Handleiding beveiligingsfuncties

Inhoudsopgave

Inleiding

Definities van opmerkingen

In deze gebruikershandleiding worden de volgende symbolen en aanduidingen gebruikt:

BELANGRIJK	BELANGRIJK geeft een mogelijk gevaarlijke situatie aan die, als deze niet wordt voorkomen, schade aan eigendommen of verminderde functionaliteit van het product tot gevolg kan hebben.
OPMERKING	OPMERKING geeft informatie over de bedieningsomgeving, installatievoorwaarden of speciale gebruiksvoorwaarden.
	Onder pictogrammen van tips vindt u nuttige hints en extra informatie.
Vetgedrukt	Vetgedrukte tekst verwijst naar knoppen op het bedieningspaneel van het apparaat of het scherm van de computer.
Cursief	Italicized gedrukte tekst emphasizes een belangrijk punt of verwijst naar een verwant onderwerp.

Verwante informatie

- Inleiding

Handelsmerken

Adobe® en Reader® zijn gedeponeerde handelsmerken of handelsmerken van Adobe Systems Incorporated in de Verenigde Staten en/of andere landen.

Elk bedrijf waarvan de softwarenaam in deze handleiding is vermeld, beschikt over een softwareLicenseovereenkomst die specifiek is voor de eigen programma's.

Alle handels- en productnamen van bedrijven die vermeld zijn op Brother-producten, de bijbehorende documenten en andere materialen zijn handelsmerken of gedeponeerde handelsmerken van de respectieve bedrijven.

Verwante informatie

- Inleiding

Auteursrecht

Verwante informatie

- Inleiding

Voor u netwerkbeveiligingsfuncties gebruikt

Uw apparaat gebruikt enkele van de meest recente protocollen voor netwerkbeveiliging en -versleuteling. Deze netwerkfuncties kunnen worden geïntegreerd in uw algemene netwerkbeveiligingsplan om uw gegevens te helpen beschermen en unauthorized toegang tot het apparaat te verhinderen.

Het is raadzaam om de FTP- en TFTP-protocollen uit te schakelen. Toegang tot het apparaat via deze protocollen is niet veilig.

Verwante informatie

- Inleiding
  - Protocollen die niet nodig zijn uitschakelen

Protocollen die niet nodig zijn uitschakelen

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. Schakel het selectievakje van protocollen die u niet nodig hebt uit.
6. Klik op **Indienen**.
7. Start uw Brother-apparaat opnieuw op om de configuratie te activeren.

Verwante informatie

- Voor u netwerkbeveiligingsfuncties gebruikt

Netwerkbeveiliging

- Certificaten configureren voor een veilig apparaat
- SSL/TLS gebruiken
- SNMPv3 gebruiken
- IPsec gebruiken
- IEEE 802.1x-verificatie voor uw netwerk gebruiken

Certificaten configureren voor een veilig apparaat

U moet een certificaat configureren om uw netwerkapparaat 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 organization.

- 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 identificator 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 ondertekeningsverzoek (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 ondertekeningsverzoek (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 identificator 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 ondertekeningsverzoek (CSR) aanmaken en een certificaat van een certificeringsinstantie (CA) installeren

Een certificaat installeren op uw apparaat

Wanneer u een certificaat ontvangt van een certificeringinstantie (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 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. 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(Poort 443)** 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 unauthorized 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. Gebruik de SNMPv3-modus om de afdrukserver veilig te beheren.
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

IPsec gebruiken

Inleiding tot IPsec

IPsec (Internet Protocol Security) is een beveiligingsprotocol waarbij een optionele Internet Protocol-functie wordt gebruikt om gegevensmanipulatie te voorkomen en de vertrouwelijkheid te waarborgen van gegevens die als IP-pakketten worden verzonden. IPsec versleutelt gegevens die via een netwerk verstuurd worden, zoals afdrukgegevens die vanaf computers naar een printer worden verzonden. Aangezien de gegevens bij de netwerklaag versleuteld worden, maken programma's die een protocol van een hoger niveau toepassen gebruik van IPsec, zelfs als de gebruiker hiervan niet op de hoogte is.

IPsec ondersteunt de volgende functies:

- IPsec-verzendingen

  Conform de voorwaarden van de IPsec-instelling verzendt een met het netwerk verbonden computer gegevens naar en ontvangt hij gegevens van het opgegeven apparaat met behulp van IPsec. Wanneer apparaten met behulp van IPsec beginnen te communiceren, worden eerst sleutels uitgewisseld met Internet Key Exchange (IKE), en worden de gegevens vervolgens verzonden met behulp van deze sleutels.

  Daarnaast heeft IPsec twee bedieningsmodi: de transportmodus en de tunnelmodus. De modus Transport wordt voornamelijk gebruikt voor communicatie tussen apparaten, en de modus Tunnel wordt gebruikt in omgevingen zoals een Virtual Private Network (VPN).

  Voor IPsec-verzendingen dient aan de volgende voorwaarden te worden voldaan:
  - Er is een computer die kan communiceren via IPsec verbonden met het netwerk.
  - Uw apparaat is geconfigureerd voor IPsec-communicatie.
  - De computer die verbonden is met uw apparaat is geconfigureerd voor IPsec-verbindingen.

- IPsec-instellingen

  Dit zijn de instellingen die nodig zijn voor verbindingen via IPsec. Deze instellingen kunnen geconfigureerd worden met behulp van Beheer via een webbrowser.

  Om de IPsec-instellingen te configureren, moet u een browser gebruiken op een computer die met het netwerk is verbonden.

Verwante informatie

- IPsec gebruiken

IPsec configureren met Beheer via een webbrowser

Wat betreft voorwaarden voor IPsec-verbindingen zijn er twee **Sjabloon**-typen: **Adres** en **IPsec**. U kunt maximaal 10 verbindingsvoorwaarden configureren.

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** > **IPsec** in de linkernavigatiebalk.

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

5. Configureer de instellingen.

Optie	Beschrijving
Status	Hiermee schakelt u IPsec in of uit.
Onderhandelingsmodus	Selecteer **Onderhandelingsmodus** voor IKE Phase 1. IKE is een protocol dat wordt gebruikt voor het uitwisselen van versleutelingscodes voor het voeren van versleutelde communicatie via IPsec. In de **Normaal**-modus is de verwerkingssnelheid traag, maar is de beveiliging hoog. In de **Agressief**-modus is de verwerkingssnelheid hoger dan in de **Normaal**-modus, maar is de beveiliging lager.
Al het niet-IPsec-verkeer	Selecteer welke actie moet worden ondernomen voor niet-IPsec-pakketten. Wanneer u Web Services gebruikt, moet u **Toestaan** selecteren voor **Al het niet-IPsec-verkeer**. Als u **Verwijderen** selecteert, kunt u Web Services niet gebruiken.
Broadcast/Multicast negeren	Selecteer **Ingeschakeld** of **Uitgeschakeld**.
Protocol negeren	Vink de selectievakjes aan voor de gewenste optie of opties.
Regels	Vink het vakje **Ingeschakeld** aan om het sjabloon te activeren. Als u meerdere selectievakjes aanvinkt, hebben de selectievakjes met een lager cijfer voorrang als de aangevinkte selectievakjes in conflict zijn met elkaar. Klik op de overeenstemmende vervolgkeuzelijst om de **Adressjabloon** te selecteren die wordt gebruikt voor de IPsec-verbindingsvoorwaarden. Om een **Adressjabloon** toe te voegen, klikt u op **Sjabloon toevoegen**. Klik op de overeenstemmende vervolgkeuzelijst om de **IPsec-sjabloon** te selecteren die wordt gebruikt voor de IPsec-verbindingsvoorwaarden. Om een **IPsec-sjabloon** toe te voegen, klikt u op **Sjabloon toevoegen**.

6. Klik op **Indienen**.

   Als het apparaat opnieuw moet worden opgestart om de nieuwe instellingen te activeren, wordt het bevestigingsscherm voor het opnieuw opstarten weergegeven.

