
2. Voer "https://IP-adres van apparaat" in de adresbalk van uw browser in (waarbij "IP-adres van apparaat" staat voor het IP-adres van het apparaat).

Bijvoorbeeld:

https://192.168.1.2

Het IP-adres van uw apparaat vindt u in het netwerkconfiguratierapport.

3. Voer zo nodig het wachtwoord in in het veld **Inloggen** en klik vervolgens op **Inloggen**.



Het standaardwachtwoord voor het beheer van de apparaatinstellingen vindt u op de achter- of onderzijde van het apparaat bij "**Pwd**". Wijzig het standaardwachtwoord aan de hand van de aanwijzingen op het scherm wanneer u zich voor het eerst aanmeldt.

4. U krijgt nu toegang tot het apparaat via HTTPS.



Verwante informatie

- [Uw netwerk veilig beheren met SSL/TLS](#)

Het zelfondertekende certificaat voor Windows-gebruikers installeren als beheerder

- De volgende stappen zijn voor Microsoft Edge. Als u een andere webbrowser gebruikt, raadpleeg dan de documentatie of online-Help van die browser voor aanwijzingen voor het installeren van certificaten.
- Zorg ervoor dat u een zelfondertekend certificaat hebt aangemaakt met Beheer via een webbrowser.

1. Klik met de rechtermuisknop op het pictogram **Microsoft Edge** en klik vervolgens op **Als administrator uitvoeren**.

Als het scherm **Gebruikersaccountbeheer** verschijnt, klik dan op **Ja**.

2. Voer "https://IP-adres van apparaat" in de adresbalk van uw browser in (waarbij "IP-adres van apparaat" staat voor het IP-adres van het apparaat).

Bijvoorbeeld:

https://192.168.1.2

Het IP-adres van uw apparaat vindt u in het netwerkconfiguratierapport.

3. Als uw verbinding niet privé is, klik dan op de knop **Geavanceerd** en ga door naar de webpagina.
4. Voer zo nodig het wachtwoord in in het veld **Inloggen** en klik vervolgens op **Inloggen**.



Het standaardwachtwoord voor het beheer van de apparaatinstellingen vindt u op de achter- of onderzijde van het apparaat bij "**Pwd**". Wijzig het standaardwachtwoord aan de hand van de aanwijzingen op het scherm wanneer u zich voor het eerst aanmeldt.

5. Klik op **Netwerk > Beveiliging > Certificaat** in de linkernavigatiebalk.



Als de linkernavigatiebalk niet zichtbaar is, begint u te navigeren bij .

6. Klik op **Exporteren**.
7. Als u het uitvoerbestand wilt versleutelen, typ dan een wachtwoord in het veld **Wachtwoord invoeren**. Als het veld **Wachtwoord invoeren** leeg is, wordt uw uitvoerbestand niet versleuteld.
8. Voer het wachtwoord opnieuw in het veld **Wachtwoord opnieuw invoeren** in en klik vervolgens op **Indienen**.
9. Klik op het gedownloade bestand om het te openen.
10. Wanneer de **Wizard Certificaat importeren** verschijnt, klikt u op **Volgende**.
11. Klik op **Volgende**.
12. Typ een wachtwoord indien nodig en klik vervolgens op **Volgende**.
13. Selecteer **Alle certificaten in het onderstaande archief opslaan** en klik daarna op **Bladeren....**
14. Selecteer **Vertrouwde basiscertificeringsinstanties** en klik vervolgens op **OK**.
15. Klik op **Volgende**.
16. Klik op **Voltooien**.
17. Klik op **Ja** als de vingerafdruk (duimafdruk) correct is.
18. Klik op **OK**.



Verwante informatie

- [Uw netwerk veilig beheren met SSL/TLS](#)

Documenten veilig afdrukken met SSL/TLS

- [Documenten afdrukken met IPPS](#)
- [Een certificaat configureren voor SSL/TLS en beschikbare protocollen](#)
- [Certificaten configureren voor een veilig apparaat](#)

Documenten afdrukken met IPPS

Om documenten veilig met het IPP-protocol af te drukken, gebruikt u het IPPS-protocol.

1. Start uw webbrowser.
2. Voer "https://IP-adres van apparaat" in de adresbalk van uw browser in (waarbij "IP-adres van apparaat" staat voor het IP-adres van het apparaat).

