Veiledning for nettverkssikkerhetsfunksjoner

Viktig sikkerhetsinformasjon

- Standardpassordet for å styre innstillingene på denne maskinen finner du under maskinen, angitt med "**Pwd:**". Vi anbefaler at du straks endrer standardpassordet for å beskytte maskinen mot uautorisert tilgang.
- Når du kobler maskinen til et eksternt nettverk, slik som Internett, er det viktig å beskytte nettverksmiljøet med en egen brannmur eller på andre måter for å forhindre lekkasje av informasjon som skyldes feil innstillinger eller uautorisert tilgang av tredjeparter med onde hensikter.
- Hvis det er et signal i nærheten, kan du fritt koble til LAN via trådløst LAN. Men dersom sikkerhetsinnstillingene ikke er riktig konfigurert, kan imidlertid signalet bli fanget opp av tredjeparter med onde hensikter, noe som kan føre til følgende:
  - Tyveri av personlig eller konfidensiell informasjon
  - Overføring av informasjon til feil parter som utgir seg for å være de aktuelle personene
  - Videresending av overført kommunikasjonsinnhold som ble fanget opp

Beslektet informasjon

- Nettverk

Konfigurere sertifikater for enhetssikkerhet

Du må konfigurere et sertifikat for å styre nettverksmaskinen på en sikker måte via SSL/TLS. Du må bruke Webbasert administrasjon til å konfigurere et sertifikat.

- Oversikt over funksjoner i sikkerhetssertifikat
- Slik lager og installerer du et sertifikat
- Lage et selvsignert sertifikat
- Opprette en forespørsel om sertifikatsignering (CSR) og installere et sertifikat fra en sertifiseringsinstans
- Importere og eksportere sertifikatet og privatnøkkelen
- Importere og eksportere et sertifikat fra en sertifiseringsinstans (CA-sertifikat)

Oversikt over funksjoner i sikkerhetssertifikat

Maskinen støtter bruk av flere sikkerhetssertifikater som muliggjør sikker pålitelighetskontroll og kommunikasjon med maskinen. Følgende funksjoner for sikkerhetssertifikater kan brukes med maskinen:

Støttede funksjoner, alternativer og innstillinger kan variere, avhengig av modellen din.

- SSL/TLS-kommunikasjon
- IEEE 802.1x-godkjenning
- IPsec

Maskinen støtter følgende:

- Forhåndsinstallert sertifikat

  Maskinen har et forhåndsinstallert selvsignert sertifikat. Med dette sertifikatet kan du bruke SSL/TLS-kommunikasjon uten å opprette eller installere et annet sertifikat.

Det forhåndsinstallerte egensignerte sertifikatet beskytter kommunikasjonen opp til et visst nivå. Vi anbefaler at du bruker et sertifikat som er utstedt av en klarert organisasjon for bedre sikkerhet.

- Selvsignert sertifikat

  Denne utskriftsserveren utsteder sitt eget sertifikat. Med dette sertifikatet kan du enkelt bruke SSL/TLS-kommunikasjon uten å opprette eller installere et annet sertifikat fra en sertifiseringsinstans (CA).
- Sertifikat fra en sertifiseringsinstans

  Du kan installere et sertifikat fra en sertifiseringsinstans på to måter. Hvis du allerede har et sertifikat fra en sertifiseringsinstans, eller hvis du vil bruke et sertifikat fra en eksternt klarert sertifiseringsinstans:
  - når du bruker en forespørsel om sertifikatsignering (CSR) fra denne utskriftsserveren.
  - når du importerer et sertifikat og en privatnøkkel.
- Sertifikat fra sertifiseringsinstans

  Når du skal bruke et CA-sertifikat som identifiserer sertifiseringsinstansen og eier privatnøkkelen sin, må du importere CA-sertifikatet fra sertifiseringsinstansen før du konfigurerer nettverkssikkerhetsfunksjoner.

- Hvis du skal bruke SSL/TLS-kommunikasjon, anbefaler vi at du først tar kontakt med systemadministrator.
- Når du tilbakestiller utskriftsserveren til standardinnstillingene fra fabrikken, slettes sertifikatet og privatnøkkelen som er installert. Hvis du vil beholde samme sertifikat og privatnøkkel etter at du har tilbakestilt utskriftsserveren, eksporterer du dem før tilbakestilling og installerer dem på nytt.

Beslektet informasjon

- Konfigurere sertifikater for enhetssikkerhet

Beslektede emner:

- Konfigurere IEEE 802.1x-pålitelighetskontroll for nettverket ditt ved hjelp av Webbasert administrasjon (webleser)

Slik lager og installerer du et sertifikat

Det er to alternativer når du velger et sikkerhetssertifikat: Bruk et selvsignert sertifikat eller bruk et sertifikat fra en sertifiseringsinstans.

Alternativ 1

Selvsignert sertifikat

1. Lag et selvsignert sertifikat med Webbasert administrasjon.
2. Installer det selvsignerte sertifikatet på datamaskinen.