Als er een leeg item is in het sjabloon dat u in de tabel **Regels** heeft ingeschakeld, verschijnt er een foutmelding. Bevestig uw keuzes en klik opnieuw op **Indienen**.

Verwante informatie

- IPsec gebruiken

Gerelateerde onderwerpen:

- Certificaten configureren voor een veilig apparaat

Een IPsec-adressjabloon configureren 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. Klik op **Netwerk** > **Beveiliging** > **IPsec-adressjabloon** in de linkernavigatiebalk.

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

5. Klik op de **Verwijderen**-knop om een **Adressjabloon** te wissen. Wanneer een **Adressjabloon** in gebruik is, kan het niet worden gewist.
6. Klik op de **Adressjabloon** die u wilt aanmaken. De **IPsec-adressjabloon** verschijnt.
7. Configureer de instellingen.

Optie	Beschrijving
Naam sjabloon	Vul de naam voor de sjabloon in (max. 16 tekens).
Lokaal IP-adres	• **IP-adres** Geef het IP-adres op. Selecteer **Alle IPv4-adressen**, **Alle IPv6-adressen**, **Alle Link-local IPv6-adressen** of **Aangepast** uit de vervolgkeuzelijst. Als u in de vervolgkeuzelijst **Aangepast** selecteert, voert u in het tekstvak het IP-adres (IPv4 of IPv6) in. • **IP-adresbereik** Vul in de tekstvelden het eerste en laatste IP-adres voor het IP-adresbereik in. Als het begin- en eind-IP-adres niet standardized zijn voor IPv4 of IPv6 of als het eind-IP-adres lager ligt dan het beginadres, zal er zich een fout voordoen. • **IP-adres/voorvoegsel** Geef het IP-adres op met behulp van de CIDR-notatie. Bijvoorbeeld: 192.168.1.1/24 Omdat het voorvoegsel wordt opgegeven in de vorm van een 24-bits subnetmasker (255.255.255.0) voor 192.168.1.1, zijn de adressen 192.168.1.xxx geldig.
Extern IP-adres	• **Elk** Als u **Elk** selecteert, worden alle IP-adressen ingeschakeld. • **IP-adres** Voer het opgegeven IP-adres (IPv4 of IPv6) in het tekstvak in. • **IP-adresbereik** Voer het eerste en laatste IP-adres voor het IP-adresbereik in. Als het eerste en laatste IP-adres niet standardized zijn voor IPv4 of IPv6 of als het laatste IP-adres lager ligt dan het eerste adres, zal er zich een fout voordoen. • **IP-adres/voorvoegsel** Geef het IP-adres op met behulp van de CIDR-notatie.

Optie	Beschrijving
	Bijvoorbeeld: 192.168.1.1/24 Omdat het voorvoegsel wordt opgegeven in de vorm van een 24-bits subnetmasker (255.255.255.0) voor 192.168.1.1, zijn de adressen 192.168.1.xxx geldig.

8. Klik op **Indienen**.

Wanneer u de instellingen voor de momenteel gebruikte sjabloon wijzigt, moet u uw apparaat opnieuw opstarten om de configuratie te activeren.

Verwante informatie

- IPsec gebruiken

Een IPsec-sjabloon configureren 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. Klik op **Netwerk** > **Beveiliging** > **IPsec-sjabloon** in de linkernavigatiebalk.

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

5. Klik op de **Verwijderen**-knop om een **IPsec-sjabloon** te wissen. Wanneer een **IPsec-sjabloon** in gebruik is, kan het niet worden gewist.
6. Klik op de **IPsec-sjabloon** die u wilt aanmaken. Het scherm **IPsec-sjabloon** verschijnt. De configuratievelden verschillen op basis van de instellingen voor **Voorgeconfigureerde sjabloon gebruiken** en **Internet Key Exchange (IKE)** die u geselecteerd hebt.
7. Voer in het veld **Naam sjabloon** een naam in voor het sjabloon (max. 16 tekens).
8. Als u **Aangepast** selecteerde in de vervolgkeuzelijst **Voorgeconfigureerde sjabloon gebruiken**, selecteert u de **Internet Key Exchange (IKE)**-opties en vervolgens wijzigt u de instellingen indien nodig.
9. Klik op **Indienen**.

Verwante informatie

- IPsec gebruiken
  - IKEv1-instellingen voor een IPsec-sjabloon
  - IKEv2-instellingen voor een IPsec-sjabloon
  - Handmatige instellingen voor IPsec-sjabloon

IKEv1-instellingen voor een IPsec-sjabloon

Optie	Beschrijving
Naam sjabloon	Vul de naam voor de sjabloon in (max. 16 tekens).
Voorgeconfigureerde sjabloon gebruiken	Selecteer **Aangepast**, **Strenge beveiliging IKEv1** of **Gemiddelde beveiliging IKEv1**. De instelitems zijn verschillend afhankelijk van het geselecteerde sjabloon.
Internet Key Exchange (IKE)	IKE is een communicatieprotocol dat wordt gebruikt voor het uitwisselen van versleutelingscodes voor het voeren van versleutelde communicatie via IPsec. Om alleen voor dat ogenblik versleutelde communicatie te voeren, wordt het versleutelingsalgoritme dat vereist is voor IPsec bepaald en worden de versleutelingscodes gedeeld. Voor IKE worden de versleutelingscodes uitgewisseld met behulp van de Diffie-Hellman-methode voor code-uitwisseling, en wordt een versleutelde communicatie die beperkt is tot IKE gevoerd. Als u **Aangepast** selecteerde in **Voorgeconfigureerde sjabloon gebruiken**, selecteert u **IKEv1**.
Verificatietype	• **Diffie-Hellman-groep** Met deze code-uitwisselingsmethode kunnen geheime codes veilig uitgewisseld worden binnen een onbeveiligd netwerk. De Diffie-Hellman-methode voor code-uitwisseling maakt gebruik van een discreet logaritmeprobleem (geen versleutelde code) om open informatie, aangemaakt met behulp van een willekeurig getal en de geheime code, te verzenden en te ontvangen. Selecteer **Groep 1**, **Groep 2**, **Groep 5** of **Groep 14**. • **Versleuteling** Selecteer **DES**, **3DES**, **AES-CBC 128** of **AES-CBC 256**. • **Hekje** Selecteer **MD5**, **SHA1**, **SHA256**, **SHA384** of **SHA512**. • **Levensduur beveiligingskoppeling** Geef voor IKE de levensduur van de beveiligingskoppeling op. Vul de tijd (seconden) en het aantal kilobytes (KByte) in.
Encapsulation-beveiliging	• **Protocol** Selecteer **ESP**, **AH** of **AH+ESP**.