Bijvoorbeeld:

https://192.168.1.2

Het IP-adres van uw apparaat vindt u in het netwerkconfiguratierapport.

3. Voer zo nodig het wachtwoord in in het veld **Inloggen** en klik vervolgens op **Inloggen**.



Het standaardwachtwoord voor het beheer van de apparaatinstellingen vindt u op de achter- of onderzijde van het apparaat bij "**Pwd**". Wijzig het standaardwachtwoord aan de hand van de aanwijzingen op het scherm wanneer u zich voor het eerst aanmeldt.

4. Klik op **Netwerk > Netwerk > Protocol** in de linkernavigatiebalk.



Als de linkernavigatiebalk niet zichtbaar is, begint u te navigeren bij .

5. Zorg ervoor dat het selectievakje **IPP** is aangevinkt.



Als het selectievakje **IPP** niet is aangevinkt, vinkt u het selectievakje **IPP** aan en klikt u vervolgens op **Indienen**.

Start uw apparaat opnieuw op om de configuratie te activeren.

Nadat het apparaat opnieuw is opgestart, keert u terug naar de webpagina van het apparaat. Typ daar het wachtwoord, ga naar de linkernavigatiebalk en klik op **Netwerk > Netwerk > Protocol**.

6. Klik op **HTTP-serverinstellingen**.
7. Vink het selectievakje **HTTPS** in de zone **IPP** aan en klik vervolgens op **Indienen**.
8. Start uw apparaat opnieuw op om de configuratie te activeren.

Communicatie via IPPS kan geen ongeoorloofde toegang tot de afdrukserver voorkomen.



Verwante informatie

- [Documenten veilig afdrukken met SSL/TLS](#)

SNMPv3 gebruiken

- [Het netwerk van uw apparaat veilig beheren met behulp van SNMPv3](#)

Het netwerk van uw apparaat veilig beheren met behulp van SNMPv3

SNMPv3 (Simple Network Management Protocol versie 3) zorgt voor gebruikersverificatie en gegevensversleuteling om netwerkapparaten veilig te kunnen beheren.

1. Start uw webbrowser.
2. Voer "https://algemene naam" in de adresbalk van uw browser in (waarbij "algemene naam" staat voor de algemene naam die u aan het certificaat hebt toegewezen; dit kan uw IP-adres, de naam van een knooppunt of domeinnaam zijn).
3. Voer zo nodig het wachtwoord in in het veld **Inloggen** en klik vervolgens op **Inloggen**.



Het standaardwachtwoord voor het beheer van de apparaatinstellingen vindt u op de achter- of onderzijde van het apparaat bij "**Pwd**". Wijzig het standaardwachtwoord aan de hand van de aanwijzingen op het scherm wanneer u zich voor het eerst aanmeldt.

4. Klik op **Netwerk > Netwerk > Protocol** in de linkernavigatiebalk.



Als de linkernavigatiebalk niet zichtbaar is, begint u te navigeren bij .

5. Zorg ervoor dat de **SNMP**-instelling ingeschakeld is en klik vervolgens op **Geavanceerde instellingen**.
6. Configureer de instellingen voor de SNMPv1/v2c-modus.

Optie	Beschrijving
Toegang lezen/schrijven SNMP v1/v2c	De afdrukserver gebruikt versie 1 en versie 2c van het SNMP-protocol. In deze modus kunt u alle toepassingen op uw apparaat gebruiken. Deze modus is echter niet veilig omdat de gebruiker niet wordt geverifieerd en de gegevens niet worden versleuteld.
SNMP v1/v2c alleen-lezentoegang	De afdrukserver gebruikt de alleen-lezen-toegang van versie 1 en versie 2c van het SNMP-protocol.
Uitgeschakeld	Schakel versie 1 en versie 2c van het SNMP-protocol uit. Alle toepassingen die gebruik maken van SNMPv1/v2c, worden beperkt. Gebruik de modus SNMP v1/v2c alleen-lezentoegang of Toegang lezen/schrijven SNMP v1/v2c om het gebruik van SNMPv1/v2c-toepassingen toe te staan.

7. Configureer de instellingen van de SNMPv3-modus.

Optie	Beschrijving
Ingeschakeld	De afdrukserver gebruikt versie 3 van het SNMP-protocol. Voor veilig beheer van de afdrukserver gebruikt u de SNMPv3-modus en configureert u de instellingen.
Uitgeschakeld	Schakel versie 3 van het SNMP-protocol uit. Alle toepassingen die gebruik maken van SNMPv3, worden beperkt. Gebruik de SNMPv3-modus om het gebruik van SNMPv3-toepassingen toe te staan.