Alternativ 2

Sertifikat fra en sertifiseringsinstans

1. Lag en forespørsel om sertifikatsignering (CSR) med Webbasert administrasjon.
2. Installer sertifikatet som er utstedt av sertifiseringsinstans på Brother-maskinen med Webbasert administrasjon.
3. Installer sertifikatet på datamaskinen.

Beslektet informasjon

- Konfigurere sertifikater for enhetssikkerhet

Lage et selvsignert sertifikat

1. Start nettleseren.
2. Skriv inn "https://maskinens IP-adresse" i nettleserens adressefelt (der "maskinens IP-adresse" er IP-adressen til maskinen din).

   Eksempel:

   https://192.168.1.2

   Maskinens IP-adresse finner du i nettverkskonfigurasjonsrapporten.
3. Hvis du blir bedt om det, skriver du inn passordet i feltet **Login (Pålogging)** og klikker deretter på **Login (Pålogging)**.

   Standardpassordet for å styre innstillingene på denne maskinen finner du bak på eller under maskinen, angitt med «**Pwd**». Endre standardpassordet ved å følge instruksjonene på skjermen når du logger på for første gang.
4. På venstre navigasjonslinje klikker du på **Network (Nettverk)** > **Security (Sikkerhet)** > **Certificate (Sertifikat)**.

   Hvis venstre navigasjonslinje ikke vises, starter du navigeringen fra ☰.
5. Klikk på **Create Self-Signed Certificate (Lag selvsignert sertifikat)**.
6. Angi et **Common Name (Fellesnavn)** og et **Valid Date (Gyldig dato)**.
   - Lengden på **Common Name (Fellesnavn)** er mindre enn 64 byte. Angi en identifikator som en IP-adresse, nodenavn eller domenenavn som skal brukes ved tilgang til maskinen gjennom SSL/TLS-kommunikasjon. Nodenavnet vises som standard.
   - En advarsel vises hvis du bruker IPPS- eller HTTPS-protokollen og oppgir et annet navn i URL-adressen enn **Common Name (Fellesnavn)** som ble brukt for det selvsignerte sertifikatet.
7. Velg innstillingen fra **Public Key Algorithm (Algoritme for fellesnøkkel)**-rullegardinlisten.
8. Velg innstillingen fra **Digest Algorithm (Sammendragalgoritme)**-rullegardinlisten.
9. Klikk på **Submit (Send inn)**.

Beslektet informasjon

- Konfigurere sertifikater for enhetssikkerhet

Opprette en forespørsel om sertifikatsignering (CSR) og installere et sertifikat fra en sertifiseringsinstans

Hvis du allerede har et sertifikat fra en eksternt klarert sertifiseringsinstans, kan du lagre sertifikatet og privatnøkkelen på maskinen og administrere dem med importering og eksportering. Hvis du ikke har et sertifikat fra en ekstern pålitelig sertifiseringsinstans, oppretter du en forespørsel om sertifikatsignering (CSR), sender den til en sertifiseringsinstans for godkjenning og installerer det returnerte sertifikatet på maskinen.

- Lage en forespørsel om sertifikatsignering (CSR)
- Installere et sertifikat på maskinen

Lage en forespørsel om sertifikatsignering (CSR)

En CSR (Certificate Signing Request – forespørsel om sertifikatsignering) er en forespørsel som er sendt til en sertifiseringsinstans for å utføre pålitelighetskontroll på berettigelsesbevisene som er i sertifikatet.

Vi anbefaler at du installerer et rotsertifikat fra sertifiseringsinstansen på datamaskinen før du oppretter CSR-en.

1. Start nettleseren.
2. Skriv inn "https://maskinens IP-adresse" i nettleserens adressefelt (der "maskinens IP-adresse" er IP-adressen til maskinen din).

   Eksempel:

   https://192.168.1.2

   Maskinens IP-adresse finner du i nettverkskonfigurasjonsrapporten.
3. Hvis du blir bedt om det, skriver du inn passordet i feltet **Login (Pålogging)** og klikker deretter på **Login (Pålogging)**.

   Standardpassordet for å styre innstillingene på denne maskinen finner du bak på eller under maskinen, angitt med «**Pwd**». Endre standardpassordet ved å følge instruksjonene på skjermen når du logger på for første gang.
4. På venstre navigasjonslinje klikker du på **Network (Nettverk)** > **Security (Sikkerhet)** > **Certificate (Sertifikat)**.

   Hvis venstre navigasjonslinje ikke vises, starter du navigeringen fra ☰.
5. Klikk på **Create CSR (Opprett CSR)**.
6. Skriv inn et **Common Name (Fellesnavn)** (kreves) og legg til annen informasjon om **Organization (Organisasjon)** (valgfritt).