Optie	Beschrijving
	- ESP is een protocol voor het voeren van versleutelde communicatie via IPsec. Met ESP wordt de payload (gecommuniceerde inhoud) versleuteld en wordt extra informatie toegevoegd. Het IP-pakket bestaat uit de header en de versleutelde gegevens die na de header komen. Behalve de versleutelde gegevens bevat het IP-pakket tevens informatie met betrekking tot de versleutelingsmethode en de coderingssleutel, de verificatiegegevens enz. - AH is het onderdeel van het IPsec-protocol dat de afzender verifieert en manipulatie van de gegevens voorkomt (garandeert volledigheid van de gegevens). In het IP-pakket worden de gegevens onmiddellijk na de kop ingevoerd. Daarnaast bevatten de pakketten hash-waarden die berekend worden aan de hand van een vergelijking van de gecommuniceerde inhoud, geheime code enz. om vervalsing van de afzender en manipulatie van de gegevens te voorkomen. In tegenstelling tot bij ESP is de gecommuniceerde inhoud niet versleuteld en worden de gegevens verzonden en ontvangen als tekst zonder opmaak. • **Versleuteling (niet beschikbaar voor de optie AH)** Selecteer **DES**, **3DES**, **AES-CBC 128** of **AES-CBC 256**. • **Hekje** Selecteer **Geen**, **MD5**, **SHA1**, **SHA256**, **SHA384** of **SHA512**. **Geen** kan alleen geselecteerd worden wanneer **ESP** geselecteerd is bij **Protocol**. • **Levensduur beveiligingskoppeling** Geef de levensduur op voor de IKE SA. Voer de tijd (seconden) en het aantal kilobytes (KByte) in. • **Encapsulation-modus** Selecteer **Transport** of **Tunnel**. • **IP-adres externe router** Voer het IP-adres (IPv4 of IPv6) van de router op afstand in. Voer deze informatie alleen in wanneer de **Tunnel**-modus is geselecteerd. SA (Security Association) is een versleutelde communicatiemethode die gebruikmaakt van IPsec of IPv6 voor het uitwisselen en delen van informatie (bv. de versleutelingsmethode en -code) om een beveiligd communicatiekanaal te kunnen invoeren vooraleer de communicatie begint. SA kan ook verwijzen naar een virtueel versleuteld communicatiekanaal dat ingevoerd werd. De SA die gebruikt wordt voor IPsec bepaalt de versleutelingsmethode, wisselt de codes uit en voert wederzijdse verificatie uit overeenkomstig de IKE (Internet Key Exchange)-standaardprocedure. De SA wordt regelmatig geüpdatet.
Perfect Forward Secrecy (PFS)	PFS leidt codes niet af van eerdere codes die gebruikt werden voor het versleutelen van berichten. Als een sleutel die wordt gebruikt om een bericht te versleutelen bovendien is afgeleid van een hoofdsleutel, wordt die hoofdsleutel niet gebruikt om er andere sleutels van af te leiden. Dat betekent dat zelfs als een sleutel niet langer veilig is, de schade beperkt zal blijven tot de berichten die versleuteld werden met die sleutel. Selecteer **Ingeschakeld** of **Uitgeschakeld**.

Optie	Beschrijving
Verificatiemethode	Selecteer de verificatiemethode. Selecteer **Vooraf gedeelde sleutel** of **Certificaten**.
Vooraf gedeelde sleutel	Tijdens het versleutelen van communicatie wordt de coderingssleutel op voorhand via een ander kanaal uitgewisseld en gedeeld. Als u **Vooraf gedeelde sleutel** selecteerde voor de **Verificatiemethode**, voert u de **Vooraf gedeelde sleutel** in (max. 32 tekens). • **Lokaal/Type id/Id** Selecteer het ID-type van de afzender en voer vervolgens het ID in. Selecteer **IPv4-adres**, **IPv6-adres**, **FQDN**, **E-mailadres** of **Certificaat** als type. Als u **Certificaat** selecteert, voert u de algemene naam van het certificaat in het **Id**-veld in. • **Extern/Type id/Id** Selecteer het ID-type van de ontvanger en voer vervolgens het ID in. Selecteer **IPv4-adres**, **IPv6-adres**, **FQDN**, **E-mailadres** of **Certificaat** als type. Als u **Certificaat** selecteert, voert u de algemene naam van het certificaat in het **Id**-veld in.
Certificaat	Als u **Certificaten** selecteerde voor **Verificatiemethode**, selecteert u het certificaat. U kunt alleen de certificaten selecteren die werden aangemaakt met behulp van de pagina **Certificaat** van het beveiligingsconfiguratiescherm van Beheer via een webbrowser.

Verwante informatie

- Een IPsec-sjabloon configureren met Beheer via een webbrowser

IKEv2-instellingen voor een IPsec-sjabloon

Optie	Beschrijving
Naam sjabloon	Vul de naam voor de sjabloon in (max. 16 tekens).
Voorgeconfigureerde sjabloon gebruiken	Selecteer **Aangepast**, **Strenge beveiliging IKEv2** of **Gemiddelde beveiliging IKEv2**. De instelitems zijn verschillend afhankelijk van het geselecteerde sjabloon.
Internet Key Exchange (IKE)	IKE is een communicatieprotocol dat wordt gebruikt voor het uitwisselen van versleutelingscodes voor het voeren van versleutelde communicatie via IPsec. Om alleen voor dat ogenblik versleutelde communicatie te voeren, wordt het versleutelingsalgoritme dat vereist is voor IPsec bepaald en worden de versleutelingscodes gedeeld. Voor IKE worden de versleutelingscodes uitgewisseld met behulp van de Diffie-Hellman-methode voor code-uitwisseling, en wordt een versleutelde communicatie die beperkt is tot IKE gevoerd. Als u **Aangepast** selecteerde in **Voorgeconfigureerde sjabloon gebruiken**, selecteert u **IKEv2**.
Verificatietype	• **Diffie-Hellman-groep** Met deze code-uitwisselingsmethode kunnen geheime codes veilig uitgewisseld worden binnen een onbeveiligd netwerk. De Diffie-Hellman-methode voor code-uitwisseling maakt gebruik van een discreet logaritmeprobleem (geen versleutelde code) om open informatie, aangemaakt met behulp van een willekeurig getal en de geheime code, te verzenden en te ontvangen. Selecteer **Groep 1**, **Groep 2**, **Groep 5** of **Groep 14**. • **Versleuteling** Selecteer **DES**, **3DES**, **AES-CBC 128** of **AES-CBC 256**. • **Hekje** Selecteer **MD5**, **SHA1**, **SHA256**, **SHA384** of **SHA512**. • **Levensduur beveiligingskoppeling** Geef voor IKE de levensduur van de beveiligingskoppeling op. Vul de tijd (seconden) en het aantal kilobytes (KByte) in.
Encapsulation-beveiliging	• **Protocol** Selecteer **ESP**. ESP is een protocol voor het voeren van versleutelde communicatie via IPsec. Met ESP wordt de payload (gecommuniceerde inhoud) versleuteld en wordt extra informatie toegevoegd. Het IP-pakket bestaat uit de header en de versleutelde gegevens die na de header komen. Behalve de versleutelde gegevens bevat het IP-pakket tevens informatie met betrekking tot de versleutelingsmethode en de coderingssleutel, de verificatiegegevens enz. • **Versleuteling** Selecteer **DES**, **3DES**, **AES-CBC 128** of **AES-CBC 256**. • **Hekje** Selecteer **MD5**, **SHA1**, **SHA256**, **SHA384** of **SHA512**. • **Levensduur beveiligingskoppeling** Geef de levensduur op voor de IKE SA. Voer de tijd (seconden) en het aantal kilobytes (KByte) in. • **Encapsulation-modus** Selecteer **Transport** of **Tunnel**.