8. Klik op **Indienen**.



Selecteer de gewenste opties wanneer de protocolinstelopties weergegeven worden op het apparaat.

9. Start uw apparaat opnieuw op om de configuratie te activeren.



Verwante informatie

- [SNMPv3 gebruiken](#)

IEEE 802.1x-verificatie voor uw netwerk gebruiken

- [Wat is IEEE 802.1x-verificatie?](#)
- [IEEE 802.1x-verificatie configureren voor uw netwerk met behulp van Beheer via een webbrowser](#)
- [IEEE 802.1x-verificatiemethodes](#)

Wat is IEEE 802.1x-verificatie?

IEEE 802.1x is een IEEE-standaard die de toegang van onbevoegde netwerkapparaten verhindert. Uw Brother-apparaat verstuurt een verificatieaanvraag naar een RADIUS-server (verificatieserver) via uw toegangspunt of hub. Nadat uw aanvraag is geverifieerd door de RADIUS-server, krijgt uw apparaat toegang tot het netwerk.



Verwante informatie

- [IEEE 802.1x-verificatie voor uw netwerk gebruiken](#)
-

IEEE 802.1x-verificatie configureren voor uw netwerk met behulp van Beheer via een webbrowser

- Als u het apparaat configureert met EAP-TLS-verificatie, moet u het door een certificatie-instantie uitgegeven clientcertificaat installeren voordat u de configuratie start. Raadpleeg uw netwerkbeheerder over het clientcertificaat. Als u meerdere certificaten hebt geïnstalleerd, raden we aan de certificaatnaam te noteren die u wilt gebruiken.
- Voordat u het servercertificaat verifieert, moet u het CA-certificaat importeren dat is uitgegeven door de certificeringsinstantie die het servercertificaat heeft ondertekend. Neem contact op met uw netwerkbeheerder of internetprovider (ISP) om na te vragen of het importeren van een CA-certificaat noodzakelijk is.



U kunt de IEEE 802.1x-verificatie ook configureren met de wizard voor de draadloze instellingen vanaf het bedieningspaneel (draadloos netwerk).

- Start uw webbrowser.
- Voer "https://IP-adres van apparaat" in de adresbalk van uw browser in (waarbij "IP-adres van apparaat" staat voor het IP-adres van het apparaat).

Bijvoorbeeld:

https://192.168.1.2

Het IP-adres van uw apparaat vindt u in het netwerkconfiguratierapport.

- Voer zo nodig het wachtwoord in in het veld **Inloggen** en klik vervolgens op **Inloggen**.



Het standaardwachtwoord voor het beheer van de apparaatinstellingen vindt u op de achter- of onderzijde van het apparaat bij "**Pwd**". Wijzig het standaardwachtwoord aan de hand van de aanwijzingen op het scherm wanneer u zich voor het eerst aanmeldt.

- Klik op **Netwerk** in de linkernavigatiebalk.



Als de linkernavigatiebalk niet zichtbaar is, begint u te navigeren bij .

- Ga op een van de volgende manieren te werk:
 - Voor een bedraad netwerk
Klik op **Bedraad** > **Authenticatie 802.1x**.
 - Voor een draadloos netwerk
Klik op **Draadloos** > **Draadloos (Bedrijf)**.
- Configureer de instellingen voor IEEE 802.1x-verificatie.



- Als u IEEE 802.1x-verificatie voor bedrade netwerken wilt inschakelen, selecteert u **Ingeschakeld** voor **Status 802.1x vast** op de pagina **Authenticatie 802.1x**.
- Als u **EAP-TLS**-verificatie gebruikt, moet u het clientcertificaat kiezen dat geïnstalleerd is (weergegeven met certificaatnaam) voor verificatie in de vervolgkeuzelijst **Clientcertificaat**.
- Als u **EAP-FAST**-, **PEAP**-, **EAP-TTLS**- of **EAP-TLS**-verificatie selecteert, kunt u de verificatiemethode selecteren in de vervolgkeuzelijst **Verificatie servercertificaat**. Verifieer het servercertificaat met behulp van het CA-certificaat dat vooraf werd geïmporteerd op het apparaat en dat werd verstrekt door de CA die het servercertificaat ondertekende.