   - Informasjon om bedriften din må angis slik at en sertifiseringsinstans kan bekrefte identiteten din overfor andre.
   - Lengden på **Common Name (Fellesnavn)** må være mindre enn 64 byte. Angi en identifikator som en IP-adresse, nodenavn eller domenenavn som skal brukes ved tilgang til maskinen gjennom SSL/TLS-kommunikasjon. Nodenavnet vises som standard. **Common Name (Fellesnavn)** er nødvendig.
   - En advarsel vises hvis du skriver inn et annet navn i URL-feltet enn fellesnavnet som ble brukt for sertifikatet.
   - Lengden på **Organization (Organisasjon)**, **Organization Unit (Organisasjonsenhet)**, **City/Locality (By/sted)** og **State/Province (Fylke/provins)** må være mindre enn 64 byte.
   - **Country/Region (Land/region)** bør være en ISO 3166-landskode bestående av to tegn.
   - Hvis du konfigurerer en X.509v3-sertifikatutvidelse, velger du **Configure extended partition (Konfigurer utvidet partisjon)**-avmerkingsboksen, og velger deretter **Auto (Register IPv4) (Auto (registrer IPv4))** eller **Manual (Manuell)**.
7. Velg innstillingen fra **Public Key Algorithm (Algoritme for fellesnøkkel)**-rullegardinlisten.
8. Velg innstillingen fra **Digest Algorithm (Sammendragalgoritme)**-rullegardinlisten.
9. Klikk på **Submit (Send inn)**.

   Forespørselen om sertifikatsignering (CSR) vises på skjermen. Lagre forespørselen om sertifikatsignering som en fil, eller kopier og lim inn den i et elektronisk skjema for forespørsel om sertifikatsignering som tilbys av en sertifiseringstinstans.
10. Klikk på **Lagre**.

- Følg sertifiseringstinstansens retningslinjer for hvilken metode du skal bruke til å sende en forespørsel om sertifikatsignering til sertifiseringstinstansen.
- Hvis du bruker Sertifiseringsinstans for organisasjonsrot i Windows Server, anbefaler vi at du bruker webserveren for sertifikatmalen når du oppretter klientsertifikatet på en sikker måte. Hvis du oppretter et klientsertifikat for et IEEE 802.1x-miljø med EAP-TLS-pålitelighetskontroll, anbefaler vi at du bruker Bruker for sertifikatmalen.

Beslektet informasjon

- Opprette en forespørsel om sertifikatsignering (CSR) og installere et sertifikat fra en sertifiseringsinstans

Installere et sertifikat på maskinen

Når du mottar et sertifikat fra en sertifiseringsinstans, følger du trinnene under for å installere det på utskriftsserveren:

> Kun et sertifikat som er utstedt med maskinens forespørsel om sertifikatsignering (CSR) kan installeres på maskinen. Hvis du vil opprette en annen forespørsel om sertifikatsignering, må du kontrollere at sertifikatet er installert før du oppretter det nye CSR. Du må kun opprette en annen forespørsel om sertifikatsignering etter at sertifikatet er installert på maskinen. Ellers vil en forespørsel om sertifikatsignering som ble opprettet før den nye forespørselen om sertifikatsignering, bli ugyldig.

1. Start nettleseren.
2. Skriv inn "https://maskinens IP-adresse" i nettleserens adressefelt (der "maskinens IP-adresse" er IP-adressen til maskinen din).

   Eksempel:

   https://192.168.1.2

   Maskinens IP-adresse finner du i nettverkskonfigurasjonsrapporten.
3. Hvis du blir bedt om det, skriver du inn passordet i feltet **Login (Pålogging)** og klikker deretter på **Login (Pålogging)**.

   Standardpassordet for å styre innstillingene på denne maskinen finner du bak på eller under maskinen, angitt med «**Pwd**». Endre standardpassordet ved å følge instruksjonene på skjermen når du logger på for første gang.
4. På venstre navigasjonslinje klikker du på **Network (Nettverk)** > **Security (Sikkerhet)** > **Certificate (Sertifikat)**.

   Hvis venstre navigasjonslinje ikke vises, starter du navigeringen fra ≡.
5. Klikk på **Install Certificate (Installer sertifikat)**.
6. Bla frem til filen som inneholder sertifikatet som utstedes av sertifiseringsinstansen, og klikk deretter på **Submit (Send inn)**.

   Sertifikatet er opprettet og lagret i minnet til maskinen.

For å bruke SSL/TLS-kommunikasjon må rotsertifikatet fra serifiseringsinstansen også installeres på datamaskinen. Kontakt nettverksadministratoren.

Beslektet informasjon

- Opprette en forespørsel om sertifikatsignering (CSR) og installere et sertifikat fra en sertifiseringsinstans

Importere og eksportere sertifikatet og privatnøkkelen

Lagre sertifikatet og privatnøkkelen på maskinen og styre dem ved å importere og eksportere.

- Importere et sertifikat og privatnøkkel
- Eksportere sertifikatet og privatnøkkelen

Importere et sertifikat og privatnøkkel

1. Start nettleseren.
2. Skriv inn "https://maskinens IP-adresse" i nettleserens adressefelt (der "maskinens IP-adresse" er IP-adressen til maskinen din).

   Eksempel:

   https://192.168.1.2

   Maskinens IP-adresse finner du i nettverkskonfigurasjonsrapporten.
3. Hvis du blir bedt om det, skriver du inn passordet i feltet **Login (Pålogging)** og klikker deretter på **Login (Pålogging)**.