Optie	Beschrijving
	• **IP-adres externe router** Voer het IP-adres (IPv4 of IPv6) van de router op afstand in. Voer deze informatie alleen in wanneer de **Tunnel**-modus is geselecteerd. SA (Security Association) is een versleutelde communicatiemethode die gebruikmaakt van IPsec of IPv6 voor het uitwisselen en delen van informatie (bv. de versleutelingsmethode en -code) om een beveiligd communicatiekanaal te kunnen invoeren vooraleer de communicatie begint. SA kan ook verwijzen naar een virtueel versleuteld communicatiekanaal dat ingevoerd werd. De SA die gebruikt wordt voor IPsec bepaalt de versleutelingsmethode, wisselt de codes uit en voert wederzijdse verificatie uit overeenkomstig de IKE (Internet Key Exchange)-standaardprocedure. De SA wordt regelmatig geüpdatet.
Perfect Forward Secrecy (PFS)	PFS leidt codes niet af van eerdere codes die gebruikt werden voor het versleutelen van berichten. Als een sleutel die wordt gebruikt om een bericht te versleutelen bovendien is afgeleid van een hoofdsleutel, wordt die hoofdsleutel niet gebruikt om er andere sleutels van af te leiden. Dat betekent dat zelfs als een sleutel niet langer veilig is, de schade beperkt zal blijven tot de berichten die versleuteld werden met die sleutel. Selecteer **Ingeschakeld** of **Uitgeschakeld**.
Verificatiemethode	Selecteer de verificatiemethode. Selecteer **Vooraf gedeelde sleutel**, **Certificaten**, **EAP - MD5** of **EAP - MS-CHAPv2**. EAP is een verificatieprotocol dat een extensie is van PPP. Door EAP met IEEE802.1x te gebruiken, wordt er voor gebruikersverificatie en voor elke sessie een andere code gebruikt. De volgende instellingen zijn alleen nodig wanneer **EAP - MD5** of **EAP - MS-CHAPv2** zijn geselecteerd in **Verificatiemethode**: • **Modus** Selecteer **Servermodus** of **Clientmodus**. • **Certificaat** Selecteer het certificaat. • **Gebruikersnaam** Vul de gebruikersnaam in (maximaal 32 tekens). • **Wachtwoord** Vul het wachtwoord in (maximaal 32 tekens). Het wachtwoord moet ter bevestiging tweemaal worden ingevuld.
Vooraf gedeelde sleutel	Tijdens het versleutelen van communicatie wordt de coderingssleutel op voorhand via een ander kanaal uitgewisseld en gedeeld. Als u **Vooraf gedeelde sleutel** selecteerde voor de **Verificatiemethode**, voert u de **Vooraf gedeelde sleutel** in (max. 32 tekens). • **Lokaal/Type id/Id** Selecteer het ID-type van de afzender en voer vervolgens het ID in. Selecteer **IPv4-adres**, **IPv6-adres**, **FQDN**, **E-mailadres** of **Certificaat** als type. Als u **Certificaat** selecteert, voert u de algemene naam van het certificaat in het **Id**-veld in.

Optie	Beschrijving
	• **Extern/Type id/Id** Selecteer het ID-type van de ontvanger en voer vervolgens het ID in. Selecteer **IPv4-adres**, **IPv6-adres**, **FQDN**, **E-mailadres** of **Certificaat** als type. Als u **Certificaat** selecteert, voert u de algemene naam van het certificaat in het **Id**-veld in.
Certificaat	Als u **Certificaten** selecteerde voor **Verificatiemethode**, selecteert u het certificaat. U kunt alleen de certificaten selecteren die werden aangemaakt met behulp van de pagina **Certificaat** van het beveiligingsconfiguratiescherm van Beheer via een webbrowser.

Verwante informatie

- Een IPsec-sjabloon configureren met Beheer via een webbrowser

Handmatige instellingen voor IPsec-sjabloon

Optie	Beschrijving
Naam sjabloon	Vul de naam voor de sjabloon in (max. 16 tekens).
Voorgeconfigureerde sjabloon gebruiken	Selecteer **Aangepast**.
Internet Key Exchange (IKE)	IKE is een communicatieprotocol dat wordt gebruikt voor het uitwisselen van versleutelingscodes voor het voeren van versleutelde communicatie via IPsec. Om alleen voor dat ogenblik versleutelde communicatie te voeren, wordt het versleutelingsalgoritme dat vereist is voor IPsec bepaald en worden de versleutelingscodes gedeeld. Voor IKE worden de versleutelingscodes uitgewisseld met behulp van de Diffie-Hellman-methode voor code-uitwisseling, en wordt een versleutelde communicatie die beperkt is tot IKE gevoerd. Selecteer **Handmatig**.
Verificatiesleutel (ESP, AH)	Voer de **In/Uit**-waarden in. Deze instellingen zijn noodzakelijk wanneer **Aangepast** is geselecteerd voor **Voorgeconfigureerde sjabloon gebruiken**, **Handmatig** is geselecteerd voor **Internet Key Exchange (IKE)** en een andere instelling dan **Geen** is geselecteerd voor **Hekje** voor hoofdstuk **Encapsulation-beveiliging**. Het aantal tekens dat u kunt instellen, verschilt afhankelijk van de instelling die u hebt gekozen voor **Hekje** in het hoofdstuk **Encapsulation-beveiliging**. Als de lengte van de opgegeven verificatiesleutel verschilt van het geselecteerde hash-algoritme, treedt er een fout op. • **MD5**: 128 bit (16 byte) • **SHA1**: 160 bit (20 byte) • **SHA256**: 256 bit (32 byte) • **SHA384**: 384 bit (48 byte) • **SHA512**: 512 bit (64 bytes) Wanneer u de sleutel in ASCII-code opgeeft, zet de tekens dan tussen dubbele aanhalingstekens (").
Codesleutel (ESP)	Voer de **In/Uit**-waarden in. Deze instellingen zijn vereist wanneer **Aangepast** geselecteerd is bij **Voorgeconfigureerde sjabloon gebruiken**, **Handmatig** geselecteerd is bij **Internet Key Exchange (IKE)** en **ESP** geselecteerd is bij **Protocol** onder **Encapsulation-beveiliging**. Het aantal tekens dat u kunt instellen, verschilt afhankelijk van de instelling die u hebt gekozen voor **Versleuteling** in het hoofdstuk **Encapsulation-beveiliging**. Als de lengte van de opgegeven verificatiesleutel verschilt van het geselecteerde versleutelingsalgoritme, treedt er een fout op. • **DES**: 64 bit (8 byte) • **3DES**: 192 bit (24 byte) • **AES-CBC 128**: 128 bit (16 byte) • **AES-CBC 256**: 256 bit (32 byte) Wanneer u de sleutel in ASCII-code opgeeft, zet de tekens dan tussen dubbele aanhalingstekens (").
SPI	Deze parameters worden gebruikt om beveiligingsinformatie te identificeren. Over het algemeen heeft een host meerdere Security

Optie	Beschrijving
	Associations (SA's) voor verschillende types IPsec-communicatie. Daarom is het nodig de toepasselijke SA te identificeren wanneer er een IPsec-pakket ontvangen wordt. De SPI-parameter, die de SA identificeert, is inbegrepen in de Authentication Header (AH) en in de Encapsulating Security Payload (ESP)-header. Deze instellingen zijn noodzakelijk wanneer **Aangepast** is geselecteerd voor **Voorgeconfigureerde sjabloon gebruiken** en **Handmatig** is geselecteerd voor **Internet Key Exchange (IKE)**. Geef waarden op voor **In/Uit**. (3-10 tekens)
Encapsulation-beveiliging	• **Protocol** Selecteer **ESP** of **AH**. - ESP is een protocol voor het voeren van versleutelde communicatie via IPsec. Met ESP wordt de payload (gecommuniceerde inhoud) versleuteld en wordt extra informatie toegevoegd. Het IP-pakket bestaat uit de header en de versleutelde gegevens die na de header komen. Behalve de versleutelde gegevens bevat het IP-pakket tevens informatie met betrekking tot de versleutelingsmethode en de coderingssleutel, de verificatiegegevens enz. - AH is het onderdeel van het IPsec-protocol dat de afzender verifieert en manipulatie van de gegevens voorkomt (garandeert volledigheid van de gegevens). In het IP-pakket worden de gegevens onmiddellijk na de kop ingevoerd. Daarnaast bevatten de pakketten hash-waarden die berekend worden aan de hand van een vergelijking van de gecommuniceerde inhoud, geheime code enz. om vervalsing van de afzender en manipulatie van de gegevens te voorkomen. In tegenstelling tot bij ESP is de gecommuniceerde inhoud niet versleuteld en worden de gegevens verzonden en ontvangen als tekst zonder opmaak. • **Versleuteling (niet beschikbaar voor de optie AH)** Selecteer **DES**, **3DES**, **AES-CBC 128** of **AES-CBC 256**. • **Hekje** Selecteer **Geen**, **MD5**, **SHA1**, **SHA256**, **SHA384** of **SHA512**. **Geen** kan alleen geselecteerd worden wanneer **ESP** geselecteerd is bij **Protocol**. • **Levensduur beveiligingskoppeling** Geef de levensduur op voor de IKE SA. Voer de tijd (seconden) en het aantal kilobytes (KByte) in. • **Encapsulation-modus** Selecteer **Transport** of **Tunnel**. • **IP-adres externe router** Voer het IP-adres (IPv4 of IPv6) van de router op afstand in. Voer deze informatie alleen in wanneer de **Tunnel**-modus is geselecteerd.