Selecteer een van de volgende verificatiemethoden in de vervolgkeuzelijst **Verificatie servercertificaat**:

Optie	Beschrijving
Geen verificatie	Het servercertificaat kan altijd vertrouwd worden. De verificatie wordt niet uitgevoerd.
CA-cert.	De verificatiemethode voor het controleren van de CA-betrouwbaarheid van het servercertificaat, door gebruik te maken van het CA-certificaat dat werd verstrekt door de CA die het servercertificaat heeft ondertekend.
CA-cert. + server-id	De verificatiemethode om de algemene naam te controleren ¹ van het servercertificaat te controleren, naast de CA-betrouwbaarheid van het servercertificaat.

7. Klik op **Indienen** als u klaar bent met de configuratie.

Voor bedrade netwerken: na de configuratie sluit u uw apparaat aan op het netwerk met IEEE 802.1x-ondersteuning. Druk na enkele minuten het netwerkconfiguratie rapport af om de **<Wired IEEE 802.1x>**-status te controleren.

Optie	Beschrijving
Success	De bedrade IEEE 802.1x-functie is ingeschakeld en de verificatie is gelukt.
Failed	De bedrade IEEE 802.1x-functie is ingeschakeld; de verificatie is echter mislukt.
Off	De bedrade IEEE 802.1x-functie is niet beschikbaar.



Verwante informatie

- [IEEE 802.1x-verificatie voor uw netwerk gebruiken](#)

Gerelateerde onderwerpen:

- [Overzicht eigenschappen beveiligingscertificaten](#)
- [Certificaten configureren voor een veilig apparaat](#)

¹ De verificatie van de algemene naam vergelijkt de algemene naam van het servercertificaat met de tekenreeks die geconfigureerd werd voor het **Server-id**. Voor u deze methode gebruikt, neemt u contact op met uw systeembeheerder voor de algemene naam van het servercertificaat en configureert u vervolgens naast de CA-betrouwbaarheid van het servercertificaat ook de waarde voor **Server-id**.

IEEE 802.1x-verificatiemethodes

EAP-FAST

Cisco Systems, Inc. heeft Extensible Authentication Protocol-Flexible Authentication via Secured Tunneling (EAP-FAST) ontwikkeld dat gebruikmaakt van een gebruikers-ID en wachtwoord voor de verificatie, en van symmetrische sleutelalgoritmes voor het verkrijgen van een getunneld verificatieproces.

Het Brother-apparaat biedt ondersteuning voor de volgende interne verificatiemethoden:

- EAP-FAST/NONE
- EAP-FAST/MS-CHAPv2
- EAP-FAST/GTC

EAP-MD5 (bedraad netwerk)

Extensible Authentication Protocol-Message Digest Algorithm 5 (EAP-MD5) maakt gebruik van een gebruikers-ID en een wachtwoord voor vraag-antwoordverificatie.

PEAP

Protected Extensible Authentication Protocol (PEAP) is een versie van de EAP-methode die door Cisco Systems, Inc., Microsoft Corporation en RSA Security is ontwikkeld. PEAP maakt een versleutelde Secure Sockets Layer (SSL)/Transport Layer Security (TLS)-tunnel tussen een client en een verificatieserver voor de verzending van een gebruikers-ID en wachtwoord. PEAP zorgt voor een wederzijdse verificatie tussen de server en de client.

Het Brother-apparaat biedt ondersteuning voor de volgende interne verificatiemethoden:

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) werd ontwikkeld door Funk Software en Certicom. EAP-TTLS maakt een versleutelde SSL-tunnel naar PEAP tussen een client en een verificatieserver voor de verzending van een gebruikers-ID en wachtwoord. EAP-TTLS zorgt voor een wederzijdse verificatie tussen de server en de client.

Het Brother-apparaat biedt ondersteuning voor de volgende interne verificatiemethoden:

- EAP-TTLS/CHAP
- EAP-TTLS/MS-CHAP
- EAP-TTLS/MS-CHAPv2
- EAP-TTLS/PAP

EAP-TLS

Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) vereist verificatie van het digitale certificaat bij zowel een client als een verificatieserver.



Verwante informatie

- [IEEE 802.1x-verificatie voor uw netwerk gebruiken](#)