Standardpassordet for å styre innstillingene på denne maskinen finner du bak på eller under maskinen, angitt med «**Pwd**». Endre standardpassordet ved å følge instruksjonene på skjermen når du logger på for første gang.

4. På venstre navigasjonslinje klikker du på **Network (Nettverk)** > **Security (Sikkerhet)** > **Certificate (Sertifikat)**.

Hvis venstre navigasjonslinje ikke vises, starter du navigeringen fra ☰.

5. Klikk på **Import Certificate and Private Key (Importer sertifikat og privatnøkkel)**.
6. Bla frem til og velg filen du vil importere.
7. Skriv inn passordet hvis filen er kryptert, og klikk deretter på **Submit (Send inn)**.

Sertifikatet og privatnøkkelen er importert til maskinen.

Beslektet informasjon

- Importere og eksportere sertifikatet og privatnøkkelen

Eksportere sertifikatet og privatnøkkelen

1. Start nettleseren.
2. Skriv inn "https://maskinens IP-adresse" i nettleserens adressefelt (der "maskinens IP-adresse" er IP-adressen til maskinen din).

   Eksempel:

   https://192.168.1.2

   Maskinens IP-adresse finner du i nettverkskonfigurasjonsrapporten.
3. Hvis du blir bedt om det, skriver du inn passordet i feltet **Login (Pålogging)** og klikker deretter på **Login (Pålogging)**.

   Standardpassordet for å styre innstillingene på denne maskinen finner du bak på eller under maskinen, angitt med «**Pwd**». Endre standardpassordet ved å følge instruksjonene på skjermen når du logger på for første gang.
4. På venstre navigasjonslinje klikker du på **Network (Nettverk)** > **Security (Sikkerhet)** > **Certificate (Sertifikat)**.

   Hvis venstre navigasjonslinje ikke vises, starter du navigeringen fra ☰.
5. Klikk på **Export (Eksporter)** som vises med **Certificate List (Sertifikatliste)**.
6. Skriv inn passordet hvis du vil kryptere filen.

   Hvis et tomt passord brukes, fungerer ikke krypteringen.
7. Skriv inn passordet igjen for å bekrefte, og klikk deretter på **Submit (Send inn)**.
8. Klikk på **Lagre**.

Sertifikatet og privatnøkkelen er eksportert til datamaskinen.

Du kan også importere sertifikatet til datamaskinen.

Beslektet informasjon

- Importere og eksportere sertifikatet og privatnøkkelen

Importere og eksportere et sertifikat fra en sertifiseringsinstans (CA-sertifikat)

Du kan importere, eksportere og lagre CA-sertifikater på Brother-maskinen.

- Importere et CA-sertifikat
- Eksportere et CA-sertifikat

Importere et CA-sertifikat

1. Start nettleseren.
2. Skriv inn "https://maskinens IP-adresse" i nettleserens adressefelt (der "maskinens IP-adresse" er IP-adressen til maskinen din).

   Eksempel:

   https://192.168.1.2

   Maskinens IP-adresse finner du i nettverkskonfigurasjonsrapporten.
3. Hvis du blir bedt om det, skriver du inn passordet i feltet **Login (Pålogging)** og klikker deretter på **Login (Pålogging)**.

Standardpassordet for å styre innstillingene på denne maskinen finner du bak på eller under maskinen, angitt med «**Pwd**». Endre standardpassordet ved å følge instruksjonene på skjermen når du logger på for første gang.

4. På venstre navigasjonslinje klikker du på **Network (Nettverk)** > **Security (Sikkerhet)** > **CA Certificate (CA-sertifikat)**.

Hvis venstre navigasjonslinje ikke vises, starter du navigeringen fra ☰.

5. Klikk på **Import CA Certificate (Importer CA-sertifikat)**.
6. Bla frem til filen som du vil importere.
7. Klikk på **Submit (Send inn)**.

Beslektet informasjon

- Importere og eksportere et sertifikat fra en sertifiseringsinstans (CA-sertifikat)

Eksportere et CA-sertifikat

1. Start nettleseren.
2. Skriv inn "https://maskinens IP-adresse" i nettleserens adressefelt (der "maskinens IP-adresse" er IP-adressen til maskinen din).

   Eksempel:

   https://192.168.1.2

   Maskinens IP-adresse finner du i nettverkskonfigurasjonsrapporten.
3. Hvis du blir bedt om det, skriver du inn passordet i feltet **Login (Pålogging)** og klikker deretter på **Login (Pålogging)**.

Standardpassordet for å styre innstillingene på denne maskinen finner du bak på eller under maskinen, angitt med «**Pwd**». Endre standardpassordet ved å følge instruksjonene på skjermen når du logger på for første gang.

4. På venstre navigasjonslinje klikker du på **Network (Nettverk)** > **Security (Sikkerhet)** > **CA Certificate (CA-sertifikat)**.

Hvis venstre navigasjonslinje ikke vises, starter du navigeringen fra ≡.