Optie	Beschrijving
	SA (Security Association) is een versleutelde communicatiemethode die gebruikmaakt van IPsec of IPv6 voor het uitwisselen en delen van informatie (bv. de versleutelingsmethode en -code) om een beveiligd communicatiekanaal te kunnen invoeren vooraleer de communicatie begint. SA kan ook verwijzen naar een virtueel versleuteld communicatiekanaal dat ingevoerd werd. De SA die gebruikt wordt voor IPsec bepaalt de versleutelingsmethode, wisselt de codes uit en voert wederzijdse verificatie uit overeenkomstig de IKE (Internet Key Exchange)-standaardprocedure. De SA wordt regelmatig geüpdatet.

Verwante informatie

- Een IPsec-sjabloon configureren met Beheer via een webbrowser

IEEE 802.1x-verificatie voor uw netwerk gebruiken

Wat is IEEE 802.1x-verificatie?

IEEE 802.1x is een IEEE-standaard die de toegang van unauthorized 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).

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** in de linkernavigatiebalk.

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

5. 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)**.
6. 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 netwerkconfiguratierapport 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 tunneled 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

Gebruikersverificatie

- Active Directory-verificatie gebruiken
- LDAP-verificatie gebruiken
- Beveiligd functieslot 3.0 gebruiken

Active Directory-verificatie gebruiken

- Inleiding tot Active Directory-verificatie
- Active Directory-verificatie configureren met Beheer via een webbrowser
- Aanmelden om de instellingen van het apparaat te wijzigen via het bedieningspaneel van het apparaat (Active Directory-verificatie)

Inleiding tot Active Directory-verificatie

Met Verificatie actieve directory kunt u het gebruik van uw apparaat beperken. Wanneer Active Directory-verificatie ingeschakeld is, is het bedieningspaneel van het apparaat vergrendeld. U kunt de instellingen van het apparaat pas wijzigen als u een gebruikers-ID en wachtwoord invoert.

Active Directory-verificatie biedt de volgende functies:

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

- Binnenkomende afdrukgegevens opslaan
- Binnenkomende faxgegevens opslaan
- Verkrijgt het e-mailadres van de Active Directory op basis van uw gebruikers-ID tijdens het verzenden van gescande gegevens naar een e-mailserver.

  Om deze functie te gebruiken, selecteert u de optie **Aan** voor de instelling **E-mailadres ophalen** en verificatiemethode **LDAP + kerberos** of **LDAP + NTLMv2**. Uw e-mailadres wordt ingesteld als de afzender als het apparaat gescande gegevens naar een e-mailserver verzendt, of als de ontvanger als u de gescande gegevens naar uw e-mailadres wilt verzenden.

Wanneer Active Directory-verificatie ingeschakeld is, slaat uw apparaat alle binnenkomende faxgegevens op. Als u zich hebt aangemeld, drukt het apparaat alle opgeslagen faxgegevens af.

U kunt de instellingen voor Verificatie actieve directory wijzigen met Beheer via een webbrowser.

Verwante informatie

- Active Directory-verificatie gebruiken

Active Directory-verificatie configureren met Beheer via een webbrowser

Active Directory-verificatie biedt ondersteuning voor Kerberos-verificatie en NTLMv2-verificatie. U moet het SNTP-protocol (netwerktijdserver) en de DNS Server-configuratie configureren voor verificatie.

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 **Beheerder** > **Functie gebruikersbeperking** of **Beperkingsbeheer** in de linkernavigatiebalk.

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

5. Selecteer **Verificatie met Active Directory**.
6. Klik op **Indienen**.
7. Klik op **Verificatie met Active Directory**.
8. Configureer de volgende instellingen:

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

Optie	Beschrijving
Opslag fax-RX-gegevens	Selecteer deze optie om binnenkomende faxgegevens op te slaan. U kunt alle binnenkomende faxgegevens afdrukken nadat u zich hebt aangemeld bij het apparaat.
Gebruikers-ID onthouden	Selecteer deze optie om uw gebruikers-ID op te slaan.
Serveradres voor Active Directory	Voer het IP-adres of de servernaam (bijvoorbeeld: ad.voorbeeld.com) van de Active Directory-server in.
Active Directory-domeinnaam	Vul de Active Directory-domeinnaam in.
Protocol en verificatiemethode	Selecteer het protocol en de verificatiemethode.
SSL/TLS	Selecteer de optie **SSL/TLS**.
LDAP-serverpoort	Typ het poortnummer in om de Active Directory-server te verbinden via LDAP (alleen beschikbaar voor de verificatiemethode **LDAP + kerberos** of **LDAP + NTLMv2**).
LDAP-zoekbasis	Voer de LDAP-zoekroot in (alleen beschikbaar voor verificatiemethode **LDAP + kerberos** of **LDAP + NTLMv2**).

Optie	Beschrijving
E-mailadres ophalen	Selecteer deze optie om het aangemelde e-mailadres van de gebruiker te verkrijgen via de Active Directory-server. (alleen beschikbaar voor verificatiemethode **LDAP + kerberos** of **LDAP + NTLMv2**)
Basismap van gebruiker ophalen	Selecteer deze optie om de basismap op te halen die wordt gebruikt als bestemming van Scannen naar netwerk. (alleen beschikbaar voor verificatiemethode **LDAP + kerberos** of **LDAP + NTLMv2**)

9. Klik op **Indienen**.

Verwante informatie

- Active Directory-verificatie gebruiken

Aanmelden om de instellingen van het apparaat te wijzigen via het bedieningspaneel van het apparaat (Active Directory-verificatie)

Wanneer Active Directory-verificatie ingeschakeld is, is het bedieningspaneel van het apparaat vergrendeld tot u een gebruikers-ID en wachtwoord invoert via het bedieningspaneel van het apparaat.

1. Voer uw gebruikers-ID en wachtwoord in via het bedieningspaneel van het apparaat om u aan te melden.
2. Wanneer de verificatie gelukt is, wordt het bedieningspaneel van het apparaat ontgrendeld.

Verwante informatie

- Active Directory-verificatie gebruiken

LDAP-verificatie gebruiken

Inleiding tot LDAP-verificatie

Met LDAP-verificatie kunt u het gebruik van uw apparaat beperken. Wanneer LDAP-verificatie ingeschakeld is, is het bedieningspaneel van het apparaat vergrendeld. U kunt de instellingen van het apparaat pas wijzigen als u een gebruikers-ID en wachtwoord invoert.

LDAP-verificatie biedt de volgende functies:

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

- Binnenkomende afdrukgegevens opslaan
- Binnenkomende faxgegevens opslaan
- Verkrijgt het e-mailadres van de LDAP-server op basis van uw gebruikers-ID tijdens het verzenden van gescande gegevens naar een e-mailserver.

  Om deze functie te gebruiken, selecteert u de optie **Aan** voor de instelling **E-mailadres ophalen**. Uw e-mailadres wordt ingesteld als de afzender als het apparaat gescande gegevens naar een e-mailserver verzendt, of als de ontvanger als u de gescande gegevens naar uw e-mailadres wilt verzenden.

Wanneer LDAP-verificatie ingeschakeld is, slaat uw apparaat alle binnenkomende faxgegevens op. Als u zich hebt aangemeld, drukt het apparaat alle opgeslagen faxgegevens af.

U kunt de instellingen voor LDAP-verificatie wijzigen met Beheer via een webbrowser.

Verwante informatie

- LDAP-verificatie gebruiken

LDAP-verificatie configureren 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. Klik op **Beheerder** > **Functie gebruikersbeperking** of **Beperkingsbeheer** in de linkernavigatiebalk.