5. Velg sertifikatet du vil eksportere, og klikk på **Export (Eksporter)**.
6. Klikk på **Submit (Send inn)**.

Beslektet informasjon

- Importere og eksportere et sertifikat fra en sertifiseringsinstans (CA-sertifikat)

Bruke SSL/TLS

- Styre nettverksmaskinen på en sikker måte via SSL/TLS
- Skrive ut dokumenter på en sikker måte med SSL/TLS
- Sende eller motta e-post på en sikker måte med SSL/TLS

Styre nettverksmaskinen på en sikker måte via SSL/TLS

- Konfigurer et sertifikat for SSL/TLS og tilgjengelige protokoller
- Få tilgang til webbasert administrasjon med SSL/TLS
- Installere det selvsignerte sertifikatet for Windows-brukere som administrator
- Konfigurere sertifikater for enhetssikkerhet

Konfigurer et sertifikat for SSL/TLS og tilgjengelige protokoller

Konfigurer et sertifikat på maskinen via Webbasert administrasjon før du bruker SSL/TLS-kommunikasjon.

1. Start nettleseren.
2. Skriv inn "https://maskinens IP-adresse" i nettleserens adressefelt (der "maskinens IP-adresse" er IP-adressen til maskinen din).

   Eksempel:

   https://192.168.1.2

   Maskinens IP-adresse finner du i nettverkskonfigurasjonsrapporten.
3. Hvis du blir bedt om det, skriver du inn passordet i feltet **Login (Pålogging)** og klikker deretter på **Login (Pålogging)**.

   Standardpassordet for å styre innstillingene på denne maskinen finner du bak på eller under maskinen, angitt med «**Pwd**». Endre standardpassordet ved å følge instruksjonene på skjermen når du logger på for første gang.
4. På venstre navigasjonslinje klikker du på **Network (Nettverk)** > **Network (Nettverk)** > **Protocol (Protokoll)**.

   Hvis venstre navigasjonslinje ikke vises, starter du navigeringen fra ☰.
5. Klikk på **HTTP Server Settings (HTTP-serverinnstillinger)**.
6. Velg sertifikatet som du vil konfigurere fra rullegardinmenyen **Select the Certificate (Velg sertifikatet)**.
7. Klikk på **Submit (Send inn)**.
8. Klikk på **Yes (Ja)** for å starte utskriftsserveren på nytt.

Beslektet informasjon

- Styre nettverksmaskinen på en sikker måte via SSL/TLS

Beslektede emner:

- Skrive ut dokumenter på en sikker måte med SSL/TLS

Få tilgang til webbasert administrasjon med SSL/TLS

For sikker behandling av nettverksmaskinen må du bruke styringsverktøy med sikkerhetsprotokoller.

- For å bruke HTTPS-protokollen må HTTPS være aktivert på maskinen. HTTPS-protokollen er aktivert som standard.
- Du kan endre HTTPS-protokollinnstillingene med Internett-basert styring-skjermen.

1. Start nettleseren.
2. Skriv inn "https://maskinens IP-adresse" i nettleserens adressefelt (der "maskinens IP-adresse" er IP-adressen til maskinen din).

   Eksempel:

   https://192.168.1.2

   Maskinens IP-adresse finner du i nettverkskonfigurasjonsrapporten.
3. Hvis du blir bedt om det, skriver du inn passordet i feltet **Login (Pålogging)** og klikker deretter på **Login (Pålogging)**.

Standardpassordet for å styre innstillingene på denne maskinen finner du bak på eller under maskinen, angitt med «**Pwd**». Endre standardpassordet ved å følge instruksjonene på skjermen når du logger på for første gang.

4. Du har nå tilgang til maskinen med HTTPS.

Beslektet informasjon

- Styre nettverksmaskinen på en sikker måte via SSL/TLS

Installere det selvsignerte sertifikatet for Windows-brukere som administrator

- Følgende trinn er for Microsoft Edge. Hvis du bruker en annen nettleser, må du se i nettleserens dokumentasjon eller nettbaserte hjelp om hvordan du installerer sertifikater.
- Pass på at du har opprettet det selvsignerte sertifikatet med Webbasert administrasjon.

1. Høyreklikk på **Microsoft Edge**-ikonet og klikk deretter på **Kjør som administrator**.

   Hvis **Brukerkontokontroll** -skjermen kommer opp, klikk **Ja**.
2. Skriv inn "https://maskinens IP-adresse" i nettleserens adressefelt (der "maskinens IP-adresse" er IP-adressen til maskinen din).

   Eksempel:

   https://192.168.1.2

   Maskinens IP-adresse finner du i nettverkskonfigurasjonsrapporten.
3. Hvis tilkoblingen ikke er privat, klikker du på **Avansert**-knappen og fortsetter til nettsiden.
4. Hvis du blir bedt om det, skriver du inn passordet i feltet **Login (Pålogging)** og klikker deretter på **Login (Pålogging)**.

   Standardpassordet for å styre innstillingene på denne maskinen finner du bak på eller under maskinen, angitt med «**Pwd**». Endre standardpassordet ved å følge instruksjonene på skjermen når du logger på for første gang.
5. På venstre navigasjonslinje klikker du på **Network (Nettverk)** > **Security (Sikkerhet)** > **Certificate (Sertifikat)**.

   Hvis venstre navigasjonslinje ikke vises, starter du navigeringen fra ≡.
6. Klikk på **Export (Eksporter)**.
7. Hvis du vil kryptere utmatingsfilen, skriver du inn et passord i feltet **Enter password (Angi passord)**. Hvis **Enter password (Angi passord)**-feltet er tomt, krypteres ikke utmatingsfilen.
8. Skriv inn passordet igjen i **Retype password (Skriv inn passord på nytt)**-feltet, og klikk deretter på **Submit (Send inn)**.
9. Klikk på den nedlastede filen for å åpne den.
10. Når **Importveiviser for sertifikat** vises, klikker du på **Neste**.
11. Klikk på **Neste**.
12. Skriv om nødvendig inn et passord, og klikk deretter på **Neste**.
13. Velg **Plasser alle sertifikater i følgende lager**, og klikk deretter **Bla gjennom...**.
14. Velg **Klarerte rotsertifiseringsinstanser**, og klikk deretter på **OK**.
15. Klikk på **Neste**.
16. Klikk på **Fullfør**.
17. Klikk **Ja** hvis fingeravtrykket (tommelavtrykket) er korrekt.
18. Klikk på **OK**.

Beslektet informasjon

- Styre nettverksmaskinen på en sikker måte via SSL/TLS

Skrive ut dokumenter på en sikker måte med SSL/TLS

- Skriv ut dokumenter med IPPS
- Konfigurer et sertifikat for SSL/TLS og tilgjengelige protokoller
- Konfigurere sertifikater for enhetssikkerhet

Skriv ut dokumenter med IPPS

Bruk IPPS-protokollen til å skrive ut dokumenter sikkert med IPP-protokollen.

1. Start nettleseren.
2. Skriv inn "https://maskinens IP-adresse" i nettleserens adressefelt (der "maskinens IP-adresse" er IP-adressen til maskinen din).

   Eksempel:

   https://192.168.1.2

   Maskinens IP-adresse finner du i nettverkskonfigurasjonsrapporten.
3. Hvis du blir bedt om det, skriver du inn passordet i feltet **Login (Pålogging)** og klikker deretter på **Login (Pålogging)**.

   Standardpassordet for å styre innstillingene på denne maskinen finner du bak på eller under maskinen, angitt med «**Pwd**». Endre standardpassordet ved å følge instruksjonene på skjermen når du logger på for første gang.
4. På venstre navigasjonslinje klikker du på **Network (Nettverk)** > **Network (Nettverk)** > **Protocol (Protokoll)**.

   Hvis venstre navigasjonslinje ikke vises, starter du navigeringen fra ☰.
5. Kontroller at **IPP**-avmerkingsboksen er valgt.

   Hvis **IPP**-avmerkingboksen ikke er valgt, velg **IPP**-avmerkingsboksen og klikk på **Submit (Send inn)**.

   Start maskinen på nytt for å aktivere konfigurasjonen.

   Når maskinen starter på nytt, går du tilbake til maskinens nettside, skriver inn passordet og klikker på **Network (Nettverk)** > **Network (Nettverk)** > **Protocol (Protokoll)** på venstre navigasjonslinje.
6. Klikk på **HTTP Server Settings (HTTP-serverinnstillinger)**.
7. Merk av avkrysningsboksen **HTTPS** i **IPP**-området og klikk deretter på **Submit (Send inn)**.
8. Start maskinen på nytt for å aktivere konfigurasjonen.

Kommunikasjon med IPPS kan ikke forhindre uautorisert tilgang til utskriftsserveren.

Beslektet informasjon

- Skrive ut dokumenter på en sikker måte med SSL/TLS

Bruke SNMPv3

- Administrere nettverksmaskinen sikkert ved hjelp av SNMPv3

Administrere nettverksmaskinen sikkert ved hjelp av SNMPv3

Simple Network Management Protocol versjon 3 (SNMPv3) tilbyr brukerautentisering og datakryptering for å styre nettverksenheter på en trygg måte.

1. Start nettleseren.
2. Skriv inn "https://Common Name" i nettleserens adresselinje (hvor "Common Name" er fellesnavnet som du tilordnet sertifikatet. Dette kan være din IP-adresse, nodenavn eller domenenavn).
3. Hvis du blir bedt om det, skriver du inn passordet i feltet **Login (Pålogging)** og klikker deretter på **Login (Pålogging)**.

Standardpassordet for å styre innstillingene på denne maskinen finner du bak på eller under maskinen, angitt med «**Pwd**». Endre standardpassordet ved å følge instruksjonene på skjermen når du logger på for første gang.

4. På venstre navigasjonslinje klikker du på **Network (Nettverk)** > **Network (Nettverk)** > **Protocol (Protokoll)**.

Hvis venstre navigasjonslinje ikke vises, starter du navigeringen fra ≡.