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

5. Selecteer **LDAP-authenticatie**.
6. Klik op **Indienen**.
7. Klik op het menu **LDAP-authenticatie**.
8. Configureer de volgende instellingen:

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

Optie	Beschrijving
Opslag fax-RX-gegevens	Selecteer deze optie om binnenkomende faxgegevens op te slaan. U kunt alle binnenkomende faxgegevens afdrukken nadat u zich hebt aangemeld bij het apparaat.
Gebruikers-ID onthouden	Selecteer deze optie om uw gebruikers-ID op te slaan.
Adres LDAP-server	Voer het IP-adres of de servernaam (bijvoorbeeld: ldap.voorbeeld.com) van de LDAP-server in.
SSL/TLS	Selecteer de optie **SSL/TLS** om LDAP over SSL/TLS te gebruiken.
LDAP-serverpoort	Vul het poortnummer van de LDAP-server in.
LDAP-zoekbasis	Voer de LDAP-zoekrootmap in.
Kenmerk van naam (Zoeksleutel)	Vul het kenmerk in dat u als zoeksleutel wilt gebruiken.
E-mailadres ophalen	Selecteer deze optie om het aangemelde e-mailadres van de gebruiker te verkrijgen via de LDAP-server.
Basismap van gebruiker ophalen	Selecteer deze optie om de basismap op te halen die wordt gebruikt als bestemming van Scannen naar netwerk.

9. Klik op **Indienen**.

Verwante informatie

- LDAP-verificatie gebruiken

Aanmelden om de instellingen van het apparaat te wijzigen via het bedieningspaneel van het apparaat (LDAP-verificatie)

Wanneer LDAP-verificatie ingeschakeld is, is het bedieningspaneel van het apparaat vergrendeld tot u een gebruikers-ID en wachtwoord invoert via het bedieningspaneel van het apparaat.

1. Voer uw gebruikers-ID en wachtwoord in via het bedieningspaneel van het apparaat om u aan te melden.
2. Wanneer de verificatie gelukt is, wordt het bedieningspaneel van het apparaat ontgrendeld.

Verwante informatie

- LDAP-verificatie gebruiken

Beveiligd functieslot 3.0 gebruiken

Beveiligd functieslot 3.0 verhoogt de beveiliging door te beperken welke functies op uw apparaat beschikbaar zijn.

Voor u Secure Function Lock 3.0 gebruikt

Gebruik Beveiligd functieslot om wachtwoorden te configureren, paginalimieten voor bepaalde gebruikers in te stellen en hun toegang te verlenen tot enkele of alle functies die hier worden vermeld.

U kunt de volgende instellingen voor Beveiligd functieslot 3.0 configureren of wijzigen met behulp van Beheer via een webbrowser:

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

- **Afdrukken**
- **Kopie**
- **Scannen**
- **Fax**
- **Media**
- **Web Connect**
- **Apps**
- **Paginalimiet**
- **Paginatellers**
- **Kaartnummer (NFC-ID)**

Modellen met touchscreen-LCD-scherm:

Wanneer Beveiligd functieslot ingeschakeld is, gaat het apparaat automatisch in de openbare modus en wordt een deel van de functionaliteit van het apparaat beperkt tot authorized gebruikers. Als u de beperkte functies van het apparaat wilt gebruiken, drukt op , waarna u uw gebruikersnaam selecteert en uw wachtwoord invoert.

Verwante informatie

- Beveiligd functieslot 3.0 gebruiken

Secure Function Lock 3.0 configureren 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. Klik op **Beheerder** > **Functie gebruikersbeperking** of **Beperkingsbeheer** in de linkernavigatiebalk.

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

5. Selecteer **Beveiligd functieslot**.
6. Klik op **Indienen**.
7. Klik op het menu **Beperkte functies**.
8. Configureer de instellingen om de beperkingen te beheren per gebruiker of groep.
9. Klik op **Indienen**.
10. Klik op het menu **Gebruikerslijst**.
11. Configureer de gebruikerslijst.
12. Klik op **Indienen**.

In het menu **Beveiligd functieslot** kunt u ook de instellingen voor het blokkeren van gebruikers instellen.

Verwante informatie

- Beveiligd functieslot 3.0 gebruiken

Scannen met Secure Function Lock 3.0

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

Scanbeperkingen opgeven (voor beheerders)

Met Beveiligd functieslot 3.0 kan een beheerder bepalen welke gebruikers mogen scannen. Als de scanfunctie is uitgeschakeld voor algemene gebruikers, hebben alleen gebruikers voor wie het selectievakje **Scannen** is ingeschakeld, het recht om te scannen.

De scanfunctie gebruiken (voor gebruikers met beperkte rechten)

- Scannen via het bedieningspaneel van het apparaat:

  Gebruikers met beperkte rechten moeten hun wachtwoord invoeren op het bedieningspaneel van het apparaat om de scanmodus te activeren.
- Scannen vanaf een computer:

  Gebruikers met beperkte rechten moeten hun wachtwoord invoeren op het bedieningspaneel van het apparaat voordat ze vanaf hun computer kunnen scannen. Als ze dit niet doen, wordt een foutmelding op het computerscherm weergegeven.

Als het apparaat chipkaartverificatie ondersteunt, hebben geregistreerde gebruikers ook toegang tot de scanmodus door het NFC-symbool op het bedieningspaneel van het apparaat aan te raken met hun chipkaart.

Verwante informatie

- Beveiligd functieslot 3.0 gebruiken

De openbare modus configureren voor Secure Function Lock 3.0

Gebruik het scherm Secure Function Lock om de openbare modus in te stellen. Deze modus beperkt welke functies beschikbaar zijn voor algemene gebruikers. Algemene gebruikers hoeven geen wachtwoord in te voeren om toegang te krijgen tot functies die via instellingen van openbare modus beschikbaar zijn.

Onder de openbare modus vallen ook afdruktaken die via Brother iPrint&Scan en Brother Mobile Connect worden verzonden.

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 **Beheerder** > **Functie gebruikersbeperking** of **Beperkingsbeheer** in de linkernavigatiebalk.

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

5. Selecteer **Beveiligd functieslot**.
6. Klik op **Indienen**.
7. Klik op het menu **Beperkte functies**.
8. Vink in de rij **Openbare modus** een selectievakje aan of uit om de weergegeven functie toe te staan of te beperken.
9. Klik op **Indienen**.

Verwante informatie

- Beveiligd functieslot 3.0 gebruiken

De instellingen van uw persoonlijke beginscherm configureren met Beheer via een webbrowser

Als beheerder kunt u aangeven welke tabbladen gebruikers kunnen weergeven op hun persoonlijke beginscherm. Via deze tabbladen hebben gebruikers snel toegang tot hun favorite snelkoppelingen. Deze kunnen zij met het bedieningspaneel van het apparaat toevoegen aan de tabbladen op hun persoonlijke beginscherm.

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

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 **Beheerder** > **Functie gebruikersbeperking** of **Beperkingsbeheer** in de linkernavigatiebalk.

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

5. Selecteer **Beveiligd functieslot**.
6. Selecteer **Tabinstellingen** in het veld **Persoonlijk** voor de namen van tabbladen die u wilt gebruiken op uw persoonlijke beginscherm.
7. Klik op **Indienen**.
8. Klik op het menu **Beperkte functies**.
9. Configureer de instellingen om de beperkingen te beheren per gebruiker of groep.
10. Klik op **Indienen**.
11. Klik op het menu **Gebruikerslijst**.
12. Configureer de gebruikerslijst.
13. Selecteer **Gebruikerslijst / Beperkte functies** in de vervolgkeuzelijst voor elke gebruiker.
14. Selecteer voor elke gebruiker de tabbladnaam in de vervolgkeuzelijst **Beginscherm**.
15. Klik op **Indienen**.

Verwante informatie

- Beveiligd functieslot 3.0 gebruiken

Extra functies van Secure Function Lock 3.0

Configureer de volgende functies in het scherm Secure Function Lock:

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

Alle tellers resetten

Klik op **Alle tellers resetten** in de kolom **Paginatellers** om de paginateller te resetten.