5. Kontroller at **SNMP**-innstillingen er aktivert, og klikk deretter på **Advanced Settings (Avanserte innstillinger)**.
6. Konfigurer innstillingene for SNMPv1/v2x-modus.

Alternativ	Beskrivelse
SNMP v1/v2c read-write access (SNMP v1/v2c lese-skrve-tilgang)	Utskriftsserveren bruker versjon 1 og versjon 2c av SNMP-protokollen. Du kan bruke alle maskinens programmer i denne modusen. Modusen er derimot ikke sikker fordi den ikke vil autentisere brukeren og dataene krypteres ikke.
SNMP v1/v2c read-only access	Utskriftsserveren bruker skrivebeskyttet versjon 1 og versjon 2c av SNMP-protokollen.
Disabled (Deaktivert)	Deaktiver versjon 1 og versjon 2c av SNMP-protokollen. Alle programmer som bruker SNMPv1/v2c, vil være begrenset. Vil du tillate bruk av SNMPv1/v2c-programmer, bruker du modusen **SNMP v1/v2c read-only access** eller **SNMP v1/v2c read-write access (SNMP v1/v2c lese-skrve-tilgang)**.

7. Konfigurer innstillingene for SNMPv3-modus.

Alternativ	Beskrivelse
Enabled (Aktivert)	Utskriftsserveren bruker versjon 3 av SNMP-protokollen. Hvis du vil administrere utskriftsserveren på en sikker måte, bruker du SNMPv3-modus og konfigurerer deretter innstillingene.
Disabled (Deaktivert)	Deaktiver versjon 3 av SNMP-protokollen. Alle programmer som bruker SNMPv3, vil være begrenset. Hvis du vil tillate bruk av SNMPv3-programmer, bruker du SNMPv3-modus.

8. Klikk på **Submit (Send inn)**.

Hvis maskinen viser alternativene for protokollinnstillinger, velger du ønsket alternativ.

9. Start maskinen på nytt for å aktivere konfigurasjonen.

Beslektet informasjon

- Bruke SNMPv3

Bruke IEEE 802.1x-pålitelighetskontroll for nettverket ditt

- Hva er IEEE 802.1x-pålitelighetskontroll?
- Konfigurere IEEE 802.1x-pålitelighetskontroll for nettverket ditt ved hjelp av Webbasert administrasjon (webleser)
- IEEE 802.1x-pålitelighetskontrollmetoder

Hva er IEEE 802.1x-pålitelighetskontroll?

IEEE 802.1x er en IEEE-standard som begrenser tilgang fra uautoriserte nettverksenheter. Brother-maskinen sender en pålitelighetsforespørsel til en RADIUS-server (pålitelighetskontrollserver) gjennom tilgangspunktet eller huben. Når forespørselen din er blitt godkjent av RADIUS-serveren, kan maskinen få tilgang til nettverket.

Beslektet informasjon

- Bruke IEEE 802.1x-pålitelighetskontroll for nettverket ditt

Konfigurere IEEE 802.1x-pålitelighetskontroll for nettverket ditt ved hjelp av Webbasert administrasjon (webleser)

- Hvis du konfigurerer maskinen ved hjelp EAP-TLS-godkjenning, må du installere klientsertifikatet som er utstedt av en sertifikatinstans før du starter konfigurasjonen. Kontakt nettverksadministratoren om klientsertifikatet. Hvis du har installert mer enn ett sertifikat, anbefaler vi at du skriver ned sertifikatnavnet du vil bruke.
- Før du bekrefter serversertifikatet, må du importere CA-sertifikatet som ble utstedt av sertifiseringsinstansen som signerte serversertifikatet. Kontakt nettverksadministrator eller Internett-leverandøren for å bekrefte om det er nødvendig å importere et CA-sertifikat.

Du kan også konfigurere IEEE 802.1x-pålitelighetskontroll med veiviseren for trådløst oppsett via kontrollpanelet (trådløst nettverk).

1. Start nettleseren.
2. Skriv inn "https://maskinens IP-adresse" i nettleserens adressefelt (der "maskinens IP-adresse" er IP-adressen til maskinen din).

   Eksempel:

   https://192.168.1.2

   Maskinens IP-adresse finner du i nettverkskonfigurasjonsrapporten.
3. Hvis du blir bedt om det, skriver du inn passordet i feltet **Login (Pålogging)** og klikker deretter på **Login (Pålogging)**.

Standardpassordet for å styre innstillingene på denne maskinen finner du bak på eller under maskinen, angitt med «**Pwd**». Endre standardpassordet ved å følge instruksjonene på skjermen når du logger på for første gang.

4. På venstre navigasjonslinje klikker du på **Network (Nettverk)**.

Hvis venstre navigasjonslinje ikke vises, starter du navigeringen fra ≡.

5. Gjør ett av følgende:
   - For kablet nettverk

     Klikk på **Wired (Kablet)** > **Wired 802.1x Authentication (Kablet 802.1x-pålitelighetskontroll)**.
   - For trådløst nettverk

     Klikk på **Wireless (Trådløst)** > **Wireless (Enterprise) (Trådløs (bedrift))**.
6. Konfigurer IEEE 802.1x-pålitelighetskontrollinnstillingene.