Exporteren als CSV-bestand

Klik op **Exporteren als CSV-bestand** om de teller voor de actuele pagina en de laatste pagina inclusief **Gebruikerslijst / Beperkte functies** als een CSV-bestand te exporteren.

Kaartnummer (NFC-ID)

Klik op het menu **Gebruikerslijst** en voer vervolgens de kaart-ID van een gebruiker in het veld **Kaartnummer (NFC-ID)** in. U kunt uw chipkaart gebruiken voor de verificatie.

Uitvoer

Als de postvakeenheid op het apparaat is geïnstalleerd, selecteert u de uitvoerlade voor elke gebruiker in de vervolgkeuzelijst.

Laatste tellerstand

Klik op **Laatste tellerstand** als u wilt dat de pagina de paginatelling onthoudt nadat de teller werd gereset.

Teller automatisch terugstellen

Klik op **Teller automatisch terugstellen** om het tijdsinterval voor het resetten van de paginateller te configureren. Kies een dagelijks, wekelijks of maandelijks interval.

Verwante informatie

- Beveiligd functieslot 3.0 gebruiken

Een nieuwe chipkaart registreren via het bedieningspaneel van het apparaat

U kunt chipkaarten registreren op uw apparaat.

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

1. Raak het NFC-symbool op het bedieningspaneel van het apparaat aan met een geregistreerde chipkaart.
2. Druk op uw gebruikers-ID op het LCD-scherm.
3. Druk op de knop Kaart registreren.
4. Raak het NFC-symbool aan met een nieuwe chipkaart.
   Het nummer van de nieuwe chipkaart wordt nu op het apparaat geregistreerd.
5. Druk op de knop OK.

Verwante informatie

- Beveiligd functieslot 3.0 gebruiken

Een externe IC-kaartlezer registreren

Als u een externe chipkaartlezer aansluit, gebruik dan Beheer via een webbrowser om de kaartlezer te registreren. Het apparaat ondersteunt externe IC-kaartlezers klasse HID.

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 **Beheerder** > **Externe kaartlezer** in de linkernavigatiebalk.

   Als de linkernavigatiebalk niet zichtbaar is, begint u te navigeren bij ☰.
5. Voer de benodigde informatie in en klik vervolgens op **Indienen**.
6. Start uw Brother-apparaat opnieuw op om de configuratie te activeren.
7. Sluit de kaartlezer aan op het apparaat.
8. Houd de chipkaart tegen de kaartlezer als verificatie.

Verwante informatie

- Beveiligd functieslot 3.0 gebruiken

E-mailberichten veilig verzenden of ontvangen

Het verzenden of ontvangen van e-mailberichten configureren met Beheer via een webbrowser

- E-mail ontvangen is slechts beschikbaar op specifieke modellen.
- U kunt het beste Beheer via een webbrowser gebruiken om het veilig verzenden van e-mail met gebruikersverificatie, of het verzenden en ontvangen van e-mail met SSL/TLS te configureren (alleen ondersteunde modellen).

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 in het veld **POP3/IMAP4/SMTP-client** op **Geavanceerde instellingen** en controleer of **POP3/IMAP4/SMTP-client** de status **Ingeschakeld** heeft.

- Welke protocollen beschikbaar zijn, kan per apparaat verschillen.
- Als het keuzescherm **Verificatiemethode** verschijnt, selecteert u uw verificatiemethode, waarna u de aanwijzingen op het scherm. volgt.

6. Configureer de **POP3/IMAP4/SMTP-client**-instellingen.
   - Controleer of de e-mailinstellingen juist zijn door na het configureren een test-e-mail te verzenden.
   - Raadpleeg uw netwerkbeheerder of internetprovider (ISP) als u niet weet wat de instellingen van de POP3-/IMAP4-/SMTP-server zijn.
7. Klik op **Indienen** wanneer u klaar bent.

   Het dialoogvenster **Configuratie voor e-mail verzenden/ontvangen testen** verschijnt.
8. Volg de instructies in het dialoogvenster om de huidige instellingen te testen.

Verwante informatie

- E-mailberichten veilig verzenden of ontvangen

Gerelateerde onderwerpen:

- E-mailberichten veilig verzenden of ontvangen met SSL/TLS

E-mailberichten verzenden met gebruikersverificatie

Uw apparaat verzendt e-mails via een e-mailserver die gebruikersverificatie vereist. Deze methode voorkomt dat unauthorized toegang krijgen tot de e-mailserver.

U kunt meldingen en rapporten verzenden per e-mail en u kunt internetfaxen (I-Fax) versturen (slechts beschikbaar op specifieke modellen) met gebruikersverificatie.

- Welke protocollen beschikbaar zijn, kan per apparaat verschillen.
- U kunt het beste Beheer via een webbrowser gebruiken om de SMTP-verificatie te configureren.

Instellingen van de e-mailserver

U moet de SMTP-verificatiemethode van uw apparaat instellen in overeenstemming met de verificatiemethode die door uw e-mailserver wordt gebruikt. Neem contact op met uw netwerkbeheerder of internetprovider (ISP) voor meer informatie over de instellingen van uw e-mailserver.

Om SMTP-serververificatie in te schakelen met Beheer via een webbrowser, selecteert u uw verificatiemethode onder **Serververificatiemethode** in het scherm **POP3/IMAP4/SMTP-client**.

Verwante informatie

- E-mailberichten veilig verzenden of ontvangen

E-mailberichten veilig verzenden of ontvangen met SSL/TLS

Uw apparaat ondersteunt SSL/TLS-communicatie. Om een e-mailserver te gebruiken die met SSL/TLS-communicatie werkt, moet u de volgende instellingen configureren.

- E-mail ontvangen is slechts beschikbaar op specifieke modellen.
- U kunt het beste Beheer via een webbrowser gebruiken om SSL/TLS te configureren.

Servercertificaat verifiëren

Als u onder **SSL/TLS** de optie **SSL** of **TLS** selecteert, wordt het selectievakje **Servercertificaat verifiëren** automatisch aangevinkt.

- 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.
- Als u het servercertificaat niet hoeft te verifiëren, schakelt u het selectievakje **Servercertificaat verifiëren** uit.

Poortnummer

Als u **SSL** of **TLS** selecteert, wordt de **Poort**-waarde afgestemd op het protocol. Als u het poortnummer handmatig wilt wijzigen, voert u het poortnummer in nadat u **SSL/TLS**-instellingen hebt geselecteerd.

U moet de communicatiemethode van uw apparaat instellen in overeenstemming met de methode die door uw e-mailserver wordt gebruikt. Neem contact op met uw netwerkbeheerder of internetprovider voor meer informatie over de instellingen van uw e-mailserver.

In de meeste gevallen zijn de volgende instellingen vereist voor de beveiligde webmailservices:

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

SMTP	**Poort**	587
	Serververificatiemethode	**SMTP-VERIF**
	SSL/TLS	**TLS**
POP3	**Poort**	995
	SSL/TLS	**SSL**
IMAP4	**Poort**	993
	SSL/TLS	**SSL**

Verwante informatie

- E-mailberichten veilig verzenden of ontvangen

Gerelateerde onderwerpen:

- Het verzenden of ontvangen van e-mailberichten configureren met Beheer via een webbrowser
- Certificaten configureren voor een veilig apparaat

Afdruklogboek op netwerk opslaan

Afdruklogboek opslaan in netwerkoverzicht

Met de functie Afdruklogboek op netwerk opslaan kunt u het bestand met het afdruklogboek van uw apparaat op een netwerkserver opslaan via Common Internet File System (CIFS). U kunt het ID, het type afdruktaak, de naam van de taak, de gebruikersnaam, de datum, de tijd en het aantal afgedrukte pagina's voor elke afdruktaak bijhouden. CIFS is een protocol dat werkt via TCP/IP en waarmee computers op een netwerk bestanden kunnen delen via een intranet of het internet.