- For å aktivere IEEE 802.1x-pålitelighetskontroll for kablet nettverk velger du **Enabled (Aktivert)** for **Wired 802.1x status (Kablet 802.1x-status)** på **Wired 802.1x Authentication (Kablet 802.1x-pålitelighetskontroll)**-siden.
- Hvis du bruker **EAP-TLS**-pålitelighetskontroll, må du velge klientsertifikatet som er installert (vises med sertifikatnavn) for verifisering fra **Client Certificate (Klientsertifikat)**-rullegardinmenyen.
- Hvis du velger **EAP-FAST**-, **PEAP**-, **EAP-TTLS**- eller **EAP-TLS**-pålitelighetskontroll, velg verifiseringsmetoden fra **Server Certificate Verification (Serversertifikatverifisering)**-rullegardinmenyen. Verifiser serversertifikatet ved hjelp av CA-sertifikatet, som er importert til maskinen på forhånd og utstedt av sertifiseringsinstansen som signerte serversertifikatet.

Velg én av følgende verifiseringsmetoder fra **Server Certificate Verification (Serversertifikatverifisering)**-rullegardinmenyen:

Alternativ	Beskrivelse
No Verification (Ingen bekreftelse)	Serversertifikatet kan alltid stoles på. Verifiseringen utføres ikke.
CA Cert. (CA-sert.)	Verifiseringsmetoden for å kontrollere CA-påliteligheten til serversertifikatet, ved hjelp av CA-sertifikatet som er utstedt av sertifikatinstansen som signerte server-sertifikatet.
CA Cert. + ServerID (CA-sert. + ServerID)	Verifiseringsmetoden for å kontrollere fellesnavnet [1]-verdien til serversertifikatet, i tillegg til CA-påliteligheten til serversertifikatet.

7. Når du er ferdig med konfigurasjonen, klikk på **Submit (Send inn)**.

   For kablede nettverk: Etter konfigurering, kobler du maskinen til det IEEE 802.1x-støttede nettverket. Etter noen minutter skriver du ut nettverksinnstillingsrapporten for å sjekke <**Wired IEEE 802.1x**>-statusen.

Alternativ	Beskrivelse
Success	Den kablede IEEE 802.1x-funksjonen er aktivert og pålitelighetskontrollen var vellykket.
Failed	Den kablede IEEE 802.1x-funksjonen er aktivert, men pålitelighetskontrollen mislyktes.
Off	Den kablede IEEE 802.1x-funksjonen er ikke tilgjengelig.

Beslektet informasjon

- Bruke IEEE 802.1x-pålitelighetskontroll for nettverket ditt

Beslektede emner:

- Oversikt over funksjoner i sikkerhetssertifikat
- Konfigurere sertifikater for enhetssikkerhet

1 Verifiseringen av fellesnavnet sammenligner fellesnavnet til serversertifikatet med tegnstrengen som er konfigurert for **Server ID (Server-ID)**. Før du bruker denne metoden, kontakter du systemadministratoren din om serversertifikatets fellesnavn og konfigurerer deretter **Server ID (Server-ID)**.

IEEE 802.1x-pålitelighetskontrollmetoder

EAP-FAST

Extensible Authentication Protocol-Flexible Authentication via Secured Tunneling (EAP-FAST) har blitt utviklet av Cisco Systems, Inc., som bruker en bruker-ID og et passord for pålitelighetskontroll samt symmetriske nøkkelalgoritmer for å oppnå en tunnelpålitelighetsprosess.

Brother-maskinen støtter følgende interne pålitelighetskontrollmetoder:

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

EAP-MD5 (kablet nettverk)

Extensible Authentication Protocol-Message Digest Algorithm 5 (EAP-MD5) bruker en bruker-ID og et passord for forespørsel/svar-godkjenning.

PEAP

PEAP (Protected Extensible Authentication Protocol) er en versjon av EAP-metoden som ble utviklet av Cisco Systems, Inc., Microsoft Corporation og RSA Security. PEAP oppretter en kryptert SSL-tunnel (Secure Sockets Layer) eller TLS-tunnel (Transport Layer Security) mellom en klient og en pålitelighetskontrollserver til sending av bruker-ID og passord. PEAP gir gjensidig pålitelighetskontroll mellom serveren og klienten.

Brother-maskinen støtter følgende interne pålitelighetskontrollmetoder:

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) er utviklet av Funk Software og Certicom. EAP-TTLS lager en lignende kryptert SSL-tunnel til PEAP, mellom en klient og en pålitelighetskontrollserver, for sending av en bruker-ID og et passord. EAP-TTLS gir gjensidig pålitelighetskontroll mellom serveren og klienten.

Brother-maskinen støtter følgende interne pålitelighetskontrollmetoder:

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

EAP-TLS

Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) krever pålitelighetskontroll av digitalt sertifikat både hos en klient og en pålitelighetskontrollserver.

Beslektet informasjon

- Bruke IEEE 802.1x-pålitelighetskontroll for nettverket ditt