De volgende afdrukfuncties worden bijgehouden in het afdruklogboek:

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

- Afdruktaken van uw computer
- Rechtstreeks afdrukken via USB
- Kopiëren
- Ontvangen fax
- Afdrukken met Web Connect

- De functie Afdruklogboek op netwerk opslaan ondersteunt Kerberos-verificatie en NTLMv2-verificatie. U moet het SNTP-protocol configureren (netwerktijdserver) of u moet de datum, tijd en tijdzone correct instellen met behulp van het bedieningspaneel voor verificatie.
- U kunt het bestandstype voor het opslaan van een bestand op de server instellen op TXT of CSV.

Verwante informatie

- Afdruklogboek op netwerk opslaan

De instellingen voor "Afdruklogboek op Netwerk opslaan" configureren 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. Klik op **Beheerder** > **Afdruklog op Netwerk opslaan** in de linkernavigatiebalk.

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

5. Klik in het veld **Afdrukrapport** op **Aan**.
6. Configureer de volgende instellingen:

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

Optie	Beschrijving
Netwerkmapnaam	Voer de bestemmingsmap in voor het opslaan van uw afdruklogboek op de CIFS-server (bijvoorbeeld: \\Computernaam\Gedeeldemap).
Bestandsnaam	Voer de bestandsnaam in die u wilt gebruiken voor het afdruklogboek (maximaal 32 tekens).
Bestandstype	Selecteer de optie **TXT** of **CSV** als bestandstype voor het afdruklogboek.
Tijdbron voor logboek	Selecteer de tijdbron voor het afdruklogboek.
Verificatiemethode	Selecteer de verificatiemethode voor toegang tot de CIFS-server: **Automatisch**, **Kerberos** of **NTLMv2**. Kerberos is een verificatieprotocol waarmee apparaten of individuen veilig hun identiteit kunnen aantonen aan netwerkservers zonder zich telkens opnieuw te moeten aanmelden. NTLMv2 is de verificatiemethode die wordt gebruikt door Windows om aan te melden bij servers. • **Automatisch**: als u **Automatisch** selecteert, wordt NTLMv2 gebruikt als verificatiemethode. • **Kerberos**: Selecteer de optie **Kerberos** om alleen Kerberos-verificatie te gebruiken. • **NTLMv2**: Selecteer de optie **NTLMv2** om alleen NTLMv2-verificatie te gebruiken. • Voor **Kerberos**- en **NTLMv2**-verificatie moet u ook de **Datum&tijd**-instellingen of het SNTP-protocol (netwerktijdserver) en de DNS-server configureren. • U kunt de datum en tijd ook via het bedieningspaneel van het apparaat configureren.

Optie	Beschrijving
Gebruikersnaam	Voer de gebruikersnaam in voor de verificatie (maximaal 96 tekens). Als de gebruikersnaam een onderdeel is van een domein, voert u de gebruikersnaam als volgt in: gebruiker@domein of domein\gebruiker.
Wachtwoord	Voer het wachtwoord in voor de verificatie (maximaal 32 tekens).
Kerberos-serveradres (indien nodig)	Voer het KDC-hostadres (Key Distribution Center) (bijvoorbeeld: kerberos.voorbeeld.com; tot 64 tekens) of het IP-adres (bijvoorbeeld: 192.168.56.189) in.
Instelling foutdetectie	Kies welke actie moet worden ondernomen wanneer het afdruklogboek niet op de server kan worden opgeslagen wegens een netwerkfout.

7. In het veld **Verbindingsstatus** controleert u de laatste logboekstatus.

U kunt ook de foutstatus controleren op de LCD van het apparaat.

8. Klik op **Indienen** om de pagina **Log afdrukken naar netwerk testen** weer te geven.

   Om uw instellingen te testen, klikt u op **Ja** en gaat u vervolgens naar de volgende stap.

   Klik op **Nee** om de test over te slaan. De instellingen worden automatisch ingediend.
9. Het apparaat test de instellingen.
10. Als de instellingen goedgekeurd zijn, wordt **Test OK** weergegeven op het scherm.

    Als **Testfout** weergegeven wordt, controleert u alle instellingen en klikt u op **Indienen** om de testpagina opnieuw weer te geven.

Verwante informatie

- Afdruklogboek op netwerk opslaan

De instelling voor foutdetectie van Afdruklogboek op netwerk opslaan

Gebruik de instellingen van foutdetectie om te selecteren welke actie er wordt ondernomen wanneer het afdruklogboek niet kan worden opgeslagen op de server wegens een netwerkfout.

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 **Beheerder** > **Afdruklog op Netwerk opslaan** in de linkernavigatiebalk.

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

5. Selecteer in het hoofdstuk **Instelling foutdetectie** de optie **Afdrukken annuleren** of **Log negeren en afdrukken**.

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

Optie	Beschrijving
Afdrukken annuleren	Als u de optie **Afdrukken annuleren** selecteert, worden de afdruktaken canceled wanneer het afdruklogboek niet kan worden opgeslagen op de server. Zelfs als u de optie **Afdrukken annuleren** selecteert, zal uw apparaat een ontvangen fax afdrukken.

Log negeren en afdrukken	Als u de optie **Log negeren en afdrukken** selecteert, drukt het apparaat het document af, ook al kan het afdruklogboek niet worden opgeslagen op de server.
	
	Wanneer de functie voor het opslaan van het afdruklogboek opnieuw werkt, wordt het afdruklogboek als volgt bijgehouden:
	
	`Id, Type, Job Name, User Name, Date, Time, Print Pages`
	`1, Print(xxxxxxx), "Document01.doc", "user01", 03/03/20xx, 14:01:32, 52`
	`2, Print(xxxxxxx), "Document02.doc", "user01", 03/03/20xx, 14:45:30, ?` (a)
	`3, <Error>, ?, ?, ?, ?, ?` (b)
	`4, Print(xxxxxxx), "Report01.xls", "user02", 03/03/20xx, 19:30:40, 4`
	
	a. Als het afdruklogboek niet kon worden opgeslagen na het afdrukken, wordt het aantal afgedrukte pagina's niet bijgehouden.
	b. Als het afdruklogboek niet kon worden opgeslagen voor en na het afdrukken, wordt het afdruklogboek van de afdruktaak niet bijgehouden. Wanneer de functie opnieuw werkt, wordt de fout weergegeven in het afdruklogboek.

6. Klik op **Indienen** om de pagina **Log afdrukken naar netwerk testen** weer te geven.

   Om uw instellingen te testen, klikt u op **Ja** en gaat u vervolgens naar de volgende stap.

   Klik op **Nee** om de test over te slaan. De instellingen worden automatisch ingediend.

7. Het apparaat test de instellingen.
8. Als de instellingen goedgekeurd zijn, wordt **Test OK** weergegeven op het scherm.

   Als **Testfout** weergegeven wordt, controleert u alle instellingen en klikt u op **Indienen** om de testpagina opnieuw weer te geven.

Verwante informatie

- Afdruklogboek op netwerk opslaan

"Afdruklogboek op netwerk opslaan" gebruiken met Secure Function Lock 3.0

Wanneer Secure Function Lock 3.0 (Beveiligd functieslot) geactiveerd is, worden de namen van de geregistreerde gebruikers voor de functies kopiëren, Fax RX, afdrukken met Web Connect en rechtstreeks afdrukken met USB bijgehouden in het rapport Afdruklogboek op netwerk opslaan. Wanneer Active Directory-verificatie is ingeschakeld, wordt de gebruikersnaam opgeslagen in het rapport Afdruklogboek op netwerk opslaan:

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

```
Id, Type, Job Name, User Name, Date, Time, Print Pages
1, Copy, -, -, 04/04/20xx, 09:05:12, 3
2, Fax, -, -, 04/04/20xx, 09:45:30, 5
3, Copy, -, "Bob", 04/04/20xx, 10:20:30, 4
4, Fax, -, "Bob", 04/04/20xx, 10:35:12, 3
5, USB Direct, -, "John", 04/04/20xx, 11:15:43, 6
```

Verwante informatie

- Afdruklogboek op netwerk opslaan

Brother Earth

www.brotherearth.com

DUT
Versie 0